Проф. А. К. СУШКЕВИЧ

ОСНОВЫ ВЫСШЕЙ АЛГЕБРЫ

ТРЕТЬЕ, ПЕРЕРАБОТАННОЕ
И ДОПОЛНЕННОЕ ИЗДАНИЕ

Цена 7 р. переплет 1 р. 50 к.

ОБЪЕДИНЕННОЕ НАУЧНО-ТЕХНИЧЕСКОЕ ИЗДАТЕЛЬСТВО НКТП СССР
ГЛАВНАЯ РЕДАКЦИЯ ТЕХНИКО-ТЕОРЕТИЧЕСКОЙ ЛИТЕРАТУРЫ
МОСКВА 1937 ЛЕНИНГРАД

Т-22-5-2
ТКК № 93

АННОТАЦИЯ

Курс высшей алгебры для университетов проф. А. К. Сушкевича хорошо известен по своим двум предыдущим изданиям. В настоящем третьем издании автор внес ряд исправлений и дополнений, а некоторые отделы существенно переработал. Книга разбита на 2 части.

Первая часть (гл. I–VIII) представляет собой основной курс высшей алгебры. Сюда входят комплексные числа, детерминанты, решение систем уравнений, алгебраическое решение уравнений 3-й и 4-й степеней. Основная теорема алгебры и общая проблема вычисления корней.

Вторая часть (гл. IX–XIV) содержит теорию матриц, теорию инвариантов и ковариантов, теорию групп, основы теории Галуа и введение в современную алгебру.

Книга является ценным пособием для студентов математиков. Она утверждена Наркомпросоы в качестве учебника для университетов.

ПРЕДИСЛОВИЕ К ТРЕТЬЕМУ ИЗДАНИЮ

Настоящее, третье издание моего учебника высшей алгебры значительно отличается от двух предыдущих его изданий. Первая часть (главы I – VIII) представляет собой основной курс высшей алгебры – до теории симметрических функций включительно: это – основы, включая сюда и основную теорему о существовании корня, и алгебраическое решение уравнений третьей и четвертой степеней и общую проблему вычисления корней. Вторая часть (главы IX – XIV) включает теорию матриц, теорию инвариантов, теорию групп, теорию Галуа и начала новой алгебры.

При подготовке этого, третьего издания я принял во внимание современные программы по алгебре наших университетов, а также те довольно многочисленные советы, указания, просьбы и даже жалобы на мой учебник, которые до меня дошли, и со стороны моих коллег по специальности, и со стороны моих нынешних и бывших учеников, и со стороны вообще преподающих и учащихся в вузах. Главная жалоба — та, что мой учебник слишком краток и сух, — что это скорее конспект, а не учебник, что поэтому он и труден для начинающих. Я вполне соглашаюсь с этим мнением и стараюсь в этом, третьем издании исправить указанный недостаток, но исправить его не так, как многие, может быть, ожидают. Дело в том, что я совсем не собираюсь разжевывать и класть в рот учащимся довольно элементарные вещи: по моему мнению, для учащихся будет только полезно, если они эту мою книгу прочтут не как легкий роман, а с некоторым трудом, с карандашом и бумагой в руках, другими словами, усвоят не «пассивно», а «активно». Поэтому «разжевывал» я только те места, которые уже действительно были весьма сжаты. Но зато я расширил или ввел заново места, разъясняющие значение вводимых или исследуемых понятий, дающие принципиальные установки или указывающие дальнейшие возможные обобщения. Я счел целесообразным уже с самого начала ознакомить читателя с основными понятиями новой алгебры; так, уже в конце главы I я ввожу понятия тела и области целости, а в главе II даю понятие группы. Эти понятия сами по себе ничего сложного не представляют, и чем раньше их себе усвоит учащийся, тем лучше.

Некоторые из моих коллег по специальности возражали против введения символа Кронекера в теории детерминантов, считая его слишком сложным для начинающих; было даже такое возражение, что символ этот «выхолащивает» содержание (?). Я никак не могу согласиться со всем этим и просто думаю, что в этих возражениях большую роль играет рутина, привычка преподавать так, а не иначе. Арабы в своей чисто риторической алгебре ввели даже особые названия «аль джебр» и «аль мукабала» для операций, которые для нас, с нашей развитой символикой, являются простыми следствиями одной общей и простой теоремы. И надо полагать, что Алькархи, который избегал употреблять даже индусские цифры,

вероятно, тоже находил, что они «выхолащивают» содержание. Во всяком случае я символ Кронекера оставляю, ибо нахожу, что этот, весьма удачный, символ придает четкость всем доказательствам и формулам теории детерминантов.

Укажу теперь конкретно на главнейшие изменения и дополнения в этом, третьем издании. Первая глава почти вся совершенно переработана, причем ей предпослана довольно обширная вводная часть, а в конце ее дается понятие о теле и об области целости. В главе II после перестановок дается сейчас же понятие о подстановках и о группе; в конце дана общая теория линейных уравнений, которая в предыдущих изданиях помещалась в начале главы VIII. Третья глава осталась почти без изменения. В главе IV выброшена теорема Вейерштрасса, весьма трудная для начинающих, и вследствие этого несколько изменен ход дальнейших доказательств; в конце этой главы помещена теорема о непрерывности корней как функций от коэфициентов, далее, в связи с этим, — понятие об алгебраических функциях, об алгебраических числах и общие замечания об основной теореме. В главе V вставлен параграф о сферических функциях, как пример ряда Штурма, полученного не при помощи Эвклидова алгорифма; значительно изменен и расширен отдел о вычислении корней: введен метод итерации и переработаны способы Горнера и Ньютона-Фурье, причем в последнем оказалось возможным отбросить условие, чтобы одновременно с функцией $f(x)$ ее две первые производные не обращались в нуль. Шестая глава дополнена: в конце включены понятия о функциях и уравнениях в каком-либо теле и о расширении тела. Седьмая глава есть объединение глав IX и X предыдущих изданий. Восьмая глава (в предыдущих изданиях – VII) трактует о симметрических функциях и их приложениях. Тут я вставил формулы Варинга, непосредственно выражающие суммы степеней через элементарные симметрические функции, и обратно, немного расширил параграф об обобщениях основной теоремы и добавил в конце главы общие замечания о функциях нескольких переменных.

Вторая часть содержит высшие отделы алгебры, которые только теперь начинают входить в общеобязательный курс высшей алгебры математических факультетов наших университетов, хотя эти отделы, как, например, теория матриц, теория инвариантов, теория групп, уже давно зарекомендовали себя большими приложениями как в самой математике, так и вне ее.

По сравнению с предыдущими изданиями моего курса высшей алгебры, во вторую часть вошел материал глав VIII, XI и XII этих изданий, при этом в значительно расширенном виде. Так, вместо одной главы VIII даются две главы (и, кроме того, общая теория линейных уравнений отошла к главе II первой части) — теория матриц и теория инвариантов и ковариантов. Теория матриц (глава IX) значительно расширена: введены ортогональные матрицы, элементарные делители и т. п. Все эти вещи в настоящее время являются совершенно необходимым математическим багажом для каждого математика. Теорию инвариантов можно излагать весьма разнообразными способами. Я в своем изложении придерживался книги Dickson'a «Höhere Algebra», у нас мало распространенной, но — с моей точки зрения — весьма хороша и систематично излагающей главу об инвариантах.

Расширена также глава XI (теория групп); глава XII (теория Галуа) осталась почти без изменения. Затем добавлены еще две главы, которых не было в предыдущих изданиях: глава XIII, трактующая о некоторых специальных типах уравнений (в частности об уравнениях деления окружности и о метациклических

уравнениях) и являющаяся продолжением теории Галуа, и глава XIV, озаглавленная: «Введение в новую алгебру». Здесь я вкратце указываю на дальнейшее развитие современной алгебры: даю основы абстрактной теории тел, упоминаю о кольцах и о гиперкомплексных числах. Эту последнюю главу я рассматриваю как первое введение к изучению современных монографий по алгебре, в первую очередь — книги Ван-дер-Вардена «Современная алгебра».

А. Сушкевич.

30/IX-1935 г.

ОГЛАВЛЕНИЕ

ГЛАВА VIII

СИММЕТРИЧЕСКИЕ ФУНКЦИИ

ЧАСТЬ ВТОРАЯ

ГЛАВА IX

ТЕОРИЯ МАТРИЦ

ГЛАВА X

ИНВАРИАНТЫ И КОВАРИАНТЫ

ГЛАВА XI

ТЕОРИЯ ГРУПП

ГЛАВА XII

ОСНОВЫ ТЕОРИИ ГАЛУА

ГЛАВА XIII

НЕКОТОРЫЕ ЧАСТНЫЕ ВИДЫ УРАВНЕНИЙ

ГЛАВА XIV

ВВЕДЕНИЕ В НОВУЮ АЛГЕБРУ

Ч А С Т Ь
П Е Р В А Я

ГЛАВА ПЕРВАЯ

КОМПЛЕКСНЫЕ ЧИСЛА

§ 1. Введение. Мы начинаем наш курс высшей алгебры с теории *комплексных чисел*, ибо вся так называемая «классическая алгебра» оперирует именно с ними, рассматривая *вещественные* (или *действительные*) числа только как частный случай комплексных, ее даже называют теперь «алгеброю комплексных чисел» — в отличие от новых обобщений алгебры (например, алгебра матриц, алгебры различных систем гиперкомплексных чисел).

Комплексные числа встречаются уже в элементарной алгебре при извлечении корня четной степени из отрицательного числа и при решении квадратных уравнений, но систематической их теории там не дается. Вводится просто новое число $i = \sqrt{-1}$, далее, извлекают квадратные корни из любого отрицательного числа следующим образом:

$$\sqrt{-a^2} = \sqrt{a^2 \cdot (-1)} = \sqrt{a^2} \cdot \sqrt{-1} = \pm ai.$$

Числа такого вида, как ai (где a — вещественное, т. е. обычное, целое или дробное, положительное или отрицательное, рациональное или иррациональное число), называются «*мнимыми*» или точнее, «чисто мнимыми». Квадратные уравнения приводят к числам вида $a + bi$, где a и b вещественные числа, эти числа $a + bi$ называются «*комплексными*» (т. е. составными). Элементарная алгебра оперирует с этими числами как с обычными суммами, складывая, вычитая, умножая и деля их по обычным своим правилам, принимая во внимание только, что $i^2 = -1$, но не заботясь о том, имеем ли мы право так оперировать с ними. Вот этот вопрос мы теперь и должны выяснить, но сначала выясним, что значит в данном случае «иметь право».

Прежде всего заметим, что название «мнимое число» (которое с частного случая чисел вида bi распространяется вообще на все комплексные числа) неудачно и имеет только историческое оправдание: эти «мнимые», или комплексные числа, так же как и «вещественные», или «действительные», выражают количественные соотношения между нещами или явлениями в действительном мире, и в этом смысле они ничуть не менее «действительны», чем «действительные» числа. Подтверждением этому могут служить широкие применения теории функций комплексного переменного в современной электротехнике, гидро- и аэродинамике и других областях современной техники. С точки зрения отвлеченной математики теория комплексных чисел представляет собой стройную логическую систему, не имеющую внутренних противоречий и не стоящую в противоречии с теорией вещественных — чисел, наоборот, дополняющую эту последнюю.

Но исторически дело сложилось так, что к понятию об этих «мнимых» числах пришли довольно отвлеченным путем (именно, через вопрос о корнях квадратных из отрицательных чисел), причем конкретно этот «мнимый» ответ указывал на невозможность задачи; поэтому эти числа и назвали «невозможными» (impossibiles); название «мнимые» числа (imaginarius) появилось в первой половине XVII в., наконец, название «комплексные» числа ввел Гаусс (Gauss) в первой половине XIX в.

Что касается невозможности многих конкретных задач с ответом в виде комплексного числа, то этому не следует удивляться: комплексные числа, как более сложные, входят, так сказать, «в свои права» при более сложных количественных соотношениях реальной действительности, при более простых соотношениях они просто не нужны. Заметим, что ведь и отрицательный ответ часто указывает на невозможность конкретной задачи, мало того, в зависимости от условий конкретной задачи и дробный ответ (например дробное число людей), даже и целый положительный ответ (например 25 часов в сутки) могут оказаться невозможными.

Укажу еще на одну особенность комплексных чисел, которая их в некотором роде противопоставляет вещественным числам: все вещественные (целые, дробные, — положительные и отрицательные, — рациональные и иррациональные) числа представляются, как известно, точками на прямой линии (при произвольном выборе начальной точки O и масштаба — единицы длины, а также положительного направления), причем эти точки, представляющие вещественные числа, заполняют всю прямую; комплексным числам на ней места нет. Для геометрического представления комплексных чисел необходимы два измерения (см. ниже, § 10).

§ 2. Алгебра рассматривает числа как объекты счета, т. е. как объекты действий над ними; определить числа данного вида или типа значит дать правила, по которым мы сможем производить наши действия над всякими числами этого типа. Но эти правила не независимы друг от друга: одни логически вытекают из других; нам достаточно положить в основу логически независимые друг от друга правила, как постулаты («требования»), выводя из них дальнейшие законы действий над нашими числами уже дедуктивным путем. Алгебра рассматривает два основных действия: сложение и умножение; вычитание и деление рассматриваются как обратные действия к сложению и умножению. Следовательно, при построении теории комплексных чисел мы должны дать, как основные постулаты, правила их сложения и их умножения. Но кроме этого мы должны ввести еще один постулат, именно, мы должны условиться, какие комплексные числа мы будем считать равными друг другу. С первого взгляда этот постулат кажется излишним: очевидно, что *равными* мы считаем числа, которые действительно одинаковы; но вот здесь-то в более сложных случаях и могут возникнуть трудности: даже в области обычных дробей трудно с первого взгляда убедиться в том, что, например, дроби $\frac{91}{221}$ и $\frac{21}{51}$ одинаковы.

Примечание 1. Понятие о равенстве принадлежит к так называемым понятиям о соотношении между данными объектами; оно подчиняется трем основным законам:

1) *закон симметрии*: если $a = b$, то и $b = a$;

2) *закон транзитивности*: если $a = b$ и $b = c$, то $a = c$;

3) *закон рефлексивности*: $a = a$.

При всяком определении равенства следует проверять выполнение этих законов.

В области вещественных чисел, кроме соотношения равенства, есть еще соотношение *упорядоченности* («неравенства»): если a и b два различных числа (т. е. a не равно b, или $a \neq b$), то или $a > b$ (a «больше» b), или $b > a$ (иначе: $a < b$, или «меньше» b); это соотношение подчиняется закону транзитивности: если $a > b$ и $b > c$, то и $a > c$. В области комплексных чисел этого соотношения упорядоченности не устанавливается, что стоит в тесной связи с тем, что комплексные числа не представляются как точки на одной прямой. Были попытки искусственно установить и для комплексных чисел соотношения «больше» и «меньше», но эти попытки не получили всеобщего признания.

Примечание 2. Устанавливаемые для определения данной системы чисел (например в нашем случае — комплексных чисел) постулаты равенства, сложения и умножения *a priori* как будто совершенно произвольны; но по существу в выборе их мы руководствуемся тем, что дает и подсказывает нам практика. Так, выставленные в следующем параграфе постулаты явились результатом довольно длительной чисто эмпирической практики счета с комплексными числами, — счета, который давал хорошие результаты. Только после этого под этот счет был подведен теоретический фундамент, и на его основе вторично, уже чисто логически проверены законность и правильность всей этой практики.

Впрочем в более отвлеченных главах математики встречаются случаи построения систем на основе постулатов, как будто произвольных, непосредственно практикой не подсказываемых; примером могут служить различные системы гиперкомплексных чисел. Цель таких построений — более глубокое изучение уже имеющихся объектов и их возможных обобщений; и здесь «произвольность» — только кажущаяся: она диктуется уже имеющимися в наличии законами, как непосредственное их обобщение или видоизменение.

Примечание 3. В качестве «основных действий в алгебре мы назвали сложение и умножение. Может возникнуть вопрос: почему мы умалчиваем о третьем «прямом» действии — возвышении в степень, Дело в том, что в своем самом общем виде (начиная со случая иррационального показателя) оно уже выходит за пределы алгебры и определяется на основе теории показательной функции. Степень же с рациональным показателем легко сводится к произведению, частному или обычному извлечению корня. Обычное же извлечение корня есть частный случай решения так называемых алгебраических уравнений, а последнее составляет основной отдел всякой алгебры.

§ 3. Определение и основные действия с комплексными числами. Мы вводим новый символ i [1], определяя его следующим образом:

$$i^2 = -1. \tag{1}$$

[1]Обозначение i ввел Гаусс; i — начальная буква латинского слова imaginarius или французского слова imaginaire (мнимый).

(1) Как известно, нет такого вещественного числа, квадрат которого был бы равен -1, так что, вводя этот символ i, мы тем самым уже расширяем нашу область чисел. Далее, мы рассматриваем символические суммы

$$a + bi,$$

где a и b — всевозможные вещественные числа. Заметим, что и «сложение» и «умножение» в этом выражении пока что чисто символические: мы не только не можем фактически b умножить на i и произведение это прибавить к a, но и не знаем даже, что это значит. Условимся писать:

$$\text{при } \ b = 0 \qquad a + 0i = a, \tag{2}$$

$$\text{при } \ a = 0 \qquad 0 + bi = bi, \tag{3}$$

$$\text{при } \ a = b = 0 \qquad 0 + 0i = 0. \tag{4}$$

Эти символические суммы $a+bi$ мы и называем *комплексными числами*: частный их случай (3), т. е. числа bi, мы называем *чисто мнимыми*. Формулы (2) и (4) показывают, что мы рассматриваем вещественные числа — в частности и нуль — как частные случаи комплексных чисел. Законность такого рассмотрения выявится из дальнейшего.

«Оживим» теперь введенные комплексные числа, определив их равенство и действия над ними следующими постулатами:

I. *Постулат равенства.* Комплексные числа равны тогда и только тогда, если отдельно равны их вещественные и мнимые части (т. е. вещественные множители при i), или: $a + bi = c + di$ тогда и только тогда, если $a = c$ и $b = d$. Отсюда и из (4) получаем, в частности: $a + bi = 0$ тогда и только тогда, если $a = b = 0$.

II. *Постулат сложения.* Чтобы сложить два комплексных числа, надо отдельно сложить их вещественные части и соответственно коэфициенты при i или

$$(a + bi) + (c + di) = (a + c) + (b + d)i. \tag{5}$$

III. *Постулат умножения.* Два комплексных числа перемножаются как обычные двучлены с последующим приведением подобных членов, причем принимается во внимание формула (1), или

$$(a + bi)(c + di) = (ac - bd) + (bc + ad)i. \tag{6}$$

Примечание. Выставленный здесь постулат I формулируется еще так: между числами 1 и i не существует линейной зависимости с вещественными коэфициентами. Этот постулат в сущности утверждает, что число i не равно никакому вещественному числу.

Из принятых постулатов непосредственно выводим следующее:

1. Сложение и умножение нескольких комплексных чисел производится по тем же (выраженным в постулатах II и III) правилам, что и для двух чисел.

2. Для сложения и для умножения верен коммутативный закон:

$$\alpha + \beta = \beta + \alpha; \qquad \alpha\beta = \beta\alpha \ ^{2}$$

[2]Греческими буквами мы обозначаем в этой главе сокращенно комплексные числа.

3. Для сложения и для умножения верен ассоциативный закон:

$$(\alpha+\beta)+\gamma=\alpha+(\beta+\gamma); \qquad (\alpha\beta)\gamma=\alpha(\beta\gamma)\ ^{3},$$

поэтому можно писать и без скобок $\alpha+\beta+\gamma$, $\alpha\beta\gamma$.

4. Из двух предыдущих законов вытекает общее следствие для случая нескольких слагаемых (сомножителей): слагаемые (сомножители) можно как угодно переставлять или соединять в какие угодно группы; от этого величина суммы (произведения) не изменится.

5. Для сложения и умножения верен дистрибутивный закон:

$$(\alpha+\beta)\gamma=\alpha\gamma+\beta\gamma\ ^{4}.$$

Он непосредственно обобщается и на сумму нескольких слагаемых.

Далее, из него следует:

6. Правило умножения сумм (многочленов) и его частные случаи, включая формулу бинома Ньютона и формулу степени многочлена.

7. Число $0+0i$, которое мы в (4) обозначили через 0, действительно играет роль нуля для сложения и умножения:

$$\alpha+0=\alpha, \qquad \alpha\cdot 0=0.$$

8. Сложение и умножение чисел вида $a+0\cdot i$ сводятся к сложению и умножению их вещественных частей a; это оправдывает формулу (2), отожествляющую такие числа с вещественными.

9. Из постулата III следует:

$$(a+bi)c=ac+bci;$$

отсюда при $a=0$ имеем $bi\cdot c=bci$; обозначая $1i=i$, имеем $i\cdot b=bi$.

10. Из постулата II, а также из п.п. 2, 9 и формул (2), (3) следует:

$$(a+0i)+(0+bi)=(0+bi)+(a+0i)=a+bi=bi+a=a+ib,$$

т. е. комплексное число $a+bi$ действительно можно рассматривать как обычную сумму вещественного числа a и чисто мнимого числа bi, которое в свою очередь есть обычное произведение вещественного числа b на «мнимую единицу» i. Таким образом вначале чисто условное обозначение комплексного числа в виде суммы теперь получило свое оправдание.

11. Отметим еще такие формулы, непосредственно получающиеся из постулатов II и III:

$$bi+di=(b+d)i, \qquad bi\cdot di=-bd.$$

§ 4. Рассмотрим теперь обратные действия — вычитание и деление. *Вычитание* есть действие, обратное сложению; следовательно, если дано

$$(a+bi)-(c+di)=x+yi,$$

[3]Для сложения это следует непосредственно из постулата II; для умножения при выводе требуются несложные выкладки; предлагаем читателям проделать их для упражнения.

[4]Предлагаем читателям вывести эту формулу из постулатов II и III.

то это значит, что

$$a + bi = (c + di) + (x + yi);$$

применяя сюда постулаты II и I, получим:

$$a + bi = (c + x) + (d + y)i,$$

т. е. $a = c + x$, $b = d + y$, и, следовательно:

$$(a + bi) - (c + di) = (a - c) + (b - d)i. \tag{7}$$

Таким образом и тут верно обычное правило вычитания двучленов.

Если $\alpha = a + bi$, то обозначим:

$$-\alpha = -a - bi;$$

это число называется *противоположным* к α. Отметим еще следующие формулы:

12. $\alpha - \beta = \alpha + (-\beta)$, т. е. вычитание сводится к прибавлению противоположного числа.

13. $\alpha - \beta = 0$ тогда и только тогда, если $\alpha = \beta$;

$$\alpha + (-\alpha) = 0, \qquad \alpha - 0 = \alpha.$$

14. Правило знаков при умножении:

$$(-\alpha)\beta = \alpha(-\beta) = -\alpha\beta, \qquad (-\alpha)(-\beta) = \alpha\beta.$$

Это проверяется непосредственно на основании постулата III.

Из самого определения вычитания следует, что оно всегда (т. е. над всякими двумя числами) выполнимо и однозначно. Это выражают, говоря, что действие сложения неограниченно и однозначно обратимо, или что для сложения верны законы неограниченной обратимости и однозначной обратимости.

§ 5. Деление есть действие, обратное умножению; следовательно, если дано

$$\frac{a + bi}{c + di} = x + yi,$$

то это значит, что

$$a + bi = (c + di)(x + yi);$$

применяя постулаты III и I, получим:

$$a + bi = (cx - dy) + (dx + cy) \cdot i,$$

т. е.

$$cx - dy = a, \qquad dx + cy = b;$$

это — система двух линейных уравнений с двумя неизвестными x и y; решая их, найдем:

$$x = \frac{ac + bd}{c^2 + d^2}, \qquad y = \frac{bc - ad}{c^2 + d^2},$$

и, следовательно:

$$\frac{a+bi}{c+di} = \frac{ac+bd}{c^2+d^2} + \frac{bc-ad}{c^2+d^2}\,i. \tag{8}$$

Эта формула имеет смысл всегда при $c^2+d^2 \neq 0$; но c^2+d^2, как сумма квадратов вещественных чисел, тогда и только тогда обращается в нуль, если и $c=0$ и $d=0$, т. е. $c+di=0$. Отсюда следует, что деление комплексных чисел всегда выполнимо и однозначно, если только делитель не равен нулю. Иными словами, *умножение неограниченно и однозначно обратимо, если только сомножители отличны от нуля.*

Отметим еще следующие формулы:

15. $\dfrac{a+bi}{c} = \dfrac{a}{c} + \dfrac{b}{d}i$;

16. $\dfrac{bi}{di} = \dfrac{b}{d}$ и вообще $\dfrac{\alpha\gamma}{\beta\gamma} = \dfrac{\alpha}{\beta}$, т. е. дроби с комплексными членами можно сокращать как обычные вещественные дроби.

17. Правило знаков при делении:

$$\frac{-\alpha}{\beta} = \frac{\alpha}{-\beta} = -\frac{\alpha}{\beta}, \qquad \frac{-\alpha}{-\beta} = \frac{\alpha}{\beta}.$$

18.

$$\frac{1}{c+di} == \frac{c}{c^2+d^2} - \frac{d}{c^2+d^2}\,i = \frac{c-di}{c^2+d^2}.$$

Число $\dfrac{1}{c+di}$ называется *обратным* к $c+di$; оно существует для всякого $c+di$, отличного от нуля.

19. $\dfrac{\alpha}{\beta} = \alpha \cdot \dfrac{1}{\beta}$, т. е. деление сводится к умножению на число, обратное делителю.

Число $c-di$ называется *сопряженным* с $c+di$; вообще два комплексных числа сопряжены, если они различаются только знаком у мнимой части; иными словами, свойство сопряженности взаимное: число $c+di$ сопряжено с $c-di$. Вещественное число сопряжено с самим собой; чисто мнимое число bi сопряжено со своим противоположным $-bi$.

По формуле (6) непосредственно находим:

$$(c+di)(c-di) = c^2+d^2, \tag{9}$$

т. е. произведение двух взаимно сопряженных чисел есть вещественное положительное число; оно называется *нормой* числа $c+di$ (а также и числа $c-di$). Норма вещественного числа a есть a^2.

Легко видеть, что правую часть формулы (8) можно получить путем умножения числителя и знаменателя левой части на число, сопряженное со знаменателем. Действительно

$$\frac{(a+bi)(c-di)}{(c+di)(c-di)} = \frac{(ac+bd)+(bc-ad)i}{c^2+d^2} = \frac{ac+bd}{c^2+d^2} + \frac{bc-ad}{c^2+d^2}\,i,$$

а отсюда следует, что деление сводится к освобождению знаменателя (делителя) от мнимой части, совершенно аналогичное освобождению знаменателя от иррациональности, рассматриваемому в элементарной алгебре.

Далее, из формулы (8) получаем: если $a+bi=0$, т. е. $a=b=0$, и $c+di\neq 0$, то и частное $\dfrac{a+bi}{c+di}=0$, ибо тогда $ac+bd=0$ и $bc-ad=0$. Иными словами, если произведение двух сомножителей равно нулю, а один из сомножителей не равен нулю, то другой сомножитель обязательно должен быть равен нулю. Отсюда следует:

Произведение двух или нескольких сомножителей равно нулю тогда и только тогда, если по крайней мере один из сомножителей равен нулю.

Это — очень важный закон умножения, так называемый *закон об отсутствии нулевых делителей.*

Таким образом мы видим, что для четырех рациональных действий (т. е. для сложения, вычитания, умножения и деления) над комплексными числами остаются в силе все основные законы этих действий над вещественными числами, а следовательно, и все следствия из них; поэтому мы имеем право во всех алгебраических формулах, куда входят только рациональные действия, давать буквам и комплексные значения: от этого формулы не теряют своей силы.

Отметим еще такие формулы:

$$\begin{array}{ccccc} i^3=i^2\cdot i=-i, & & i^4=(i^2)^2=+1, & & i^5=i^4\cdot i=i, \\ i^6=i^4\cdot i^2=i^2=-1, & & i^7=i^4\cdot i^3=-i, & & i^8=+1 \qquad \text{и т. д.;} \end{array}$$

вообще, все степени i являются повторениями четырех чисел $i, -1, -i, +1$ в периодическом порядке.

Далее

$$(a+bi)^2=(a^2-b^2)+2abi. \tag{10}$$

§ 6. Извлечение квадратного корня. Пусть нам дано

$$\sqrt{a+bi}=x+yi;$$

возвышая обе части в квадрат, найдем [по формуле (10)]:

$$a+bi=(x^2-y^2)+2xyi;$$

отсюда по постулату I получаем два уравнения для x и y:

$$x^2-y^2=a, \qquad 2xy=b. \tag{11}$$

Для решения этой системы уравнений второй степени возвышаем обе части каждого уравнения в квадрат и затем складываем:

$$(x^2-y^2)^2+4x^2y^2=(x^2+y^2)^2=a^2+b^2;$$

отсюда

$$x^2=y^2=\sqrt{a^2+b^2},$$

причем корень следует брать положительный, ибо x и y вещественны, а следовательно, $x^2+y^2>0$.

Теперь из уравнений

$$x^2+y^2=\sqrt{a^2+b^2}, \qquad x^2-y^2=a$$

находим:

$$x^2 = \frac{1}{2}(a + \sqrt{a^2 + b^2}), \qquad y = \frac{1}{2}(-a + \sqrt{a^2 + b^2}).$$

Для x и y получаем по два значения, а это дает четыре комбинации (x, y); но второе из равенств (11) говорит, что знак у xy должен быть тот же, что и знак у b, т. е. при $b > 0$ x и y должны иметь одинаковые знаки, а при $b < 0$ x и y должны иметь разные знаки. Это дает всего две комбинации (x, y) и, следовательно, два корня; если $x + yi$ — один из них, то другой будет $-x - yi = -(x + yi)$. Итак, из всякого комплексного числа можно извлечь квадратный корень, причем корень имеет два значения, различающиеся только знаком. Исключение представляет только одно число 0, единственный квадратный корень из которого есть также 0.

Частные случаи. Пусть $a > 0$, $b = 0$; тогда

$$\sqrt{a^2 + b^2} = \sqrt{a^2} = a, \qquad x^2 = \frac{1}{2}(a + a) = a, \qquad y^2 = \frac{1}{2}(-a + a) = 0,$$

и мы получим два вещественных значения квадратного корня из положительного числа a, в согласии с правилами элементарной алгебры.

Пусть теперь опять $a > 0$ и мы желаем найти $\sqrt{-a} = \sqrt{-a + 0i}$. Здесь $\sqrt{(-a)^2 + 0^2} = \sqrt{(-a)^2} = a$ (ибо этот корень положителен); далее

$$x^2 = \frac{1}{2}(-a + a) = 0; \qquad y^2 = \frac{1}{2}(a + a) = a; \quad \text{т. е.} \quad \sqrt{-a} = \pm\sqrt{a} \cdot i.$$

Таким образом в то время как в области вещественных чисел не существует квадратных корней из отрицательных чисел, в области комплексных чисел такие корни существуют и являются чисто мнимыми числами. Между прочим пример, упомянутый в § 1, теперь поставлен на строгую основу.

Упражнения

1) Найти $(3 + 5i)94 - i)$.
Отв. $17 + 17i$.
2) Найти $(6 + 11i)(7 + 3i)$.
Отв. $9 + 95i$.
3) Найти $\left(\frac{3}{4} + \frac{1}{2}i\right)\left(1\frac{1}{3} - \frac{1}{3}i\right)$.
Отв. $1\frac{1}{6} + \frac{5}{12}i$.
4) Найти $\frac{3 - i}{4 + 5i}$.
Отв. $\frac{7}{41} - \frac{19}{41}i$.
5) Найти $\frac{2 + 3i}{2 + i}$.
Отв. $\frac{7}{5} + \frac{4}{5}i$.
6) Найти $(4 - 7i)^3$.
Отв. $-524 + 7i$.
7) Найти $(1 + i)^4$.
Отв. -4.

8) Найти $i^{26}, i^{35}, i^{81}, i^{136}$.
Отв. $-1, -i, i, 1$.
9) Найти i^{-6}, i^{-15}, i^{-37}.
Отв. $-1, i, -i$.
10) Найти $\sqrt{i}$.
Отв. $\pm\dfrac{1+i}{\sqrt{2}}$.
11) Найти $\sqrt[4]{2i}$.
Отв. $\pm\left(\sqrt{\dfrac{1+\sqrt{2}}{2}}+i\sqrt{\dfrac{-1+\sqrt{2}}{2}}\right)$.
12) Найти $\sqrt{1-12i}$.
Отв. $\pm\left(\sqrt{\dfrac{1+\sqrt{145}}{2}}-i\sqrt{\dfrac{-1+\sqrt{145}}{2}}\right)$.
13) Найти $\sqrt{-5-12i}$.
Отв. $\pm(2-3i)$.
14) Найти $\sqrt{1+2i}$.
Отв. $\pm\left(\sqrt{\dfrac{1+\sqrt{5}}{2}}+i\sqrt{\dfrac{-1+\sqrt{5}}{2}}\right)$.

§ 7. Тригонометрическая форма комплексного числа. Мы уже видели [§ 4 (9)], что произведение двух взаимно сопряженных комплексных чисел вещественно и положительно; это — так называемая *норма* каждого из сомножителей. Положительный квадратный корень из нормы данного комплексного числа называется его *абсолютной величиной* или *модулем* [5]. Абсолютную величину комплексного числа $a+bi$ принято обозначать через $|a+bi|$. Итак

$$|a+bi|=\sqrt{a^2+b^2}. \tag{12}$$

Очевидно, $|a+bi|=|a-bi|$, $|\alpha|=|-\alpha|$, $|a|$ есть обычная абсолютная величина числа a, $|bi|=|b|$.

Обозначив $|a+bi|$ через r, напишем данное число в виде:

$$a+bi=r\left(\frac{a}{r}+\frac{b}{r}i\right).$$

Так как $\left(\dfrac{a}{r}\right)^2+\left(\dfrac{b}{r}\right)^2=\dfrac{a^2+b^2}{r^2}=1$, то можно найти такой угол φ, что

$$\cos\varphi=\frac{a}{r}=\frac{a}{\sqrt{a^2+b^2}},\qquad \sin\varphi=\frac{b}{r}=\frac{b}{\sqrt{a^2+b^2}};$$

[5] Я предпочитаю — по примеру немецкой литературы — термин «абсолютная величина» взамен более распространенного у нас термина «модуль», хотя этот последний и короче; дело в том, что термин «модуль» имеет в математике и ее приложениях самые разнообразные значения: есть модуль и в теории чисел, и в теории эллиптических функций и в новой области гиперкомплексных чисел, и в теории логарифмов, и в теории упругости (модуль упругости); зачем же еще раз вводить этот «универсальный» термин, если есть более подходящее название. Ведь «модуль» комплексного числа играет совершенно ту же роль, что и «абсолютная величина» вещественного числа: он является обобщением этой последней, причем обобщением с соблюдением принципа перманентности.

этот угол φ называется *аркусом* числа $a + bi$ [6], т. е.

$$\varphi = \operatorname{arc}(a + bi);$$

аркус данного числа однозначно определен в пределах одной окружности, например от 0 до 2π (или от 0° до 360°); вообще же он имеет для данного числа бесчисленное множество значений, отличающихся друг от друга на целое кратное 2π.

Имеем

$$a + bi = r(\cos\varphi + i\sin\varphi); \tag{13}$$

это и есть *тригонометрическая форма комплексного числа.* Очевидно, $|\cos\varphi + i\sin\varphi| = 1$ для любого φ. Заметим, что

$$\frac{b}{a} = \operatorname{tg}\varphi.$$

Если a — вещественное положительное число, то $\operatorname{arc} a = 0$, или вообще $2k\pi$; если a — вещественное отрицательное число, то $\operatorname{arc} a = \pi$, или вообще $(2k+1)\pi$; при вещественном b

$$\operatorname{arc}(bi) = \pm\frac{\pi}{2} + 2k\pi.$$

Число 0 — единственное, для которого аркус совершенно не определен, ибо для нуля $a = b = r = 0$ и $\sin\varphi$ и $\cos\varphi$ получают неопределенную форму $\frac{0}{0}$.

§ 8. Сумма, произведение и частное комплексных чисел, заданных в тригонометрической форме.

Теорема 1. *Абсолютная величина суммы или разности двух комплексных чисел не может быть больше суммы или меньше разности абсолютных величин этих чисел:*

$$||\alpha| - |\beta|| \le |\alpha \pm \beta| \le |\alpha| + |\beta|. \tag{14}$$

Доказательство. Пусть

$$\alpha = r_1(\cos\varphi_1 + i\sin\varphi_1), \qquad \beta = r_2(\cos\varphi_2 + i\sin\varphi_2),$$

$$\gamma = \alpha \pm \beta = R(\cos\psi + i\sin\psi)\ ^{7}$$

отсюда по постулату 1 § 3 выводим:

$$r_1\cos\varphi_1 \pm r_2\cos\varphi_2 = R\cos\psi,$$

$$r_1\sin\varphi_1 \pm r_2\sin\varphi_2 = R\sin\psi;$$

[6] У разных авторов этот угол φ носит разные названия: *аргумент*, *амплитуда*, *фаза*, *азимут*; чаще всего встречается «аргумент». Я избегаю этого названия, могущего привести к недоразумению. Слово аркус — латинское и означает: дуга.

[7] Двойной знак означает, что мы по желанию можем выбрать тот или другой и для каждого из них провести аналогичные доказательства.

умножаем обе части первого из этих равенств на $\cos\psi$, а обе части второго — на $\sin\psi$ и складываем:

$$r_1(\cos\varphi_1\cdot\cos\psi+\sin\varphi_1\cdot\sin\psi)\pm r_2(\cos\varphi_2\cdot\cos\psi+\sin\varphi_2\cdot\sin\psi)=R(\cos^2\psi+\sin^2\psi),$$

или

$$r_1\cos(\varphi_1-\psi)\pm r_2\cos(\varphi_2-\psi)=R. \tag{15}$$

Это равенство и доказывает нашу теорему; действительно, наибольшее значение для косинуса есть $+1$, а наименьшее есть -1, следовательно, R имеет наибольшее значение, когда в левой части формулы (15) оба члена складываются и имеют наибольшие значения, т. е. когда левая часть (15) есть r_1+r_2; иными словами: $R\le r_1+r_2$ или $|\gamma|=|\alpha\pm\beta|\le|\alpha|+|\beta|$. Но так как $\alpha=\gamma\mp\beta$, то по доказанному $|\alpha|\le|\gamma|+|\beta|$, откуда $|\gamma|=|\alpha\pm\beta|\ge|\alpha|-|\beta|$; точно так же

$$\pm\beta=\gamma-\alpha,\qquad |\beta|\le|\gamma|+|\alpha|,\qquad |\gamma|=|\alpha\pm\beta|\ge|\beta|-|\alpha|,$$

и формула (14) доказана во всех своих частях.

Следствие 1. Доказанная теорема непосредственно обобщается на *любое число слагаемых*:

$$|\alpha_1\pm\alpha_2\pm\ldots\pm\alpha_m|\le|\alpha_1|+|\alpha_2|+\ldots+|\alpha_m|.$$

Следствие 2. В частности

$$|a+bi|\le|a|+|b|,$$

так как $|bi|=|b|$; с другой стороны $|a+bi|=+\sqrt{a^2+b^2}\ge|a|$, а также $\ge|b|$.

Теорема 2. *Абсолютная величина произведения равна произведению абсолютных величин, а аркус произведения равен сумме аркусов сомножителей:*

$$|\alpha\beta|=|\alpha|\,|\beta|,\qquad \operatorname{arc}(\alpha\beta)=\operatorname{arc}\alpha+\operatorname{arc}\beta.$$

Доказательство. Сохраняя обозначения предыдущей теоремы, имеем:

$$\begin{aligned}\alpha\beta &= r_1(\cos\varphi_1+i\sin\varphi_1)\cdot r_2(\cos\varphi_2+i\sin\varphi_2)=\\ &= r_1r_2[\cos\varphi_1\cdot\cos\varphi_2-\sin\varphi_1\cdot\sin\varphi_2+i(\sin\varphi_1\cdot\cos\varphi_2+\cos\varphi_1\cdot\sin\varphi_2)]=\\ &= r_1r_2[\cos(\varphi_1+\varphi_2)+i\sin(\varphi_1+\varphi_2)];\end{aligned}$$

это и доказывает нашу теорему.

Следствие 1. Теорема 2 непосредственно обобщается на *любое число сомножителей.*

Следствие 2. При одинаковых сомножителях имеем: *абсолютная величина степени, равна той же степени абсолютной величины; аркус степени равен аркусу основания, умноженному на показатель степени:*

$$|\alpha^n|=|\alpha|^n,\qquad \operatorname{arc}(\alpha^n)=n\operatorname{arc}\alpha.$$

При $|\alpha|=1$ получаем формулу Моавра (Moivre):

$$(\cos\varphi+i\sin\varphi)^n=\cos n\varphi+i\sin n\varphi. \tag{16}$$

Это пока доказано для целых положительных показателей; вообще же эти формулы верны (с некоторыми оговорками) и для любых показателей.

Теорема 3. *Абсолютная величина частного (дроби) равна частному абсолютных величин, а аркус частного равен разности аркусов делимого и делителя (числителя и знаменателя):*

$$\left|\frac{\alpha}{\beta}\right| = \frac{|\alpha|}{|\beta|}, \qquad \operatorname{arc}\left(\frac{\alpha}{\beta}\right) = \operatorname{arc}\alpha - \operatorname{arc}\beta.$$

Доказательство. Применяя те же обозначения, что и раньше, имеем:

$$\begin{aligned}\frac{r_1(\cos\varphi_1 + i\sin\varphi_1)}{r_2(\cos\varphi_2 + i\sin\varphi_2)} &= \frac{r_1(\cos\varphi_1 + i\sin\varphi_1)(\cos\varphi_2 - i\sin\varphi_2)}{r_2(\cos^2\varphi_2 + \sin^2\varphi_2)} = \\ &= \frac{r_1}{r_2}\left[\cos\varphi_1\cdot\cos\varphi_2 + \sin\varphi_1\sin\varphi_2 + i(\sin\varphi_1\cdot\cos\varphi_2 - \cos\varphi_1\cdot\sin\varphi_2)\right] = \\ &= \frac{r_1}{r_2}\left[\cos(\varphi_1-\varphi_2) + i(\sin(\varphi_1-\varphi_2)\right],\end{aligned}$$

что и требовалось доказать.

Следствие. Если $\alpha = r(\cos\varphi + i\sin\varphi)$, то

$$\alpha^{-1} = \frac{1}{\alpha} = \frac{1}{r}(\cos\varphi - i\sin\varphi) = r^{-1}[\cos(-\varphi) + i\sin(-\varphi)];$$

следовательно:

$$|\alpha^{-1}| = |\alpha|^{-1}, \qquad \operatorname{arc}(\alpha^{-1}) = -\operatorname{arc}\alpha.$$

Так как $\alpha^{-n} = (\alpha^{-1})^n$, то по следствию 2 из теоремы 2 находим, что

$$|\alpha^{-n}| = |\alpha|^{-n}, \qquad \operatorname{arc}(\alpha^{-n}) == -n\operatorname{arc}\alpha,$$

т. е. что следствие 2 теоремы 2 и в частности формула Моавра верны и для целых отрицательных показателей.

§ 9. Извлечение корня n-й степени. Пусть $\alpha = r(\cos\varphi + i\sin\varphi)$; обозначим:

$$\sqrt[n]{\alpha} = \rho(\cos\omega + i\sin\omega);$$

возвышая обе части в n-ю степень, найдем:

$$\rho^n = r, \qquad n\omega = \varphi + 2k\pi,$$

где k любое целое число $\gtreqless 0$; отсюда

$$\rho = \sqrt[n]{r}, \qquad \omega = \frac{\varphi + 2k\pi}{n}.$$

Как r, так и ρ больше нуля.

Как известно, у всякого положительного числа r всегда существует один и только один положительный корень n-й степени, т. е. ρ всегда однозначно определен. Что касается ω, то оно зависит от произвольного целого числа k; мы получаем таблицу:

$$\begin{array}{rcccccccc} k &=& 0 & 1 & 2 & \dots & n-1 & n & n+1 \\ \omega &=& \dfrac{\varphi}{n} & \dfrac{\varphi+2\pi}{n} & \dfrac{\varphi+4\pi}{n} & \dots & \dfrac{\varphi+2(n-1)\pi}{n} & \dfrac{\varphi}{n}+2\pi & \dfrac{\varphi+2\pi}{n}+2\pi \end{array}$$

и т. д.

При всех остальных целых k значения ω отличаются от найденных nп значений (для $k = 0, 1, 2, \ldots, n-1$ на кратные от 2π, т. е. соответствующие им комплексные числа те же, что и при $k = 0, 1, 2, \ldots, n-1$, так что *всего имеем n и только n различных корней n-й степени из всякого комплексного числа $\alpha \neq 0$*:

$$\beta_k = \sqrt[n]{r}\left(\cos\frac{\varphi + 2k\pi}{n} + i\sin\frac{\varphi + 2k\pi}{n}\right), \qquad k = 0, 1, 2, \ldots, n-1.$$

Частный случай:

$$\alpha = 1, \qquad \sqrt[n]{1} = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}, \qquad k = 0, 1, 2, \ldots, n-1.$$

При $k = 0$ получаем обычный корень $\sqrt[n]{1} = 1$.

По § 8, теореме 2

$$\sqrt[n]{r}\left(\cos\frac{\varphi + 2k\pi}{n} + i\sin\frac{\varphi + 2k\pi}{n}\right) =$$
$$= \sqrt[n]{r}\left(\cos\frac{\varphi}{n} + i\sin\frac{\varphi}{n}\right)\left(\cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}\right);$$

отсюда следует $\beta_k = \beta_0\xi_k$, где ξ_k — различные корни n-й степени из единицы.

Пусть α — вещественное положительное число; тогда

$$\varphi = 0, \qquad \alpha = r, \qquad \sqrt[n]{\alpha} = \beta_k = \beta_0\xi_k, \qquad \beta_0 = \sqrt[n]{r} = \rho > 0;$$

при n нечетном все ξ_k (для $k = 1, 2, \ldots, n-1$) мнимые, т. е. существует только один вещественный корень n-й степени из вещественного числа $\alpha > 0$, именно ρ; остальные $n-1$ корней — мнимые.

Если же n четное, то $\xi_{\frac{n}{2}} = \cos\pi + i\sin\pi = -1$ тоже вещественно и $\beta_{\frac{n}{2}} = -\rho$, т. е. тогда существуют два вещественных корня n-й степени из αа: $\pm\rho$, остальные корни мнимые.

Пусть теперь α вещественно и отрицательно: $\varphi = \pi$, $\alpha = -r$, тогда

$$\beta_0 = \sqrt[n]{r}\left(\cos\frac{\pi}{n} + i\sin\frac{\pi}{n}\right)$$

мнимый корень.

При n нечетном существует один вещественный корень, именно:

$$\beta_{\frac{n-1}{2}} = \beta_0\xi_{\frac{n-1}{2}} = \sqrt[n]{r}\left(\cos\frac{\pi}{n} + i\sin\frac{\pi}{n}\right)\left(\cos\frac{(n-1)\pi}{n} + i\sin\frac{(n-1)\pi}{n}\right) =$$
$$= \sqrt[n]{r}(\cos\pi + i\sin\pi) = -\sqrt[n]{r};$$

он тоже отрицательный.

Остальные корни мнимые.

При n четном и $\alpha < 0$ совсем нет вещественных корней.

§ 10. Геометрическое представление комплексных чисел. Комплексные числа представляются геометрически как точки на плоскости, по принципу аналитической геометрии при прямоугольной системе координат: число $a + bi$

изображается точкой с абсциссой a и ординатой b (черт. 1). Абсолютная величина $|a+bi|$ и $\arg\alpha$ суть не что иное, как полярные координаты точки $a+bi$, как видно из формул:

$$r^2 = a^2 + b^2, \qquad \operatorname{tg}\varphi = \frac{b}{a},$$

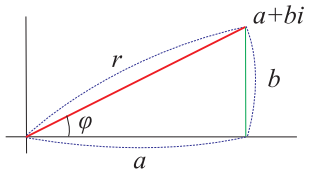
$$a = r\cos\varphi, \qquad b = r\sin\varphi.$$

Сложение комплексных чисел $(a + bi) + (c + di)$ геометрически сводится к построению параллелограмма со сторонами $|a + bi|$ и $|c + di|$ (черт. 2).

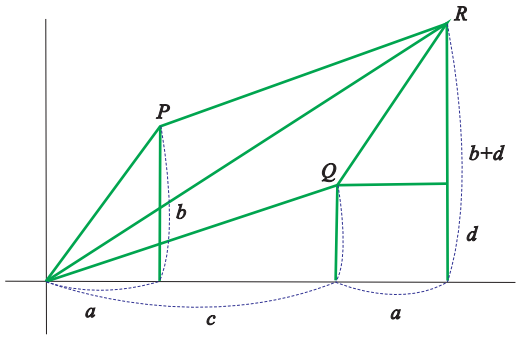
Умножение комплексных чисел сводится к построению подобных треугольников (черт. 3); именно, для абсолютных величин имеем:

$$\frac{r_1 r_2}{r_2} = \frac{r_1}{1};$$

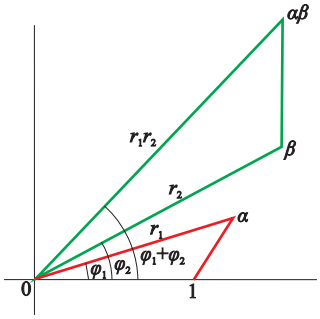
отсюда видно, что треугольник с вершинами $0, 1, \alpha$ подобен треугольнику с вершинами $o, \beta, \alpha\beta$.



Черт. 1



Черт. 2



Черт. 3

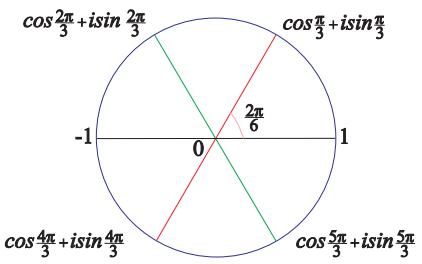
Решение уравнения $x^n = 1$ или извлечение корня n-й степени из единицы геометрически сводится к делению на n равных частей окружности с центром O и радиусом, равным единице (см. черт. 4 для случая $n = 6$).

Разность $|\alpha - \beta|$ геометрически изображается как расстояние между точками α и β (черт. 5).

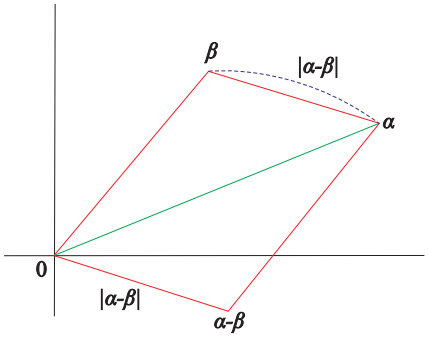
Условие $|\xi - \omega| < \delta$ выражает геометрически, что точка ξ лежит внутри круга радиуса δ с центром ω (черт. 6).

Существует еще иное геометрическое представление комплексного числа $a+bi$; именно, как *вектора на плоскости* с составляющими a и b; при этом $|a + bi| = +\sqrt{a^2 + b^2}$ является длиной этого вектора, а $\varphi = \arg(a + bi)$ дает направление вектора; точка приложения вектора безразлична. При таком представлении комплексного числа сумма комплексных чисел очень просто интерпретируется как обычная сумма векторов. Для произведения же комплексных чисел в теории векторов нет соответствующей аналогии.

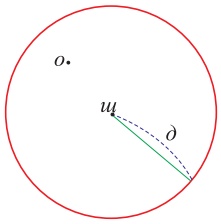
Замечание. Начинающие часто задают вопрос: как же «правильнее» представлять аналитически точки на плоскости — в виде двух координат a и b или в



Черт. 4



Черт. 5



Черт. 6

виде комплексного числа $a+bi$. Этот вопрос не имеет смысла: точка на плоскости аналитически представляется двумя вещественными числами, ее координатами a и b, которые можно либо просто писать рядом, отделяя запятою друг от друга, либо соединить в «комплексное число» $a+bi$. Последнее целесообразно делать только в том случае, если в дальнейшем нам требуется с этими числами $a+bi$ оперировать именно как с комплексными числами. В обычной же аналитической геометрии оперируют с каждой координатой точки отдельно (например, линия аналитически выражается посредством уравнения между координатами точки), следовательно, там нет никакого смысла объединять обе координаты в комплексное число.

§ 11. Предел последовательности комплексных чисел. Пусть имеем последовательность комплексных чисел $c_1, c_2, c_3, \ldots$, где

$$c_n = a_n + b_n i$$

и пусть существует:

$$\lim\ a_n = \alpha, \qquad \lim\ b_n = \beta, \qquad \alpha + \beta i = \gamma;$$

тогда определяем:

$$\lim\ c_n = \lim\ a_n + i \lim\ b_n = \gamma.$$

Пусть при $n > N$ будет $|\alpha - a_n| < \dfrac{\varepsilon}{2}$ и $|\beta - b_n| < \dfrac{\varepsilon}{2}$; тогда $|\gamma - c_n| < \varepsilon$ (см. § 8, теорема 1, следствие 2).

Обратно: пусть $|\gamma - c_n| < \varepsilon$ тогда и подавно:

$$|\alpha - a_n| < \varepsilon \quad \text{и} \quad |\beta - b_n| < \varepsilon.$$

Следовательно, можно дать другое определение предела: последовательность $c_1, c_2, c_3, \ldots$ стремится к пределу γ, если, взяв любое $\varepsilon > 0$, можно найти $N > 0$ так, что при $n > N$ будет $|\gamma - c_n| < \varepsilon$. Это определение — такое же, как и для предела вещественных чисел. Подобным же образом определяем: члены последовательности $c_1, c_2, c_3, \ldots$ становятся бесконечно большими, если, взяв любое $M > 0$, можно найти $N > 0$ так, что при $n > N$ будет $|c_n| > M$.

Для пределов последовательности с комплексными членами верны все те же теоремы, что и для пределов последовательности с вещественными членами.

§ 12. Приложение формулы Моавра. Имеем:

$$(\cos\varphi + i\sin\varphi)^n = \cos^n\varphi + ni\cos^{n-1}\varphi\sin\varphi - \binom{n}{2}\cos^{n-2}\varphi\sin^2\varphi -$$
$$- \binom{n}{3} i\cos^{n-3}\varphi\sin^3\varphi + \binom{n}{4}\cos^{n-4}\varphi\sin^4\varphi + \ldots = \cos n\varphi + i\sin n\varphi.$$

Отсюда, отделяя вещественную часть от мнимой, получаем:

$$\cos n\varphi = \cos^n\varphi - \binom{n}{2}\cos^{n-2}\varphi\sin^2\varphi + \binom{n}{4}\cos^{n-4}\varphi\sin^4\varphi - \ldots,$$
$$\sin n\varphi = \binom{n}{1}\cos^{n-1}\varphi\sin\varphi - \binom{n}{3}\cos^{n-3}\varphi\sin^3\varphi + \binom{n}{5}\cos^{n-5}\varphi\sin^5\varphi - \ldots$$

Здесь

$$\binom{n}{k} = \frac{n(n-1)(n-2)\cdots(n-k+1)}{1\cdot 2\cdot 3\cdots k}, \qquad \binom{n}{1} = n, \qquad \binom{n}{0} = 1.$$

Обратные формулы. Положим

$$u = \cos\varphi + i\sin\varphi, \qquad v\cos\varphi - i\sin\varphi;$$

тогда

$$u + v = 2\cos\varphi, \qquad u - v = 2i\sin\varphi, \qquad uv = 1; \qquad u^m = \cos m\varphi + i\sin m\varphi,$$
$$v^m = \cos m\varphi - i\sin m\varphi, \qquad u^m + v^m = 2\cos m\varphi, \qquad u^m - v^m 2i\sin m\varphi,$$
$$2^n\cos^n\varphi = (u+v)^n = u^n + nu^{n-1}v + \binom{n}{2}u^{n-1}v^2 + \ldots + \binom{n}{2}u^2v^{n-2} + nuv^{n-1} + v^n =$$
$$= u^n + v^n + nuv(u^{n-2} + v^{n-2}) + \binom{n}{2}u^2v^2(u^{n-4} + v^{n-4}) + \ldots;$$

при n четном

$$(-1)^{\frac{n}{2}}2^n\sin^n\varphi = (u-v)^n = u^n + v^n - nuv(u^{n-2} + v^{n-2}) +$$
$$+ \binom{n}{2}u^2v^2(u^{n-4} + v^{n-4}) - \ldots;$$

при n нечетном

$$(-1)^{\frac{n-1}{2}} \cdot i \cdot 2^n \sin^n \varphi = (u-v)^n = u^n - v^n - nuv(u^{n-2} - v^{n-2}) +$$

$$+ \binom{n}{2} u^2 v^2 (u^{n-4} - v^{n-4}) - \dots$$

Отсюда получаем: при n четном

$$2^n \cos^n \varphi = 2\cos n\varphi + 2n\cos(n-2)\varphi + 2\binom{n}{2}\cos(n-4)\varphi + \dots + \binom{n}{\frac{n}{2}},$$

$$(-1)^{\frac{n}{2}} \sin^n \varphi = 2\cos n\varphi - 2n\cos(n-2)\varphi + \binom{n}{2}\cos(n-4)\varphi - \dots + (-1)^{\frac{n}{2}}\binom{n}{\frac{n}{2}};$$

при n нечетном

$$2^n \cos^n \varphi = 2\cos n\varphi + 2n\cos(n-2)\varphi + 2\binom{n}{2}\cos(n-4)\varphi + \dots + 2\binom{n}{\frac{n}{2}}\cos\varphi,$$

$$(-1)^{\frac{n-1}{2}} 2^n \sin^n \varphi = 2\sin n\varphi - 2n\sin(n-2)\varphi + 2\binom{n}{2}\sin(n-4)\varphi +$$

$$- \dots + (-1)^{\frac{n-1}{2}} 2\binom{n}{\frac{n-1}{2}}\sin\varphi.$$

Упражнения

15) Найти $\left|\left(\frac{1}{2} - \frac{1}{3}i\right)(3+2i)\right|$ (Два способа).

Отв. $2\frac{1}{6}$.

16) Найти $\left|\frac{2+i}{3-i}\right|$ (два способа).

Отв. $\sqrt{\frac{1}{2}} = \frac{\sqrt{2}}{2}$.

17) Найти $|(8-3i)^2|$.

Отв. 73.

18) Привести к тригонометрическому виду $1+i$ и $1-i$.

Отв. $\sqrt{2}\left(\cos\frac{\pi}{4} + i\sin\frac{\pi}{4}\right)$; $\sqrt{2}\left(\cos\frac{7\pi}{4} + i\sin\frac{7\pi}{4}\right)$.

19) Привести к тригонометрическому виду при помощи логарифмических таблиц $3+2i$.

Отв. $\sqrt{13}(\cos 33°41'24'' + i\sin 33°41'24'')$.

20) При помощи логарифмической линейки привести к тригонометрическому виду $3+4i$, $8+5i$.

Отв. $5(\cos 53°10' + i\sin 53°10')$, $9,44(\cos 32° + i\sin 32°)$.

21) Найти $\sqrt[3]{-1}$.

Отв. $\begin{cases} \cos\frac{\pi}{3} + i\sin\frac{\pi}{3} = \frac{1+i\sqrt{3}}{2}, \\ \cos\pi + i\sin\pi = -1, \\ \cos\frac{5\pi}{3} + i\sin\frac{5\pi}{3} = \frac{1-i\sqrt{3}}{2}. \end{cases}$

22) При помощи логарифмической линейки найти $\sqrt[3]{2+i}$.

Отв. $\begin{cases} 1,38(\cos 9^\circ + i\sin 9^\circ) = 1,37 + 0,216i, \\ 1,38(\cos 129^\circ + i\sin 129^\circ) = -0,87 + 1,07i, \\ 1,38(\cos 249^\circ + i\sin 249^\circ) = -0,495 - 1,29i. \end{cases}$

23) Вычислить при помощи логарифмических таблиц $\sqrt[1]{1}$.

Отв. $\pm 1,\ \pm - 0,8090, \pm i \cdot 0,5878,\ \pm 0,3090,\ \pm i \cdot 0,9511.$

24) Найти и вычислить при помощи логарифмических таблиц $\sqrt[5]{1+i}$.

Отв. $\begin{cases} \sqrt{102}(\cos 9^\circ + i\sin 9^\circ) = 1,0586 + 0,1677i, \\ \sqrt{102}(\cos 81^\circ + i\sin 81^\circ) = 0,1677 + 1,0586i, \\ \sqrt{102}(\cos 153^\circ + i\sin 153^\circ) = -0,9550 + 0,4866i,\ . \\ \sqrt{102}(\cos 225^\circ + i\sin 225^\circ) = -0,7579(1+i), \\ \sqrt{102}(\cos 297^\circ + i\sin 297^\circ) = 0,4866 - 0,9550i. \end{cases}$

25) По формулам § 11 разложить $\sin 2x$, $\sin 3x$, $\sin 4x$, $\sin 5x$, $\sin 6x$.

26) По формулам § 11 разложить $\cos 2x$, $\cos 3x$, $\cos 4x$, $\cos 5x$, $\cos 6x$.

27) По формулам § 11 разложить $\cos^2 x$, $\cos^3 x$, $\cos^4 x$, $\cos^5 x$, $\cos^6 x$.

28) По формулам § 11 разложить $\sin^2 x$, $\sin^3 x$, $\sin^4 x$, $\sin^5 x$, $\sin^6 x$.

29) Выяснить, при каких условиях произведение двух комплексных чисел вещественно.

Отв. Если один из сомножителей равен числу, сопряженному с другим сомножителем и умноженному на любое вещественное число.

30) Выяснить, при каких условиях произведение двух комплексных чисел чисто мнимо.

Отв. Если $a + bi$ есть один из сомножителей, то другой должен быть, равен $\lambda(b + ai)$, где λ — любое вещественное число.

31) Исследовать (аналитически и геометрически), при каких условиях абсолютная величина суммы двух комплексных чисел равна сумме абсолютных величин этих чисел.

Отв. Если аркусы слагаемых одинаковы.

32) Исследовать, при каких условиях абсолютная величина суммы двух комплексных чисел равна разности абсолютных величин слагаемых.

Отв. Если аркусы слагаемых различаются на π.

§ 13. Область рациональности. Делитель области. Кольцо. Итак, мы, расширили нашу область вещественных чисел тем, что ввели числа комплексные — более общие, такие, что вещественное число является частным случаем, комплексного. В этой расширенной области комплексных чисел выполнимы четыре действия — сложение, вычитание, умножение и деление, причем для этих действий остаются в силе все основные законы, которые имеют место для тех же действий над вещественными числами [8]. Перечислим еще раз кратко эти основные законы [9]: для сложения и вычитания — законы коммутативный, ассоциативный, неограниченной и однозначной обратимости, существование числа 0 («единицы»

[8] В § 6 и 9 мы видели, что в области комплексных чисел неограниченно выполнимо и действие извлечения корня всякой степени; в дальнейшем мы убедимся, что и более общее действие — решение алгебраических уравнений всех степеней — неограниченно выполнимо в области комплексных чисел. Но сейчас это нас не интересует.

[9] Перечисляя здесь эти основные законы, мы не занимаемся вопросом об их зависимости или независимости друг от друга.

для сложения), числа $-\alpha$ для каждого числа α («противоположные» числа); для умножения (и деления) — законы коммутативный, ассоциативный, неограниченной и однозначной обратимости для случая неравных нулю сомножителей, существование числа 1 («единицы» для умножения), числа $\frac{1}{\alpha}$ для каждого числа $\alpha \neq 0$ («обратные» числа); далее, дистрибутивный закон, связывающий сложение с умножением; наконец, закон об отсутствии нулевых делителей (§ 5).

Эти четыре действия называются *рациональными действиями*, ибо, совершая их над рациональными числами, мы получаем и результаты рациональные, т. е. из области рациональных чисел не выходим. Вообще такая система чисел, в которой неограниченно выполнимы рациональные действия (конечно, кроме деления на нуль), так что взяв два любые числа a и b (причем может быть и $a = b$) из этой системы, мы всегда получим, что и $a + b$, $a - b$, ab и $\frac{a}{b}$ (при $b \neq 0$) тоже принадлежат к этой системе, — называется *областью рациональности*, или *телом*, или *полем*. Так, все обычные рациональные числа составляют область рациональности; это — так называемая *абсолютная* область рациональности; система всех вещественных чисел тоже является областью рациональности (или телом или полем); точно также областью рациональности является система всех комплексных чисел (содержащих вещественные числа как частный случай). Мы видим, что одно тело может содержать другое как свою часть; тело, содержащееся в другом, называется *делителем* этого последнего. Собственно, одно уже число 0 составляет тело; но его обычно не причисляют к телам, дополняя определение тела еще условием, чтобы оно содержало больше, чем одно число. При этом условии верна такая теорема:

Всякое тело содержит делителем абсолютную область рациональности.

Действительно, пусть данное тело содержит число $a \neq 0$; следовательно, оно содержит и число $\frac{a}{a} = 1$, а значит и числа $1 + 1 = 2$, $2 + 1 = 3$ и т. д. и $1 - 1 = 0$, $0 - 1 = -1$, $-1 - 1 = -2$ и т. д., т. е. и все целые числа, а следовательно, и их частные, т. е. и все дроби, т. е. вообще все рациональные числа, что и требовалось доказать.

Кроме упомянутых тел или областей рациональности существует еще бесчисленное множество других числовых тел.

Так, числа вида $a + b\sqrt{2}$, где a и b — всевозможные рациональные числа, составляют тело; комплексные числа $a + bi$ с рациональными компонентами a и b тоже составляют тело и т. д. Но все целые числа (как положительные, так и отрицательные, включая и 0) тела не составляют, ибо действие деления тут не всегда возможно (т. е. частное двух целых чисел не всегда — целое число), иначе говоря, не выполнен закон неограниченной обратимости для умножения. Система целых чисел составляет *область целости* — так называется система чисел, где неограниченно выполнимы действия сложения, вычитания и умножения, но не деления. Другие примеры областей целости: числа $a + b\sqrt{2}$, где a и b — целые числа, числа $a + bi$ с целыми a и b, все *четные* целые числа и т. д. Область целости есть частный случай так называемого *кольца*, о котором будет речь еще впереди (см. главу XIV, ч. II). В каждом вопросе, в каждой теореме алгебры важно знать, какую область рациональности мы берем за основную, т. е. из какой области рациональности мы берем «данные» числа, коэфициенты наших функций и уравнений. В дальнейшем

в главах II, III, IV, VII этой первой части нашего курса за основную область рациональности мы берем тело комплексных чисел, в главе V — тело вещественных чисел, и главе VI — преимущественно абсолютную область рациональности.

ГЛАВА ВТОРАЯ

ДЕТЕРМИНАНТЫ

§ 14. Детерминанты второго порядка. Возьмем систему двух линейных уравнений с двумя неизвестными:

$$a_1x + b_1 = c_1,$$
$$a_2x + b_2 = c_2.$$

Умножаем сперва обе части верхнего уравнения на b_2, а нижнего — на $-b_1$, затем верхнего на $-a_2$, а нижнего на a_1 и оба раза складываем; разделив на $a_1b_2 - a_2b_1$, получаем:

$$x = \frac{c_1b_2 - c_2b_1}{a_1b_2 - a_2b_1}, \qquad y = \frac{a_1c_2 - a_2c_1}{a_1b_2 - a_2b_1},$$

при условии

$$a_1b_2 - a_2b_1 \neq 0.$$

Обозначают:

$$a_1b_2 - a_2b_1 = \begin{vmatrix} a_1 & b1 \\ a_2 & b_1 \end{vmatrix};$$

это выражение называется *детерминантом* (*определителем*) *второго порядка*; он состоит из четырех элементов ?, расположенных в две строки и два столбца, строки и столбцы называются рядами детерминанта.

§ 15. Свойства детерминантов второго порядка.

I. *Детерминант не изменяется от перестановки строк со столбцами:*

$$\begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix} = \begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix},$$

ибо оба детерминанта равны одному и тому же выражению

$$a_1b_2 - a_2b_1.$$

II. *От перестановки двух строк (или двух столбцов) детерминант меняет знак:*

$$\begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix} = -\begin{vmatrix} a_2 & b_2 \\ a_1 & b_1 \end{vmatrix} = -\begin{vmatrix} b_1 & a_1 \\ b_2 & a_2 \end{vmatrix} = \begin{vmatrix} b_2 & a_2 \\ b_1 & a_1 \end{vmatrix}.$$

Это тоже непосредственно следует из определения детерминанта.

III. *Если все элементы одного ряда имеют общий множитель, то его можно вынести за знак детерминанта.*

Например:

$$\begin{vmatrix} a_1c & b_1c \\ a_2 & b_2 \end{vmatrix} = c\begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix} \quad \text{или} \quad \begin{vmatrix} a_1c & b_1c \\ a_2 & b_2 \end{vmatrix} = a_1b_2c - a_2b_1c = c(a_1b_2 - a_2b_1).$$

IV. *Детерминант равен нулю, если элементы его двух рядов соответственно равны или пропорциональны.*

Например:

$$\begin{vmatrix} a_1 & b_1 \\ a_1 & b_1 \end{vmatrix} = 0, \qquad \begin{vmatrix} a_1 & b_1 \\ a_1c & b_1c \end{vmatrix} = 0.$$

Это следует из II и III.

V. *Если элементы какого-нибудь ряда суть суммы k слагаемых, то детерминант представляется как сумма k детерминантов.*

Например:

$$\begin{aligned} \begin{vmatrix} a_1 + c_1 & b_1 + d_1 \\ a_2 & b_2 \end{vmatrix} &= (a_1 + c_1)b_2 - a_2(b_1 + d_1) = \\ &= (a_1b_2 - a_2b_1) + (c_1b_2 - a_2d_1) = \begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix} + \begin{vmatrix} c_1 & d_1 \\ a_2 & b_2 \end{vmatrix}. \end{aligned}$$

Следствие I. Если элементы одного ряда — суммы k слагаемых, а элементы другого ряда — суммы l слагаемых, то детерминант представляется как сумма kl детерминантов.

Следствие II. Детерминант не изменится, если к элементам какого-нибудь ряда прибавить соответствующие элементы другого ряда, умноженные на один и тот же постоянный множитель.

Например:

$$\begin{vmatrix} a_1 + ca_2 & b_1 + cb_2 \\ a_2 & b_2 \end{vmatrix} = \begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix} + c\begin{vmatrix} a_2 & b_2 \\ a_2 & b_2 \end{vmatrix} = \begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix}$$

(по V, III, IV).

§ 16. Теорема умножения. Дан детерминант

$$\begin{vmatrix} a_1x_1 + b_1y_1 & a_1x_2 + b_1y_2 \\ a_2x_1 + b_2y_1 & a_2x_2 + b_2y_2 \end{vmatrix};$$

применяя к нему свойства V, III, IV, II, получим:

$$\begin{aligned} \begin{vmatrix} a_1x_1 + b_1y_1 & a_1x_2 + b_1y_2 \\ a_2x_1 + b_2y_1 & a_2x_2 + b_2y_2 \end{vmatrix} &= \begin{vmatrix} a_1x_1 & a_1x_2 \\ a_2x_1 & a_2x_2 \end{vmatrix} + \begin{vmatrix} a_1x_1 & b_1y_2 \\ a_2x_1 & b_2y_2 \end{vmatrix} + \\ + \begin{vmatrix} b_1y_1 & a_1x_2 \\ b_2y_1 & a_2x_2 \end{vmatrix} + \begin{vmatrix} b_1y_1 & b_1y_2 \\ b_2y_1 & b_2y_2 \end{vmatrix} &= x_1x_2\begin{vmatrix} a_1 & a_1 \\ a_2 & a_2 \end{vmatrix} + x_1y_2\begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix} + \\ + x_2y_1\begin{vmatrix} b_1 & a_1 \\ b_2 & a_2 \end{vmatrix} + y_1y_2\begin{vmatrix} b_1 & b_1 \\ b_2 & b_2 \end{vmatrix} &= x_1y_2\begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix} - x_2y_1\begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix} = \\ = (x_1y_2 - x_2y_1)\begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix} &= \begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix} \cdot \begin{vmatrix} x_1 & x_2 \\ x_2 & y_2 \end{vmatrix}, \end{aligned}$$

видим что *произведение двух детерминантов представляется в виде детерминанта*. Так как и во множимом и во множителе можно переставить строки со столбцами (по 1, § 15), то сообразно этому получаем четыре способа составления произведения:

$$1) \qquad \begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix} \cdot \begin{vmatrix} x_1 & y_1 \\ x_2 & b_2 \end{vmatrix} = \begin{vmatrix} a_1x_1 + b_1y_1 & a_1x_2 + b_1y_2 \\ a_2x_1 + b_2y_1 & a_2x_2 + b_2y_2 \end{vmatrix}$$

(комбинирование строк со строками),

$$2) \qquad \begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix} \cdot \begin{vmatrix} x_1 & y_1 \\ x_2 & b_2 \end{vmatrix} = \begin{vmatrix} a_1x_1 + a_2y_1 & a_1x_2 + a_2y_2 \\ b_1x_1 + b_2y_1 & b_1x_2 + b_2y_2 \end{vmatrix}$$

(комбинирование столбцов со строками),

$$3) \qquad \begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix} \cdot \begin{vmatrix} x_1 & y_1 \\ x_2 & b_2 \end{vmatrix} = \begin{vmatrix} a_1x_1 + b_1x_2 & a_1y_1 + b_1y_2 \\ a_2x_1 + b_2x_2 & a_1y_1 + b_2y_2 \end{vmatrix}$$

(комбинирование строк со столбцами),

$$4) \qquad \begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix} \cdot \begin{vmatrix} x_1 & y_1 \\ x_2 & b_2 \end{vmatrix} = \begin{vmatrix} a_1x_1 + a_2x_2 & a_1y_1 + a_2y_2 \\ b_1x_1 + b_2x_2 & b_1x_1 + b_2y_2 \end{vmatrix}$$

(комбинирование столбцов со столбцами).

Пример.

$$\begin{vmatrix} 5 & 3 \\ 1 & 4 \end{vmatrix} \cdot \begin{vmatrix} 2 & 5 \\ 3 & 8 \end{vmatrix} = \begin{vmatrix} 25 & 39 \\ 22 & 35 \end{vmatrix} = \begin{vmatrix} 15 & 23 \\ 26 & 41 \end{vmatrix} = \begin{vmatrix} 19 & 40 \\ 14 & 37 \end{vmatrix} = \begin{vmatrix} 13 & 33 \\ 18 & 47 \end{vmatrix} = 17.$$

§ 17. Однородные уравнения. Возьмем систему двух однородных уравнений с тремя неизвестными:

$$a_1x + b_1y + c_1z = 0,$$
$$a_2x + b_2y + c_2z = 0.$$

Принимая z за известное, решим их относительно x и y:

$$x = \frac{z(b_1c_2 - b_2c_1)}{a_1b_2 - a_2b_1} \qquad \frac{z(c_1a_2 - c_1a_1)}{a_1b_2 - a_2b_1}$$

(при условии $a_1b_2 - a_2b_1 \neq 0$).

Другими словами:

$$x : y : z = \begin{vmatrix} b_1 & c_1 \\ b_2 & c_2 \end{vmatrix} : \begin{vmatrix} c_1 & a_1 \\ c_2 & a_2 \end{vmatrix} : \begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix}.$$

Эта формула верна всегда, если только хоть один из входящих в нее детерминантов не равен нулю.

Упражнения

33) Перемножить всеми четырьмя способами $\begin{vmatrix}5 & 3\\ 1 & 2\end{vmatrix}\cdot\begin{vmatrix}4 & 1\\ 3 & 5\end{vmatrix}$.

34) Найти (четырьмя способами) $\begin{vmatrix}3 & 7\\ 5 & 11\end{vmatrix}^2$.

Отв. Один из способов дает $\begin{vmatrix}58 & 92\\ 92 & 146\end{vmatrix}$.

35) Даны уравнения $3x+5y-z=0$, $2x-3y+4z=0$; найти отношения неизвестных.

Отв. $x:y:z=-17:14:19$.

36) Из уравнений $2x-5y+2z=0$, $x+4y-3z=0$ найти отношения неизвестных.

Отв. $x:y:z=7:8:13$.

§ 18. Детерминанты третьего порядка. Возьмем систему трех линейных уравнений с тремя неизвестными:

$$\left.\begin{array}{l|ll} a_1x+b_1y+c_1z=d_1 & \text{умнож. на} & k,\\ a_2x+b_2y+c_2z=d_2 & \quad\prime\prime & l,\\ \underline{a_3x+b_3y+c_3z=d_3} & \quad\prime\prime & m, \end{array}\right\}\text{ и складываем.}$$

$$\begin{aligned}(ka_1+la_2+ma_3)x+(kb_1+lb_2+mb_3)y+(kc_1+lc_2+mc_3)z=\\ =kd_1+ld_2+ld_3.\end{aligned}\qquad(1)$$

Для определения x выберем неопределенные множители k, l, m так, чтобы было

$$kb_1+lb_2+mb_3=0,\qquad kc_1+lc_1+mc_3=0.$$

По § 17

$$k:l:m=(b_2c_3-b_3c_2):(b_3c_1-b_1c_3):(b_1c_2-b_2c_1).$$

Так как нам нужны какие-нибудь значения k, l, m, удовлетворяющие этой пропорции, то можно просто взять

$$k=(b_2c_3-b_3c_2),\qquad l=(b_3c_1-b_1c_3),\qquad m=(b_1c_2-b_2c_1).$$

Тогда коэфициент при x обращается в

$$\begin{aligned}a_1((b_2c_3-b_3c_2))+a_2(b_3c_1-b_1c_3)+a_3((b_1c_2-b_2c_1)=\\ =a_1b_2c_3-a_1b_3c_2+a_2b_3c_1-a_2b_1c_3+a_3b_1c_2-a_3b_2c_1.\end{aligned}\qquad(2)$$

Это выражение называется *детерминантом третьего порядка* и обозначается

$$\begin{vmatrix}a_1 & b_1 & c_1\\ a_2 & b_2 & c_2\\ a_3 & b_3 & c_3\end{vmatrix}.$$

Теперь правая часть равенства (1) получает вид:

$$d_1(b_2c_3-b_3c_2)+d_2(b_3c_1-b_1c_3)+d_3(b_1c_2-b_2c_1)=\begin{vmatrix}d_1 & b_1 & c_1\\ d_2 & b_2 & c_2\\ d_3 & b_3 & c_3\end{vmatrix}.$$

Итак

$$x = \begin{vmatrix} d_1 & b_1 & c_1 \\ d_2 & b_2 & c_2 \\ d_3 & b_3 & c_3 \end{vmatrix} : \begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix}$$

Подобно же выяисляем y и z. Найдем:

$$y = \begin{vmatrix} a_1 & d_1 & c_1 \\ a_2 & d_2 & c_2 \\ a_3 & d_3 & c_3 \end{vmatrix} : \begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix}, \qquad z = \begin{vmatrix} a_1 & b_1 & d_1 \\ a_2 & b_2 & d_2 \\ a_3 & b_3 & d_3 \end{vmatrix} \begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix}$$

Знаменатель у x, y и z один и тот же; числители же получаются из знаменателя, если мы в нем коэфициенты при определяемом неизвестном заменим свободными членами.

Выведенные формулы имеют место, если только

$$\begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix} \neq 0.$$

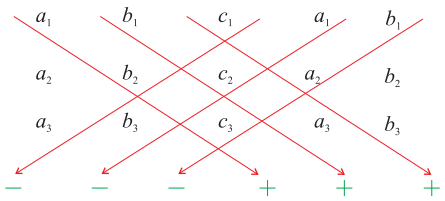


Схема I

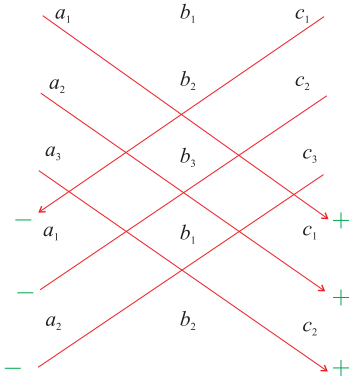


Схема II

По своему определению (2) детерминант третьего порядка составляется так: в произведении $a_\varkappa b_\lambda c_\mu$ индексы $\varkappa, \lambda, \mu$ пробегают всевозможные перестановки цифр $1, 2, 3$, причем произведения, соответствующие перестановкам $1, 2, 3$; $2, 3, 1$; $3, 1, 2$, берутся со знаком $+$, а произведения, соответствующие перестановкам $2, 1, 3$; $1, 3, 2$; $3, 2, 1$, берутся со знаком $-$; детерминант равен сумме этих шести количеств. На

прилагаемых схемах I и II указан практический способ вычисления детерминанта, данного в своем обычном виде: количества, соединенные одною и дою же чертой, перемножаются, причем на схеме указано, какие произведения брать со знаком +, какие со знаком −.

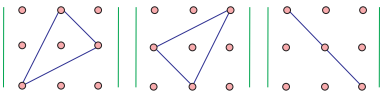


Схема III

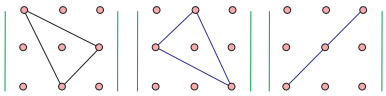


Схема IV

Другой способ вычисления детерминанта указан на прилагаемых схемах III и IV.

Линиями указаны перемножаемые элементы: на схеме III со знаком +, на схеме IV со знаком −.

Упражнения

37) Вычислить детерминанты

$$\begin{vmatrix} 5 & 8 & -6 \\ 1 & -2 & 5 \\ 4 & 7 & 1 \end{vmatrix}, \qquad \begin{vmatrix} \frac{3}{4} & \frac{1}{2} & \frac{1}{3} \\ \frac{2}{5} & 1 & 1\frac{1}{2} \\ \frac{2}{3} & 2 & 2\frac{1}{2} \end{vmatrix}.$$

Отв. -123, $-\frac{119}{360}$.

38) Решить систему уравнений

$$3x - 2y + 4z = 37, \qquad 5x + 3y - 2z = 20, \qquad 4x - 2y + 3z = 35.$$

Отв. $x = 5$, $y = 3$, $z = 7$.

§ 19. Свойства детерминантов третьего порядка.

I. *Детерминант не изменяется от перестановки строк со столбцами.*

Доказательство. Как указано в предыдущем параграфе, детерминант образуется путем перестановок в произведении $a_1b_2c_3$ цифр $1, 2, 3$ и приписывания получающимся произведениям определенных знаков. Но вместо того чтобы в выражении $a_1b_2c_3$ переставлять цифры $1, 2, 3$, оставляя a, b, c на местах, можно переставлять a, b, c, оставляя $1, 2, 3$ на местах и соблюдая те же правила относительно знаков; а это и сведется к тому, что мы переставим строки со столбцами.

Другое доказательство. Фигуры в схемах III и IV в конце § 18 не изменятся, если мы перевернем все шесть таблиц вокруг главной диагонали (идущей сверху слева вниз направо); это перевертывание равносильно перестановке строк со столбцами.

II. *От перестановки двух строк (или двух столбцов) детерминант меняет знак.*

Доказательство. Переставим, например, первую и вторую строки; это сводится к перестановке индексов 1 и 2; но тогда знак + дадут перестановки 213, 132, 321, а знак − перестановки 123, 231 312, т. е. как раз противоположно тому, что было раньше; детерминант изменил знак.

III. *Если все элементы, одного ряда имеют общий множитель, то его можно вынести за знак детерминанта.*

Доказательство. Это следует из того, что в каждом члене $a_\varkappa b_\lambda c_\mu$ имеется множителем один, и только один, элемент из каждой строки и один, и только один, элемент из каждого столбца.

IV. *Детерминант равен нулю, если элементы его двух рядов соответственно равны или пропорциональны.*

Доказательство. Это следует из II и III.

V. *Если элементы какого-нибудь ряда являются суммами k слагаемых, то детерминант представляется как сумма k детерминантов.*

Доказательство. В этом случае каждый член $\pm a_\varkappa b_\lambda c_\mu$ есть сумма k слагаемых, т. е. детерминант есть сумма k сумм, каждая из которых есть детерминант.

Следствие I. Если элементы одного ряда — суммы k слагаемых, элементы другого ряда — суммы l слагаемых, а элементы третьего ряда — суммы m слагаемых, то детерминант представляется как сумма klm детерминантов.

Следствие II. Детерминант не изменится, если к элементам какого-нибудь ряда прибавить соответствующие элементы другого ряда, умноженные на один и тот же множитель.

Это следует из V, III, IV.

VI. *Если все элементы какого-нибудь ряда равны нулю кроме одного, то детерминант равен произведению этого не равного нулю элемента на некоторый детерминант второго порядка.*

Доказательство. В этом случае не равны нулю только два члена, содержащие множителем этот не равный нулю элемент, который, следовательно, выносится за скобки; в скобках же остается детерминант второго порядка, получаемый, если вычеркнуть ту строку и тот столбец, к которым принадлежит вынесенный за скобки элемент, и приписать множитель $(-1)^r$, где r — сумма номеров вычеркнутых строки и столбца.

Пример.

$$\begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & 0 \\ a_3 & b_3 & 0 \end{vmatrix} = c_1 \cdot (-1)^{1+3} \begin{vmatrix} a_2 & b_2 \\ a_3 & b_3 \end{vmatrix} = c_1(a_2b_3 - a_3b_2).$$

Получаемый таким образом детерминант второго порядка $a_2b_3 - a_3b_2$ называется *минором*, соответствующим выносимому за скобки элементу c_{1r} [10].

Свойство VI вмес!е с предыдущим следствием II позволяет вычисление детерминанта третьего порядка свести к вычислению детерминанта второго порядка; покажем это на примере.

[10]Некоторые авторы называют минором самый детерминант 2-го порядка, без множителя $(-1)^r$, называя *алгебраическим дополнением* то, что мы назвали минором [т. е. детерминант вместе с множителем $(-1)^r$]. Я считаю нерациональным введение большого количества разных названий, тем более, что минор без множителя $(-1)^r$ в дальнейшем нигде не применяется.

Пример 1. Вычислить детерминант

$$D = \begin{vmatrix} 3 & 2 & 5 \\ 1 & 3 & -4 \\ -2 & 5 & 3 \end{vmatrix}.$$

Прибавим сначала к элементам первой строки соответствующие элементы второй строки, умноженные на -3, а затем к элементам третьей строки — элементы второй, умноженные на 2; от этого по следствию II детерминант не изменится; получим

$$D = \begin{vmatrix} 3-3\cdot 1 & 2-3\cdot 3 & 5+3\cdot 4 \\ 1 & 3 & -4 \\ -2 & 5 & 3 \end{vmatrix} = \begin{vmatrix} 0 & -7 & 17 \\ 1 & 3 & -4 \\ -2 & 5 & 3 \end{vmatrix} = \begin{vmatrix} 0 & -7 & 17 \\ 1 & 3 & -4 \\ 0 & 11 & -5 \end{vmatrix};$$

теперь по свойству VI получаем:

$$D = (-1)^{1+2} \begin{vmatrix} -7 & 17 \\ 11 & -5 \end{vmatrix} = -(35 - 187) = 152.$$

Пример 2. Вычислить детерминант

$$\begin{vmatrix} 1 & a & a^2 \\ 1 & b & b^2 \\ 1 & c & c^2 \end{vmatrix}.$$

Вычитая из второй и из третьей строк первую, найдем:

$$\begin{vmatrix} 1 & a & a^2 \\ 1 & b & b^2 \\ 1 & c & c^2 \end{vmatrix} = \begin{vmatrix} 1 & a & a^2 \\ 0 & b-a & b^2-a^2 \\ 0 & c-a & c^2-a^2 \end{vmatrix} = \begin{vmatrix} b-a & b^2-a^2 \\ c-a & c^2-a^2 \end{vmatrix}$$
$$= (b-a)(c-a) \begin{vmatrix} 1 & b+a \\ 1 & c+a \end{vmatrix} = (b-a)(c-a)(c-b).$$

Упражнение

39) Вычислить указанным приемом детерминанты

$$\begin{vmatrix} 3 & 2 & 1 \\ 4 & 3 & 1 \\ 2 & 1 & 2 \end{vmatrix}, \qquad \begin{vmatrix} 5 & 4 & 2 \\ 3 & 2 & -3 \\ 1 & -3 & 5 \end{vmatrix}.$$

Отв. 1, -89.

§ 20. Теорема умножения. Возьмем детерминант

$$\begin{vmatrix} a_1x_1 + b_1y_1 + c_1z_1 & a_1x_2 + b_1y_2 + c_1z_2 & a_1x_3 + b_1y_3 + c_1z_3 \\ a_2x_1 + b_2y_1 + c_2z_1 & a_2x_2 + b_2y_2 + c_2z_2 & a_2x_3 + b_2y_3 + c_2z_3 \\ a_3x_1 + b_3y_1 + c_3z_1 & a_3x_2 + b_3y_2 + c_3z_2 & a_3x_3 + b_3y_3 + c_3z_3 \end{vmatrix};$$

по V он представляется как сумма 27 детерминантов. Но из них 21 детерминант по IV равны нулю, так как в этих детерминантах имеются пропорциональные столбцы. Остаются следующие 6 детерминантов:

$$\begin{vmatrix} a_1x_1 & b_1y_2 & c_1z_3 \\ a_2x_1 & b_2y_2 & c_2z_3 \\ a_3x_1 & b_3y_2 & c_3z_3 \end{vmatrix} = x_1y_2z_3D, \qquad \begin{vmatrix} a_1x_1 & b_1z_2 & c_1y_3 \\ a_2x_1 & b_2z_2 & c_2y_3 \\ a_3x_1 & b_3y_2 & c_3z_3 \end{vmatrix} = -x_1y_3z_2D,$$

$$\begin{vmatrix} a_1y_1 & b_1x_2 & c_1z_3 \\ a_2y_1 & b_2x_2 & c_2z_3 \\ a_3y_1 & b_3x_2 & c_3z_3 \end{vmatrix} = -x_2y_1z_3D, \qquad \begin{vmatrix} a_1y_1 & b_1z_2 & c_1x_3 \\ a_2y_1 & b_2z_2 & c_2x_3 \\ a_3y_1 & b_3z_2 & c_3x_3 \end{vmatrix} = x_3y_1z_2D,$$

$$\begin{vmatrix} a_1z_1 & b_1x_2 & c_1y_3 \\ a_2z_1 & b_2x_2 & c_2y_3 \\ a_3z_1 & b_3x_2 & c_3y_3 \end{vmatrix} = x_2y_3z_1D, \qquad \begin{vmatrix} a_1z_1 & b_1y_2 & c_1x_3 \\ a_2z_1 & b_2y_2 & c_2x_3 \\ a_3z_1 & b_3y_2 & c_3x_3 \end{vmatrix} = -x_3y_2z_1D,$$

где

$$D = \begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix}.$$

Сумма всех этих детерминантов равна

$$\begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix} \cdot \begin{vmatrix} x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \\ x_3 & y_3 & z_3 \end{vmatrix}.$$

Итак, *произведение двух детерминантов третьего порядка, есть тоже детерминант третьего порядка.* И здесь, как и у детерминантов второго порядка, возможны четыре способа составления произведения:

1) комбинирование строк со строками;
2) ″ столбцов со строками;
3) ″ строк со столбцами;
4) ″ столбцов со столбцами.

Особенно важны способы 1) и 3).

Пример.

$$\begin{vmatrix} 3 & -2 & 1 \\ 1 & 4 & -3 \\ 2 & -1 & 2 \end{vmatrix} \cdot \begin{vmatrix} 1 & 2 & -1 \\ 3 & 2 & 1 \\ 2 & 1 & 3 \end{vmatrix} = \begin{vmatrix} -2 & 6 & 7 \\ 12 & 8 & -3 \\ -2 & 6 & 9 \end{vmatrix} = \begin{vmatrix} 3 & 13 & 13 \\ 7 & 1 & -3 \\ -7 & -1 & 5 \end{vmatrix} =$$

$$= \begin{vmatrix} -1 & 3 & -2 \\ 7 & 7 & -6 \\ 3 & 4 & 3 \end{vmatrix} = \begin{vmatrix} 10 & 10 & 4 \\ 8 & 3 & 3 \\ -4 & -2 & 2 \end{vmatrix} = -176.$$

Упражнение

40) Перемножить всеми четырьмя способами

$$\begin{vmatrix} 3 & 1 & 2 \\ 1 & 2 & 4 \\ 2 & 4 & 1 \end{vmatrix} \cdot \begin{vmatrix} 0 & 3 & 1 \\ -3 & 0 & 2 \\ -1 & -2 & 0 \end{vmatrix}.$$

Отв.
$$\begin{vmatrix} 5 & -5 & -5 \\ 10 & 5 & -5 \\ 13 & -4 & -10 \end{vmatrix} = \begin{vmatrix} -5 & 5 & 5 \\ -10 & -5 & 5 \\ -13 & 4 & 10 \end{vmatrix} = 0.$$

§ 21. Разложение детерминанта третьего порядка по минорам. Определение минора, соответствующего данному элементу, дано в конце § 19. Миноры мы обозначаем большими буквами с теми же индексами, что и у соответствующих им элементов. Имеем (по V и VI § 19)

$$\begin{aligned} D &= \begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix} = \begin{vmatrix} a_1+0+0 & 0+b_1+0 & 0+0+c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix} = \\ &= \begin{vmatrix} a_1 & 0 & 0 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix} + \begin{vmatrix} 0 & b_1 & 0 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix} + \begin{vmatrix} 0 & 0 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix} = A_1a_1 + B_1b_1 + C_1c_1. \end{aligned}$$

Применяя этот прием ко всем строкам и столбцам, получаем в итоге

$$\left.\begin{aligned} A_1a_1 + B_1b_1 + C_1c_1 &= D, & A_1a_1 + A_2a_2 + A_3a_3 &= D, \\ A_2a_2 + B_2b_2 + C_2c_2 &= D, & B_1b_1 + B_2b_2 + B_3b_3 &= D, \\ A_3a_3 + B_3b_3 + C_3c_3 &= D, & C_1c_1 + C_2c_2 + C_3c_3 &= D. \end{aligned}\right\} \tag{3}$$

С другой стороны,
$$A_1a_2 + B_1b_2 + C_1c_2 = 0,$$
ибо левая часть есть детерминант
$$\begin{vmatrix} a_2 & b_2 & c_2 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix},$$
который равен нулю по IV § 19.

Подобно же найдем

$$\left.\begin{aligned} A_1a_2 + B_1b_2 + C_1c_2 &= 0, & A_1b_1 + A_2b_2 + A_3b_3 &= 0, \\ A_2a_1 + B_2b_1 + C_2c_1 &= 0, & B_1a_1 + B_2a_2 + B_3a_3 &= 0, \\ A_1a_3 + B_1b_3 + C_1c_3 &= 0, & A_1c_1 + A_2c_2 + A_3c_3 &= 0, \\ A_3a_1 + B_3b_1 + C_3c_1 &= 0, & C_1a_1 + C_2a_2 + C_3a_3 &= 0, \\ A_2a_3 + B_2b_3 + C_2c_3 &= 0, & B_1c_1 + B_2c_2 + B_3c_3 &= 0, \\ A_3a_2 + B_3b_2 + C_3c_2 &= 0, & C_1b_1 + C_2b_2 + C_3b_3 &= 0, \end{aligned}\right\} \tag{4}$$

Детерминант
$$\begin{vmatrix} A_1 & B_1 & C_1 \\ A_2 & B_2 & C_2 \\ A_3 & B_3 & C_3 \end{vmatrix}$$

составленный из миноров, называется *взаимным* к детерминанту D. По теореме умножения и по (3) и (4) найдем:

$$\begin{vmatrix} A_1 & B_1 & C_1 \\ A_2 & B_2 & C_2 \\ A_3 & B_3 & C_3 \end{vmatrix} \cdot \begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix} = \begin{vmatrix} D & 0 & 0 \\ 0 & D & 0 \\ 0 & 0 & D \end{vmatrix} = D^3,$$

т. е.

$$\begin{vmatrix} A_1 & B_1 & C_1 \\ A_2 & B_2 & C_2 \\ A_3 & B_3 & C_3 \end{vmatrix} = \begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix}^2.$$

Упражнения

41) Дан детерминант

$$\begin{vmatrix} 3 & 2 & -5 \\ -1 & 1 & 3 \\ -1 & 3 & -4 \end{vmatrix};$$

найти, его миноры и проверить, что взаимный детерминант равен квадрату данного.

42) Вычислить детерминант

$$\begin{vmatrix} 3 & 2 & 5 \\ 1 & 4 & 5 \\ 3 & 1 & 7 \end{vmatrix},$$

разложив его по элементам первой колонны.

Отв. 33.

§ 22. Однородные уравнения. Рассмотрим систему трех однородных уравнений с четырьмя неизвестными:

$$\begin{aligned} a_1x + b_1y + c_1z + d_1t &= 0, \\ a_2x + b_2y + c_2z + d_2t &= 0, \\ a_3x + b_3y + c_3z + d_3t &= 0. \end{aligned}$$

Рассматривая t как известное, решим эту систему относительно x, y, z; при этом обозначим для сокращения

$$\begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix} = (a, b, c)$$

и подобно же другие детерминанты.

Найдем:

$$x = \frac{(-dt, b, c)}{(a, b, c)} = -t\frac{(b, c, d)}{(a, b, c)}, \qquad y = \frac{a, -dt, c)}{(a, b, c)} = +t\frac{(a, c, d)}{(a, b, c)},$$
$$z = -t\frac{(a, b, d)}{(a, b, c)}.$$

Следовательно:

$$x : y : z : t == -(b.c.d) : (a, c, d) : -(a, b, d) : (a, b, c).$$

Эта формула верна, если хоть один из детерминантов правой части не равен нулю; в этом случае три однородных уравнения с четырьмя неизвестными однозначно определяют отношения этих неизвестных.

Упражнение

43) Даны уравнения:

$$2x + y - 3z + 2t = 0,$$
$$3x - 2y - 4z + 3t = 0,$$
$$x - 4y - 2z - 2t = 0.$$

Найти отношения неизвестных.

Отв. $x : y : z : t = 38 : 3 : 21 : -8$.

§ 23. Перестановки n символов. *Перестановки* (расположения) определяются в элементарной алгебре. Число всех перестановок n символов равно $n! = 1 \cdot 2 \cdot 3 \cdots n$. Перестановка двух символов друг с другом называется транспозицией,

Теорема. *Все $n!$ перестановок n символов можно расположить в таком порядке, чтобы каждая следующая получалась из предыдущей путем одной транспозиции.*

Доказательство. Это очевидно при $n = 2$. Применим способ полной индукции; пусть теорема верна для $n - 1$ символов; докажем, что она верна и для n символов. Напишем сначала все перестановки с первым символом 1; число их равно $(n - 1)!$, и по предположению они могут быть расположены в таком порядке, что каждая следующая получается из предыдущей посредством одной транспозиции; теперь переставим символы 1 и 2 и напишем по тому же принципу все перестановки с первым символом 2; затем переставим 2 и 3 и т. д.

Пример. $n = 3$: $123; 132; 231; 213; 312; 321$.

§ 24. Инверсии. Если в перестановке символ с высшим номером стоит раньше символа с низшим номером, то такое явление называется *инверсией* (иначе: *нарушением*, *беспорядком*). В расположении $123 \ldots n$ нет ни одной инверсии; во всяком другом расположении всегда бывают инверсии. Каждый символ дает столько инверсий, сколько символов с меньшим номером следует за ним.

Например, при $n = 7$ перестановка 6312475 имеет 8 инверсий.

Теорема. *От одной транспозиции число инверсий в перестановке изменяется на нечетное число.*

Доказательство. Рассмотрим сначала случай, когда переставляемые символы g и h стоят рядом; в таком случае ясно, что от перестановки g и h друг с другом число инверсий или увеличится на единицу или уменьшится на единицу.

Возьмем теперь общий случай: дана перестановка

$$a_1 a_2 \ldots a_k g b_1 b_2 \ldots h c_1 c_2 \ldots c_m, \qquad \text{(A)}$$

которая после нашей транспозиции переходит в

$$a_1a_2\dots a_khb_1b_2\dots gc_1c_2\dots c_m,. \qquad \text{(B)}$$

Но для того чтобы от (A) перейти к (B), надо сначала g переставить с b_1, затем g переставить с b_2 и т. д., наконец, g переставить с h, далее g переставить с h, затем h переставить с b_l, затем h переставить с b_{l-1} и т. д., наконец, h переставить с b_1. Каждая такая перестановка есть транспозиция двух рядом стоящих символов, т. е. представляет собою уже рассмотренный частный случай; мы знаем, что от этого число инверсий изменяется (т. е. увеличивается или уменьшается) каждый раз на единицу; всего таких транспозиций при переходе от (A) к (B) у нас $l+1+l = 2l+1$.

Ясно, что при переходе от (A) к (B) и число инверсий в нашей перестановке изменится на нечетное число, ибо сумма нечетного числа положительных и отрицательных единиц есть число нечетное [11].

Различают перестановки двух родов: первого рода — с четным числом инверсий и второго рода — с нечетным числом инверсий. По теореме § 23 число тех и других одинаково и равно $\frac{1}{2}\,n!$.

Число транспозиций при переходе от одной перестановки к другой или всегда четное (если перестановки одного рода), или всегда нечетное (если перестановки разных родов).

Упражнение

44) Определить числа инверсий в перестановках 1) 20314, 2) 3560124, 3) 3024159867, 4) 4921650873.

Отв. 1) 3, 2) 11, 3) 10, 4) 23.

§ 25. Символ Кронекера. Если $\alpha\beta\gamma\dots\theta$ — некоторая перестановка чисел $1, 2, 3, \dots, n$, то символ Кронекера $[\alpha\beta\gamma\dots\theta]$ определяется так: $[\alpha\beta\gamma\dots\theta] = +1$, если перестановка $\alpha\beta\gamma\dots\theta$ первого рода, и $[\alpha\beta\gamma\dots\theta] = -1$, если эта перестановка второго рода. Другими словами, если ω — число инверсий в перестановке $\alpha\beta\gamma\dots\theta$, то

$$[\alpha\beta\gamma\dots\theta] = (-1)^{\omega}.$$

Выведем следующую формулу:

$$[\alpha\beta\gamma\dots\theta\varkappa\lambda\dots\tau] = [\alpha\beta\gamma\dots\theta]\ [\varkappa\lambda\dots\tau]\cdot(-1)^{\alpha+\beta+\gamma+\dots+\theta-\frac{r(r+1}{2}}, \qquad (5)$$

где r — число символов $\alpha, \beta, \gamma, \dots, \theta$.

Пусть сперва $\alpha < \beta < \gamma < \dots < \theta$ и $\varkappa < \lambda < \dots < \tau$, все же вместе символы $\alpha\beta\gamma\dots\theta\varkappa\lambda\dots\tau$ суть: $1, 2, \dots, n$, только в другом порядке. Между собой $\alpha, \beta, \gamma, \dots, \theta$, равно как и $\varkappa, \lambda, \dots, \tau$, не образуют ни одной инверсии. Если $\alpha > 1$, то $\varkappa = 1$, и α образует с $\varkappa, \lambda, \dots, \tau$, $\alpha - 1$ инверсию, ибо все символы, меньшие чем α, находятся среди $\varkappa, \lambda, \dots, \tau$. Точно так же β образует с $\varkappa, \lambda, \dots, \tau$ — $\beta - 2$

[11] Если отрицательных единиц k, то положительных $2l+1-k$ сумма всех есть

$$2l+1-k-k = 2(l-k)+1$$

— нечетное число.

инверсии, ибо все символы, меньшие чем β, кроме α, находятся среди $\varkappa, \lambda, \ldots, \tau$. Аналогично γ образует с $\varkappa, \lambda, \ldots, \tau$ — $\gamma - 3$ инверсии и т. д. Следовательно, число всех инверсий будет:

$$\alpha - 1 + \beta - 2 + \gamma - 3 + \ldots + \theta - r = \alpha + \beta + \gamma + \ldots + \theta - (1 + 2 + 3 + \ldots + r) =$$
$$= \alpha + \beta + \gamma + \ldots + +\theta - \frac{r(r+1)}{2}.$$

Если условия $\alpha < \beta < \gamma < \ldots < \theta$ и $\varkappa < \lambda < \ldots < \tau$ не выполнены, то к найденному числу следует прибавить еще число инверсий, которые образуют $\alpha, \beta, \gamma, \ldots, \theta$ между собой и $\varkappa, \lambda, \ldots, \tau$ между собой. Таким образом и получаем формулу (5).

Упражнение

45) Проверить формулу

$$[36520714] = [3652][0714] \cdot (-1)^{3+6+5+2-\frac{4\cdot 3}{2}}.$$

§ 26. Подстановки. Слово «перестановка» имеет двоякий смысл: во-первых, это слово, как было уже указано в начале § 23, означает определенное расположение данных предметов (символов); во-вторых, оно может означать и самое действие, перестанавливание данных символов, т. е. переход от одного их расположения к другому; для обозначения этого действия употребляется еще и термин подстановка, ибо тут мы вместо каждого из данных символов подставляем некоторый другой символ—тоже из данных (в частном случае можем оставить символ и без изменения, т. е. подставить вместо него его же самого). Так, если мы имеем 6 символов, обозначаемых номерами $1, 2, 3, 4, 5, 6$, и от расположения 314625 переходим к расположению 624153, то при этом переходе мы подставляем 6 вместо 3, 2 вместо 1, 4 вместо 4, 1 вместо 6, 5 вместо 2 и 3 вместо 5. Это обозначают тем, что просто пишут подставляемые символы под теми, вместо которых они подставляются, и затем берут все в скобки; например, рассматриваемая подстановка напишется так:

$$\begin{pmatrix} 3 & 1 & 4 & 6 & 2 & 5 \\ 6 & 2 & 4 & 1 & 5 & 3 \end{pmatrix}.$$

В подстановке важны не самые расположения символов, а то, какими именно символами какие символы заменяются, т. е. одно из расположений (верхнее или нижнее) мы можем выбрать произвольно; таким образом, например, вышеприведенную подстановку можно представить в таких формах:

$$\begin{pmatrix} 3 & 1 & 4 & 6 & 2 & 5 \\ 6 & 2 & 4 & 1 & 5 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 6 & 4 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 6 & 1 & 5 & 4 & 2 & 3 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} =$$
$$\begin{pmatrix} 5 & 4 & 6 & 1 & 3 & 2 \\ 3 & 4 & 1 & 2 & 6 & 5 \end{pmatrix}$$

и т. д. Это все — разные виды одной и той же подстановки, ибо всюду 1 переходит в 2, 2 в 5, 3 в 6, 4 в 4, 5 в 3, 6 в 1.

Обычно верхнее расположение берут «нормальным», т. е. в виде $12345\ldots$; нижнее же может быть любой перестановкой данных символов, и разные перестановки дают и разные подстановки. Следовательно, различных подстановок столько же, сколько и различных перестановок, т. е. $n!$, если и число всех наших символов. В дальнейшем мы часто будем сокращенно обозначать подстановки большими латинскими буквами.

Пусть нам даны две подстановки, например, восьми символов:

$$A = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 1 & 8 & 5 & 6 & 4 & 2 & 7 \end{pmatrix},$$
$$B = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 5 & 6 & 2 & 7 & 1 & 4 & 3 \end{pmatrix};$$

будем производить эти подстановки последовательно; в результате получим одну подстановку C, как «равнодействующую» этих двух, следующим образом: в A 1 переходит в 3, в B 3 переходит в 6, значит в C 1 перейдет в 6; в A 2 переходит в 1, в B 1 переходит в 8, значит в C 2 перейдет в 8 и т. д.

Найдем

$$C = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 8 & 3 & 7 & 1 & 2 & 5 & 4 \end{pmatrix}.$$

Это соединение двух подстановок в одну называется *композицией* или (символическим) *умножением* подстановок; C называется *произведением* A на B; обозначают:

$$C = AB;$$

причем порядок, в каком стоят «сомножители», не произволен, т. е. для этого символического умножения подстановок коммутативный закон неверен. Так, в данном примере

$$BA = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 6 & 4 & 1 & 2 & 3 & 5 & 8 \end{pmatrix} \neq AB.$$

Но в некоторых частных случаях коммутативный закон может оказаться верным; две подстановки, для произведения которых верен коммутативный закон, называются *переместимыми* (или *перестановочными*; говорят также, что они *коммутируют* друг с другом). Например, подстановки

$$A = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 5 & 6 & 1 & 2 \end{pmatrix}$$

и

$$B = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 6 & 5 & 2 & 1 \end{pmatrix}$$

переместимы, ибо

$$AB = BA = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 2 & 1 & 3 & 4 \end{pmatrix}.$$

Докажем, что ассоциативный закон (см. гл. 1, § 3,3) верен для произведения всяких подстановок. Обозначим сокращенно подстановку A символом $\begin{pmatrix} r \\ s \end{pmatrix}$; здесь r

означает верхнее (начальное) расположение наших символов, а ss — нижнее (конечное) их расположение; подстановку B мы можем взять в таком виде; $\binom{s}{t}$, т. е. верхнее расположение в B взять такое же, что и нижнее расположение в A, ибо ведь одно из расположений в подстановке произвольно; наконец, возьмем еще подстановку C в таком виде: $\binom{t}{u}$. Тогда, очевидно,

$$AB = \binom{r}{s}\binom{s}{t} = \binom{r}{t};$$

аналогично

$$BC = \binom{s}{t}\binom{t}{u} = \binom{s}{u}.$$

Тогда

$$(AB)C = \binom{r}{t}\binom{t}{u} = \binom{r}{u},$$

$$A(BC) = \binom{r}{s}\binom{s}{u} = \binom{r}{u},$$

следовательно:

$$(AB)C = A(BC),$$

что и требовалось доказать. Таким образом произведение перестановок A, B и C мы можем просто записывать в виде ABC. Отсюда легко следует, что в произведении нескольких подстановок мы можем по нашему желанию заключать в скобки любую часть этого произведения, или уничтожать имеющиеся скобки, лишь бы только мы при этом не переставляли сомножителей.

Обратим внимание на подстановку, в которой нижнее расположение одинаково с верхним:

$$\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ 1 & 2 & 3 & \dots & n \end{pmatrix};$$

здесь каждый символ заменяется им же самим, т. е. собственно никакой «подстановки» и не происходит, это — так называемая тождественная или единичная или главная подстановка; мы ее обозначим буквою ?E [12]. При композиции подстановок она играет роль единицы, ибо, если A — любая подстановка тех же символов, то, как легко убедиться,

$$AE = EA = A.$$

Мы видим, что E переместима со всякой другой подстановкой тех же символов; в частности $EE = E$.

Если в данной подстановке A мы переставим друг с другом верхнее и нижнее расположения, то получим новую подстановку, которая называется обратной к A и обозначается в виде (-1)-й степени A, т. е. в виде A^{-1}. Очевидно, обратная к обратной есть данная подстановка, т. е.

$$(A^{-1})^{-1} = A.$$

[12]Некоторые авторы обозначают ее просто цифрой 1.

Обе взаимно обратные подстановки переместимы и дают при композиции друг с другом тождественную подстановку:

$$AA^{-1} = A^{-1}A = E.$$

Пример.

$$A = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 5 & 6 & 4 & 3 & 1 \end{pmatrix}, \qquad A^{-1} = \begin{pmatrix} 2 & 5 & 6 & 3 & 3 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 5 & 4 & 2 & 3 \end{pmatrix}.$$

Упражнения

46) «Перемножить» подстановки:

а) $\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 0 & 2 & 1 & 5 & 4 & 6 & 7 \end{pmatrix}$ и $\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 3 & 5 & 4 & 1 & 0 & 7 & 6 & 2 \end{pmatrix}$,

б) $\begin{pmatrix} \alpha & \beta & \gamma & \delta & \varepsilon \\ \alpha & \gamma & \varepsilon & \beta & \delta \end{pmatrix}$ и $\begin{pmatrix} \alpha & \beta & \gamma & \delta & \varepsilon \\ & \gamma & \delta & \alpha & \beta \end{pmatrix}$,

в) $\begin{pmatrix} x_1 & x_2 & x_3 & x_4 & x_5 & x_6 \\ x_3 & x_1 & x_5 & x_6 & x_4 & x_2 \end{pmatrix}$ и $\begin{pmatrix} x_1 & x_2 & x_3 & x_4 & x_5 & x_6 \\ x_2 & x_6 & x_1 & x_5 & x_3 & x_4 \end{pmatrix}$.

Отв.

$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 2 & 8 & 5 & 3 & 0 & 1 & 7 & 6 \end{pmatrix}$ или $\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 2 & 5 & 1 & 1 & 8 & 3 & 6 & 0 \end{pmatrix}$

$\begin{pmatrix} \alpha & \beta & \gamma & \delta & \varepsilon \\ \varepsilon & \delta & \beta & \gamma & \alpha \end{pmatrix}$ или $\begin{pmatrix} \alpha & \beta & \gamma & \delta & \varepsilon \\ \delta & \varepsilon & \beta & \alpha & \gamma \end{pmatrix}$, в) E.

47) Проверить ассоциативный закон на подстановках:

$$A = \begin{pmatrix} a & b & c & d \\ b & a & d & c \end{pmatrix}, \qquad B = \begin{pmatrix} a & b & c & d \\ d & a & b & c \end{pmatrix}, \qquad C = \begin{pmatrix} a & b & c & d \\ d & c & b & a \end{pmatrix}.$$

48) Найти обратные к следующим подстановкам:

а) $\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 0 & 5 & 1 & 6 & 3 & 2 & 4 \end{pmatrix}$, б) $\begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_5 & a_1 & a_2 & a_3 & a_4 \end{pmatrix}$

в) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 3 & 2 & 7 & 1 & 6 & 4 \end{pmatrix}$, г) E.

Отв.

а) $\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 3 & 6 & 5 & 7 & 2 & 4 & 0 \end{pmatrix}$, б) $\begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_5 & a_1 & a_2 & a_3 & a_4 \end{pmatrix}$,

в) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 3 & 2 & 7 & 1 & 6 & 4 \end{pmatrix}$, г) E.

§ 27. Понятие о группе. Рассмотрим совокупность всех подстановок данных n символов; всего этих подстановок $n!$ и они образуют замкнутую систему в

том смысле, что «произведение» всяких двух подстановок, взятых в определенном порядке, есть тоже подстановка тех же символов, т. е. принадлежит к той же совокупности. Это свойство такой замкнутости называется *групповым* свойством, а такая система (в данном случае — подстановок) называется *группой*. Итак, все $n!$ подстановок данных n символов составляют *группу*.

Вообще группой называется (конечная или бесконечная) совокупность каких-то элементов (не обязательно подстановок) такая, что над каждыми двумя (различными или равными) из этих элементов, взятыми в определенном порядке, определено действие (символически обычно обозначаемое как «умножение»), причем результат этого действия над двумя любыми элементами этой совокупности есть тоже элемент из той же совокупности. При этом действие в группе — не произвольно: оно должно подчиняться основным законам обычного действия сложения или умножения чисел, за исключением коммутативного закона; эти законы такие: ассоциативный закон, существование единицы, существование обратного элемента для каждого данного. Заметим, что каждый из этих законов имеет здесь две стороны — правую и левую, так как коммутативный закон не предполагается. В каждом конкретном случае следует проверить, верны ли эти законы; в предыдущем параграфе мы видели, что для композиции подстановок эти законы верны. Заметим, что законы неограниченной и однозначной обратимости (см. конец § 4 и § 5) являются следствиями из приведенных выше законов, т. е. для действия группы всегда выполнены; в частности они выполнены и для композиции подстановок. Закон неограниченной обратимости выражается так: *при данных элементах A и B всегда существуют такие элементы X и Y, что*

$$AX = B \qquad \text{(правая сторона)},$$
$$YA = B \qquad \text{(левая сторона)}.$$

Действительно, $X = A^{-1} \cdot B$, $Y = BA^{-1}$..

Закон однозначной обратимости выражается так:

$$\text{из} \quad AX_1 = AX_2 \quad \text{следует} \quad X_1 = X_2 \quad \text{(правая сторона)},$$
$$\text{из} \quad Y_1A = Y_2A \quad \text{следует} \quad Y_1 = Y_2 \text{(левая сторона)}.$$

Действительно, пусть $AX_1 = AX_2$; умножим обе части этого равенства слева на A^{-1}:

$$A^{-1}(AX_1) = A^{-1}(AX_2),$$

или, по ассоциативному закону,

$$(A^{-1}A)X_1 = (A^{-1}A)X_2;$$

или $AA^{-1}A = E$, следовательно, $EX_1 = EX_2$, или $X_1 = X_2$.

Подобно же доказывается и левая сторона.

Группа, в которой элементы не конкретизированы, которая, следовательно, определяется только законами своего действия, называется отвлеченной или *абстрактной*. Абстрактная теория групп, о которой речь будет итти в главе XI, благодаря своей общности имеет широкие применения можно сказать во всех областях математики и многих ее приложений. Всюду, где мы имеем какие-либо

конкретные элементы (числа, подстановки, матрицы, геометрические преобразования и т. п.) и конкретное действие над ними, — всюду там мы имеем группу, если только это действие подчиняется приведенным выше основным законам. Мы видели уже, что все подстановки данных n символов образуют группу, при этом конечную, так как всего таких подстановок $n!$, т. е. конечное число; говорят, что эта группа порядка $n!$. Приведем еще следующие примеры групп: все целые числа составляют группу относительно сложения; эта группа бесконечна; единицей группы здесь является число 0; обратным элементом к числу a служит число $-a$; все рациональные положительные числа составляют бесконечную группу относительно умножения, единицей здесь является число 1; обратный элемент к числу a есть число $\frac{1}{a}$; все вещественные числа составляют группу относительно сложения; все вещественные числа за исключением числа 0 составляют группу относительно умножения; подобно же и все комплексные числа (включая и вещественные как частный вид) составляют группу относительно сложения и — без числа 0 — относительно умножения; число 1 одно составляет группу относительно умножения; число 0 одно составляет группу относительно сложения.

В дальнейшем нам еще встретятся конкретные примеры групп.

§ 28. Разложение подстановок на транспозиции. Транспозиции, определенные в § 23, являются частными случаями подстановок, — именно, если в подстановке все символы остаются на своих местах кроме двух, которые меняются местами, т. е. переходят друг в друга. Если в транспозиции переставляются символы α и β, то мы будем обозначать такую транспозицию так:

$$(\alpha, \beta).$$

Эту транспозицию можно записать в виде обычной подстановки:

$$(\alpha,\beta) = \begin{pmatrix} 1 & 2 & \dots & \alpha & \dots & \beta & \dots & n \\ 1 & 2 & \dots & \beta & \dots & \alpha & \dots & n \end{pmatrix};$$

например, при $n = 8$:

$$(2,5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 5 & 3 & 4 & 2 & 6 & 7 & 8 \end{pmatrix}.$$

Теорема в § 23 гласит, что всякое расположение наших символов можно получить из «нормального» расположения посредством нескольких транспозиций, произведенных последовательно друг за другом; иными словами, всякую подстановку можно представить как произведение транспозиций, или разложить на транспозиции.

Пример.

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 7 & 1 & 5 & 6 & 4 & 3 \end{pmatrix} = (1,2)(1,7)(1,3)(4,5)(4,6) =$$
$$= (1,5)(1,7)(1,2)(1,6)(1,4)(1,3)(2,3)(2,5)(6,7).$$

Из этого примера видно, что разложение подстановки на транспозиции возможно многими способами, даже бесчисленным множеством способов, ибо ведь

всегда можно к данному произведению приписать (в конце его, или в начале, или даже в середине) сколько угодно раз по два множителя вида $(\alpha, \beta)(\alpha, \beta)$, взаимно уничтожающих друг друга [13].

Так как в «нормальном» расположении символов совсем нет инверсий, а от одной транспозиции число инверсий в перестановке меняется на нечетное число (по теореме § 24), то в нижнем расположении подстановки число инверсий четное или нечетное в зависимости от того, раскладывается ли она на четное или нечетное число транспозиций. А так как в данной подстановке при верхнем нормальном расположении нижнее расположение вполне определено, т. е. имеет и вполне определенное число инверсий, то этим доказано следующее:

Теорема. *Каким бы способом мы не раскладывали данную подстановку на транспозиции, число этих транспозиций будет всегда одной и той же четности, т. е. всегда четное, или всегда нечетное.*

Сообразно с этим все $n!$ подстановок данных n символов разделяются на два вида — на *четные* и *нечетные* подстановки; первые раскладываются на четное число транспозиций, вторые — на нечетное. А так как (§ 24) перестановок с четным числом инверсий столько же, сколько и с нечетным, то и подстановок четных столько же, сколько и нечетных: по $\frac{1}{2}n!$. Легко видеть следующее:

тождественная подстановка E четная;

транспозиция является нечетной подстановкой;

взаимно обратные подстановки имеют одну и ту же четность, т. е. или обе четные, или обе нечетные.

Последнее следует из того, что по самому определению обратной подстановки мы получим ее, если проделаем все транспозиции данной подстановки, только в обратном порядке, т. е. число их остается то же самое.

Отметим еще следующее очевидное предложение: если две подстановки различны, то обратные к ним подстановки тоже различны.

§ 29. Детерминант n-го порядка. Мы его определяем формулой:

$$\begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} = \sum [\varkappa\lambda\mu\dots\tau]\, a_{1\varkappa} a_{2\lambda} a_{3\mu} \cdots a_{n\tau}. \tag{6}$$

Он зависит от n^2 чисел, называемых его *элементами* и расположенных в n *строк* и n *столбцов*; строки и столбцы вместе мы будем называть *рядами*. Элементы детерминанта в общем виде мы будем обозначать одной буквою, например a, с двумя значками, из которых первый дает номер строки, а второй — номер столбца; так, $a_{\alpha\beta}$ есть элемент, стоящий на пересечении α-й строки и β-го столбца.

Значки $\varkappa, \lambda, \mu, \dots, \tau$ в формуле (6) означают какую-то перестановку чисел $1, 2, \dots, n$; сумма берется по всевозможным таким перестановкам вторых значков (т. е. номеров столбцов); символ Кронекера $[\varkappa\lambda\mu\dots\tau]$ дает знак $+$ или $-$ в зависимости от того, будет ли $\varkappa, \lambda, \mu, \dots, \tau$ четной или нечетной перестановкой (§ 24, 25). Таким образом в D всего $n!$ слагаемых, из которых половина со знаком

[13] Именно $(\alpha, \beta)(\alpha, \beta) = E$.

+, а половина со знаком −. Легко видеть, что определенные выше (§ 14, 18) детерминанты второго и третьего порядков — частные случаи определенного теперь детерминанта n-го порядка.

Элементы детерминанта могут быть какими угодно числами, как вещественными, так и комплексными.

Существуют еще такие сокращенные обозначения детерминанта в общем виде:

$$D = \sum \pm a_{11}a_{22}\cdots a_{nn} \quad \text{(Jacobi)},$$

$$D = |a_{h1}a_{h2}\cdots a_{hn} \quad \text{(Kronecker)},$$

$$D = |a_{ik}| \quad \text{(S. Smith)}$$

$$i, k = 1, \ldots, n.$$

§ 30. Свойства детерминантов n-го порядка.

I. *Детерминант не изменится от перестановки строк со столбцами.*

Доказательство. Ее ли мы в произведении $a_{1\varkappa}a_{2\lambda}a_{3\mu}\cdots a_{n\tau}$ переставим сомножители так, чтобы вторые значки стали в нормальном расположении $123\ldots n$„ то первые значки, бывшие сначала в нормальном расположении, теперь будут в некотором расположении $\alpha\beta\gamma\ldots\theta$; этим мы произвели подстановку (§ 26), которую можно представить в таких двух видах:

$$\begin{pmatrix} \varkappa & \lambda & \mu & \ldots & \tau \\ 1 & 2 & 3 & \ldots & n \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ \alpha & \beta & \gamma & \ldots & \theta \end{pmatrix};$$

подстановка эта обратная к подстановке

$$\begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ \varkappa & \lambda & \mu & \ldots & \tau \end{pmatrix},$$

а следовательно, одинаковой с нею четности (§ 28); но подстановка с верхним нормальным расположением четная или нечетная в зависимости от того, имеет ли нижнее ее расположение четное или нечетное число инверсий (§ 28); а отсюда следует, что расположения $\varkappa\lambda\mu\ldots\tau$ и ? имеют числа инверсий одинаковой четности, т. е. соответствующие символы Кронекера (§ 25) равны:

$$[\varkappa\lambda\mu\ldots\tau] = [\alpha\beta\gamma\ldots\theta];$$

следовательно:

$$[\varkappa\lambda\mu\ldots\tau]a_{1\varkappa}a_{2\lambda}a_{3\mu}\cdots a_{n\tau} = [\alpha\beta\gamma\ldots\theta]a_{\alpha1}a_{\beta2}a_{\gamma3}\cdots a_{\theta n}.$$

Проделав такую операцию в каждом члене суммы правой части (6), получим:

$$D = \sum [\alpha\beta\gamma\ldots\theta]a_{\alpha1}a_{\beta2}a_{\gamma3}\cdots a_{\theta n}, \tag{7}$$

причем сумма берется по всевозможным перестановкам первых значков (т. е. номеров строк), ибо разным перестановкам $\varkappa\lambda\mu\ldots\tau$ вторых значков в (6) соответствуют разные перестановки первых значков $\alpha\beta\gamma\ldots\theta$ в (7) (см. конец § 28). Но в

(7) строки играют ту же роль, что столбцы в (6), т. е. мы получим (7) из (6), переставив в детерминанте строки со столбцами; от этого, как мы видим, величина детерминанта не изменится.

Следствие. Из свойства I вытекает, что все, что мы докажем для строк, будет верно и для столбцов, и обратно, т. е. чтобы доказать какое-либо свойство детерминанта, верное и для строк, и для столбцов, достаточно доказать его только для строк (или только для столбцов).

II. *От перестановки двух строк (или двух столбцов) детерминант меняет знак.*

Доказательство. Возьмем детерминант в виде (6) и переставим, например, первую и вторую строки; это сведется к тому, что вместо произведения $a_{1\varkappa}a_{2\lambda}a_{3\mu}\cdots a_{n\tau}$ мы должны взять

$$a_{2\varkappa}a_{1\lambda}a_{3\mu}\cdots a_{n\tau} = a_{1\lambda}a_{2\varkappa}a_{2\lambda}a_{3\mu}\cdots a_{n\tau}$$

т. е. значки $\varkappa$ и λ переменились местами. Итак, от этой перестановки (т. е. транспозиции $(\varkappa, \lambda)$ в каждом члене) наш детерминант D перейдет в такой:

$$\sum[\varkappa\lambda\mu\ldots\tau]a_{1\varkappa}a_{2\lambda}a_{3\mu}\cdots a_{n\tau} = -\sum[\lambda\varkappa\mu\ldots\tau]a_{1\lambda}a_{2\varkappa}a_{3\mu}\cdots a_{n\tau},$$

ибо от одной транспозиции символ Кронекера изменит знак; но в правой части у нас стоит $-D$, ибо сумма та же, что и в (6), только обозначение несколько иное: $\varkappa$ поставлена вместо λ, а λ вместо $\varkappa$; итак, детерминант действительно изменил знак. То же будет, если переставим любые две строки или любые два столбца.

Следствие. Если сделаем в строках детерминанта такую перестановку: на первом месте поставим α-ю строку, на втором β-ю, на третьем γ-ю и т. д., на n-м θ-ю, и одновременно в столбцах сделаем такую перестановку: на первом месте поставим $\varkappa$-й столбец, на втором λ-й, на третьем — μ-й и т. д., на n-м τ-й (причем $\alpha\beta\gamma\ldots\theta$ и $\varkappa\lambda\mu\ldots\tau$ — какие-то две перестановки чисел $1, 2, \ldots, n$), то детерминант получит множитель

$$[\alpha\beta\gamma\ldots\theta]\ [\varkappa\lambda\mu\ldots\tau],$$

т. е.

$$\begin{vmatrix} a_{\alpha\varkappa} & a_{\alpha\lambda} & \ldots & a_{\alpha\tau} \\ a_{\beta\varkappa} & a_{\beta\lambda} & \ldots & a_{\beta\tau} \\ \ldots\ldots\ldots\ldots\ldots \\ a_{\theta\varkappa} & a_{\theta\lambda} & \ldots & a_{\theta\tau} \end{vmatrix} = [\alpha\beta\gamma\ldots\theta]\ [\varkappa\lambda\mu\ldots\tau] \begin{vmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots\ldots\ldots\ldots\ldots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{vmatrix}. \qquad (8)$$

Действительно, мы произвели со строками подстановку

$$\begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ \alpha & \beta & \gamma & \ldots & \theta \end{pmatrix}$$

а со столбцами подстановку

$$\begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ \varkappa & \lambda & \mu & \ldots & \tau \end{pmatrix};$$

каждая из этих подстановок разбивается на транспозиции (§ 28), а от каждой транспозиции детерминант меняет знак. Таким образом в конечном результате

детерминант не изменится или изменит знак в зависимости от того, четно ли или нечетно число всех транспозиций; с другой стороны (§ 28), число транспозиций, на которые раскладывается подстановка, той же четности, что и число инверсий в ее нижнем расположении (при нормальном верхнем); от того же, четное или нечетное число инверсий в расположении $\alpha\beta\gamma\ldots\theta$, и символ Кронекера $[\alpha\beta\gamma\ldots\theta]$ будет равен $+1$ или -1; то же справедливо и для $\varkappa\lambda\mu\ldots\tau$; этим и доказывается формула (8).

III. *Если все элементы одного ряда имеют общий множитель c, то его можно вынести за знак детерминанта.*

Доказательство. Это следует из того, что в каждый член детерминанта входит множителем по одному элемент из каждой строки и из каждого столбца, значит, в частности содержится множитель c.

IV. *Детерминант равен нулю, если элементы его двух рядов соответственно равны или пропорциональны.*

Это следует из II и III.

V. *Если элементы какого-нибудь ряда суть суммы k слагаемых, то детерминант представляется как сумма k детерминантов.*

Доказательство. Пусть, например,

$$a_{1\varkappa} = a'_{1\varkappa} + a''_{1\varkappa} \qquad (\varkappa = 1, 2, \ldots, n);$$

тогда

$$\begin{vmatrix} a'_{11}+a''_{11} & a'_{12}+a''_{12} & \ldots & a'_{1n}+a''_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{vmatrix} =$$

$$= \sum [\varkappa\lambda\ldots\tau](a'_{1\varkappa}+a''_{1\varkappa})a_{2\lambda}\cdots a_{2\tau} = \sum [\varkappa\lambda\ldots\tau]a'_{1\varkappa}a_{2\lambda}\cdots a_{2\tau} +$$

$$+ \sum [\varkappa\lambda\ldots\tau]a''_{1\varkappa}a_{2\lambda}\cdots a_{2\tau} =$$

$$= \begin{vmatrix} a'_{11} & a'_{12} & \ldots & a'_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{vmatrix} + \begin{vmatrix} a''_{11} & a''_{12} & \ldots & a''_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{vmatrix}.$$

Следствие I. Если элементы одного ряда — суммы k_1 слагаемых, элементы другого ряда — суммы k_2 слагаемых и т. д., элементы n-го ряда — суммы k_n слагаемых, то детерминант представляется как сумма $k_1k_2\cdots k_n$ детерминантов.

Следствие II. Детерминант не изменится, если к элементам какого-нибудь ряда прибавить элементы другого ряда, умноженные на один и тот же множитель.

Это следует из V, III, IV.

VI. *Если в детерминанте n-го порядка все элементы какого-нибудь ряда, кроме одного, равны нулю, то детерминант равен произведению этого не равного нулю элемента на некоторый детерминант $(n-1)$-го порядка.*

Доказательство. Пусть, например, все элементы первой строки, кроме a_{11}, равны нулю. Имеем:

$$\sum [\varkappa\lambda\mu\ldots\tau]a_{1\varkappa}a_{2\lambda}a_{3\mu}\cdots a_{n\tau} = \sum [1\lambda\ldots\tau]a_{11}a_{2\lambda}\cdots a_{n\tau},$$

ибо при $x > 1$ $a_{1x} = 0$. Во всех членах a_{11} входит множителем, следовательно, выносится за скобки; далее:

$$[1\lambda\mu\cdots\tau] = [\lambda\mu\cdots\tau],$$

следовательно:

$$D = a_{11}\sum[\lambda\mu\cdots\tau]a_{2\lambda}a_{3\mu}\cdots a_{n\tau} = a_{11}\begin{vmatrix} a_{22} & a_{23} & \dots & a_{2n} \\ a_{32} & a_{33} & \dots & a_{3n} \\ \dots & \dots & \dots & \dots \\ a_{n2} & a_{n3} & \dots & a_{nn} \end{vmatrix}$$

[см. (6)], т. е. для этого случая теорема доказана.

Пусть теперь все элементы α-й строки равны нулю кроме $a_{\alpha\beta}$. Ставим на первое место α-ю строку и β-й столбец так, чтобы элемент $a_{\alpha\beta}$ стал первым. От этого D получит знак [см. (8)]

$$[\alpha, 1, 2, \dots, \alpha-1, \alpha+1, \dots, n]\ [\beta, 1, 2, \dots, \beta-1, \beta+1, \dots, n] = (-1)^{\alpha-1}\cdot(-1)^{\beta-1} = (-1)^{\alpha+\beta}.$$

Введем еще обозначение:

$$\begin{vmatrix} a_{11} & \dots & a_{1,\beta-1} & a_{1,\beta+1} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ a_{\alpha-1,1} & \dots & a_{\alpha-1,\beta-1} & a_{\alpha-1,\beta+1} & \dots & a_{\alpha-1,n} \\ a_{\alpha+1,1} & \dots & a_{\alpha+1,\beta-1} & a_{\alpha+1,\beta+1} & \dots & a_{\alpha+1,n} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ a_{n1} & \dots & a_{n,\beta-1} & a_{n,\beta+1} & \dots & a_{nn} \end{vmatrix}\cdot(-1)^{\alpha+\beta} = A_{\alpha\beta},$$

так что $A_{\alpha\beta}$ получается из D вычеркиванием α-й строки и β-го столбца и присоединением множителя $(-1)^{\alpha+\beta}$. Тогда по-предыдущему:

$$D = a_{\alpha\beta}A_{\alpha\beta}.$$

$A_{\alpha\beta}$ есть минор $(n-1)$-го порядка, соответствующий элементу $a_{\alpha\beta}$. Если все элементы какого-нибудь столбца, кроме одного, равны нулю, то по I, переставив строки со столбцами, применяем то же рассуждение.

Следствие из свойства V и свойство VI применяются для вычисления детерминантов.

Пример 1.

$$\begin{vmatrix} 5 & 3 & -1 & 0 \\ 2 & 4 & 0 & 3 \\ 1 & 1 & 5 & 2 \\ 0 & 1 & 3 & 4 \end{vmatrix} = \begin{vmatrix} 5 & 3 & -1 & 0 \\ 2 & 4 & 0 & 3 \\ 1+5\cdot5 & 1+3\cdot5 & 5+(-1)\cdot5 & 2+0\cdot5 \\ 0+5\cdot3 & 1+3\cdot3 & 3+(-1)\cdot3 & 4+0\cdot3 \end{vmatrix} =$$

$$= \begin{vmatrix} 5 & 3 & -1 & 0 \\ 2 & 4 & 0 & 3 \\ 26 & 16 & 0 & 2 \\ 15 & 10 & 0 & 4 \end{vmatrix} = (-1)^{1+3}\cdot(-1)\cdot\begin{vmatrix} 2 & 4 & 3 \\ 26 & 16 & 2 \\ 15 & 10 & 4 \end{vmatrix} =$$

$$= (-1)^4 \cdot (-1) \cdot 4 \cdot \begin{vmatrix} 2 & 2 & 3 \\ 13 & 4 & 1 \\ 15 & 5 & 4 \end{vmatrix} =$$

$$= -4 \cdot \begin{vmatrix} 2+13\cdot(-3) & 2+4\cdot(-3) & 3+1\cdot(-3) \\ 13 & 4 & 1 \\ 15+13\cdot(-4) & 5+4\cdot(-4) & 4+1\cdot(-4) \end{vmatrix} = 4 \cdot \begin{vmatrix} -37 & -10 & 0 \\ 13 & 4 & 1 \\ -37 & -11 & 0 \end{vmatrix} =$$

$$= -4 \cdot (-1)^{5+2} \cdot \begin{vmatrix} -37 & 10 \\ -37 & -11 \end{vmatrix} = 4 \cdot 37 \cdot \begin{vmatrix} 1 & 10 \\ 1 & 11 \end{vmatrix} = 4 \cdot 37 \cdot 1 = +148.$$

Пример 2.

$$\begin{vmatrix} 5 & 3 & 1 & 2 & 0 \\ 4 & 6 & 0 & 1 & -2 \\ -3 & 1 & -1 & 1 & 5 \\ 1 & 3 & 1 & 0 & 4 \\ 4 & 0 & 3 & -2 & -1 \end{vmatrix} =$$

$$= \begin{vmatrix} 5+1\cdot(-5) & 3+1\cdot(-3) & 1 & 2+1\cdot(-2) & 0 \\ 4+0\cdot(-5) & 6+0\cdot(-3) & 0 & 1+0\cdot(-2) & -2 \\ -3+(-1)(-5) & 1+(-1)(-3) & -1 & 1+(-1)(-2) & 5 \\ 1+1\cdot(-5) & 3+1\cdot(-2) & 1 & 0+1\cdot(-2) & 4 \\ 4+3\cdot(-5) & 0+3\cdot(-3) & 3 & -2+3\cdot(-2) & -1 \end{vmatrix} =$$

$$= \begin{vmatrix} 0 & 0 & 1 & 0 & 0 \\ 4 & 6 & 0 & 1 & -2 \\ 2 & 4 & -1 & 3 & 5 \\ -4 & 0 & 1 & -2 & 4 \\ -11 & -9 & 3 & -8 & -1 \end{vmatrix} =$$

$$= (-1)^{1+3} \cdot 1 \cdot \begin{vmatrix} 4 & 6 & 1 & -2 \\ 2 & 4 & 3 & 5 \\ -4 & 0 & -2 & 4 \\ -11 & -9 & -8 & -1 \end{vmatrix} = (-1) \cdot (-1) \cdot 2 \cdot \begin{vmatrix} 4 & 6 & 1 & -2 \\ 2 & 4 & 3 & 5 \\ 2 & 0 & 1 & -2 \\ 11 & 9 & 8 & 1 \end{vmatrix} =$$

$$= 2 \cdot \begin{vmatrix} 4+1\cdot(-2) & 6 & 1 & -2+1\cdot 2 \\ 2+3\cdot(-2) & 4 & 3 & 5+3\cdot 2 \\ 2+1\cdot(-2) & 0 & 1 & -2+1\cdot 2 \\ 11+8\cdot(-2) & 9 & 8 & 1+8\cdot 2 \end{vmatrix} = 2 \begin{vmatrix} 2 & 6 & 1 & 0 \\ -4 & 4 & 3 & 11 \\ 0 & 0 & 1 & 0 \\ -5 & 9 & 8 & 17 \end{vmatrix} =$$

$$= 2 \cdot (-1)^{3+3} \cdot 1 \cdot \begin{vmatrix} 2 & 6 & 0 \\ -4 & 4 & 11 \\ -5 & 9 & 17 \end{vmatrix} = 2 \cdot 2 \cdot \begin{vmatrix} 1 & 3 & 0 \\ -4 & 4 & 11 \\ -5 & 9 & 17 \end{vmatrix} =$$

$$= 4 \cdot \begin{vmatrix} 1 & 3+1\cdot(-3) & 0 \\ -4 & 4+(-4)(-3) & 11 \\ -5 & 9+(-5)(-3) & 17 \end{vmatrix} = 4 \cdot \begin{vmatrix} 1 & 0 & 0 \\ -4 & 16 & 17 \\ -5 & 24 & 17 \end{vmatrix} =$$

$$= 4 \cdot 8 \cdot \begin{vmatrix} 2 & 11 \\ 3 & 17 \end{vmatrix} = 32 \cdot (34 - 33) == 32.$$

Пример 3. 3. Детерминант Вандермонда (Vandermcmde):

$$D = \begin{vmatrix} 1 & a_1 & a_1^2 & \dots & a_1^{n-1} \\ 1 & a_2 & a_2^2 & \dots & a_2^{n-1} \\ 1 & a_3 & a_3^2 & \dots & a_3^{n-1} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & a_n & a_n^2 & \dots & a_n^{n-1} \end{vmatrix}.$$

Мы уже имели такой детерминант третьего порядка (см. § 19, пример 2) и видели, что он равен произведению разностей входящих в него величин. Докажем то же самое и для нашего детерминанта n-го порядка D, при этом применим метод полной индукции. Пусть указанная формула верна для детерминантов $(n-1)$-го порядка того же вида, что и D, т. е.

$$\begin{vmatrix} 1 & a_2 & a_2^2 & \dots & a_2^{n-1} \\ 1 & a_3 & a_3^2 & \dots & a_3^{n-1} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & a_n & a_n^2 & \dots & a_n^{n-1} \end{vmatrix} = \prod_{\substack{\varkappa > \lambda \\ \varkappa, \lambda = 1, 2, \dots, n}} (a_\varkappa - a_\lambda)$$

($\prod$ — знак произведения). Докажем, что и для нашего детерминанта D будет верна такая же формула. Для этого в D от последнего столбца отнимем предпоследний умноженный на a_1, от предпоследнего — предшествующий ему, умноженный тоже на a_1 и т. д., наконец, от второго первый, умноженный на a_1, далее, применяем свойства VI и III:

$$\begin{aligned} D &= \begin{vmatrix} 1 & 0 & 0 & \dots & 0 \\ 1 & a_2 - a_1 & a_2^2 - a_1 a_2 & \dots & a_2^{n-1} - a_1 a_2^{n-2} \\ 1 & a_3 - a_1 & a_3^2 - a_1 a_3 & \dots & a_3^{n-1} - a_1 a_3^{n-2} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & a_n - a_1 & a_n^2 - a_1 a_n & \dots & a_n^{n-1} - a_1 a_n^{n-2} \end{vmatrix} = \\ &= (a_2 - a_1)(a_3 - a_1) \cdots (a_n - a_1) \cdot \begin{vmatrix} 1 & a_2 & a_2^2 & \dots & a_2^{n-1} \\ 1 & a_3 & a_3^2 & \dots & a_3^{n-1} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & a_n & a_n^2 & \dots & a_n^{n-1} \end{vmatrix} = \\ &= (a_2 - a_1)(a_3 - a_1) \cdots (a_n - a_1) \cdot \prod_{\substack{\varkappa > \lambda \\ \varkappa, \lambda = 2, 3, \dots, n}} (a_\varkappa - a_\lambda) = \prod_{\substack{\varkappa > \lambda \\ \varkappa, \lambda = 1, 2, \dots, n}} (a_\varkappa - a_\lambda). \end{aligned}$$

Упражнения

49) Вычислить:

$$\begin{vmatrix} 1 & -1 & 0 & 3 \\ 3 & 2 & 1 & -1 \\ 1 & 2 & -1 & 3 \\ 4 & 0 & 1 & 2 \end{vmatrix}.$$

Отв. 10.

50) Вычислить:

$$\begin{vmatrix} 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ -1 & -1 & 1 & 1 \\ -1 & 1 & -1 & 1 \end{vmatrix}.$$

Отв. 0 (почему?).

51) Вычислить:

$$\begin{vmatrix} 1 & 2 & 3 & 4 \\ 0 & 1 & 2 & 3 \\ -1 & 0 & 1 & 2 \\ -2 & -1 & 0 & 1 \end{vmatrix}.$$

Отв. 0.

§ 31. Теорема умножения. Пусть

$$A = \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix}, \qquad B = \begin{vmatrix} b_{11} & b_{12} & \dots & b_{1n} \\ b_{21} & b_{22} & \dots & b_{2n} \\ \dots & \dots & \dots & \dots \\ b_{n1} & b_{n2} & \dots & b_{nn} \end{vmatrix}$$

$$C = \begin{vmatrix} c_{11} & c_{12} & \dots & c_{1n} \\ c_{21} & c_{22} & \dots & c_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix},$$

$$c_{\alpha\beta} = a_{\alpha 1}b_{\beta 1} + a_{\alpha 2}b_{\beta 2} + \dots + a_{\alpha 1n}b_{\beta n} = \sum a_{\alpha\lambda}b_{\beta\lambda} \qquad (\alpha, \beta = 1, 2, \dots, n).$$

Докажем, что $C = A \cdot B$.

Имеем по V:

$$C = \sum_{\varkappa,\lambda,\dots,\tau} \begin{vmatrix} a_{1\varkappa}b_{1\varkappa} & a_{1\lambda}b_{2\lambda} & \dots & a_{1\tau}b_{n\tau} \\ a_{2\varkappa}b_{1\varkappa} & a_{2\lambda}b_{2\lambda} & \dots & a_{2\tau}b_{n\tau} \\ \dots & \dots & \dots & \dots \\ a_{n\varkappa}b_{1\varkappa} & a_{n\lambda}b_{2\lambda} & \dots & a_{n\lambda}b_{n\tau} \end{vmatrix}; \tag{9}$$

эта сумма имеет n^n слагаемых соответственно значениям: $\varkappa = 1, 2, \dots, n$; $\lambda = 1, 2, \dots, n$; $\dots$; $\tau = 1, 2, \dots, n$.

Но если $\varkappa, \lambda, \dots, \tau$ в данном слагаемом не все различны, то это слагаемое по IV равно нулю, ибо в нем два столбца пропорциональны. Следовательно, в (9) не равны нулю только $n!$ слагаемых, соответствующих $n!$ перестановкам $\varkappa, \lambda, \dots, \tau$ чисел $1, 2, \dots, n$.

Имеем, далее, по III и (8):

$$C = \sum b_{1\varkappa}b_{2\lambda}\dots b_{n\tau} \begin{vmatrix} a_{1\varkappa} & a_{1\lambda} & \dots & a_{1\tau} \\ a_{2\varkappa} & a_{2\lambda} & \dots & a_{2\tau} \\ \dots & \dots & \dots & \dots \\ a_{n\varkappa} & a_{n\lambda} & \dots & a_{n\tau} \end{vmatrix} = \sum [\varkappa\lambda\dots\tau]\, b_{1\varkappa}b_{2\lambda}\dots b_{n\tau} \cdot A;$$

A, как общий множитель всех слагаемых, выносится за знак суммы; далее, по (6) имеем:

$$C = A \cdot \sum [\varkappa\lambda\dots\tau]\, b_{1\varkappa}b_{2\lambda}\dots b_{n\tau} = A \cdot B,$$

что и требовалось доказать.

И здесь возможны четыре способа составления произведения;

1) комбинирование строк со строками;
2) $''$ столбцов со строками;
3) $''$ строк со столбцами;
4) $''$ столбцов со столбцами.

Особенно важны способы 1 и 3.

§ 32. Разложение детерминанта по элементам ряда. Имеем (по V и VI):

$$D = \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} =$$

$$= \begin{vmatrix} a_{11}+0+\dots+0 & 0+a_{12}+\dots+0 & \dots & 0+0+\dots+a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} =$$

$$= \begin{vmatrix} a_{11} & 0 & \dots & 0 \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} + \begin{vmatrix} 0 & a_{12} & \dots & 0 \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} + \dots +$$

$$+ \begin{vmatrix} 0 & 0 & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} = A_{11}a_{11} + A_{12}a_{12} + \dots + A_{1n}a_{1n}.$$

Подобное же выражение мы можем получить для всякой строки и для всякого столбца. Итак

$$\left.\begin{aligned} A_{\varkappa 1}a_{\varkappa 1} + A_{\varkappa 2}a_{\varkappa 2} + \dots + A_{\varkappa n}a_{\varkappa n} = D; \\ A_{1\varkappa}a_{1\varkappa} + A_{2\varkappa}a_{2\varkappa} + \dots + A_{n\varkappa}a_{n\varkappa} = D \end{aligned}\right\} \qquad (\varkappa = 1, 2, \dots, n). \tag{10}$$

Но, с другой стороны (при $\varkappa \neq \lambda$):

$$\left.\begin{aligned} A_{\varkappa 1}a_{\lambda 1} + A_{\varkappa 2}a_{\lambda 2} + \dots + A_{\varkappa n}a_{\lambda n} = 0; \\ A_{1\varkappa}a_{1\lambda} + A_{2\varkappa}a_{2\lambda} + \dots + A_{n\varkappa}a_{n\lambda} = 0. \end{aligned}\right\} \tag{11}$$

ибо левые части — детерминанты с двумя одинаковыми рядами (см. § 30, IV). Всего мы имеем, таким образом, $2n^2$ формул. Их можно сокращенно представить двумя формулами. Введем для этого символ $e_{\alpha\beta}$.

Пусть

$$e_{\alpha\beta} = \begin{cases} 1 & \text{при } \alpha = \beta, \\ 0 & \text{при } \alpha \neq \beta. \end{cases}.$$

Тогда
$$\sum_{\varkappa=1}^{n} A_{\varkappa\alpha}a_{\varkappa\beta} = e_{\alpha\beta}\cdot D; \qquad \sum_{\varkappa=1}^{n} A_{\alpha\varkappa}a_{\beta\varkappa} = e_{\alpha\beta}\cdot D. \tag{12}$$

При помощи этих формул, применяя первый способ составления произведения, найдем:
$$\begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} \cdot \begin{vmatrix} A_{11} & A_{12} & \dots & A_{1n} \\ A_{21} & A_{22} & \dots & A_{2n} \\ \dots & \dots & \dots & \dots \\ A_{n1} & A_{n2} & \dots & A_{nn} \end{vmatrix} = \begin{vmatrix} D & 0 & \dots & 0 \\ 0 & D & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & D \end{vmatrix} = D^n;$$
отсюда
$$\begin{vmatrix} A_{11} & A_{12} & \dots & A_{1n} \\ A_{21} & A_{22} & \dots & A_{2n} \\ \dots & \dots & \dots & \dots \\ A_{n1} & A_{n2} & \dots & A_{nn} \end{vmatrix} = D^{n-1}.$$

Это так называемый *взаимный* детерминант.

§ 33. Линейные уравнения. Возьмем систему п линейных уравнений с n неизвестными:
$$\left.\begin{aligned} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n = b_1,\\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n = b_2,\\ \dots\dots\dots\dots\dots\dots\dots\dots,\\ a_{n1}x_1 + a_{n2}x_2 + \dots + a_{nn}x_n = b_n, \end{aligned}\right\} \tag{13}$$
пусть
$$D = \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix} \neq 0;$$
D — так называемый *детерминант системы* (13). Помножим обе части первого из уравнений (13) на $A_{1\gamma}$, обе части второго на $A_{2\gamma}$ и т. д., обе части последнего на $A_{n\gamma}$ (γ — одно из чисел $1, 2, \dots, n$; через $A_{\alpha\beta}$ мы, как и раньше, обозначаем минор детерминанта D, соответствующий элементу $a_{\alpha\beta}$ и сложим почленно после этого все полученные уравнения; тогда найдем:
$$\begin{aligned} &(A_{1\gamma}a_{11} + A_{2\gamma}a_{21} + \dots + A_{n\gamma}a_{n1})x_1 + \\ &+(A_{1\gamma}a_{12} + A_{2\gamma}a_{22} + \dots + A_{n\gamma}a_{n2})x_1 + \\ &\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ &+(A_{1\gamma}a_{1\gamma} + A_{2\gamma}a_{2\gamma} + \dots + A_{n\gamma}a_{n\gamma})x_\gamma + \\ &\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ &+(A_{1\gamma}a_{1n} + A_{2\gamma}a_{2n} + \dots + A_{n\gamma}a_{nn})x_n = \\ &= (A_{1\gamma}b_1 + A_{2\gamma}b_2 + \dots + A_{n\gamma}b_n. \end{aligned}$$

Но по (11) § 32 все суммы в скобках обращаются в нуль за исключением суммы, на которую умножается x_γ, и которая [по (10) § 32] равна D; следовательно:
$$Dx_\gamma = A_{1\gamma}b_1 + A_{2\gamma}b_2 + \dots + A_{n\gamma}b_n.$$

Правая часть этого равенства получается из

$$D = A_{1\gamma}a_{1\gamma} + A_{2\gamma}a_{2\gamma} + \ldots + A_{n\gamma}a_{n\gamma},$$

если заменить $a_{1\gamma}, a_{2\gamma}, \ldots, a_{n\gamma}$ через $b_1, b_2, \ldots, b_n$, т. е. это тоже детерминант n-го порядка, получаемый из D заменою в D γ-го столбца столбцом правых частей наших уравнений (13). Итак

$$x_\gamma = \frac{\begin{vmatrix} a_{11} & a_{12} & \ldots & b_1 & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & b_2 & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ a_{n1} & a_{n2} & \ldots & b_n & \ldots & a_{nn} \end{vmatrix}}{\begin{vmatrix} a_{11} & a_{12} & \ldots & a_{1\gamma} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2\gamma} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ a_{n1} & a_{n2} & \ldots & a_{n\gamma} & \ldots & a_{nn} \end{vmatrix}} \qquad (\gamma = 1, 2, \ldots, n). \tag{14}$$

Применяя знак $\sum$ для суммы, можно значительно сократить предыдущие выкладки. Напишем уравнения (13) в сокращенном виде:

$$\sum_{\beta=1}^{n} a_{\alpha\beta}x_\beta = b_\beta \qquad (\alpha = 1, 2, \ldots, n). \tag{13a}$$

) Уравнение (13а) с номером α умножим на $A_{\alpha\gamma}$ ($\gamma\gamma$ — одно из чисел $1, 2, \ldots, n$ и сложим почленно все полученные таким образом уравнения (иначе: «просуммируем их по α»); получим:

$$\sum_{\alpha=1}^{n}\sum_{\beta=1}^{n} A_{\alpha\gamma}a_{\alpha\beta}x_\beta = \sum_{\alpha=1}^{n} A_{\alpha\gamma}b_\gamma;$$

но в левой части мы можем переставить оба знака суммы, т. е. сначала суммировать по α, а затем по β (так, чтобы сумма по α была «внутренняя», а по β «внешняя»), ибо это сводится к иному распределению слагаемых, отчего сумма не изменится.

Это дает:

$$\sum_{\beta=1}^{n}\sum_{\alpha=1}^{n} A_{\alpha\gamma}a_{\alpha\beta}x_\beta = \sum_{\beta=1}^{n}\left(\sum x_\beta \sum_{\alpha=1}^{n} A_{\alpha\gamma}a_{\alpha\beta}\right),$$

ибо x, не зависит от α, а следовательно, его можно вынести за знак внутренней суммы. Но по (12) § 32

$$\sum_{\alpha=1}^{n} A_{\alpha\gamma}a_{\alpha\beta} = e_{\gamma\beta} \cdot D,$$

т. е. изо всей нашей двойной суммы только одно слагаемое не равно нулю, именно то, для которого $\beta = \gamma$, — оно равно Dx_γ;, следовательно:

$$x_\gamma = \frac{1}{D}\sum_{\alpha=1}^{n} A_{\alpha\gamma}b_\gamma \qquad (\gamma = 1, 2, \ldots, n). \tag{14a}$$

Это та же формула, что и (14), только написанная сокращенно.

Итак, мы вывели следующее: если существуют решения уравнений (13), то они находятся по формуле (14), которая дает только одну систему решений $x_1, x_2, \ldots, x_n$. Остается доказать, что эти решения действительно удовлетворяют данным уравнениям, т. е. подставить выражения (14) в левые части уравнений (13). Для этого изменим немного обозначения:

$$x_\beta = \frac{1}{D}\sum_{\gamma=1}^{n} A_{\gamma\beta} b_\gamma \qquad (\beta = 1, 2, \ldots, n).$$

Теперь имеем [по (12) § 32]:

$$\sum_{\beta=1}^{n} a_{\alpha\beta} x_\beta = \sum_{\beta=1}^{n} \left(a_{\alpha\beta} \cdot \frac{1}{D} \sum_{\gamma=1}^{n} A_{\gamma\beta} b_\gamma \right) = \frac{1}{D} \sum_{\gamma=1}^{n} \left(b_\gamma \sum_{\beta=1}^{n} A_{\gamma\beta} a_{\alpha\beta} \right) = \frac{1}{D} b_\alpha D = b_\alpha,$$

т. е. действительно получаем правую часть уравнения (13).

Итак:

Теорема. *Если $D \neq 0$, то система* (13) *n линейных уравнений с n неизвестными, имеет всегда одну и только одну систему решений.*

Следствие I. Если система n линейных уравнений с n неизвестными имеет более, чем одну систему решений, то для нее $D = 0$.

В частности, если уравнения однородны, т. е. все $b_\alpha = 0$, то они всегда имеют очевидную систему решений, где все $x_\beta = 0$; при $D \neq 0$ эта система решений — единственная. Таким образом:

Следствие II. Если система n однородных линейных уравнений с n неизвестными имеет систему решений, где не все неизвестные равны нулю, то детерминант, составленный из коэфициентов этих уравнений, равен нулю.

Это следствие имеет очень большое применение.

Упражнения

52) Решить систему:

$$\begin{cases} 5x_1 - 3x_2 + 4x_3 - x_4 = 7, \\ 3x_1 + 2x_2 - 5x_3 + 2x_4 = 0, \\ x_1 + 8x_2 - x_3 - 3x_4 = 2, \\ 3x_1 - 2x_2 - 5x_3 + 4x_4 = 0. \end{cases}$$

Отв. $x_1 = 1$, $x_2 = 2$, $x_3 = 3$, $x_4 = 4$.

53) Дана система однородных уравнений:

$$\begin{cases} 3x_1 - 4x_2 + x_3 + 6x_4 + 8x_5 = 0, \\ 3x_1 + 3x_2 - 2x_3 - 5x_4 - 6x_5 = 0, \\ x_1 + x_2 - 5x_3 + 4x_4 - 2x_5 = 0, \\ 2x_1 - 2x_2 - 3x_3 + 4x_4 + 4x_5 = 0, \\ 2x_1 - x_2 + 3x_3 - x_4 + 2x_5 = 0. \end{cases}$$

Этой системе удовлетворяют значения:

$$x_1 = 0, \quad x_2 = 2, \quad x_3 = 0, \quad x_4 = 0, \quad x_5 = 1.$$

Проверить, равен ли нулю детерминант этой системы.

§ 34. Миноры. Пусть дан детерминант n-го порядка; выберем в нем r каких-нибудь строк с номерами $\alpha, \beta, \ldots, \theta$ и r столбцов с номерами $\varkappa, \lambda, \ldots, \tau$. Составим детерминант из элементов, стоящих на пересечении взятых r строк и r столбцов; этот детерминант r-го порядка:

$$\begin{vmatrix} a_{\alpha\varkappa} & a_{\alpha\lambda} & \ldots & a_{\alpha\tau} \\ a_{\beta\varkappa} & a_{\beta\lambda} & \ldots & a_{\beta\tau} \\ \ldots\ldots\ldots\ldots\ldots \\ a_{\theta\varkappa} & a_{\theta\lambda} & \ldots & a_{\theta\tau} \end{vmatrix}$$

называется *минором r-го порядка* данного детерминанта и обозначается: $|a^{\alpha\beta\ldots\theta}_{\varkappa\lambda\ldots\tau}|$. При $r = n-1$ получаем миноры $(n-1)$-го порядка, которые мы уже рассматривали.

Пусть дан детерминант:

$$D = \begin{vmatrix} a_{11} & a_{12} & \ldots & a_{1r} & 0 & \ldots & 0 \\ a_{21} & a_{22} & \ldots & a_{2r} & 0 & \ldots & 0 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{r1} & a_{r2} & \ldots & a_{rr} & 0 & \ldots & 0 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{r+1,1} & a_{r+1,2} & \ldots & a_{r+1,r} & a_{r+1,r+1} & \ldots & a_{r+1,n} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{n1} & a_{n2} & \ldots & a_{nr} & a_{n,r+1} & \ldots & a_{nn} \end{vmatrix}.$$

В нем равны нулю все элементы, стоящие на пересечении первых r строк и последних $n - r$ столбцов. Имеем по (6):

$$D = \sum [\varkappa\lambda \ldots \rho\sigma \ldots \tau]\, a_{1\varkappa} a_{2\lambda} \cdots a_{r\rho} a_{r+1,\sigma} \cdots a_{n\tau},$$

где сумма берется по всем перестановкам $\varkappa\lambda \ldots \tau$ чисел $1, 2, \ldots, n$. Но если хоть одно из первых r чисел $\varkappa\lambda \ldots \rho$ больше, чем r, то соответствующий член суммы равен нулю вследствие особого вида D. Следовательно, $\varkappa\lambda \ldots \rho$ в неравных нулю членах есть перестановка чисел $1, 2, ..., r$, а $\sigma \ldots \tau$ — перестановка чисел $r+1, \ldots, n$ С другой стороны, имеем по (5) § 25 :

$$[\varkappa\lambda \ldots \rho\sigma \ldots \tau] = [\varkappa\lambda \ldots \rho]\,[\sigma \ldots \tau](-1)^{\varkappa+\lambda+\ldots+\rho-\frac{r(r+1)}{2}},$$

но

$$\varkappa + \lambda + + \ldots + \rho = 1 + 2 + \ldots + + r = \frac{r(r+1)}{2},$$

следовательно:

$$[\varkappa\lambda \ldots \rho\sigma \ldots \tau] = [\varkappa\lambda \ldots \rho]\,[\sigma \ldots \tau].$$

Заметим, что $\varkappa\lambda \ldots \rho$ пробегает все перестановки чисел $1, 2, \ldots, r$, а $\sigma \ldots \tau$ — все перестановки чисел $r + 1, \ldots, n$ и каждая перестановка $\varkappa\lambda \ldots \rho$ комбинируется с каждой перестановкой $\sigma \ldots \tau$.

Следовательно, сумму можно преобразовать в произведение двух сумм:

$$D = \sum [\varkappa\lambda \dots \rho\sigma \dots \tau]\, a_{1\varkappa} a_{2\lambda} \cdots a_{r\rho} a_{r+1,\sigma} \cdots a_{n\tau} =$$

$$= \sum [\varkappa\lambda \dots \rho]\, a_{1\varkappa} a_{2\lambda} \cdots a_{r\rho} \cdot \sum [\sigma \dots \tau]\, a_{r+1,\sigma} \cdots a_{n\tau};$$

иными словами, по (6):

$$D = \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1r} \\ a_{21} & a_{22} & \dots & a_{2r} \\ \dots & \dots & \dots & \dots \\ a_{r1} & a_{r2} & \dots & a_{rr} \end{vmatrix} \cdot \begin{vmatrix} a_{r+1,r+1} & \dots & a_{r+1,1n} \\ \dots & \dots & \dots \\ a_{n,r+1} & \dots & a_{nn} \end{vmatrix} = .$$

$$= |a^{12\dots r}_{12\dots r}| \cdot |a^{r+1\dots n}_{r+1\dots n}|.$$

Обобщение. Пусть теперь равны нулю элементы, стоящие на пересечении r строк с номерами $\alpha, \beta, \dots, \theta$ и $n-r$ столбцов с номерами $\varkappa, \lambda, \dots, \tau$. Переставим в данном детерминанте (мы его снова обозначим через D) строки так, чтобы первые r строк были с номерами $\alpha, \beta, \dots, \theta$, и столбцы так, чтобы последние $n-r$ столбцов были с номерами $\varkappa, \lambda, \dots, \tau$. От этого D получит множитель:

$$\eta = [\alpha\beta \dots \theta\varkappa_1\lambda_1 \dots \tau_1]\, [\alpha_1\beta_1 \dots \theta_1\varkappa\lambda \dots \tau]$$

[см. § 30, (8)]; здесь $\varkappa_1, \lambda_1, \dots, \tau_1$ — номера последних $n-r$ строк, а $\alpha_1, \beta_1, \dots, \theta_1$ — номера первых r столбцов. Но по (5) § 25

$$[\alpha\beta \dots \theta\varkappa_1\lambda_1 \dots \tau_1]\, [\alpha_1\beta_1 \dots \theta_1\varkappa\lambda \dots \tau] = [\alpha\beta \dots \theta]\, [\varkappa_1\lambda_1 \dots \tau_1] \times$$
$$\times [\alpha_1\beta_1 \dots \theta_1]\, [\varkappa\lambda \dots \tau]\, (-1)^{\alpha+\beta+\dots+\theta-\frac{r(r+1)}{2}} \times \qquad !$$
$$\times (-1)^{\alpha_1+\beta_1+\dots+\theta_1-\frac{r(r+1)}{2}}.$$

Пусть

$$\alpha_1 < \beta_1 < \dots < \theta_1 \quad \text{и} \quad \varkappa_1 < \lambda_1 < \dots < \tau_1,$$

тогда

$$[\alpha_1\beta_1 \dots, \theta_1] = [\varkappa_1\lambda_1 \dots \tau_1] = +1,$$

следовательно'

$$\eta = [\alpha\beta \dots \theta\varkappa_1\lambda_1 \dots \tau_1]\, [\alpha_1\beta_1 \dots \theta_1\varkappa\lambda \dots \tau] =$$
$$= [\alpha\beta \dots \theta]\, [\varkappa\lambda \dots \tau](-1)^{\alpha+\beta+\dots+\theta+\alpha_1+\beta_1+\theta_1}.$$

Если и $\alpha < \beta < \dots < \theta$ и $\varkappa < \lambda < \dots < \tau$, то

$$\eta = (-1)^{\alpha+\beta+\dots+\theta+\alpha_1+\beta_1+\dots+\theta_1}.$$

Итак, в общем случае:

$$D = \left|a^{\alpha\beta\dots\theta}_{\alpha_1\beta_1\dots\theta_1}\right| \cdot \left|a^{\varkappa_1\lambda_1\dots\tau_1}_{\varkappa\lambda\dots\tau}\right| \cdot \eta, \tag{15}$$

где $\eta = \pm 1$.

Пусть теперь в D равны нулю все элементы, стоящие на пересечении r строк, и больше чем $n-r$ столбцов; в этом случае, применяя формулу (15), мы увидим, что в одном из миноров правой части один ряд состоит из нулей, т. е. $D=0$.

Итак:

Следствие. Если в детерминанте D равны нулю все элементы, стоящие на пересечении r строк и больше чем $n-r$ столбцов, то $D=0$.

Если дан минор r-го порядка $|a^{\alpha\beta\ldots\theta}_{\alpha_1\beta_1\ldots\theta_1}|$, то *дополнительным к нему минором* называется минор $n-r$-го порядка $|a^{\varkappa_1\lambda_1\ldots\tau_1}_{\varkappa\lambda\ldots\tau}|\cdot\eta$, где η имеет то же значение, что и раньше.

Пример.

$$\begin{vmatrix}5&0&3&0\\2&1&1&4\\3&2&5&1\\2&0&4&0\end{vmatrix}=\begin{vmatrix}5&3\\2&4\end{vmatrix}\cdot\begin{vmatrix}1&4\\2&1\end{vmatrix}\cdot[1423]\,[1324]=14\cdot(-7)\cdot(-1)^2(-1)^1=98.$$

Упражнения

54) Применяя формулу (15), вычислить:

$$\begin{vmatrix}0&3&0&0&2\\4&1&5&3&1\\1&-1&3&2&-2\\0&3&0&0&5\\2&1&-3&2&1\end{vmatrix}.$$

Отв. 279.

55) Не применяя формулы (15), проверить, что

$$\begin{vmatrix}3&1&0&3&0&0\\5&4&2&1&4&7\\2&5&0&2&0&0\\1&2&0&5&0&0\\3&3&1&2&4&2\\1&3&0&4&0&0\end{vmatrix}.$$

56) Дан детерминант 6-го порядка:

$$\begin{vmatrix}a_{11}&a_{12}&\ldots&a_{16}\\a_{21}&a_{22}&\ldots&a_{26}\\\ldots&\ldots&\ldots&\ldots\\a_{61}&a_{62}&\ldots&a_{66}\end{vmatrix},$$

его минору $\begin{vmatrix}a_{23}&a_{26}\\a_{53}&a_{56}\end{vmatrix}$ найти дополнительный.

Отв.

$$\begin{vmatrix}a_{11}&a_{12}&a_{14}&a_{15}\\a_{31}&a_{32}&a_{34}&a_{35}\\a_{41}&a_{42}&a_{44}&a_{45}\\a_{61}&a_{62}&a_{64}&a_{65}\end{vmatrix}.$$

§ 35. Возьмем детерминант n-го порядка:

$$D = \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix}.$$

Через $A_{\alpha\beta}$ как и раньше, обозначим его минор $(n-1)$-го порядка, соответствующий элементу $a_{\alpha\beta}$. Пусть $r < n$ — целое положительное число. Возьмем произведение:

$$D \cdot \begin{vmatrix} A_{11} & \dots & A_{1r} \\ \dots & \dots & \dots \\ A_{r1} & \dots & A_{rr} \end{vmatrix} =$$

$$\begin{vmatrix} a_{11} & \dots & a_{1r} & a_{1,r+1} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ a_{r1} & \dots & a_{rr} & a_{r,r+1} & \dots & a_{rn} \\ a_{r+1,1} & \dots & a_{r+1,r} & a_{r+1,r+1} & \dots & a_{r+1,n} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ a_{n1} & \dots & a_{nr} & a_{n,r+1} & \dots & a_{nn} \end{vmatrix} \cdot \begin{vmatrix} A_{11} & \dots & A_{1r} & A_{1,r+1} & \dots & A_{1n} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ A_{r1} & \dots & A_{rr} & A_{r,r+1} & \dots & A_{rn} \\ 0 & \dots & 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & 0 & \dots & 1 \end{vmatrix}$$

и вычислим его, комбинируя строки со строками и принимая во внимание формулы (10) и (11) § 32. Найдем по § 34:

$$D \cdot \begin{vmatrix} A_{11} & \dots & A_{1r} \\ \dots & \dots & \dots \\ A_{r1} & \dots & A_{rr} \end{vmatrix} = \begin{vmatrix} D & 0 & \dots & 0 & a_{1,r+1} & \dots & a_{1n} \\ 0 & D & \dots & 0 & a_{2,r+1} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & D & a_{r,r+1} & \dots & a_{rn} \\ 0 & 0 & \dots & 0 & a_{r+1,r+1} & \dots & a_{rn} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & a_{n,r+1} & \dots & a_{nn} \end{vmatrix} =$$

$$= D^r \begin{vmatrix} a_{r+1,r+1} & \dots & a_{r+1,n} \\ \dots & \dots & \dots \\ a_{n,r+1} & \dots & a_{nn} \end{vmatrix};$$

предполагая, что $D \neq 0$, и применяя обозначение миноров § 34, получим

$$\left|A^{12\dots r}_{12\dots r}\right| = D^{r-1} \cdot \left|a^{r+1\dots n}_{r+1\dots n}\right|. \tag{16}$$

Обобщим эту формулу. Пусть $\alpha, \beta, \gamma, \dots$ — номера каких-нибудь r строк, а $\alpha', \beta', \gamma' m \dots$ — номера остальных $n - r$ строк; пусть, далее, $\varkappa, \lambda, \mu, \dots$ — номера каких-нибудь r столбцов, а $\varkappa', \lambda', \mu', \dots$ — номера остальных $n - r$ столбцов. В детерминанте D поставим на первое место строку с номером α, на второе место — строку с номером β и т. д., на $(r+1)$-е место строку с номером α', на $(r+2)$-е — строку с номером β' и т. д. Подобным же образом переставим столбцы в таком порядке: $\varkappa$-й, λ-й, μ-й, …, $\varkappa'$-й, λ'-й, μ'-й, …; от этого (см. следствие свойства II, § 30) D перейдет в ηD, где

$$\eta = [\alpha\beta\gamma \dots \alpha'\beta'\gamma' \dots]\,[\varkappa\lambda\mu \dots \varkappa'\lambda'\mu' \dots];$$

но легко видеть, что от этого и $A_{\alpha\beta}$ перейдет в $\eta A_{\alpha\beta}$ [14].

Применим теперь к детерминанту ηD формулу (16):

$$\eta^r \cdot \left|A^{\alpha\beta\gamma\ldots}_{\varkappa\lambda\mu\ldots}\right| = \eta^{r-1} D^{r-1} \cdot \left|a^{\alpha'\beta'\gamma'\ldots}_{\varkappa'\lambda'\mu'\ldots}\right|;$$

так как $\eta = \pm 1$, то $\eta^{-1} = \eta$, следовательно, сокращая на η^r, найдем:

$$\left|A^{\alpha\beta\gamma\ldots}_{\varkappa\lambda\mu\ldots}\right| = \eta D^{r-1} \cdot \left|a^{\alpha'\beta'\gamma'\ldots}_{\varkappa'\lambda'\mu'\ldots}\right|. \tag{17}$$

Эта формула выражает зависимость минора взаимного детерминанта и дополнительного минора данного детерминанта. При $r = 1$ получаем обычную формулу, определяющую $A_{\varkappa\lambda}$ как детерминант $(n-1)$-го порядка (§ 30). При $r = 2$ получаем из (16):

$$\begin{vmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{vmatrix} = D \cdot \begin{vmatrix} a_{33} & \ldots & a_{3n} \\ \ldots\ldots\ldots\ldots \\ a_{n3} & \ldots & a_{nn} \end{vmatrix}.$$

Упражнение

57) Пусть

$$D = \begin{vmatrix} 3 & 4 & 1 & 2 \\ 1 & 3 & 1 & 1 \\ 4 & 1 & 2 & 2 \\ 1 & 3 & 2 & 1 \end{vmatrix};$$

проверить формулу (16) при $r = 2$.

§ 36. Разложение детерминанта по элементам строки и столбца. Обозначим:

$$D = \begin{vmatrix} a_{00} & a_{01} & \ldots & a_{0n} \\ a_{10} & a_{11} & \ldots & a_{1n} \\ \ldots\ldots\ldots\ldots\ldots \\ a_{n0} & a_{n1} & \ldots & a_{nn} \end{vmatrix}, \qquad A = \begin{vmatrix} a_{11} & \ldots & a_{1n} \\ \ldots\ldots\ldots\ldots \\ a_{n1} & \ldots & a_{nn} \end{vmatrix};$$

через $A_{\alpha\beta}$ обозначим минор $(n-1)$-го порядка детерминанта A, соответствующий элементу $a_{\alpha\beta}$. Имеем по § 32, (10):

$$D = a_{00}A - a_{01}\begin{vmatrix} a_{10} & a_{12} & \ldots & a_{1n} \\ \ldots\ldots\ldots\ldots\ldots \\ a_{n0} & a_{n2} & \ldots & a_{nn} \end{vmatrix} + a_{02}\begin{vmatrix} a_{10} & a_{11} & a_{13} & \ldots & a_{1n} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{n0} & a_{n1} & a_{n3} & \ldots & a_{nn} \end{vmatrix} -$$
$$-a_{03}\begin{vmatrix} a_{10} & a_{11} & a_{12} & a_{14} & \ldots & a_{1n} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{n0} & a_{n1} & a_{n2} & a_{n4} & \ldots & a_{nn} \end{vmatrix} + \ldots.$$

[14] Это следует из (10) § 32: умножив, например, обе части первого уравнения (10) на η, получим

$$\eta A_{\varkappa 1} a_{\varkappa 1} + \eta A_{\varkappa 2} a_{\varkappa 2} + \ldots + \eta A_{\varkappa n} a_{\varkappa n} = \eta D,$$

т. е. в детерминанте ηD элементу $a_{\varkappa\lambda}$ соответствует минор $n-1$ порядка $\eta A_{\varkappa\lambda}$

Но по тем же формулам § 32 (10) имеем:

$$\begin{vmatrix} a_{10} & a_{12} & \dots & a_{1n} \\ \dots\dots\dots\dots\dots \\ a_{n0} & a_{n2} & \dots & a_{nn} \end{vmatrix} = a_{10}A_{11} + \dots + a_{n0}A_{n1} = \sum_{\alpha=1}^{n} a_{\alpha 0}A_{\alpha 1},$$

$$\begin{vmatrix} a_{10} & a_{11} & a_{13} & \dots & a_{1n} \\ \dots\dots\dots\dots\dots\dots \\ \dots\dots\dots\dots\dots\dots \\ a_{n0} & a_{n1} & a_{n3} & \dots & a_{nn} \end{vmatrix} = -(a_{10}A_{12} + \dots + a_{n0}A_{n2} = \sum_{\alpha=1}^{n} a_{\alpha 0}A_{\alpha 2},$$

$$\begin{vmatrix} a_{10} & a_{11} & a_{12} & a_{14} & \dots & a_{1n} \\ \dots\dots\dots\dots\dots\dots\dots \\ \dots\dots\dots\dots\dots\dots\dots \\ a_{n0} & a_{n1} & a_{n2} & a_{n4} & \dots & a_{nn} \end{vmatrix} = (-1)^2 \cdot \begin{vmatrix} a_{11} & a_{12} & a_{10} & a_{14} & \dots & a_{1n} \\ \dots\dots\dots\dots\dots\dots\dots \\ \dots\dots\dots\dots\dots\dots\dots \\ a_{n1} & a_{n2} & a_{n0} & a_{n4} & \dots & a_{nn} \end{vmatrix} =$$

$$= \sum_{\alpha=1}^{n} a_{\alpha 0}A_{\alpha 3} \qquad \text{и т. д.}$$

Следовательно, получаем:

$$D = a_{00}A - \sum_{\beta=1}^{n} a_{0\beta} \sum_{\alpha=1}^{n} a_{\alpha 0}A_{\alpha\beta},$$

или

$$D = a_{00} - \sum_{\alpha,\beta=1}^{n} a_{\alpha 0}a_{0\beta}A_{\alpha\beta}. \tag{18}$$

Это и есть разложение D по элементам первой строки и первого столбца. Перестановками строк и столбцов мы сумеем разложить D по элементам какой-нибудь строки и какого-нибудь столбца. Например, легко видеть, что формула (18) остается верной, если строка и столбец со значком 0 не первые, а последние.

Упражнения

58) По формуле (18) разложить детерминант по элементам первой строки и первого столбца:

$$D = \begin{vmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{vmatrix}.$$

Отв.

$$D = a_{11}\begin{vmatrix} a_{22} & a_{23} & a_{24} \\ a_{32} & a_{33} & a_{22} \\ a_{42} & a_{43} & a_{44} \end{vmatrix} - a_{21}a_{12}\begin{vmatrix} a_{33} & a_{34} \\ a_{43} & a_{44} \end{vmatrix} - a_{21}a_{13}\begin{vmatrix} a_{34} & a_{32} \\ a_{44} & a_{42} \end{vmatrix} - a_{21}a_{14}\begin{vmatrix} a_{32} & a_{33} \\ a_{42} & a_{43} \end{vmatrix} -$$

$$-a_{31}a_{12}\begin{vmatrix} a_{24} & a_{23} \\ a_{41} & a_{43} \end{vmatrix} - a_{31}a_{13}\begin{vmatrix} a_{22} & a_{24} \\ a_{42} & a_{44} \end{vmatrix} - a_{31}a_{14}\begin{vmatrix} a_{23} & a_{22} \\ a_{43} & a_{42} \end{vmatrix} - a_{41}a_{12}\begin{vmatrix} a_{23} & a_{24} \\ a_{33} & a_{34} \end{vmatrix} -$$

$$-a_{41}a_{13}\begin{vmatrix} a_{24} & a_{22} \\ a_{31} & a_{32} \end{vmatrix} - a_{41}a_{14}\begin{vmatrix} a_{22} & a_{23} \\ a_{32} & a_{33} \end{vmatrix}.$$

59) Пользуясь формулой предыдущего упражнения, вычислить детерминант:

$$\begin{vmatrix} 3 & 4 & 1 & 5 \\ 2 & 3 & 1 & 1 \\ 4 & 1 & 2 & 3 \\ 1 & 2 & 4 & 1 \end{vmatrix}.$$

Отв. 122.

§ 37. Теорема Лапласа. Предварительное замечание. Пусть дано найти все перестановки n символов. Можно поступить следующим образом: делить n символов всевозможными способами на две группы: в r символов и в $n-r$ символов; число таких способов есть $\binom{n}{r}$. Возьмем одно такое деление на две группы; в первой группе делаем всевозможные перестановки r символов (число их равно $r!$), во второй группе — всевозможные перестановки $n-r$ символов [число их равно $(n-r)!$] и комбинируем каждую перестановку первой группы с каждой перестановкой второй группы; получим $r!\,(n-r)!$ перестановок всех n символов. Проделав это с каждым из делений на группы, получим всего

$$r!\,(n-r)!\,\binom{n}{r} = r!\,(n-r)!\,\frac{n!}{r!(n-r)!} = n!$$

перестановок всех n символов, т. е. таким способом мы получаем все перестановки n символов.

Пример. $n=4$, $r=2$, $n-r=2$; получаем все 24 перестановки:

12	34	13	24	14	23	23	14	24	13	34	12
12	43	13	42	14	32	23	41	24	31	34	21
21	34	31	24	41	23	32	14	42	13	43	12
21	43	31	42	41	32	32	41	42	31	43	21

Теорема Лапласа (Laplace). Дан детерминант n-го порядка:

$$D = \sum [\varkappa\lambda \dots \rho\sigma \dots \tau]\, a_{1\varkappa} a_{\lambda} \cdots a_{r\rho} a_{r+1,\sigma} \cdots a_{n\tau};$$

сумма берется по всем перестановкам: $\varkappa\lambda \dots \rho\sigma \dots \tau$ n чисел $1, 2, ..., n$. По-предыдущему мы можем получить все эти перестановки, деля все n символов на две группы: в r символов: $\varkappa\lambda \dots \rho$ и в $n-r$ символов: $\sigma \dots \tau$.

Получаем:

$$D = \sum \sum [\varkappa\lambda \dots \rho\sigma \dots \tau]\, a_{1\varkappa} a_{\lambda} \cdots a_{r\rho} a_{r+1,\sigma} \cdots a_{n\tau},$$

где внешняя сумма берется по всем $\binom{n}{r}$ делениям на группы, а внутренняя сумма берется по всем перестановкам взятых при данном делении r символов $\varkappa, \lambda, \dots, \rho$ и $n-r$ символов $\sigma, \dots, \tau$, причем каждая перестановка символов $\varkappa, \lambda, \dots, \rho$ комбинируется с каждой перестановкой символов $\sigma, \dots, \tau$.

Имеем [см. § 25, (5)]:

$$[\varkappa\lambda \dots \rho\sigma \dots \tau] = [\varkappa\lambda \dots \rho]\,[\sigma \dots \tau](-1)^{\varkappa+\lambda+\dots+\rho-\frac{r(r+1)}{2}}.$$

Для данного деления на группы множитель

$$\eta = (-1)^{\varkappa+\lambda+\ldots+\rho-\frac{r(r+1)}{2}}$$

один и тот же; его можно вынести за знак внутренней суммы. Получаем:

$$\begin{aligned} D &= \sum\left(\eta\sum[\varkappa\lambda\ldots\rho]\,[\sigma\ldots\tau]\,a_{1\varkappa}a_{\lambda}\cdots a_{r\rho}a_{r+1,\sigma}\cdots a_{n\tau}\right) = \\ &= \sum\left\{\eta\left(\sum[\varkappa\lambda\ldots\rho]\,a_{1\varkappa}a_{\lambda}\cdots a_{r\rho}\right)\left(\sum[\sigma\ldots\tau]\,a_{r+1,\sigma}\cdots a_{n\tau}\right)\right\}. \end{aligned}$$

Но под знаком внешней суммы стоит произведение двух дополнительных друг к другу миноров r-го порядка и $n-r$-го порядка; обозначим первый через $A_{\varkappa}$, а второй — через $B_{\varkappa}$. Тогда

$$D = \sum_{\varkappa=1}^{\binom{n}{r}} A_{\varkappa}B_{\varkappa}. \tag{19}$$

Эта формула и выражает теорему Лапласа. Здесь в сумму входят всевозможные миноры r-го порядка, составленные из первых r строк, и дополнительные к ним миноры. Конечно, вместо первых r строк можно было бы взять r каких-нибудь строк или r каких-нибудь столбцов.

Пример.

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \\ a_{41} & a_{42} & a_{43} & a_{44} \end{vmatrix} = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix}\cdot\begin{vmatrix} a_{33} & a_{34} \\ a_{43} & a_{44} \end{vmatrix} + \begin{vmatrix} a_{11} & a_{13} \\ a_{21} & a_{23} \end{vmatrix}\cdot\begin{vmatrix} a_{34} & a_{32} \\ a_{44} & a_{42} \end{vmatrix} +$$
$$+\begin{vmatrix} a_{11} & a_{14} \\ a_{21} & a_{24} \end{vmatrix}\cdot\begin{vmatrix} a_{32} & a_{33} \\ a_{42} & a_{43} \end{vmatrix} + \begin{vmatrix} a_{12} & a_{13} \\ a_{22} & a_{23} \end{vmatrix}\cdot\begin{vmatrix} a_{31} & a_{34} \\ a_{41} & a_{44} \end{vmatrix} + \begin{vmatrix} a_{12} & a_{14} \\ a_{22} & a_{24} \end{vmatrix}\cdot\begin{vmatrix} a_{33} & a_{31} \\ a_{43} & a_{41} \end{vmatrix} +$$
$$+\begin{vmatrix} a_{13} & a_{14} \\ a_{23} & a_{24} \end{vmatrix}\cdot\begin{vmatrix} a_{31} & a_{32} \\ a_{41} & a_{42} \end{vmatrix}.$$

§ 38. Обобщенная теорема умножения. В дальнейшем нам часто придется рассматривать системы чисел, расположенные прямоугольником в r строк и n столбцов:

$$\begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{r1} & a_{r2} & \ldots & a_{rn} \end{pmatrix};$$

такая система, которую мы для ясности заключаем в скобки, называется матрицей; обычно ее для краткости обозначают одной буквой, например матрица A. При $r \neq n$ матрица называется *прямоугольной*, при $r = n$ *квадратной*; числа, из которых состоит матрица, называются ее *элементами*. Так вот пусть нам даны две прямоугольные матрицы, имеющие по r строк и по n столбцов и пусть $r \leq n$:

$$A = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{r1} & a_{r2} & \ldots & a_{rn} \end{pmatrix}, \qquad B = \begin{pmatrix} b_{11} & b_{12} & \ldots & b_{1n} \\ b_{21} & b_{22} & \ldots & b_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ b_{r1} & b_{r2} & \ldots & b_{rn} \end{pmatrix}.$$

Составим r^2 чисел $c_{\alpha\beta}$ следующим образом:

$$c_{\alpha\beta} = \sum_{\varkappa=1}^{n} a_{\alpha\varkappa} b_{\beta\varkappa}, \qquad \alpha, \beta = 1, 2, \ldots, r.$$

Из этих чисел $c_{\alpha\beta}$ можно составить детерминант r-го порядка:

$$C = \begin{vmatrix} c_{11} & c_{12} & \ldots & c_{1r} \\ c_{21} & c_{22} & \ldots & c_{2r} \\ \ldots\ldots\ldots\ldots\ldots \\ c_{r1} & c_{r2} & \ldots & c_{rr} \end{vmatrix}.$$

Обозначим еще:

$$A_\mu = \left|a^{12\ldots r}_{\alpha\beta\ldots\theta}\right|, \qquad B_\mu = \left|b^{12\ldots r}_{\alpha\beta\ldots\theta}\right|;$$

это детерминанты r-го порядка, которые составляются из элементов матриц A и B следующим образом: берутся элементы, стоящие на пересечении всех r строк этих матриц со столбцами с номерами $\alpha, \beta, \ldots, \theta$ и из них в том же порядке, как идут эти номера, составляются детерминанты r-го порядка; конечно, число взятых номеров $\alpha, \beta, \ldots, \theta$ предполагается равным r. Не обращая внимания на порядок, в каком мы берем номера $\alpha, \beta, \ldots, \theta$, беря только за $\alpha, \beta, \ldots, \theta$ всевозможные сочетания из n номеров по r, мы можем составить всего $s = \binom{n}{r}$ детерминантов A_μ и столько же детерминантов B_μ.

Мы выведем следующую формулу:

$$C = A_1 B_1 + A_2 B_2 + \ldots + A_s B_s. \tag{20}$$

Она и выражает «обобщенную теорему умножения детерминантов», ибо она является обобщением обычной теоремы умножения (§ 31): последняя есть частный случай формулы (20) при $r = n$.

Доказательство. К матрице A припишем еще $n - r$ строк с произвольными элементами:

$$\begin{matrix} a_{r+1,1}, & a_{r+1,2}, & \ldots, & a_{r+1,n}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{n1}, & a_{n2}, & \ldots, & a_{nn} \end{matrix}$$

но только так, чтобы детерминант n-го порядка:

$$D = \begin{vmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots\ldots\ldots\ldots\ldots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{vmatrix}$$

не был равен нулю. Определим теперь $c_{\alpha\beta} = \sum_{\varkappa=1}^{n} a_{\alpha\varkappa} b_{\beta\varkappa}$ и для $\alpha = r+1, \ldots, n$. Через $A_{\alpha\beta}$ обозначим миноры $(n-1)$-го порядка детерминанта D; введем еще обозначение

$$\Delta = \begin{vmatrix} b-11 & b_{12} & \ldots & b_{1n} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ b_{r1} & b_{r2} & \ldots & b_{rn} \\ A_{r+1,1} & A_{r+1,2} & \ldots & A_{r+1,n} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ A_{n1} & A_{n2} & \ldots & A_{nn} \end{vmatrix}$$

и найдем произведение $D \cdot \Delta$, комбинируя строки со строками:

$$D \cdot \Delta = \begin{vmatrix} c_{11} & \dots & c_{1r} & 0 & \dots & a_{1n} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ c_{r1} & \dots & c_{rr} & 0 & \dots & 0 \\ c_{r+1,1} & \dots & c_{r+1,r} & D & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ c_{n1} & \dots & c_{nr} & 0 & \dots & D \end{vmatrix} = C \cdot D^{n-r} (\text{по } \S\, 34). \qquad (21)$$

С другой стороны, по теореме Лапласа (§ 37):

$$\Delta = \sum \left| b^{12\dots r}_{\alpha\beta\dots\theta} \right| \cdot \left| A^{r+1\dots n}_{\varkappa\lambda\dots\tau} \right| [\alpha\beta\dots\theta\varkappa\lambda\dots\tau],$$

но по формуле (17) § 35:

$$\left| A^{r+1\dots n}_{\varkappa\lambda\dots\tau} \right| = \\ = D^{n-r-1} \cdot \left| a^{12\dots r}_{\alpha\beta\dots\theta} \right| \cdot [r+1, \dots, n, 1, 2, \dots, r]\, [\varkappa\lambda\dots\tau\alpha\beta\dots\theta];$$

так как

$$\left.\begin{gathered} [r+1, \dots, n, 1, 2, \dots, r]\, [\varkappa\lambda\dots\tau\alpha\beta\dots\theta] = [\alpha\beta\dots\theta\varkappa\lambda\dots\tau], \\ [\alpha\beta\dots\theta\varkappa\lambda\dots\tau]^2 = 1, \end{gathered}\right.,$$

то, следовательно:

$$\Delta = D^{n-r-1} \sum \left| a^{12\dots r}_{\alpha\beta\dots\theta} \right| \cdot \left| b^{12\dots r}_{\alpha\beta\dots\theta} \right|,$$

а отсюда и из (21)

$$C = \sum \left| a^{12\dots r}_{\alpha\beta\dots\theta} \right| \cdot \left| b^{12\dots r}_{\alpha\beta\dots\theta} \right| = \sum A_\mu B_\mu,$$

и теорема доказана.

Пример. При $r = 2$, $n = 4$ имеем:

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \end{pmatrix}, \qquad B = \begin{pmatrix} b_{11} & b_{12} & b_{13} & b_{14} \\ b_{21} & b_{22} & b_{23} & b_{24} \end{pmatrix};$$

$c_{\alpha\beta} = a_{\alpha 1} b_{\beta 1} + a_{\alpha 2} b_{\beta 2} + a_{\alpha 3} b_{\beta 3} + a_{\alpha 4} b_{\beta 4}$; $\alpha, \beta = 1, 2$ и (20) дает:

$$\begin{vmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{vmatrix} = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} \cdot \begin{vmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{vmatrix} + \begin{vmatrix} a_{11} & a_{13} \\ a_{21} & a_{23} \end{vmatrix} \cdot \begin{vmatrix} b_{11} & b_{13} \\ b_{21} & b_{23} \end{vmatrix} +$$

$$+ \begin{vmatrix} a_{11} & a_{14} \\ a_{21} & a_{24} \end{vmatrix} \cdot \begin{vmatrix} b_{11} & b_{14} \\ b_{21} & b_{24} \end{vmatrix} + \begin{vmatrix} a_{12} & a_{13} \\ a_{22} & a_{23} \end{vmatrix} \cdot \begin{vmatrix} b_{12} & b_{13} \\ b_{22} & b_{23} \end{vmatrix} + \begin{vmatrix} a_{12} & a_{14} \\ a_{22} & a_{24} \end{vmatrix} \cdot \begin{vmatrix} b_{12} & b_{14} \\ b_{22} & b_{24} \end{vmatrix} +$$

$$+ \begin{vmatrix} a_{13} & a_{14} \\ a_{23} & a_{24} \end{vmatrix} \cdot \begin{vmatrix} b_{13} & b_{14} \\ b_{23} & b_{24} \end{vmatrix}.$$

Упражнение

60) По формуле предыдущего примера найти детерминант C при:

$$A = \begin{pmatrix} 4 & 3 & 1 & 2 \\ 2 & 5 & 3 & 6 \end{pmatrix}, \qquad B = \begin{pmatrix} 1 & 3 & 1 & 2 \\ 2 & 3 & 2 & 3 \end{pmatrix}.$$

Отв. -26.

§ 39. Некоторые общие замечания о детерминантах. Понятие о детерминантах первый дал Лейбниц (Leibnitz) в письме к Лопиталю, в 1693 г., в связи с исключением неизвестных из системы трех линейных уравнений с двумя неизвестными. Повидимому, независимо от Лейбница ввел снова понятие о детерминантах Крамер (Gabriel Cramer) в 1750 г. в связи с решением системы n линейных уравнений с n неизвестными; Крамер дает правило решения, которое у нас выражено формулой (14); оно и до сих пор носит название «правила Крамера». Далее, детерминанты рассматривали Безу (Bézout), Вандермонд (Vandermonde), Лаплас (Laplace), Лагранж (Lagrange), и Гаусс (Gauss) в своем знаменитом сочинении «Disquisitiones arithmeticae (1801 г.), где он ввел и самое название «детерминант». Разработали теорию детерминантов Бинэ (Binet), Коши (Cauchy) и Якоби (Jacobi) в первой половине XIX в.; Коши ввел и современное обозначение в виде таблицы с n строками и n колоннами.

Детерминанты в математике широко распространены, но имеют лишь вспомогательное значение; детерминант есть вполне определенная функция от своих элементов, и, кажется, нет такой области и в математике, и в ее приложениях, где бы эта функция не встречалась. Теория детерминантов дает удобные средства для сокращенного обозначения и выкладок с этими функциями; в этом ее большое значение. Но практическим отделом теорию детерминантов нельзя назвать: мы видели, как громоздко вычисление детерминантов, уже начиная с четвертого порядка. Поэтому там, где требуется эффективный числовой результат, теория детерминантов нам почти ничего не дает; она имеет скорее теоретическое значение, как удобное обозначение в формулах, при доказательствах, и т. п.

Как мы уже упомянули, детерминант n-го порядка есть некоторая функция от своих n^2 элементов. Его можно определить не просто формально, как некоторое данное выражение, как это сделали мы в § 29, а на основании его функциональных свойств, и при этом несколькими способами; я укажу два из них.

Мы определяем детерминант n-го порядка как функцию D от n^2 переменных, расположенных в n строк и n столбцов, обладающую следующими свойствами:

1) D — линейная однородная функция от элементов первой строки;

2) от перестановки первой строки с какой-нибудь другой строкою детерминант только меняет знак;

3) если все элементы в D, кроме элементов главной диагонали, равны нулю, а элементы главной диагонали (т. е. элементы $a_{\alpha\alpha}$) все равны единице, то $D = 1$.

Первые два свойства определяют D с точностью до числового, независимого от элементов, множителя.

Другое определение детерминанта — как функции от его n^2 элементов, обладающей такими свойствами:

$1'$) D не изменится, если к элементам какой-либо строки прибавить соответствующие элементы какой-либо другой; строки;

$2'$) если все элементы какой-либо строки умножить на один и тот же множитель c, то и весь детерминант D умножится на c;

$3'$) то же, что и 3).

Чтобы вычислить детерминант, требуется над его элементами производить только действия сложения, вычитания и умножения; отсюда следует, что если все

элементы детерминанта принадлежат в данной области целости или рациональности (§ 13), то и значение детерминанта тоже принадлежит к той же области целости или рациональности.

Теория детерминантов в настоящее время очень развита. Имеется и обобщение детерминанта на случай бесконечного числа строк и столбцов; это так называемый бесконечный детерминант, определяемый следующим образом: пусть имеем таблицу, имеющую бесконечное (но исчислимое) множество строк и столбцов:

$$\begin{vmatrix} a_{11} & a_{12} & a_{13} & \dots \\ a_{21} & a_{22} & a_{23} & \dots \\ a_{31} & a_{32} & a_{33} & \dots \\ \dots & \dots & \dots & \dots \end{vmatrix}.$$

Возьмем n первых строк и n первых столбцов и из элементов, стоящих на их пересечении, построим детерминант n-го порядка D_n; пусть теперь $n \to \infty$; если существует

$$\lim_{n\to\infty} D_n = D,$$

то D и называется бесконечным детерминантом:

$$D = \begin{vmatrix} a_{11} & a_{12} & a_{13} & \dots \\ a_{21} & a_{22} & a_{23} & \dots \\ a_{31} & a_{32} & a_{33} & \dots \\ \dots & \dots & \dots & \dots \end{vmatrix}.$$

§ 40. Общая теория линейных уравнений. Рассмотрим общий случай системы m линейных уравнений с n неизвестными, где вообще $m \neq n$:

$$\sum_{\beta=1}^{n} a_{\alpha\beta} x_\beta = b_\alpha \qquad (\alpha = 1, 2, \dots, m). \tag{22}$$

В зависимости от различных случаев такая система может или совсем не иметь решений (быть несовместной), или иметь одно решение (определенная система), или, наконец, иметь бесчисленное множество решений (неопределенная система). Эти случаи имеют место в зависимости от тех или иных значений коэфициентов и свободных членов уравнений. Поэтому в первую очередь мы должны рассмотреть систему коэфициентов наших уравнений:

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}.$$

Это — не что иное, как матрица (§ 38), имеющая m строк и n столбцов. Мы можем, выбрав в ней какие-нибудь k строк и k столбцов, составить детерминант k-го порядка из элементов, стоящих на пересечении взятых k строк и k столбцов, беря эти элементы в том порядке, как они стоят. Назовем этот детерминант детерминантом k-то порядка матрицы A. Конечно, мы можем взять $k = 1, 2, \dots, l$, где l —

наименьшее из чисел m и n. Можно определить детерминант матрицы и при $k > l$, добавляя нули на место недостающих строк или столбцов. Очевидно, что все такие детерминанты при $k > l$ будут равны нулю. Но может случиться, что уже при некотором $k \leq l$ все детерминанты k-го порядка матрицы A равны нулю. Очевидно, что тогда и все детерминанты $(k+1)$-го, $(k+2)$-го и т. д. порядков матрицы A будут тоже равны нулю [15]. Следовательно, для всякой матрицы A можно найти целое число $r \geq 0$, отличающееся следующим свойством: имеется по крайней мере один детерминант r-го порядка данной матрицы, который не равен нулю; но все детерминанты $(r+1)$-го (а, следовательно, и высшего) порядка нашей матрицы равны нулю. Такое число r называется *рангом* матрицы. Самое большое значение для r есть l; самое меньшее — нуль (если все элементы матрицы равны нулю). От расширения матрицы приписыванием к ней новых строк или столбцов ранг ее может увеличиться (а может и не измениться); от приписывания к матрице одной новой строки или одного нового столбца ранг ее или не изменится, или увеличится на единицу.

Пусть A матрица коэфициентов наших уравнений (22); припишем к A еще столбец — свободных членов уравнений (22); получим матрицу:

$$B = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} & b_1 \\ a_{21} & a_{22} & \dots & a_{2n} & b_2 \\ \dots & \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} & b_m \end{pmatrix}.$$

Если r — ранг A, то ранг B равен или r, или $r+1$.

Теорема 1. *Система* (22) *имеет решение тогда и только тогда, если ранг матрицы B тот же, что и ранг матрицы A (равен r).*

Доказательство. 1. Пусть ранг A равен рангу B равен r; имеется по крайней мере один детерминант r-го порядка матрицы A, который не равен нулю. Не нарушая общности, можно положить:

$$\Delta = \begin{vmatrix} a_{11} & \dots & a_{1r} \\ \dots & \dots & \dots \\ a_{r1} & \dots & a_{rr} \end{vmatrix} \neq 0,$$

ибо от нас зависит, как перенумеровать и уравнения, и неизвестные.

Возьмем r первых уравнений (1) в таком виде:

$$\left.\begin{array}{l} a_{11}x_1 + \dots + a_{1r}x_r = b_1 - a_{1,r+1}x_{r+1} - \dots - a_{1n}x_n, \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ a_{r1}x_1 + \dots + a_{rr}x_r = b_r - a_{r,r+1}x_{r+1} - \dots - a_{rn}x_n. \end{array}\right\} \qquad (23)$$

Дадим для $x_{r+1}, \dots, x_n$ совершенно произвольные значения $\overline{x}_{r+1}, \dots, \overline{x}_n$ и решим после этого систему (23) относительно $x_1, \dots, x_r$; детерминант этой системы есть $\Delta \neq 0$, а следовательно, (23) имеет одну и только одну систему решений (§ 33) $\overline{x}_1, \dots, \overline{x}_r, \overline{x}_{r+1}, \dots, \overline{x}_n$. Итак, значения $\overline{x}_1, \dots, \overline{x}_r, \overline{x}_{r+1}, \dots, \overline{x}_n$ удовлетворяют

[15] Это следует хотя бы из возможности разложения детерминанта по элементам какого-нибудь ряда (§ 32): для детерминанта $(k+1)$-го порядка минорами будут детерминанты k-го порядка матрицы A, а они все равны нулю.

первым r уравнениям (22); докажем, что они удовлетворяют и остальным $m-r$ уравнениям (1). Обозначим: $a_{\varkappa 1}\overline{x}_1+\ldots+a_{\varkappa n}\overline{x}_n-b_{\varkappa}=H_{\varkappa},$, так что $H_1=0,\ldots,$ $H_r=0$; мы докажем, что при $s=r+1,\ldots,n$ тоже будет $H_s=0$. Рассмотрим

$$D=\begin{vmatrix} a_{11} & \ldots & a_{1r} & H_1\\ \ldots & \ldots & \ldots & \ldots\\ a_{r1} & \ldots & a_{rr} & H_r\\ a_{s1} & \ldots & a_{sr} & H_s \end{vmatrix}=\overline{x}_1\begin{vmatrix} a_{11} & \ldots & a_{1r} & a_{11}\\ \ldots & \ldots & \ldots & \ldots\\ a_{r1} & \ldots & a_{rr} & a_{r1}\\ a_{s1} & \ldots & a_{sr} & a_{s1} \end{vmatrix}+$$

$$+\overline{x}_2\begin{vmatrix} a_{11} & \ldots & a_{1r} & a_{12}\\ \ldots & \ldots & \ldots & \ldots\\ a_{r1} & \ldots & a_{rr} & a_{r2}\\ a_{s1} & \ldots & a_{sr} & a_{s2} \end{vmatrix}+\ldots+\overline{x}_n\begin{vmatrix} a_{11} & \ldots & a_{1r} & a_{1n}\\ \ldots & \ldots & \ldots & \ldots\\ a_{r1} & \ldots & a_{rr} & a_{rn}\\ a_{s1} & \ldots & a_{sr} & a_{sn} \end{vmatrix}-$$

$$-\begin{vmatrix} a_{11} & \ldots & a_{1r} & b_1\\ \ldots & \ldots & \ldots & \ldots\\ a_{r1} & \ldots & a_{rr} & b_1\\ a_{s1} & \ldots & a_{sr} & b_s \end{vmatrix};$$

все детерминанты правой части (полученной по § 30, свойства V и III) равны нулю, как детерминанты $(r+1)$-го порядка матрицы B, следовательно, $D=0$, или

$$D=\begin{vmatrix} a_{11} & \ldots & a_{1r} & 0\\ \ldots & \ldots & \ldots & \ldots\\ a_{r1} & \ldots & a_{rr} & 0\\ a_{s1} & \ldots & a_{sr} & H_s \end{vmatrix}=\Delta\cdot H_s=0,$$

а так как $\Delta\neq 0$, то $H_s=0$, что и требовалось доказать.

2. Обратно, пусть система (22) имеет решение $x_1=\overline{x}_1,\ \ldots,\ x_n=\overline{x}_n$. Докажем, что *ранг r матрицы A есть также ранг и матрицы B*. Для этого достаточно доказать, что всякий детерминант $(r+1)$-го порядка матрицы B, содержащий последний столбец из B, равен нулю. Пусть

$$D=\begin{vmatrix} a_{\alpha\varkappa} & \ldots & a_{\alpha\tau} & b_{\alpha}\\ \ldots & \ldots & \ldots & \ldots\\ a_{\theta\varkappa} & \ldots & a_{\theta\tau} & b_{\theta}\\ a_{\rho\varkappa} & \ldots & a_{\rho\tau} & b_{\rho} \end{vmatrix}$$

такой детерминант; здесь $\varkappa,\ldots,\tau$ какие-то r из чисел $1,2,\ldots,n$, а $\alpha,\ldots,\theta,\rho$ — какие-то $r+1$ из чисел $1,2,\ldots,n$. Но по условию

$$b_{\alpha}=\sum_{s=1}^{n}a_{\alpha s}\overline{x}_s,\ \ldots,\ b_{\theta}=\sum_{s=1}^{n}a_{\theta s}\overline{x}_s,\quad b_{\rho}=\sum_{s=1}^{n}a_{\rho s}\overline{x}_s;$$

подставляя это в D и применяя к D свойства V и III § 30, получим:

$$D = \overline{x}_1 \begin{vmatrix} a_{\alpha\varkappa} & \dots & a_{\alpha\tau} & a_{\alpha 1} \\ \dots\dots\dots\dots\dots\dots \\ a_{\theta\varkappa} & \dots & a_{\theta\tau} & a_{\theta 1} \\ a_{\rho\varkappa} & \dots & a_{\rho\tau} & a_{\rho 1} \end{vmatrix} + \overline{x}_2 \begin{vmatrix} a_{\alpha\varkappa} & \dots & a_{\alpha\tau} & a_{\alpha 2} \\ \dots\dots\dots\dots\dots\dots \\ a_{\theta\varkappa} & \dots & a_{\theta\tau} & a_{\theta 2} \\ a_{\rho\varkappa} & \dots & a_{\rho\tau} & a_{\rho 2} \end{vmatrix} + \dots +$$

$$+ \overline{x}_n \begin{vmatrix} a_{\alpha\varkappa 1} & \dots & a_{\alpha\tau} & a_{\alpha n} \\ \dots\dots\dots\dots\dots\dots \\ a_{\theta\varkappa} & \dots & a_{\theta\tau} & a_{\theta n} \\ a_{\rho\varkappa} & \dots & a_{\rho\tau} & a_{\rho n} \end{vmatrix};$$

но каждый детерминант правой части равен нулю, как детерминант $(r+1)$-го порядка матрицы A или как такой детерминант, у которого есть два одинаковых столбца; следовательно, $D = 0$ и наша теорема доказана.

§ 41. Из доказательства предыдущей теоремы видно, что если ранг A равен рангу B равен r, то система (22) имеет решение, в котором $n-r$ неизвестных получают произвольные значения (в нашем случае $x_{r+1}, \dots, x_n$). Но верно и обратное предложение:

Теорема 2. *Если ранг A равен рангу $B = r$, ото система* (22) *имеет решение, в котором $n - r$ неизвестных получают произвольные значения. Обратно: если система* (22) *имеет решение, в котором s неизвестных (но не больше, чем s) получают произвольные значения, то $r = n - s$ есть ранг A (а, следовательно, по теореме* 1 *и ранг B).*

Доказательство. Нам остается доказать вторую часть теоремы. Очевидно, что ранг A не может быть $< r$, ибо тогда (см. доказательство теоремы 1) больше чем s неизвестных получили бы произвольные значения. Таким образом ранг $A > r$; но мы докажем, что он равен r, т. е. что все детерминанты $(r+1)$-го порядка матрицы A равны нулю. Возьмем такой детерминант $(r+1)$-го порядка матрицы A, у которого по крайней мере один из миноров r-го порядка не равен нулю. Не нарушая общности, мы можем предположить, что этот взятый детерминант имеет вид:

$$D = \begin{vmatrix} a_{11} & \dots & a_{1r} & a_{1\lambda} \\ \dots\dots\dots\dots\dots\dots \\ a_{r1} & \dots & a_{rr} & a_{r\lambda} \\ a_{\mu 1} & \dots & a_{\mu r} & a_{\mu\lambda} \end{vmatrix},$$

где λ — одно из значений $r+1, \dots, n$, μ — одно из значений $r+1, \dots, n$ и

$$\Delta = \begin{vmatrix} a_{11} & \dots & a_{1r} \\ \dots\dots\dots\dots\dots \\ a_{r1} & \dots & a_{rr} \end{vmatrix} \neq 0.$$

В таком случае мы можем (как и в § 40) всегда решить первые r уравнений (22), давая для $x_{r+1}, \dots, x_n$ произвольные значения; пусть $\overline{x}_1, \dots, \overline{x}_n$ такое решение; но тогда эти значения $\overline{x}_1, \dots, \overline{x}_n$ удовлетворят и остальным уравнениям (22). Действительно, пусть $x_{\alpha 1}, \dots, x_{\alpha s}$ те неизвестные, которым по условию теоремы мы можем придать произвольные значения; возьмем как раз $x_{\alpha 1} = \overline{x}_{\alpha 1}$, …, $x_{\alpha s} = \overline{x}_{\alpha s}$; в таком случае по условию теоремы мы можем подобрать остальные

неизвестные так, чтобы все уравнения (22) удовлетворились; но для того чтобы первые r уравнений удовлетворялись при $x_{\alpha 1} = \overline{x}_{\alpha 1}, \ldots, x_{\alpha s} = \overline{x}_{\alpha s}$, все остальные неизвестные должны иметь полученные раньше значения $\overline{x}_1, \overline{x}_2, \ldots, \overline{x}_n$, которые, таким образом, удовлетворят и остальным уравнениям (22) [16]. Отсюда же следует, что мы всегда можем удовлетворить уравнениям (22), придав последним s неизвестным $x_{r+1}, \ldots, x_n$ произвольные значения.

Если теперь окажется, что $D \neq 0$, то, рассуждая совершенно так же, мы найдем, что можно решить первые r уравнений и еще μ-е уравнение, давая для $x_{r+1}, \ldots, x_{\lambda-1}, x_{\lambda+1}, \ldots, x_n$ произвольные значения. Таким образом мы пришли к противоречию: с одной стороны, мы можем дать для x_λ произвольное значение, с другой стороны, не можем. Следовательно, должно быть $D = 0$, и наша теорема доказана.

Это наибольшее число s неизвестных, которым мы можем давать произвольные значения, называется *степенью неопределенности* системы (22); теорема 2 говорит, что степень неопределенности есть так называемое «дополнение ранга» $n - r$. Конечно, не следует думать, что мы любым s из наших неизвестных можем давать произвольные значения. В частности при $r = n$ будет $s = 0$; в этом случае ни одному из неизвестных нельзя давать произвольных значений: система определенна. Это может быть только при $m \geq n$. Если же $m < n$, то система всегда неопределенна (если только она совместна).

§ 42. Укажем еще на одно значение ранга r матрицы A. Обозначим через y_α левые части уравнений (22), т. е.

$$y_\alpha = \sum_{\beta=1}^{n} a_{\alpha\beta} x_\beta \qquad (\alpha = 1, 2, \ldots, m). \tag{24}$$

Если считать $x_1, \ldots, x_n$ независимыми переменными, то $y_1, \ldots, y_m$ будут линейными однородными функциями от $x_1, \ldots, x_n$, или *линейными формами* от $x_1, \ldots, x_n$. Формы $y_1, \ldots, y_m$ называются *линейно зависимыми*, если можно подобрать постоянные количества $k_1, \ldots, k_m$, которые не все равны нулю, так, чтобы было тождественно:

$$k_1 y_1 + k_2 y_2 + \ldots + k_m y_m = 0. \tag{25}$$

Если же это тождество возможно только при $k_1 = k_2 = \ldots = k_m = 0$, то $y_1, \ldots, y_m$ *линейно независимы*. Если, например, $k_1 \neq 0$, то, разделив обе части (25) на k_1 и обозначив $-\dfrac{k_\lambda}{k_1} = l_\lambda$, получим:

$$y_1 = l_2 y_2 + l_3 y_3 + \ldots + l_m y_m. \tag{26}$$

В этом случае говорят, что y_1 *линейно зависит* от $y_2, \ldots, y_m$. Зная значения $y_2, \ldots, y_m$, мы из (26) найдем и значение y_1. Поэтому в данной системе линейных форм важно определить, сколько и какие из них линейно независимы.

Теорема 3. *Число линейно независимых форм* (24) *равно рангу* r *матрицы* A *коэфициентов форм.*

[16] По условию теоремы при данных $\overline{x}_1, \ldots, \overline{x}_n$ все остальные неизвестные должны получать вполне определенные значения $\overline{x}_1, \ldots, \overline{x}_n$ для того, чтобы уравнения (22) удовлетворились.

Доказательство. 1. Пусть ранг $A = r$, причем

$$\Delta = \begin{vmatrix} a_{11} & \dots & a_{1r} \\ \dots\dots\dots\dots\dots \\ a_{r1} & \dots & a_{rr} \end{vmatrix} \neq 0;$$

покажем, что формы $y_1, \dots, y_r$ линейно независимы, а всякая другая фирма y_λ из системы (24) линейно зависит от $y_1, \dots, y_r$. Положив в (25) $m = r$ и подставив выражения для $y_1, \dots, y_r$ получим, приравняв нулю коэфициенты при $x_1, \dots, x_r$:

$$\begin{gathered} a_{11}k_1 + a_{21}k_2 + \dots + a_{r1}k_r = 0, \\ a_{12}k_1 + a_{22}k_2 + \dots + a_{r2}k_r = 0, \\ \dots\dots\dots\dots\dots\dots\dots\dots \\ a_{1r}k_1 + a_{2r}k_2 + \dots + a_{rr}k_r = 0; \end{gathered}$$

это — система r линейных однородных уравнений с r неизвестными $k_1, \dots, k_r$, причем детерминант этой системы $\Delta \neq 0$; такая система (§ 33) имеет единственную систему решений: $k_1 = k_2 = \dots = k_r = 0$; значит, $y_1, \dots, y_r$ линейно независимы.

Пусть λ — одно из чисел $r+1, \dots, m$; докажем, что y_λ линейно зависит от $y_1, \dots, y_r$, т. е. что можно найти числа $l_1, \dots, l_r$ так, чтобы было тождественно: $y_\lambda \equiv l_1y_1 + l_2y_2 + \dots + l_ry_r$, это дает такую систему уравнений для $l_1, \dots, l_r$ (получаемых приравниванием коэфициентов при $x_1, \dots, x_r$ в обеих частях):

$$\begin{gathered} a_{11}l_1 + a_{21}l_2 + \dots + a_{r1}l_r = a_{\lambda 1}, \\ a_{12}l_1 + a_{22}l_2 + \dots + a_{r2}l_r = a_{\lambda 2}, \\ \dots\dots\dots\dots\dots\dots\dots\dots \\ a_{1r}l_1 + a_{2r}l_2 + \dots + a_{rr}l_r = a_{\lambda r}. \end{gathered}$$

Детерминант этой системы $\Delta \neq 0$; следовательно (по § 33), система имеет одну и только одну систему решений $l_1, l_2, \dots, l_r$; эти же значения $l_1, \dots, l_r$ удовлетворят и уравнениям (получаемым приравниванием коэфициентов при $x_{r+1}, \dots, x_n$):

$$\begin{gathered} a_{1,r+1}l_1 + a_{2,r+1}l_2 + \dots + a_{r,r+1}l_r = a_{\lambda,r+1}, \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ a_{1n}l_1 + a_{2n}l_2 + \dots + a_{rn}l_r = a_{\lambda n}, \end{gathered}$$

что следует из теоремы 1, § 40, на основании того, что ранг A есть r; следовательно, действительно для найденных значений $l_1, \dots, l_r$ будет тождественно

$$y_\lambda \equiv l_1y_1 + l_2y_2 + \dots + l_ry_r.$$

2. Пусть теперь $y_1, y_2, \dots, y_r$ линейно независимы, а $y_{r+1}, \dots, y_m$ зависят от $y_1, \dots, y_r$. Докажем, что r есть ранг матрицы A. Тождество (25) равносильно следующей системе равенств:

$$\begin{gathered} a_{11}k_1 + a_{21}k_2 + \dots + a_{r1}k_r = 0, \\ a_{12}k_1 + a_{22}k_2 + \dots + a_{r2}k_r = 0, \\ \dots\dots\dots\dots\dots\dots\dots\dots \\ a_{1r}k_1 + a_{2r}k_2 + \dots + a_{rr}k_r = 0. \end{gathered} \quad .$$

Это — система n линейных однородных уравнений с r неизвестными $k_1, \ldots, k_r$, имеющая только одну систему решений: $k_1 = k_2 = \ldots = k_r = 0$, ибо $y_1, \ldots, y_r$ линейно независимы. Следовательно, по теореме 2, § 41, ранг матрицы

$$\begin{pmatrix} a_{11} & \ldots & a_{r1} \\ \ldots\ldots\ldots\ldots \\ a_{1n} & \ldots & a_{rn} \end{pmatrix}$$

должен равняться числу неизвестных r, т. е. один из детерминантов r-го порядка этой матрицы должен быть не равен нулю. Не нарушая общности, мы можем положить:

$$\Delta = \begin{vmatrix} a_{11} & \ldots & a_{1r} \\ \ldots\ldots\ldots\ldots \\ a_{r1} & \ldots & a_{rr} \end{vmatrix} \neq 0.$$

Нам остается доказать, что все детермиранты $(r+1)$-го порядка матрицы A равны нулю. Заметим, что всякие $r+1$ наших форм $y_{\alpha_1}, y_{\alpha_2} \ldots, y_{\alpha_{r+1}}$, линейно зависимы; действительно, все они зависят от $y_1, y_2, \ldots, y_r$, т. е.

$$\begin{gathered} y_{\alpha_1} = l_{11}y_1 + \ldots + l_{1r}y_r, \\ y_{\alpha_2} = l_{21}y_1 + \ldots + l_{2r}y_r, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ y_{\alpha_{r+1}} = l_{r+1,1}y_1 + \ldots + l_{r+1,r}y_r. \end{gathered}$$

Возьмем такую систему равенств:

$$\begin{gathered} l_{11}k_1 + l_{21}k_2 + \ldots + l_{r+1,1}k_{r+1} = 0, \\ l_{12}k_1 + l_{22}k_2 + \ldots + l_{r+1,2}k_{r+1} = 0, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ l_{1r}k_1 + l_{2r}k_2 + \ldots + l_{r+1,r}k_{r+1} = 0. \end{gathered} \tag{27}$$

Это — система r линейных однородных уравнений с $r+1$ неизвестными $k_1, \ldots, k_{r+1}$; по теореме 2 по крайней мере одно из неизвестных мы можем выбрать произвольно, т. е. можно найти такую систему решений уравнений (27), где не все неизвестные равны нулю. Но из (27) следует: $k_1y_{\alpha_1} + k_2y_{\alpha_2} + \ldots + k_{r+1}y_{\alpha_{r+1}} = 0$, причем не все $k_\lambda = 0$, т. е. $y_{\alpha_1}, \ldots, y_{\alpha_{r+1}}$ линейно зависимы. Это нам дает, если выразить $y_{\alpha_1}, \ldots, y_{\alpha_{r+1}}$ через $x_1, \ldots, x_n$:

$$\begin{gathered} a_{\alpha_1 1}k_1 + a_{\alpha_2 1}k_2 + \ldots + a_{\alpha_{r+1}1}k_{r+1} = 0, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{\alpha_1 n}k_1 + a_{\alpha_2 n}k_2 + \ldots + a_{\alpha_{r+1}n}k_{r+1} = 0. \end{gathered}$$

Если возьмем какие-нибудь $r+1$ из этих n уравнений, то получим систему $r+1$ линейных однородных уравнений с $r+1$ неизвестными $k_1, \ldots, k_{r+1}$; эта система удовлетворяется значениями неизвестных, из которых не все равны нулю; по § 33, следствию II, детерминант, составленный из коэфициентов этой системы, должен быть равен нулю, а это — любой детерминант $r+1$ порядка из A; таким образом наша теорема доказана.

Теорема 4. *Условие: в системе* (22) *ранг* A *равен рангу* B, *равносильно такому: всякое тождественное соотношение* $k_1y_{\alpha_1} + k_2y_{\alpha_2} + \ldots + k_\lambda y_{\alpha_\lambda} = 0$, *влечет за собой соотношение:*

$$k_1b_{\alpha_1} + k_2b_{\alpha_2} + \ldots + k_\lambda b_{\alpha_\lambda} = 0.$$

Доказательство. 1. Пусть ранг A равен рангу B; тогда система (22) имеет решения; для всякого решения будет: $y_{\alpha_1} = b_{\alpha_1}$, $y_{\alpha_2} = b_{\alpha_2}$, $\ldots$, $y_{\alpha_\lambda} = b_{\alpha_\lambda}$,; следовательно, если вообще

$$k_1y_{\alpha_1} + k_2y_{\alpha_2} + \ldots + k_\lambda y_{\alpha_\lambda} = 0,$$

то отсюда следует и $k_1b_{\alpha_1} + k_2b_{\alpha_2} + \ldots + k_\lambda b_{\alpha_\lambda} = 0$.

2. Пусть теперь нам дано, что из $k_1y_{\alpha_1} + \ldots + k_\lambda y_{\alpha_\lambda} = 0$ следует

$$k_1b_{\alpha_1} + k_2b_{\alpha_2} + \ldots + k_\lambda b_{\alpha_\lambda} = 0.$$

Пусть ранг $A = r$, и пусть

$$\Delta = \begin{vmatrix} a_{11} & \ldots & a_{1r} \\ \ldots\ldots\ldots\ldots \\ a_{r1} & \ldots & a_{rr} \end{vmatrix} \neq 0;$$

тогда формы $y_1, \ldots, y_r$ линейно независимы, но каждая из остальных форм y_λ (по теореме 3) линейно зависит от $y_1, \ldots, y_r$:

$$y_\lambda = l_1y_1 + l_2y_2 + \ldots + l_ry_r;$$

в этом случае по условию:

$$b_\lambda = l_1b_1 + l_2b_2 + \ldots + l_rb_r.$$

Решив первые r уравнений: $y_1 = b_1$, $y_2 = b_2$, $\ldots$, $y_r = b_r$, мы увидим, что этими решениями и остальные уравнения (1) $y_\lambda = b_\lambda$ удовлетворяются; следовательно, система (22) имеет решение, а следовательно, по теореме 1 ранг A равен рангу B.

Отсюда видно, что если только система (22) совместна (т. е. ранг A равен рангу B), то для ее решения достаточно взять только те ее уравнения, левые части которых линейно независимы друг от друга; число таких уравнений как раз и равняется рангу A.

§ 43. Общее решение уравнений (22) представляется в виде:

$$x_\varkappa = d_\varkappa + \sum_{\lambda=1}^{s} c_{\varkappa\lambda}t_\lambda; \qquad \varkappa == 1, 2, \ldots, n; \qquad s = n - r. \tag{28}$$

Действительно, пусть мы даем произвольные значения неизвестным $x_{r+1}, \ldots, x_n$ (число их равно $n-r = s$); положим $x_{r+1} = t_1, \ldots, x_n = t_s$; в таком случае $x_1, \ldots, x_r$ найдутся из некоторых r уравнений (22); например, из r первых уравнений, которые будут иметь вид:

$$\sum_{\beta=1}^{r} a_{\alpha\beta}x_\beta = b_\alpha - a_{\alpha,r+1}t_1 - \ldots - a_{\alpha n}t_s; \qquad \alpha = 1, 2, \ldots, r.$$

Из них найдем, например:

$$x_1 = \frac{\begin{vmatrix} b_1 - a_{1,r+1}t_1 - \ldots - a_{1n}t_s & a_{12} & \ldots & a_{1r} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ b_r - a_{r,r+1}t_1 - \ldots - a_{rn}t_s & a_{r2} & \ldots & a_{rr} \end{vmatrix}}{\begin{vmatrix} a_{11} & \ldots & a_{1r} \\ \ldots\ldots\ldots \\ a_{r1} & \ldots & a_{rr} \end{vmatrix}}$$

$$= \frac{1}{\Delta}\begin{vmatrix} b_1 & a_{12} & \ldots & a_{1r} \\ \ldots\ldots\ldots\ldots\ldots \\ b_r & a_{r2} & \ldots & a_{rr} \end{vmatrix} - t_1 \cdot \frac{1}{\Delta}\begin{vmatrix} a_{1,r+1} & a_{12} & \ldots & a_{1r} \\ \ldots\ldots\ldots\ldots\ldots \\ a_{r,r+1} & a_{r2} & \ldots & a_{rr} \end{vmatrix} -$$

$$- \ \ldots - t_s \cdot \frac{1}{\Delta}\begin{vmatrix} a_{1n} & a_{12} & \ldots & a_{1r} \\ \ldots\ldots\ldots\ldots\ldots \\ a_{rn} & a_{r2} & \ldots & a_{rr} \end{vmatrix},$$

где, как и раньше,

$$\Delta = \begin{vmatrix} a_{11} & \ldots & a_{1r} \\ \ldots\ldots\ldots \\ a_{r1} & \ldots & a_{rr} \end{vmatrix} \neq 0.$$

Но это выражение для x_1 как раз и имеет вид (28); такие же выражения получим для $x_2, \ldots, x_r$; для $x_{r+1}, \ldots, x_n$ имеем прямо: $x_{r+1} = t_1$, $\ldots$, $x_n = t_s$; это — тоже частные случаи формулы (28) (где один из коэфициентов равен единице, а остальные равны нулю).

Итак, наши неизвестные представляются как линейные (но неоднородные) функции s параметров.

Пример. Дана система:

$$3x + 2y - 5z - 4t = 1,$$
$$5x - 3y - z + 3t = 3,$$
$$x + 7y - 9z - 11t = -1,$$
$$2x - 5y + 4z + 7t = 2,$$
$$13x - 4y - 7z + 2t = 7.$$

Здесь

$$A = \begin{pmatrix} 3 & 2 & -5 & -4 \\ 5 & -3 & -1 & 3 \\ 1 & 7 & -9 & -11 \\ 2 & -5 & 4 & 7 \\ 13 & -4 & -7 & 2 \end{pmatrix}, \qquad B = \begin{pmatrix} 3 & 2 & -5 & -4 & 1 \\ 5 & -3 & -1 & 3 & 3 \\ 1 & 7 & -9 & -11 & -1 \\ 2 & -5 & 4 & 7 & 2 \\ 13 & -4 & -7 & 2 & 7 \end{pmatrix}.$$

Легко убедиться, что ранг A равен рангу B равен 2. Здесь детерминант, составленный из элементов, общих первым двум строкам и первым двум столбцам: $\begin{vmatrix} 3 & 2 \\ 5 & -3 \end{vmatrix} \neq 0$. Система имеет решения, зависящие от $4 - 2 = 2$ параметров; независимых уравнений в системе два; например, первые два уравнения независимы;

за произвольные параметры можно принять z и t. Решаем первые два уравнения системы относительно x и y:

$$\begin{aligned} 3x + 2y &= 1 + 5z + 4t, \\ 5x - 3y &= 3 + z - 3t, \end{aligned}\quad ,$$

найдем

$$\begin{aligned} x &= \frac{9}{19} + \frac{7}{19}z + \frac{6}{19}t, \\ y &= -\frac{4}{19} + \frac{22}{19}z + \frac{29}{19}t, \\ z &= z, \\ t &= t. \end{aligned}$$

Эти формулы и дают общее решение всей нашей системы.

Упражнения

61) Исследовать и решить систему:

$$\begin{aligned} 2x - 3y + 5z &= 0, \\ 8x + 2y - z &= 21, \\ 10x - y + 4z &= 21. \end{aligned}$$

Отв. $x = \dfrac{9 - z}{4}$, $y = \dfrac{3 + 3z}{2}$.

62) Исследовать и решить систему:

$$\begin{aligned} 8x + 6y - z - t &= 12, \\ x - 3y + 2z + 2t &= 2, \\ x + 2y + z - 4t &= 0, \\ 6x + 7y - 4z + t &= 10, \\ 6x + 2y - 3z + 7t &= 12. \end{aligned}$$

Отв. $x = \dfrac{20 - 9t}{11}$, $y = \dfrac{17t - 6}{11}$, $z = \dfrac{19t - 8}{11}$.

§ 44. Особенно важен случай, когда все правые части уравнений (22), b_α равны нулю, т. е. когда система (22) есть система *однородных* линейных уравнений. В этом случае последний столбец матрицы B состоит из нулей, так что ранг A всегда равен рангу B. Следовательно, система однородных линейных уравнений всегда имеет решение; действительно, одно решение очевидно: это, когда все $x_\beta = 0$ («тривиальное» решение). Все остальные теоремы § 40 и 43, конечно, верны и для однородных уравнений. В частности верна и формула (28), причем здесь все $d_\varkappa = 0$ (ибо все $b_\varkappa = 0$); таким образом общее решение системы однородных уравнений ранга r дает значения x_k как линейные *однородные* функции от $s = n - r$ параметров:

$$x_\varkappa = \sum_{\lambda=1}^{s} c_{\varkappa\lambda} t_\lambda \qquad (\varkappa = 1, 2, \ldots, n). \tag{29}$$

Дав для t_μ значение, равное единице, а для остальных t_λ значения, равные нулю, мы получим из (29): $x_1 = c_{1\mu}$, $x_2 = c_{2\mu}$, $\ldots$, $x_n = c_{n\mu}$, т. е. эти системы коэфициентов $c_{1\mu}, c_{2\mu}, \ldots, c_{n\mu}$, представляют собою частные решения наших однородных уравнений (22); формула (29) дает s таких систем частных решений.

Заметим, что если дано несколько систем каких-либо частных решений системы линейных однородных уравнений: $x'_1, x'_2, \ldots, x'_n$; $x''_1, x''_2, \ldots, x''_n$; $\ldots$; $x_1^{(h)}, x_2^{(h)}$, $\ldots, x_n^{(h)}$, то выражения:

$$\begin{aligned} z_1 &= x'_1 k_1 + x''_1 k_2 + \ldots x_1^{(h)} k_h, \\ z_2 &= x'_2 k_1 + x''_2 k_2 + \ldots x_2^{(h)} k_h, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ z_n &= x'_n k_1 + x''_n k_2 + \ldots n_1^{(h)} k_h \end{aligned}$$

при всяких значениях $k_1, k_2, \ldots, k_h$, тоже будут представлять собою систему решений наших уравнений. Мы говорим, что решение $z_1, z_2, \ldots, z_n$ *линейно зависит* от решений $x'_\varkappa, x''_\varkappa, \ldots, x_\varkappa^{(h)}$. Сами решения $x'_\varkappa, x''_\varkappa, \ldots, x_\varkappa^{(h)}$ назовем *линейно независимыми*, если $z_1, z_2, \ldots, z_n$ будут все равны нулю только при $k_1 = k_2 = \ldots = k_h = 0$; в противном случае наши h систем решений *линейно зависимы*. Очевидно, что наши решения будут линейно зависимыми или независимыми, смотря по тому, будут ли линейные формы:

$$v_\varkappa = \sum_{\lambda=1}^{n} x_\lambda^{(\varkappa)} u_\lambda \qquad (\varkappa = 1, 2, \ldots, h) \tag{30}$$

линейно зависимыми или независимыми. Число линейно независимых форм (30), а следовательно, и линейно независимых решений по теореме 3, § 42 равно рангу матрицы

$$\begin{pmatrix} x'_1 & x'_2 & \ldots & x'_n \\ x''_1 & x''_2 & \ldots & x''_n \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots \\ x_1^{(h)} & x_2^{(h)} & \ldots & x_n^{(h)} \end{pmatrix}.$$

Мы докажем следующее:

Теорема 5. *s частных решений $c_{1\mu}, c_{2\mu}, \ldots, c_{n\mu}$ [формула (29)] системы линейных однородных уравнений линейно независимы; всякое другое решение той же системы линейно зависит от этих s решений.*

Доказательство. 1. Нам надо доказать, что ранг матрицы

$$\begin{pmatrix} c_{11} & c_{21} & \ldots & c_{n1} \\ c_{12} & c_{22} & \ldots & c_{n2} \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots \\ c_{1s} & c_{2s} & \ldots & c_{ns} \end{pmatrix}$$

равен s, т. е. что по крайней мере один из детерминантов s-го порядка этой матрицы равен нулю [все детерминанты $(s+1)$-го порядка, очевидно, равны нулю, так как наша матрица имеет всего s строк]. Но мы имеем [см. вывод формулы (28), частным случаем которой является формула (29)]:

$$x_{r+1} = t_1, \quad x_{r+2} = t_2, \ \ldots, \ x_n = t_s,$$

т. е.

$$\begin{aligned} &c_{r+1,1}=1, \quad c_{r+1,2}=0,\ldots \quad c_{r+1,s}=0,\\ &c_{r+2,1}=0, \quad c_{r+2,2}=1,\ldots \quad c_{r+2,s}=0,\\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\ &c_{n,1}=0, \qquad c_{n,2}=0,\ldots \qquad c_{ns}=1, \end{aligned}$$

значит, детерминант s-го порядка, составленный из s последних столбцов нашей матрицы, есть

$$\begin{vmatrix} 1 & 0 & 0 & \ldots & 0\\ 0 & 1 & 0 & \ldots & 0\\ 0 & 0 & 1 & \ldots & 0\\ \ldots & \ldots & \ldots & \ldots & \ldots\\ 0 & 0 & 0 & \ldots & 1 \end{vmatrix} = 1 \neq 0,$$

и первая часть нашей теоремы доказана.

2. Формула (29) показывает, что всякое решение нашей системы линейных однородных уравнений линейно зависит от решений $c_{\varkappa\lambda}$.

Определение. Система решений однородных линейных уравнений называется *полной*, если все решения этой системы линейно независимы, а всякое другое решение тех же уравнений линейно зависит от решений системы.

Таким образом решения $c_{1\mu}, c_{2\mu}, \ldots, c_{n\mu}$ $(\mu = 1, 2, \ldots, s)$ составляют полную систему решений.

Пусть $x_1^{(\lambda)}, x_2^{(\lambda)}, \ldots, x_n^{(\lambda)}$ $(\lambda = 1, 2, \ldots, h)$ — какие-нибудь h решений нашей системы линейных однородных уравнений; найдем условия, при которых эти h решений представляют полную систему решений.

Имеем:

$$\left.\begin{aligned} x_1^{(\lambda)} &= \sum_{\mu=1}^{s} c_{1\mu}t_{\mu\lambda},\\ x_2^{(\lambda)} &= \sum_{\mu=1}^{s} c_{2\mu}t_{\mu\lambda},\\ &\ldots\ldots\ldots\ldots\ldots\\ x_n^{(\lambda)} &= \sum_{\mu=1}^{s} c_{n\mu}t_{\mu\lambda}, \end{aligned}\right\} \tag{31}$$

где $t_{\mu\lambda}$ какие-то коэфициенты; $\lambda = 1, 2, \ldots, h$. Пусть $u_1, \ldots, u_n$ независимые переменные; умножим (31) соответственно на $u_1, u_2, \ldots, u_n$ и сложим; получим:

$$v_\lambda = \sum_{\mu=1}^{s} t_{\mu\lambda}w_\mu, \tag{32}$$

где

$$v_\lambda = \sum_{\varkappa=1}^{n} x_\varkappa^{(\lambda)}u_k, \quad w_\mu = \sum_{\varkappa=1}^{n} c_{\varkappa\mu}u_\varkappa, \qquad \lambda = 1, 2, \ldots, h, \quad \mu = 1, 2, \ldots, s.$$

(32) показывает, что линейные формы v_λ зависят от линейных форм w_μ; для того чтобы v_λ были линейно независимыми друг от друга, их число h должно быть

$\leq s$ Но если $x_{\varkappa}^{(\lambda)}$ должны составлять полную систему решений, то, обратно, и w_μ должны быть линейно зависимыми от v_λ, т. е. должно быть $\leq s$; следовательно, $h = s$. Мы можем рассматривать формы v_λ как линейные однородные функции от w_μ согласно (32); по теореме 3 для линейной независимости форм v_λ друг от друга, ранг матрицы

$$\begin{pmatrix} t_{11} & t_{21} & \dots & t_{s1} \\ t_{12} & t_{22} & \dots & t_{s2} \\ \dots\dots\dots\dots\dots \\ t_{1s} & t_{2s} & \dots & t_{ss} \end{pmatrix}$$

должен быть равен s, т. е. ее единственный детерминант s-го порядка должен быть не равен нулю:

$$\begin{vmatrix} t_{11} & t_{21} & \dots & t_{s1} \\ t_{12} & t_{22} & \dots & t_{s2} \\ \dots\dots\dots\dots\dots \\ t_{1s} & t_{2s} & \dots & t_{ss} \end{vmatrix} \neq 0. \tag{33}$$

Обратно, если это условие выполнено, то уравнения (31)

$$x_{\varkappa}^{(\lambda)} = \sum_{\mu=1}^{s} c_{\varkappa\mu} t_{\mu\lambda} \qquad (\lambda = 1, 2, \dots, s)$$

можно решить относительно $c_{\varkappa 1}, c_{\varkappa 2}, \dots, c_{\varkappa s}$ при всяком $\varkappa = 1, 2, \dots, n$, т. е. $c_{\varkappa\lambda}$ можно выразить через $x_{\varkappa}^{(\lambda)}$ (линейно и однородно); следовательно, $x_{\varkappa}^{(\lambda)}$ представят полную систему решений. Итак:

Теорема 6. *Во всякой полной системе решений однородных линейных уравнений число решений одно и то же, т. е. равно s (дополнению ранга системы). Формулы* (31) *дают полную систему решений тогда и только тогда, если выполнено условие* (33).

§ 45. Возвратимся еще раз к системе (22) неоднородных линейных уравнений. Пусть $x_1^{(0)}, x_2^{(0)}, \dots, x_n^{(0)}$ какое-нибудь решение этой системы, а $x_1, x_2, \dots, x_n$ какое-нибудь другое решение той же системы. Имеем:

$$\sum_{\beta=1}^{n} a_{\alpha\beta} x_\beta = b_\alpha, \qquad \sum_{\beta=1}^{n} a_{\alpha\beta} x_\beta^{(0)} = b_\alpha;$$

отсюда, вычитая, найдем:

$$\sum_{\beta=1}^{n} a_{\alpha\beta} (x_\beta - x_\beta^{(0)}) = 0,$$

т. е.

$$u_\beta = x_\beta - x_\beta^{(0)} \qquad (\beta = 1, 2, \dots, n)$$

есть решение так называемой «приведенной» системы, т. е. системы однородных линейных уравнений:

$$\sum_{\beta=1}^{n} a_{\alpha\beta} u_\beta = 0 \qquad (\alpha = 1, 2, \dots, n). \tag{34}$$

Обратно, если u_β — решение системы (34), то $x_\beta = x_\beta^{(0)} + u_\beta$ будет решением системы (22). Итак:

Теорема 7. *Общее решение системы* (22) *равно сумме какого-нибудь частного решения этой системы и общего решения «приведенной» системы* (34).

Например, в формулах (28) $d_\varkappa$ являются частным решением системы (22) (именно, при всех $t_\lambda = 0$), а $\sum_{\lambda=1}^{s} c_{\varkappa\lambda} t_\lambda$ — общим решением приведенной системы (34).

Упражнения

63) Найти полную систему решений системы уравнений

$$\begin{aligned} 3x_1 - 4x_2 + 2x_3 + x_4 - x_5 - x_6 &= 0, \\ 5x_1 + 2x_2 - x_3 - 3x_4 + x_5 - 4x_6 &= 0, \\ 2x_1 + x_2 - 5x_3 + 6x_4 - 2x_5 - 2x_6 &= 0. \end{aligned} \quad .$$

Отв. $45, 158, 190, 117, 0, 0$; $9, 68, 64, 0, -117, 0$; $9, 3, -1, 0, 0, 13$.

64) Выяснить, составят ли решения $40, -15, 5, 5$; $0, 33, 5, 45$ полную систему решений системы уравнений:

$$\begin{aligned} 3x + 5y - 6z - 3t &= 0, \\ 2x + 5y + 3z - 4t &= 0. \end{aligned} \quad .$$

ГЛАВА ТРЕТЬЯ

РАЦИОНАЛЬНЫЕ ФУНКЦИИ

§ 46. Целая рациональная функция. Выражение вида:

$$a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \ldots + a_{n-1}x + a_n,$$

является *целой рациональной функцией* x здесь $a_0, a_1, a_2, \ldots, a_{n-1}, a_n$ — данные («постоянные» или «известные») числа; x — переменное количество. $a_0, a_1, \ldots, a_n$ могут быть любыми, комплексными или вещественными числами; точно так же и x может принимать любые вещественные или комплексные значения. Целое положительное число n — *степень* данной функции. Итак, целая функция есть многочлен, зависящий от x и обычно расположенный по степеням x; мы будем сокращенно обозначать ее через $f(x)$ или $g(x)$, $\varphi(x)$, $F(x)$ и т. д. В зависимости от значения x и целая рациональная функция принимает различные значения, и в этом смысле она и есть «функция от x». Целая рациональная функция n-й степени имеет $n+1$ член.

Примеры.

1. $f(x) = 5x^4 - 8x^3 + x^2 - 3x - 2$ есть ц. р. [17] функция 4-й степени; здесь $a_0 = 5$, $a_1 = -8$, $a_2 = 1$, $a_3 = -3$, $a_4 = -2$, $n = 4$.

2. $f(x) = x^7 - (3+2i)x^6 - \dfrac{3}{4}x^4 + (4-i)x^3 - 8ix^2 + 0,43x$ есть ц. р. функция 7-й степени; здесь $a_0 = 1$, $a_1 = -(3+2i)$, $a_2 = 0$, $a_3 = -\dfrac{3}{4}$, $a_4 = 4 - i$, $a_5 = -8i$, $a_6 = 0,43$, $a_7 - 0$.

3. $f(x) = x^3 + 1$ есть ц. р функция 33-й степени; здесь $a_0 = 1$, $a_1 = a_2 = 0$, $a_3 = 1$.

4. $f(x) = x$ есть ц. р. функция 11-й степени; здесь $a_0 = 1$, $a_1 = 0$.

5. Всякое постоянное количество a можно рассматривать как ц. р. функцию 0-й степени; она при всяком значении x равна одному и тому же числу a.

«Высший коэфициент» a_0 мы всегда предполагаем неравным нулю; остальные же коэфициенты могут быть частью или все равны нулю.

Итак, ц. р. функция есть многочлен и действия над ц. р. функциями совершаются по тем же правилам, как и над многочленами. В частности, сумма или разность двух или нескольких ц. р. функций есть тоже ц. р. функция. Относительно степени суммы или, разности заметим, что, если среди слагаемых имеется одно наивысшей степени, то и сумма будет иметь ту же степень; если же имеются несколько слагаемых, имеющих одну и ту же наивысшую степень n, то сумма

[17] Ц. р. — целая рациональная; в дальнейшем мы будем применять всюду это сокращение.

может быть и более низкой степени, чем n, ибо высшие члены в слагаемых n-й степени могут сократиться. В частности, если все слагаемые одной и той же степени, то степень суммы не выше степени каждого из слагаемых.

Пример.

$$f_1(x) = 5x^4 - 3x^3 + 2x^2 - 4x - 8,$$
$$f_2(x) = 3x^3 - 4x^2 + 9x + 2,$$
$$f_3(x) = -5x^4 + 4x^2 + 3,$$
$$f_1(x) + f_2(x) + f_3(x) = 2x^2 + 5x - 3.$$

Здесь в сумме сократились члены с x^4 и с x^3.

Из элементарного правила умножения расположенных многочленов выводим: *степень произведения целых рациональных функций равняется сумме степеней сомножителей.*

Пусть

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n; \quad g(x) = b_0x^m + b_1x^{m-1} + \ldots + b_{m-1}x + b_m;$$
$$f(x) \cdot g(x) = c_0x^{n+m} + c_1x^{n+m-1} + c_2x^{n+m-2} + \ldots + c_{n+m};$$

тогда легко видеть, что

$$c_0 = a_0b_0, \quad c_1 = a_0b_1 + a_1b_0, \quad c_2 = a_0b_2 + a_1b_1 + a_2b_0,$$

и вообще

$$c_{\alpha+\beta} = a_0b_{\alpha+\beta} + a_1b_{\alpha+\beta-1} + \ldots + a_\alpha b_\beta + \ldots + a_{\alpha+\beta}b_0,$$

причем при $\varkappa > n$, $\lambda > m$ следует положить $a_\varkappa = b_\lambda = 0$.

Пример.

$$f(x) = 3x^4 - 5x^3 - x + 2, \qquad g(x) = 2x^3 + 4x^2 - 3x - 1;$$

здесь

$$c_0 = 3 \cdot 2 = 6, \quad c_1 = 3 \cdot 4 - 5 \cdot 2 = 2, \quad c_2 = -3 \cdot 3 - 5 \cdot 4 + 0 \cdot 2 = -29,$$
$$c_3 = -3 \cdot 1 + 5 \cdot 3 + 0 \cdot 4 - 1 \cdot 2 = 10, \quad c_4 = 5 \cdot 1 - 0 \cdot 3 - 1 \cdot 4 + 2 \cdot 2 = 5,$$
$$c_5 = -0 \cdot 1 + 1 \cdot 3 + 2 \cdot 4 = 11, \quad c_6 = 1 \cdot 1 - 3 \cdot 2 = -5, \quad c_7 = -1 \cdot 2 = -2.$$

$$f(x) \cdot g(x) = 6x^7 + 2x^6 - 29x^5 + 10x^4 + 5x^3 + 11x^2 - 5x - 2.$$

§ 47. Деление целых рациональных функций. Пусть $f(x)$ и $g(x)$ имеют тот же вид, что и в предыдущем параграфе, и пусть n. Положим:

$$f(x) - \frac{a_0}{b_0}x^{n-m}g(x) = f_1(x);$$

$f_1(x)$ — ц. р. функция степени $n_1 < n$, ибо члены, содержащие x^n, сократятся. Продолжая тот же процесс, найдем ряд равенств:

$$f_1(x) - \frac{a_0'}{b_0}x^{n_1-m}g(x) = f_2(x),$$
$$f_2(x) - \frac{a_0''}{b_0}x^{n_2-m}g(x) = f_3(x),$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

Здесь $f_1(x)$, $f_2(x)$, $f_3(x)$, ... — ц. р. функции степеней $n_1, n_2, n_3, \ldots$, причем $n > n_1 > n_2 > n_3 > \ldots$, $a_0', a_0'', a_0''', \ldots$ — высшие коэфициенты в $f_1(x)$, $f_2(x)$, $f_3(x)$, ... Этот процесс мы продолжаем до тех пор, пока получаемые степени $n_1, n_2, n_2, \ldots$ все больше или равны m, и оканчиваем его, как только достигнем функции $f_\lambda(x)$ степени $n_\lambda < m$ (что непременно случится).

Сложим после этого все полученные равенства почленно; найдем;

$$f(x) - \left(\frac{a_0}{b_0}x^{n-m} + \frac{a_0'}{b_0}x^{n_1-m} + \frac{a_0''}{b_0}x^{n_2-m} + \ldots\right)g(x) = f_1(x).$$

Положим:

$$\frac{a_0}{b_0}x^{n-m} + \frac{a_0'}{b_0}x^{n_1-m} + \frac{a_0''}{b_0}x^{n_2-m} + \ldots\, q(x); \qquad f_\lambda(x) = r(x);$$

тогда

$$f(x) = g(x)q(x) + r(x),$$

причем степень $q(x) = n - m$, степень $r(x) < m$.

В случае, если $n < m$, имеем:

$$q(x) = 0, \qquad r(x) = f(x).$$

В случае, если $n = m$, имеем:

$$q(x) = \frac{a_0}{b_0}, \qquad r(x) = f(x) - \frac{a_0}{b_0}g(x).$$

Итак:

Теорема. *Если $f(x)$ и $g(x)$ — две любые целые рациональные функции, то можно всегда найти целые рациональные функции $q(x)$ и $r(x)$ такие, что будет:*

$$f(x) = g(x)q(x) + r(x),$$

и степень $r(x)$ меньше степени $g(x)$ при этом функции $g(x)$, $r(x)$ определяются однозначно.

Примечание. Равенство $f(x) = g(x)q(x) + r(x)$ есть тождество; это значит, что в обеих его частях стоит одна и та же ц. р. функция, или: если в правой части произвести указанные умножения и сложения, то получится ц. р. функция та же самая (т. е. с теми же коэфициентами при соответствующих степенях x), что и в левой части.

В тождествах часто вместо знака $=$ пишут: $\equiv$.

Докажем вторую часть теоремы.

Пусть

$$f(x) = g(x)q(x) + r(x) = g(x)q_1(x) + r_1(x),$$

где степень $r(x)$ меньше степени $g(x)$ и степень $r_1(x)$ меньше степени $g(x)$. Имеем отсюда:

$$g(x)[q(x) - q_1(x)] = r_1(x) - r(x);$$

степень правой части меньше m, степень же левой больше или равна m, если только $q(x) - q_1(x) \neq 0$; но степени обеих частей равенства должны совпадать; следовательно:

$$q(x) - q_1(x) \equiv 0; \qquad q(x) \equiv q_1(x),$$

а отсюда $r(x) \equiv r_1(x)$, что и требовалось доказать.

Процесс, посредством которого мы находим $q(x)$ и $r(x)$, есть не что иное, как обычное деление функции $f(x)$ на $g(x)$; $q(x)$ — *неполное частное*, $r(x)$ — *остаток*. Если $r(x) \equiv 0$, то говорят, что $f(x)$ «делится» на $g(x)$; в этом случае $q(x)$ — *полное частное*; $f(x) = g(x)q(x)$; $\dfrac{f(x)}{g(x)} = q(x)$; $g(x)$ есть *делитель* функции $f(x)$.

Фактически деление ц. р. функций производится по известному из элементарной алгебры правилу деления многочленов, расположенных по убывающим степеням буквы x, т. е. по правилу, аналогичному правилу деления целых чисел.

Упражнения

65) $x^4 - 8x^3 - 11x^2 + 3x - 2$ разделить на $3x^2 - 2x + 1$.
Отв. Частное: $\dfrac{1}{3}x^2 - \dfrac{27}{9}x - \dfrac{146}{7}$; остаток: $-\dfrac{145}{27}x + \dfrac{92}{27}$.
66) $(1+i)x^3 + ix^2 + 2x - 1$ разделить на $x^2 + (2-i)x + 1$.
Отв. Частное: $(1+i)x - 3$; остаток: $(7-4i)x + 2$.

§ 48. Теоремы о делимости. Для сокращения мы напишем $f, \varphi, \ldots$ вместо $f(x), \varphi(x), \ldots$

I. *Если целая рациональная функция F делится на f, а f делится на φ, то и F делится на φ.*

Доказательство. По условию $F = ff_1$, $f = \varphi\varphi_1$, следовательно, $F\varphi \cdot (\varphi_1 f_1)$, что и требовалось доказать.

II. *Если F делится на f и G — любая целая рациональная функция, то и FG делится на f.*

Доказательство. По условию $F = ff_1$, следовательно, $FG = f \cdot (f_1 G)$, что и требовалось доказать.

III. *Если F и G делятся на f, то и $F \pm G$ делится на f.*

Доказательство. $F = ff_1$, $G = fg_1$, следовательно, $F \pm G = f \cdot (f_1 \pm g_1)$, что и требовалось доказать.

IV. *Если каждая из целых рациональных функций $F_1, F_2, \ldots, F_n$ делится на f, а $G_1, G_2, \ldots, G_n$ — любые целые рациональные функции, то и $F_1G_1 + F_2G_2 + \ldots + F_nG_n$ делится на f* (следствие из II, III).

V. *Целая рациональная функция делится на любое постоянное количество.*

Доказательство. Если $f = a_0x^n + a_1x^{n-1} + \ldots + a_n$, то

$$\frac{f}{c} = \frac{a_0}{c}x^n + \frac{a_1}{c}x^{n-1} + \ldots + \frac{a_n}{c}$$

тоже является ц. р. функцией.

VI. *Если F делится на f и $= \text{const}$, (постоянное количество), то F делится на cf.*

Доказательство. $F = ff_1 = (cf) \cdot \left(\dfrac{1}{c}f_1\right)$, $\dfrac{1}{c}f_1$ — ц.р. функция, следовательно, F делится на cf.

VII. *Всякая целая рациональная функция, делится на самое себя*, ибо $f = f \cdot 1$.

VIII. *Если f делится на g; а g делится на f, то $f = cg$, где $= \text{const}$.*

Доказательство. $f = gg_1$, $g = ff_1$, следовательно, $f = f \cdot (f_1 g_1)$, т. е. $f_1 g_1 = 1$; но степень произведения равна сумме степеней сомножителей, следовательно, и f_1 и g 0-й степени, т. е. $g_1 = \ = \text{const}$.

§ 49. Рассмотрим случай деления на линейную функцию, т. е. на функцию первой степени, вида: $x - \alpha$, где $\alpha = \text{const}$, в этом случае остаток будет нулевой степени, т. е. постоянным количеством r. Имеем:

$$f(x) = (x - \alpha)q(x) + r;$$

это равенство верно при всяком x; положим $x = \alpha$; тогда получим:

$$f(\alpha) = r.$$

$f(\alpha)$ есть значение функции $f(x)$ при $x = \alpha$.

Итак

$$f(x) = (x - \alpha)q(x) + f(\alpha),$$

или

$$\frac{f(x) - f(\alpha)}{x - \alpha} = q(x),$$

т. е. $f(x) - f(\alpha)$ делится на $x - \alpha$.

Здесь α — вообще произвольное количество: можно его считать переменным; напишем y вместо ?. Итак, получаем:

Теорема Декарта (Descartes). *Если $f(x)$ — любая целая рациональная функция, а y — произвольное число, то $f(x) - f(y)$ делится без остатка на $x - y$.*

Следствие. Уравнение $f(x) = 0$ тогда и только тогда имеет корень α, если $f(x)$ делится без остатка на $x - \alpha$.

Доказательство. Если α — корень, то $f(\alpha) = 0$ и по теореме Декарта $f(x)$ делится на $x - \alpha$. Обратно, пусть $f(x)$ делится на $x - \alpha$; по теореме Декарта $f(x) - f(\alpha)$ тоже делится на $x - \alpha$, т. е. и $f(\alpha)$ делится на $x - \alpha$, но так как $f(\alpha) = \text{const}$, т. е. 0-й степени, а $x - \alpha$ — первой степени, то может быть только $f(\alpha) = 0$.

§ 50. Алгебраическое уравнение. Формулы Вьета. Приравняв, нулю ц. р. функцию, мы получим алгебраическое уравнение. Главная задача первой части настоящего курса алгебры есть решение алгебраических уравнений, т. е. нахождение тех значений x («корней» уравнения), для которых ц. р. функция обращается в нуль. Но возникает вопрос: для всякого ли уравнения существуют корни? Ответ, и притом утвердительный, на этот вопрос дает основная теорема алгебры, которую мы докажем в следующей главе. Теперь же, приняв заранее известной эту теорему, выведем дальнейшие следствия из теоремы Декарта [18]

Пусть $f(x) = 0$ данное уравнение n-й степени: по основной теореме оно имеет корень; обозначим его через x_1, тогда по § 49: $f(x) = (x - x_1)f_1(x)$, где $f_1(x)$ тоже ц. р. функция; следовательно, уравнение $f_1(x) = 0$ тоже имеет корень; обозначим его через x_2; тогда $f_1(x) = (x - x_2)f_2(x)$, следовательно, $f(x) = (x - x_1)(x - x_2)f_2(x)$,

[18] Мы только не должны при доказательстве основной теоремы опираться на выводимые сейчас из нее следствия.

и $f_2(x)$ тоже ц. р. функция; обозначим через x_3 корень уравнения $f_2(x) = 0$; тогда подобным же образом найдем: $f(x) = (x - x_1)(x - x_2)(x - x_3)f_3(x)$ и т. д.; степени функций $f, f_1, f_2, \ldots$ последовательно уменьшаются на единицу: значит, после n таких шагов мы дойдем до функции f_n, которая равна const, а именно — высшему коэфициенту a_0 функции $f(x)$. [Это легко найдем, сравнив коэфициенты при x^n в обеих частях равенства (1)]. Таким образом получаем:

$$f(x) = a_0(x - x_1)(x - x_2)\cdots(x - x_n), \tag{1}$$

т. е. всякая ц. р. функция n-й степени представляется в виде произведения n линейных множителей; эти множители могут и не быть все различными; в общем случае мы получаем:

$$f(x) = a_0(x - a)^\alpha(x - b)^\beta(c - c)^\gamma\cdots, \tag{1a}$$

где $a, b, c, \ldots$ — все различны, а $\alpha, \beta, \gamma, \ldots$ — целые неотрицательные числа.

Очевидно, что при $x = a, b, c, \ldots$ $f(x)$ обращается в нуль т. е. $a, b, c, \ldots$ — корни уравнения $f(x) = 0$; число их меньше или равно n. Но обычно принимают, что всякое уравнение n-степени имеет n корней: именно, корень a считается α раз и называется α-кратным корнем; подобно же b — β-кратный корень, c — γ-кратный и т. д. Итак:

Теорема. *Всякое алгебраическое уравнение n-й степени имеет n различных или равных корней, или всякая целая рациональная функция n-й степени разлагается на n линейных множителей; это разложение возможно только единственным образом.*

Докажем последнюю часть теоремы; пусть имеем два разложения:

$$\begin{aligned} f(x) &= a_0(x - x_1)(x - x_2)\cdots(x - x_n) = \\ &= a_0'(x - x_1')(x - x_2')\cdots(x - x_n'); \end{aligned}$$

во-первых, $a_0 = a_0'$ ибо это коэфициент при x^n в обеих частях. Далее, левая часть равна нулю при $x = x_1$, т. е. и в правой части при $x = x_1$ один из сомножителей должен обращаться в нуль; пусть это будет $x - x_1'$; следовательно, $x_1' = x_2$, и на $x - x_1$ можно обе части равенства сократить; теперь таким же образом докажем, что, например, $x_2' = x_2$, и т. д.; при этом, если, скажем, $x_2 = x_1$, то и $x_2' = x_1' = x_1$, т. е. каждый из линейных сомножителей встречается в обеих частях одинаковое число раз, следовательно, оба разложения тождественны.

Теорема. *Если уравнение n-й степени имеет больше чем n различных корней, то все его коэфициенты, равны нулю, т. е. уравнение обращается в тождество.*

Доказательство. Пусть

$$f(x) = (x - x_1)(x - x_2)\cdots(x - x_n) = 0$$

имеет $n + 1$ различных корней: $x_1, x_2, ..., x_n, x_{n+1}$; имеем:

$$a_0(x_{n+1} - x_1)(x_{n+1} - x_2)\cdots(x_{n+1} - x_n) = 0;$$

но ни один из сомножителей $x_{n+1} - x_\lambda$ не равен нулю; следовательно, a_0, и уравнение не n-й, а $(n - 1)$-й степени; но теперь мы также докажем, что $a_1 = 0$, и т. д.

Следствие. Если две ц. р. функции степеней меньших или равных n равны друг другу больше чем при n различных значениях x, то они тождественно равны друг другу, т. е. коэфициенты при одинаковых степенях x у них одинаковы.

Доказательство. Если $f(x)$ и $g(x)$ — две такие ц. р. функции, то уравнение $f(x) - g(x) = 0$ степени меньшей или равной n имеет больше чем n различных корней, т. е. все его коэфициенты равны нулю, и значит коэфициенты в $f(x)$ те же, что и в $g(x)$.

Перемножим линейные функции в правой части формулы (1) и сравним коэфициенты при одинаковых степенях x в обеих частях (1); получим:

$$\begin{aligned}
&a_1 = -a_0(x_1 + x_2 + \ldots + x_n),\\
&a_2 = a_0(x_1x_2 + x_1x_3 + \ldots + x_1x_n + x_2x_3 + \ldots + x_{n-1}x_n),\\
&a_3 = -a_0(x_1x_2x_3 + x_1x_2x_4 + \ldots + x_{n-2}x_{n-1}x_n),\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\
&a_n = (-1)^n \cdot a_0 \cdot x_1x_2\cdots x_n,
\end{aligned}$$

или

$$x_1 + x_2 + \ldots + x_n = -\frac{a_1}{a_0}; \qquad \sum x_\alpha x_\beta = +\frac{a_2}{a_0},$$
$$\sum x_\alpha x_\beta x_\gamma = -\frac{a_3}{a_0}; \quad \ldots\ , \quad x_1x_2\cdots x_n = (-1)^n\,\frac{a_n}{a_0}.$$

Это так называемые *формулы Вьета* (Viète); они выражают зависимость между корнями и коэфициентами алгебраического уравнения и дают возможность составить уравнение по данным его корням.

Пример 1. Составить уравнение четвертой степени с корнями $3, -2, 1+2i, 1-2i$.

Мы принимаем $a_0 = 1$ и находим по формулам Вьета :

$$\begin{aligned}
a_1 &= -(3 - 2 + 1 - 2i + 1 - 2i) = -3,\\
a_2 &= 3\cdot(-2) + 3(1+2i) + 3\cdot(1-2i) + (-2)\cdot(1+2i) +\\
&\qquad + (-2)\cdot(1-2i) + (1+2i)(1-2i) = 1,\\
a_3 &= -[3\cdot(-2)\cdot(1+2i) + 3\cdot(-2)\cdot(1-2i) + 3(1+2i)(1-2i) +\\
&\qquad + (-2)(1+2i)(1-2i) = +7,\\
a_4 &= 3\cdot(-2)\cdot(1+2i)(1-2i) = -30;
\end{aligned}$$

следовательно, искомое уравнение имеет вид:

$$x^4 - 3x^3 + x^2 + 7x - 30 = 0.$$

Пример 2. Составить уравнение пятой степени, которое имело бы тройной корень -2 и двойной корень 1.

Здесь требуется при составлении коэфициентов корень 2 считать три раза, а корень 1 — два раза. Берем опять $a_0 = 1$; находим:

$$\begin{aligned}
a_1 &= -(-2 - 2 - 2 + 1 + 1) = 4,\\
a_2 &= (-2)^2 + (-2)^2 - 2\cdot 1 = \cdot 1 + (-2)^2 - 2\cdot 1 - 2\cdot 1 - 2\cdot 1 + 1\cdot 1 = 1,\\
a_3 &= -(-8 + 4 + 4 + 4 + 4 - 2 + 4 + 4 - 2 - 2) = -10,\\
a_4 &= -8 - 8 + 4 + 4 + 4 = -4,\\
a_5 &= -(-8) = 8;
\end{aligned}$$

следовательно, искомое уравнение имеет вид:

$$x^5 + 4x^4 + x^3 - 10x^2 - 4x + 8 = 0.$$

§ 51. Способ Горнера деления на линейную функцию. Укажем еще способ Горнера (Hörner) деления ц. р. функции на линейную функцию вида $x - \alpha$. Пусть

$$a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \ldots + a_n =$$
$$= (x - \alpha)(b_0x^{n-1} + b_1x^{n-2} + \ldots + b_{n-1}) + r;$$

сравнивая коэфициенты при одинаковых степенях x, найдем:

$$\left.\begin{array}{l} a_0 = b_0 \\ a_1 = -\alpha b_0 + b_1, \\ a_2 = -\alpha b_1 + b_2, \\ \ldots\ldots\ldots\ldots \\ a_n = -\alpha b_{n-1} + r \end{array}\right\} \quad \text{отсюда} \quad \begin{array}{l} b_0 = a_0, \\ b_1 = \alpha a_0 + a_1, \\ b_2 = \alpha b_1 + a_2, \\ \ldots\ldots\ldots\ldots \\ r = \alpha b_{n-1} + a_n, \end{array}$$

т. е. каждый последующий коэфициент b_λ, получается умножением предыдущего на α и прибавлением соответствующего коэфициента $a - \lambda$; таким же путем из b_{n-1} получается остаток r.

Пример 1. $f(x) = 5x^4 - 2x^3 + 4x^2 + 2x - 3$ разделить на $x - 2$.

Составляем таблицу:

	5	−2	4	2	−3
2	5	8	20	42	81

;

следовательно, частное: $5x^3 + 8x^2 + 20x + 42$; остаток: $81 = f(2)$.

Пример 2. $f(x) = 3x^6 - 5x^4 + 2x^3 - x + 4$ разделить на $x + 1$.

Здесь $\alpha = -1$.

Имеем:

	3	0	−5	2	0	−1	4
−1	3	−3	−2	4	−4	3	1

,

т. е. $f(x) = (x + 1)(3x^5 - 3x^4 - 2x^3 + 4x^2 - 4x + 3) + 1$; здесь $f(-1) = 1$.

Упражнения

67) $f(x) = x^3 - 4x^2 + 8x - 1$ разделить на $x + 4$.

Отв. $f(x) = (x + 4)(x^2 = 8x + 40) - 161$.

68) $f(x) = x^4 + 12x^3 + 54x^2 + 108x + 81$ разделить на $x + 3$.

Отв. $f(x) = (x + 3)(x^3 + 9x^2 + 27x + 27)$.

69) $x^7 - 1$ разделить на $x - 1$.

Отв. $x^7 - 1 = (x - 1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$.

70) $f(x) = x^8 - 4x^7 + 2x^5 - x^2 + 4x + 1$; вычислить $f(3)$.

Отв. -1697.

71) $f(x) = x^4 - 2ax^3 + 4a^2x^2 + 3a^3x - -2a^4$; вычислить $f(a)$.

Отв. $4a^4$.

§ 52. Алгорифм Эвклида. Пусть R и R_1 — две ц. р. функции, и пусть степень R больше или равна степени R_1; делим R на R, пусть частное равно Q_1 остаток равен R_2; степень R_2 меньше степени R_1. Делим R_1 на R_2 и обозначим частное через Q_2, а остаток через R_3, и т. д.; степень R_1 больше степени R_2, больше степени R_3, больше ...; следовательно, этот процесс должен когда-нибудь окончиться, т. е. некоторый остаток R_{m+1} должен стать равным нулю. Получаем, таким образом, ряд равенств:

$$\begin{aligned} R &= Q_1R_1 + R_2 \\ R_1 &= Q_2R_2, \\ R_2 &= Q_3R_3 + R_4, \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ R_{m-2} &= Q_{m-1}R_{m-1} + R_m, \\ R_{m-1} &= Q_mR_m \end{aligned} \tag{2}$$

Отсюда заключаем: если φ — общий делитель функций R и R_1, то первое равенство (2) показывает, что R_2 делится на φ, второе равенство, — что R_3 делится на φ и т. д., наконец, предпоследнее, — что R_m делится на φ; значит R_m делится на все общие делители функций R и R_1. Обратно, если R_m делится на φ, то последнее равенство говорит, что R_{m-1} делится на φ и т. д., наконец, и R и R_1 делятся на φ. В частности и R и R_1 делятся на R_m; R_m есть *общий наибольший* делитель функций R и R_1; мы его обозначим: $R_m = D(R, R_1)$; он — общий делитель наивысшей степени, но определен он не однозначно: если c — любое постоянное количество, то вместо R_m можно взять: cR_m [19]; c можно выбрать так, чтобы, например, высший коэфициент в cR_m был равен единице. Если $R_m = \text{const}$, то функции R и R_1 не имеют иных общих делителей, кроме постоянных количеств; в этом случае они называются *взаимно простыми*, и можно взять $D(R, R_1) = 1$.

Этот способ нахождения R_m принадлежит Эвклиду и называется «*алгорифмом Эвклида*» [20]. Итак:

Теорема. *Среди общих делителей двух целых рациональных функций f и g существует общий делитель наивысшей степени, определенный с точностью до постоянного множителя и находимый посредством последовательных делений; он делится на всякий другой общий делитель функций f и g и называется общим наибольшим делителем этих функций.*

Из предпоследнего равенства (2) имеем:

$$R_m = R_{m-2} - Q_{m-1}R_{m-1},$$

из предыдущего:

$$R_{m-1} = R_{m-3} - Q_{m-2}R_{m-2},$$

далее

$$R_{m-2} = R_{m-4} - Q_{m-3}R_{m-3}$$

[19] См. § 48, VI.

[20] Словом «алгорифм» в математике обозначают цепь вычислений, в которой каждое последующее звено находится по тем же правилам, как и предыдущее; это слово — исковерканное имя арабского математика Альховаризми, жившего в IX в. нашей эры.

и т. д.; подставляя последовательно $R_{m-1}, R_{m-2}, \ldots$ в первое из написанных равенств, найдем в конце концов:

$$R_m = RX + R_1 Y,$$

где X и Y — некоторые ц. р. функции, т. е.

Теорема. *Если f, g — целые рациональные функции и $D(f,g) = \varphi$, то можно найти такие целые рациональные функции f_1, g_1, что*

$$ff_1 + gg_1 \equiv \varphi. \tag{3}$$

В частности, если f и g — взаимно простые, получим:

$$ff_1 + gg_1. \tag{3a}$$

Упражнения

72) Найти $D(3x^3 - 22x^2 + 30x + 27, x^2 - 8x + 15)$.

Отв. $x - 3$.

73) Найти $D(36x^4 - 54x^3 + 78x^2 + 18x - 30, 18x^3 - 9x^2 + 18x + 45)$.

Отв. $2x^2 - 3x + 5$.

74) Найти функции f_1 и g_1 удовлетворяющие равенству: $ff_1 + gg_1 = 1$, где $f = x^4 + 1$, $g = x^3 - 1$.

Отв. $f_1 = \frac{1}{2}(x^2 - x + 1)$, $g_1 = -\frac{1}{2}(x^3 - x^2 + x + 1)$.

75) $f(x) = x^3 + x + 2$, $g = x^3 - x$; найти $D(f,g)$ и функции f_1 и g_1 так, чтобы $ff_1 + gg_1 = D(f,g)$.

Отв. $D(f,g) = x + 1$, $f_1 = \frac{1}{2}$, $g_1 = -\frac{1}{2}$.

§ 53. Теоремы о взаимно простых функциях.

Теорема 1. *Если f, g, φ целые рациональные функции и fg делится на φ, тогда как g и φ — взаимно простые, то f делится на φ.*

Доказательство. Имеем: $gg_1 + \varphi\varphi_1 = 1$ (см. конец § 52); умножаем на f: $(fg)\cdot g_1 + \varphi\cdot(f\varphi_1) = f$; так как левая часть делится на φ, то и правая, т. е. f, тоже делится на φ.

Теорема 2. *Если целая рациональная функция f взаимно простая порознь с φ и ψ, то f взаимно простая и с произведением $\varphi\psi$.*

Доказательство. По условию $ff_1 + \varphi\varphi_1 = 1$ (§ 52); умножаем ψ: $f\cdot(f_1\psi) + (\varphi\psi)\cdot\varphi_1 = \psi$; отсюда видно, что всякий общий делитель f и $\varphi\psi$ есть также делитель ψ; но $D(f,\psi) = 1$, следовательно, и $D(f,\varphi\psi) = 1$.

Отсюда непосредственно вытекает:

Следствие I. Если каждая из ц. р. функций $f_1, f_2, \ldots, f_k$ взаимно простая с каждой из ц. р. функций $g_1, g_2, \ldots, g_l$, то и произведение $f_1, f_2, \ldots, f_k$ взаимно просто с произведением $g_1 g_2 \cdots g_l$.

При $f_1 = f_2 = \ldots = f_k$ и $g_1 = g_2 = \ldots = g_l$ получаем:

Следствие II. Если ц. р. функции f и g — взаимно простые, то и f^k и g^l тоже взаимно простые.

При $a \neq b$ функции $x-a$ и $x-b$ — взаимно простые; поэтому:

Следствие III. Если $a \neq b$, то $(x-a)^k$ и $(x-b)^l$ — взаимно простые функции.

Теорема 3. *Если f, φ, ψ — целые рациональные функции, $D(\varphi,\psi)=1$ и f делится порознь на φ и ψ, то f делится и на произведение $\varphi\psi$.*

Доказательство. По условию $\dfrac{f}{\varphi}=g$ — целая функция; $f=g\varphi$ делится на ψ, но $D(\varphi,\psi)=1$, следовательно, g делится на ψ, т. е. $\dfrac{g}{\psi}=\dfrac{f}{\varphi\psi}$ — целая функция, что и требовалось доказать.

Эта теорема непосредственно обобщается:

Следствие. Если ц. р. функции $\varphi_1,\varphi_2,\ldots,\varphi_m$ попарно взаимно простые и ц. р. функция f делится порознь на $\varphi_1,\varphi_2,\ldots,\varphi_m$, то f делится и на произведение $\varphi_1\varphi_2\cdots\varphi_m$.

§ 54. Производные. Ряд Тэйлора. Пусть

$$f(x)=a_0x^n+a_1x^{n-1}+a_2x^{n-2}+\ldots+a_{n-1}x+a_n$$

данная ц. р. функция. Подставим $x+h$ вместо x и расположим $f(x+h)$ по степеням h:

$$\begin{aligned}
f(x+h) &= a_0(x+h)^n+a_1(x+h)^{n-1}+a_2(x+h)^{n-2}+\ldots+a_{n-1}(x+h)+a_n= \\
&= a_0\Big[x^n+nx^{n-1}h+\frac{n(n-1)}{2!}x^{n-2}h^2+\frac{n(n-1)(n-2)}{3!}x^{n-3}h^3+ \\
&\qquad +\ldots+\binom{n}{n-1}xh^{n-1}+\binom{n}{n}h^n\Big]+ \\
&+ a_1\Big[x^{n-1}+(n-1)x^{n-2}h+\frac{(n-1)(n-2)}{2!}x^{n-3}h^2+ \\
&\qquad +\frac{(n-1)(n-2)(n-3)}{3!}x^{n-4}h^3+\ldots+\binom{n-1}{n-1}h^{n-1}\Big]+ \\
&+ a_2\Big[x^{n-2}+(n-2)x^{n-3}h+\frac{(n-2)(n-3)}{2!}x^{n-4}h^2+ \\
&\qquad +\frac{(n-2)(n-3)(n-4)}{3!}x^{n-4}h^3+\ldots\Big]+ \\
&+ \ldots+a_{n-1}(x+h)+a_n.
\end{aligned}$$

Обозначим:

$$\begin{aligned}
f'(x) &= na_0x^{n-1}+(n-1)a_1x^{n-2}+\ldots+1\cdot a_{n-1}, \\
f''(x) &= n(n-1)x^{n-2}+(n-1)(n-2)x^{n-3}+\ldots+1\cdot2\cdot a_{n-2} \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
f^{(n-1)}(x) &= n(n-1)(n-2)\cdots3\cdot2\cdot1\cdot a_0x+(n-1)(n-2)\cdots2\cdot1, \\
f^{(n)}(x) &= n(n-1)(n-2)\cdots2\cdot1\cdot1=n!a_0.
\end{aligned}$$

Тогда

$$f(x+h)=f(x)+hf'(x)+\frac{h^2}{2!}f''(x)+\frac{h^3}{3!}f'''(x)+\ldots+\frac{h^n}{n!}\cdot f^{(n)}(x). \qquad (4)$$

Это — ряд Тэйлора (Taylor). Функции $f'(x)$, $f''(x)$, ..., $f^{(n)}(x)$ называются *первой, второй* и т. д. n-*й производными* от функции $f(x)$ [21].

Мы видим, что для того, чтобы построить первую производную для ц. р. функции $f(x)$, нужно каждый член в $f(x)$ помножить на показатель x в этом члене и после этого показатель x уменьшить на единицу, таким образом свободный член $a_n = a_n x^0$ умножается на нуль.

Вторая производная для $f(x)$ есть первая производная для $f'(x)$; третья производная для $f(x)$ — вторая для $f'(x)$ и первая для $f''(x)$ и т. д. Производная постоянного количества принимается равной нулю. Для ц. р. функции n-й степени первые n производных не равны нулю, последующие же все считаются равными нулю.

Ряд Тэйлора можно вывести короче, применяя знак $\sum$ для суммы:

$$\begin{aligned} f(x) &= \sum_{\varkappa=0}^{n} a_\varkappa (x+h)^{n-\varkappa} = \sum_{\varkappa=0}^{n} \left(a_\varkappa \sum_{\lambda=0}^{n-\varkappa} \binom{n-\lambda}{\lambda} x^{n-\varkappa-\lambda} h^\lambda \right) = \\ &= \sum_{\varkappa=0}^{n} \sum_{\lambda=0}^{n-\varkappa} \binom{n-\lambda}{\lambda} a_\varkappa x^{n-\varkappa-\lambda} h^\lambda; \end{aligned}$$

здесь $0 \le \varkappa \le n$, $0 \le \lambda \le n-\varkappa$, т.е. $0 \le \varkappa + \lambda \le n$, и при данном $\lambda \ge 0$ и $\le n$ должно быть: $0 \le \varkappa \le n-\lambda$, т. е. можно переменить порядок суммирования следующим образом:

$$\begin{aligned} f(x+h) &= \sum_{\varkappa=0}^{n} \sum_{\lambda=0}^{n-\varkappa} \binom{n-\lambda}{\lambda} a_\varkappa x^{n-\varkappa-\lambda} h^\lambda = \\ &= \sum_{\lambda=0}^{n} \left(\frac{h^\lambda}{\lambda!} \sum_{\varkappa=0}^{n-\lambda} (n-\varkappa)(n-\varkappa-1)\cdots(n-\varkappa-\lambda+1) a_\varkappa x^{n-\varkappa-\lambda} \right). \end{aligned}$$

Введем $f^{(\lambda)}(x)$ из равенства

$$\sum_{\varkappa=0}^{n-\lambda} (n-\varkappa)(n-\varkappa-1)\cdots(n-\varkappa-\lambda+1) a_\varkappa x^{n-\varkappa-\lambda} = f^{(\lambda)}(x);$$

как легко видеть, $f^{(\lambda)}(x)$ есть не что иное, как λ-я производная для $f(x)$; тогда

$$f(x+h) = \sum_{\lambda=0}^{n} \frac{h^n}{\lambda!} f^{(\lambda)}(x);$$

это и есть ряд Тэйлора, если мы еще под символом $f^{(0)}(x)$ будем подразумевать самое функцию $f(x)$.

[21] Таким образом мы определяем здесь производные ц. р. функции чисто формально; это мы делаем по той причине, что в алгебре как для коэфициентов наших функций, так и для переменного x допускаются и комплексные значения, тогда как в обычном диференциальном исчислении и независимые переменные, и функции рассматриваются исключительно в области вещественных чисел. Позже (в § 66) мы увидим, что это формальное определение в действительности совпадает с тем, которое обычно дается для производной в диференциальном исчислении.

Переменим в (4) обозначения: напишем a вместо x и x вместо $x+h$; тогда h заменится через $x-a$, и мы получим:

$$f(x)=f(a)+(x-a)f'(a)+\frac{(x-a)^2}{2!}f''(a)+\ldots+\frac{(x-a)^n}{n!}f^{(n)}(a). \qquad (5)$$

Это *ряд Маклорена* (Maclaurin); он дает разложение данной ц. р. функции по степеням $x-a$, где a — любое данное число.

При $a=0$ получаем специальный ряд Маклорена:

$$f(x)=f(0)+xf'(0)+\frac{x^2}{2!}f''(0)+\ldots+\frac{x^n}{n!}f^{(n)}(0); \qquad (6)$$

отсюда заключаем:

$$a_n=f(0),\quad a_{n-1}=f'(0),\quad a_{n-2}=\frac{1}{2!}f''(0),\quad \ldots\ ,$$
$$a_1=\frac{1}{(n-1)!}f^{(n-1)}(0),\quad a_0=\frac{1}{n!}f^{(n)}(0).$$

Упражнения

Найти производные всех порядков и написать ряд Тэйлора для функций:
76) $x^5-8x^4+3x^3+4x^2-x-6$.
77) $3x^4-4x^2+2x-3$.
78) $x^7+x^6+x^5+x^4$.
79) $x^4+4x^3+6x^2+4x+1$.

§ 55. Напишем формулу (5) в таком виде:

$$f(x)=f(a)+(x-a)\Big[f'(a)+\frac{x-a}{2!}f''(a)+$$
$$+\frac{(x-a)^2}{3!}f'''(a)+\ldots+\frac{(x-a)^{n-1}}{n!}f^{(n)}(a)\Big];$$

функцию в скобках обозначим через $\varphi(x)$; тогда

$$f(x)=f(a)=(x-a)\varphi(x),$$

отсюда видно (§ 47 и 49), что $\varphi(x)$ — частное, а $f(a)$ — остаток от деления $f(x)$ на $x-a$. Далее, имеем:

$$\varphi(x)=f'(a)=(x-a)\Big[\frac{1}{2}f''(a)+\frac{x-a}{2!}f''(a)+$$
$$+\frac{(x-a)^2}{3!}f'''(a)+\ldots+\frac{x-a}{3!}f'''(a)+\ldots\Big]$$

$$=f'(a)+(x-a)\psi(a),$$

если через $\psi(x)$ и здесь обозначим функцию в скобках; следовательно, $\psi(x)$ — частное, а $f(a)$ — остаток от деления $\varphi(x)$ на $x-a$, и т. д. Отсюда вытекает способ Горнера разложения $f(x)$ по степеням $x-a$: делим $f(x)$ на $x-a$; частное снова делим на $x-a$; частное опять делим на $x-a$ и т. д., пока не получим в частном постоянное количество; остатки от этих делений и последнее частное и являются коэфициентами в (5), т. е.

$$f(a),\quad f'(a),\quad \frac{1}{2!}f''(a),\quad \frac{1}{3!}f'''(a),\ \ldots$$

Деления на $x-a$ производятся по способу Горнера (§ 51).

Пример 1. $f(x)=x^4-5x^3+x-4$ разложить по степеням $x+2$.

Здесь $a=-2$.

Составляем таблицу:

	3	-5	0	1	-4
-2	3	-11	22	-43	$\mathbf{82}=f(-2)$
-2	3	-17	56	$-\mathbf{155}=f'(-2)$	
-2	3	-23	$\mathbf{102}=\frac{1}{2!}f''(-3)$		
-2	3	$-\mathbf{29}=\frac{1}{3!}f'''(-2)$			
	$\mathbf{3}=\frac{1}{4!}f^{IV}(-2)$				

Мы на одной и той же таблице совершаем деление несколько раз подряд, ибо числа каждой строки кроме последнего числа — коэфициенты частного, последнее же число — остаток.

Получаем:

$$f(x)=82-155(x+2)+102(x+2)^2-29(x+2)^3+3(x+2)^4.$$

Пример 2. $f(x)=x^5+x^4+x^3+x^2+x+1$ разложить по степеням $x-1$.

	1	1	1	1	1	1
1	1	2	3	4	5	**6**
1	1	3	6	10	**15**	
1	1	4	10	**20**		
1	1	5	**15**			
1	1	**6**				
	1					

Получаем:

$$f(x)=6+15(x-1)+20(x-1)^2+15(x-1)^3+6(x-1)^4+(x-1)^5.$$

Упражнения

80) x^3+5x^2-7x-3 разложить по степеням $x-4$.
Отв. $113+81(x-4)+17(x-4)^2+(x-4)^3$.
81) x^7 разложить по степеням $x+1$.
Отв. $-1+7(x+1)-21(x+1)^2+35(x+1)^3-35(x+1)^4+21(x+1)^5-7(x+1)^6+(x+1)^7$.
82) $x^4+4x^3+6x^2+4x+1$ разложить по степеням $x+1$.
Отв. $(x+1)^4$.
83) $4x^4-13x^3+17x^2-10x+2$ разложить по степеням $x-1$.
Отв. $(x-1)+2(x-1)^2+3(x-1)^3+4(x-1)^4$.

§ 56. Теорема. *Если $f(x)$ и $g(x)$ — целые рациональные функции и $F(x)=f(x)\cdot g(x)$, то*

$$F'(x)=f(x)g'(x)+g(x)f'(x). \tag{7}$$

Доказательство [22]. Мы будем применять сокращенное обозначение сумм. Пусть

$$f(x)=\sum_{k=0}^{n}a_kx^{n-k},\qquad g(x)=\sum_{k=0}^{m}b_kx^{m-k},\qquad F(x)=\sum_{k=0}^{m+n}c_kx^{m+n-k};$$

здесь

$$c_k=\sum_{\lambda=0}^{k}a_\lambda b_{k-\lambda}$$

(§ 46), причем при $k>n$ следует считать $a_\lambda=0$, а при $k-\lambda>m$, $b_{k-\lambda}=0$. Далее (по § 54):

$$F'(x)=\sum_{k=0}^{m+n}(m+n-k)c_kx^{m+n-k-1};$$

подставим значение для c_k:

$$F'(x)=\sum_{k=0}^{m+n}\sum_{\lambda=0}^{k}(m+n-k)a_\lambda b_{k-\lambda}x^{m+n-k-1};$$

здесь $0\le k\le\le m+n$; пусть $k=\lambda+\mu$, $\mu=k-\lambda$; мы можем давать для λ значения от 0 до n, а для μ от 0 до m независимо друг от друга, ибо тогда всегда $0\le\lambda+\mu\le n+m$, тогда как при $\lambda>n$ или при $\mu>m$ будет $a_\lambda=0$ или $b_\mu=0$.

Итак, получим:

$$F'(x)=\sum_{\lambda=0}^{n}\sum_{\mu=0}^{m}(m+n-\lambda-\mu)a_\lambda b_\mu x^{m+n-\lambda-\mu-1}.$$

[22] Эту теорему мы выводим чисто алгебраическим путем, основываясь на формальном определении производной (§ 54),

Разбив каждое слагаемое нашей двойной суммы на два, мы представим ее как сумму двух двойных сумм следующим образом:

$$\begin{aligned} F'(x) &= \sum_{\lambda}^{n}\sum_{\mu=0}^{m}(m-\mu)a_\lambda b_\mu x^{m+n-\lambda-\mu-1}+ \\ &+ \sum_{\lambda=0}^{n}\sum_{\mu=0}^{m}(n-\lambda)a_\lambda b_\mu x^{m+n-\lambda-\mu-1}. \end{aligned}$$

Берем первую сумму и преобразовываем ее следующим образом:

$$\sum_{\lambda=0}^{n}\sum_{\mu=0}^{m}(m-\mu)a_\lambda b_\mu x^{n-\lambda}x^{m-\mu-1} = \sum_{\lambda=0}^{n}a_\lambda x^{n-\lambda}\ \sum_{\mu=0}^{m}(m-\mu)b_\mu x^{m-\mu-1}x^{m-\mu-1} =$$
$$= \sum_{\lambda=0}^{n}a_\lambda x^{n-\lambda}\cdot\sum_{\mu=0}^{m}(m-\mu)b_\mu x^{m-\mu-1} = f(x)\cdot g'(x);$$

подобным же образом найдем, что вторая сумма равна $g(x)\cdot f'(x)$, и формула (7), таким образом, доказана.

Обобщение. Если $F = f_1 f_2 \cdots f_n$, где $f_1, f_2, \ldots, f_n$ — ц. р. функции от x, то

$$F' = f_2 f_3 \cdots f_n \cdot f_1' + f_1 f_3 \cdots f_n \cdot f_2' + \ldots + f_1 f_2 \cdots f_{n-1}\cdot f_n'. \tag{8}$$

Доказательство. Применим метод полной индукции: пусть для произведения n функций теорема верна. Имеем:

$$F = (f_1 f_2 \cdots f_{n-1})\cdot f_n; \qquad F' = (f_1 f_2 \cdots f_{n-1})'\cdot f_n + (f_1 f_2 \cdots f_{n-1})\cdot f_n';$$

но по предположению

$$(f_1 f_2 \cdots f_{n-1})'(f_2 f_3 \cdots f_{n-1})f_1' + (f_1 f_3 \cdots f_{n-1})f_2' + \ldots + (f_1 f_2 \cdots f_{n-2})f_{n-1}';$$

подставив это выражение, получим (8).

Частный случай:

$$F = (x-x_1)(x-x_2)\cdots(x-x_n);$$

по (8)

$$\begin{aligned} F' &= (x-x_2)(x-x_3)\cdots(x-x_n) + (x-x_1)(x-x_3)\cdots(x-x_n)+ \\ &+ \ldots + (x-x_1)(x-x_2)\cdots(x-x_{n-1}) = \\ &= F\cdot\left(\frac{1}{x-x_1}+\frac{1}{x-x_2}+\ldots+\frac{1}{x-x_n}\right). \end{aligned} \tag{9}$$

Отсюда

$$\frac{F'}{F} = \frac{1}{x-x_1}+\frac{1}{x-x_2}+\ldots+\frac{1}{x-x_n}; \tag{10}$$

это довольно важная формула.

Далее, имеем из (9):

$$F'(x_1) = (x_1 - x_2)(x_1 - x_3)\cdots(x_1 - x_n);$$

остальные члены обращаются в нуль.

Вообще

$$F'(x_\lambda) = (x_\lambda - x_1)(x_\lambda - x_2)\cdots(x_\lambda - x_{\lambda-1})(x_\lambda - x_{\lambda+1})\cdots(x_\lambda - x_n). \qquad (11)$$

Положив в (9) $x_1 = x_2 = \ldots = x_n$, получим из (9):

$$F' = n(x - x_1)^{n-1} \qquad (12)$$

при

$$F = (x - x_1)^n.$$

§ 57. Кратные корни. Пусть $x = x_1$ — α-кратный корень уравнения $f(x) = 0$; это значит (§ 50), что

$$f(x) = (x - x_1)^\alpha \cdot \varphi(x),$$

где $\varphi(x)$ — ц. р. функция, уже не делящаяся на $x - x_1$.

Отсюда по § 56 (7) и (12)

$$f'(x) = \alpha(x - x_1)^{\alpha-1} \cdot \varphi(x) + (x - x_1)^\alpha \cdot \varphi'(x),$$

или

$$f'(x) = (x - x_1)^{\alpha-1} \cdot [\alpha\varphi(x) + (x - x_1)\varphi'(x)],$$

причем выражение в скобках не делится без остатка на $x - x_1$; таким образом x_1 есть корень и уравнения $f'(x)$, при этом $(\alpha - 1)$-й кратности. Предыдущее применимо и к случаю $\alpha = 1$, т. е. *простой* корень (т. е., корень первой кратности) уравнения $f(x) = 0$ совсем не удовлетворяет уравнению $f'(x) = 0$. А отсюда следует: если x_1 — корень уравнения $f(x) = 0$ и $(\alpha - 1)$-кратный корень уравнения $f'(x)$, то x_1 есть α-кратный корень уравнения $f(x) = 0$; итак,

Теорема 1. *Необходимое и достаточное условие того, чтобы x_1 было α-кратным корнем уравнения $f(x) = 0$, состоит в следующем: x_1 должно быть $(\alpha-1)$-кратным корнем уравнения $f'(x) = 0$ и удовлетворять уравнению $f(x) = 0$.*

Если x_1 — α-кратный корень уравнения $f(x) = 0$ и, следовательно, $(\alpha - 1)$-кратный корень уравнения $f'(x) = 0$, то аналогичным образом заключаем, что x_1 — $(\alpha - 2)$-кратный корень уравнения $f''(x) = 0$ и т. д., простой корень уравнения $f^{(\alpha-1)}(x) = 0$ и, наконец, совсем не удовлетворяет уравнению $f^{(\alpha)}(x) = 0$.

Обратно, если x_1 удовлетворяет уравнениям

$$f(x) = 0, \quad f'(x) = 0, \ \ldots\ , \ f^{(\alpha-1)}(x) = 0,$$

но не удовлетворяет уравнению $f^{(\alpha)}(x) = 0$, то последовательно заключаем, что x_1 — простой корень для $f^{(\alpha-1)}(x) = 0$, двойной — для $f^{(\alpha-2)}(x) = 0$ и т. д., наконец α-кратный — для $f(x) = 0$.

Итак,

Теорема 2. *Необходимое и достаточное условие того, чтобы x_1 было α-кратным корнем уравнения $f(x)=0$, состоит в следующем:*

$$f(x_1)=f'(x_1)=f''(x_1)=\ldots=f^{(\alpha-1)}(x_1)=0, \quad \text{но} \quad f^{(\alpha)}(x_1)\neq 0.$$

Это же легко вывести и из ряда Маклорена (5).

§ 58. Выделение кратных корней. Дано уравнение $f(x)=0$. Его левая часть раскладывается на линейные множители (§ 50). Обозначим через X_1 произведение линейных множителей, соответствующих простым корням уравнения $f(x)=0$, через X_2 — произведение линейных множителей, соответствующих двойным корням, взятых по одному разу; через X_3 — произведение линейных множителей, соответствующих тройным корням, и т. д. При этом, если, например, двойных корней уравнение не имеет, то мы считаем $X_2=1$ и т. д. Пусть, например, уравнение не имеет корней выше 5-й кратности (мы берем для простоты этот частный случай, хотя рассуждения наши — общие). Тогда

$$f(x)=a_0X_1X_2^2X_3^3X_4^4X_5^5,$$

где a_0 — высший коэфициент в $f(x)$.

Пример.

$$f(x)=(x-3)(x-4)^4(x+1)^2(x+2)^4(x-1-2i)(x-1+2i)\left(x-\frac{1}{2}\right)^2;$$

здесь

$$a_0=1, \quad X_1=(x-3)(x-1-2i)(x-1+2i), \quad X_2(x+1)\left(x-\frac{1}{2}\right),$$

$$X_3=1, \quad X_4=(x-4)(x+2).$$

По теореме 1 § 57 имеем:

$$D=\mathbf{D}(f,f')=X_2X_3^2X_4^3X_5^4$$

(§ 52).

Далее, подобным же образом

$$D_1=\mathbf{D}(D,D')=X_3X_4^2X_5^3,$$
$$D_2=\mathbf{D}(D_1,D_1')=X_4X_5^2,$$
$$D_3=\mathbf{D}(D_2,D_2')=X_5;$$

функции D, D_1, D_2, D_3 находятся посредством делений (§ 52),

Далее, делениями же находим:

$$E_1=\frac{f(x)}{D}=a_0X_1X_2X_3X_4X_5,$$
$$E_2=\frac{D}{D_1}=X_2X_3X_4X_5,$$
$$E_3=\frac{D_1}{D_2}=X_3X_4X_5,$$
$$E_4=\frac{D_2}{D_3}=X_4X_5,$$
$$E_5=D_3=X_5;$$

наконец,

$$\frac{E_1}{E_2} = a_0 X_1, \quad \frac{E_2}{E_3}, \quad \frac{E_3}{E_4} = X_3, \quad \frac{E_4}{E_5} = X_4, \quad E_5 = X_5.$$

Таким образом, если дано уравнение $f(x) = 0$, причем разложение f на линейные множители неизвестно, то мы можем путем последовательных делений найти функции $X_1, X_2, X_3, \ldots$ и наше уравнение заменить такими: $X_1 = 0$, $X_2 = 0$, $X_3 = 0$, …, каждое из которых имеет только простые (т. е. все различные) корни.

Пример.

$$f(x) = x^5 - 3x^4 + 4x^3 - 4x^2 + 3x - 1 = 0.$$

Имеем здесь:

$$f'(x) = 5x^4 - 12x^3 + 12x^2 - 8x + 3.$$

При делении $f(x)$ на $f'(x)$ предварительно умножим $f(x)$ на 5, чтобы избежать дробей. Производим [23] деление:

$$\begin{array}{r|l}
5x^5 - 15x^4 + 20x^3 - 20x^2 + 15x - 5 & 5x^4 - 12x^3 + 12x^2 - 8x + 3 \\
\underline{5x^5 - 12x^4 + 12x^3 - 8x^2 + 3x} & \underline{x - 3} \\
-3x^4 + 8x^3 - 12x^2 + 12x - 5 & \\
-15x^4 + 40x^3 - 60x^2 + 60x - 25 & \\
\underline{-15x^4 + 36x^3 - 36x^2 + 24x - 9} & \\
-4x^3 - 24x^2 + 36x - 16 &
\end{array}$$

$$\begin{array}{r|l}
5x^4 - 12x^3 + 12x^2 - 8x + 3 & x^3 - 6x^2 + 9x - 4 \\
\underline{5x^4 - 30x^3 + 45x^2 - 20x} & \underline{5x + 6} \\
18x^3 - 33x^2 + 12x + 3 & \\
6x^3 - 11x^2 + 4x + 1 & \\
\underline{6x^3 - 36x^2 + 54x - 24} & \\
25x^2 - 50x + 25 &
\end{array}$$

$$\begin{array}{r|l}
x^3 - 6x^2 + 9x - 4 & x^2 - 2x + 1 \\
\underline{x^3 - 2x^2 + x} & \underline{x - 1} \\
-4x^2 + 8x - 4 & \\
-x^2 + 2x - 1 & \\
\underline{x^2 - 2x + 1} &
\end{array}$$

Итак

$$D = x^2 - 2x + 1.$$

Далее

$$D' = 2x - 2 = 2(x - 1)$$

$$(x^2 - 2x + 1) : (x - 1) = x - 1;$$

следовательно, $D_1 = x - 1$, $D_1' = 1$, $D_2 = 1$, и здесь наш процесс прекращается.

[23] Так как при нахождении общего наибольшего делителя для нас важны остатки от делений, а не частные, то мы, чтобы избежать дробей, можем умножить получаемые в середине деления остатки на одно и то же число, или делить все члены остатка на общий постоянный множитель, если таковой имеется; от этого получаемые частные будут неверны, но нам это неважно; остатки же от делений получат постоянные множители, что тоже неважно. При делении же $f(x)$ на D, DD на D_1 и т. д. мы этого уже не имеем права делать, так как там для нас важны частные.

Далее, находим:

$$\begin{array}{l|l}
x^5-3x^4+4x^3-4x^2+3x-1 & x^2-2x+1 \\
\underline{x^5-2x^2+x^3} & \overline{x^3-x^2+x-1} \\
\quad -\ x^4+3x^3-4x^2 & \\
\quad \underline{-\ x^4+2x^3-\ x^2} & \\
\qquad x^3-3x^2+3x & \\
\qquad \underline{x^3-2x^2+\ x} & \\
\qquad\quad -\ x^2+2x-1 &
\end{array}$$

Итак

$$E_1=\frac{f(x)}{D}=x^3-x^2+x-1.$$

Далее

$$E_2=\frac{D}{D_1}=\frac{x^2-2x+1}{x-1}=x-1,$$
$$E_3=D_1=x-1.$$

Наконец

$$X_1=\frac{E_1}{E_2}=x^2+1,$$
$$X_2=\frac{E_2}{E_3}=1,$$
$$X_3=E_3=x-1.$$

Итак

$$f(x)=(x^2+1)(x-1)^3;$$

наше уравнение имеет два простых корня: $\pm i$ и один тройной $+1$.

Упражнения

Выделить кратные корни у уравнений:

84) $x^6-4x^4+16x^2+64=0$.

Отв. $(x^2+4)(x^2-4)^2$.

85) $x^4+4x^3-18x^2+20x-7=0$.

Отв. $(x+7)(x-1)^3$.

86) $x^4-2x^3-11x^2+12x+36=0$.

Отв. $(x-3)^2(x+2)^2$.

87) $x^5-x^4-14x^3-26x^2-19x-5=0$.

Отв. $(x-5)(x+1)^4$.

88) $x^5-3x^4+4x^3-4x^2+3x-1=0$.

Отв. $(x^2+1)(x-1)^3$.

89) $x^8+2x^7+x^6-3x^4-6x^3-5x^2-4x-2=0$.

Отв. $(x^3+x^2+x+1)^2(x^2-2)$.

90) $x^5-13x^4+67x^3-171x^2216x-108=0$.

Отв. $(x-2)^2(x-3)^3$.

91) $x^4-\frac{1}{2}+\frac{3}{16}=0$.

Отв. $\frac{1}{16}(2x-1)^2(4x62+4x+3)$.

92) Доказать, что двучленное уравнение, т. е. уравнение вида $x^n - a = 0$, не имеет кратных корней.

93) Найти условие, при котором уравнение $x^3 + px + q = 0$ имеет кратные корни.

Отв. Для этого должно быть $4p^3 + 27q^2 = 0$.

§ 59. Дробные рациональные функции. *Дробная рациональная функция* есть частное двух целых рациональных функций (ее числителя и знаменателя). Дробь называется *правильной*, если степень числителя меньше степени знаменателя; в противном случае дробь *неправильная*. Пусть дробь $\dfrac{f(x)}{g(x)}$ — неправильная; разделим числитель на знаменатель (§ 47):

$$f(x) = g(x)q(x) + r(x);$$

степень $r(x)$ меньше степени $g(x)$, отсюда

$$\frac{f(x)}{g(x)} = q(x) + \frac{r(x)}{g(x)},$$

при этом $q(x)$ и $r(x)$ определены однозначно. Итак:

Теорема. *Всякую неправильную дробь можно представить в виде суммы целой функции и правильной дроби; такое представление возможно только одним образом; оно называется выделением целой части из неправильной дроби.*

Из элементарной алгебры известны правила преобразования дробей и рациональных действий над ними; результат рациональных действий над дробными рациональными функциями всегда есть тоже рациональная функция (дробная или целая). Докажем еще следующую теорему.

Теорема. *Сумма правильных дробей есть тоже правильная дробь.*

Доказательство. Достаточно доказать эту теорему для двух правильных дробей, пусть $\dfrac{f_1}{g_1}$ и $\dfrac{f_2}{g_2}$ — две такие дроби; имеем:

$$\frac{f_1}{g_1} + \frac{f_2}{g_2} = \frac{f_1 g_2 + f_2 g_1}{g_1 g_2};$$

пусть степень $f_1 = m_1$, степень $f_2 = m_2$, степень $g_1 = n_1$, степень $g_2 = n_2$; тогда по условию $m_1 < n_1$, $m_2 < n_2$; по § 56 степень $g_1 g_2 = n_1 + n_2$, степень $f_1 g_2 = m_1 + n_2$, степень $f_2 g_1 = m_2 + n_1$; степень $f_1 g_2 + f_2 g_1$ не выше наибольшего из чисел $m_1 + n_2$, $m_2 + n_1$; но так как $m_1 + n_2 < n_1 + n_2$, $m_2 + n_1 < n_1 + n_2$, то, следовательно, степень $f_1 g_2 + f_2 g_1$ меньше степени $g_1 g_2$, что и требовалось доказать.

§ 60. Разложение на простейшие дроби.

Теорема. *Если* $\dfrac{f}{g_1 g_2}$ *— правильная дробь и* $\mathbf{D}(g_1, g_2) = 1$, *то можно эту дробь представить в виде* $\dfrac{f}{g_1 g_2} = \dfrac{f_1}{g_1} + \dfrac{f_2}{g_2}$, *где* $?\dfrac{f_1}{g_1}$, $\dfrac{f_2}{g_2}$ *— тоже правильные дроби; это представление возможно только одним способом.*

Доказательство. По § 52 (3) можно найти такие ц. р. функции φ_1 и φ_2, что будет $g_2\varphi_1 + g_1\varphi_2 \equiv 1$; умножая обе части этого равенства на f и обозначив:

$$\varphi_1 f = F_1, \qquad \varphi_2 f = F_2,$$

получим:

$$g_2F_1 + g_1F_2 = f;$$

разделив обе части на g_1g_2, найдем:

$$\frac{F_1}{g_1} + \frac{F_2}{g_2} = \frac{f}{g_1g_2};$$

если $\dfrac{F_1}{g_1}$, $\dfrac{F_2}{g_2}$ неправильные дроби, то выделим целые части:

$$\frac{F_1}{g_1} = q_1 + \frac{f_1}{g_1}; \qquad \frac{F_2}{g_2} = q_2 + \frac{f_2}{g_2};$$

следовательно:

$$\frac{f_1}{g_1} + \frac{f_2}{g_2} + q_1 + q_2 = \frac{f}{g_1g_2};$$

отсюда

$$q_1 + q_2 = \frac{f}{g_1g_2} - \frac{f_1}{g_1} - \frac{f_2}{g_2};$$

правая часть (§ 59, последняя теорема) — правильная дробь; левая часть — ц. р. функция; следовательно, должно быть: $q_1 + q_2 \equiv 0$, т. е.

$$\frac{f}{g_1g_2} = \frac{f_1}{g_1} + \frac{f_2}{g_2}.$$

Докажем теперь, что такое представление однозначно. Пусть

$$\frac{f}{g_1g_2} = \frac{f_1}{g_1} + \frac{f_2}{g_2} = \frac{\varphi_1}{g_1} + \frac{\varphi_2}{g_2},$$

причем $\dfrac{\varphi_1}{g_1}$ и $\dfrac{\varphi_2}{g_2}$ — правильные дроби. Тогда

$$\frac{f_1 - \varphi_1}{g_1} = \frac{\varphi_2 - f_2}{g_2}, \qquad g_2(f_-\varphi_1) = g_1(\varphi_2 - f_2);$$

так как $\mathbf{D}(g_1, g_2) = 1$ и $g_2(f_1 - \varphi_1)$ делится на g_1, то (§ 53, теорема 1) $f_1 - \varphi_1$ делится на g_1; но степень $f_1 - g_1$ меньше степени g_1; следовательно, $f_1 - \varphi_1 \equiv 0$, $f_1 \equiv \varphi_1$, откуда и $f_2 \equiv \varphi_2$ и теорема доказана.

Обобщение. Если ц. р. функции $g_1, g_2, \ldots, g_n$ попарно взаимно простые и дробь $\dfrac{f}{g_1g_2\cdots g_n}$ — правильная, то

$$\frac{f}{g_1g_2\cdots g_n} = \frac{f_1}{g_1} + \frac{f_2}{g_2} + \ldots + \frac{f_n}{g_n}, \tag{13}$$

где все дроби правой части правильные. Это представление возможно только одним образом.

Доказательство. Метод полной индукции: для $n = 2$ теорема верна; пусть она верна для $n-1$ сомножителей в знаменателе; имеем:

$$\frac{f}{g_1 g_2 \cdots g_n} = \frac{f}{(g_1 g_2 \cdots g_{n-1}) g_n} = \frac{F}{g_1 g_2 \cdots g_{n-1}} + \frac{f_n}{g_n};$$

но для $\dfrac{F}{g_1 g_2 \cdots g_{n-1}}$ по нашему предположению имеем:

$$F g_1 g_2 \cdots g_{n-1} = \frac{f_1}{g_1} + \frac{f_2}{g_2} + \ldots + \frac{f_{n-1}}{g_{n-1}};$$

подставив это, и получим (13).

Пусть возможны два разложения:

$$\frac{f}{g_1 g_2 \cdots g_n} = \frac{f_1}{g_1} + \frac{f_2}{g_2} + \ldots + \frac{f_n}{g_n} = \frac{\varphi_1}{g_1} + \frac{\varphi_2}{g_2} + \ldots + \frac{\varphi_n}{g_n},$$

тогда

$$\frac{f_1 - \varphi_1}{g_1} = \frac{\varphi_2 - f_2}{g_2}\frac{\varphi_3 - f_3}{g_3} + \ldots + \frac{\varphi_n - f_n}{g_n}.$$

Отсюда

$$(f_1 - \varphi_1) g_2 g_3 \cdots g_n = g_1 \cdot \Phi,$$

где

$$\Phi = (\varphi_2 - f_2) g_3 \cdots g_n + (\varphi_3 - f_3) g_2 g_4 \cdots g_n + \ldots + (\varphi_n - f_n) g_2 g_3 \cdots g_{n-1};$$

Φ — ц. р. функция; $(f_1 - \varphi_1) g_2 g_3 \cdots g_n$ делится на g_1, но (по § 53, теорема 2, следствие I) g_1 и $g_2 g_3 \cdots g_n$ взаимно простые; следовательно (по § 53, теореме 1), $f - \varphi_1$ делится на g_1, но $\dfrac{f_1}{g_1}$, $\dfrac{\varphi_1}{g_1}$ — правильные дроби, следовательно, степень $f_1 - \varphi_1$ меньше степени g_1, т. е. $f_1 - \varphi_1 \equiv 0$, $f_1 \equiv \varphi_1$. Подобным же образом докажем:

$$f_2 = \varphi_2, \ \ldots, \ f_n \equiv \varphi_n.$$

Если $\dfrac{f}{g}$ — правильная дробь и $g = (x-a)^\alpha (x-b)^\beta (x-c)^\gamma \cdots$, то, применяя предыдущую теорему, получим (§ 53, теорема 2, следствие III):

$$\frac{f}{g} = \frac{\varphi}{(x-a)^\alpha} + \frac{\psi}{(x-b)^\beta} + \frac{\omega}{(x-c)^\gamma} + \ldots,$$

где $\varphi, \psi, \omega, \ldots$ — ц. р. функции, φ имеет степень меньшую или равную α, ψ имеет степень меньшую или равную β, ω имеет степень меньшую или равную γ и т. д.

Разложим φо по степеням $x - a$; пусть

$$\varphi = A_\alpha + A_{\alpha-1}(x-a) + A_{\alpha-2}(x-a)^2 + \ldots + A_1 (x-a)^{\alpha-1};$$

тогда

$$\frac{\varphi}{(x-a)^\alpha} = \frac{A_\alpha}{(x-a)^\alpha} + \frac{A_{\alpha-1}}{(x-a)^{\alpha-1}} + \ldots + \frac{A_1}{x-a}.$$

Подобные же представления найдем для

$$\frac{\psi}{(x-b)^{\beta}},\quad \frac{\omega}{(x-c)^{\gamma}},\ \dots$$

Соединяя их вместе, получим:

$$\left.\begin{aligned} \frac{f}{g} &= \frac{A_\alpha}{(x-a)^\alpha}+\frac{A_{\alpha-1}}{(x-a)^{\alpha-1}}+\ldots+\frac{A_1}{x-a}+ \\ &+ \frac{B_\beta}{(x-b)^{\beta-1}}\frac{B_{\beta-1}}{(x-b)^{\beta-1}}+\ldots+\frac{B_1}{x-b}+ \\ &+ \frac{C_\gamma}{(x-c)^\gamma}+\frac{C_{\gamma-1}}{(x-c)^{\gamma-1}}+\ldots+\frac{C_1}{x-c}+\ldots \end{aligned}\right\} \qquad (14)$$

Это и есть *разложение на простейшие дроби*; здесь все коэфициенты: $A_\alpha, A_{\alpha-1}$, $\ldots, A_1,\ B_\beta, B_{\beta-1}, \ldots$ однозначно определены. Если дробь $\frac{f}{g}$ неправильная, то к правой части (14) прибавляется еще целая функция $q(x)$. Итак:

Теорема. *Если* $\frac{f(x)}{g(x)}$ *— любая дробная рациональная функция, и* $g(x)=(x-a_1)^{\alpha_1}(x-a_2)^{\alpha_2}\cdots(x-a_m)^{\alpha_m}$, *то разложение на простейшие дроби возможно только одним образом;*

$$\frac{f(x)}{g(x)}=\sum_{k=1}^{m}\sum_{\lambda=1}^{\alpha_k}\frac{A_{k\lambda}}{(x-a_k)^\lambda}+q(x),$$

где $q(x)$ *— ц. р. функция, которая тождественно равна* 0 *тогда и только тогда, когда дробь* $\frac{f(x)}{g(x)}$ *— правильная.*

Практически количества $A_{k\lambda}$ находятся методом неопределенных коэфициентов.

Пример. Разложить на простейшие дроби

$$\frac{x^2+2}{(x-1)^2(x+1)^3}.$$

Имеем:

$$\frac{x^2+2}{(x-1)^2(x+1)^3}=\frac{A_2}{(x-1)^2}+\frac{A_1}{x-1}+\frac{B_3}{(x+1)^3}+\frac{B_2}{(x+1)^2}+\frac{B_3}{x+1};$$

освободимся от знаменателей:

$$\begin{gathered} x^2+3=A_2(x+1)^3+A(x-1)(x+1)^3+B_3(x-1)^2+ \\ +B_2(x+1)(x-1)^3+B_1(x+1)^2(x-1)^2; \end{gathered}$$

сравнивая коэфициенты при одинаковых степенях x, получаем:

$$A_1+B_1=0, \qquad (I)$$

$$A_2+2A_1+B_1=0, \qquad (II)$$

$$3A_2 + B_3 - B_2 - 2B_1 = 1, \qquad (III)$$

$$3A_2 - 2A_1 - 2B_3 - B_2 = 0, \qquad (IV)$$

$$A_2 - A_1 + B_3 + B_2 + B_1 = 2. \qquad (V)$$

Вычитая (II) из (V), получаем:

$$-3A_1 + B_3 + B_1 = 2; \qquad (VI)$$

вычитая же (IV) из (III) —

$$2A_1 + 3b_3 - 2B_1 = 1; \qquad (VII)$$

решив (I), (VI) и (VII), найдем:

$$B_3 = \frac{3}{4}, \quad A_1 = -\frac{5}{16}, \quad B_1 = \frac{5}{16}.$$

Подставляя ? в (II), получаем:

$$A_2 + B_2 = \frac{5}{8}; \qquad (VIII)$$

подставляя B_1 и B_3 в (III), находим:

$$3A_2 - B_2 = \frac{7}{8}; \qquad (IX)$$

из (VIII) и (IX) следует:

$$A_2 = \frac{3}{8}, \quad B_2 = \frac{1}{4}.$$

Итак, получаем:

$$\frac{x^2+2}{(x-1)^2(x+1)^3} = \frac{3}{8(x-1)^2} - \frac{3}{16(x-1)} + \frac{3}{4(x+1)^3} + \frac{1}{4(x+1)^2} + \frac{5}{16(x+1)}.$$

Упражнения

Разложить на простейшие дроби:

94) $\dfrac{1}{(x-2)(x+1)^4}$.

Отв. $\dfrac{1}{81(x-2)} - \dfrac{1}{3(x+1)^4} - \dfrac{1}{9(x+10^3} - \dfrac{1}{27((x+1)^2} - \dfrac{1}{81(x+1)}$.

95) $\dfrac{x}{(x-i)^2(x+2i)}$.

Отв. $\dfrac{1}{3(x-i)^2} - \dfrac{2i}{9(x-i)} + \dfrac{2i}{9(x+2i)}$.

96) $\dfrac{x+2}{(x+\sqrt{2})^2(x-\sqrt{2})^2}$.

Отв. $\dfrac{2+\sqrt{2}}{8(x-\sqrt{2})^2} - \dfrac{\sqrt{2}}{8(x-\sqrt{2})} + \dfrac{2-\sqrt{2}}{8(x+\sqrt{2})^2} + \dfrac{\sqrt{2}}{8(x+\sqrt{2})}$.

§ 61. Разберем частный случай, когда в (14) $\alpha = \beta = \gamma = \ldots = 1$, т. е. когда

$$g(x) = (x-x_1)(x-x_2)(x-x_3)\cdots(x-x_n),$$

где $x_1, x_2, \ldots, x_n$ все различны; тогда (14) принимает вид:

$$\frac{f(x)}{g(x)} = \frac{A_1}{x-x_1} + \frac{A_2}{x-x_2} + \ldots + \frac{A_n}{x-x_n};$$

для определения A_1, умножаем обе части этого равенства на $x-x_1$ и затем берем $x = x_1$; тогда правая часть обращается в A_1 и мы получим:

$$A_1 = \frac{f(x_1)}{(x_1-x_2)(x_1-x_3)\cdots(x_1-x_n)} = \frac{f(x_1)}{g'(x_1)}$$

[§ 56 (II)]. Подобным же образом найдем вообще

$$A_k = \frac{f(x_k)}{g'(x_k)};$$

следовательно:

$$\frac{f(x)}{g(x)} = \frac{f(x_1)}{(x-x_1)g'(x_1)} + \frac{f(x_2)}{(x-x_2)g'(x_2)} + \ldots + \frac{f(x_n)}{(x-x_n)g'(x_n)}. \qquad (15)$$

Здесь предполагается, что степень f ниже степени g; иначе к правой части следует прибавить еще целую функцию $q(x)$.

Заметим, что при $f(x) = g'(x)$ формула (15) обращается в (10), § 56.

Пример.

$$\frac{x}{(x-1)(x-2)(x-3)} = \frac{A_1}{x-1} + \frac{A_2}{x-2} + \frac{A_3}{x-3};$$

A_1 определим, умножая левую часть на $x-1$ и беря затем $x = 1$; аналогично найдем и A_2 и A_3

$$A_1 = \frac{1}{2}, \qquad a_2 = -2, \qquad A_3 = \frac{3}{2}.$$

Упражнения

Разложить на простейшие дроби:

97) $\dfrac{1}{x^2-1}$.

Отв. $\dfrac{1}{2(x-1)} - \dfrac{1}{2(x+1)}$.

98) $\dfrac{x}{x^2+1}$.

Отв. $\dfrac{1}{2}\left[\dfrac{1}{x-i} + \dfrac{1}{x+i}\right]$.

99) $\dfrac{x+1}{x^2-2}$.

Отв. $\dfrac{2+\sqrt{2}}{4(x-\sqrt{2})}+\dfrac{2-\sqrt{2}}{4(x+\sqrt{2})}$.

100) $\dfrac{x^3-2}{x(x+1)(x-1)(x+2)(x-2)}$.

Отв. $-\dfrac{1}{2x}+\dfrac{1}{2(x+1)}+\dfrac{1}{6(x-1)}-\dfrac{5}{12(x+2)}+\dfrac{1}{4(x-2)}$.

101) $\dfrac{x^3}{(x-1)(x+2)}$.

Отв. $x-1+\dfrac{1}{3(x-1)}+\dfrac{8}{3(x+2)}$.

§ 62. Интерполяционная формула Лагранжа. Умножив обе части (15) на $g(x)$, получим:

$$f(x)=\frac{g(x)}{x-x_1}\frac{f(x_1)}{g'(x_1)}+\frac{g(x)}{x-x_2}\frac{f(x_2)}{g'(x_2)}+\ldots+\frac{g(x)}{x-x_n}\frac{f(x_n)}{g'(x_n)}. \tag{16}$$

Это — так называемая *интерполяционная формула Лагранжа* (Lagrange).

Значение ее заключается в следующем: пусть $f(x)$ — искомая функция, относительно которой известно, что при $x=x_1$ она принимает значение $y_1=f(x_1$, при $x=x_2$ — значение $y_2=f(x_2)$ и т. д., наконец, при $x=x_n$ — $y_n=f(x_n)$; по этим данным надо определить функцию $f(x)$. В таком виде задача, конечно, неопределенна. Но мы поставим условие, чтобы искомая функция $f(x)$ была наиболее простая; наиболее простой мы считаем ц. р. функцию наинизшей степени. Формула (16) и дает нам такую ц. р. функцию $f(x)$ степени меньшей или равной n. По следствию в конце § 50 такая функция $f(x)$ может быть только одна, т. е. функция $f(x)$, находимая по формуле (16), действительно наинизшей степени при поставленных условиях.

Пример 1. Дано: $x_1=0$, $x_2=1$, $x_3=2$, $x_4=4$; $y_1=f(0)=3$, $y_2=f(1)=3$, $y_3=f(2)=11$, $y_4=f(4)=75$.

Здесь

$$g(x)=x(x-1)(x-2)(x-4);$$

по формуле (11) § 56 находим:

$$g'(0)=(-1)(-2)(04)=-8,\quad g'(1)=1\cdot(1-2)(1-4)=3,$$
$$g'(2)=2\cdot(2-1)(2-4)=-4,\quad g'(4)=4\cdot(4-1)(4-2)=24.$$

Теперь применяем (16):

$$f(x)=-\frac{3}{8}(x-1)(x-2)(x-4)+$$
$$+\frac{3}{8}x(x-2)(x-4)-\frac{11}{4}x(x-1)(x-4)+\frac{75}{24}x(x-1)(x-2);$$

вычислив, найдем:

$$f(x)=x^3+x^2-2x+3.$$

Пример 2. Дано: $x_1=0$, $x_2=1$, $x_3=-1$, $x_4=2$, $x_5=-2$; $y_1=f(0)=2$, $y_2=f(1)=0$, $y_2=f(-1)=4$, $y_4=f(2)=4$, $y_5=f(-2)=0$.

Здесь

$$g(x) = x(x-1)(x+1)(x-2)(x+2), \quad g'(0) = (-1)\cdot 1\cdot(-2)\cdot 2 = 4,$$
$$g'(1) = 1\cdot 2\cdot(-1)\cdot 3 = -6, \quad g'(-1) = (-1)(-2)(-3)\cdot 1 = -6,$$
$$g'(2) = 2\cdot 1\cdot 3\cdot 4 = 24, \quad g'(-2) = (-2)(-3)(-1)(-4) = 24.$$

Применяем теперь (16):

$$f(x) = \frac{2}{4}(x-1)(x+1)(x-2)(x+2) - \frac{0}{6}x(x+1)(x-2)(x+2) -$$
$$-\frac{4}{6}x(x-1)(x-2)(x+2) + \frac{4}{24}x(x-1)(x+1)(x+2) +$$
$$+\frac{0}{24}x(x-1)(x+1)(x-2).$$

Вычислив, найдем:

$$f(x) = x^3 - 3x + 2.$$

Упражнения

Найти ц. р. функцию $f(x)$ наинизшей степени при условиях:
102) $f(4) = 13$, $f(5) = 21$, $f(-3) = 13$.
Отв. $f(x) = x^2 - x + 1$.
103) $f(0) = 1$, $f(1) = 5$, $f(-1) = 1$, $f(2) = 31$, $f(3) = 121$.
Отв. $f(x) = x^4 + x^3 + x^2 + x + 1$.
104) $f(0) = 5$, $f(1) = 4$, $f(-1) = 8$, $f(-2) = 13$, $f(4) = 13$, $f(6) = 29$.
Отв. $f(x) = x^2 - 2x + 5$.
105) $f(i) = 2 - 5i$, $f(-i) = 2 + 5i$, $f(1+i) = -4 - 2i$, $f(1-i) = -4 + 2i$.
Отв. $f(x) = x^3 - 4x + 2$.
106) $f(0) = 0$, $f(\sqrt{2}) = 0$, $f(\sqrt{8}) = 4$.
Отв. $f(x) = x^2 - \sqrt{2}$.

§ 63. Интерполяционная формула Ньютона. Формула Лагранжа, хотя теоретически вполне закончена, тем не менее представляет практические неудобства: предположим, что мы построили функцию $f(x)$, для которой даны значения $f(x_1)$, $f(x_2)$, ..., $f(x_n)$ при n различных значениях x: $x_1, x_2, \ldots, x_n$; эта функция степени меньшей или равной $n-1$.

Пусть теперь дано добавочное условие: при $x = x_{n+1}$ функция должна принимать заданное наперед значение $f(x_{n+1}$. Это будет уже новая функция $f(x)$ степени меньшей или равной n (хотя в частном случае она может и совпасть с прежней); чтобы ее найти, мы должны вновь применить формулу Лагранжа, проделать все вычисления с самого начала, ибо все предыдущие вычисления уже не годятся. От этого недостатка свободна интерполяционная формула Ньютона, которая имеет следующий вид:

$$f(x) = A_0 + A_1(x - x_1) + A_2(x - x_1)(x - x_2) + \ldots + \\ + A_{n-1}(x - x_1)(x - x_2)\cdots(x - x_{n-1}). \tag{17}$$

Коэфициенты $A_0, A_1, \ldots, A_{n-1}$ мы найдем, давая для x значения: $x_1, x_2, \ldots, x_n$. При $x = x_1$

$$f(x_1) = A_0;$$

при $x = x_2$

$$f(x_2) = A_0 + A_1(x_2 - x_1);$$

отсюда найдем A_1, при $x = x_3$

$$f(x_3) = A_0 + A_1(x_3 - x_1) + A_2(x_3 - x_1)(x_3 - x_2);$$

отсюда найдем A_2 и т. д. Наконец, положив $x = x_n$, найдем A_{n-1}.

Отсюда видно, что A_0 зависит только от x_1, $f(x_1)$; A_1 зависит только от x_1, x_2, $f(x_1)$, $f(x_2)$ и т. д., вообще A_{k-1} зависит только от x_1, x_2, $\ldots$, x_k, $f(x_1)$, $f(x_2)$, $\ldots$, $f(x_k)$. Если теперь дано добавочное условие: при $x = x_{n+1}$ функция принимает значение $f(x_{n+1})$, то новая функция получится просто прибавлением к найденной выражения

$$A_n(x - x_1)(x - x_2)\cdots(x - x_{n+1});$$

A_n мы найдем, положив $x = x_{n+1}$.

Пример. Пусть $x_1 = 0$, $x_2 = 1$, $x_3 = 2$, $x_4 = -1$; $f(0) = 3$, $f(1)? = 0$, $f(2) = 7$, $f(-1) = 4$.

Имеем:

$$f(x) = A_1 + A_1x + A_2x(x-1) + A_3x(x-1)(x-2)$$

давая для x значения 0, 1, 22, -1, получаем:

$$3 = A_0, \quad 0 = A_0 + A_1, \quad 7 = A_0 + 2A_1 + 2A_2, \quad 4 = A_0 - A_1 + 2A_2 - 6A_3;$$

отсюда найдем:

$$A_0 = 3, \quad A_1 = -3, \quad A_2 = 5, \quad A_3 = 2;$$

$$f(x) = 3 - 3x + 5x(x-1) + 2x(x-1)(x-2) = 2x^3 - x^2 - 4x + 3.$$

Упражнения

Определить ц. р. функцию наинизшей степени по условиям:

107) $f(0) = 2$, $f(1) = 3$, $f93) = 11$, $f(-2) = 6$.

Отв. $f(x) = x^2 + 2$.

108. $f(3) = 1$, $f(5) = 2$, $f(1) = 0$, $f(-1) = -1$.

Отв. $f(x) = \dfrac{1}{2}x - \dfrac{1}{2}$.

109) $f(0) = -1$, $f(1) = f(-1) = 0$, $f(2) = f(-2) = 15$.

Отв. $f(x) = x^4 - 1$.

110) $f(0) = \dfrac{1}{2}$, $f\left(\dfrac{1}{2}\right) = 2$, $f\left(-\dfrac{1}{2}\right) = 1$.

Отв. $f(x) = 4x^2 + x + \dfrac{1}{2}$.

ГЛАВА ЧЕТВЕРТАЯ

НЕПРЕРЫВНОСТЬ ЦЕЛОЙ ФУНКЦИИ И СУЩЕСТВОВАНИЕ КОРНЕЙ

§ 64. Теоремы о стремлении функции к нулю и о беспредельном возрастании функции. В этой главе, как и в предыдущей, мы будем коэфициенты наших функций и уравнений предполагать любыми комплексными числами и для x давать любые комплексные значения.

Теорема 1. *Если целая рациональная функция $f(x)$ такова, что $f(0) = 0$ [т. е. свободный член в $f(x)$ равен нулю], то при любом данном $\varepsilon > 0$ существует такое $\delta > 0$, что при всяком x, для которого $|x| < \delta$, будет $|f(x)| < \varepsilon$. [Это выражают, говоря: «$f(x)$ становится вместе с x бесконечно малой».]*

Доказательство. Пусть $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x$; обозначим: $|a_0| = \alpha_0$, $|a_1| = \alpha_1$, $\ldots$, $|a_{n-1}| = \alpha_{n-1}$; $|x| = \xi$; обозначим через α наибольшее из количеств $\alpha_0\alpha_1, \ldots, \alpha_{n-1}$.

Тогда

$$|f(x)| \leq \alpha_0\xi^n + \alpha_1\xi^{n-1} + \ldots + \alpha_{n-1}\xi \leq \alpha(\xi^n + \xi^{n-1} + \ldots + \xi);$$

но

$$\xi^n + \xi^{n-1} + \ldots + \xi = \frac{\xi - \xi^{n+1}}{1 - \xi};$$

положим $\xi < 1$; тогда $\xi^{n+1} < \xi$ и

$$\frac{\xi - \xi^{n+1}}{1 - \xi} < \frac{\xi}{1 - \xi},$$

следовательно:

$$|f(x)| < \frac{\alpha\xi}{1 - \xi};$$

поставим теперь условие: $\dfrac{\alpha\xi}{1 - \xi} < \varepsilon$; отсюда найдем: $\xi < \dfrac{\varepsilon}{\alpha + \varepsilon}$; обозначив $\dfrac{\varepsilon}{\alpha + \varepsilon} = \delta$, мы и будем иметь при $\xi = |x| < \delta$, что $|f(x)| < \varepsilon$, что и требовалось доказать. (Заметим, что $\delta = \dfrac{\varepsilon}{\alpha + \varepsilon} < 1$, т. е. прежде поставленное условие для ξ: $\xi < 1$ будет выполнено, если $\xi < \delta$.)

Теорема 2. *Если $f(x)$ — любая целая рациональная функция, то, взяв произвольное число $M > 0$, можно найти, такое число $N > 0$, что при $|x| > N$ будет $|f(x)| > M$. (Иначе: «$f(x)$ становится вместе с x бесконечно большой».)*

Доказательство. Пусть $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n$; положим: $\frac{1}{x} = z$; тогда можно написать:

$$f(x) = x^n(a_0 + a_1z + a_2z^2 + \ldots + a_nz^n);$$

далее (по § 8):

$$|f(x)| \geq |x|^n \cdot [|a_0| - |a_1z + a_2z^2 + \ldots + a_nz^n|];$$

но по теореме (1) можно найти $\delta > 0$ так, что при $|z| < \delta$, т. е. при $|x| > \frac{1}{\delta}$ будет:

$$|a_1z + a_2z^2 + \ldots + a_nz^n| < \frac{|a_0|}{2},$$

т. е. при $|x| > \frac{1}{\delta}$ будет:

$$|f(x)| > |x|^n \left[|a_0| - \frac{|a_0|}{2}\right],$$

или

$$|f(x)| > \frac{1}{2}|a_0| \cdot |x|^n;$$

но при достаточно большом $|x|$ будет:

$$\frac{1}{2}|a_0| \cdot |x|^n > M,$$

и теорема, таким образом, доказана.

§ 65. Верхний предел абсолютной величины корней. Теорема 3. *Если* $f(x) = x^n + a_1x^{n-1} + a_2x^{n-2} + \ldots + a_n$ *и* α *— наибольшее из количеств* $|a_1|, |a_2|, \ldots, |a_n|$, *то при* $|x| > \alpha + 1$ *будет* $|f(x)| > 0$, *т. е. всякий корень уравнения* $f(x) = 0$ *по абсолютной величине* $\leq \alpha + 1$; $\alpha + 1$ *— верхний предел абсолютной величины корней.*

Доказательство. Обозначая опять $|a_1| = \alpha_1$, $|a_2| = \alpha_2$, …, $|a_n = \alpha_n$, $|x| = \xi$ имеем по § 8:

$$|f(x)| \geq \xi^n - |a_1x^{n-1} + a_2x^{n-2} + \ldots + a_n| \geq \xi_n - \alpha_1\xi^{n-1} - \alpha_2\xi^{n-2} - \ldots - \alpha_n \geq$$
$$\geq \xi^n - \alpha(\xi^{n-1} + \xi^{n-2} + \ldots + 1);$$

но

$$\xi^{n-1} + \xi^{n-2} + \ldots + 1 = \frac{\xi^n - 1}{\xi - 1};$$

следовательно:

$$|f(x)| \geq \xi^n - \frac{\alpha(\xi^n - 1)}{\xi - 1};$$

пусть $\xi > 1$; тогда

$$\alpha\frac{\xi^n - 1}{\xi - 1} < \frac{\alpha\xi^n}{\xi - 1};$$

следовательно;

$$|f(x)| > \xi^n - \frac{\alpha\xi^n}{\xi - 1}$$

или

$$|f(x)| > \xi^n \frac{\xi - (\alpha + 1)}{\xi - 1};$$

отсюда видно, что при $\xi > \alpha + 1$ $|f(x)| > 0$, что и требовалось доказать.

Обобщение. Пусть теперь $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n$, где $a_0 \neq 1$; тогда, разделив на a_0, найдем: при $|x|.\alpha+1$ будет справедливо $\left|\frac{f(x)}{a_0}\right| > 0$, т. е. и $|f(x)| > 0$, только здесь α — наибольшее из количеств:

$$\left|\frac{a_1}{a_0}\right|, \quad \left|\frac{a_2}{a_0}\right|, \ \ldots, \ \left|\frac{a_n}{a_0}\right|.$$

Примеры. Для уравнения

$$x^5 - 3x^4 + 4x^2 - x - 2 = 0$$

верхний предел абсолютной величины корней есть 5; для уравнения

$$3x^3 - 4x^2 + 7x + 2 = 0 \quad \text{он есть} \quad 3\frac{1}{3};$$

для уравнения

$$x^4 + (3 - i)x^3 + \left(\frac{1}{2} + 3i\right)x^2 - \sqrt{5} \cdot x - 1 = 0 \quad \text{он равен} \quad \sqrt{10} + 1 < 5.$$

§ 66. Непрерывность целой рациональной функции. Теорема 4. *Если $f(x)$ — целая рациональная функция, то для всякого значения x при данном $\varepsilon > 0$ можно найти $\delta > 0$ так, что при $|h| < \delta$ будет: $|f(x + h) - f(x)| < \varepsilon$. (Иначе: целая рациональная функция непрерывна для всякого значения x.)*

Доказательство. По формуле Тэйлора [§ 54, (4)] имеем:

$$f(x + h) - f(x) = c_1h + c_2h^2 + \ldots + c_nh^n,$$

где $c_1 = f'(x)$, $c_2 = \frac{1}{2!}f''(x)$ и т. д.; в правой части у нас — ц. р. функция от h без свободного члена; по теореме 1 при данном $\varepsilon > 0$ можно найти $\delta > 0$ так, что при $|h| < \delta$ будет:

$$|f(x + h) - f(x)| = |c_1h + c_2h^2 + \ldots + c_nh^n| < \varepsilon,$$

а это и требовалось доказать.

Так как

$$\big|\,|f(x + h) - f(x)| - |f(x)|\,\big| \leq |f(x + h) - f(x)|,$$

т. е. при $|h| < \delta$ и $\big|\,|f(x + h) - f(x)| - |f(x)|\,\big| \leq \varepsilon$, то заключаем:

Следствие. Абсолютная величина целой рациональной функции тоже непрерывна при всяком значении x.

Абсолютная величина ц. р. функции есть тоже функция от x, но не целая рациональная; при всяком x она вещественна и положительна, в крайнем случае она равна нулю, именно для тех и только для тех значений x, для которых и сама

ц. р. функция $f(x) = 0$. Следовательно, чтобы доказать, что всякое алгебраическое уравнение имеет корень, нам достаточно доказать, что абсолютная величина всякой ц. р. функции обращается в нуль хоть для одного значения x.

Замечание. Из той же формулы Тэйлора [§ 54, (4)] выводим:

$$\frac{f(x+h)-f(x)}{h} = f'(x) + \frac{h}{2!}f''(x) + \ldots + \frac{h^{n-1}}{n!}f^{(n)}(x);$$

если h стремится к нулю, то все члены правой части, начиная со второго, приближаются к нулю; первый же член не зависит от h. Таким образом мы получаем:

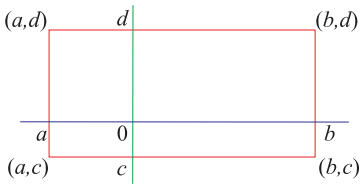
$$\lim_{h\to 0} \frac{f(x+h)-f(x)}{h} = f'(x), \qquad (1)$$

т. е, мы приходим к обычному определению производной как предела отношения приращения функции к приращению независимого переменного, когда это последнее приращение стремится к нулю. Только теперь мы видим, что этот предел для ц. р. функции существует и в области комплексных чисел.

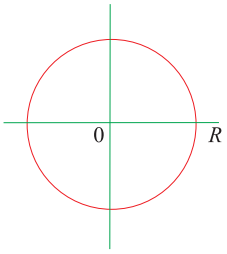
Применяя к пределу (1) обычные теоремы о пределах, мы докажем, что основные формулы диференцирования верны и в комплексной области — для ц. р. функций.

Заметим, что для функции $|f(x)|$ формула (1) уже неверна.

§ 67. Когда рассматриваются функции вещественного переменного x, то значения для x обычно берутся в некотором *интервале* — конечном или бесконечном; если интервал конечен, то обычно даются его «концы», значения a и b. Если x принимает значения, лежащие только внутри интервала, то интервал называется *незамкнутым*; если же x может принимать и значения a и b («границы» интервала), то интервал — *замкнутый*.



Черт. 7



Черт. 8

Если x принимает комплексные значения, то вместо интервала мы имеем уже *область* в плоскости комплексных чисел — конечную или бесконечную. Различают области *замкнутые* и *незамкнутые*, в зависимости от того, может ли x принимать значения, лежащие на границе области, или не может и принимает значения только внутри области. Граница конечной области есть некоторая замкнутая кривая; эти границы могут быть весьма разнообразны, в зависимости от чего и области имеют разнообразные формы.

На черт. 7 представлена прямоугольная область, которая аналитически определяется так:

$$a < u < b, \qquad c < v < d,$$

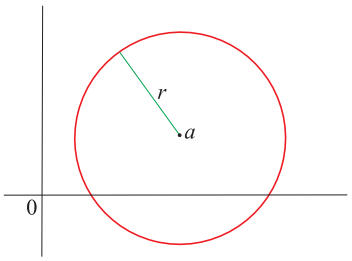
где $x = u + iv$; или (если область замкнута) $a \leq u \leq b$, $c \leq v \leq d$.

На черт. 8 представлена круговая область, которая определяется аналитически следующим образом: $|x| < R$ (где R — радиус круга), если область незамкнута или $|x| \leq R$, если область замкнута.

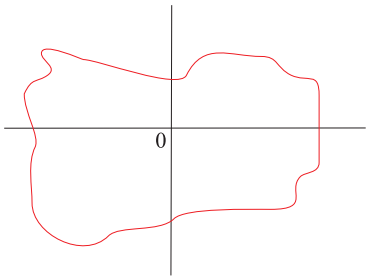
На черт. 9 представлена тоже круговая область, но с центром не в нуле, а в некоторой точке α; она определяется аналитически $|x - \alpha| < r$ или $|x - \alpha| \leq r$, где r — радиус круга.

Наконец, на черт. 10 представлена конечная область с произвольной, совершенно неправильной границей. Заметим, что можно всегда из точки O описать круг таким большим радиусом, что внутри этого круга будет целиком лежать всякая данная конечная область; точно так же всякую конечную область можно заключить в прямоугольник со сторонами, параллельными координатным осям.

Теорема 5. *Если $f(x)$ — целая рациональная функция, а E — данная конечная область, то существует такое число $G > 0$, что для всякого x, лежащего в E, $|f(x)| < G$. (Иначе: целая рациональная функция ограничена во всякой конечной области.)*



Черт. 9



Черт. 10

Доказательство. Заключим область E в круг с центром O и радиусом R, тогда для x в E $|x| < R$. Пусть $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n$, имеем

$$|f(x)| \leq |a_0|\,|x|^n + |a_1|\,|x|^{n-1} + \ldots |a_n| \leq$$
$$\leq |a_0|R^n + |a_1|R^{n-1} + \ldots + |a_n|$$

для всех x в E.

Обозначим $|a_0|R^n + |a_1|R^{n-1} + \ldots + |a_n| = G$, тогда и получим для всех $x \in E$ $|f(x)| < G$.

§ 68. В теореме о непрерывности целой рациональной функции (§ 66) количество δ зависело вообще от ε и x, теперь мы докажем, что для всех значений x в конечной области можно выбрать δ независящим от x. Именно:

Теорема 6. *Если $f(x)$ — целая рациональная функция, а E — конечная область, то, взяв произвольное $\varepsilon > 0$, можно найти $\delta > 0$, независящее от x, так что при $|h| < \delta$ для всякого x из E будет: $|f(x + h) - f(x)| < \varepsilon$. (Иначе: целая рациональная функция равномерно непрерывна во всякой конечной области.)*

Доказательство: По формуле Тэйлора [§ 54, (4)]

$$f(x + h) - f(x) = hf'(x) + h^2\,\frac{f''(x)}{2!} + \ldots + h^n\,\frac{f^{(n)}(x)}{n!};$$

так как $f'(x)$, $\dfrac{f''(x)}{2!}$, $\ldots$, $\dfrac{f^{(n)}(x)}{n!}$ — ц. р. функции от x, то по предыдущей теореме можно найти такие количества $k_1, k_2, \ldots, k_n$ — все положительные, что для всякого x в области E будет:

$$|f'(x)| < k_1, \quad \left|\frac{f''(x)}{2!}\right| < k_2, \ \ldots, \ \left|\frac{f^{(n)}(x)}{n!}\right| < k_n.$$

Обозначим еще: $|h| = \eta$; тогда

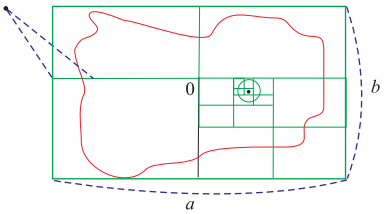
$$|f(x+h) - f(x)| < k_1\eta + k_2\eta^2 + \ldots + k_n\eta^n;$$

правая часть этого неравенства совершенно не зависит от x и есть ц. р. функция от η без свободного члена; по теореме 1 § 69 при данном $\varepsilon > 0$ можно найти $\delta > 0$ (при этом независимо от x), так что при $\eta < \delta$ (мы пишем η], а не $|\eta|$, ибо η положительно) будет: $k_1\eta + k_2\eta^2 + \ldots + k_n\eta^n < \varepsilon$ и $|f(x+h) - f(x)| < \varepsilon$ — для всякого x в E, что и требовалось доказать.

Следствие. Из того, что $||f(x+h)| - |f(x)|| \leq |f(x+h) - f(x)|$ (§ 8), заключаем, что и функция $|f(x)|$ равномерно непрерывна во всякой конечной области.

§ 69. Нижняя и верхняя границы функции. Пусть $F(x)$ — какая-нибудь вещественная (т. е. принимающая только вещественное значение) функция от комплексного (или вещественного) переменного x; пусть в конечной области E [или в интервале (a, b)] для x функция $F(x)$ ограничена, т. е. $|F(x)| < G$, где G — некоторое определенное число, иначе: $-G < F(x) < +G$, т. е. все значения функции $F(x)$ лежат в интервале от $-G$ до $+G$.

Все числа этого интервала разделим на два класса: к первому классу относим те числа C, которые меньше всех значений $F(x)$ для x в области E [или в интервале (a, b)]; ко второму классу относим остальные числа, т. е. такие числа C, что по крайней мере для одного x из E [или из (a, b) $C \geq F(x)$. К первому классу принадлежит, например, число $-G$, ко второму классу — число $+G$. Очевидно, что каждое число первого класса меньше каждого числа второго класса и при этом каждое число в интервале $(-G, +G)$ войдет в один и только в один из классов, т. е. это деление есть *сечение Дедекинда* (Dedekind); оно определит некоторое число k, отличающееся следующим свойством: при любом $\eta > 0$ число $k - \eta$ принадлежит к первому классу, тогда как число $k + \eta$ — ко второму; само же число k, вообще говоря, может принадлежать или к первому, или ко второму классу. Итак:



Черт. 11

Теорема. *Если $F(x)$ — вещественная функция от комплексного (или вещественного) переменного x, ограниченная в области E [или в интервале (a, b)], то существует такое число k, что при любом $\eta > 0$ $k - \eta$ меньше всех значений $F(x)$ в области E [или в интервале (a, b)], тогда как существует в E [или в интервале (a, b)] по крайней мере одно такое значение x, для которого $k + \eta \geq F(x)$.*

Это число k называется нижней границей функции $F(x)$ в области E [или в интервале (a, b)]. Если k принадлежит ко второму классу, то при некотором x из

E [или из (a, b)] $F(x) = k$; легко видеть, что это — наименьшее значение, которое вообще $F(x)$ принимает в области E [или в интервале (a, b)]; оно есть минимум функции в E [или в (a, b)]. Если же k принадлежит к первому классу, то $F(x)$ не имеет минимума в E [или в (a, b)], но тогда при всяком $\eta > 0$ существует бесчисленное множество значений $F(x)$, лежащих между k и $k + \eta$; в этом случае k — низший предел для $F(x)$ в области E [или в (a, b)].

Аналогично определяется *верхняя граница* функции и доказывается ее существование; верхняя граница функции есть или максимум функции, или ее высший предел. Но на этом мы не будем останавливаться, ибо это нам в дальнейшем не понадобится.

§ 70. Точки сгущения точечных множеств. Для дальнейшего нам необходима одна теорема из теории точечных множеств. Пусть нам дано бесконечное множество точек, лежащих в некоторой конечной области на плоскости. Это множество (обозначим его через A) вполне определено в том смысле, что для каждой точки нашей области мы имеем возможность решить, принадлежит ли она ко множеству A или нет. Заключим нашу область в прямоугольник (это возможно, ибо область конечна) и разделим этот прямоугольник на четыре равных прямоугольника прямыми, параллельными его сторонам (черт. 11); тогда по крайней мере в одном из этих прямоугольников будет лежать бесконечное множество точек из A; этот прямоугольник мы опять разделим таким же образом на 4 части и выберем ту из них, где лежит бесчисленное множество точек из A и т. д. Если мы обозначим через a и b длины сторон первого прямоугольника, то у второго стороны будут $\frac{a}{2}$ и $\frac{b}{2}$ и т. д., вообще у n-го — $\frac{a}{2^n}$ и $\frac{b}{2^n}$; при беспредельном возрастании n эти стороны стремятся к нулю, а так как эти прямоугольники вложены один в другой, так что все последующие лежат внутри предыдущего, то при $n \to \infty$ все эти прямоугольники будут стягиваться в некоторой точке x_0, лежащей внутри *всех* их. Если мы возьмем круг с центром x_0 и со сколь угодно малым радиусом ε, то, как бы мало ε ни было, можно взять n таким большим, чтобы $\frac{a}{2^n}$ и $\frac{b}{2^n}$ были меньше, чем $\frac{\varepsilon}{\sqrt{2}}$; тогда n-й прямоугольник, а следовательно, и все последующие, будут лежать внутри этого круга, а так как внутри каждого прямоугольника лежит бесчисленное множество точек из A, то, следовательно, и внутри взятого круга тоже находится бесчисленное множество точек из A; иными словами, как угодно близко от x_0 лежит бесчисленное множество точек данного множества A. Сама точка x_0 может тоже принадлежать к A, а может и не принадлежать; во всяком случае x_0 лежит *внутри* или *на границе* данной области. Такая точка x_0, в какой угодно близости которой лежит бесчисленное множество точек данного точечного множества A, называется *точкой сгущения*, или *предельной точкой* для A. Мы доказали следующее:

Теорема. *Всякое бесконечное точечное множество, лежащее в конечной области, имеет по крайней мере одну точку сгущения, лежащую внутри или на границе этой области.*

§ 71. Минимум непрерывной функции. Теорема. *Вещественная, ограниченная, непрерывная функция от комплексного (или вещественного) переменного*

в конечной замкнутой области E [или в замкнутом интервале (a, b)] имеет в этой области минимум, т. е. для некоторого значения своего аргумента принимает значение, которое $\leq$ всех остальных ее значений в этой области [24].

Доказательство. Пусть $F(x)$ функция, удовлетворяющая условиям теоремы, и k — ее нижняя граница в E. Мы должны доказать, что при некотором значении $x = x_0$, $F(x_0) = k$ [ибо по § 69, если минимум для $F(x)$ существует, то он равен k]. Возьмем бесконечную последовательность чисел, стремящихся к нулю: $\varepsilon_1 > \varepsilon_2 > \varepsilon_3 > \ldots > 0$, $\varepsilon_n \to 0$. По определению нижней границы (§ 69) мы можем найти ряд значений для x: $x_1, x_2, x_3, \ldots$ так, чтобы было $F(x_n) \leq k + \varepsilon_n$ $(n = 1, 2, 3, \ldots)$; бесконечное множество точек $x_1, x_2, x_3, \ldots$ имеет (по теореме § 70) по крайней мере одну точку сгущения x_0; как угодно близко от x_0 лежит бесчисленное множество наших точек x_n (но не обязательно все, начиная с некоторого n), а следовательно, лежат точки x_n с как угодно большими номерами n; для них $F(x_n)$ как угодно мало отличается от k. Пусть $F(x_0) = k + l$ и $l > 0$; так как функция $F(x)$ непрерывна при $x = x_0$, то можно найти $\delta > 0$ так, что при $|x - x_0| < \delta$ будет:

$$|F(x) - F(x_0| < \frac{l}{2};$$

это условие равносильно такому:

$$-\frac{l}{2} < F(x) - F(x_0) < \frac{l}{2};$$

или, подставляя вместо $F(x_0)$ ее значение $k + l$ и беря только левую часть последнего двойного неравенства:

$$-\frac{l}{2} < F(x) - k - l, F(x) > k + \frac{l}{2}. \tag{2}$$

Условие $|x - x_0| < \delta$ дает для x точки круга радиуса δ с центром x_0; следовательно, для всех таких точек выполнено неравенство (2). С другой стороны, в этом круге лежат и точки x_n нашего множества с как угодно большими значками n; для них

$$F(x_n \leq k + \varepsilon_n. \tag{3}$$

Но при достаточно большом n $\varepsilon_n < \frac{l}{2}$; следовательно, формула (3) стоит в противоречии с формулой (2), ибо (2) должно быть верно при $x = x_n$. Это противоречие устраняется только при $l = 0$, т. е. $F(x_0) = k$, и наша теорема, таким образом, доказана [25].

§ 72. Лемма Даламбера и теорема о существовании корней. Предыдущая теорема применима к функции $|f(x)|$, где $f(x)$ — ц. р. функция. За область E примем круг, описанный вокруг точки O радиусом, равным ?, где $\alpha+1$ имеет то же значение, что и в § 65. По § 65 мы заключаем, что если корни уравнения $f(x) = 0$

[24] Аналогичная теорема существует и для максимума.

[25] Условие замкнутости области E существенно для этой теоремы: ведь может случиться, что точка x_0 будет лежать на границе области E; тогда, в случае, если E незамкнута, значения $F(x_0)$ не существует.

существуют, то они лежат все внутри этого круга E. Функция $|f(x)|$ непрерывна (§ 66, 68); следовательно, по предыдущей теореме, она имеет минимум в области E. Так как $|f(x)|$ не может быть отрицательна, то и ее минимум должен быть ≥ 0. Если он больше нуля, то $|f(x)|$, а следовательно, и $f(x)$ нигде не обращается в нуль, т. е. уравнение $f(x) = 0$ не имеет корней. Но если мы докажем, что для всякой ц. р. функции $f(x)$ минимум функции $|f(x)|$ равен нулю, то этим самым будет доказано, что всякое алгебраическое уравнение $f(x) = 0$ имеет корень. Что минимум для $|f(x)|$ действительно равен нулю, следует из леммы Даламбера:

Лемма Даламбера. *Если для данного значения $x = x_1$ $|f(x_1)| > 0$, то можно найти такое значение $x = x_2$, для которого будет:*

$$|f(x_2)| < |f(x_1)|.$$

Доказательство. Имеем (по формуле Тэйлора, § 54):

$$f(x_1 + h) = f(x_1) + hf'(x_1) + \frac{h^2}{2!}f''(x_1) + \ldots + \frac{h^n}{n!}f^{(n)}(x_1);$$

$f(x_1) \neq 0$, но может случиться, что $f'(x_1) = 0$; положим для общности:

$$f'(x_1) = f''(x_1) = \ldots = f^{(\lambda-1)}(x_1) = 0, \quad \text{но} \quad f^{(\lambda)}(x_1) \neq 0;$$

тогда

$$f(x_1 + h) = f(x_1) + \frac{h^\lambda}{\lambda!}f^{(\lambda)}(x_1) + \frac{h^{\lambda+1}}{(\lambda+1)!}f^{(\lambda+1)}(x_1) + \ldots + \frac{h^n}{n!},$$

$$\frac{f(x_1 + h)}{f(x_1)} = 1 + c_\lambda h^\lambda + c_{\lambda+1}h^{\lambda+1} + \cdots + c_n h^n,$$

где $c_\lambda = \dfrac{f^{(\lambda)}(x_1)}{\lambda! f(x_1)}$, $c_{\lambda+1} = \dfrac{f^{(\lambda+1)}(x_1)}{(\lambda+1)! f(x_1)}$, $\ldots$; как $c_\lambda, c_{\lambda+1}, \ldots, c_n$, так и h — вообще комплексные числа. Положим:

$$c_k = t_k(\cos\tau_k + i\sin\tau_k) \quad (k = \lambda, \lambda+1, \ldots, n)$$
$$h = \rho(\cos\omega + i\sin\omega);$$

тогда

$$\left|\frac{f(x_1 + h)}{f(x_1)}\right| \leq |1 + t_\lambda\rho^\lambda[\cos(\lambda\omega + \tau_\lambda) + i\sin(\lambda\omega + \tau_\lambda)]| + \\ + t_{\lambda+1}\rho^{\lambda+1} + \ldots + t_n\rho^n$$

(по § 8). Приращение h, а следовательно, ρ и ω произвольны; выберем ω так, чтобы было $\lambda\omega + \tau_\lambda = \pi$, т. е. $\omega = \dfrac{\pi - \tau_\lambda}{\lambda}$; тогда

$$\left|\frac{f(x_1 + h)}{f(x_1)}\right| \leq |1 - t_\lambda\rho^\lambda| + t_{\lambda+1}\rho^{\lambda+1} + \ldots + t_n\rho^n;$$

далее, выберем ρ так, чтобы было $t_\lambda\rho^\lambda < 1$, т. е. $\rho < \sqrt[\lambda]{\dfrac{1}{t_\lambda}}$ (при этом всегда $\rho > 0$); будем иметь:

$$\left|\frac{f(x_1 + h)}{f(x_1)}\right| \leq 1 - t_\lambda\rho^\lambda\left(1 - \frac{t_{\lambda+1}}{t_\lambda}\rho - \frac{t_{\lambda+2}}{t_\lambda}\rho^2 - \ldots - \frac{t_n}{t_\lambda}\rho^{n-\lambda}\right); \qquad (4)$$

все $t_\lambda, t_{\lambda+1}, \ldots, t_n > 0$; следовательно, при $\rho > 0$ будет и

$$\frac{t_{\lambda+1}}{t_\lambda}\rho + \frac{t_{\lambda+2}}{t_\lambda}\rho^2 + \ldots + \frac{t_n}{t_\lambda}\rho^{n-\lambda} > 0;$$

при достаточно малом ρ эта функция будет < 1 (§ 64); тогда получим:

$$0 < 1 - \frac{t_{\lambda+1}}{t_\lambda}\rho - \ldots - \frac{t_n}{t_\lambda}\rho^{n-\lambda} < 1,$$

следовательно, и вся правая часть в (4) будет меньше единицы; следовательно для такого h будет $\left|\dfrac{f(x_1+h)}{f(x_1)}\right| < 1$, т. е. $|f(x_1+h)| < |f(x_1)|$; обозначив $x_1 + h = x_2$, будем иметь $|f(x_2)| < |f(x_1 0|$, и лемма Даламбера доказана.

Пусть теперь $|f(x)|$ имеет минимум (а мы уже знаем, что эта функция минимума достигает) в точке x_0. Тогда, очевидно, $|f(x_0)| = 0$, ибо если бы $|f(x_0)|$ было положительно, то существовало бы значение $x = x_1$, в котором $|f(x_1)| < |f(x_0)|$ и $|f(x_0)|$ не было бы минимумом. Итак, минимум для $|f(x0|$ должен быть равен нулю, т. е. этим доказана и основная теорема алгебры.

Основная теорема. *Всякое алгебраическое уравнение с вещественными или комплексными коэфициентами имеет по крайней мере один вещественный или комплексный корень.*

Отсюда по § 50 непосредственно следует, что всякое уравнение n-й степени имеет n корней, которые могут быть не все различны, и левая часть уравнения раскладывается на n линейных множителей. Предлагается проверить, что при доказательстве основной теоремы мы не основывались на выводах § 50, т. е. наше доказательство не содержит порочного круга.

В XVIII в. лемму Даламбера считали тождественной с основной теоремой н рассуждали так: «найдем по этой лемме ряд значений $x_1, x_2, x_3, \ldots$ таких, что

$$|f(x_1)| > |f(x_2)| > |f(x_3)| > \ldots;$$

в конце концов дойдем до такого значения x_n, для которого $|f(x_n)| = 0$». Это, конечно, нелогично: последовательность $|f(x_1)|, |f(x_2)|, \ldots$ убывающих положительных чисел может никогда не дойти до нуля и, более того, может даже не иметь своим пределом нуль, как, например, последовательность $2, \frac{3}{2}, \frac{4}{3}, \frac{5}{4}, \frac{6}{5}, \ldots$

Гаусс (Gauss) первый строго доказал основную теорему алгебры в своей диссертации: «Demonstratio nova theorematis, omnem functionera algebraicam rationalem integram unius variabilis in factores reales primi vel sectmdi gradus resolvi posse». [26] в Helmstedt'e в 1799 г. В начале этого сочинения он выясняет несостоятельность всех бывших да него попыток доказать эту теорему; затем он дает первое строгое ее доказательство. Идея его такова:

Пусть $z = x + iy$ — наше независимое переменное, а $f(z) = u(x,y) + iv(x,y)$ — ц. р. функции и $u(x,y)$, и $v(x,y)$ — две вещественные ц. р. функции от двух вещественных переменных x и y. Гаусс рассматривает кривые, выражаемые уравнениями $u(x,y) = 0$, $v(x,y)$, и доказывает, что эти кривые по крайней мере один

[26] «Новое доказательство теоремы, что всякая алгебраическая рациональная целая функция одного переменного может быть разложена на вещественные сомножители первой или второй степени».

раз должны пересечься; если (x_0, y_0) — точка их пересечения, то $z_0 = x_0 + iy_0$ и есть корень уравнения $f(z) = 0$. Недостаток этого доказательства, как признал и сам Гаусс, есть, если можно так выразиться, его «слищком геометрический» облик (что, впрочем, не мешает ему быть строгим). Затем, как показывает самое заглавие диссертации, Гаусс имеет ввиду только уравнения с вещественными коэфициентами. В конце Гаусс дает идею другого доказательства, именно того, которое привели мы.

16 лет спустя после первого доказательства, Гаусс дал второе доказательство основной теоремы, основанное на совсем других принципах. Основная мысль есть сведение данного уравнения четной степени на другое, степень которого содержит множитель 2 в меньшей степени, чем его содержит степень данного уравнения, — пока не придем к уравнению нечетной степени с вещественными ксэфициентами, которое непременно имеет вещественный корень (ср. следствие II, § 77); применяемые преобразования основаны на теории симметрических функций. Доказательство это замечательно тем, что оно чисто алгебраическое (за исключением как раз теоремы о существовании вещественного корня у уравнения нечетной степени с вещественными коэфициентами). Позже Гордан (Gordan) несколько видоизменил это доказательство, распространив его на случай уравнений с комплексными коэфициентами.

Третье доказательство Гаусса появилось сейчас же после второго. Оно основано на интеграле, приводящем к функции arctg. По существу в нем применяется теория функций комплексного переменного.

50 лет спустя после появления первого доказательства, Гаусс вновь возвратился к нему, сильно видоизменив его и освободив от излишней «геометричности». Это четвертое доказательство Гаусса замечательно, во-первых, тем, что имеет в виду уравнения и с комплексными коэфициентами, а во-вторых, тем, что выявляет сразу существование n корней у уравнения n-й степени.

Из других доказательств основной теоремы алгебры упомянем о доказательстве Коши (Cauchy), основанном на интеграле $\dfrac{1}{2\pi i}\displaystyle\int \frac{f'(z)}{f(z)}\,dz$ в комплексной области, и о доказательстве Вейерштрасса, основанном на теореме Лиувилля (Liouville) о том, что однозначная аналитическая функция комплексного переменного не может быть ограниченной, если только она не равняется постоянному количеству.

§ 73. Непрерывность корней алгебраического уравнения.

Теорема. *Корни алгебраического уравнения являются непрерывными функциями от его коэфициентов, если высший коэфициент не равен нулю.*

Доказательство. Примем сначала, что высший коэфициент $a_0 = 1$. Пусть левая часть уравнения имеет вид:

$$\begin{gathered} f(x) = a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \ldots + a_n = \\ = (x - c_1)^{\alpha_1}(x - c_2)^{\alpha_2}\cdots(x - c_k)^{\alpha_k}; \qquad \alpha_1 + \alpha_2 + \ldots + \alpha_k = n; \end{gathered} \tag{5}$$

коэфициенты $a_1, a_2, \ldots, a_n$ — любые комплексные числа. Нам надо доказать, что при достаточно малых приращениях коэфициентов приращения корней будут как угодно малы. Пусть $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_k$ — заданные положительные, сколь угодно малые числа, такие, что каждое ε_λ меньше половины расстояния точки c_λ от ближайшей

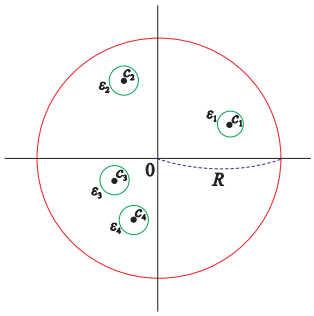
из остальных $c_1, c_2, \ldots, c_k$. Опишем вокруг этих точек, как центров, круги с радиусами $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_k$ (черт. 12); назовем их кругами $(\varepsilon_1), (\varepsilon_2), \ldots, (\varepsilon_k)$; никакие два из них не налегают друг на друга и не соприкасаются. Докажем следующее:

Теорема. *Можно найти такие положительные числа* $\delta_1, \delta_2, \ldots, \delta_n$, *что при* $|h_1| < \delta_1$, $|h_2| < \delta_2$, $\ldots$, $|h_n| < \delta_n$ *уравнение*

$$f_1(x) = x^n + (a_1 + h_1)x^{n-1} + (a_2 + h_2)x^{n-2} + \ldots + (a_n + h_n) = 0 \tag{6}$$

будет иметь α_1 *корней в круге* (ε_1), α_2 *корней в круге* (ε_2), $\ldots$, α_k *корней в круге* (ε_k) *(при этом принимаются во внимание и кратности корней); вне этих кругов* $f_1(x)$ *не обращается в нуль.*

Опишем в плоскости x круг с центром O и с таким большим радиусом R, чтобы вне этого круга $f_1(x)$ ни при каких значениях $h_1, h_2, \ldots, h_n$, удовлетворяющих указанным неравенствам, не обращалось в нуль; для этого (по § 65, теореме 3) достаточно взять R на единицу больше, чем наибольшая из сумм $|a_1| + \delta_1, |a_2| + \delta_2, \ldots, |a_n| + \delta_n$. Обозначим через g область, получающуюся из этого круга радиуса R после исключения из него кругов с радиусами $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_k$, о которых говорилось выше (все эти круги будут лежать внутри круга радиуса R; во всяком случае мы добьемся этого, увеличив в случае надобности R).



Черт. 12

Если x лежит в области g, то

$$|x - c_1| > \varepsilon_1, \quad |x - c_2| > \varepsilon_2, \ \ldots, |x - c_k| > \varepsilon_k;$$

следовательно:

$$|f(x)| > \varepsilon_1^{\alpha_1}\varepsilon_2^{\alpha_2}\cdots\varepsilon_k^{\alpha_k}. \tag{7}$$

Имеем, далее:

$$f_1(x) = f(x) + \varphi(x), \tag{8}$$

где

$$\varphi(x) == h_1x^{n-1} + h_2x^{n-2} + \ldots + h_{n-1}x + h_n; \tag{9}$$

если x лежит в области g, то $|x| < R$, следовательно:

$$|\varphi(x)| < \delta_1R^{n-1} + \delta_2R^{n-2} + \ldots \delta_{n-1}R + \delta_n < n\delta R^{n-1},$$

где δ — наибольшее из чисел $\delta_1, \delta_2, \ldots, \delta_n$, а по условию $R > 1$. Выберем теперь $\delta_1, \delta_2, \ldots, \delta_n$ столь малыми, чтобы δ удовлетворяло условию

$$\delta < \frac{\varepsilon_1^{\alpha_1}\varepsilon_2^{\alpha_2}\cdots\varepsilon_k^{\alpha_k}}{nR^{n-1}};$$

тогда для всякого x в области g будет:

$$|\varphi(x)| < \varepsilon_1^{\alpha_1}\varepsilon_2^{\alpha_2}\cdots\varepsilon_k^{\alpha_k}. \tag{10}$$

Пусть теперь c' — корень уравнения $f_1(x) = 0$; тогда по (8)

$$f(c') = -\varphi(c'); \tag{11}$$

c' лежит внутри круга радиуса R, но не в области g, ибо для последней было бы по (7) и (10):

$$|f(c')| > \varepsilon_1^{\alpha_1}\varepsilon_2^{\alpha_2}\cdots\varepsilon_k^{\alpha_k} > |\varphi(c')|,$$

а это противоречит равенству (11). Итак, *все корни уравнения* $f_1(x) = 0$ *лежат внутри кругов радиусов* $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_k$.

Рассмотрим круг радиуса ε_1 с центром c_1, пусть $c_1', c_1'', c_1''', \ldots$ — корни уравнения $f_1(x) = 0$, лежащие в этом круге, и $\alpha_1', \alpha_2'', \alpha_3''', \ldots$ — их кратности. Тогда

$$f_1(x) = \psi_1(x)(x - c_1')^{\alpha_1'}(x - c_1')^{\alpha_1''}(x - c_1''')^{\alpha_1'''}\cdots; \tag{12}$$

тут $\psi_1(x)$ — целая рациональная функция, которая в круге с радиусом ε_1 не обращается в нуль; но она в этом круге ограничена (§ 67, теорема 5), т. е. можно найти такое число $B > 0$, что в рассматриваемом круге (т. е. при $|x - c_1| \le \varepsilon_1$)

$$|\psi_1(x)| < B. \tag{13}$$

С другой стороны, пусть

$$f(x) = \psi(x)(x - c_1)^{\alpha_1}, \tag{14}$$

где $\psi(x) = (x - c_2)^{\alpha_2}\cdots(x - c_k)^{\alpha_k}$; пусть l — половина наименьшего из расстояний c_1 от $c_2, c_3, \ldots, c_k$; тогда для x, лежащих в круге радиуса ε_1:

$$|x - c_2|^{\alpha_2} > l^{\alpha_2}, \quad |x - c_3|^{\alpha_3} > l^{\alpha_3}, \ \ldots, \ |x - c_k|^{\alpha_k} > l^{\alpha_k};$$

следовательно:

$$|\psi 9x)| > A = l^{\alpha_2+\alpha_3+\ldots+\alpha_k}. \tag{15}$$

Далее, если x лежит в круге радиуса ε_1 или на его границе, то

$$|x - c_1'| < 2\varepsilon_1, \quad |x - c_1''| < 2\varepsilon_1, \quad |x - c_1'''| < 2\varepsilon_1, \ \ldots \tag{16}$$

Из (8) имеем:

$$|f(x)| = |f_1(x) - \varphi(x)| \le |f_1(x)| + |\varphi(x)|,$$

или по (14) и (12):

$$|\psi(x)| \cdot |x - c_1|^{\alpha_1} \le$$
$$\le |\psi_1(x)| \cdot |x - c_1'|^{\alpha_1'} \cdot |x - c_1''|^{\alpha_1''} \cdot |x - c_1'''|^{\alpha_1'''}\cdots + |\varphi(x)|;$$

на основании же (13), (15) и (16), беря x на границе круга радиуса ε_1 и принимая во внимание, что тогда $|x - c_1| = \varepsilon_1$, получим:

$$A \cdot \varepsilon_1^{\alpha_1} < B \cdot (2\varepsilon_1)^{\alpha_1'+\alpha_1''+\alpha_1'''+\ldots} + |\varphi(x). \tag{17}$$

Но уменьшая, если потребуется, еще больше наши пределы $\delta_1, \delta_2, \ldots, \delta_n$ приращений коэфициентов, мы можем достигнуть того, что будет:

$$|\varphi(x)| < \varepsilon_1^{\alpha_1} \cdot A',$$

где $A' < A$; тогда (17) дает:

$$A - A' < B \cdot 2^{\alpha'_1+\alpha''_1+\alpha'''_1+\ldots} \cdot \varepsilon_1^{-\alpha_1+\alpha'_1+\alpha''_1+\alpha'''_1+\ldots}. \tag{18}$$

Но мы можем взять ε_1 *как угодно малым*; A и A' не зависят от ε_1; с другой стороны, если $\alpha_1 < \alpha'_1 + \alpha''_1 + \alpha'''_1 + \ldots$, то при достаточно малом ε_1 (18) перестанет быть правильным; следовательно:

$$\alpha_1 \geq \alpha'_1 + \alpha''_1 + \alpha'''_1 + \ldots;$$

но к такому же выводу мы придем относительно корней уравнения $f_1(x) = 0$, лежащих внутри кругов с радиусами $\varepsilon_2, \ldots, \varepsilon_k$ (если надо, уменьшая еще дальше $\delta_1, \delta_2, \ldots, \delta_n$). Вводя для этих кругов соответствующие обозначения, получим:

$$\begin{gathered}\alpha_2 \geq \alpha'_2 + \alpha''_2 + \alpha'''_2 + \ldots,\\ \ldots\ldots\ldots\ldots\ldots\ldots,\\ \alpha_k \geq \alpha'_k + \alpha''_k + \alpha'''_k + \ldots,\end{gathered}$$

но сумма кратностей всех корней как уравнения $f(x) = 0$, так и уравнения $f_1(x) = 0$? одна и та же и равна n; следовательно, в последних формулах всюду верны знаки равенства, ибо вне кругов $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_k$, уравнение $f_1(x) = 0$, как мы выше видели, корней не имеет. Итак

$$\begin{gathered}\alpha_1 = \alpha'_1 + \alpha''_1 + \alpha'''_1 + \ldots, \quad \alpha_2 = \alpha'_2 + \alpha''_2 + \alpha'''_2 + \ldots,\\ \ldots, \ \alpha_k = \alpha'_k + \alpha''_k + \alpha'''_k + \ldots\end{gathered}$$

и наша теорема доказана.

Заметим что если свободный член a_n равен нулю, то нуль есть один из корней уравнения $f(x) = 0$ (простой, если $a_{n-1} \neq 0$, и кратный если кроме a_n, еще несколько последних коэфициентов равны нулю). Следовательно, если свободный член стремится к нулю, то по доказанной теореме по крайней мере один из корней стремится к нулю.

Пусть теперь высший коэфициент $a_0 \neq 1$, а также может меняться. Если a_0, то, разделив на него обе части уравнения, получим:

$$x^n + \frac{a_1}{a_0}x^{n-1} + \frac{a_2}{a_0}x^{n-2} + \ldots + \frac{a_n}{a_0} = 0,$$

т. е. предыдущий случай; а так как дроби $\frac{a_1}{a_0}, \frac{a_2}{a_0}, \ldots, \frac{a_n}{a_0}$ при $a_0 \neq 0$ являются непрерывными функциями от $a_0, a_1, a_2, \ldots, a_n$, то доказанная теорема верна и для этого случая. Для исследования случая, когда a_0 стремится к нулю, сделаем подстановку $x = \frac{1}{y}$; тогда наше уравнение после умножения обеих частей на y^n перейдет в следующее:

$$a_n y^n + a_{n-1}y^{n-1} + \ldots + a_1 y + a_0 = 0.$$

Если теперь a_0 стремится к нулю, то по крайней мере один из корней y стремится к нулю, а следовательно, соответствующий корень $x = \frac{1}{y}$ беспредельно возрастает. Итак:

Следствие 1. Если высший коэфициент a_0 стремится к нулю, то по крайней мере один из корней данного уравнения беспредельно возрастает.

Как известно (§ 57), кратные корни имеются тогда и только тогда, если левая часть уравнения $f(x)$ не взаимно простая со своей производной $f'(x)$. Беря $f(x)$ в общем виде (т. е. с буквенными коэфициентами $a_0, a_1, \ldots, a_n$) и находя по способу Эвклида (§ 52) общий наибольший делитель функций $f(x)$ и $f'(x)$, мы придем к последнему, постоянному остатку, который будет рациональной функцией от коэфициентов $a_0, a_1, \ldots, a_n$; обозначим эту функцию через D (она по существу есть дискриминант уравнения $f(x) = 0$ (§ 149 гл. VIII); приравняв D нулю, получим условие, при котором $f(x)$ и $f'(x)$ не взаимно простые, т. е. при котором уравнение $f(x) = 0$ имеет кратные корни; это условие $D = 0$ есть некоторое соотношение между коэфициентами $a_0, a_1, \ldots, a_n$. Если мы теперь дадим этим коэфициентам $a_0, a_1, \ldots, a_n$ приращения $h_0, h_1, h_2, \ldots, h_n$, то эти приращения даже при условиях $|h_k| < \delta_k$ можно будет выбрать так, чтобы D сделалось или осталось неравным нулю, т. е. чтобы уравнение $f_1(x) = 0$ имело только простые корни. Итак:

Следствие 2. Мы всегда можем дать коэфициентам уравнения такие, при этом сколь угодно малые приращения, чтобы вновь полученное уравнение имело только простые корни.

А отсюда непосредственно вытекает:

Следствие 3. α-кратный корень уравнения можно рассматривать как получившийся от слияния α простых корней.

§ 74. Алгебраические функции. Предыдущая теорема о непрерывности корней алгебраических уравнений не ставит никаких условий для коэфициентов $a_0, a_1, \ldots, a_n$; они могут быть независимыми переменными или непрерывными функциями от одной или нескольких независимых переменных, некоторые коэфициенты могут оставаться постоянными и т. п. Корни уравнения называются алгебраическими функциями от коэфициентов этого уравнения; но так как эти корни при подходящим образом подобранных изменениях коэфициентов могут иногда сливаться, могут и переходить один в другой, то они рассматриваются не как отдельные n функций, а как n ветвей одной и той же алгебраической функции. В самом общем виде алгебраическая функция определяется следующим образом: пусть $a_0, a_1, a_2, \ldots, a_n$ — целые рациональные функции от s переменных $t_1, t_2, \ldots, t_s$ [27]; тогда корни уравнения $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n$ в своей совокупности представляют алгебраическую функцию от $t_1, t_2, \ldots, t_s$; каждый корень дает одну из ветвей этой функции.

Особенно важен случай, когда $s = 1$, т. е. случай алгебраической функции одного переменного t. Из теоремы § 73 следует, что алгебраическая функция от t непрерывна при всех значениях t, при которых a_0 не обращается в нуль; при каждом значении t алгебраическая функция имеет вообще n различных значений, которые иногда сливаются друг с другом, именно, при таких значениях t, которые обращают в нуль дискриминант D данного уравнения; но D, будучи рациональной функцией от коэфициентов уравнения, есть также рациональная функция от t; следовательно, D есть алгебраическое уравнение с неизвестным t, т. е. оно

[27] Целой рациональной функцией от s переменных $t_1, t_2, \ldots, t_s$ называется многочлен вида $\sum A_{\alpha_1,\ldots,\alpha_s} t_1^{\alpha_1} \cdots t_s^{\alpha_s}$, где $A_{\alpha_1,\ldots,\alpha_s}$ — данные численные коэфициенты.

имеет только конечное число корней, следовательно, существует конечное число таких значений t (так называемых «*точек разветвления*» функции), для которых несколько ветвей алгебраической функции сливаются и вблизи которых они могут переходить друг в друга. Те значения t, при которых $a_0 = 0$, называются «*полюсами*» алгебраической функции; при них одна или несколько ветвей функции обращаются в бесконечность.

Подробно теорию алгебраических функций изучает так называемая теория *функций комплексного переменного*. Алгебра является источником алгебраических функций, но исследование их как функций к алгебре не относится.

Заметим, что целая рациональная функция $f(t)$ и дробная рациональная функция $\dfrac{f(t)}{g(t)}$ являются частными видами алгебраических функций: они суть корни уравнений первой степени:

$$x - f(t) = 0 \quad \text{и} \quad g(t) \cdot x - f(t) = 0.$$

§ 75. Алгебраические числа. Основная теорема о существовании корней алгебраических уравнений не ставит никаких условий для коэфициентов уравнения: они могут быть любыми комплексными числами (лишь бы высший коэфициент был отличен от нуля). Но практически нам приходится иметь дело исключительно с уравнениями, имеющими вещественные и даже рациональные коэфициенты. В тех случаях, когда рассматриваемый практический вопрос (например в технике) приводит к уравнениям с иррациональными коэфициентами, нам приходится брать их приближенные рациональные значения (обычно в форме десятичной дроби), а теорема о непрерывности корней (§ 73) говорит, что, взяв приближение коэфициентов с достаточной точностью, мы можем получить и корни с заданною наперед какою угодно точностью.

Итак, рассмотрим уравнение с рациональными коэфициентами; умножив обе части такого уравнения на общий знаменатель всех коэфициентов, мы получим уравнение с целыми коэфициентами, которое мы можем еще сократить на общий наибольший делитель этих коэфициентов, если он больше единицы. Поэтому, не нарушая общности, мы можем рассматривать уравнения с целыми, взаимно простыми коэфициентами; такие уравнения называются первообразными (подробнее о них речь будет в главе VI). Пусть дано такое уравнение:

$$a_0 x^n + a_1 x^{n-1} + a_2 x^{n-2} + \ldots + a_n = 0;$$

корни его называются *алгебраическими числами*; они могут быть вещественны или комплексны; в частном случае, корнями таких уравнений могут быть и рациональные, даже целые числа, которые являются, таким образом, частными случаями алгебраических чисел. Так называемые целые и рациональные комплексные числа, т. е. числа вида $a+bi$ с вещественными целыми, соответственно рациональными a и b, тоже являются алгебраическими числами, ибо они удовлетворяют уравнениям вида $x^2 - 2ax + (a^2 + b^2) = 0$ с целыми, соответственно рациональными коэфициентами. Обычные корни n-й степени из целых и дробных чисел — тоже алгебраические числа, ибо, например, $\sqrt[n]{a}$ есть корень уравнения $x^n - a = 0$ с целым или рациональным a. Доказано, что сумма, разность, произведение и частное

(при делителе неравном нулю) алгебраических чисел — тоже алгебраические числа, т. е. все алгебраические числа составляют тело (§ 13). Но это самое широкое алгебраическое тело, содержащее как вещественные, так и комплексные числа, имеет много делителей; одним из них, например, является совокупность всех вещественных алгебраических чисел, которая тоже является телом. Упомянутое в § 13 тело чисел вида $a+b\sqrt{2}$ с рациональными a и b — тоже алгебраическое, — делитель тела всех рациональных алгебраических чисел. Далее, доказано, что корни всякого алгебраического уравнения, все коэфициенты которого — алгебраические числа, являются тоже алгебраическими числами (т. е. корнями алгебраических уравнений с целыми рациональными коэфициентами). Возникает вопрос: исчерпывают ли алгебраические числа все комплексные и вещественные числа вообще? Или существуют еще числа неалгебраические, т. е. такие, которые не являются корнями никакого алгебраического уравнения с целыми коэфициентами. Оказывается, что такие числа действительно существуют; в отличие от алгебраических их называют *трансцендентными*; это название ввел Лейбниц (Leibnitz) в 1686 г. Лиувилль (Liouville) в 1844 г. первый строго доказал существование вещественных трансцендентных чисел; гораздо более простое доказательство этому дал Г. Кантор (G. Cantor) в 1874 г. В 1876 г. Эрмит (Hermite) доказал трансцендентность числа e (основания натуральных логарифмов), а в 1882 г. Линдеман (Lindemann) доказал трансцендентность числа π. Наконец, в 1929 г. Гельфонд (в Москве) доказал трансцендентность числа e^{π}.

Главная идея доказательства Г. Кантора состоит в том, что множество всех вещественных алгебраических чисел исчислимо или счетно, т. е. все эти числа можно расположить в ряд, где каждое число получит определенный конечный номер, и номера разных чисел будут различны, тогда как множество вообще всех вещественных чисел неисчислимо, т. е. их нельзя расположить в такой ряд (нельзя не потому, что не удалось, а строго доказано, что и не может удасться). Следовательно, кроме алгебраических существуют еще трансцендентные числа; при этом доказывается, что множество одних только трансцендентных чисел тоже неисчислимо [28].

Подробное исследование алгебраических чисел относится к теории чисел и составляет особую ветвь последней, так называемую алгебраическую теорию чисел; эта ветвь стоит, конечно, в самой тесной связи с алгеброй. Следует заметить, что алгебраические числа изучены весьма подробно; среди них выделен особый класс так называемых *целых алгебраических чисел*; это — корни уравнений с целыми коэфициентами и с высшим коэфициентом, равным единице. Построена теория делимости целых алгебраических чисел в данном алгебраическом теле; эта теория является обобщением теории делимости обычных целых чисел и приводит к рассмотрению особых систем целых чисел, так называемых «идеалов» (гл. XIV) [29].

[28] Подсобное доказательство читатель может найти хотя бы в книге Александрова и Колмогорова «Введение в теорию функций действительного переменного».

[29] Хотя и раньше в России, и сейчас в СССР были и есть большие специалисты в алгебраической теории чисел (например, Вороной, Золотарев, Делоне, Венков), но, как это ни странно, на русском языке нет по этому отделу ни одного учебника (не считая литографированных лекций академика Граве, являющихся библиографической редкостью, и небольшого отдела в его «Элементарном курсе теории чисел»). На украинском языке недавно вышла книга Гекке «Теория алгебраических чисел» (перевод с немецкого).

§ 76. Общие замечания. Основная теорема о существовании корней алгебраических уравнений принадлежит к так называемым «теоремам, или доказательствам существования» («Existenzbeweise»): доказывается существование определенных объектов (в данном случае — корней алгебраических уравнений), но совершенно не указывается, где их отыскивать, как их найти, да и вообще принципиально возможно ли их найти. Некоторые доказательства этой теоремы (например доказательство Lipschitz'a) имеют своею целью избежать указанный недостаток: там дается построение последовательности чисел $a_1, a_2, a_3, \ldots$ таких, что $\lim\limits_{n\to\infty} a_n = x$ и есть искомый корень уравнения, иными словами, дается средство подойти к корню как угодно близко, но это делается чисто теоретически, практически же этот путь, можно сказать, неосуществим.

В чем же значение теоремы о существовании корней?

Раньше ее считали основной теоремой алгебры; сейчас, в связи с развитием совершенно новых областей в алгебре, такого значения этой теореме не придают: теорема эта относится только к атгебре обычных комплексных чисел, т. е. только к одной из многих существующих алгебр (правда, практически очень важной); она говорит, что в теле всех комплексных чисел всякая целая рациональная функция одного переменного раскладывается на линейные множители; это иначе выражается так: тело комплексных чисел *алгебраически замкнуто* (т. е. его уже нельзя больше алгебраически расширить). Это, конечно, очень важное свойство тела комплексных чисел. Заметим, что доказывается оно на основании свойства непрерывности тела комплексных чисел; это свойство очень существенно, и ни одно доказательство не обходится без его применения в той или иной форме. Но для алгебраической замкнутости тела свойство непрерывности не необходимо: например, тело всех алгебраических (как вещественных, так и комплексных) чисел тоже алгебраически замкнуто (что следует из § 75), но оно не непрерывно.

В следующей главе мы займемся фактическим решением уравнений (с вещественными коэфициентами), т. е. приближенным вычислением их корней. Теорема о существовании корней является общей основой, общим, так сказать, оправданием этих вычислений, общим их синтезом; она дает уверенность в том, что эти вычисления не производятся впустую, что вычисляемая величина действительно существует. В этом ее глубокое значение. И поскольку она находит свое дополнение в практике вычисления корней, нет ничего страшного в том, что она дает лишь «доказательство существования»: она просто сложит теоретической основой для практики.

ГЛАВА ПЯТАЯ

УРАВНЕНИЯ С ВЕЩЕСТВЕННЫМИ КОЭФИЦИЕНТАМИ; ВЫЧИСЛЕНИЕ КОРНЕЙ

§ 77. Свойства целых функций с вещественными коэфициентами. Теорема Ролля. В настоящий главе мы будем предполагать, что коэфициенты всех наших функций вещественные; в этом случае при вещественных значениях X значения функций будут тоже вещественными и к ним можно применять теорию вещественных функций от вещественного переменного.

Теорема. *При достаточно малом $|x|$ целая рациональная функция имеет знак своего низшего члена; при достаточно большом $|x|$ она имеет знак своего высшего члена.*

Доказательство. Положим для общности, что наинизший не равный нулю член содержит x в m-й степени; пусть

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-m}x^m, \qquad m \leq n, \qquad a_0 \neq 0, \qquad a_{n-m} \neq 0.$$

Имеем:

$$\begin{aligned} f(x) &= x^m(a_0x^{n-m} + a_1x^{n-m-1} + \ldots + a_{n-m-1}x + a_{n-m}) = \\ &= x^m \cdot [\varphi(x) + a_{n-m}], \end{aligned}$$

где $\varphi(x) = a_0x^{n-m} + a_1x^{n-m-1} + \ldots + a_{n-m-1}x$; по теореме § 64 при достаточно малом x будет: $|\varphi(x)| < a_{n-m}$, т. е. знак $\varphi(x) + a_{n-m}$ будет тот же, что и у a_{n-m}; следовательно, знак у $f(x)$ будет тот же, что и у $a_{n-m}x^m$, и первая часть теоремы доказана.

Для доказательства второй части положим: $x = \dfrac{1}{z}$, $f(x) = x^n \cdot (a_0 + a_1z + \ldots + a_{n-m}z^{n-m}$; согласно первой части функция $a_0+a_1z+\ldots+a_{n-m}z^{n-m}$ при достаточно малом $|z|$ будет иметь тот же знак, что и a_0; следовательно, при достаточно малом $|z|$, или, так как $z = \dfrac{1}{x}$, при достаточно большом $|x|$ функция $f(x)$ будет иметь тот же знак, что и a_0x^n, и теорема доказана.

Обозначение. Символ $\operatorname{sign} a$ означает $+1$, если $a > 0$, -1, если $a < 0$ и 0, если $a = 0$ (sign — сокращение слова signum — знак).

§ 78. Теорема. *Если $f(x)$ — непрерывная функция в замкнутом интервале (a, b) и $f(a)$ и $f(b)$ имеют разные знаки, то между a и ? лежат по крайней мере один корень уравнения $f(x) = 0$.*

Эта теорема собственно не принадлежит алгебре, хотя алгебра пользуется ею; мы здесь ее докажем для полноты.

Доказательство. Разделим все точки интервала (a, b) на два класса: точку c мы относим к первому классу, если в интервале (a, c) функция $f(x)$ не меняет знака:

$$\operatorname{sign} f(x) = \operatorname{sign} f(a);$$

точку C мы относим ко второму классу, если в интервале (a, C) функция $f(x)$ меняет знак: $\operatorname{sign} f(x)$ не равен все время $\operatorname{sign} f(a)$. Это деление есть сечение Дедекинда, ибо в каждом классе есть точки; например, точка a принадлежит к первому классу, точка b — ко второму. Каждая точка в (a, b) принадлежит к одному и только к одному классу. Очевидно, что все точки первого класса левее всех точек второго класса (или всякое c меньше всякого C). Это сечение определяет число x_0; все числа большие x_0 — второго класса, а меньшие x_0 — первого класса. Докажем, что $f(x_0) = 0$. Пусть это неверно; пусть $|f(x_0)| = k > 0$; так как $f(x)$ непрерывна при $x = x_0$, то при $|x - x_0|$, меньшем некоторого числа δ, $|f(x) - f(x_0)|$ будет меньше k, т. е. $-k < f(x) - f(x_0) < +k$; $f(x_0) = \pm k$; следовательно, если $f(x_0) = +k$, то $f(x) > 0$; если $f(x_0) = -k$, то $f(x) < 0$, т. е. $\operatorname{sign} f(x) = \operatorname{sign} f(x_0)$ при всяком x, удовлетворяющем условию $|x - x_0| < \delta$, т. е. при $x_0 - \delta < x < x_0 + \delta$. Отсюда заключаем: если $\operatorname{sign} f(x_0) = \operatorname{sign} f(a)$, то все точки в интервале $(x_0, x_0 + \delta)$ — первого класса, ибо для них тоже $\operatorname{sign} f(x) = \operatorname{sign} f(x_0) = \operatorname{sign} f(a)$; но это неверно. Если же $\operatorname{sign} f(x_0) = \operatorname{sign} f(b)$, то все точки в интервале $(x_0 - \delta, x_0)$ — второго класса, что тоже неверно. Остается положить $f(x_0) = 0$, и теорема доказана.

Конечно, может случиться, что x_0 не единственный корень в интервале (a, b); в этом интервале могут быть и другие корни уравнения $f(x) = 0$, только все они больше, чем x_0.

Геометрическое представление этой теоремы изображено на черт. 13: если точки A и B лежат по разные стороны от оси X, то всякая кривая, соединяющая A и B, должна по крайней мере один раз пересечь ось X. Геометрически это очевидно.

Следствие I. Если в замкнутом интервале (a, b) $f(x)$ — непрерывная функция, то она в этом интервале принимает но крайней мере один раз всякое значение, лежащее между $f(a)$ и $f(b)$.

Доказательство. Пусть число C лежит между числами $f(a)$ и $f(b)$; возьмем функцию $\varphi(x) = f(x) - C$; тогда $\varphi(a) = f(a) - C$ и $\varphi(b) = f(b) - C$ имеют разные знаки; следовательно, по предыдущей теореме для некоторого значения $x = x_0$ внутри интервала (a, b) $\varphi(x_0) = f(x_0) - C = 0$, т. е. $f(x_0) = C$, что и требовалось доказать.

Это свойство раньше принимали за определение непрерывности, функции, однако, оказалось, что им обладают и некоторые разрывные функции; при современном, более тонком определении непрерывности это свойство далеко не так очевидно, как может показаться сначала. Так как ц. р. функция непрерывна для всякого x, то предыдущая теорема применима и к ц. р. функциям. Отсюда заключаем:

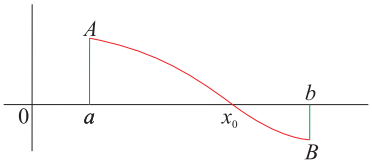
Следствие II. Всякое. уравнение нечетной степени имеет по крайней мере один вещественный корень [30].

Доказательство. При достаточно большом $|x|$ ц. р. функция не обращается в нуль (§ 65) и имеет знак своего высшего члена $a_0 x^n$; но этот член имеет разные

[30] Напоминаем, что все коэфиииенты наших уравнений мы предполагаем вещественными.

знаки при $x > 0$ и при $x < 0$; следовательно, по доказанной теореме такая ц. р. функция должна обращаться в нуль при некотором вещественном x.

Следствие III. Всякое уравнение четной степени, в котором высший коэфициент и свободный член имеют разные знаки, имеет по крайней мере два вещественных корня: один положительный и один отрицательный.



Черт. 13

Доказательство. При достаточно большом $|x|$ левая часть уравнения имеет знак своего высшего коэфициента a_0 как при $x > 0$, так и при $x < 0$; при $x = 0$ левая часть уравнения обращается в свободный член a_n так как знаки a_0 и a_n различны, то из теоремы этого параграфа и следует существование одного положительного и одного отрицательного корня: [31].

Следствие IV. Если непрерывная функция не обращается в нуль в интервале (a, b), то она в нем не меняет знака.

Это непосредственно следует из теоремы в начале этого параграфа.

Теорема. *Если x, возрастая, проходит через m-кратный корень уравнения $f(x) = 0$, то знак функции $f(x)$ умножается на $(-1)^m$, т. е. если m — четное, она не меняет знака, если же m нечетное, она меняет знак.*

Доказательство. Пусть x_0 m-кратный корень для $f(x) = 0$; тогда (§ 50) имеем: $f(x) = (x - x_0)^m \cdot \varphi(x)$, где $\varphi(x_0) \neq 0$. При проходе x через x_0 $\varphi(x)$не меняет знака, тогда как $(x - x_0)^m$ меняет знак или нет, смотря по тому, будет ли m нечетным или четным. Отсюда и вытекает наша теорема.

Следствие I. Если в интервале (a, b) лежит нечетное число корней уравнения $f(x) = 0$, то $\operatorname{sign} f(a) = -\operatorname{sign} f(b)$; если же в этом интервале лежит четное число корней уравнения $f(x) = 0$, то $\operatorname{sign} f(a) = \operatorname{sign} f(b)$. (При этом для каждого корня считается и его кратность.)

Следствие II. Если $\operatorname{sign} f(a) = \operatorname{sign} f(b)$, то в интервале (a, b) лежит четное число корней уравнения $f(x) = 0$ (т. е. может и не быть ни одного); если же $\operatorname{sign} f(a) = -\operatorname{sign} f(b)$, то в интервале (a, b) лежит нечетное число корней уравнения $f(x) = 0$ (и, значит, по крайней мере один). Для каждого корня считается и его кратность.

§ 79. Теорема. *Если $f'(x_0) \neq 0$ и если x, возрастая, проходит через x_0, то целая рациональная функция $f(x)$ при этом возрастает или убывает, смотря по тому, будет ли $f'(x_0) > 0$ или < 0* [32].

Доказательство. По формуле Тэйлора [§ 54, (4)]:

$$f(x_0 + h) - f(x_0) = hf'(x_0) + \frac{h^2}{2!}f''(x_0) + \ldots;$$

[31] Уравнение же четной степени, в котором знаки у a_0 и a_n одинаковы, может и совсем не иметь вещественных корней; например, $x^2 + 1 = 0$.

[32] Теоремы этого параграфа верны не только для целых рациональных функций.

правая часть — ц. р. функция от h; она (по § 77) при достаточно малом h имеет знак своего низшего члена, т. е. $hf'(x_0)$; отсюда следует при достаточно малом h: если $f'(x_0) > 0$, то для $h > 0$ $f(x_0+h) - f(x_0) > 0$, для $h < 0$ $f(x_0+h) - f(x_0) < 0$, если $f'(x_0) < 0$, то для $h > 0$ $f(x_0+h) - f(x_0) < 0$, для $h < 0$ $f(x_0+h) - f(x_0) > 0$.

Этим и доказывается наша теорема.

Теорема. *Если x, возрастая, проходит через корень уравнения $fx) = 0$, то $\dfrac{f(x)}{f'(x)}$ переходит при этом от отрицательных значений к положительным.*

Доказательство. Пусть x_0 — m-кратный корень уравнения $f(x) = 0$ (в частном случае может быть $m = 1$); тогда x_0 будет $(m-1)$-кратный корень уравнения $f'(x) = 0$ (§ 57, теорема 1).

Имеем:

$$f(x_0+h) = \frac{h^m}{m!}f^{(m)}(x_0) + \frac{h^{m+1}}{(m+1)!}f^{(m+1)}(x_0) + \dots$$

$$f'(x_0+h) = \frac{h^{m-1}}{(m-1)!}f^{(m)}(x_0) + \frac{h^m}{m!}f^{(m+1)}(x_0) + \dots$$

(§ 57); следовательно,

$$\frac{f(x_0+h)}{f'(x_0+h)} = \frac{\dfrac{1}{m!}f^{(m)}(x_0) + \dfrac{h}{(m+1)!}f^{(m+1)}(x_0) + \dots}{\dfrac{1}{(m-1)!}f^{(m)}(x_0) + \dfrac{h}{m!}f^{(m+1)}(x_0) + \dots}.$$

При достаточно малом $|h|$ числитель и знаменатель дроби правой части будут иметь знак первого члена (§ 77), т. е. дробь будет положительна; значит, $\dfrac{f(x_0+h)}{f'(x_0+h)}$ будет иметь тот же знак, что и h: при $h < 0$ и $\dfrac{f(x_0+h)}{f'(x_0+h)} < 0$, при $h > 0$ и $\dfrac{f(x_0+h)}{f'(x_0+h)} > 0$; этим наша теорема доказана.

Теорема Ролля (Rolle). *Между двумя соседними корнями a и b уравнения $f(x) = 0$ всегда лежит по крайней мере один корень уравнения $f'(x) = 0$.*

Доказательство. По предыдущей теореме, при достаточно малом $h > 0$ будет $\dfrac{f(a+h)}{f'(a+h)} > 0$ и $\dfrac{f(b-h)}{f'(b-h)} < 0$, но по следствию IV, в интервале (a, b) $f(x)$ не меняет знака; следовательно, $f'(a+h)$ и $f'(b-h)$ имеют разные знаки, т. е. (по первой теореме § 78) в интервале (a, b) лежит по крайней мере один корень уравнения $f'(x) = 0$.

Следствие. Если все корни уравнения $f(x) = 0$ вещественны, то и все корни уравнения $f'(x) = 0$ тоже вещественны.

Доказательство. Пусть $a_1 < a_2 < \dots < a_k$ — все различные вещественные корни уравнения $f(x) = 0$, $m_1, m_2, \dots, m_k$ — их кратности; n, где $m_1 + m_2 + \dots + m_k = n$ — степень уравнения. Для уравнения $f'(x) = 0$ корни $a_1, a_2, \dots, a_k$ имеют кратности: $m_1 - 1, m_2 - 1, \dots, m_k - 1$ (по § 57, теорема 1); кроме того, по теореме Ролля уравнение $f'(x) = 0$ имеет по крайней мере по одному корню: между a_1 и a_2, между a_2 и a_3, …, между a_{k-1} и a_k, т. е. всего $f'(x) =0$ имеет вещественных

корней не меньше

$$(m_1 - 1) + (m_2 - 1) + \ldots + (m_k - 1) + (k - 1) =$$
$$= m_1 + m_2 + \ldots + m_k - k + k - 1 = n - 1;$$

но так как уравнение $f'(x) = 0$ $(n-1)$-й степени, то это — все его корни; они вещественны.

Следствие. Если все корни уравнения: $f(x) = 0$ вещественны и различны, то и все корни уравнения $f'(x) = 0$ вещественны и различны.

Доказательство. Это вытекает из предыдущего следствия: если $m_1 = m_2 = \ldots = m_k = 1$ и $k = n$, то $f'(x) = 0$ имеет только следующие $n - 1$ вещественных корней; один между a_1 и a_2, один между a_2 и a_3 и т. д., один между a_{n-1} и a_n.

Дополнение. В этом случае и все корни уравнений: $f''(x) = 0$, $f'''(x) = 0$, ... вещественны и различны, и между всякими двумя соседними корнями уравнения $f^{(\lambda)}(x) = 0$ лежит один и только один корень уравнения $f^{(\lambda+1)}(x) = 0$.

§ 80. Комплексные корни уравнений с вещественными коэфициентами. Пусть $f(x)$ — данная ц. р. функция; подставим в нее $x = \alpha + \alpha i$; пусть $f(\alpha + \beta i) = P + Qi$, где P и Q вещественны; если мы подставим $x = \alpha - \beta i$, то это сведется к тому, что мы в $f(\alpha + \beta i)$ подставим $-i$ вместо i, ибо все коэфициенты в $f(x)$ вещественны. Итак, $f(\alpha - \beta i) = P - Qi$. Отсюда следует: если $f(\alpha + \beta i) = 0$, то и $f(\alpha - \beta i) = 0$. Пусть $\alpha + \beta i$ — m-кратный корень уравнения $f(x) = 0$; тогда (§ 57, теорема 2) $f(\alpha + \beta i) = 0$, $f'(\alpha + \beta i) = 0$, ..., $f^{(m-1)}(\alpha + \beta i) = 0$, но $f^{(m)}(\alpha + \beta i) \neq 0$; но так как $f, f', f'', \ldots, f^{(m-1)}, f^{(m)}$, — ц. р. функции с вещественными коэфициентами, то и $f(\alpha - \beta i) = 0$, $f'(\alpha - \beta i) = 0$, ..., $f^{(m-1)}(\alpha - \beta i) = 0$, но $f^{(m)}(\alpha - \beta i) = 0$ [ибо иначе было бы и $f^{(m)}(\alpha + \beta i) = 0$]; следовательно (по § 57, теорема 2), и $\alpha - \beta i$ является m-кратным корнем уравнения ?. Итак:

Теорема. *В уравнение с вещественными коэфициентами комплексные корни входят всегда парами: если $\alpha + \beta i$ — корень, то и $\alpha - \beta i$ — корень той же самой кратности, что и $\alpha + \beta i$.*

В разложении ц. р. функции $f(x)$ на линейные множители (§ 50) можно соединить множители, соответствующие сопряженным комплексным корням; произведение двух таких множителей есть квадратная функция с вещественными коэфициентами, именно:

$$(x - \alpha - \beta i)(x - \alpha + \beta i) = (x - \alpha)^2 + \beta^2 = x^2 - 2\alpha x + \alpha^2 + \beta^2.$$

Итак:

Теорема. *Всякая целая рациональная функция с вещественными коэфициентами раскладывается и притом только одним образом на вещественные сомножители первой и второй степеней, причем сомножители второй степени имеют мнимые корни.*

§ 81. Вещественные простейшие дроби. Дробная рациональная функция с вещественными коэфициентами может быть разложена на вещественные простейшие дроби.

Именно, пусть $\dfrac{f(x)}{g(x)}$ — такая функция; разложим $g(x)$ на вещественные множители первой и второй степеней и пусть $(x^2 + ax + b)^m$ — один из множите-

лей знаменателя, соответствующий двум сопряженным комплексным корням m-й кратности. Пусть $g(x) = (x^2 + ax + b)^m \cdot g_1(x)$; функции $(x^2 + ax + b)^m$ и $g_1(x)$ — взаимно простые; следовательно, по теореме § 60:

$$\frac{f(x)}{g(x)} = \frac{F(x)}{(x^2 + ax + b)^m} + \frac{f_1(x)}{g_1(x)}.$$

Если $\dfrac{f(x)}{g(x)}$ — правильная дробь, то и обе дроби правой части могут быть взяты правильными, т. е. $F(x)$ — ц. р. функция степени $\leq m - 1$. Разделим $F(x)$ на $x^2 + ax + b$; пусть $F(x) = (x^2 + ax + b) \cdot F_1(x) + Ax + B$ (§ 47); тогда

$$\frac{F(x)}{(x^2 + ax + b)^m} = \frac{F_1(x)}{(x^2 + ax + b)^{m-1}} + \frac{Ax + B}{(x^2 + ax + b)^m};$$

разделим теперь $F_1(x)$ на $x^2 + ax + b$ и подобным же образом найдем:

$$\frac{F_1(x)}{(x^2 + ax + b)^{m-1}} = \frac{F_2(x)}{(x^2 + ax + b)^{m-2}} + \frac{A_1x + B_1}{(x^2 + ax + b)^{m-1}}$$

и т. д.; окончательно найдем:

$$\frac{F(x)}{(x^2 + ax + b)^m} = \frac{Ax + B}{(x^2 + ax + b)^m} + \frac{A_1x + B_1}{(x^2 + ax + b)^{m-1}} + \ldots + \frac{A_{m-1}x + B_{m-1}}{x^2 + ax + b}.$$

Здесь все количества A, B, A_1, B_1, …, A_{m-1}, B_{m-1} — вещественны; A и B одновременно не равны нулю (если дробь $\dfrac{f(x)}{g(x)}$ несократима), количества же A_1, B_1, …, A_{m-1}, B_{m-1} могут быть и все равны нулю. Найти количества A, B, A_1, B_1, … можно способом неопределенных коэфициентов. Итак:

Теорема. *Всякая дробная рациональная функция с вещественными коэфициентами раскладывается на вещественные простейшие дроби; при этом те части разложения, которые соответствуют вещественным корням знаменателя, имеют тот же вид, что в* § 60, (14)*; часть же, соответствующая сопряженным комплексным корням m-й кратности, имеет вид:*

$$\frac{Ax + B}{(x^2 + ax + b)^m} + \frac{A_1x + B_1}{(x^2 + ax + b)^{m-1}} + \ldots + \frac{A_{m-1}x + B_{m-1}}{x^2 + ax + b}.$$

Пример 1..

$$\frac{x^2 + x + 1}{x^4 - 1} = \frac{x^2 + x + 1}{(x^2 + 1)(x - 1)(x + 1)} = \frac{A}{x - 1} + \frac{B}{x + 1} + \frac{Cx + D}{x^2 + 1};$$

приводя к общему знаменателю, найдем:

$$x^2 + x + 1 = A(x + 1)(x^2 + 1) + B(x - 1)(x^2 + 1) + (Cx + D)((x^2 - 1);$$

сравнивая коэфициенты при одинаковых степенях x, найдем:

$$\left.\begin{aligned} A + B + C &= 0, \\ A - B + D &= 1, \\ A + B - C &= 1, \\ A - B - D &= 1; \end{aligned}\right\}$$

отсюда

$$C = -\frac{1}{2}, \quad D = 0, \quad A = \frac{3}{4}, \quad B = -\frac{1}{4};$$

следовательно:

$$\frac{x^2+x+1}{x^4-1} = \frac{3}{4(x-1)} - \frac{1}{4(x+1)} - \frac{x}{2(x^2+1)}.$$

Пример 2.

$$\frac{x}{(x^2+x+1)^2(x^2+1)} = \frac{Ax+B}{(x^2+x+1)^2} + \frac{A_1x+B_1}{x^2+x+1} + \frac{Cx+D}{x^2+1}$$

приводя к общему знаменателю, найдем:

$$x = (Ax+B)(x^2+1) + (A_1x+B_1)((x^2+x+1)(x^2+1) + (Cx+D)(x^2+x+1)^2;$$

сравнивая коэфициенты при одинаковых степенях x, получим:

$$\begin{aligned}
&A_1 + C = 0, \quad A_1 + B_1 + 2C + D &&= 0,\\
&A + 2A_1 + B_1 + 3C + 2D &&= 0,\\
&B + A_1 + 2B_1 + 2C + 3D &&= 0,\\
&A + A_1 + B_1 + C + 2D &&= 1,\\
&B + B_1 + D &&= 0.
\end{aligned}$$

Решив эти уравнения, получим:

$$C = -1, \quad B = -1, \quad A_1 = 1, \quad A = 0, \quad D = 0, \quad B_1 = 1;$$

следовательно:

$$\frac{x}{(x^2+x+1)^2(x^2+1)} = -\frac{1}{(x^2+x+1)^2} + \frac{x+1}{x^2+x+1} - \frac{x}{x^2+1}.$$

Упражнения

Разложить на простейшие дроби:

111) $\dfrac{x^2+1}{(x^2+2x+2)^3}$.

Отв. $-\dfrac{2x+1}{(x^2+2x+2)^3} + \dfrac{1}{(x^2+2x+2)^2}$.

112) $\dfrac{x}{(x^2-2x+2)(x^2+x+1)}$.

Отв. $\dfrac{6-x}{13(x^2-2x+2)} + \dfrac{x-3}{13(x^2+x+1)}$.

113) $\dfrac{2x+1}{(x-1)^2(x^2-3x+4)}$.

Отв. $\dfrac{3}{2(x-1)^2} + \dfrac{7}{4(x-1)} + \dfrac{8-7x}{4(x^2-3x+4}$.

114) $\dfrac{x^3}{(x^2+1)^3}$.

Отв. $-\dfrac{x}{(x^2+1)^3}+\dfrac{x}{(x^2+1)^2}$.

§ 82. Пределы вещественных корней. Переходя к фактическому решению уравнения с вещественными коэфициентами, в частности — к вычислению его вещественных корней, мы расчленим эту общую проблему на следующие три более специальные задачи:

1) *Нахождение пределов вещественных корней*, т. е. нахождение таких чисел a и b, между которыми лежат все вещественные корни; специально — нахождение пределов положительных корней и пределов отрицательных корней.

2) *Отделение корней*, т. е. нахождение таких интервалов, в каждом из которых лежит только по одному вещественному корню, а также нахождение числа корней, лежащих в данном интервале.

3) *Вычисление корней*, т. е. приемы, позволяющие возможно быстро вычислить вещественные корни с любой точностью.

Переходя к задаче 1), заметим, что теорема 3 § 65 собственно уже решает эту задачу: если выведенное там число $K=\alpha+1$ есть верхний предел абсолютной величины всех корней уравнения, то ясно, что все вещественные корни этого уравнения находятся в интервале $(-K,+K)$. Но этот интервал вообще слишком велик; мы укажем способы нахождения более выгодных пределов вещественных корней. При этом нам достаточно уметь находить только верхний предел положительных корней: именно, в данном уравнении $f(x)=0$ сделаем подстановку $x=\frac{1}{z}$ и получим некоторое уравнение $\varphi(z)=0$; если K — верхний предел положительных корней, уравнения $\varphi(z)=0$, то $\dfrac{1}{K}$ будет нижним пределом положительных корней данного уравнения $f(x)=0$. Подобным же образом, если в данном уравнении сделаем подстановку $x=-t$, то найдем нижний (в алгебраическом смысле) предел отрицательных корней данного уравнения. Наконец, сделав подстановку $u=-\dfrac{1}{x}$, мы аналогично найдем и верхний (в алгебраическом смысле) предел отрицательных корней данного уравнения.

§ 83. Различные способы нахождения верхнего предела положительных корней. *Первый способ* (*Маклорена*). Если в уравнении

$$f(x)=a_0x^n+a_1x^{n-1}+\ldots+a_n,\qquad a_0>0$$

a_m — первый отрицательный коэфициент в ряде $a_0,a_1,a_2,\ldots$, и a — наибольший по абсолютной величине из отрицательных коэфициентов, то

$$K_1=1+\sqrt[m]{\frac{|a|}{a_0}}$$

можно принять за верхний предел положительных корней данного уравнения.

Доказательство. Очевидно, что при значениях $x>0$ будет:

$$f(x)>a_0x^n-|a|(x^{n-m}+x^{n-m-1}+\ldots+x+1),$$

или, суммируя стоящую в скобках геометрическую прогрессию:

$$f(x)>a_0x^n-|a|\cdot\frac{x^{n-m-1}-1}{x-1}>a_0x^n-\frac{|a|x^{n-m-1}}{x-1},$$

или

$$f(x) > \frac{a_0 x^{m-1}(x-1) - |a|}{x-1}\, x^{n-m-1}.$$

Пусть теперь

$$x > 1 + \sqrt[m]{\frac{|a|}{a_0}};$$

тогда

$$x^m > (x-1)^m \geq \frac{|a|}{a_0},$$

$$f(x) > \frac{a_0(x-1)^m - |a|}{x-1}\, x^{n-m-1} \geq 0,$$

т. е. при этих значениях x $f(x) > 0$, что и доказывает наше предложение.

Второй способ. Не переставляя членов в нашей ц. р. функции $f(x)$, представим ее в виде суммы $f(x) = \varphi_1(x) + \varphi_2(x) + \ldots$, где $\varphi_1(x), \varphi_2(x), \ldots$ — полиномы, каждый из которых содержит только одну перемену знака в ряде его коэфициентов (причем последний из этих полиномов может и совсем не иметь ни одной перемены знака); если при $x = a > 0$ все эти полиномы положительны: $\varphi_1(a) > 0, \varphi_2(a) > 0, \ldots$, то a можно принять за верхний предел положительных корней уравнения $f(x) = 0$.

Доказательство. Нам достаточно доказать, что если $\varphi_\varkappa(a) > 0$, то при $x > a$ будет также $\varphi_\varkappa(a0 > 0$. Пусть

$$\varphi_\varkappa(x) = a_0 x^m + a_1 x^{m-1} + \ldots + a_k x^{m-k} - a_{k+1} x^{m-k-1} - \ldots - a_l x^{m-l},$$

где все $a_\lambda > 0$; $m \geq l > k > 0$. Имеем:

$$\varphi_\varkappa(x) = x^{m-k} \cdot \left[(a_0 x^k + a_1 x^{k-1} + \ldots + a_k) - \left(\frac{a_{k+1}}{x} + \ldots + \frac{a_l}{x^{l-k}} \right) \right];$$

так как с увеличением x функция в первых скобках возрастает, а функция во вторых скобках уменьшается, то $\varphi_\varkappa(x)$ возрастает вместе с x при $x > 0$; следовательно, при $x > a$

$$\varphi_\varkappa(x) > \varphi_\varkappa(a) > 0.$$

Третий способ (*Ньютона*). Если при $x = a > 0$ как сама ц. р. функция $f(x)$, так и все ее производные (которые не равны тождественно нулю) положительны, то a можно принять за верхний предел положительных корней уравнения.

Доказательство. Это непосредственно следует из формулы Маклорена (5) § 54, ибо в таком случае при $x > a$ $f(x)$ представляется по этой формуле как сумма положительных слагаемых.

Пример. Найти пределы вещественных корней уравнения:

$$f(x) = x^7 + 3x^6 + 6x^5 - 4x^4 + 2x^3 - x^2 + 2x + 4 = 0.$$

Для верхнего предела положительных корней теорема 3 § 65 дает число

$$6 + 1 = 7.$$

Первый способ дает:

$$1 + \sqrt[3]{4} < 2.$$

Второй способ:

$$f(x) = \varphi_1(x) + \varphi_2(x) + \varphi_3(x),$$

где

$$\varphi_1(x) = x^7 + 3x^6 + 6x^5 - 4x^4, \qquad \varphi_2(x) = 2x^3 - x^2, \qquad \varphi_3(x) = 2x + 4;$$

очевидно, что $\varphi_1(1) > 0$, $\varphi_2(1) > 0$, $\varphi_3(1) > 0$; следовательно, за верхний предел положительных корней можно принять число 1.

Третий способ удобно применять, пользуясь способом Горнера, — разложения $f(x)$ по степеням $x - a$ (§ 55); коэфициенты этого разложения и будут $f(a), f'(a), \frac{1}{2!}f''(a), \ldots$ При этом, если в процессе применения этого способа мы получим строку со всеми положительными числами, то на этом мы можем уже остановиться, ибо все дальнейшие числа будут тоже положительными. Так, в нашем примере, беря $a = 1$, будем иметь:

	1	3	6	−4	2	−1	2	4
1	1	4	10	6	8	7	9	13

.

Дальше можно не вычислять; ясно, что все получаемые в дальнейшем числа будут положительны. Берем еще $a = 0,5$:

	1	3	6	−4	2	−1	2	4
0,5	1	3,5	7,75	−0,125	1,9375	−0,03125	1,984375	4,9921875
0,5	1	4	9,75	4,75	4,3125	2,125		

.

На этом останавливаемся, ибо все дальнейшие числа будут положительными. Итак, за верхний предел положительных корней можно принять $0,5$. Мы видим, что способ Ньютона оказался в этом случае самым выгодным.

Для нижнего предела положительных корней делаем подстановку $x = \frac{1}{z}$ и получаем:

$$4z^7 + 2z^6 - z^5 + 2z^4 - 4z^3 + 6z^2 + 3z + 1 = 0;$$

для этого уравнения находим верхний предел положительных корней.

Теорема 3 § 65 дает $1 + \frac{6}{4} = 2\frac{1}{2}$, т. е. нижний предел положительных корней данного уравнения равен $\frac{2}{5}$.

Первый способ дает $1 + \sqrt{\frac{4}{4}}$, т. е. нижний предел положительных корней данного уравнения равен $\frac{1}{2}$.

Второй способ. Рассматриваем функции

$$\varphi_1(z) = 4z^7 + 2z^6 - z^5 = z^5(4z^2 + 2z - 1),$$
$$\varphi_2(z) = 2z^4 - 4z^3 = 2z^3(z - 2),$$
$$\varphi_3(z) = 6z^2 + 3z + 1;$$

при $z = 2$ $\varphi_1(2) > 0$, $\varphi_3(2) > 0$; но $\varphi_2(2) = 0$; при $z > 2$ и $\varphi_2(z) > 0$, т. е. можно взять 2 за верхний предел (так же, как и при первом способе).

Третий способ. Берем $a = 1$:

	4	2	−1	2	−4	6	3	1
1	4	6	5	7	3	9	12	13

,

т. е. нижний предел положительных корней данного уравнения равен $\frac{1}{1} = 1$.

Мы видим, что и здесь способ Ньютона оказался самым выгодным. Но после первого способа применять способ Ньютона уже не было смысла, так как если нижний предел положительных корней данного уравнения оказался равным $\frac{1}{2}$ (по первому способу), а верхний предел положительных корней того же уравнения (по способу Ньютона) оказался тоже равным $\frac{1}{2}$, то очевидно, что наше уравнение совсем не имеет положительных корней.

Для нижнего предела отрицательных корней делаем подстановку $x = -t$; получаем:

$$t^7 - 3t^6 + 6t^5 + 4t^4 + 2t^3 + t^2 + 2t - 4 = 0.$$

Теорема 3 § 65 дает -7.

Первый способ дает: $-(1 + 4) = -5$ (ибо здесь $m = 1$).

Второй способ:

$$\varphi_1(t) = t^7 - 3t^6 = t^6(t - 3), \qquad \varphi_2(t) = 6t^5 + 4t^4 + 2t^3 + t^2 + 2t - 4;$$

при $t = 3$ $\varphi_1(3) = 0$, $\varphi_2(3) > 0$, т. е. нижний предел отрицательных корней данного уравнения равен -3.

Третий способ. Берем $a = 1$:

	1	−3	6	4	2	1	2	−4
1	1	−2	4	8	10	11	13	9
1	1	−1	3	11				
1	1	0	3					
1	1	1						

,

т. е. нижний предел отрицательных корней равен $^-1$.

Способ Ньютона и здесь оказался самым выгодным.

Для верхнего предела отрицательных корней делаем подстановку $x = -\frac{1}{u}$, получаем:

$$4u^7 - 2u^6 - u^5 - 2u^4 - 4u^3 - 6u^2 + 3u - 1 = 0.$$

Теорема 3 § 65 дает $-\dfrac{1}{1 + \dfrac{6}{4}} = -\dfrac{2}{5}$.

Первый способ дает то же самое $-D\frac{2}{5}$.

Второй способ дает $-\dfrac{1}{2}$.

Третий способ дает при $a = 1,5$:

	4	−2	−1	−2	−4	−6	3	−1
1,5	4	4	5	5,5	4,25	0,375	3,5625	4,34375

;

следовательно, верхний предел отрицательных корней равен

$$-\frac{1}{1,5} = -\frac{2}{3}.$$

Способ Ньютона и здесь самый выгодный.

Упражнения

115) Найти пределы вещественных корней для уравнения

$$x^4 - 5x^3 + 3x^2 - 2x + 4 = 0.$$

Отв. 4, 5, 1, отрицательных корней нет.

116) То же для уравнения

$$x^5 - x^4 - 2x^3 + 4x^2 - 3x + 5 = 0.$$

Отв. Положительных корней нет; для отрицательных корней

$$-2, \quad -1.$$

117) То же для уравнения

$$x^4 - 3x^2 - x + 2 = 0.$$

Отв. 2, $\frac{2}{3}$, $-1,5$, -1.

§ 84. Отделение корней. Способ Штурма. Существует несколько способов отделения корней; самый совершенный из них (теоретически) — способ Штурма (Sturm), к изложению которого мы и приступаем.

Пусть $R(x) = 0$ — данное алгебраическое уравнение. Мы можем предположить, что оно не имеет кратных корней, ибо кратные корни мы могли бы заранее выделить (§ 58).

Таким образом ц. р. функция $R(x)$ — взаимно простая со своей производной (§ 57), которую мы обозначим через $R_1(x)$.

Будем находить общий наибольший делитель для $R(x)$ и $R_1(x)$ способом Эвклида (§ 52), при этом только у получаемых остатков будем во всех членах менять знаки на обратные. Получим:

$$\left.\begin{aligned} R(x) &= Q_1(x)R_1(x) - R_2(x), \\ R_1(x) &= Q_2(x)R_2(x) - R_3(x), \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ R_{\lambda-1}(x) &= R_\lambda(x)Q_\lambda(x) - R_{\lambda+1}(x), \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ R_{n-2}(x) &= Q_{n-1}(x)R_{n-1}(x) - R_n; \end{aligned}\right\} \qquad (1)$$

R_n — постоянное количество, ибо $R(x)$ и $R_1(x)$ — взаимно простые. Итак, мы получаем ряд ц. р. функций:

$$R(x), \quad R_1(x), \ \ldots, \ R_n(x). \tag{2}$$

Этот ряд отличается следующими свойствами:

1) Последняя функция в этом ряду не обращается в нуль и, следовательно, не меняет знака (ибо она равна const).

2) Ни для какого значения $x = x_0$ две соседние функции вместе не обращаются в нуль, ибо если $R_{\lambda-1}(x_0) = R_\lambda(x_0) = 0$, то из (1) заключаем: $R_{\lambda+1}(x_0) = 0$, $R_{\lambda+2}(x_0) = 0, \ldots$, наконец, $R_n(x_0) = 0$, что невозможно, ибо $R_n = \text{const} \neq 0$.

3) Если для некоторого значения $x = x_0$ одна из средних функций $R_\lambda(x_0) = 0$, то две соседние с ней функции $R_{\lambda-1}$ и $R_{\lambda+1}$ при $x = x_0$ имеют разные знаки, ибо из (1) при $x = x_0$ получаем:

$$R_{\lambda-1}(x_0) = -R_{\lambda+1}(x_0).$$

4) Если для некоторого значения $x = x_0$ $D(x_0) = 0$, то в то время как x, возрастая, проходит через x_0, отношение $\dfrac{R(x)}{R_1(x)}$ переходит от отрицательных значений к положительным.

Это следует из второй теоремы § 79.

Ряд функций, обладающий в данном интервале (a, b) значений x этими четырьмя свойствами [причем свойство 1) достаточно выразить так: «в интервале (a, b) функция R_n не меняет знака»; не необходимо, чтобы R_n было равно const, или не обращалось в нуль], называется *рядом Штурма* для функции $R(x)$ [или для уравнения $R(x) = 0$] *в интервале* (a, b); при этом безразлично, как этот ряд получился: посредством ли алгорифма Эвклида или другим каким-либо путем.

Пусть дан некоторый ряд Штурма для уравнения $R(x) = 0$: $R(), R_1(x), R_2(x), ..., R_n(x)$ в интервале (a, b). Находим ряд чисел:

$$R(a), \quad R_1(a), \quad R_2(a), \ \ldots, \ R_n(a) \tag{3}$$

и ряд чисел:

$$R(b), \quad R_1(b), \quad R_2(b), \ \ldots, \ R_n(b). \tag{4}$$

Если $\operatorname{sign} R_\lambda(a) = \operatorname{sign} R_{\lambda+1}(a)$, то скажем, что здесь имеется *сохранение знака*; если же $\operatorname{sign} R_\lambda(a) = -\operatorname{sign} R_{\lambda+1}(a)$, то назовем это *переменой знака*. Таким образом мы можем сосчитать, сколько перемен знака в ряду (3) и сколько в ряду (4); пусть в ряду (3) их α, в ряду (4) β, тогда:

Теорема Штурма. *При $b > a$ всегда $\beta < \alpha$; $\alpha - \beta$ есть число вещественных корней уравнения $R(x) = 0$ в интервале (a, b).*

Или: при возрастании x от a до b в ряду Штурма вообще теряются перемены знака; число потерянных перемен знака в точности равно числу вещественных корней уравнения $R(x) = 0$ в интервале (a, b).

Доказательство. Мы предположим, что ни при $x = a$, ни при $x = b$ ни одна из функций ряда Штурма не обращается в нуль. Пусть при некотором $x = c$ $R_\lambda(c) = 0$ $(1 \leq \lambda < n)$; тогда по свойству 3) $\operatorname{sign} R_{\lambda-1}(c) = -\operatorname{sign} R_{\lambda+1}(c)$; при достаточно малом ε в интервале $(c - \varepsilon, c + \varepsilon)$ $R_{\lambda-1}(x)$ и $R_{\lambda+1}(x)$ не обращаются

в нуль и, следовательно, не меняют знака, $R_\lambda(x)$ обращается в нуль только при $x = c$. Следовательно, при прохождении x через c в ряду $R_{\lambda-1}, R_\lambda, R_{\lambda+1}$ могут быть только следующие комбинации знаков [где $\eta = \operatorname{sign} R_{\lambda-1}(c) = -\operatorname{sign} R_{\lambda+1}(c)$:

	$R_{\lambda-1}$	R_λ	$R_{\lambda+1}$
$c-\varepsilon$	η	η	$-\eta$
c	η	0	$-\eta$
$c+\varepsilon$	η	η	$-\eta$

	$R_{\lambda-1}$	R_λ	$R_{\lambda+1}$
$c-\varepsilon$	η	$-\eta$	$-\eta$
c	η	0	$-\eta$
$c+\varepsilon$	η	$-\eta$	$-\eta$

	$R_{\lambda-1}$	R_λ	$R_{\lambda+1}$
$c-\varepsilon$	η	$-\eta$	$-\eta$
c	η	0	$-\eta$
$c+\varepsilon$	η	η	$-\eta$

	$R_{\lambda-1}$	R_λ	$R_{\lambda+1}$
$c-\varepsilon$	η	η	$-\eta$
c	η	0	$-\eta$
$c+\varepsilon$	η	$-\eta$	$-\eta$

Из этих таблиц видно, что при проходе x через c в ряду $R_{\lambda-1}, R_\lambda, R_{\lambda+1}$ не приобретается и не теряется ни одной перемены знака; как была, так и остается одна перемена знака. В остальных частях ряда Штурма, где при $x = c$ ни одна из функций не обращается в нуль, также и знаки у функций, а следовательно, и число перемен знака не меняются.

Пусть теперь при $x = c$ $R(c) = 0$; тогда при переходе x через c по свойству 4) теряется одна перемена знака, ибо если $\operatorname{sign} R_1(c) = \eta$, то мы имеем таблицу:

	R	R_1	
$c-\varepsilon$	$-\eta$	η	1 перемена знака
c	η	0	
$c+\varepsilon$	η	η	0 перемен знака

Итак, при возрастании x от a до b изменение в числе перемен знака происходит только при прохождении x через корень уравнения $R(x) = 0$ и при каждом таком прохождении теряется одна перемена знака. Отсюда и вытекает теорема Штурма.

Если при $x = a$ или при $x = b$ некоторые из средних функций ряда Штурма обращаются в нуль, то при подсчете числа перемен знака эти нули можно просто пропускать: ведь по свойству 2) функции, соседние с нулем, не равны нулю, а по свойству 3) эти соседние функции имеют разные знаки; следовательно, какой бы знак ни приписать нулю, всегда имеется в этом месте одна перемена знака.

Теорему Штурма можно облечь в следующую формулу:

$$\sum_{\varkappa=1}^{n} \operatorname{sign}\left[R_{\varkappa-1}(b), R_\varkappa(b)\right] - \sum_{\varkappa=1}^{n} \operatorname{sign}\left[R_{\varkappa-1}(a), R_\varkappa(a)\right] = 2r, \tag{5}$$

где r — число вещественных корней уравнения $R(x) = 0$ в интервале (a, b). При этом $R_0 \equiv R$. Ибо если α — число перемен знака в ряду $R(a), R_1(a), \ldots, R_n(a)$, а β — число перемен знака в ряду $R(b), R_1(b), \ldots, R_n(b)$, то первая сумма в формуле (5) равна $n - 2\beta$, а вторая сумма равна $n - 2\alpha$, т. е. вся левая часть (5) равна $2(\alpha - \beta) = 2r$, ибо $\alpha - \beta = r$.

При доказательстве теоремы Штурма мы пользовались исключительно свойствами 1), 2), 3), 4) ряда Штурма, совершенно не принимая во внимание, каким

образом этот ряд получился. Обычно берут ряд, получающийся посредством алгорифма Эвклида, хотя практически его весьма неудобно находить; но он имеется, во-первых, для всякого уравнения, во-вторых, он годен для всякого интервала. Чтобы отделить корни уравнения $R(x) = 0$, обычно поступают так: подставляют вместо x очень большое по абсолютной величине отрицательное число $(-\infty)$; затем — очень большое положительное число $(+\infty)$ и, пользуясь теоремой § 77, определяют таким образом число всех вещественных корней; затем, подставляя различные промежуточные значения для x, находят интервалы, в которых лежит только по одному корню.

Подставив $x = 0$, можно определить число положительных и число отрицательных корней. Достаточно вставлять промежуточные значения между нижним и верхним пределами вещественных корней. Если корни отделены, то можно, суживая пределы для каждого корня (применяя первую теорему § 83), вычислить каждый вещественный корень с любой точностью. Но практически такое вычисление неудобно; ниже будут даны более удобные способы вычисления корней.

При нахождении ряда Штурма посредством алгорифма Эвклида можно делать те же практические упрощения, что из § 58: можно умножать или делить получаемые остатки на постоянные положительные множители, в частности R_n можно всегда заменить через ± 1. Если в ряде Штурма одна из средних функций $R_\lambda(x)$ не меняет знака в рассматриваемом интервале [например, когда уравнение $R_\lambda(x) = 0$ имеет все корни мнимые], то этой функцией можно и закончить ряд Штурма, отбросив все дальнейшее.

Рассмотрим, каков должен быть ряд Штурма, если все корни уравнения $R(x) = 0$ вещественны. Пусть m — степень уравнения $R(x) = 0$. При переходе x от $-\infty$ до $+\infty$ в ряду Штурма должно теряться m перемен знака; следовательно, число функций в ряду должно быть $\geq m + 1$. Если ряд найден способом (1), то степени функций $R, R_1, R_2, \ldots$ убывают, но R m-й степени; последняя функция R_m 0-й степени; следовательно, число их $\leq m+1$, и если все корни уравнения $R = 0$ вещественны, то число функций в ряду $(2) = m+1$, и степень каждой последующей на единицу меньше степени предыдущей. Далее, при $x = -\infty$ в ряду $R, R_1, R_2, \ldots, R_m$ имеется m перемен знака, а при $x = +\infty$ 0 перемен, т. е. высшие коэфициенты в $R, R_1, R_2, , \ldots, R_m$ — все одного и того же знака. Эти условия необходимы и достаточны для того, чтобы все корни уравнения $R = 0$ были вещественны.

Пример.

$$R = x^4 + x^3 + x - 1, \qquad R_1 = 4x^3 + 3x^2 + 1;$$

делим R на R_1, предварительно умножив R на 4:

$$\begin{array}{r|l}
4x^4 + 4x^3 + 4x - 4 & 4x^3 + 3x^2 - 1 \\
\underline{4x^4 + 3x^3 + x} & \underline{\quad x + 1} \\
x^3 + 3x - 4 & \\
4x^3 + 12x - 16 & \\
\underline{4x^3 + 3x^2 - 1} & \\
-3x^2 + 12x - 17 &
\end{array}$$

$$
\begin{array}{l|l}
12x^3+\ 9x^2+\ 3 & 3x^2-12x+17 \\
\cline{2-2}
12x^3-48x^2+68x & 4x+19 \\
\cline{1-1}
57x^2-68x+\ \ 3 & \\
57x^2-228x+323 & \\
\cline{1-1}
160x-320 &
\end{array} = R_2
$$

$$
\begin{array}{l|l}
3x^2-12x+17 & -x+2 \\
\cline{2-2}
3x^2-\ 6x & -3x+6 \\
\cline{1-1}
-6x+17 & \\
6x-12 & \\
\cline{1-1}
+5 &
\end{array} = R_3
$$

$$-1 = R_4$$

Итак,

$$
\begin{aligned}
R &= x^4+x^3+x-1,\\
R_1 &= 4x^3+3x^2+1,\\
R_2 &= 3x^2-12x+17,\\
R_3 &= -x+2\\
R_4 &== -1.
\end{aligned}
$$

Составляем теперь таблицу:

	R	R_1	R_2	R_3	R_4		
$-\infty$	$+$	$-$	$+$	$+$	$-$	3	перемены знака
$+\infty$	$+$	$+$	$+$	$-$	$-$	1	$''$
0	$-$	$+$	$+$	$+$	$-$	2	$''$
$+1$	$+$						
-1	$-$						
-2	$+$						

Здесь существует один положительный корень, лежащий между нулем и единицей, и один отрицательный, лежащий между -1 и -2. При $x = 1, -1, -2$ мы находим только знак R и применяем первую теорему § 78.

Упражнения

Отделить способом Штурма вещественные корни в уравнениях;

118) $x^5-2x^4+x^3-8x+6=0$.

Отв. 3 вещественных корня в интервалах $(0,1)$, $(2,3)$, $(-1,-2)$.

119) $x^5-3x^3+2x-1=0$.

Отв. 1 вещественный корень в интервале $(1,2)$.

120) $x^4+2x^3+x^2+1=0$.

Отв. Вещественных корней нет.

121) $x^3-6x+2=0$.

Отв. 3 вещественных корня в интервалах $(-3,-2)$, $(0,1)$, $(2,3)$.

§ 85. Пусть теперь уравнение $R(x) = 0$ имеет кратные корни; эти кратные корни суть все корни уравнения $D(x) = 0$, где $D(x) = D(R, R_1)$, причем R_1 — производная от R (§ 57 и 58). Уравнение же $\dfrac{R(x)}{D(x)} = 0$ имеет те же корни, что и $R(x) = 0$, только каждый из них простой. Найдем по способу (1) предыдущего параграфа $D(x)$:

$$\left.\begin{array}{rcl} R(x) & = & Q_1(x)R_1(x) - R_2(x), \\ R_1(x) & = & Q_2(x)R_2(x) - R_3(x), \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, & & \\ R_{n-2}(x) & = & Q_{n-1}(x)R_{n-1}(x) - D(x), \\ R_{n-1}(x) & = & Q_n(x)D(x). \end{array}\right\} \tag{6}$$

Как известно (§ 52), все функции $R, R_1, \ldots, R_{n-1}$, делятся без остатка на D; разделив обе части каждого из равенств (6) на D, получаем

$$\left.\begin{array}{rcl} \dfrac{R(x)}{D(x)} & = & Q_1(x) \cdot \dfrac{R_1(x)}{D(x)} - \dfrac{R_2(x)}{D(x)}, \\ \dfrac{R_1(x)}{D(x)} & = & Q_2(x) \cdot \dfrac{R_2(x)}{D(x)} - \dfrac{R_3(x)}{D(x)}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, & & \\ \dfrac{R_{n-2}(x)}{D(x)} & = & Q_{n-1}(x) \cdot \dfrac{R_{n-1}(x)}{D(x)} - 1. \end{array}\right\} \tag{7}$$

Легко видеть, что ряд

$$\frac{R(x)}{D(x)}, \quad \frac{R_1(x)}{D(x)}, \ \ldots, \ \frac{R_{n-1}(x)}{D(x)}, \quad 1 \tag{8}$$

есть ряд Штурма: свойство 1) очевидно, свойства 2) и 3) доказываются, как в § 84, свойство 4) следует из того, что

$$\frac{R(x)}{D(x)} : \frac{R_1(x)}{D(x)} = \frac{R(x)}{R_1(x)}$$

(§ 79). Значит8 при помощи ряда (8) можно определить корни уравнения $\dfrac{R}{D} = 0$, т. е. и уравнения $R = 0$; только каждый кратный корень считается за простой.

Заметим, что ряд (8) не есть обычный ряд Штурма, получаемый посредством алгорифма Эвклида; это следует хотя бы из того, что $\dfrac{R_1}{D}$ не есть производная для $\dfrac{R}{D}$.

Но вместо ряда (8) можно пользоваться и рядом

$$R, \quad R_1, \quad R_2, \ \ldots, \ R_{n-1}, \quad D, \tag{9}$$

не деля каждый его член на D. Именно, для ряда (9) верны все четыре свойства ряда Штурма для всякого x за исключением тех значений x, для которых $D = 0$;

но для таких значений и все члены ряда (9) равны нулю и $R = 0$, т. е. такие значения являются корнями уравнения $R = 0$, и при проходе x через эти значения (по § 79) теряется одна перемена знака.

Следует только заметить, что ряд (9) дает число *различных* вещественных корней уравнения $R = 0$ в данном интервале, не считая их кратности.

Пример. $R = x^4 + 2x^3 - x^2 - 2x + 1$. Находим $R_1 = 2x^3 + 3x^2 - x - 1$ (мы берем здесь за R_1 половину производной от R); $R_2 = x^2 + x - 1$; R_1 делится на R_2 без остатка. Следовательно, имеем ряд R, R_1, R_2. Составляем таблицу:

	R	R_1	R_2		
$-\infty$	$+$	$-$	$+$	2	перемены знака
$+\infty$	$+$	$+$	$+$	0	перемен $''$
0	$+$	$-$	$-$	1	перемена $''$
1	$+$	$+$	$+$	0	перемен $''$
-1	$+$	$-$	$-$	1	перемена $''$
-2	$+$	$-$	$-$	2	перемены $''$

Имеются два вещественных корня: один лежит между нулем и единицей, другой — между -1 и -2.

§ 86. Неполный ряд Штурма. Вследствие большой практической трудности построения ряда Штурма посредством алгорифма Эвклида желательно иметь возможность строить ряды Штурма иными способами. При этом наиболее трудно выполнимым оказывается свойство 4). Разберем, какое влияние оказывает это свойство на теорему Штурма, т. е. как эта теорема видоизменяется), если это свойство не выполнено.

Итак, пусть ряд,

$$R(x), \quad R_1(x), \ \ldots, \ R_n(x) \tag{10}$$

обладает тремя первыми свойствами, но не обладает последним свойством ряда Штурма; назовем такой ряд *неполным* или *обобщенным* рядом Штурма.

Если x проходит через корень одной из средних функций ряда (10), то условия здесь такие же, как и для полного ряда Штурма, а следовательно, таковы же и следствия, т. е. никакого изменения в числе перемен знака от этого не происходит. Пусть теперь x проходит через корень c уравнения $R(x) = 0$; возьмем опять очень малый интервал от $c - \varepsilon$ до $c + \varepsilon$; пусть $\operatorname{sign} R_1(c) = \eta$; могут представиться следующие случаи:

	R	R_1
$c-\varepsilon$	η	η
c	0	η
$c+\varepsilon$	η	η

	R	R_1
$c-\varepsilon$	$-\eta$	η
c	0	η
$c+\varepsilon$	$-\eta$	η

	R	R_1
$c-\varepsilon$	$-\eta$	η
c	0	η
$c+\varepsilon$	η	η

	R	R_1
$c-\varepsilon$	η	η
c	0	η
$c+\varepsilon$	$-\eta$	η

Из этих схем видно, что при переходе x через корень уравнения $R = 0$ иногда теряется одна перемена знака, иногда приобретается одна перемена знака, а иногда не теряется и не приобретается ни одной перемены знака. Пусть в интервале (a, b)

лежат $\varkappa+\lambda+\mu$ различных корней уравнения $R=0$, из которых $\varkappa$ корней дают потери перемен знака, λ корней дают приобретение перемен знака, а μ не дают ни потерь, ни приобретений перемен знака; тогда при переходе x от a до b (где $a<b$) теряется $\varkappa-\lambda$ перемен знака (при $\varkappa>\lambda$) или приобретается $\lambda-\varkappa$ перемен знака (при $\lambda>\varkappa$). Во всяком случае $\varkappa+\lambda+\mu\geq|\varkappa-\lambda|$, т. е. число различных корней уравнения $R=0$ в интервале (a,b) не меньше числа потерь или приобретений перемен знака в неполном ряде Штурма при переходе от a к b. В частном случае, если уравнение $R=0$ не имеет кратных корней, то $\mu=0$, так как при переходе x через простой корень уравнения $R=0$ R меняет знак (§ 78); в этом случае $\varkappa+\lambda-(\varkappa-\lambda)=2\lambda$, $\varkappa+\lambda-(\lambda-\varkappa)=2\varkappa$, т. е. число корней уравнения $R=0$ в интервале (a,b) или равно, или на четное число больше числа потерь или приобретений перемен знака в неполном ряде Штурма при переходе x от a к b.

В частном случае, если $R(x)=0$ уравнение n-й степени без кратных корней и неполный ряд Штурма в интервале (a,b) дал n или $n-1$ потерь или приобретений перемен знака, то можно сказать, что в интервале (a,b) лежит ровно n или $n-1$ корней уравнения $R(x)=0$.

Один из способов построения неполного ряда Штурма таков: пусть R_1 — любая ц. р. функция от x степени ниже, чем R, не имеющая в интервале (a,b) общих корней с R. Беря R и R_1 за первые две функции ряда, строим ряд по способу (1) в § 84, т. е. делим R на R_1, остаток обозначаем через $-R_2$ и т. д. Получаемый ряд $R,R_1,R_2,\ldots,R_n$ будет неполным рядом Штурма: легко видеть, что свойства 1), 2), 3) у него выполнены, тогда как свойство 4) не выполнено, ибо R_1 не есть производная для R. Функцию R_1 иногда удается выбрать так, что деление R на R_1, R_1 на R_2 и т. д. совершается довольно легко, — легче, чем при нахождении полного ряда Штурма.

Пример. $R=x^4+x^3-4x^2-4x+1$, $R_1=x^2-1$, корни R_1 суть ±1; они не являются корнями для R.

Делим:

$$\begin{array}{l|l}
x^4+x^3-4x^2-4x+1 & x^2-1\\
\underline{x^4\qquad -x^2\qquad\qquad} & \overline{x^2+x-3}\\
x^3-3x^2-4x & \\
\underline{x^3\qquad -x\qquad} & \\
-3x^2-3x+1 & \\
\underline{-3x^2\qquad +3} & \\
-3x-2 &
\end{array}$$

$$\begin{array}{l|l}
3x^2-3 & 3x+2 \\
\underline{3x^2+2x} & \overline{x-2}\\
-2x-3 & \\
-6x-9 & \\
\underline{-6x-4} & \\
-5 & \\
+1=R_3 &
\end{array}\quad =R_2$$

Итак, получаем ряд:

$$R = x^4 + x^3 - 4x^2 - 4x + 1, \quad R_1 = x^2 - 1, \quad R_2 = 3x + 2, \quad R_3 = +1.$$

Строим таблицу:

	R	R_1	R_2	R_3			
$-\infty$	$+$	$+$	$-$	$+$	2	перем.	знака
$+\infty$	$+$	$+$	$+$	$+$	0	$''$	$''$
0	$+$	$-$	$+$	$+$	2	$''$	$''$
1	$-$	0	$+$	$+$	1	$''$	$''$
2	$+$				0	$''$	$''$

Отсюда видно, что уравнение $R = 0$ во всяком случае имеет два вещественных положительных корня; один между 0 и 1, другой — между 1 и 2.

Предлагается найти для этого уравнения полный ряд Штурма и определить точное число вещественных корней.

§ 87. Сферические функции. Разложим выражение

$$\frac{1}{\sqrt{1 - 2xz + z^2}}$$

в бесконечный ряд по степеням z; коэфициенты этого ряда будут функциями от x, которые мы обозначим через $P_n(x)$:

$$\frac{1}{\sqrt{1 - 2xz + z^2}} = \sum_{n=0}^{\infty} P_n(x) z^n. \tag{11}$$

Очевидно, $P_0(x) = 1$. Для определения $P_n(x)$ для всякого n продиференцируем обе части формулы (11) по z [33]:

$$\frac{x - z}{\sqrt{(1 - 2xz + z^2)^3}} = \sum_{n=0}^{\infty} P_n(x) n x^{n-1} \tag{12}$$

или

$$\frac{x - z}{\sqrt{1 - 2xz + z^2}} = \sum_{n=0}^{\infty} P_n(x) n z^{n-1} (12xz + z^2);$$

подставляя по (11) вместо $\dfrac{1}{\sqrt{1 - 2xz + z^2}}$ ряд $\displaystyle\sum_{n=0}^{\infty} P_n(x) z^n$ находим:

$$(x - z) \sum_{n=0}^{\infty} P_n(x) z^n = \sum_{n=0}^{\infty} P_n(x) n z^{n-1} (1 - 2xz + z^2). \tag{13}$$

[33] Мы допускаем возможность почленного диференцирования степенного ряда, которая обосновывается в теории аналитических функций.

Сравнивая коэфициенты при z^n в обеих частях, получим:

$$xP_n(x) - P_{n-1}(x) = (n+1)P_{n+1}(x) - 2xnP_n(x) + (n-1)P_{n-1}(x),$$

или

$$(n+1)P_{n+1}(x) - (2n+1)xP_n(x) + nP_{n-1}(x) = 0. \tag{14}$$

Это *формула приведения* для функций $P_n(x)$; она дает возможность вычислить $P_{n+1}(x)$, если известны две предшествующие функции $P_n(x)$ и $P_{n-1}(x)$. Мы видели, что $P_0(x) = 1$; сравнивая, далее, свободные члены в обеих частях (13), найдем:

$$xP_0(x) = P_1(x),$$

т. е.

$$P_1(x) = x.$$

Теперь по формуле (14) можно последовательно найти $P_2(x), P_3(x), \ldots$ Получим:

$$P_2(x) = \frac{3}{2}x^2 - \frac{1}{2}, \quad P_3(x) = \frac{5}{2}x^3 - \frac{3}{2}x, \quad P_4(x) = \frac{35}{8}x^4 - \frac{15}{4}x^2 + \frac{3}{8}.$$

Отсюда и из (14) видно, что все $P_n(x)$ — целые рациональные функции; это так называемые *сферические функции* или *полиномы Лежандра* (Legendre); они имеют приложения в разных областях механики и математической физики. Можно доказать, что $P_n(x)$ является интегралом диференциаяьного уравнения

$$(x^2-1)y'' + 2xy' - n(n+1)y = 0.$$

Эти функции $P_n(x)$ можно еще определить следующим образом:

$$P_n(x) = \frac{1}{2^n \cdot n!} \frac{d^n[(x^2-1)^n]}{dx^n}.$$

Пусть c_n — высший коэфициент (т. е. коэфициент при x^n) в $P_n(x)$ $(n = 1, 2, 3, \ldots)$; сравним коэфициенты при x^{n+1} в обеих частях формулы (13); получим:

$$(n+1)c_{+1} - (2n+1)c_n = 0;$$

эта формула дает возможность вычислить высший коэфициент c_{n+1} у $P_{n+1}(x)$, если известен высший коэфициент c_n у $P_n(x)$. Мы видим, что при всяком n $c_n > 0$, ибо при $n = 1, 2, 3, 4$, как мы видели, $c_n > 0$. Следовательно, функция $P_n(x)$ при каждом n будет n-й степени, ибо высший коэфициент ни при каком n не обращается в нуль.

Рассмотрим ряд:

$$P_m(x), \quad P_{m-1}(x), \ \ldots, \ P_1(x), \quad P_0(x) \tag{15}$$

при некотором данном m. Имеем:

1) $P_0(x) = 1$.

2) Пусть при некотором x две соседние функции ряда (15) обращаются в нуль, например, $P_k(x) = P_{k-1}(x) = 0$; тогда из (14) следует (при $n = k-1$), что при этом

же значении x и $P_{k-2}(x) = 0$; далее (при $n = k-2$), следует, что при этом x и $P_{k-3}(x) = 0$ и т. д., наконец, и $P_0(x) = 0$, что неверно. Следовательно, две соседние функции ряда (15) не могут обе быть равными нулю при одном и том же x.

3) Пусть теперь при некотором x $P_k(x) = 0$; тогда для этого x (14) дает при $n = k$:

$$(k+1)P_{k+1}(x) = -kP_{k-1}(x),$$

т. е. при этом x P_{k-1} и P_{k+1} имеют разные знаки.

Следовательно, ряд (15) обладает тремя первыми свойствами ряда Штурма, т. е. (15) есть неполный ряд Штурма.

Вычислим $P_n(x)$ при $x = \pm 1$; имеем при $x = +1$:

$$\frac{1}{\sqrt{1-2xz+z^2}} = \frac{1}{1-z}\sum_{n=0}^{\infty} P_n(1)z^n = \sum_{n=0}^{\infty} z^n;$$

следовательно, $P_n(1) = 1$ [34]. При $x = -1$ имеем:

$$\frac{1}{\sqrt{1-2xz+z^2}} = \frac{1}{1+z} = \sum_{n=0}^{\infty} P_n(-1)z^n = \sum_{n=0}^{\infty}(-1)z^n;$$

следовательно, $P_n(-1) = (-1)^n$. Итак, ряд (15) при $x = -1$ имеет m перемен знака, а при $x = +1$ — ни одной перемены знака; следовательно, в интервале $(-1, +1)$ уравнение $P_m(x) = 0$ имеет по крайней мере m различных корней; но это уравнение m-й степени, т. е. оно не может иметь больше чем m различных корней. Следовательно:

Теорема. *Все m корней m-й сферической функции $P_m(x)$ вещественны и различны и лежат в интервале $(-1, +1)$.*

Но мы докажем, что в интервале $(-1, +1)$ ряд (15) есть полный ряд Штурма, т. е. в этом интервале выполнено и четвертое свойство ряда Штурма. Для этого диференцируем обе части (11) по x; сократив на z, получим:

$$\frac{1}{\sqrt{(1-2xz+z^2)^3}} = \sum_{n=1}^{\infty} P'_n(x)z^{n-1} \tag{16}$$

(мы принимаем во внимание, что $P'_0(x) = 0$). Умножаем теперь обе части (12) на $x - z$; а обе части (16) умножаем на $1 - x^2$ и складываем; получаем в числителе левой части:

$$(x-z)^2 + 1 - x^2 = 1 - 2xz + z^2;$$

следовательно, левая часть после сложения будет:

$$\frac{1-2xz+z^2}{\sqrt{(1-2xz+z^2)^3}} = \frac{1}{\sqrt{1-2xz+z^2}} = \sum_{n=0}^{\infty} P_n(x)z^n,$$

[34] Формула $\frac{1}{1-z} = 1 + z + z^2 + \ldots = \sum_{n=0}^{\infty} z^n$ находится простым делением единицы на $1 - z$; заключение $P_n(1) = 1$ делается на том основании, что разложение аналитической функции в степенной ряд однозначно. Аналогичные замечания можно сделать и для случая $x = -1$.

и мы получим:

$$\sum_{n=0}^{\infty} P_n(x)z^n = (x-z)\sum_{n=0}^{\infty} P_n(x)nz^{n-1} + (1-x^2)\sum_{n=0}^{\infty} P'_n(x)z^{n-1};$$

сравниваем в обеих частях коэфициенты при z^{n-1}:

$$P_{n-1}(x) = xnP_n(x) - (n-1)P_{n-1}(x) + (1-x^2)P'_n(x),$$

или

$$nP_{n-1}(x) = xnP_n(x) + (1-x^2)P'_n(x).$$

Пусть теперь x — корень уравнения $P_n(x) = 0$ (он лежит, как мы видели, между -1 и $+1$); тогда для этого x

$$nP_{n-1}(x) = (1-x^2)P'_n(x).$$

Это показывает, что $\operatorname{sign} P_{n-1}(x) = \operatorname{sign} P'_n(x)$ (ибо $1-x^2 > 0$), а отсюда на основании второй теоремы § 79 заключаем, что $\dfrac{P_n(x)}{P_{n-1}(x)}$, так же как и $\dfrac{P_n(x)}{P'_n(x)}$, переходит от отрицательных значений к положительным, если x, возрастая, проходит через корень функции $P_n(x)$. При $n = m$ это и есть четвертое свойство ряда Штурма для ряда (15). Итак:

Теорема. *Ряд сферических функций $P_m, P_{m-1}, \ldots, P_1, P_0$ есть полный ряд Штурма.*

[В формулировке этой теоремы мы не указали интервала $(-1, +1)$, для которого, собственно, мы только и доказали четвертое свойство ряда Штурма; но дело в том, что ведь вне этого интервала сферические функции, как мы видели, вообще не имеют корней, так что там и не встретится случая, где бы могло осуществиться это четвертое свойство.]

§ 88. Теорема Бюдана – Фурье. Вследствие практического неудобства нахождения ряда Штурма предпочитают применять другие способы отделения корней, не столь совершенные теоретически, но более удобные практически.

Мы изложим основания способа Бюдана (Budan) и Фурье (Fourier). Пусть $f(x) = 0$ данное уравнение n-й степени; возьмем ряд производных от функции $f(x)$:

$$f(x), \quad f'(x), \quad f''(x), \ \ldots, \ f^{(n)}(x). \tag{17}$$

Этот ряд обладает следующими свойствами:

1) $f^{(n)}(x) = \text{const}$.

2) Если x, возрастая, проходит через корень функции $f^{(\lambda)}(x)$, то отношение $\dfrac{f^{(\lambda)}(x)}{f^{(\lambda+1)}(x)}$ переходит при этом от отрицательных значений к положительным. Это следует из второй теоремы § 79, так как ведь $f^{(\lambda+1)}(x)$ есть производная для $f^{(\lambda)}(x)$. Здесь это верно для $\lambda = 0, 1, 2, \ldots, n-1$, если считать, что $f^{(0)}(x) = f(x)$.

Итак, для ряда (17) выполнены свойства 4) и 1) ряда Штурма (при этом свойство 1) — в расширенном объеме) и не выполнены, вообще говоря, свойства 2) и 3): может, например, случиться, что при одном и том же x несколько рядом стоящих

функций обратятся в нуль, и соседние с ними с обеих сторон при этом вовсе не должны иметь разные знаки. Докажем следующее:

Теорема Бюдана и Фурье. *Если x возрастает от a до b $(a < b)$, то в ряду* (17) *происходит потеря перемен знака; число потерянных перемен знака равно числу корней уравнения $f(x) = 0$ в интервале (a, b) или на четное число больше числа этих корней; при этом каждый кратный корень считается за столько корней, сколько единиц в показателе его кратности.*

Доказательство. Пусть при $x = c$ обращаются в нуль функции $f^{(k)}(x)$, $f^{(k+1)}(x), \ldots, f^{(l+l-1)}(x)$, но $f^{(k-1)}(x) \neq 0$, $f^{(k+l)}(x) \neq 0$; $k \geq 1$, $k + l \leq n$. Обозначим $\operatorname{sign} f^{(k+l)}(c) = \eta$, $\operatorname{sign} f^{(k-1)}(c) = \zeta$ и возьмем интервал от $c - \varepsilon$ до $c + \varepsilon$, в котором ни $f^{(k-1)}(x)$, ни $f^{(k+l)}(x)$ не обращаются в нуль, а $f^{(k)}(x), f^{(k+1)}(x), \ldots, f^{k+l-1)}(x)$ обращаются в нуль только при $x = c$. Принимая во внимание свойство 2) ряда (17), получим следующую таблицу знаков:

	$f^{(k-1)}$	$f^{(k)}$	$f^{(k+1)}$	$f^{(k+2)}$	$\ldots$	$f^{(k+l-2)}$	$F^{(k+l-1)}$	$f^{(k+l)}$
$c - \varepsilon$	ζ	$(-1)^l \cdot \eta$	$(-1)^{l-1} \cdot \eta$	$(-1)^{l-2} \cdot \eta$		η	$-\eta$	η
c	ζ	0	0	0		0	0	η
$c + \varepsilon$	ζ	η	η	η		η	η	η

Разберем четыре случая:

Случай 1. $\zeta = \eta$, l — четное; тогда при $x = c - \varepsilon$ имеем l перемен знака, при $x = c + \varepsilon$ — ни одной; всего потерялось l перемен при переходе x от $c - \varepsilon$ до $c + \varepsilon$.

Случай 2. $\zeta = \eta$, l — нечетное; при $x = c - \varepsilon$ имеем $l + 1$ перемену знака, при $x = c + \varepsilon$? — ни одной; всего потерялась $l + 1$? перемена.

Случай 3. $\zeta = -\eta$, l — четное; при $x = c - \varepsilon$ имеем $l + 1$ перемену знака; при $x = c + \varepsilon$ — одну; всего потерялось l перемен.

Случай 4. $\zeta = -\eta$, l — нечетное; при $x = c - \varepsilon$ имеем l перемен знака, при $x = c + \varepsilon$ — одну; всего потерялась $l - 1$ перемена. Таким образом во всех случаях при переходе от $c - \varepsilon$ до $c + \varepsilon$ теряется четное число перемен знака.

Если $k = 0$, т. е. $f^{(k)}(x) = f(x)$ обращается в нуль при $x = c$, то, беря ту же таблицу, отбрасывая в ней только первый столбец, мы убедимся, что при переходе от $c - \varepsilon$ и $c + \varepsilon$ всегда теряется l перемен знака, если $f(c) = f'(c) = \ldots = f^{(l-1)}(c) = 0$, но $f^{(l)}(c) \neq 0$, т. е. если c — l-кратный корень уравнения $f(x) = 0$.

Пусть x изменяется от a до b $(a < b)$; пусть при $x = a$ и при $x = b$ ни одна из функций ряда (17) не обращается в нуль. Тогда по предыдущим рассуждениям следует: при переходе от a к b в ряду (17) происходит потеря перемен знака; число потерянных перемен знака равно $r + 2s$, где r — число корней уравнения $f(x) = 0$ (считая и их кратности) в (a, b), а s — некоторое целое положительное число. Тем самым теорема Бюдана и Фурье доказана.

Если при $x = a$ некоторые из функций (17) обращаются в нуль, например, $f^{(k)}(a) = f^{(k+1)}(a) = \ldots = f^{(k+l-1)}(a) = 0$, но $f^{(k+l)}(a) \neq 0$, то вместо a берем $a + \varepsilon$, где $\varepsilon > 0$ очень мало; по свойству 2) мы знаем, что $f^{(k)}(a + \varepsilon), f^{(k+1)}(a + \varepsilon), \ldots, f^{(k+l-1)}(a + \varepsilon), f^{(k+l)}(a + \varepsilon)$ дают одни повторения знака. Подобно же, если $f^{(k)}(b) = f^{(k+1)}(b) = \ldots = f^{(k+l-1)}(b) = 0$, но $f^{(k+l)}(b) \neq 0$, то вместо b берем $b - \varepsilon$ при $\varepsilon > 0$ очень малом; по свойству 2) функции $f^{(k)}(b - \varepsilon), f^{(k+1)}(b - \varepsilon), \ldots, f^{(k+l-1)}(b - \varepsilon), f^{(k+l)}(b - \varepsilon)$ дают одни перемены знака. Таким образом и в этом случае устанавливается число потерянных перемен знака при переходе от a к b.

Итак, теорема Бюдана и Фурье не дает нам точного числа корней уравнения $f(x) = 0$ в интервале (a, b); только если число потерянных перемен знака при переходе от a к b равно нулю или единице, то можно наверно сказать, что в интервале (a, b) нет ни одного или имеется только один корень уравнения $f(x) = 0$. Основываясь на теореме Бюдана и Фурье, Фурье дал способ отделения вещественных корней, применимый ко всем случаям. Этот способ несколько громоздкий теоретически; мы его излагать не будем; желающих с ним ознакомиться отсылаем к книге Сохоцкого, Высшая алгебра, часть I, Решение численных уравнений.

§ 89. Теорема Декарта. Заметим, что в ряде (17) при переходе x от $-\infty$ до $+\infty$ всегда теряется n перемен знака, ибо высшие коэфициенты в $f, f', f'', \ldots$ суть a_0, na_0, $n(n-1)a_0$, $n(n-1)(n-2)a_0$, $\ldots$; они всегда одного знака; следовательно, при $x = -\infty$в ряде (17) n перемен знака, а при $x = +\infty$ — ни одной перемены.

Если число всех вещественных корней уравнения $f(x) = 0$ есть r, то по теореме Бюдана и Фурье $n = r + 2s$, откуда заключаем, что $2s$ есть число комплексных корней уравнения $f(x) = 0$.

При $x = 0$ ряд (17) обращается в ряд $a_n, 1 \cdot a_{n-1}, 2! \cdot a_{n-2}, 3! \cdot a_{n-3}, \ldots, n! \cdot a_0$, где $a_0, a_1, a_2, ..., a_n$ — коэфициенты $f(x)$. Итак, пусть λ — число перемен знака в ряду коэфициентов $a_0, a_1, a_2, \ldots, a_n$; при переходе x от 0 до $+\infty$ все эти перемены теряются; следовательно, λ или есть число положительных корней уравнения $f(x) = 0$, или на четное число больше числа положительных корней. Если некоторые из коэфициентов равны нулю, то при счете перемен знака эти коэфициенты можно не считать, ибо если, например,

$$f^{(k)}(0) = f^{(k+1)} = \ldots = f^{(k+l-1)}(0) = 0, \quad \text{но} \quad f^{(k+l)}(0) \neq 0,$$

то при достаточно малом $x = \varepsilon > 0$ по свойству 2) ряда (17) $f^{(k)}(\varepsilon), f^{(k+1)}(\varepsilon), \ldots$, $f^{(k+l-1)}(\varepsilon)$ будут иметь один и тот же знак, — тот же, что и у $f^{(k+l)}(\varepsilon)$, т. е. у a_{n-k-l}. Итак:

Теорема Декарта. *Число положительных корней уравнения $f(x) = 0$ равно или на четное число меньше числа перемен знака в ряде коэфициентов этого уравнения (причем равные нулю коэфициенты просто не считаются).*

Эта теорема была доказана Декартом, независимо от теоремы Бюдана и Фурье, задолго до открытия этой последней.

Для определения числа отрицательных корней уравнения $f(x) = 0$ заменяем x через $-x$ и применяем теорему Декарта. При этом если в уравнении $f(x) = 0$ ни один из коэфициентов не равен нулю (т. е. если $f(x) = 0$ так называемое «полное» уравнение), то при замене x через $-x$ все перемены знака перейдут в сохранения знака, а сохранения — в перемены. То-есть:

Следствие I. Если $f(x) = 0$ — «полное» уравнение, то число его отрицательных корней равно числу сохранений знака в ряде его коэфициентов или на четное число меньше.

Таким образом, если уравнение полное, то верхний предел числа вещественных корней, получаемый по правилу Декарта, равен степени уравнения n, ибо в ряде всех коэфициентов уравнения число перемен знака плюс число сохранений знака всегда равно n. Если же уравнение неполное, то этот верхний предел числа вещественных корней может быть и меньше [35]; если он равен r, то $n - r$ будет

[35] Что и в неполном уравнении этот верхний предел числа вещественных корней, получаемый

нижним пределом числа комплексных корней. Докажем, что $n - r$ всегда четное число. Действительно, если данное уравнение имеет s вещественных корней и $2t$ комплексных (они всегда входят парами по теореме 1 § 80), то $n = s+2t$, $r = s+2k$ (по теореме Декарта); следовательно, $n - r = 2(t - k)$.

Разберем подробнее, какое влияние оказывает на верхний предел числа вещественных корней отсутствие нескольких средних членов в уравнении.

1. Пусть между двумя членами ax^m и bx^{m-2k-1} отсутствует $2k$ промежуточных членов; если бы они были налицо, то они дали бы для верхнего предела положительных и отрицательных корней $2k + 1$ перемен знака; на самом же деле ax^m и bx^{m-2k-1} (без этих промежуточных членов) дают только одну перемену знака (для положительных корней, если aа и b разных знаков, и для отрицательных корней, если a и b одного знака), т. е. от того, что этих $2k$ промежуточных членов нет, потерялось $2k$ перемен знака, т. е. наше уравнение, наверное, имеет $2k$ комплексных корней.

2. Пусть отсутствует нечетное число $2k + 1$ промежуточных членов между ax^m и bx^{m-2k-2}; если бы они были налицо, то они дали бы $2k + 2$ перемен знака (для положительных и для отрицательных корней); вместо них ax^m и bx^{m-2k-2} дают две перемены знака (одну для положительных, другую для отрицательных корней), если a и b разных знаков, или ни одной, если a и b одинаковых знаков, т. е. от отсутствия этих промежуточных членов теряется или $2k$ или $2k + 2$ перемен знаков.

Итак:

Следствие II. Если в уравнении между двумя членами отсутствуют t рядом стоящих членов, то при четном t уравнение имеет, наверное, t комплексных корней, а при нечетном t — $t-1$ комплексных корней, если козфициенты тех двух членов, в промежутке между которыми отсутствует t членов, имеют разные знаки, и $t+1$ комплексных корней, если эти козфициенты имеют одинаковые знаки.

Пример 1. $f(x) = x^n - a = 0$. По теореме Декарта заключаем, что при $a > 0$ число положительных корней равно единице, а число отрицательных корней равно единице при n четном и равно нулю при n нечетном; при $a < 0$ число положительных корней равно нулю, а число отрицательных корней равно нулю при n четном и равно единице при n нечетном. Здесь теорема Декарта дает точное число вещественных корней. По следствию II заключаем, что при n нечетном наше уравнение имеет $n-1$ комплексных корней, а при n четном n комплексных корней при $a < 0$ и $n - 2$ при $a > 0$.

Пример 2. $f(x) = x^4 + x^3 - 4x^2 - 4x + 1 = 0$. По теореме Декарта заключаем, что число положительных корней равно двум или равно нулю. Но в конце § 86 мы видели, что число положительных корней этого уравнения не меньше двух; следовательно, теперь заключаем, что это число как раз равно двум.

Заменяя x через $-x$, получим $x^4 - x^3 - 4x^2 + 4x + 1 = 0$, откуда по теореме Декарта заключаем, что число отрицательных корней равно двум или равно нулю (здесь оно равно двум).

§ 90. Вычисление корней. Существует довольно много способов вычисления корней; каждый из них имеет свои достоинства и свои недостатки, так что

по правилу Декарта, может быть равен n показывает следующий пример: $x^4 - x^2 + 1 = 0$.

нельзя безусловно отдать преимущество какому-нибудь одному из них. Приближенные вычисления корней уравнения относятся, собственно, не к алгебре, а к теории приближенных вычислений. При практическом вычислении корней приходится сталкиваться со многими мелочами, которые подчас позволяют в том или ином случае производить те или иные упрощения; в теоретическом изложении все это учесть невозможно. Научиться быстро и безошибочно вычислять корни уравнения с любой точностью можно только после большой практики в этом; на практике только вполне оцениваются преимущества того или иного способа и возможные упрощения. Мы изложим способ Горнера, способ Ньютона (исправленный Фурье), так называемое «regula falsi», метод итераций, способ Греффе и Энке и некоторые другие способы.

§ 91. Способ Горнера. Пусть в уравнении $f(x) = 0$ корни отделены, и между k и $k+1$ (k — целое) лежит простой корень. Берем $y = x - k$ и располагаем $f(x)$ по степеням y (по способу Горнера, § 55); получаем уравнение $\varphi(y) = 0$, имеющее корень между 0 и 1; берем $z = 10y$ и подставляем z вместо y (это сведется к тому, что a_0 не изменится, вместо a_1 получим $10a_1$, вместо a_2 $100a_2$ и т. д., вместо a_n, $10^n a_n$); получим уравнение $\psi(z) = 0$, имеющее корень между 0 и 10; пусть этот корень лежит между l и $l+1$ (где l — целое число, меньшее десяти, т. е. цифра); подставляем $t = z - l$ и располагаем $\psi(z)$ по степеням t, получим $\chi(t) = 0$, имеющее корень между 0 и 1; подобным же образом поступаем далее. Очевидно, что k — целая часть искомого корня уравнения $f(x) = 0$, l — число десятых этого корня; так же найдем число сотых и т. д.; таким путем можно вычислить корень с любой заданной наперед точностью.

Мы видим, что способ Горнера есть не что иное, как упорядоченный способ испытаний; по существу это даже не способ вычисления, а схема расположения вычислений: если мы каким-нибудь образом, хотя бы просто при помощи испытаний, нашли, что корень уравнения $f(x) = 0$ лежит между k и $k+1$ kk — целое) и желаем найти число десятых l корня, то нам приходится в функцию $f(x)$ подставлять $x = k + \dfrac{l}{10}$, где l — испытуемое число десятых. Но $f\left(k + \dfrac{l}{10}\right)$ проще всего вычислить, пользуясь формулой Тэйлора (§ 54):

$$f\left(k + \frac{l}{10}\right) = f(k) + \frac{l}{10} f'(k) + \frac{l^2}{200} f''(k) + \ldots + \frac{l^n}{n!\ 10^n} f^{(n)}(k);$$

так как $f(n)(k), f^{(n-1)}(k), \ldots, f'(k), f(k)$ — как раз коэфициенты функции φ, получаемой из $f(x)$ при $y = x - k$, то

$$f\left(k + \frac{l}{10}\right) = \varphi\left(\frac{l}{10}\right).$$

Для удобства вычислений (чтобы не иметь дела с дробями) мы заменяем функцию $\varphi(y)$ функцией $\psi(z)$; эта замена удобна, но совершенно необязательна: вместо приписки λ нулей к коэфициенту α_λ в $\varphi(y)$ мы могли бы сразу $\varphi(y)$ расположить по степеням $u = y - \dfrac{l}{10}$, только при умножении пришлось бы учитывать запятые в десятичных дробях.

Отыскивая теперь число сотых корня и найдя его равным m, желая испытать значение $x = k + \frac{l}{10} + \frac{m}{100}$, мы должны вычислить:

$$f\left(k + \frac{l}{10} + \frac{m}{100}\right) = \varphi\left(\frac{l}{10} + \frac{m}{100}\right) = \psi\left(l + \frac{m}{10}\right) \cdot \frac{1}{10^n},$$

ибо ведь $\varphi(y) = \varphi\left(\frac{z}{10}\right) = \psi(z) \cdot \frac{1}{10^n}$. Значит, нам надо вычислить $\psi\left(l + \frac{m}{10}\right)$, что мы делаем так же, как мы вычисляли $f\left(k + \frac{l}{10}\right)$, т. е. располагаем $\psi(z)$ по степеням $t = z - l$, и, получив

$$\psi(z) = \chi(t),$$

находим:

$$\psi\left(l + \frac{m}{10}\right) = \chi\left(\frac{m}{10}\right).$$

Вводя, далее, $u = 10t$, $\chi(t) = \omega(u) \cdot \frac{1}{10^n}$, вычисляем $\omega(m)$ и т. д. Таким образом мы с каждым шагом как бы увеличиваем наш масштаб в 10^n раз.

Изложенную схему вычислений можно обобщить следующим образом. Пусть требуется вычислить $f\left(k + \frac{a}{b}\right)$; вычисляя по формуле Тэйлора, мы располагаем $f(x)$ по степеням, $y = x - k$, отчего $f(x)$ перейдет в $\varphi(y)$; итак,

$$f\left(k + \frac{a}{b}\right) = \varphi\left(\frac{a}{b}\right).$$

Далее, мы делаем подстановку: $z = by$, т. е., иными словами, в функции $\varphi(y) = a_0 y^n + a_1 y^{n-1} + \ldots + a_n$ заменяем a_λ через $b^\lambda a_\lambda$ $(\lambda = 0, 1, 2, \ldots, n)$, получая таким образом

$$\varphi(y) = \psi(z)\ \frac{1}{b^n}.$$

Теперь имеем:

$$f\left(k + \frac{a}{b}\right) = \varphi\left(\frac{a}{b}\right) = \psi(a) \cdot \frac{1}{b^n}.$$

Иными словами, мы в $\varphi\left(\frac{a}{b}\right)$ сразу выделяем общего знаменателя b^n и отбрасываем его, увеличивая этим наш масштаб в b^n раз. Этим обобщением мы в дальнейшем воспользуемся (§ 97).

Пример. Дано уравнение $x^3 - x - 1 = 0$. Находим для него ряд Штурма:

$$\begin{aligned} R &= x^3 - x - 1, \\ R_1 &= 3x^2 - 1, \\ R_2 &= 2x + 3, \\ R_4 &= -1. \end{aligned} \quad .$$

Составляем таблицу:

	R	R_1	R_2	R_3		
$-\infty$	$+$	$+$	$-$	$-$	2	перемены знака
$+\infty$	$+$	$+$	$+$	$-$	1	перемена $''$
0	$-$	$-$	$+$	$-$	2	перемены $''$
1	$-$	$+$	$+$	$-$	2	перемены $''$
2	$+$	$+$	$+$	$-$	1	перемена $''$

Отсюда заключаем, что наше уравнение имеет только один вещественный корень, содержащийся между 1 и 22; следовательно, *целая часть его равна единице.* Дальше находим:

	1	0	-1	-1
1	1	1	1	-1
1	1	2	2	
1	1	3		
	1			

Умножая сразу полученные коэфициенты на 1, 10, 100, 1000, находим новое уравнение:

$$\varphi(x) = x^3 + 30x^2 + 200x - 1000 = 0;$$

его корень лежит между 0 и 10. Подставляя $x = 1, 2, 3, \ldots$, находим, что

$$\varphi(1) < 0, \qquad \varphi(2) < 0, \qquad \varphi(3) < 0, \qquad \text{но} \quad \varphi(4) > 0,$$

т. е. корень лежит между 3 и 4; итак, 3 — число десятых корня данного уравнения. Далее, находим:

	1	30	200	$-1\,000$
3	1	33	299	-103
3	36	407		
3	1	39		
	1			

и уравнение:

$$\psi(x) = x^3 + 390x^2 + 40\,700x - 103\,000 = 0;$$

здесь $\psi(2) < 0$, но $\psi(3) > 0$, т. е. корень лежит между 2 и 3, так что 2 — *число сотых корня данного уравнения.* Далее, подобно же находим:

	1	390	40 700	$-103\,000$
2	1	392	41 484	$-20\,032$
2	1	394	42 272	
2	1	3 396		
	1			

и уравнение:

$$\chi(x) = x^3 + 3\,960x^2 + 4\,227\,200x - 20\,032\,000 = 0;$$

здесь $\chi(4) < 0$, но $\chi(5) > 0$, т. е. корень лежит между 4 и 5; значит, 4 — *число тысячных корня данного уравнения.* Остановимся на этом; итак, получаем искомый корень данного уравнения $x = 1,324$ — с точностью до $0,001$, с недостатком. Мы видим, что при дальнейших вычислениях коэфициенты получаемых уравнений сильно возрастают; в этом и заключается неудобство способа Горнера.

§ 92. Рассмотрим теперь вопрос: не велика или не мала ли взятая нами цифра при применении способа Горнера. Заметим, что все получаемые нами последовательно десятичные знаки получаются с недостатком. Если вычисляемый корень простой [36], и взятый сначала интервал $(k, k+1)$, в котором этот корень находится, не содержит корней производной функции $f'(x)$ [37], то данная функция $f(x)$ в этом интервале монотонна (т. е. все время возрастает или все время убывает). Но мы имели (применяя те же обозначения, что и в § 91):

$$\varphi(y) = f(y+k), \qquad \psi(z) = 10^n \cdot \varphi\left(\frac{z}{10}\right),$$

$$\chi(t) = \psi(t+l), \qquad \omega(u) = 10^n \cdot \chi\left(\frac{u}{10}\right) \qquad \text{и т. д.,}$$

т. е. и все функции: $\varphi(y)$, $\psi(z)$, $\chi(t)$, $\omega(u)$ и т. д. монотонны в том же смысле, что и $f(x)$. А следовательно, для значений x, y, z, t, u, ... с недостатком эти функции должны иметь знак, противоположный знаку своих производных, а для значений с избытком эти функции имеют тот же знак, что и их производные. Так, если все наши функции возрастающие, то, например, $\psi(l) < 0$, но тогда $\psi'(l) > 0$; с другой стороны, $\psi(l+1) > 0$. Отсюда получаем такое правило:

Если для взятой цифры исследуемая функция по знаку противоположна своей производной, то цифра l не слишком велика; если же эта функция при $l+1$ имеет тот же знак, что и ее производная, то цифра l не слишком мала. Если выполнены оба условия, то цифра l найдена правильно.

Практически значения $\psi(l)$, $\psi(l+1)$, $\psi'(l)$ находятся из той же самой схемы Горнера. Пусть, например

$$\psi(z) = A_0 z^n + A_1 z^{n-1} + \ldots + A_{n-1} z + A_n;$$

тогда имеем схему Горнера для $z = l$:

	A_0	A_1	A_2	...	A_{n-1}	A_n
l	A_0	$A_0 l + A_1$		...	K	L
l	A_0	$2A_0 l + A_1$		...	M	
l	A_0	$3A_0 + A_1$		...	N	
	.....					
	A_0					

[36] В практике случай кратных корней совершенно невероятен; так что случай простого корня — единственный интересный для практики случай.

[37] В противном случае следует увеличить наш масштаб в 10 раз указанным уже в § 91 способом.

при этом (§ 55) $\psi(l) = L$, $\psi'(l) = M$, $\frac{1}{2}\psi''(l) = N$. Вычисляя $\psi(l+1)$ по формуле Тэйлора (§ 54) при $h = 1$, найдем:

$$\psi(l+1) = \psi(l) + \psi'(l) + \frac{1}{2}\psi''(l) + \ldots + \frac{1}{n!}\psi^{(n)}(l) =$$
$$= L + M + N + \ldots + A_0.$$

Следовательно, цифра l найдена правильно, если

$$\operatorname{sign} L = -\operatorname{sign} M = -\operatorname{sign}(M + N + \ldots + A_0),$$
$$|M + N + \ldots + A_0| > L.$$

Так, например (§ 91), имеем в первой схеме:

$$L = -1, \qquad M = 2, \qquad M + N + A_0 = 6;$$

во второй схеме:

$$L = -103, \qquad M = 407, \qquad M + N + A_0 = 447;$$

а третьей схеме:

$$L = -20\,032, \qquad M = 42\,272, \qquad M + N + A_0 = 42\,669.$$

Упражнения

Вычислить вещественные корни уравнений

122) $x^5 - 2 = 0$.

Отв. $x = 1,14\ldots$

123) $x^3 + 2x - 11 = 0$.

Отв. $x = 1,926\ldots$

124) $x^3 - 2x - 5 = 0$.

Отв. $x = 2,0945\ldots$

125) $x^4 + 4x - 2 = 0$.

Отв. $x_1 = 0,48\ldots$, $x_2 = 1,72\ldots$

126) $x^3 - 6x + 2 = 0$.

Отв. $x_1 = 2,261\ldots$, $x_2 = 0,339\ldots$, $x_3 = -2,601\ldots$

127) $x^3 - 4x^2 + 2 = 0$.

Отв. $x_1 = 1,675\ldots$, $x_2 = 2,539\ldots$, $x_3 = -2,214\ldots$

128) Показать, что обычное извлечение, квадратных и кубических корней, излагаемое в элементарной алгебре, является частным случаем способа Горнера.

§ 93. Способ Ньютона – Фурье. Пусть известно, что в интервале (a, b) находится один корень x уравнения $f(x) = 0$. Положим $x = a + h$ и разложим $f(a + h)$ по формуле Тэйлора; если пределы a и b достаточно близки, то мы можем в формуле Тэйлора удержать только два первых члена, ибо h очень мало, и высшими степенями h можно пренебречь. Получаем:

$$f(a+h) = f(a) + hf'(a) = 0, \qquad h = -\frac{f(a)}{f'(a)}, \qquad a_1 = a - \frac{f(a)}{f'(a)};$$

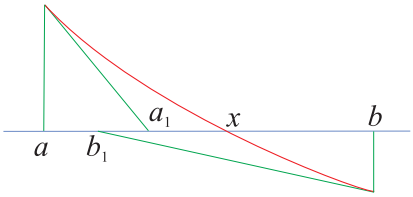
a_1 есть новое приближение корня. Беря теперь a_1 вместо a, получим далее, $a_2 = a_1 - \dfrac{f(a_1)}{f'(a_1)}$, далее $a_3 = a_2 - \dfrac{f(a_2)}{f'(a_2)}$ и т. д. Аналогично можно было начать с предела b и найти приближения:

$$b_1 = b - \frac{f(b)}{f'(b)}, \qquad b_2 = b_1 - \frac{f(b_1)}{f'(b_1)}$$

и т. д.

Это — способ Ньютона в его первоначальном виде. Но здесь возникают два вопроса: 1) будут ли последующие приближения лучше предыдущих, т. е. a_1 лучше, чем a, a_2 лучше, чем a_1 и т. д.? 2) Если, например, $a < x$ (x — искомый корень), то будет ли и $a_1 < x$, $a_2 < x$ и т. д., т. е., находя ряд приближений $a, a_1, a_2, \ldots$, не можем ли мы перескочить через корень? Без добавочных условий мы не можем удовлетворительно ответить ни на один из этих вопросов.

Фурье ввел эти добавочные условия, исправив, таким образом, способ Ньютона.

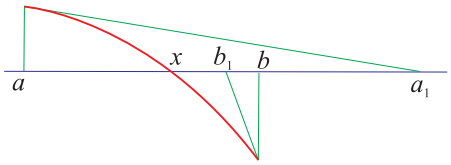


Черт. 14

Раньше чем говорить о тех исправлениях, которые сделал Фурье, дадим геометрическое представление способа Ньютона. Рассмотрим кривую $y = f(x)$ в интервале (a, b). Уравнение $y = f(a) + hf'(a)$, которым мы пользуемся для определения h, есть не что иное, как уравнение касательной к кривой $y = f(x)$ в точке a (при этом $h = x - a$); следовательно, значение

$$a_1 = a - \frac{f(a)}{f'(a)}$$

есть абсцисса точки пересечения этой касательной с осью x; т. е. вместо точки пересечения самой кривой с осью x мы берем точку пересечения ее касательной с осью x; $h = a_1 - a$ есть длина так называемой *подкасательной* в точке a; поэтому способ Ньютона иначе называется «*способ подкасательных*». Все сказанное относится также и к точкам b и b_1. Ниже мы помещаем ряд чертежей, дающих различные случаи, которые здесь могут встретиться.

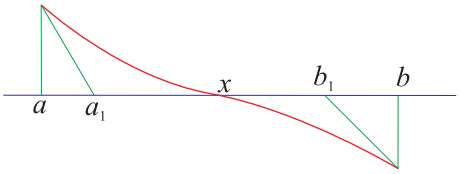


Черт. 15

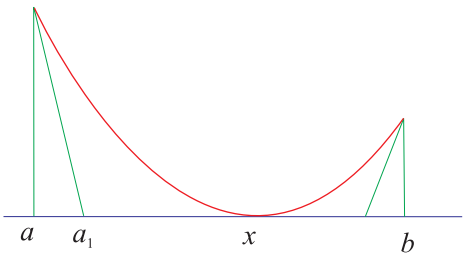
Чертежи 14, 15 и 18 показывают, что новые приближения могут иногда попасть по другою сторону от корня по сравнению со старыми; черт. 15 и 18 при этом показывают, что новые приближения могут оказаться хуже старых. Те же чертежи показывают, что оба эти случая бывают (причем первый непременно, второй — не обязательно) тогда, когда способ Ньютона применяется с того конца

нашего интервала (a, b), где кривая, изображающая функцию $f(x)$, обращена к оси x вогнутою стороною, т. е. где $\operatorname{sign} f(x) = -\operatorname{sign} f''(x)$ [иначе, где $f(x)f''(x) < 0$] [38]. Мы с самого начала возьмем наш интервал (a, b) настолько узким, чтобы в нем уравнение $f(x) = 0$ имело только один корень x; (может быть и кратный), т. е. чтобы за исключением этого значения x ни $f(x)$, ни $f'(x)$, ни $f''(x)$ в этом интервале, включая и его границы, не обращались в нуль [39]. При этих условиях мы докажем следующую теорему:

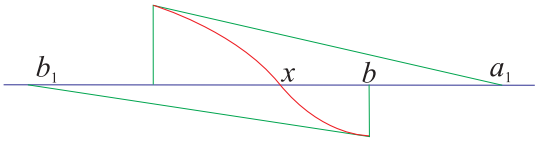
Теорема. *Если применить способ Ньютона с того конца нашего интервала* (a, b), *где* $\operatorname{sign} f(x) = \operatorname{sign} f''(x)$, *то новое приближение корня лежит с того же конца и ближе к корню. Если же применить способ Ньютона с того конца, где* $\operatorname{sign} f(x) = -\operatorname{sign} f''(x)$, *то новое приближение будет с другого конца и может оказаться хуже предыдущего.*



Черт. 16



Черт. 17



Черт. 18

Доказательство. По формуле Тэйлора с остаточным членом, обозначая через $a + h = x$ точный корень нашего уравнения $f(x) = 0$, а через a — один из концов нашего интервала, имеем:

$$f(a + h) = f(a) + hf'(a) + \frac{h^2}{2}f''(a + \theta h) = 0^{40}$$

[38] В диференциальном исчислении доказывается следующая теорема: кривая $y = f(x)$ обращена в данной точке x к оси x выпуклою или вогнутою стороною в зависимости от того, будет ли в этой точке $yy'' > 0$ или $yy'' < 0$.

[39] Обычно ставится еще условие, чтобы корень нашего уравнения был простой; но это условие совершенно не необходимо; поэтому я и откинул его.

[40] В общем виде эта формула выводится в диференциальном исчислении и имеет такой вид:

$$f(a + h) = f(a) + hf'(a) + \frac{h^2}{2!} + \ldots +$$
$$+ \frac{h^{n-1}}{(n-1)!}f^{(n-1)}(a) + \frac{h^n}{n!}f^{(n)}(a + \theta h),$$

где θ — некоторое число, лежащее между нулем и единицей; $x \neq a$. Отсюда

$$h = -\frac{f(a0}{f'(a)} - \frac{h^2}{2}\ \frac{f''(a+\theta h)}{f'a)},$$

или, обозначив

$$a_1 = a - \frac{f(a)}{f'(a)};$$

$$x - a_1 = x - a + \frac{f(a)}{f'(a)} = -\frac{h^2}{2}\ \frac{f''(a+\theta h)}{f'(a)}, \qquad a_1 - a = -\frac{f(a)}{f'(a)}. \tag{18}$$

Заметим, что $a+\theta h$ лежит между a и $x = a+h$, т. е. $f''(a+\theta h)$ имеет тот же знак, что и $f''(a)$. Формулы (18) показывают:

1) Если $\operatorname{sign} f''(a) = \operatorname{sign} f(a)$, то $\operatorname{sign}(x - a_1) = \operatorname{sign}(a_1 - a)$, т. е. a_1 лежит между a и x, значит, по ту же сторону от x, что и a, и ближе к x, чем a.

2) Если же $\operatorname{sign} f''(a) = -\operatorname{sign} f(a)$, то $\operatorname{sign}(x - a_1) = -\operatorname{sign}(a_1 - a)$, т. е. x и a лежат по одну сторону от a_1; но, с другой стороны, первая, формула (18) показывает, что при $x > a$, т. е. $x - a > 0$, будет $x - a_1 < x - a$, при $x < a$, т. е. $x - a < 0$, будет $x - a_1 > x - a$, ибо при $x > a$ $f(a)$ и $f'(a)$ имеют разные знаки, т. е. $\dfrac{f(a)}{f'(a)} < 0$, а при $x < a$ $f(a0$ и $f'(a)$ имеют одинаковые знаки, т. е. $\dfrac{f(a)}{f'(a)} > 0$ [41]. Это показывает, что в обоих случаях x лежит между a и a_1. Именно, при $x > a$ $x - a_1 < x - a$; если было бы $x - a_1 > 0$, то a_1 лежало бы между x и a, в противоречие с доказанным выше; следовательно, $x - a_1 < 0$, т. е. x лежит между a и a_1. Аналогично докажем, что при $x < a$ будет $x - a_1 > 0$, т. е. опять x находится между a и a_1. Наша теорема, таким образом, доказана. Остается выяснить, при каких условиях приближение a_1 может оказаться хуже, чем a, т. е. когда может быть

$$|x - a_1| > |x - a|.$$

Ясно, что в случае 1) этого не может быть. В случае 2) из первой формулы (18) заключаем, что $x - a_1$ имеет тот же знак, что и $\dfrac{f(a)}{f'(a)}$; следовательно, в этом случае:

$$|x - a_1| = \left|\frac{f(a)}{f'(a)}\right| - |x - a|;$$

где θ — некоторое число, большее нуля и меньшее единицы. От формулы (4) § 42 она отличается (кроме того, что мы x заменили через a) аргументом функции $f^{(n)}$ в последнем члене; этот последний член называется остаточным членом, и именно в форме Лагранжа. Эта формула верна для всякой функции, имеющей производные до n-го порядка включительно, где $n > 0$ — какое-нибудь целое число. Мы применяем эту формулу при $n = 2$ и принимаем во внимание, что $f(a+h) = 0$.

[41] Это следует из того, что ни в a, ни в промежутке между a и x, $f'(x)$ по условию не обращается в нуль и, значит, сохраняет постоянный знак, и так как функция $f(z)$ при изменении z от a до x приближается к нулю, т. е. при $a < x$ и $f(a) > 0$ уменьшается, а при $a < x$ и $f(a) < 0$ увеличивается, то в первом случае $f'(a) < 0$, а во втором $f'(a) > 0$; в обоих случаях $\dfrac{f(a)}{f'(a)} < 0$. При $a > x$ рассуждения аналогичны.

это будет больше чем $|x-a$, если

$$\left|\frac{f(a)}{f'(a)}\right| > 2|x-a|. \tag{19}$$

Заметим, что $f(a)$ вообще мало по абсолютной величине, если a достаточно близко к корню x; следовательно, формула (19) требует, чтобы $|f'(a)|$ было очень мало.

§ 94. Теорема. *Если x — кратный корень уравнения $f(z)=0$, то при $z \neq x$* $\operatorname{sign} f(z) = \operatorname{sign} f''(z)$, *если только z достаточно близко к x, т. е. с обеих сторон от кратного корня мы имеем случай* 1).

Доказательство. Пусть $z < x$ и возрастает до x; при $f(z) > 0$ эта функция уменьшается до нуля, т. е. $f'(z) < 0$; но $f'(x) = 0$, ибо x — кратный корень для $f(z) = 0$; следовательно, при возрастании z до x $f'(z)$ возрастает до нуля, а следовательно, $f''(z) > 0$; при $f(z) < 0$ $f(z)$ возрастает до нуля, т. е. $f'(z) > 0$ и уменьшается до нуля, т. е. $f''(z) < 0$; в обоих случаях $\operatorname{sign} f(z) = \operatorname{sign} f''(z)$. При $z > x$ рассуждение аналогично.

Следствие. Случай 2) § 93 может быть, хотя бы с одной стороны, только у простого корня.

Замечание. Не следует думать, что у простого корня случай 2) обязательно будет, хотя бы с одной стороны (черт. 19).

Теорема. *Если, с данной стороны от корня мы имеем случай* 2) § 93, *т. е.* $\operatorname{sign} f(a) = -\operatorname{sign} f''(a)$, *то, взяв a достаточно близким к x, мы всегда достигнем того, что приближение a_1 будет лучше, чем a, т. е. будет $|x-a_1| < |x-a|$.*

Доказательство. Корень x (см. предыдущее следствие) простой, следовательно

$$\lim_{z\to x}\left|\frac{f(z)}{x-z}\right| = |f'(x)| > 0^{42}$$

поэтому

$$\lim_{z\to x}\left|\frac{f(z)}{(x-z)f'(z)}\right| = \left|\frac{f'(x)}{f'(x)}\right| = 1;$$

это показывает, что при z, достаточно близком к x, будет:

$$\left|\frac{f(z)}{(x-z)f'(z)}\right| = 1+\varepsilon < 2,$$

иначе

$$\left|\frac{f(z)}{f'(z)}\right| < 2|x-z|;$$

[42]Это легко следует из формулы (9) § 56; она имеет вид:

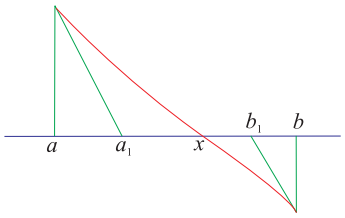
$$F'(x) = \frac{F(x)}{x-x_1} + \frac{F(x)}{x-x_2} + \ldots;$$

при $x \to x_1$ все члены правой части, начиная со второго, стремятся к нулю, таким образом

$$\lim_{x\to x_1}\frac{F(x)}{x-x_1} = F'(x_1).$$

взяв такое z с той стороны, где $\operatorname{sign} f(z) = -\operatorname{sign} f''(z)$, и положив это взятое значение z равным a, мы увидим, что условие (19) не будет выполнено, и, следовательно, $|x - a_1| < |x - a|$.

Напоминаем, что во всех предыдущих рассуждениях считается выполненным условие, поставленное перед теоремой в § 93: наш интервал, содержащий корень x, так мал, что в нем, за исключением самой точки x, нигде не обращаются в нуль ни $f(z)$, ни $f'(z)$, ни $f''(z)$.

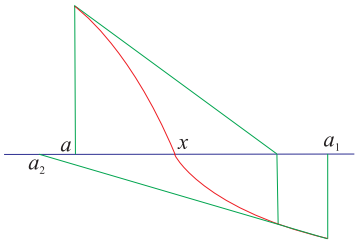


Черт. 19

§ 95. Найдя приближение a_1 и подставляя его вместо a в выражение $a - \dfrac{f(a)}{f'(a)}$, найдем приближение $a_2 = a_1 - \dfrac{f(a_1)}{f'(a_1)}$. Возникает вопрос: будет ли приближение a_2 лучше, чем a_1? В случае 1) § 93 это, очевидно, будет; в случае же 2) этого может и не быть, как показывает черт. 20; но в таком случае — по второй теореме § 94 — мы приближаем a_1 к x и, приблизив достаточно, достигаем того, что a_2 будет лучше, чем a_1. Далее, находим $a_3 = a_2 - \dfrac{f(a_2)}{f'(a_2)}$ и т. д. Получаем ряд все лучших лучших приближений к корню x:

$$a, \quad a_1, \quad a_2, \quad a_3, \quad \ldots$$

Возникает вопрос: можно ли этим способом вычислить корень с какою угодно точностью? То-есть, иными словами, будет ли $\lim\limits_{m\to\infty} a_m = x$? Ответ на этот вопрос утвердительный; мы докажем это для случая, когда корень x простой; практически этот случай только и имеет значение.



Черт. 20

Пусть в интервале (a, b) $|f'(x)| > A$, $|f''(x)| < B$, $\dfrac{B}{2A} = M$, $e_m = x - a_m$, $x = a_m + e_m = a_{m-1} + e_{m-1}$, $f(a_{m-1} + e_{m-1}) = 0$, или по формуле Тэйлора:

$$f(a_{m-1} + e_{m-1} f'(a_{m-1}) + \frac{e_{m-1}^2}{2} f''(a_{m-1} + \theta e_{m-1}) = 0;$$

отсюда

$$e_{m-1} + \frac{f(a_{m-1})}{f'(e_{m-1})} = -\frac{e_{m-1}^2}{2} \; \frac{f''(a_{m-1} + \theta e_{m-1})}{f'(a_{m-1}};$$

но

$$e_{m-1} + \frac{f(a_{m-1})}{f'(a_{m-1})} = x - \left[a_{m-1} - \frac{f(a_{m-1})}{f'(a_{m-1})}\right] = x - a_m = e_m;$$

итак,

$$e_m = -\frac{e_{m-1}^2}{2} \; \frac{f''(a_{m-1} + \theta e_{m-1})}{f'(a_{m-1})},$$

$$|e_m| = e_{m-1}^2 \left| \frac{f''(a_{m-1} + \theta e_{m-1})}{2f'(a_{m-1})} \right| < M e_{m-1}^2;$$

следовательно:

$$|e_1| < M e_0^2, \quad |e_2| < M e_1^2, \ \ldots, \qquad |e_0| < |a - b|,$$

поэтому

$$|e_m| < M^{2^m - 1} |a - b|^{2^m};$$

при $|M(a - b)| < 1$ получаем: $\lim\limits_{m \to \infty} e_m = 0$;

$$\lim_{m \to \infty} a_m = 0.$$

Это дает и формулу для оценки погрешности. Итак:

Теорема. *Если x — единственный (простой) корень уравнения $f(x) = 0$ в интервале (a, b), причем в этом интервале:* 1) *$f'(x)$ не обращается в нуль;* 2) *если $|f'(x)| > A$, $|f''(x)| < B$, $\dfrac{B}{2A} = M$, то $|M(a - b)| < 1$, то, начав с какого угодно конца интервала применять способ Ньютона, найдя, таким образом, ряд приближений $a_1, a_2, a_3, \ldots$, мы будем иметь: $\lim\limits_{m \to \infty} a_m = x$, т. е. сможем этим способом вычислить корень с какою угодно точностью.*

Из самого хода доказательства видно, что оно обнимает как случай 1), так и случай 2) § 93; точно так же оно не требует, чтобы $f''(x)$ не обращалось в нуль. Условия этой теоремы и являются по существу условиями, которые ввел Фурье; только он потребовал еще, чтобы $f''(x)$ не обращалось в нуль в интервале (a, b); это условие для нас оказалось лишним.

Пример. $f(x) = x^3 - x - 1 = 0$; это уравнение имеет корень между 1 и 2. Находим:

$$f'(x) = 3x^2 - 1, \qquad f''(x) = 6x;$$

в интервале $(1, 2)$ ни $f'(x)$ ни $f''(x)$ не обращаются в нуль. Здесь $A = 2$, $B = 12$, $M = 3$; следовательно, интервал $(1, 2)$ очень велик. Но мы знаем (пример § 91), что искомый корень лежит между $1,3$ и $1,4$; для этого интервала можно взять $A = 4$, $B = 10$, $M = 1,25$. За число a мы здесь должны взять $1,4$.

Итак, имеем:

$$a_1 = 1,4 - \frac{f(1,4)}{f'(1,4)} = 1,4 - \frac{0,344}{4,88} = 1,33,$$

$$a_2 = 1,33 - \frac{0,022637}{4,3067} = 1,33 - 0,052 = 1,3248;$$

здесь погрешность

$$|e_2| < M^{2^2 - 1} |a - b|^{2^2}, \quad \text{т. е.} \quad |e_2| < \frac{1}{5\,120},$$

и, значит, во всяком случае верны первые три десятичных знака.

Замечание. Мы имеем $|e_{m+1}| < M^{2^{m+1} - 1} |a - b|^{2^{m+1}}$, т. е. предел погрешности при переходе от приближения a_m к следующему приближению a_{m+1} уменьшается в

$$[[M^{2^m - 1} |a - b|^{2^m}] : [M^{2^{m+1} - 1} |a - b|^{2^{m+1}}] =$$

$$= M^{2^m - 2^{m+1}} |a - b|^{2^m - 2^{m+1}} = [M^{2^m} |a - b|^{2^m}]^{-1} \quad \text{раз.}$$

Принимая во внимание, что $M^{2^m} \cdot |a-b|^{2^m}$ есть верхний предел для $|e_m|$, умноженный на M, мы получаем, таким образом, что при переходе от a_m к a_{m+1} верхний предел погрешности приближенно возвышается в квадрат. То-есть если a_m давало нам искомый корень с k верными десятичными знаками, то a_{m+1} будет давать этот корень с $2k$ верными десятичными знаками. Но следует заметить, что иногда бывают и небольшие отклонения от этого правила в ту или иную сторону.

Упражнение

Решить по способу Ньютона уравнения, данные в упражнениях к § 92.

§ 96. Regula falsi или «правило ложного положения». Под этим именем известен применявшийся еще со времен древних египтян прием вычисления неизвестных, состоявший в том, что вместо неизвестных подставляли их приближенные значения, определявшиеся «на-глаз», и, идя обратно от неизвестных к известным величинам, получали результат, конечно расходящийся с данными; далее, из пропорций определяли уже более точные значения неизвестных. Для уравнений первой степени вида $ax = b$ такой метод давал в результате точное значение x. Для более сложных уравнений применялся более сложный прием, представляющий собою дальнейшее развитие regula falsi, так называемый regula duorum falsorum, или «правило двух ложных положений», состоящий в следующем: пусть дано найти корень уравнения $f(x) = a$; пусть каким-нибудь образом найдены приближенные значения x_1 и x_2 для x и пусть $f(x_1) = a_1$, $f(x_2) = a_2$; в таком случае мы определяем x из пропорции:

$$\frac{x - x_1}{x_2 - x_1} = \frac{a - a_1}{a_2 - a_1},$$

из которой находим:

$$\begin{gathered} x = x_1 + \frac{(x_2 - x_1)(a - a_1)}{a_2 - a_1} = x_2 + \frac{(x_1 - x_2)(a - a_2)}{a_1 - a_2} = \\ = \frac{(a_2 - a)x_1 - a_1 - a)x_2}{a_2 - a_1} = \frac{(a_1 - a)x_2 - (a_2 - a)x_1}{a_1 - a_2}. \end{gathered} \tag{20}$$

Для уравнений первой степени вида $ax + b = c$ этот метод дает точное значение для x. Для всех же других уравнений этот метод дает приближенное значение корня. Применив его к нашему уравнению $f(x) = 0$, рассматривая a и b как приближенные значения для x, получим:

$$x = a - \frac{(b - a)f(a)}{f(b) - f(a)} = b - \frac{(a - b)f(b)}{f(a) - f(b)}, \tag{21}$$

или

$$x = a - \frac{f(a)}{\dfrac{f(b) - f(a)}{b - a}} = b - \frac{f(b)}{\dfrac{fa) - f(b)}{a - b}}. \tag{21a}$$

Отсюда видно, что regula falsi дает нам одно только приближение нашего корня, независимо от того, с какого конца (a или b) нашего интервала мы начинаем.

Формула (21a) отличается от формулы:

$$x = a - \frac{f(a)}{f'(a)},$$

которую дает способ Ньютона, только тем, что в знаменателе вместо $f'(a)$ стоит $\frac{f(b) - f(a)}{b - a}$. Геометрически regula falsi выражается в том, что в интервале (a, b) мы заменяем кривую $y = f(x)$ ее хордой $\overline{AB}$. Из черт. 21 видно, что если для интервала (a, b) соблюдены условия, введенные Фурье в способе Ньютона, то regula falsi дает приближение b_1 лежащее всегда по другую сторону от корня по сравнению с приближением a_1 в способе Ньютона. Докажем это аналитически. Обозначим через x точный корень, а через a_1 и b_1 его приближения по способу Ньютона и по regula falsi; тогда

$$x - a_1 = x - a + \frac{f(a)}{f'(a)},$$

$$x - b_1 = x - a + \frac{f(a)}{[f(b) - f(a)] : (b - a)} = x - a + \frac{f(a)}{f'(\xi)},$$

где ξ — некоторое среднее значение, лежащее между a и b? [43]. Нам надо доказать, что $x - a_1$ и $x - b_1$ разных знаков.

Имеем:

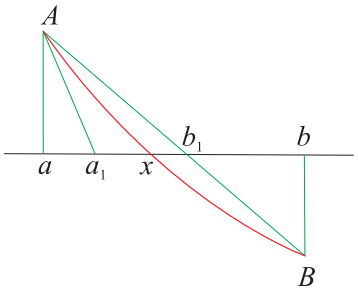
$$\frac{f(x) - f(a)}{x - a} = f'(\eta,$$

где η — некоторое среднее значение между a и x. Но $f(x) = 0$; следовательно:

$$-\frac{f(a)}{x - a} = f'(\eta),$$

или

$$x - a = -\frac{f(a)}{f'(\eta)}.$$



Черт. 21

[43] $\frac{f(b) - f(a)}{b - a} = f'(\xi)$; это так называемая формула Лагранжа, известная из диференциального исчисления и являющаяся частным случаем формулы Тэйлора или Маклорена (см. сноску в § 93).

Отсюда получаем:

$$\left.\begin{aligned} x - a_1 &= -\frac{f(a)}{f'(\eta)} + \frac{f(a)}{f'(a)}, \\ x - b_1 &= -\frac{f(a)}{f'(\eta)} + \frac{f(a)}{f'(\xi)}. \end{aligned}\right\} \tag{22}$$

Рассмотрим функцию

$$\varphi(t) = \frac{f(t) - f(a)}{t - a},$$

причем определяем: $\varphi(a) = \lim\limits_{t \to a} \varphi(t) = f'(a)$ (см. конец § 66); в таком случае $\varphi(t)$ определена во всем замкнутом интервале (a, b). Имеем:

$$\begin{aligned} \varphi'(t) &= \frac{(t-a)f'(t) - f(t) + f(a)}{(t-a)^2} = \\ &= \frac{(t-a)f'(t) - (t-a)f'[a + \theta(t-a)]}{(t-a)^2} = \frac{f'(t) - f'[a + \theta(t-a)]}{t-a} = \\ &= \frac{t - a - \theta(t-a)}{t-a} f''(\xi_1) = (1-\theta) f''(\xi_1) \end{aligned}$$

(мы применили два раза формулу Лагранжа), где ξ_1 — некоторое среднее значение между t и $a + \theta(t-a)$, т. е. вообще между a и b; $0 < \theta < 1$. Так как в интервале (a, b) $f''(t)$ не меняет знака, то, следовательно, и $\varphi'(t)$ сохраняет постоянный знак, так что $\varphi(t)$ — функция монотонная (т. е. все время возрастает или все время убывает). Следовательно:

$$\varphi(a) < \varphi(x) < \varphi(b) \quad \text{или} \quad \varphi(a) > \varphi(x) > \varphi(b),$$

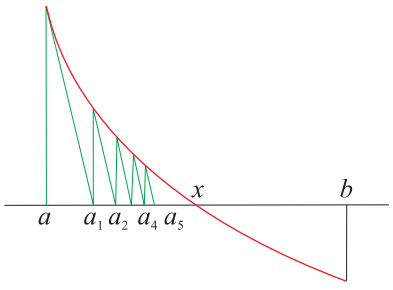
но

$$\varphi(a) = f'(a), \qquad \varphi(x) = f'(\eta), \qquad \varphi(b) = f'(\xi);$$

следовательно, $f'(\eta)$ всегда лежит между $f'(a)$ и $f'(b)$, т. е. формулы (22) показывают, что

$$\operatorname{sign}(x - a_1) = -\operatorname{sign}(x - b_1),$$

что и требовалось доказать.



Черт. 22

Regula falsi удобно объединять со способом Ньютона, так как оба они дают новый интервал (a_1, b_1) для корня, более узкий, чем (a, b). Исходя из этого нового

интервала, можно снова применить способ Ньютона и regula falsi и получить еще более узкий интервал (a_2, b_2) и т. д. При этом нет надобности вычислять предел погрешности

$$M^{2^m-1} \cdot |a-b|^{2^m}$$

(§ 95): разности $|b_1 - a_1|$, $|b_2 - a_2|$, ... и будут последовательными пределами погрешности. Практически мы просто обращаем a_1 и b_1 в десятичные дроби и берем общие у a_1 и b_1 десятичные знаки, пока в первый раз не встретим расхождения; тогда число a_1', составленное из этих общих для a_1 и b_1 цифр, и будет новым нижним пределом корня, а верхним его пределом будет число b_1', получающееся из a_1' увеличением на единицу его последнего десятичного знака.

Так, в примере § 95 мы имеем $a = 1,4$, $b = 1,3$; найдем:

$$f(a) = f(1,4) = 0,344, \qquad f(b) = f(1,3) = -0,103, \quad \frac{f(b)-f(a)}{b-a} = 4,47;$$

применяя regula falsi, получим:

$$b_1 = 1,4 - \frac{0,344}{4,47} = 1,4 - 0,076 = 1,324;$$

в § 95 по способу Ньютона получено $a_1 = 1,33$. За новый интервал для дальнейшего вычисления можно взять $(1,32,\ 1,33)$.

Примечание 1.. Regula falsi применяется только в случае простого корня или вообще корня нечетной кратности, причем в последнем случае неизвестно, с какой стороны от искомого корня лежит найденное его приближение. В случае же корня четной кратности хорда AB совсем не пересекает оси X в интервале (a, b), т. е. мы никакого приближения не получаем.

Примечание 2. В способе Ньютона в приближениях

$$a_1 = a - \frac{f(a)}{f'(a)}, \qquad a_2 = a_1 - \frac{f(a_1)}{f'(a_1)}, \qquad a_3 = a_2 - \frac{f(a_2)}{f'(a_2)}, \ldots$$

в случае 1) § 93 мы можем все знаменатели заменить через наибольший из них по абсолютной величине, т. е. через $f'(a)$; тогда получим:

$$a_2' = a_1 - \frac{f(a_1)}{f'(a)}, \qquad , a_3' = a_2' - \frac{f(a_2')}{f'(a)}, \qquad \ldots$$

Эти приближения $a_2', a_3', \ldots$ (черт. 22) несколько хуже, чем $a_2, a_3, \ldots$, т. е. посредством их мы не так скоро приближаемся к корню, но они практически удобнее, ибо не требуется вычислять $f'(a_1), f'(a_2) \ldots$

Примечание 3. Способ Ньютона и regula falsi имеют еще то преимущество, что применимы не только к алгебраическим, но и к трансцендентным уравнениям, так как основанием их является анализ; выводя эти способы, мы применяем общие функциональные свойства левой части нашего уравнения $f(x) = 0$, но не принимали специально во внимание, что $f(x)$ — целая рациональная функция.

§ 97. Комбинированный способ. Для того чтобы с пользой применить способ Ньютона, требуется с самого начала взять достаточно узкий интервал (a, b),

т. е. заранее найти не только целую часть корня, но и один-два десятичных знака. Это проще всего сделать способом Горнера. Но после того как мы способом Горнера нашли два десятичных знака, нам нет надобности для дальнейшего применения способа Ньютона и regula falsi возвращаться к первоначальному уравнению $f(x) = 0$, а следует исходить из полученного уравнения $\omega(u) = 0$ или просто из той схемы Горнера, на которой мы остановились. Эта схема приведена в § 92 [только вместо $\omega(u)$ там стоит $\psi(z)$]; по этой схеме, вводя в нее обозначение $\omega(u)$, имеем [l пусть будет хотя бы вторым десятичным знаком искомого корня уравнения $f(x) = 0$]:

$$\omega(l) = L, \qquad \omega'(l) = M, \qquad \frac{1}{2}\omega''(l) = N, \quad \ldots \quad =$$
$$\omega(l+1) = L + M + N + \ldots + A_0$$
$$\frac{\omega(l+1) - \omega(l)}{(l+1) - l} = \omega(l+1) - \omega(l) = M + N + \ldots + A_0.$$

Таким образом в способе Ньютона нам следует разделить L на M, а в regula falsi [§ 96, (31a)] следует разделить L на $M + N + \ldots + A_0$. При этих делениях мы получаем десятые, сотые и т. д. доли корня уравнения $\omega(u) = 0$, т. е. тысячные, десятитысячные и т. д. доли корня уравнения $f(x) = 0$. Следует продолжать оба эти деления до тех пор, пока не получим расхождения в находимых цифрах; тут надо остановиться; общие для обеих частных первые цифры и будут правильными десятичными знаками корня. Если перед тем было найдено (способом Горнера) два десятичных знака, то весьма вероятно, что способ Ньютона и regula falsi даст еще два новых правильных десятичных знака (см. замечание в конце § 94).

Если требуется вычислить корень с большей точностью, т. е. применить во второй раз способ Ньютона и regula falsi, то мы опять пользуемся схемой Горнера (§ 91, «Обобщение»): именно, если r и s — два новых найденных десятичных знака, то, следовательно, уравнение $\omega(u) = 0$ имеет корень $l + \dfrac{r}{10} + \dfrac{s}{100} + \ldots$, т. е. следует вычислить $\omega\left(l + \dfrac{r}{10} + \dfrac{s}{100}\right) = \omega\left(l + \dfrac{10r+s}{100}\right)$; это мы сделаем, увеличив предварительно корни в 100 раз, т. е. произведя подстановку: $u = \dfrac{v}{100}$, $\omega_1(v) = 10^{2n} \cdot \omega\left(\dfrac{v}{100}\right)$, что фактически сводится к тому, что мы оставляем без изменения высший коэфициент в $\omega(u)$, к следующему коэфициенту приписываем два нуля, к следующему за ним — четыре нуля и т. д. А далее применяем схему Горнера.

Подобным же образом поступаем, если необходимо применить в третий раз способ Ньютона и regula falsi.

Замечание. Легко видеть, что частные $\dfrac{L}{M}$ и $\dfrac{L}{M + N + \ldots + A_0}$ отрицательны (§ 92) и меньше единицы по абсолютной величине, т. е. фактически нам приходится к найденной части корня что-то прибавлять, т. е. приписывать новые знаки.

Пример 1. Дано уравнение $x^4 + 2x^3 - 3x - 2 = 0$. Легко убедиться, что оно имеет корень, лежащий между 1 и ?2. Находим по способу Горнера два его десятичных

знака:

	1	2	0	−3	−2
1	1	3	3	0	−2
1	1	4	7	7	
1	1	5	12		
1	1	6			
	1				

	1	60	1 200	7 000	−20 000
2	1	62	1 324	9 648	−704
2	1	64	1 452	12 552	
2	1	66	1 584		
2	1	68			
	1				

Легко видеть, что следующая цифра корня — нуль, а потому приписываем к полученным коэфициентам двойное количество нулей:

	1	6 800	15 840 000	12 552 000 000	−70 400 000 000
5	1	6 805	15 874 025	12 631 370 125	−7 243 149 375
5	1	6 810	15 908 075	12 710 910 500	
5	1	6 815	15 942 150		
5	1	6 820			
	1				

Итак, мы нашли корень $x = 1,205\ldots$ Теперь применяем способ Ньютона и regula falsi:

$$\begin{array}{r} 12\,710\,910\,500 \\ 15\,942\,150 \\ 6\,821 \\ \hline 12\,726\,859\,471 \end{array}$$

Делим сокращенным способом:

7 243 149 375	12 710 910 500
6 355 455	0, 569
887 694	
762 654	
125 400	
114 390	
10 650	

7 243 049 375	12 726 859 471
6 363 425	0, 569
889 724	
763 608	
116 116	
114 534	
1 582	

В следующих цифрах будет уже расхождение, но первые три цифры сходятся в обоих способах, как и надо было ожидать, принимая во внимание, что способом Горнера мы нашли уже три десятичных знака. Итак, искомый корень $x = 1,205569\ldots$, с точностью до 10^{-6}.

Пример 2. Дано уравнение $x^3 - 2x - 14 = 0$; вычислим его положительный корень; легко видеть, что он лежит между 2 и 3, т. е. целая его часть есть 2. По

способу Горнера находим два его первых десятичных знака:

	1	0	−2	−14
2	1	2	2	−10
2	1	4	10	
2	1	6		
	1			

	1	60	1 000	−10 000
6	1	66	1 396	−1 624
6	1	72	1 828	
6	1	78		
	1			

	1	780	182 800	−1 624 000
8	1	788	189 104	−111 168
8	1	796	195 472	
8	1	804		
	1			

Итак, искомый корень $x = 2,68\ldots$ Теперь применим способ Ньютона и regula falsi; для этого следует разделить 111 168 на 195 472 (способ Ньютона) и на 195 472 + 804 + 1 (regula falsi); при этом мы ожидаем, что в частных сойдутся два первых десятичных знака:

111 168	195 472
97 736	0,56
134 320	
117 282	
17 038	

111 168	196 277
981 385	0,56
130 295	
117 762	
12 533	

Итак, искомый корень $x = 2,6856\ldots$; применяем еще раз способ Ньютона и regula falsi; для этого строим далее схему Горнера:

	1	80 400	1 954 720 000	−111 168 000 000
56	1	80 456	1 959 225 536	−1 451 369 984
56	1	80 512	1 963 734 208	
56	1	80 568		
	1			

1 963 734 208
80 569
1 963 814 777

14 513 699 840	1 963 734 208
13 746 139 456	0,7390
767 560 384	
589 120 260	
178 440 124	
176 736 078	
1 704 046	

14 513 699 840	1 963 814 777
13 746 704 993	0,7390
766 994 847	
589 144 431	
177 850 416	
176 743 323	
1 107 093	

Как и следовало ожидать, в частных сошлись четыре первых цифры. Итак, искомый корень

$$x = 2,68567390\ldots$$

с точностью до 10^{-8}.

Упражнения

129) Вычислить с точностью до $0,0001$ корни уравнения $x^3 - 4x + 2 = 0$.

Отв. $x_1 = 1,6751\ldots$, $x_2 = 0,5391\ldots$, $x_3 = -2,2143\ldots$

130) Вычислить вещественный корень уравнения $x^3 - 3x^2 - 3 = 0$.

Отв. $x_1 = 3,279018\ldots$

131) Вычислить корни уравнения $x^3 - 16x^2 - 256x + 256 = 0$.

Отв. $x_1 = 25,6069\ldots$, $x_2 = 0,9472\ldots$, $x_3 = -10,5541\ldots$

132) Вычислить вещественные корни уравнения $x^5 - x - 1 = 0$ с точностью до 10^{-8}.

Отв. Единственный вещественный корень: $1,167303$.

133) То же самое для уравнения $x^3 + 3x^2 - 3 = 0$.

Отв. $0,879385$, $-1,347296$, $-2,532088$.

§ 98. Метод итерации. Принцип итерации (повторения) состоит в следующем: пусть данное уравнение приведено к виду:

$$f_1(x) = f_2(x), \tag{23}$$

причем $f_1(x)$ такая функция, что уравнение $f_1(x) = \alpha$ при всяком α однозначно решается. Предположим, что нам известно приближенное значение $x = x_1$ корня уравнения (23); подставим это значение в правую часть (23), т. е. вычислим $f_2(x_1)$ и решим (относительно x) уравнение:

$$f_1(x) = f_2(x_2);$$

это решение x_2 не равно в точности x_1 [как должно было бы быть, если бы x_1 было, точным корнем уравнения (23)]. Теперь вычислим $f_2(x_2)$ и решим уравнение:

$$f_1(x) = f_2(x_2);$$

пусть x_3 его решение; вычислим $f_2(x_3)$ и решим уравнение:

$$f_1(x) = f_2(x_3);$$

найдем x_4 и т. д. Таким образом мы находим ряд чисел:

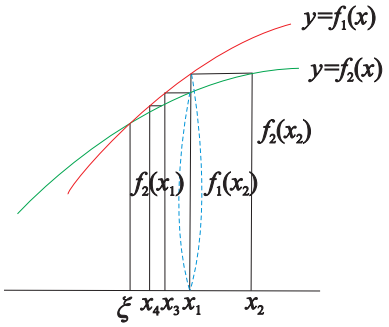
$$x_1,\ \ x_2,\ \ x_3,\ \ldots;$$

если существует $\lim\limits_{n\to\infty} x_n = \xi$, то ξ и есть точный корень уравнения (23), ибо мы имеем:

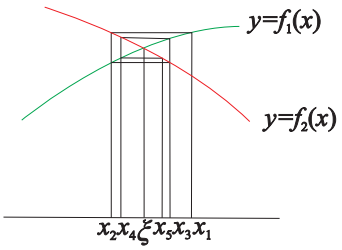
$$f_1(x_{n+1}) = f_2(x_n),$$

и следовательно:

$$\lim_{n\to\infty} f_1(x_{n+1}) = \lim_{n\to\infty} f_2(x_n);$$



Черт. 23



Черт. 24

а так как все наши функции непрерывны, то

$$\lim_{n\to\infty} f(x_{n+1}) = f_1\left(\lim_{n\to\infty} x_{n+1}\right) = f_1(\xi),$$

подобно же

$$\lim_{n\to\infty} f_2(x_n) = f_2\left(\lim_{n\to\infty} x_n\right) = f_2(\xi),$$

следовательно:

$$f_1(\xi) = f_2(\xi).$$

Чертежи 23, 24 дают геометрическое представление метода итерации (два разных случая). Следует заметить, что этот метод далеко не всегда приводит к цели, т. е. действительно дает приближения искомого корня: может случиться, что ряд чисел $x_1, x_2, x_3, \ldots$ не имеет предела, например, эти числа могут удаляться от корня, как это представлено на черт. 25, вместо того чтобы приближаться к нему. В каждом отдельном случае необходимо специальное исследование, — выяснение того, существует ли предел ξ.

Весьма простой случай метода итерации имеем, если $f_1(x) = x$, т. е. данное уравнение имеет вид:

$$x = \varphi(x). \tag{24}$$

Корень этого уравнения геометрически представляется как пересечение кривой $y = \varphi(x)$ прямой $y = x$ (черт. 26).

Здесь мы имеем:

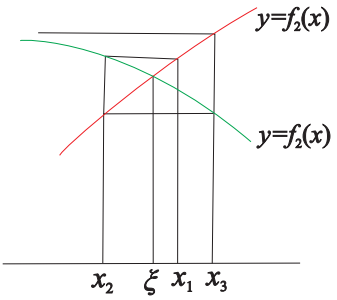
$$x_2 = \varphi(x_1), \quad x_3 = \varphi(x_2), \quad \text{вообще} x_{n+1} = \varphi(x_n).$$

Уравнение $f(x) = 0$ сводится к виду (24), если его написать следующим образом:

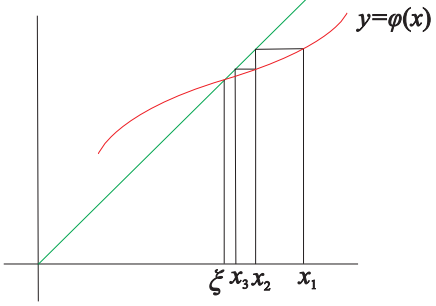
$$x = x + f(x), \quad \text{или} \quad x = x - f(x),$$

причем функцию $f(x)$ можно предварительно разделить на какое-нибудь число или функцию, не обращающуюся в нуль вблизи искомого корня. Разделив, например, $f(x)$ на $f'(x)$, заменим наше уравнение таким:

$$x = x - \frac{f(x)}{f'(x)},$$



Черт. 25



Черт. 26

следовательно:

$$x_2 = x_1 - \frac{f(x_1)}{f'(x_1)}, \quad x_3 = x_2 - \frac{f(x_2)}{f'(x_2)}, \ \ldots$$

это — способ Ньютона, являющийся, таким образом, специальным случаем метода итерации.

Пример. Дано уравнение:

$$x = \sqrt{x} + 1.$$

При $x = 2$ его левая часть меньше правой; при x =3 — наоборот; следовательно, между 2 и 3 лежит корень данного уравнения. Берем $x = 2$ и вычисляем:

$$\begin{aligned}
x_2 &= \sqrt{2} + 1 \approx 2,4142,\\
x_3 &= \sqrt{2,4142} + 1 \approx 2,5532,\\
x_4 &= \sqrt{2,5532} + 1 \approx 2,5978,\\
x_5 &= \sqrt{2,5978} + 1 \approx 2,6117,\\
x_6 &= \sqrt{2,6117} + 1 \approx 2,6160,\\
x_7 &= \sqrt{2,6160} + 1 \approx 2,6174,\\
x_8 &= \sqrt{2,6174} + 1 \approx 2,6178,\\
x_9 &= \sqrt{2,6178} + 1 \approx 2,6179,
\end{aligned}$$

а далее будет $x_{10} = x_{11} = \ldots \approx 2,6179$; следовательно, наш корень равен $2,6179$ с точностью до 10^{-4}.

Упражнения

Методом итерации вычислить с точностью до $0,001$ корни следующих уравнений:

134) $x = 1 + \dfrac{1}{x^2}$.

Отв. $x = 1,467$.

135) $x = \sqrt{x} + \sqrt{x+1}$.

Отв. $x = 4,437$.

136) $x = \sqrt{x} + \dfrac{1}{\sqrt{x}}$.

Отв. $x = 2,149$.

§ 99. Способ Грэффе и Энке (Graffe, Encke). Идея этого способа состоит в следующем: пусть данное уравнение $f(x) = 0$ n-й степени имеет корни

$x_1, x_2, \ldots, x_n$.

Построим уравнение, корнями которого были бы k-е степени корней данного уравнения, т. е. $x_1^k, x_2^k, \ldots, x_n^k$. Пусть это уравнение имеет вид:

$$x_n - F_1 x^{n-1} + F_2 x^{n-2} - \ldots + (-1)^n F_n = 0. \tag{25}$$

Тогда по формулам Вьета (§ 50) имеем:

$$F_1 = x_1^k + x_2^k + \ldots + x_n^k = x_1^k\left[1 + \left(\frac{x_2}{x_1}\right)^k + \left(\frac{x_3}{x_1}\right)^k + \ldots\right],$$

$$F_2 = x_1^k x_2^k + x_1^k x_3^k + \ldots + x_{n-1}^k x_n^k = x_1^k x_2^k\left[1 + \left(\frac{x_1 x_3}{x_1 x_2}\right)^k + \ldots\right],$$

$$F_3 = x_1^k x_2^k x_3^k + x_1^k x_2^k x_4^k + \ldots = x_1^k x_2^k x_3^k\left[1 + \left(\frac{x_1 x_2 x_4}{x_1 x_2 x_3}\right)^k + \ldots\right],$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,$$

$$F_n = x_1^k x_2^k \cdots x_n^k.$$

Пусть между абсолютными величинами корней существует соотношение: $|x_1| > |x_2| > \ldots > |x_n|$; тогда при достаточно большом k степенями $\left(\frac{x_2}{x_1}\right)^k$, $\left(\frac{x_3}{x_1}\right)^k$, $\ldots$, $\left(\frac{x_3}{x_2}\right)^4$, $\ldots$ можно будет пренебречь, и мы приближенно получим

$$F_1 \approx x_1^k, \quad F_2 \approx x_1 6k x_2^k, \ \ldots, \ F_n \approx x_1^k x_2^k \cdots x_n^k,$$

и, значит,

$$x_1^k = F_1, \ \ x_2^k = \frac{F_2}{F_1}, \ \ x_3^k = \frac{F_3}{F_2}, \ \ldots, \ x_n^k = \frac{F_n}{F_{n-1}}.$$

Отсюда, извлекая корни k-й степени и беря подходящим образом знаки этих корней, найдем $x_1, x_2, \ldots, x_n$ (если все они вещественны).

В главе VIII мы изложим общие способы нахождения коэфициентов $F_1, F_2, \ldots$, F_n уравнения (25) для любого целого положительного показателя k. Теперь же мы разберем случай $k = 2$, т. е. укажем, как построить уравнение, корни которого были бы квадратами корней данного уравнения. Применяя тот же способ к получаемому уравнению, найдем уравнение, корни которого уже четвертые степени корней данного уравнения и т. д. Пусть в данном уравнении высший коэфициент равен единице: $f(x) = x^n + a_1 x^{n-1} + \ldots + a_n = 0$; корни его: $x_1, x_2, \ldots, x_n$; уравнение $f_1(x) = x^n - a_1 x^{n-1} + a_2 x^{n-2} - \ldots + (-1)^n a_n = 0$ имеет, очевидно, корни: $-x_1, -x_2, \ldots, -x_n$. Отсюда, очевидно:

$$f(x) f_1(x) = (x^2 - x_1^3)(x^2 - x_2^2) \cdots (x^2 - x_n^2) = F(x^2) = F(z)$$

при $z = x^2$; уравнение $F(z) = 0$ имеет корни $x_1^2, x_2^2, \ldots, x_n^2$. Но мы заменим в функции $F(z)$ z на $-z$ и умножим все коэфициенты на $(-1)^n$; получим уравнение $G(z) = 0$, корни которого суть $-x_1^2, -x_2^2, \ldots, -x_n^2$. Вычисляя произведение $f(x) \cdot f_1(x)$, мы легко найдем коэфициенты функции $G(z)$:

$$G(z) = z^n + (a_1^2 - 2a_2) z^{n-1} + (a_2^2 - 2a_1 a_3) + 2a_4) z^{n-2} +$$
$$+ (a_3^2 - 2a_2 a_4 + 2a_1 a_5 - 2a_6) z^{n-3} + \ldots + a_n^2 = 0.$$

Здесь видно, по какому закону составляются дальнейшие коэфициенты. Если уравнение невысокой степени, например, четвертой, то $a_5, a_6, \ldots$ в этих формулах следует просто положить равными нулю.

Найдя коэфициенты $A_1 = a_1^2 - 2a_2$, $A_2 = a_2^2 - 2a_1a_3 + 2a_4, \ldots$ функции $G(z)$, мы с ними поступаем так же, как с коэфициентами $a_1, a_2, \ldots$, т. е. находим $B_1 = A_1^2 - 2A_2$, $B_2 = A_1^2 - 2A_1A_3 + 2A_4, \ldots,$ — коэфициенты уравнения $G_1(z) = 0$ с корнями $-x_1^4, -x_2^4, \ldots, -x_n^4$, и т. д. Мы заменяем в функции $F(z)$ z на $-z$ и переходим к функции $G(z)$ для того, чтобы прямо получить:

$$a_1^2 - 2a_2 = x_1^2 + x_2^2 + \ldots + x_n^2,$$
$$a_2^2 - 2a_1a_3 + 2a_4 = x_1^2x_2^2 + x_1^2x_3^2 + \ldots$$

и т. д. (без изменения знаков). Переходя от $f(x) = 0$ к $G(z)$, далее к $G_1(z) = 0$ и т. д., мы получаем все большие коэфициенты; поэтому уже со второго или с третьего этапа вычислений приходится пользоваться логарифмами для вычислений: $A_1^2 - 2A_2$, $A_2^2 - 2A_1A_3 + 2A_4$ и т. д.; так как эти выражения представляют собою алгебраические суммы, то необходимо применять гауссовы логарифмы суммы и разности [44], без которых способ Грэффе было бы совершенно невозможно практически применять.

Пример. Решить уравнение $x^3 - 4x^2 + 2 = 0$.

Легко видеть, что все три корня этого уравнения вещественны; из них два положительных и один отрицательный; последний находится между 0 и -1. Применяя способ Грэффе, строим таблицу:

k	$a_1^2 - 2a_2$	$a_2^2 - 2a_1a_3$	a_3^2
2	16	16	4
4	224	128	16
	2,35025	2,10721	1,20412
8	4,69828	3,96451	2,40824
16	9,39656	7,77360	4,81648
32	18,79312	15,50497	9,63296
64	37,58624	31,00766	19,26592
128	75,17248	62,01531	38,53184

Начиная со второго этапа, мы применяем уже логарифмы, т. е. на соответственных местах таблицы стоят уже не самые коэффициенты, а их логарифмы. Мы видим, что, начиная с $k = 16$, логарифм первого коэфициента просто удваивается каждый раз; это значит, что вычитаемое $2a_2$ так мало по сравнению с уменьшаемым a_1^2, что на пятизначных таблицах вычитание $2a_2$ не отражается. Логарифм второго коэфициента начинает удваиваться при переходе от $k = 64$ к $k = 128$. Продолжать этот процесс уже не имеет смысла, так как в дальнейшем (при $k = 256, 512, \ldots$) логарифмы коэфициентов будут просто удваиваться, т. е.

[44] Как это ни странно, но логарифмы Гаусса малоизвестны широким кругам лиц, изучающим математику; не имея возможности изложить здесь эти элементарные вещи, могу рекомендовать желающим ознакомиться с ними хотя бы вступительную главу в таблицах логарифмов Пржевальского.

мы достигли уже предельной точности для пятизначных таблиц. Таким образом имеем:

$$\begin{aligned}
\lg F_1 &= \lg x_1^{128} = 75,17248,\\
\lg \frac{F_2}{F_1} &= \lg x_2^{128} = 62,0531 - 75,17248 = \overline{14},84283,\\
\lg \frac{F_3}{F_2} &= \lg x_3^{128} = 38,53184 - 62,01531 = \overline{24},51653;
\end{aligned}$$

делим теперь эти логарифмы на 128 и получаем:

$$\lg |x_1| = 0,58729, \qquad \lg |x_2| = \overline{1},89721, \qquad \lg |x_3| = \overline{1},81654,$$

отсюда

$$|x_1| = 3,866, \qquad |x_2| = 0,789, \qquad |x_3| = 0,655;$$

очевидно, что $x_1 > 0$; из корней же x_2 и x_3 один меньше нуля. Определить их знаки мы могли бы в общем случае хотя бы непосредственной подстановкой их в заданное уравнение; в данном же примере мы можем воспользоваться тем, что $x_1 + x_2 + x_3 = 4$; но мы имеем $3,856 + 0,789 - 0,655 = 4$; следовательно, $x_1 = 3,866$, $x_2 = 0,789$, $x_3 = -0,655$.

Если нужно вычислить корни с большей точностью, то, исходя из найденных значений их, применяем способ Ньютона и regula falsi.

§ 100. Разберем еще случай существования комплексных корней у данного уравнения. Пусть все коэфициенты уравнения вещественны, но пусть, например, корни x_2 и x_3 — сопряженные комплексные, тогда как x_1 и x_4 вещественны; пусть

$$x_2 = r(\cos\varphi + i\sin\varphi) \quad \text{и} \quad x_3 = r(\cos\varphi - i\sin\varphi);$$

пусть $x_1 > r > x_4 > \ldots$ Имеем:

$$\begin{aligned}
F_1 &= x_1^k + x_2^k + \ldots + x_n^k \approx x_1^k,\\
F_2 &= x_1^k(x_2^k + x_3^k) + x_1^k x_4^k + \ldots = 2x_1^4 r^k \cos k\varphi + \ldots,\\
F_3 &= x_1^k x_2^k x_3^k + \ldots \approx x_1^k x_2^k x_3^k = x_1^k r^{2k},\\
F_4 &= x_1^k x_2^k x_3^k x_4^k = x_1^k r^{2k} x_4^k.
\end{aligned}$$

Отсюда видно, что коэфициент F_2 выказывает неправильности; он может, например, менять знак, и логарифм его с увеличением k вообще не будет удваиваться хотя бы приближенно.

Далее, имеем $x_1^k = F_1$, $r^{2k} = \dfrac{F_3}{F_1}$, $x_4^k = \dfrac{F_4}{F_3}$. Отсюда найдем r.

Чтобы найти φ в случае одной пары комплексных корней, воспользуемся равенством:

$$-a_1 = x_1 + x_2 + \ldots + x_n = x_1 + 2r\cos\varphi + x_4 + \ldots + x_n,$$

откуда найдем $\cos\varphi$ и самый угол φ.

В случае существования нескольких пар комплексных корней абсолютные их величины находятся так же; для определения же их аркусов, кроме равенства

$-a_1 = x_1 + x_2 + \ldots + x_n$ можно взять еще $-\dfrac{a_{n-1}}{a_n} = \dfrac{1}{x_1} + \dfrac{1}{x_2} + \ldots + \dfrac{1}{x_n}$, где каждая пара (например, x_2 и x_3) сопряженных комплексных корней дает:

$$\frac{1}{x_2} + \frac{1}{x_3} = \frac{2}{r} cos\varphi$$

и т. д.

Для трех пар комплексных корней берем еще равенство:

$$x_1^2 + x_2^2 + \ldots + x_n^2 = a_1^2 - 2a_2;$$

здесь

$$x_2^2 + x_3^2 = 2r^2 \cos 2\varphi.$$

Таким образом мы всегда можем найти достаточное число уравнений для определения аркусов всех пар сопряженных комплексных корней. Очень не выгоден случай, когда имеется несколько пар комплексных корней с равными абсолютными величинами; в таком случае делаем в нашем уравнении подстановку $y = x - b$; за b можно взять $|a_n^{\frac{1}{n}}|$ — среднее значение абсолютной величины корней. Так же можно поступить, если уравнение имеет два вещественных корня с одной и той же абсолютной величиной α и $-\alpha$. Впрочем в этом последнем случае, как и вообще в случае существования двух корней, абсолютные величины которых мало отличаются друг от друга, можно применить следующий прием: пусть, например, $|x_2| \approx |x_3|$; это выявится опять на неправильностях коэфициента $F_2 = x_1^k x_2^k + x_1^k x_3^k + \ldots$. Но $F_3 \approx x_1^k x_2^k x_3^k$, $F_1 \approx x_1^k$; следовательно:

$$\frac{F_3}{F_1} \approx x_2^k x_3^k = v^k;$$

тут $v = x_2 x_3$, $|v| \approx \sqrt[k]{\dfrac{F_3}{F_1}}$. Из формулы же

$$-a_1 + x_1 + x_2 + \ldots + x_n$$

найдем $x_2 + x_3 = t$ (если остальные корни известны). Теперь решаем уравнение $x^2 - tx + v = 0$ и находим x_2 и x_3.

Трудность заключается только, в определении знака у v; иногда этого можно достичь путем простого соображения. Желающим подробнее ознакомиться с этим способом могу рекомендовать книгу акад. А.Н. Крылова, Лекции о приближенных вычислениях, 2-е издание ГТТИ, 1932, гл. II. См. также Э. Уиттекер и Г. Робинсон, Математическая обработка результатов наблюдений, ГТТИ, 1933, гл. VI; Дж. Скарборо, Численные методы математического анализа, ГТТИ, 1934, гл. X.

Пример. Решить уравнение:

$$x^3 + x - 6 = 0.$$

Строим таблицу[45]:

k	$a_1^2 - 2a_2$	$a_2^2 - 2a_1a_3$	a_3^2
2	-2	1	36
4	2	145	1296
	$0,30103$	$2,16137$	$3,11261$
8	$2,45637n$	$4,19978$	$6,22522$
16	$4,69997$	$9,08340$	$12,45044$
32	$7,94494$	$18,07386$	$24,90088$
64	$18,07242n$	$36,14729$	$49,80176$
128	$36,14973n$	$72,29461$	$99,60352$

Из того, что первые коэфициенты выказывают неправильность и меняют знак, следует, что корки x_1, x_2 сопряженно комплексны. Таким образом второй коэфициснт (при $k = 128$) приближенно равен $r^{2k} = r^{256}$, где $r = |x_1| = |x_2|$; частное третьего и второго приближенно равно $|x_3|^{128} = x_3^{128}$. Итак,

$$256 \lg r = 72,29461, \qquad \lg r = 0,28240, \qquad r = 1,9150,$$
$$128 \lg x_3 = 99,60352 - 72,29461 = 27,30891, \qquad \lg x_3 = 0,21334, \qquad x_3 = 1,6343$$

(здесь, очевидно, $x_3 > 0$). Сумма всех корней здесь равна нулю; следовательно, имеем:

$$2r\cos\varphi = -x_2, \qquad \cos\varphi = -\frac{x_3}{2r}, \qquad \cos(180^\circ - \varphi) = \frac{x_3}{2r},$$
$$\lg\cos(180^\circ - \varphi) = 0,21334 - 0,58343 = \overline{1},62991, \qquad 180^\circ - \varphi = 64^\circ 45' 18'',$$
$$\varphi = 115^\circ 14' 42'',$$
$$\lg\sin\varphi = \overline{1},95640, \qquad \lg(r\cos\varphi) = 1,91231n, \qquad \lg(r\sin\varphi) = 0,23880,$$

отсюда

$$r\cos\varphi = -0,8172, \qquad r\sin\varphi = 1,7330.$$

Итак, наши корни:

$$x_1 = -0,8172 + i1,7330 = 1,9150(\cos 115^\circ 14' 42'' + i\sin 115^\circ 14' 42''),$$
$$x_2 = -0,8172 - i1,7330 = 1,9150(\cos 115^\circ 14' 42'' - i\sin 115^\circ 14' 42''), \ .$$
$$x_3 = 1,6343.$$

Способ Грэффе в настоящее время признается самым практичным способом вычисления корней. Его преимущества перед другими способами состоят в том, что он не требует предварительного отделения корней, дает сразу все вещественные корни, а также позволяет вычислить и комплексные корни, причем он — единственный более или менее практичный способ вычисления комплексных корней. Недостатки способа Грэффе следующие: во-первых, он требует вычислений с логарифмами, да при этом еще с логарифмами суммы и разности, следовательно,

[45]Буква n означает, что число отрицательное и логарифм берется от его абсолютной величины.

точность вычисления весьма ограничена [46]; во-вторых, по существу он дает только абсолютные величины корней: для определения знаков вещественных корней, собственно, правил никаких не имеется; определение же аркусов комплексных корней (особенно, если таких корней несколько пар) весьма громоздко и по существу является только дополнением к способу Грэффе.

За последнее время способ Грэффе применяют и без логарифмов, но с помощью арифмометра; подробнее с этим можно ознакомиться в упомянутой уже выше книге Скарборо, Численные методы математического анализа.

Упражнения

Решить способом Грэффе уравнения, данные в упражнениях 126, 127, 129, 130, 131, 132 и 133.

§ 101. Способ Лагранжа. Пусть известно, что уравнение $f(x) = 0$ имеет корень между двумя целыми числами: a и $a+1$; подставляем $x = a + \dfrac{1}{y}$ и получаем уравнение для y: $\varphi(y) = 0$, которое должно иметь корень $y > 1$; пусть этот корень лежит между целыми числами b и $b+1$; подставляем $y = b + \dfrac{1}{z}$ и получаем уравнение для z: $\psi(z) = 0$ и т. д.

Получаем искомый корень в виде непрерывной дроби:

$$x = a + \cfrac{1}{b + \cfrac{1}{c + \dots}}.$$

Пример. $f(x) = x^3 - x - 1$; подставляем:

$$x = y + \frac{1}{y};$$

вычисляем:

	1	0	−1	−1
1	1	1	0	−1
1	1	2	2	
1	1	4		
	1			

и получаем уравневие для y: $y^3 - 2y^2 - 3y - 1 = 0$; его корень лежит между 3 и 4,

[46] У нас имеются лишь пятизначные таблицы гауссовых логарифмов суммы и разности; в семизначных таблицах Вега гауссовых логарифмов нет. Существуют отдельные семизначные таблицы гауссовых логарифмов, но они являются редкостью.

подставляем: $y = 3 + \dfrac{1}{z}$ и вычисляем:

	1	−2	−3	−1
1	1	1	3	−1
1	1	2	12	
1	1	7		
	1			

Получаем уравнение для z:

$$z^3 - 12z^2 - 7z - 1 = 0;$$

его корень лежит между 12 и 13.

Итак, $x = 1 + \dfrac{1}{3 + \dfrac{1}{12 + \dots}} = 1,324$ с точностью до $0,001$.

Упражнения

137) Разложить, в непрерывные дроби вещественные корни уравнения $x^4 + x - 5 = 0$.

Отв. $(1, 2, 1, 1, 1, \dots)$, $(-2, 2, 1, 1, 12, \dots)$.

138) Найти 4 звена непрерывной дроби для вещественного корня уравнения $3x^3 - 2x^2 - 10 = 0$ и вычислить этот корень посредством найденной непрерывной дроби.

Отв. $x = (1, 1, 3, 27, \dots) = 1,7522$.

§ 102. Общие замечания. Решение алгебраических уравнений, т. е. приближенное вычисление их корней, очень важно для приложений: и в других областях математики часто решение поставленной задачи сводится к вычислению корней уравнений (алгебраических, а часто и трансцендентных), например, при нахождении экстремума функций, при интегрировании линейных диференциалыих уравнений, при исследовании кривых и поверхностей в геометрии и т. п., в механике и во многих областях техники, наконец, в астрономии тоже применяются алгебраические уравнения и приходится их решать. Поэтому нет ничего удивительного в том, что исследования в области решения уравнений имеют свое начало еще в древности. Трудность решения алгебраического уравнения сильно возрастает с возрастанием его степени. Естественно, что исторически дело шло так, что раньше были найдены решения уравнений низших степеней и только в XVIII–XIX веках люди научились вычислять корни всяких уравнений вообще.

Уравнения первой степени, можно сказать, были известны уже древним египтянам за 2000 лет до нашей эры, конечно, не в нашей символической форме, а в виде определенного типа задач; было даже специальное название для неизвестного «хау», что значит «куча»; еще с того времени идет и способ нахождения неизвестного, называемый теперь regula falsi, о чем уже было сказано выше (§ 96). Наша обычная формула решения квадратного уравнения по существу (как определенное «правило», выраженное словами) была знакома древним грекам (Герон, 100 г. до

н. э., Диофант, III в, н. э.); правда, они знали только одно положительное решение, отрицательных чисел они совсем не знали. Эту же формулу знали и индусы (Ариабхатта, конец V в. н. э., Брамагупта, VII в. н. э.), при этом позже они нашли оба корня квадратного уравнения (Бхаскара, XII, в.).

Это «правило» или, по-современному, — формула решения квадратного уравнения дает нам определенную, конечную совокупность действий (начиная от сложения и кончая извлечением корня) в определенной последовательности, которые нужно произвести над коэфициентами, чтобы получить искомые корни. Это так называемое «алгебраическое» решение, или решение в «радикалах». Естественно, что и, решение уравнений высших степеней старались найти в радикалах, да и вообще такие решения считались вполне естественными, об иных решениях не было и речи. Но в дальнейшем дело пошло туже; арабы нашли решения некоторых типов уравнений третьей и четвертой степеней в геометрическом виде (как пересечения кривых второго порядка). Общие решения уравнений третьей и четвертой степеней в радикалах найдены в первой половине XVI в. в Италии. Сципионе даль Ферро (Scipione dal Ferro) первый в 1505 г. нашел решение кубического уравнения, но не опубликовал его; оно вскоре было переоткрыто математиком Николо Тарталья (Nicolo Tartaglia); Гиеронимо Кардано (Hieronimo Cardano) опубликовал это решение (с указанием имен и Тарталья, и Ферро) в 1545 г. в сочинении «Ars magna sive de rebis algebraicis, über unus» [47]; отсюда и формула решения кубического уравнения неправильно называется «формулой Кардано» (см. гл. VII, § 124). В этом же сочинении «Ars magna» находится и способ алгебраического решения общего уравнения четвертой степени, открытый учеником Кардано, Лодовико Феррари (Lodovico Ferrari).

Что касается уравнений степени выше четвертой, то их не удавалось решить в общем виде в радикалах, пока, наконец, Паоло Руффини (Paolo Ruffini) в 1799 г. и Нильс Генрик Абель (Nils Henrik Abel) в 1825 г. [48] не доказали, что таких решений и не существует, т. е. не существует общих формул, содержащих, кроме рациональних действий, еще только радикалы, для решения уравнений степени выше четвертой.

Но приближенное вычисление корней алгебраических уравнений было известно весьма давно, хотя общие методы этих вычислений появились только в XVII в. Еще Леонард Пизанский (начало XIII в.) вычислил корень уравнения $x^3 + 2x^2 + 10x = 20$ с ошибкою, меньшей чем $\frac{1}{3}10^{-10}$; к сожалению, метод, которым он пользовался, остался неизвестным. В конце XV в. Бюрги (Bürgi) вычислил корень уравнения для стороны правильного девятиугольника: $9 - 30x^2 + 27x^4 - 9x^6 + x^8 = 0$; способ, применяемый им, есть не что иное, как regula falsi. Приблизительно в то же время Ф. Вьет (F. Viète) дал общий способ вычисления корней в виде формулы, несколько напоминающей формулу Ньютона.

В настоящее время имеется весьма много способов приближенного вычисления корней; кроме тех способов, которые приведены у нас, существует еще способ Даниэля Бернулли (Daniel Bernoulli), являющийся прототипом способа Грэффе; он был далее разработан Эйлером (Euler) и Якоби (Jacobi). В практике весьма

[47] «Великое искусство или об алгебраических вещах, одна книга».

[48] Доказательство Абеля опубликовано в первом томе «Journal für die eine und angewandte Mathematik (Crelle)».

распространены графические способы решения уравнений [49]; эти способы хоть и неточны, но зато практически удобны для нахождения первого приближения, к которому затем уже следует вычислять поправку; для отдельных типов уравнений имеются номограммы, а также и таблицы. Были найдены способы вычисления корней алгебраических уравнений посредством бесконечных рядов [50]; Г. М. Баженов (в Воронеже) [51] проанализировал эти способы и дал практический способ вычисления корней с заранее заданной точностью. Из иных способов вычисления корней алгебраических уравнений, которые разрабатывались в СССР, назовем еще способ Л.И. Креера (в г. Орджоникидзе на Кавказе) вычисления корней посредством тригонометрических функций [52] и интересный способ В.Ф. Бржечки (в Харькове), родственный способу Грэффе[53]. Но все эти способы уже выходят из пределов собственно алгебры, а относятся к теории приближенных вычислений.

[49]См., например, Arthur Schultze, Graphic Algebra; есть украинский перевод: А Шульце, Графічна алгебра, ОНТВУ, 1933.

[50]См. Максимович, О разложении функций от корней уравнения в ряды, Казань, 1882; см. также Gosh, New methods of approximating to the roots of a numerical equation, «Journ. of the Department of Science,» vol. VII, Calcutta, 1925.

[51]G.M. Bazenow, Über die Berechnung der Wurzeln von algebraischen Gleichungen mit Hilfe der unendlichen Reihen. «Записки Харк. матем. т-ва», сер. 4, т. VII (1933), стр. 39–44.

[52]Л.И. Креер, Приближенное вычисление вещественных корней алгебраических уравнений (гониометрическая метода), «Математический сборник», т. 41 (1934), стр. 317–331.

[53]В. Бржечка, Решение численных уравнений, «Наукові записки наук.-досл. матем. катедр Україні», т. III (1928).

ГЛАВА ШЕСТАЯ

УРАВНЕНИЯ С РАЦИОНАЛЬНЫМИ КОЭФИЦИЕНТАМИ. УРАВНЕНИЯ В ДАННОМ ТЕЛЕ

§ 103. Нахождение рациональных корней. В этой главе мы будем предполагать, что все коэфициенты наших уравнений не только вещественные, но и рациональные числа. Приведя все их к одному знаменателю и умножив на него обе части уравнения, мы получим уравнение, все коэфициенты которого целые числа. Такие уравнения мы и рассмотрим. Наша задача будет состоять в нахождении рациональных корней таких уравнений.

Теорема. Если в уравнении с целыми коэфициентами высший коэфициент равен единице, то все рациональные корни уравнения целые числа.

Доказательство. Пусть $x^n + a_1x^{n-1} + \ldots + a_n = 0$ данное уравнение и $x = \dfrac{a}{b}$ — его рациональный корень; a и b целые, взаимно простые числа. Имеем:

$$\frac{a^n}{b^n} + a_1\frac{a^{n-1}}{b^{n-1}} + \ldots + a_{n-1}\frac{a}{b} + a_n = 0;$$

умножим обе части на b^{n-1} и перенесем все члены кроме первого в правую часть:

$$\frac{a^n}{b} = a_1a^{n-1} - a_2a^{n-2}b - \ldots - a_{n-1}ab^{n-2} - a_nb^{n-1};$$

правая часть — целое число; следовательно, $\dfrac{a^n}{b}$ — целое, т. е. $b =$, ибо a^n и b — взаимно простые; таким образом корень $x = a$ целый.

Займемся теперь разысканием целых корней таких уравнений с целыми коэфициентами и высшим коэфициентом единицей. Если $x_1, x_2, \ldots, x_n$ все корни нашего уравнения, то, как известно (§ 50):

$$f(x) = x^n + a_1x^{n-1} + \ldots + a_n = (x - x_1)(x - x_2)\cdots(x - x_n),$$

откуда следует:

$$a_n = (-1)^n x_1x_2\cdots x_n.$$

Из этой последней формулы самой по себе нельзя еще заключить, что всякий целый корень нашего уравнения является делителем числа a_n — ведь произведение $n-1$ остальных корней могло бы и не быть целым! Покажем, что это утверждение тем не менее справедливо. Пусть a — целый корень уравнения

$$f(x) = x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n = 0$$

с целыми коэфициентами и старшим коэфациентом, равным единице. Как мы знаем, $f(x)$ делится нацело на $x-a$, так что

$$f(x)=(x-a)(x^{n-1}+\alpha_1 x^{n-2}+\ldots+\alpha_{n-2}x+\alpha_{n-1}).$$

Так как $a\alpha_{n-1}=-a_n$, то достаточно показать, что α_{n-1} — целое.

Но (§ 51, способ Горнера)

$$\begin{aligned}
\alpha_1 &= a_1+a,\\
\alpha_2 &= a_2+a\alpha_1,\\
\alpha_3 &= a_3+a\alpha_2,\\
&\ldots\ldots\ldots\ldots\ldots,\\
\alpha_{n-1} &= a_{n-1}+a\alpha_{n-2}.
\end{aligned}$$

Так как a и все коэфициенты $a_1,\ldots,a_{n-1}$ — целые числа,, то получаем последовательно, что α_1, α_2, α_3 и т. д. и, наконец, α_{n-1} — тоже целые числа. Тем самым наше утверждение доказано: всякий целый корень нашего уравнения есть делитель целого числа a_n; найдя все целые делители числа a_n (как положительные, так и отрицательные), мы получим числа, среди которых имеются все целые корни нашего уравнения, если только наше уравнение вообще имеет целые корни. Остается только подставить все эти делители в данное уравнение и отбросить те, которые ему не удовлетворяют. Далее, если $x=a$ — целый корень нашего уравнения, то $f(x)$ делится нацело на $x-a$ и на $a-x$ (§ 49) при всяком целом x. В частности $f(1)$ делится на $a-1$? $f(-1)$ на $a+1$. Значения $f(1)$ и $f(-1)$ легко вычислить. Следовательно, мы можем с самого начала отбросить те делители a числа a_n, для которых хоть одно из чисел $\dfrac{f(1)}{a-1}$, $\dfrac{f(-1)}{a+1}$ не целое.

Пусть $x=a$ целый корень нашего уравнения; меняя несколько предыдущие обозначения, напишем:

$$\frac{f(x)}{x-a}=-b_0x^{n-1}-b_1x^{n-2}-\ldots-b_{n-1};$$

$b_0,b_1,\ldots,b_{n-1}$ — тоже целые числа. Имеем:

$$x^n+a_1x^{n-1}+\ldots+a_{n-1}x+a_n=(x-a)(-b_0x^{n-1}-b_1x^{n-2}-\ldots-b_{n-1})$$

откуда, сравнивая коэфициенты при одинаковых степенях x, находим

$$\begin{aligned}
a_n &= ab_{n-1},\\
a_{n-1} &= ab_{n-2}-b_{n-1},\\
a_{n-2} &= ab_{n-2}-b_{n-2},\\
&\ldots\ldots\ldots\ldots\ldots,\\
a_1 &= ab_0-b_1\\
1 &= -b_0.
\end{aligned}$$

Отсюда:

$$\begin{aligned} b_{n-1} &= \frac{a_n}{a}, \\ b_{n-2} &= \frac{a_{n-1}+b_{n-1}}{a}, \\ b_{n-3} &= \frac{a_{n-2}+b_{n-2}}{a}, \\ &\dots\dots\dots\dots\dots, \\ b_0 &= \frac{a_1+b_1}{a} = -1. \end{aligned}$$

Другими словами, a_n делится на a; $a_{n-1}+b_{n-1}$ делится (нацело) на a; $a_{n-2}+b_{n-2}$ делится на a и т. д.; наконец, $a_1+b_1=-a$.

Если, деля a_n на a, $a_{n-1}+b_{n-1}$ на a и т. д., мы встретимся с дробным частным, то это число a следует отбросить. Действие располагается, как и в способе Горнера (§ 51), в таблицу:

	a_n	a_{n-1}	a_{n-2}	$\dots$	a_1	1
a	b_{n-1}	b_{n-2}	b_{n-3}	$\dots$	-1	

Каждое найденное число b_k складывается с a_k и делится на a; получается в частном следующее число: b_{k-1}.

Пример. $x^4+2x^3-4x^2-5x-6=0$. Делители числа -6 суть: ±1, ±2, ±3, ±6. Имеем $f(1)=-12$, $f(-1)=-6$; исследуя числа $\dfrac{f(1)}{a-1}$ и $\dfrac{f(-1)}{a+1}$, находим, что следует отбросить числа ±1, ±6 и $+3$.

Остается испробовать числа 2, -2, -3. Пробы эти можно производить в одной таблице, беря для следующих делений числа, получаемые от предыдущих делений: одно и то же число a можно пробовать несколько раз, ибо корень $x=a$ может оказаться кратным. Итак, получаем:

	-6	-5	-4	2	1	
$+2$	-3	-4	-4	-1	0	— годится;
-2	-3					— не годится, ибо -3 не делится на ±2;
-3	1	!	1	0		годится; больше целых корней нет.

Итак,

$$x^4+2x^3-4x^2-5x-6=(x-2)(x+3)(x^2+x+1).$$

Упражнения

Найти целые корни уравнений:

139) $x^5-x^4-25x^3+43x^2+72x-90=0$.

Отв. 1, 3, -5.

140) $x^5-x^4-7x^3+11x^2-8x+12=0$.

Отв. 2, 2, -3.

141) $x^4+4x^3-2x^2-12x+9=0$.

Отв. 1, 1, -3, -3.

142) $x^5+6x^4-17x^3-102x^2+16x+96=0$.

Отв. 1, -11, 4, -4, -6.

143) $x^3 - 10x^2 - 9x - 22 = 0$.

Отв. 11.

§ 104. Пусть теперь дано уравнение:

$$a_0x^n + a_1x^{n-1} + \ldots + a_n = 0,$$

где все коэфициенты целые, и $a_0 > 1$. Умножим обе части уравнения на a_0 и сделаем подстановку: $a_0x = y$; тогда получим:

$$y^n + a_1y^{n-1} + a_0a_2y^{n-2} + \ldots + a_0^{n-1}a_n = 0.$$

Таким образом этот случай сводится к предыдущему. Найдя целые решения y, получим рациональные решения $x = \dfrac{y}{a_0}$ данного уравнения; конечно, дробь — может оказаться и сократимой, может даже быть равной целому числу. Итак:

Теорема. *Все рациональные корни уравнения с целыми коэфициентами имеют знаменателями делители высшего коэфициента.*

Пример. $8x^3 - 14x^2 - 7x + 6 = 0$; умножаем на $8^2 = 64$:

$$512x^3 - 896x^2 - 448x + 384 = 0;$$

положим

$$8x = y;$$

тогда

$$y^3 - 14y^2 - 56y + 384 = 0.$$

Имеем:

$$384 = 2^7 \cdot 3;$$

делители 384:

$$\pm1,\ \pm2,\ \pm3,\ \pm4,\ \pm6,\ \pm8,\ \pm12,\ \pm16,\ \pm24,\ \pm32,\ \pm48,\ \pm64,$$
$$\pm96,\ \pm128,\ \pm192,\ \pm384.$$

Далее: $f(1) = 315$, $f(-1) = 425$; находя $\dfrac{315}{a-1}$ и $\dfrac{425}{a+1}$ видим, что из делителей a числа 384 следует испытать только -2, $+4$, -6, ±16.

Получаем:

	384	-56	-14	1	
-4	-192	124	-55		— не годится,
4	96	10	-1		— годится,
-6	-16	1			— годится,
16	-1				— годится.

Итак, имеются три целых корня: $y = 4, -6, 16$ и соответственно им 3 рациональных корня: $x = \dfrac{1}{2}, -\dfrac{3}{4}, 2$.

Упражнения

Найти рациональные корни уравнений:

144) $24x^4 + 22x^3 - 11x^2 - 7x + 2 = 0$.

Отв. $\frac{1}{2}$, $\frac{2}{3}$, $\frac{1}{4}$, -1.

145) $6x^6 - x^5 - 23x^4 - x^3 - 2x^2 + 20x - 8 = 0$.

Отв. $\frac{1}{2}$, $\frac{2}{3}$, 2, -2.

146) $3x^3 + x^2 + x + 35 = 0$.

Отв. -2, $\frac{1}{3}$.

147) $3x^4 - 50x^2 - 104x - 105 = 0$.

Отв. 5, -3.

§ 105. Приводимые и неприводимые функции. Если уравнение $f(x) = 0$ с рациональными коэфициентами имеет рациональный корень a, то $f(x)$ делится на $x - a$: $f(x) \equiv (x - a)\varphi(x)$; $\varphi(x)$ — тоже ц. р. функция с рациональными коэфициентами. Таким образом в этом случае $f(x)$ раскладывается на два целых множителя с рациональными коэфициентами, из которых один — линейный.

Разберем теперь вообще случай, когда ц. р. функция с рациональными коэфициентами $f(x)$ раскладывается на два целых множителя тоже с рациональными коэфициентами: $f(x) \equiv \varphi(x)\psi(x)$. Такая функция $f(x)$ называется *приводимой*; если же такое разложение невозможно, то функция называется *неприводимой* [54]; сообразно с этим и уравнение $f(x) = 0$ называется *приводимым* или *неприводимым*. Решение приводимого уравнения $f(x) = 0$ распадается на решения уравнений $\varphi(x) = 0$ и $\psi(x) = 0$, степени которых ниже, чем степень уравнения $f(x) = 0$.

§ 106. Функции с целыми коэфициентами. Теорема Гаусса. Рассмотрим ц. р. функции с *целыми* коэфициентами. Пусть $f(x)$ такая функция и δ общий наибольший делитель ее коэфициентов: $f(x) = \delta \cdot \varphi(x)$ — ц. р. функция, в которой коэфициенты взаимно простые: такая функция называется *первообразной*; δ называется делителем функции $f(x)$.

Теорема Гаусса. *Произведение двух первообразных функций — тоже первообразная функция.*

Доказательство. Пусть $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n$ и $g(x) = b_0x^m + b_1x^{m-1} + \ldots + b_m$ первообразные функции;

$$F(x) = f(x)g(x) = c_0x^{n+m} + c_1x^{n+m-1} + \ldots + c_{n+m},$$

где (§ 46)

$$c_{\alpha+\beta} = a_0b_{\alpha+\beta} + a_1b_{\alpha+\beta-1} + \ldots + a_{\alpha-1}b_{\beta+1} + \\ + a_\alpha b_\beta + a_{\alpha+1}b_{\beta-1} + \ldots + a_{\alpha+\beta}b_0.$$

[54] При этом принимаются во внимание только те разложения $f(x) = \varphi(x)\psi(x)$, где степень $\varphi(x) \geq 1$ и степень $\psi(x) \geq 1$; разложения же вида

$$f(x) = C \cdot \left[\frac{1}{C} f(x)\right], \quad \text{где} \quad C = \text{const},$$

не считаются.

Пусть p — любое простое число, большее единицы, и пусть $a_0, a_1, a_2, \ldots, a_{\alpha-1}$ делятся на p, но a не делится на p; точно так же $b_0, b_1, \ldots, b_{\beta-1}$ делятся на p, но b_β не делится на p. [*Все* a_λ или *все* b_μ не могут делиться на p, ибо функции $f(x)$ и $g(x)$ первообразные.] Но тогда $c_{\alpha+\beta}$ не делится на p, ибо в нем все слагаемые делятся на p кроме одного: $a_\alpha b_\beta$. Итак, все c_ν не могут делиться на одно и то же простое число p, т, е. они — взаимно простые, и $F(x)$ первообразная функция.

Эта теорема непосредственно обобщается на случай нескольких сомножителей.

Следствие. Делитель произведения ц. р. функций с целыми коэфициентами равен произведению делителей этих функций.

Доказательство. Пусть $f(x)$ и $g(x)$ такие функции; δ, ε их делители, тогда $f(x) = \delta \cdot f_1(x)$, $g(x) = \varepsilon \cdot g_1(x)$, где $f_1(x)$, $g_1(x)$ — первообразные функции. Далее, $f(x)g(x) = \delta\varepsilon \cdot f_1(x)g_1(x)$; по теореме Гаусса $f_1(x)g_1(x)$ — первообразная функция; следовательно, $\delta\varepsilon$ есть делитель функции $f(x)g(x)$. Это предложение непосредственно обобщается на несколько сомножителей.

§ 107. Теорема. *Если целая рациональная функция с целыми коэфициентами приводима, т. е. раскладывается на два множителя с рациональными коэфициентами, то она раскладывается и на два множителя с целыми коэфициентами.*

Доказательство. Пусть $f(x) = \varphi(x)\psi(x)$; $f(x)$ — с целыми коэфициентами, $\varphi(x)$, $\psi(x)$ — с рациональными коэфициентами. Приведем все коэфициенты в $\varphi(x)$ к одному знаменателю ρ и вынесем за скобки общий наибольший делитель δ числителей всех коэфициентов в $\varphi(x)$; тогда $\varphi(x) = \dfrac{\delta}{\rho} \cdot \varphi_1(x)$, где $\varphi_1(x)$ — первообразная функция; можно предполагать, что $D(\delta, \rho) = 1$, иначе дробь $\dfrac{\delta}{\rho}$ можно сократить. Подобным же образом найдем $\psi(x) = \dfrac{\varepsilon}{\sigma} \cdot \psi_1(x)$, где $\psi_1(x)$ — первообразная функция, и $D(\sigma, \varepsilon) = 1$.

Итак

$$f(x) = \frac{\delta\varepsilon}{\rho\sigma} \cdot \varphi_1(x)\psi_1(x), \qquad \rho\sigma \cdot f(x) = \delta\varepsilon \cdot \varphi_1(x)\psi_1(x);$$

$\varphi_1(x)\psi_1(x)$ — первообразная функция (по теореме Гаусса); следовательно, $\delta\varepsilon$ — делитель правой части, т. е. $\delta\varepsilon$ делится на $\rho\sigma$, т. е. ε делится на ρ, а δ — на σ. Разделив, получим $f(x) = k\varphi_1(x)\psi_1(x)$, где k — некоторое целое число. Итак, $f(x)$ разложилось на два множителя с целыми коэфициентами, что и требовалось доказать.

§ 108. Теорема Эйзенштейна (Eisenstein). *Если* $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n$ *— ц. р. функция с целыми коэфициентами, причем* a_0 *не делится на некоторое простое число* p, $a_1, a_2, \ldots, a_n$ *все делятся на* p, *но* a_n, *делясь на* p, *не делится на* p^2, *— то в этом случае функция* $f(x)$ *неприводима.*

Доказательство. Пусть $f(x)$ — приводимая функция; тогда (по § 107) она раскладывается на два множителя с целыми коэфициентами:

$$\begin{aligned} a_0x^n + a_1x^{n-1} + \ldots + a_n &= \\ &= (b_0x^k + b_1x^{k-1} + \ldots + b_k) \cdot (c_0x^l + c_1x^{l-1} + \ldots + c_l); \end{aligned}$$

отсюда:

$$\begin{aligned} a_n &= b_k c_l, \\ a_{n-1} &= b_k c_{l-1} + b_{k-1} c_l, \\ a_{n-2} &= b_k c_{l-2} + b_{k-1} c_{l-1} + b_{k-2} c_l, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ a_0 &= b_0 c_0. \end{aligned} \tag{1}$$

Отсюда видно: $b_k c_l$ делится на p; следовательно, b_k *или* c_l делится на p; вместе b_k и c_l не могут делиться на p, ибо a_n не делится на p^2. Итак, пусть b_k делится на p. Тогда из второго равенства (1) заключаем: $b_{k-1} c_l$ делится на p, но c_l не делится на p, следовательно, b_{k-1} делится на p. Подобно же из третьего равенства (1) заключим, что b_{k-2} делится на p и т. д.; наконец, из $(k+1)$-го равенства заключим, что b_0 делится на p; но тогда из последнего равенства выводим, что a_0 делится на p, что неверно. Следовательно, функция $f(x)$ неприводима.

Теорема Эйзенштейна дает признак неприводимости функций, имеющий довольно большое применение. Из нее же вытекает:

Следствие. Существуют неприводимые функции какой угодно степени. Например, хотя бы $x^n + 2x^{n-1} + 2x^{n-2} + \ldots + 2x + 2$.

§ 109. Разложение функции на неприводимые множители. Задача: найти, приводима ли данная функция, и, если приводима, разложить ее на множители с рациональными коэфициентами, — практически удобного решения не имеет; существует один способ нахождения множителей с целыми коэфициентами для данной функции с целыми коэфициентами, но это в конце концов способ упорядоченных испытаний, и практическое его значение невелико. Его мы и изложим.

Пусть $f(x)$ — ц. р. функция с целыми коэфициентами; если $f(x)$ приводима, то она раскладывается на множители с целыми коэфициентами; такие множители мы и будем искать. Пусть $f(x) = \varphi(x)\psi(x)$, где $\varphi(x)$ и $\psi(x)$ — ц. р. функции с целыми коэфициентами; при x — целом $f(x)$, $\varphi(x)$, $\psi(x)$ — также целые числа, и $f(x)$ делится на $\varphi(x)$. Пусть функция $\varphi(x)$ m-й степени. Пусть $x_0, x_1, x_2, \ldots, x_m$ $m+1$ различных целых значений для x, и $\varphi(x_\lambda) = z_\lambda$, $f(x_\lambda) = y_\lambda$; y_λ делится на z_λ; значениями $z_0, z_1, z_2, \ldots, z_m$ функция $\varphi(x)$ вполне определена (§ 50). Итак, если мы хотим найти всевозможные делители для $f(x)$ с целыми коэфициентами степени $\leq m$, то находим всевозможные делители чисел y_λ; пусть:

делители	числа	y_0	суть	$z_0,\ z_0',\ z_0'',\ \ldots,$
″	″	y_0	″	$z_0,\ z_0',\ z_0'',\ \ldots,$
″	″	y_0	″	$z_0,\ z_0',\ z_0'',\ \ldots,$
. . . .	. . . .	. . . .	. . . .	. . . . ,
″	″	y_0	″	$z_0,\ z_0',\ z_0'',\ \ldots$

Комбинируем каждого делителя y_0 с каждым делителем y_1 с каждым делителем y_2 и т. д. Пусть $z_0^{(\varkappa)}, z_1^{(\lambda)}, z_2^{(\mu)}, \ldots, z_m^{(\rho)}$ — одна такая комбинация. Находим ц. р. функцию степени $\leq m$, которая при $x = x_0$ равна $z_0^{(\varkappa)}$, при $x = x_1$ равна $z_1^{(\lambda)}$; $\ldots$, при $x = x_m$ равна $z_m^{(\rho)}$ (§ 62 и 63). Если в найденной таким образом функции $\varphi(x)$

не все коэфициенты будут целые, то мы ее отбрасываем; если же $\varphi(x)$ имеет все целые коэфициенты, то пробуем, делится ли $f(x)$ на $\varphi(x)$. Если степень функции $f(x)$ есть n, то достаточно положить $m = \frac{n}{2}$ при n четном или $m = \frac{n-1}{2}$ при n нечетном, чтобы получить, таким образом, все делители с целыми коэфициентами функции $f(x)$ если их не окажется, то $f(x)$ — неприводимая функция.

Пример. $f(x) = x^5 - 4x^4 + 6x^2 - 4x^2 - 7x + 3$. Здесь $\frac{n-1}{2} = 2$. Возьмем $x_0 = 0$, $x_1 = 1$, $x_2 = -1$; имеем $f(0) = 3$, $f(1) = -5$, $f(-1) = -5$.

$$\begin{array}{rcccl} 3 & \text{имеет} & \text{делителя:} & \pm 1, & \pm 3, \\ -5 & '' & '' & \pm 1, & \pm 5, \\ -5 & '' & '' & \pm 1, & \pm 5. \end{array}$$

Всего нам придется испробовать $4 \cdot 4 \cdot = 64$ комбинации. Но пары комбинаций, отличающихся друг от друга только разными знаками (например, $1, 5, -5$ и $-1, -1, 5$), дают, очевидно, функции $\varphi(x)$ и $-\varphi(x)$ не отличающиеся существенно друг от друга. Следовательно, всего остается 32 комбинации. Имеем (§ 63):

$$\varphi(x) = A + Bx + Cx(x-1), \qquad \varphi(0) = A, \qquad \varphi(1) = A + B, \qquad \varphi(-1) = A - B + 2C.$$

1. Комбинация $\varphi(0) = 1$, $\varphi(1) = 1$, $\varphi(-1) = 1$ дает, очевидно, $\varphi(x) = 1$ — постоянное число.

2. Комбинация $\varphi(0) = 1$, $\varphi(1) = -1$, $\varphi(-1) = 1$ дает $A = 1$, $B = -2$, $C = -1$, $\varphi(x) = x^2 + x - 1$[55]. Это — не делитель.

3. Комбинация $\varphi(0) = 1$, $\varphi(1) = 1$, $\varphi(-1) = -1$ дает $A = 1$, $B = 0$, $C = -1$, $\varphi(x) = x^2 - x - 1$. Это — не делитель.

4. Комбинация $\varphi(0) = -1$, $\varphi(1) = 1$, $\varphi(-1) = 1$ дает $A = -1$, $B = 2$, $C = 2$, $\varphi(x) = 2x^2 - 1$. Это — не делитель.

5. Комбинация $\varphi(0) = 1$, $\varphi(1) = 1$, $\varphi(-1) = 5$ дает $A = 1$, $B = 0$, $= 2$, $\varphi(x) = 2x^2 - 2x + 1$. Это — не делитель.

6. Комбинация $\varphi(0) = 1$, $\varphi(1) = -1$, $\varphi(-1) = 5$ дает $A = 1$, $B = -?$, $C = 1$, $C = 1$, $\varphi(x) = x^2 - 3x + 1$. Это — делитель, ибо

$$\begin{array}{l|l} x^5 - 4x^4 + 6x^3 - 4x^2 - 7x + 3 & x^2 - 3x + 1 \\ \underline{x^5 - 3x^4 + x^3} & x^3 - x^2 + 2x + 3 \\ \quad - \ x^4 + 5x^3 - 4x^2 & \\ \quad \underline{- \ x^4 + 3x^3 + \ x^2} & \\ \qquad + 2x^3 - 3x^2 - 7x & \\ \qquad \underline{+2x^3 - 6x^2 + 2x} & \\ \qquad\quad + 3x^2 - 9x + 3 & \\ \qquad\quad \underline{+ 3x^2 - 9x + 3} & \end{array}$$

Далее, нам предстоит исследовать, приводимы ли функции $x^2 - 3x + 1$ и $x^3 - x^2 + 2x + 3$. Для квадратной функции это проверяемся непосредственно нахождением ее корней; для кубической же функции заметим, что она приводима тогда и только тогда, если имеет рациональный корень. В данном случае функции $x^2 - 3x + 1$ и $x^3 - x^2 + 2x + 3$ обе неприводимы.

[55] Я сразу изменяю знаки у всех членов $\varphi(x)$, беря высший коэфициент положительным.

Упражнения

Найти, приводимы ли функции:

148) $x^4 + 2x^3 - x - 2$.

Отв. $(x^2 + x + 1)(x - 1)(x + 2)$.

149) $x^4 + x^3 - 5x^2 + 2$.

Отв. $(x^2 - x - 1)(x^2 + 2x - 2)$.

150) $x^5 + 3x^3 - x^2 + 2x - 1$.

Отв. $(x^3 + 2x - 1)(x^2 + 1)$.

§ 110. Общие свойства неприводимых функций. Предполагая теперь коэфициенты в наших функциях числами рациональными (не непременно целыми), выведем еще некоторые их свойства.

Теорема. *Общий наибольший делитель двух (или нескольких) функций с рациональными коэфициентами есть тоже функция с рациональными коэфициентами.*

Доказательство. Это следует из того, что при нахождении общего наибольшего делителя над коэфициентами наших функций совершаются только действия: сложение, вычитание, умножение и деление (§ 47, 52).

Следствие I. Если $\varphi(x)$ — неприводимая функция, а $f(x)$ — любая функция (с рациональными коэфициентами), то может быть только два случая: 1) или $f(x)$ делится на $\varphi(x)$; 2) или $f(x)$ и $\varphi(x)$ взаимно простые.

Доказательство. Это следует из предыдущей теоремы, ибо $\varphi(x)$ может делиться только на самое себя и на постоянное количество [56].

Следствие II. Если уравнение $f(x) = 0$ имеет общий корень с неприводимым уравнением $\varphi(x) = 0$, то и все корни уравнения $\varphi(x) = 0$ удовлетворяют уравнению $f(x)$, и $f(x)$ делится на $\varphi(x)$).

Доказательство. $f(x)$ и $\varphi(x)$ не могут быть взаимно простыми, а потому по следствию I $f(x)$ делится на $\varphi(x)$.

Следствие III. Если все корни уравнения $f(x) = 0$ удовлетворяют и неприводимому уравнению $\varphi(x) = 0$, то $f(x) = C \cdot \varphi(x)^k$, где $C = \text{const}$, $k > 0$ — целое число.

Доказательство. По следствию II / $f(x)$ делится на $\varphi(x)$: $f(x) = \varphi(x) f_1(x)$, но и $f_1(x)$ делится на $\varphi(x)$, т. е. $f(x) = \varphi(x)^2 \cdot f_2(x)$ и т. д.

Следствие IV. Неприводимое уравнение не может иметь общих корней с уравнением низшей степени.

Доказательство. Это вытекает из следствия II.

Следствие V. Если уравнение $f(x) = 0$ имеет общий корень с неприводимым уравнением $\varphi(x) = 0$ и известно, что степень $f(x)$ меньше степени $\varphi(x)$, то все коэфициенты в $f(x)$ равны нулю.

Доказательство. Это вытекает из следствия II.

Следствие VI. Неприводимое уравнение не может иметь кратных корней.

Доказательство. Это вытекает из следствия IV (§ 57, теорема 1).

Следствие VII. Два различных неприводимых уравнения не могут иметь общих корней. (Под различными уравнениями подразумеваются такие, левые части

[56] Во всем этом параграфе имеются в виду функции и уравнения только с рациональными коэфициентами.

которых отличаются друг от друга не только на постоянный множитель.)

Доказательство. Если степени уравнений различны, то это вытекает из следствия IV. Если же степень у них одна и та же, то пусть $\varphi(x) = 0$, $\psi(x) = 0$ — данные неприводимые уравнения с высшими коэфициентами, равными единице (этого мы всегда можем достигнуть); тогда общий их корень удовлетворяет и уравнению низшей степени: $\varphi(x) - \psi(x) = 0$, что по следствию IV невозможно.

Следствие VIII. Если произведение нескольких функций делится на неприводимую функцию, то по крайней мере один из сомножителей делится на эту неприводимую функцию.

Доказательство. Это вытекает из следствия (§ 53, теорема I).

Следствие IX. Всякая ц. р. функция (с рациональными коэфициентами) может быть представлена и только одним образом как произведение неприводимых функций (если не считать за различные функции, отличающиеся друг от друга постоянными множителями).

Доказательство. Очевидно, что всякая функция делится на неприводимую функцию, откуда легко следует, что она может быть представлена как произведение неприводимых множителей. Пусть возможны два различных представления:

$$f(x) = \varphi\varphi_1\varphi_2\cdots = \psi\psi_1\psi_2\cdots;$$

отсюда видно: произведение $\psi\psi_1\psi_2\cdots$ делится на φ, и, таким образом (по следствию VIII), один из сомножителей делится на φ, например, ψ, но ψ — неприводима; следовательно, $\psi = C\varphi$; сокращая на φ, получим:

$$\varphi_1\varphi_2\cdots = C\psi_1\psi_2\cdots;$$

теперь подобным же образом докажем, что, например, $\varphi_1 = C_1\psi_1$, $\varphi_2 = C_2\psi_2$ и т.д.

§ 111. Функции в данном теле. Все следствия предыдущего параграфа вытекали из доказанной в начале его теоремы и из общих свойств целых рациональных функций, изложенных в главе III. Но эта теорема основывается на том (см. ее доказательство), что коэфициенты общего наибольшего делителя функций f и g получаются из коэфициентов этих функций посредством четырех рациональных действий, т. е. принадлежат к той же области рациональности (или тому же телу, § 13), к которой принадлежат и коэфициенты функций f и g. Это дает возможность обобщить как понятие приводимых и неприводимых функций, так и все выводы предыдущего параграфа на случай, когда все данные функции имеют коэфициенты из данной области рациональности P, причем P — любая, наперед заданная область рациональности. Итак, мы вводим следующее определение:

Целая рациональная функция (или алгебраическое уравнение), все коэфициаенты которой (которого) принадлежат телу P, называется функцией (уравнением) в теле P.

Аналогично определяем функцию и уравнение в данной *области целости.*

Подобно тому как мы строили теорию делимости целых рациональных функций вообще (в главе III), т. е. в области всех комплексных чисел, мы можем построить теорию делимости целых рациональных функций в любой данной области рациональности (тела) или даже в области целости. Эта теория основана на том простом факте, что при действиях сложения, вычитания и умножения целых рациональных функций мы над коэфициентами их совершаем те же действия, т. е.

из данной области целости (а, следовательно, и подавно из данного тела) не выходим; при действии же деления коэфициенты делимого приходится делить на высший коэфициент «делителя», т. е. при делении мы не выходим из данного тела, а если высший коэфициент делителя равен единице, то и из данной области целости. Отсюда следует:

Все целые рациональные функции в данном теле P или в данной области целости I образуют область целости.

В дальнейшем мы для простоты ограничимся случаем, когда наши функции даны в некотором теле. Понятия делимости функций, разложимости функций на множители и т. п. мы теперь будем применять только в отношении к данному телу P, рассматривая исключительно только функции в этом теле. Основным является такое определение:

Целая рациональная функция в теле P называется неприводимой в этом теле, если она не может быть разложена на два множителя (являющихся целыми рациональными функциями степеней больших нуля), тоже в теле P (т. е. с коэфициентами из P).

В противном случае она называется *приводимой*.

Из предыдущих замечаний следует:

Теорема и все девять следствий § 110 остаются правильными и для целых рациональных функций в любом данном теле P, если только слова «с рациональными коэфициентами» заменить всюду словами «с коэфициентами из P», или просто «в теле P».

Заметим, что в «алгебраически замкнутом» теле (§ 76), в частности в теле всех комплексных чисел, единственными неприводимыми функциями являются линейные [57]; в теле всех вещественных чисел неприводимыми функциями являются линейные, а также и квадратные с отрицательными дискриминантами [58].

В теории делимости целых рациональных функций (иначе, *многочленов* или *полиномов*) в данном теле неприводимые в этом теле функции играют роль простых чисел. Особенно важны тут следствия VIII и IX § 110, аналогичные известным теоремам из теории делимости целых чисел.

Заметим, что если данная функция имеет все коэфициенты из тела P, то и ее производная тоже функция в теле P. А отсюда легко следует, что обе теоремы ,§ 57 могут быть обобщены для функций в данном теле:

Теорема 1. *Необходимое и достаточное условие того, чтобы функция $f(x)$ теле P имела делителем α-ю (но не выше) степень неприводимой в этом теле функции $\varphi(x)$, следующее: $\varphi(x)$ должна быть делителем $f(x)$ и входить в разложение функции $f'(x)$ на неприводимые множители как раз в степени $\alpha - 1$.*

Теорема 2. *Необходимое и достаточное условие того, чтобы, функция $f(x)$ в теле P делилась на α-ю (но не выше) степень неприводимой в этом теле функции $\varphi(x)$ следующее: $\varphi(x)$ должна быть делителем функций $f(x)f'(x), f''(x), \ldots, f^{(\alpha-1)}(x)$, но не функции $f^{(\alpha)}(x)$.*

Именно, пусть

$$f(x) = \varphi(x)^{\alpha} \cdot g(x),$$

[57] По определению неприводимых функций к ним же как будто бы следует причислять и постоянные количества как функции нулевой степени; однако по некоторым причинам этого не делают, подобно тому как число 1 не причисляют к простым числам.

[58] Дискриминантом функции $ax^2 + bx + c$ называется выражение $b^2 - 4ac$.

где $g(x)$ не делится на $\varphi(x)$, а следовательно (по следствию I § 110), взаимно проста $\varphi(x)$; имеем:

$$f'(x) = \varphi(x)^{\alpha-1} \cdot [\alpha\varphi'(x)g(x) + \varphi(x)g'(x)];$$

в квадратных скобках первый член взаимно простой с $\varphi(x)$ [ибо и $g(x)$, и $\varphi'(x)$ по следствию VI § 110 взаимно простые с $\varphi(x)$], а второй член делится на $\varphi(x)$, следовательно, вся сумма взаимно простая с $\varphi(x)$, т. е. $f'(x)$ делится на $\varphi(x)^{\alpha-1}$, но не на высшую степень $\varphi(x)$. Обратное доказывается легко. Этим теорема 1 доказана. Теорема 2 доказывается, как и в § 57, повторным применением теоремы 1.

Из всего сказанного здесь следует, что все рассуждения § 58 целиком применимы и для функций в данном теле P; только под X_1 надо подразумевать произведение неприводимых в P множителей данной функции $f(x)$ в P, входящих в $f(x)$ в первой степени; под X_2 — произведение неприводимых множителей функции $f(x)$, входящих в $f(x)$ во второй степени (причем в X_2 они берутся по одному разу) и т. д. Эти произведения $X_1, X_2, \ldots$ мы по существу и выделяем, оставаясь в том теле P, к которому принадлежат коэфициенты данной функции $f(x)$, например, в примере и упражнениях § 58 мы остаемся все время в абсолютной области рациональности.

§ 112. Расширения тела. «Расширением» тела P называется превращение его в более обширное тело P_1, содержащее P как часть; это расширение, происходит путем присоединения к P одного, нескольких или бесчисленного множества новых количеств $\alpha, \beta, \gamma, \ldots$ и всевозможных рациональных функций от этих количеств с коэфициентами из P. Последнее необходимо, чтобы P_1 оставалось телом; но P_1 мы можем рассматривать как совокупность этих рациональных функций от $\alpha_1, \beta_1, \gamma_1, \ldots$ с коэфициентами из P, рассматривая сами количества из P как частный случай таких функций, именно как целые рациональные функции от $\alpha, \beta, \gamma, \ldots$ нулевой степени. Сейчас мы подробнее рассмотрим присоединение к P *одного* нового количества α (и, конечно, всех рациональных функций от него с коэфициентами из P). Тело, получающееся после этого присоединения, мы обозначим через $P(\alpha)$ [59].

Пусть $\dfrac{\varphi(\alpha)}{\psi(\alpha)}$ и $\dfrac{\varphi_1(\alpha)}{\psi_1(\alpha)}$ — две рациональные функции от α в P [т. е. два числа из $P(\alpha)$]; φ, ψ, φ_1, ψ_1 — целые функции в P; при этом дроби $\dfrac{\varphi(x)}{\psi(x)}$, $\dfrac{\varphi_1(x)}{\psi_1(x)}$ мы считаем алгебраически несократимыми. Посмотрим, могут ли эти функции иметь одно и то же численное значение при $x = \alpha$; из

$$\frac{\varphi(\alpha)}{\psi(\alpha)} = \frac{\varphi_1(\alpha)}{\psi_1(\alpha)} \tag{2}$$

следует:

$$\varphi(\alpha)\psi_1(\alpha) = \varphi_1(\alpha)\psi(\alpha), \tag{2a}$$

[59] При присоединении многих количеств обозначают аналогично:

$$P(\alpha, \beta, \gamma, \ldots).$$

причем это равенство не тождество. Следовательно, α в этом случае удовлетворяет алгебраическому уравнению (2) в теле P; такое количество α называется *алгебраическим количеством, происходящим из тела* P, или *алгебраическим количеством над телом* P; это понятие об «относительно» алгебраическом количестве (именно, по отношению к телу P) есть обобщение понятия алгебраического числа, введенного в § 75; там, так сказать, «абсолютно» алгебраические числа являются алгебраическими количествами над абсолютной областью рациональности (§ 13).

Присоединение к P алгебраических количеств над P называется *алгебраическим расширением* тела P. Всякое не-алгебраическое расширение тела P называется *трансцендентным расширением* тела P; там равенство (2) существует только, если функции $\dfrac{\varphi(x)}{\psi(x)}$ и $\dfrac{\varphi_1(x)}{\psi_1(x)}$ тождественно равны друг другу.

Пример 1. Пусть P — абсолютная область рациональности; присоединим к ней число $\sqrt{2}$; получим тело $P(\sqrt{2})$; это — алгебраическое расширение, ибо $\sqrt{2}$ есть корень уравнения $x^2 - 2 = 0$ с рациональными коэфициентами. В теле $P(\sqrt{2})$ мы, например, имеем:

$$\frac{1}{5+\sqrt{2}} = \frac{5-\sqrt{2}}{23};$$

действительно, освободившись от знаменателей, получим:

$$(5+\sqrt{2})\cdot(5-\sqrt{2}) = 23,$$

это верно, ибо $(\sqrt{2})^2 = 2$.

Пример 2. Присоединим теперь к абсолютной области рациональности P число π (отношение длины окружности к длине диаметра, как известно, — трансцендентное число); это — трансцендентное присоединение. Здесь $\dfrac{\varphi(\pi)}{\psi(\pi)} = \dfrac{\varphi_1(\pi)}{\psi_1(\pi)}$ — тогда и только тогда, если тождественно

$$\frac{\varphi(x)}{\psi(x)} = \frac{\varphi_1(x)}{\psi_1(x)}$$

при переменном x. Но так как в этой части алгебры мы совсем не рассматриваем самый *процесс изменения* наших функций, а только их *состав*, то для исследования тела $P(\pi)$ безразлично, если мы вместо буквы π напишем букву x и будем исследовать тело $P(x)$, где x — независимая переменная; $P(x)$ есть совокупность всех целых и дробных рациональных функций от x: в теле P эта совокупность есть, очевидно, тело; и мы видим, что это присоединение переменной x следует считать трансцендентным. Ясно, что между числами тела $P(\pi)$ и между рациональными функциями от x в P [т. е. между «элементами» тела $P(x)$] существует взаимно однозначное соответствие; будем подразумевать под $F_1, F_2, \ldots$ рациональные функции в P; тогда числу $F_k(\pi)$ соответствует функция $F_k(x)$; разным числам соответствуют разные функции, и обратно; если $F_1(\pi)$, $F_2(\pi)$ соответстуют $F_1(x)$, $F_2(x)$, то

$$\begin{aligned}
F_1(\pi) + F_2(\pi) &\quad \text{соответствует} \quad F_1(x) + F_2(x),\\
F_1(\pi) - F_2(\pi) &\quad \text{соответствует} \quad F_1(x) - F_2(x),\\
F_1(\pi)\cdot F_2(\pi) &\quad \text{соответствует} \quad F_1(x)\cdot F_2(x),\\
\frac{F_1(\pi)}{F_2(\pi)} &\quad \text{соответствует} \quad \frac{F_1(x)}{F_2(x)},
\end{aligned}$$

если $F_2(x) \not\equiv 0\mathrm{F}$ (тогда само собою и $F_2(\pi) \neq 0$). Такие тела $P(\pi)$ и $P(x)$ называются *изоморфными* друг с другом.

§ 113. Посмотрим, как изменяются свойства делимости функций при расширении данного тела. От такого расширения неприводимая функция может в расширенном теле сделаться приводимой; в таком случае она распадается на множители, которые в расширенном теле будут неприводимы. От дальнейшего расширения тела и эти неприводимые множители (т. е. те из них, которые не линейны) могут сделаться приводимыми. Пусть нам удалось так расширить наше тело P, что в расширенном теле $P-1$ наша целая рациональная функция N-й степени $f(x)$ распалась на n линейных множителей;

$$f(x) = a_0(x-x_1)(x-x_2)\cdots(x-x_n);$$

тогда тем самым мы решили уравнение $f(x)=0$: его корни — $x_1, x_2, ..., x_n$, все они — количества из P_1, а это тело (т. е. все его количества) мы считаем известным; в нем мы можем найти $x_1, x_2, \ldots, x_n$ уже рациональным путем. Вопрос в том, как именно следует расширить тело P, т. е. какие именно количества к нему присоединять, чтобы в расширенном теле P наша функция $f(x)$ распалась на линейные множители. Этот вопрос рассматривает теория Галуа (Galois; см. гл. XII) и дает на него исчерпывающий ответ с помощью теории групп. Важно, что мы при этом можем обойтись исключительно только алгебраическими присоединениями.

Пример. Функция $f(x) = x^4 - x^2 + 1$ неприводима в абсолютной области рациональности P; но в теле $P(\sqrt{3})$ она приводима, именно

$$x^4 - x^2 + 1 = (x^2 + x\sqrt{3} + 1)(x^2 - x\sqrt{3} + 1).$$

ГЛАВА СЕДЬМАЯ

ДВУЧЛЕННЫЕ УРАВНЕНИЯ. УРАВНЕНИЯ НИЗШИХ СТЕПЕНЕЙ

§ 114. Двучленное уравнение. *Двучленными* уравнениями называются уравнения вида $x^n - a = 0$, где a — любое (вещественное или комплексное) число. Решение такого уравнения сводится к извлечению корня n-й степени из a. Извлечение корня из комплексных чисел нами уже рассматривалось в § 9; решение этой задачи было там дано в тригонометрической форме. В настоящей главе мы рассмотрим двучленные уравнения чисто алгебраически.

Теорема. *Все корни уравнения $x^n - a = 0$ различны при $a \neq 0$; если α — один из корней, то все другие найдутся умножением α на всевозможные корни n-й степени из единицы, т. е. на корни уравнения $x^n = 1$.*

Доказательство. Уравнение $f(x) = x^n - a = 0$ кратных корней не имеет, ибо уравнение $f'(x) = nx^{n-1} = 0$ имеет единственный корень 0, который не удовлетворяет уравнению $x^n - a = 0$ [§ 57, теорема 1]. Далее, имеем $\alpha^n = a$; пусть ρ — корень n-й степени из единицы, т. е. $\rho^n = 1$; тогда $(\alpha\rho)^n = a$, т. е. $\alpha\rho$ — тоже корень уравнения $x^n = a$. Обратно: если α и α_1 — два корня уравнения $x^n = a$, то $\left(\dfrac{\alpha_1}{\alpha}\right)^n = \dfrac{\alpha_1^n}{\alpha^n} = \dfrac{a}{a} = 1$, т. е. $\rho = \dfrac{\alpha_1}{\alpha}$ есть корень n-й степени из единицы, и $\alpha_1 = \alpha\rho$, т. е. теорема доказана.

§ 115. Вспомогательная теорема из теории чисел. В дальнейшем нам понадобится следующая теорема из теории чисел, аналогичная второй теореме § 52.

Теорема. *Если a и b — два целых числа и $d = D(a, b)$, то уравнение $ax + by = d$ разрешимо в целых числах.*

Доказательство. Найдем d по способу Эвклида:

$$\left.\begin{aligned} a &= bq + r, \\ b &= rq_1 + r_1, \\ &\cdots\cdots\cdots\cdots\cdots\cdots, \\ r_{m-2} &= r_{m-1}q_m + d, \\ r_{m-1} &= dq_{m+1}. \end{aligned}\right\} \qquad (1)$$

Предпоследнее уравнение (1) дает $r_{m-2} - r_{m-1}q_m = d$?; вместо r_{m-1} можно подставить из предыдущего уравнения $r_{m-1} = r_{m-3} - r_{m-2}q_{m-1}$ и d представится в виде $d = kr_{m-3} + lr_{m-2}$; теперь подобным же образом подставляем значение для r_{m-2} из предыдущего уравнения $r_{m-2} = r_{m-4} - r_{m-3}q_{m-2}$ и т. д. Идя назад, мы в

конце концов дойдем до чисел a и b и представим d в виде $d = ax + by$, где x и y — целые числа.

Следствие. Если числа a и b — взаимно простые, то уравнение $ax + by = 1$ разрешимо в целых числах.

§ 116. Неприводимость двучленного уравнения простой степени. Обращаясь теперь снова к уравнению $x^n - a = 0$, докажем следующее:

Теорема. *Если $n = p$ — простое число, а a — рациональное число, не являющееся точной p-й степенью другого рационального числа, то уравнение $x^p - a = 0$ неприводимо в абсолютной области рациональности.*

Доказательство. Пусть α — один из корней уравнения $x^p - a = 0$; тогда α — иррациональное число; остальные корни этого уравнения будут $\alpha\rho_1, \alpha\rho_2, \alpha\rho_3, \ldots$ (§ 114), где $\rho_1, \rho_2, \rho_3, \ldots$ — все корни p-й степени из единицы. Пусть наше уравнение приводимо и пусть $x^p - a = \varphi(x)\psi(x)$, где $\varphi(x)$ — ц. р. Функция ν-й степени с рациональными коэфициентами и с высшим коэфициентом, равным единице, $\nu < p$. Пусть, далее, корни $\varphi(x) = 0$ суть: $\alpha\rho_1, \alpha\rho_2, \ldots, \alpha\rho_\nu$; тогда свободный член функции $\varphi(x)$ есть $\alpha^\nu \rho_1\rho_2 \cdots \rho_\nu$; обозначим $\rho_1\rho_2 \cdots \rho_\nu = \rho$; ρ — тоже корень p-й степени из единицы, ибо $\rho^p = (\rho_1\rho_2 \cdots \rho_\nu)^p = \rho_1^p\rho_2^p \cdots \rho_\nu^p = 1$.

Обозначим, далее, $\alpha^\nu\rho = k$; k — рациональное число, так как все коэфициенты в функции $\varphi(x)$ рациональны. Итак, имеем:

$$\alpha^p = a, \qquad \alpha^\nu\rho = k; \tag{2}$$

так как $\nu < p$, а p — простое, то числа ν и p взаимно простые; найдем целые числа λ и μ так, чтобы было $\lambda p + \mu\nu = 1$ (§ 115); возвышаем обе части первого из уравнений (2) в степень λ, обе части второго из уравнений (2) в степень μ и перемножаем левые и правые части этих уравнений; получаем $\alpha^{\lambda p + \mu\nu}\rho^\mu = a^\lambda k^\mu = l$ — рациональное число, или $\alpha\rho^\mu = l$; но ρ^μ — тоже корень p-й степени из единицы, ибо $(\rho^\mu)^p = \rho^{\mu p} = (\rho^p)^\mu = 1$; следовательно (по § 114), $\alpha\rho^\mu$ — тоже корень уравнения $x^p - a = 0$ и этот корень равен l — рациональному числу, что противоречит нашему условию. Следовательно, уравнение $x^p = a$ неприводимо.

Но если n — число не простое, то теорема уже неверна, например, $x^6 - 9 = (x^3 - 3)(x^3 + 3)$.

§ 117. Корни из единицы. Рассмотрим теперь уравнение $x^n = 1$. По § 114 оно имеет n различных корней, из которых при n нечетном только один корень вещественен — $x = 1$, а при n четном два корня вещественны — $x = \pm 1$.

Теорема. *Если $x = p + qi$ — комплексный корень n-й степени из единицы, то $\overline{x} = p - qi = \dfrac{1}{x}$, значит, тоже является корнем из единицы.*

Доказательство. $x\overline{x} = p^2 + q^2 > 0$, $(x\overline{x})^n = (p^2 + q^2)^n = 1$; следовательно, $\overline{x} = \dfrac{1}{x}$.

Теорема. *Если x_1 и x_2 — корни n-й степени из единицы, то x_1x_2 $\dfrac{x_1}{x_2}$, x_1^k тоже корни (k -—- любое целое число).*

Доказательство. Имеем:

$$(x_1x_2)^n = x_1^n \cdot x_2^n = 1, \qquad \left(\frac{x_1}{x_2}\right)^n = \frac{x_1^n}{x_2^n} = 1, \qquad (x_1^k)^n = x_1^{kn} = (x_1^n)^k = 1.$$

Теорема. *Общими корнями, уравнений $x^r = 1$ и $x^s = 1$ служат все t корней уравнения $x^t = 1$, где $t = D(r, s)$.*

Доказательство. Пусть x — общий корень, т. е. $x^r = 1$, $x^s = 1$; найдем (по § 115) u и v так, чтобы было $ru + sv = t$; тогда $x^{ru} = 1$, $x^{sv} = 1$; перемножим $x^{ru+sv} = x^t = 1$. Обратное очевидно: если x — корень уравнения $x^t = 1$, то, обозначив $\frac{r}{t} = r_1$, $\frac{s}{t} = s_1$, найдем $x^{tr_1} = x^r = 1$, $x_1^{ts_1} = 1$, что и требовалось доказать.

Следствие. Если $Dr, s) = 1$, то уравнения $x^r = 1$ и $x^s = 1$ не имеют общих корней кроме $x = 1$.

§ 118. Первообразные корни. Пусть z — корень из единицы какой-нибудь степени; наименьшее число $m > 0$, для которого $z = 1$, называется показателем, к которому принадлежит корень z из единицы; z — первообразный корень m-й степени из единицы.

Теорема. *Если z — первообразный корень m-й степени из единицы, то количества $z, z^2, z^3, \ldots, z^{m-1}$, $z^m = 1$ — все различны, тогда как $z^{m+1} = z$, $z^{m+2} = z$, ... вообще $z^\varkappa = z^\lambda$ тогда и только тогда, если $\varkappa - \lambda$ делится на m.*

Доказательство. Пусть $\varkappa = \lambda + rm$; тогда $z^\varkappa = z^{\lambda+rm} = z^\lambda z^{rm} = z^\lambda$. Обратно: пусть $z^\varkappa = z^\lambda$ или $z^{\varkappa-\lambda} = 1$; пусть $\varkappa - \lambda = rm + r_1$, где $r_1 < m$; тогда $z^{\varkappa-\lambda} = z^{rm+r_1}$, $z^{rm} z^{r_1} = z^{r_1} = 1$, что невозможно, ибо $r_1 < m$, а m — наименьший показатель, для которого $z^m = 1$.

Отсюда же следует, что $z, z^2, z^3, \ldots, z^m$ все различны, ибо при $\varkappa$ и $\lambda < m\varkappa - \lambda$ не может делиться на m, если только $\varkappa \neq \lambda$.

Следствие. Если z — первообразный корень m-й степени из единицы, то количества $z, z^2, z^3, \ldots, z^{m-1}$, $z^m = 1$ исчерпывают собой все корни m-й степени из единицы, ибо число их равно m и все они различны.

Теорема. *Если z принадлежит к показателю m, то z^k принадлежит к показателю $m' = \frac{m}{d}$, где $d = D(m, k)$.*

Доказательство. Пусть $(z^k)^r = 1$; тогда $kr = lm$; пусть $k = k_1 d$; $m = m_1 d$; следовательно, $k_1 r = l m_1$; $k_1 r$ делится на m_1; но k_1 и m_1 взаимно простые; следовательно, r делится на m_1, если r — наименьшее число, для которого $(x^k)r = 1$, то $r = m_1$; действительно, $(z^k)^{m_1} = z^{k_1 d m_1} = (z^m)^{k_1} = 1$. Итак, $r = \frac{m}{d}$ и есть показатель, к которому принадлежит z.

Следствие I. При $D(m, k) = 1$ и только в этом случае z^k тоже принадлежит к показателю m.

Следствие II. Если существует один первообразный корень m-й степени из единицы, то число всех первообразных корней m-й степени из единицы равно числу целых чисел больших нуля и меньших m и взаимно простых с m.

Возникает вопрос: для всякого ли целого числа $m > 0$ существуют первообразные корни m-й степени из единицы. В дальнейшем мы ответим утвердительно на этот вопрос. Число первообразных корней m-й степени обозначается знаком $\varphi(m)$.

§ 119. Теорема. *Если $D(r, s) = 1$, то все корни уравнения $x^{rs} = 1$ получаются умножением всех корней уравнения $x^r = 1$ на все корни уравнения $x^s = 1$, а все первообразные корни уравнения $x^{rs} = 1$ получаются умножением всех первообразных корней уравнения $x^r = 1$ на все первообразные корни уравнения $x^s = 1$.*

Доказательство. Пусть $\alpha^r = 1$, $\beta^s = 1$; тогда $(\alpha\beta)^{rs} = \alpha^{rs} \times \beta^{rs} = 1$; если $\alpha\beta = \alpha_1\beta_1$ (где α_1 — тоже корень уравнения $x^r = 1$, а β_1 — корень уравнения $x^s = 1$), то $\dfrac{\alpha}{\alpha_1} = \dfrac{\beta}{\beta_1}$, ибо $\dfrac{\alpha}{\alpha_1} = \dfrac{\beta}{\beta_1}$ — корень и уравнения $x^r = 1$ и уравнения $x^s = 1$, а эти уравнения имеют только один общий корень $x = 1$ (§ 117, следствие); следовательно, $\alpha_1 = \alpha$, $\beta_1 = \beta$, т. е. если не будет одновременно $\alpha_1 = \alpha$, $\beta_1 = \beta$, то и $\alpha_1\beta_1 \neq \alpha\beta$, т. е. в виде $\alpha\beta$ представляются все $r \cdot s$ корней уравнения $x^{rs} = 1$. Далее, если $\alpha^{r'} = 1$, $\beta^{s'} = 1$, то $(\alpha\beta)^{r's'} = 1$; если выполнено хоть одно неравенство $r' < r$, $s' < s$, то и $r's' < rs$.

Пусть теперь α — первообразный корень r-й степени, а β — первообразный корень s-й степени из единицы и пусть $(\alpha\beta)^t = 1$; следовательно, $\alpha^t = \beta^{-t} = 1$, ибо уравнения $x^r = 1$ и $x^s = 1$ кроме единицы не имеют общих корней; следовательно, t делится на r и на s, ибо α и β — первообразные корни r-й и s-й степеней из единицы. Но $D(r, s) = 1$, т. е. t делится на rs; следовательно, $\alpha\beta$ — первообразный корень степени rs из единицы.

Следствие. $\varphi(rs) = \varphi(r)\varphi(s)$; если каждая пара чисел $r, s, t, \ldots$ взаимно простая, то $\varphi(rst\cdots) = \varphi(r)\varphi(s)\varphi(t)\cdots$ В частности, если $m = p^\alpha q^\beta r^\gamma \cdots$ разложение числа m на простые множители, то $\varphi(m) = \varphi(p^\alpha)\varphi(q^\beta)\varphi(r^\gamma)\cdots$; следовательно, нам достаточно определить $\varphi(m)$ для случая, когда m — степень простого числа.

§ 120. Уравнения деления окружности. Пусть $m = p$ — простое число; в этом случае при $k < p$ всегда k и p взаимно простые; следовательно, все корни уравнения $z^p - 1 = 0$ первообразны, кроме корня $z = 1$, т. е. $\varphi(p) = p - 1$. Обозначим через $\Phi_m(x) = 0$ уравнение, имеющее корнями все первообразные корни m-й степени из единицы; тогда

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + 1.$$

Пусть теперь $m = p^n$, где p — простое; все делители числа m, меньшие, чем m, суть $1, p, p^2, \ldots, p^{n-1}$; пусть x принадлежит к показателю p^τ; $\tau \leq n - 1$; тогда $x^{p\tau} = 1$; возвысим обе части в степень $p^{n-1-\tau}$; получим $x^{p^{n-1}} = 1$. Итак, все непервообразные корни уравнения $x^{p^n} = 1$ удовлетворяют уравнению $x^{p^{n-1}} = 1$; отсюда же следует, что все первообразные корни уравнения $x^{p^n} = 1$ удовлетворяют уравнению:

$$\Phi_{p^n}(x) = \frac{x^{p^n} - 1}{x^{p^{n-1}} - 1} = x^{p^{n-1}(p-1)} + x^{p^{n-1}(p-2)} + \ldots + x^{p^{n-1}} + 1 = 0;$$

число их

$$\varphi(p^n) = p^{n-1}(p-1) = p^n\left(1 - \frac{1}{p}\right).$$

Отсюда и из следствия § 119 вытекает:

Теорема. *Для всякого числа m существуют первообразные корни m-й степени из единицы; число их:*

$$\begin{aligned}\varphi(m) = \varphi(p^\alpha)\varphi(q^\beta)\varphi(r^\gamma)\cdots &= p^\alpha\left(1 - \tfrac{1}{p}\right) q^\beta\left(1 - \tfrac{1}{q}\right) r^\gamma\left(1 - \tfrac{1}{r}\right)\cdots = \\ &= m\left(1 - \tfrac{1}{p}\right)\left(1 - \tfrac{1}{q}\right)\left(1 - \tfrac{1}{r}\right)\cdots\end{aligned}$$

Теорема. *Если $\alpha_1, \alpha_2, \ldots, \alpha_m$ все корни m-й степени из единицы, то $\alpha_1^k + \alpha_2^k + \ldots + \alpha_m^k = 0$ при k, не делящемся на m, или равно m при k, делящемся на m.*

Доказательство. Пусть α — первообразный корень m-й степени из единицы; тогда все корни m-й степени суть (§ 118) $1, \alpha, \alpha^2, \ldots, \alpha^{m-1}$; следовательно:

$$1^k + \alpha^k + \alpha^{2k} + \ldots + \alpha^{(m-1)^k} = \frac{1 - \alpha^{mk}}{1 - \alpha^k} = 0,$$

если $\alpha^k \neq 1$, т. е. k не делится на m. Если же k делится на m, то

$$\alpha^k = \alpha^{2k} = \ldots = \alpha^{(m-1)k} = 1, \quad \text{и} \quad 1^k + \alpha^k + \alpha^{2k} + \ldots + \alpha^{(m-1)k} = m.$$

§ 121. Найдем теперь функцию $\Phi_m(x)$ для всякого m.

Лемма. Если $n = p^\alpha \cdot m$, p — простое, m не делится на p, то

$$\Phi_n(x) = \frac{\Phi_m(x^{p^\alpha})}{\Phi_m(x^{p^{\alpha-1}})}.$$

Доказательство. Пусть μ — первообразный корень уравнения $x^m = 1$, ρ — любой корень уравнения $x^{p^\alpha} = 1$, а ρ' — не первообразный корень уравнения $x^{p^\alpha} = 1$; тогда (§ 120) $\rho'^{p^{\alpha-1}} = 1$. Обозначим $\rho\mu = \sigma$; тогда $\sigma^{p^\alpha} = \mu^{p^\alpha}$; это тоже первообразный корень уравнения $x^m = 1$, ибо p^α взаимно просто с m (§ 118, следствие I). Уравнение $\Phi_m(x^{p^\alpha}) = 0$ будет степени $p^\alpha \varphi(m)$, ему удовлетворяют все корни $\sigma = \rho\mu$; число их равно $p^\alpha \varphi(m)$, и все они различны (§ 119), т. е. это — все корни уравнения $\Phi_m(x^{p^\alpha}) = 0$. Подобным же образом убедимся, что количества $\sigma' = \rho'\mu$ суть все корни уравнения $\Phi_m(x^{p^{\alpha-1}}) = 0$. Отсюда следует, что уравнению

$$\frac{\Phi_m(x^{p^\alpha})}{\Phi_m(x^{p^{\alpha-1}})} = 0$$

удовлетворяют все количества $\sigma = \rho\mu$, где ρ — первообразный корень уравнения $x^{p^\alpha} = 1$, а μ — первообразный корень уравнения $x^m = 1$, т. е. этому уравнению удовлетворяют все первообразные корни уравнения $x^n = 1$ (§ 119); следовательно:

$$\frac{\Phi_m(x^{p^\alpha})}{\Phi_m(x^{p^{\alpha-1}})} = \Phi_n(x)$$

(мы определяем функцию $\Phi_n(x)$ как такую, у которой высший коэфициент равен единице). Например, при $n = p^\alpha q^\beta$ (p и q простые), положив $m = q^\beta$, получим:

$$\Phi_n(x) = \frac{(x^n - 1)(x^{\frac{n}{pq}} - 1)}{(x^{\frac{n}{p}} - 1)(x^{\frac{n}{q}} - 1)}.$$

Отсюда методом полной индукции легко доказать общую теорему: если $n = p^\alpha q^\beta r^\gamma \cdots$ разложение n на простые множители, то

$$\Phi_n(x) = \frac{(x^n - 1)(x^{\frac{n}{pq}} - 1)(x^{\frac{n}{pr}} - 1)(x^{\frac{n}{qr}} - 1)\cdots}{(x^{\frac{n}{p}} - 1)(x^{\frac{n}{q}} - 1)(x^{\frac{n}{pqr}} - 1)\ldots} = \frac{\prod(x^{\frac{n}{n_1}} - 1)}{\prod(x^{\frac{n}{n_2}} - 1)}, \tag{3}$$

где n_1 — всевозможные произведения чисел $p, q, r, \ldots$, взятых в четном числе (включая сюда и единицу), а n_2 — всевозможные произведения чисел $p, q, r, \ldots$, взятых в нечетном числе.

Итак, пусть формула (3) доказана для чисел n, раскладывающихся на k простых множителей; докажем, что она будет верна и для всех чисел n, раскладывающихся на $k+1$ простых множителей. Пусть n такое число: $n = p^\alpha q^\beta r^\gamma \cdots$; обозначим $q^\beta r^\gamma \cdots = m$; для числа m формула (3) верна, т. е.

$$\Phi_m(x) = \frac{\prod(x^{\frac{m}{m_1}} - 1)}{\prod(x^{\frac{m}{m_2}} - 1)};$$

имеем по лемме:

$$\begin{aligned}\Phi_n(x) = \frac{\Phi_m(x^{p^\alpha})}{\Phi_m(x^{p^{\alpha-1}})} &= \frac{\prod(x^{\frac{m}{m_1}p^\alpha} - 1)}{\prod(x^{\frac{m}{m_2}p^\alpha} - 1)} : \frac{\prod(x^{\frac{m}{m_1}p^{\alpha-1}} - 1)}{\prod(x^{\frac{m}{m_2}p^{\alpha-1}} - 1)} = \\ &= \frac{\prod(x^{\frac{m}{m_1}} - 1)\prod(x^{\frac{n}{pm_2}} - 1)}{\prod(x^{\frac{m}{m_2}} - 1)\prod(x^{\frac{n}{m_1 p}} - 1)} = \frac{\prod(x^{\frac{n}{n_1}} - 1)}{\prod(x^{\frac{n}{n_2}} - 1)},\end{aligned}$$

т. е. формула (3) верна и для числа n.

Пример. Найти $\Phi_{12}(x)$. Здесь $12 = 2^2 \cdot 3$; следовательно, имеем:

$$\Phi_{12}(x) = \frac{(x^{12} - 1)(x^{\frac{12}{2\cdot 3}} - 1)}{x^{\frac{12}{2}} - 1)(x^{\frac{12}{3}} - 1)} = \frac{(x^{12} - 1)(x^2 - 1)}{(x^6 - 1)(x^4 - 1)} = x^4 - x^2 + 1;$$

степень $\Phi_{12}(x) = \varphi(12) = 12 \cdot \frac{1}{2}\frac{2}{3} = 4$.

Упражнения

151) Вычислить $\varphi(15)$, $\varphi(18)$, $\varphi(20)$, $\varphi(60)$, $\varphi(275)$, $\varphi(5\,896)$.

Отв. 8, 6, 8, 16, 200, 2 640.

152) Найти $\Phi_3(x)$, $\Phi_8(x)$, $\Phi_{10}(x)$, $\Phi_{15}(x)$, $\Phi_{20}(x)$.

Отв. $x^2 + x + 1$, $x^4 + 1$, $x^4 - x^3 + x^2 - x + 1$, $x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$, $x^8 - x^6 + x^4 - x^2 + 1$.

§ 122. Уравнение $\Phi_m(x) = 0$ степени $\varphi(m)$, дающее все первообразные корни m-й степени из единицы, называется *уравнением деления окружности*, ибо к его решению сводится задача деления окружности на m равных частей.

Теорема. *Уравнение деления окружности* $\Phi_m(x) = 0$ *неприводимо (в абсолютной области рациональности).*

Мы докажем эту теорему для случая, когда $m = p^n$, где p — простое число. В функции $\Phi_{p^n}(x)$ все коэфициенты целые. Пусть функция $\Phi_{p^n}(x)$ приводима; тогда (по § 107) она может быть разложена на два множителя с целыми коэфициентами $\Phi_{p^n}(x) = f(x)g(x)$; в таком случае $\Phi_{p^n}(1) = f(1)g(1)$; но $\Phi_{p^n}(1) = p$ — простое число; следовательно, из чисел $f(1)$, $g(1)$ одно равно ± 1, а другое равно $\pm p$; например, $f(1) = \pm 1$, $g(1) = \pm p$. Пусть $\rho, \rho^a, \rho^b, \ldots$ — корни уравнения $\Phi_{p^n}(x) = 0$ (ρ — один из первообразных корней уравнения $x^{p^n} = 1$); числа $a, b, \ldots$ не делятся на

p. Пусть, например, $f(\rho) = 0$; тогда уравнение $f(x)f(x^a)f(x^b)\cdots = 0$ имеет корни: $\rho, \rho^a, \rho^b, \ldots$ [60], т. е. левая часть его делится на $\Phi_{p^n}(x)$

$$f(x)f(x^a)f(x^b)\cdots = \Phi_{p^n}(x)\psi(x);$$

пусть $\psi(1) = s$ — целое число [ибо в $\psi(x)$ все коэфициенты целые]; имеем при $?x = 1$: $\pm 1 = p \cdot s$, что невозможно. Следовательно, функция $\Phi_{p^n}(x)$ неприводима.

§ 123. Квадратные уравнения. Квадратные уравнения подробно рассматриваются в элементарной алгебре. Мы здесь выведем только ни общую формулу решения квадратных уравнений.

Пусть $f(x) = ax^2 + 2bx + c = 0$ — данное уравнение, x — один из его корней; следовательно, $f(x_1) = ax_1^2 + 2bx_1 + c = 0$. Возьмем функцию $f(x, x_1) = axx_1 + b(x+x_1)+c$; назовем ее (по аналогии с геометрией) *полярой* функции $f(x)$. Имеем:

$$f(x, x_1 0^2 - f(x)f(x_1) = (b^2 - 4ac)(x - x_1)^2;$$

но $f(x_1) = 0$; следовательно:

$$f(x, x_1)^2 = (b^2 - 4ac)(x - x_1)^2, \qquad f(x, x_1) = \sqrt{b^2 - 4ac}\cdot(x - x_1),$$

или

$$axx_1 + b(x + x_1) + c = (x - x_1)\sqrt{b^2 - ac};$$

отсюда

$$x_1 = -\frac{(b - \sqrt{b^2 - 4ac})x + c}{ax + (b + \sqrt{b^2 - ac})}.$$

Это и есть формула решения, которую мы хотели вывести: здесь квадратный корень имеет два значения, сообразно чему получаются оба корня квадратного уравнения.

Замечательна эта формула тем, что в правую часть ее входит переменная x, могущая иметь любое значение; корень x_1 от x не зависит. Таким образом, давая для x различные значения, мы получаем бесчисленное множество различных по виду формул решения квадратного уравнения. Обычная формула получается при $x \to \infty$.

§ 124. Кубические уравнения. Общий вид кубического уравнения:

$$a_0x^3 + a_1x^2 + a_2x + a_3 = 0, \qquad a_0 \neq 0.$$

[60] Конечно, ρ^a не есть корень уравнения $f(x^a) = 0$; но по теореме § 115 можно найти целые числа γ и s так, что будет

$$a\gamma + p^n s = 1,$$

ибо $D(a, p^n) = 1$, при этом γ, как и a, не делится на p, то есть одно из чисел $a, b, \ldots$; далее, имеем:

$$a\gamma = 1 - p^n s,$$
$$(\rho^\gamma)^a = \rho^{a\gamma} = \rho^{1-p^n s} = \rho,$$

ибо $\rho^{-p^{n}s} = 1$;

$$f[(\rho^\gamma)^a] = f(\rho) = 0,$$

т. е. ρ^γ есть корень уравнения $f(x^a) = 0$. Подобно же рассуждаем для $f(x^b) = 0$ и т. д., т. е. для всех этих уравнений корнями будут $\rho, \rho^a, \rho^b, \ldots$, только в ином порядке.

Делим обе части на a_0 и производим подстановку:

$$x = y - \frac{a_1}{3a_0},$$

обозначим:

$$a = \frac{a_2}{a_0} - \frac{a_1^2}{3a_0^2}, \qquad b = \frac{2a_1^3}{27a_0^3} - \frac{a_1 a_2}{3a_0^2} + \frac{a_3}{a_0};$$

тогда данное уравнение принимает вид:

$$y^3 + ay + b = 0. \tag{4}$$

Положим $y = u + v$; тогда (4) примет вид:

$$u^3 + v^3 + (u + v)(3uv + a) + b = 0.$$

Так как мы вместо одного неизвестного y ввели два неизвестных u и v, то одно из них произвольно; или иначе, мы можем установить между ними произвольную зависимость.

Пусть

$$3uv + a = 0 \quad \text{или} \quad uv = -\frac{a}{3}. \tag{5}$$

Тогда данное уравнение примет вид: $u^3 + v^3 = -b$; из (2) получаем:

$$u^3 v^3 = -\frac{a^3}{27},$$

т. е. u^3 и v^3 суть корни квадратного уравнения:

$$z^2 + bz - \frac{a^3}{27} = 0,$$

откуда

$$z = -\frac{b}{2} \pm \sqrt{\frac{b^2}{4} + \frac{a^3}{27}};$$

следовательно;

$$u^3 = -\frac{b}{2} + \sqrt{\frac{b^2}{4} + \frac{a^3}{27}}, \qquad v^3 = -\frac{b}{2} - \sqrt{\frac{b^2}{4} + \frac{a^3}{27}};$$

отсюда же

$$y = \sqrt[3]{-\frac{b}{2} + \sqrt{\frac{b^2}{4} + \frac{a^3}{27}}} + \sqrt[3]{-\frac{b}{2} - \sqrt{\frac{b^2}{4} + \frac{a^3}{27}}}. \tag{6}$$

Это — так называемая *формула Кардано* решения кубического уравнения (§ 102); способ же решения кубического уравнения, который мы изложили, принадлежит голландскому математику Гудде (Hudde).

Заметим, что кубический корень из любого числа имеет всегда три значения: если $\sqrt[3]{\alpha} = \xi$ — одно значение, то два другие суть $\omega\xi$, $\omega^2\xi$, где ω и ω^2 — мнимые кубические корни из единицы, именно, корни уравнения

$$\frac{x^3 - 1}{x - 1} = x^2 + x + 1 = 0,$$

т. е.

$$\omega = \frac{-1+\sqrt{3}}{2}, \qquad \omega^2 = \frac{-1-i\sqrt{3}}{2};$$

можно непосредственно проверить, что ω^2 есть действительно квадрат числа ω.

Итак, и u, и v имеют по три значения, комбинируя которые друг с другом, мы получим всего девять значений для y; но из них только три являются корнями уравнения (4), ибо u и v связаны условием (5). Это условие допускает всего лишь три комбинации u и v и соответственно, им три значения для y. Пусть u, v — одна пара значений, удовлетворяющих условию (5); тогда $y_0 = u + v$ — один из корней; два других корня будут: $y_1 = \omega u + \omega^2 v$, $y_2 = \omega^2 u + \omega v$.

Соответственно им существуют и три корня уравнения с неизвестным x:

$$x_0 = -\frac{a_1}{3a_0} + u + v, \qquad x_1 = -\frac{a_1}{3a_0} + \omega u + \omega^2 v,$$
$$x_2 = -\frac{a_1}{3a_0} + \omega^2 u + \omega v.$$

Все эти три корня различны при $\dfrac{b^2}{4} + \dfrac{a^3}{27} \neq 0$; выражение $\dfrac{b^2}{4} + \dfrac{a^3}{27}$ есть так называемый *дискриминант* уравнения (4), если к нему приписать еще множитель $-4 \cdot 27$. Если подставим значения для a и b через a_0, a_1, a_2, a_3, то получим:

$$-4 \cdot 27 \left(\frac{b^2}{4} + \frac{a^3}{27} \right) = \frac{1}{a_0^4};$$

D — дискриминант данного уравнения для x.

Итак, при $D \neq 0$ все три корня различны.

Пусть теперь $D = 0$, т. е. $\dfrac{b^2}{4} + \dfrac{a^3}{27} = 0$; тогда

$$u = v = \sqrt[3]{-\frac{b}{2}};$$

но так как здесь $\left(-\dfrac{b}{2} \right)^2 = \left(-\dfrac{a}{3} \right)^3$, то находим:

$$\sqrt[3]{-\frac{b}{2}} = -\frac{b}{2} : \sqrt[3]{\left(-\frac{b}{2} \right)} = -\frac{b}{2} : \sqrt[3]{\left(-\frac{a}{3} \right)^3} =$$
$$= -\frac{b}{2} : \left(-\frac{a}{3} \right) = \frac{3b}{2a}.$$

Докажем, что при $u = v = \dfrac{3b}{2a}$ условие (2) удовлетворяется; действительно:

$$uv = \frac{9b^2}{4a^3} = -\frac{9a^3}{27a^2} = -\frac{a}{3}, \quad \text{ибо} \quad \frac{b^2}{4} = -\frac{a^3}{27}.$$

Итак, в этом случае

$$y_0 = u + v = \frac{3b}{a}, \qquad y_1 = y_2 = \frac{3b}{2a}(\omega + \omega^2) = -\frac{3b}{2a}.$$

Соответственно этому:

$$x_0 = -\frac{a_1}{3a_0} + \frac{2a_1^3 - a_0a_1a_2 + 3a_0^2a_3}{a_0(3a_0a_2 - a_1^2)} = \frac{7a_1^3 - 6a_0a_1a_2 + 9a_0^2a_3}{a_0(3a_0a_2 - a_1^2)},$$

$$x_1 = x_2 = -\frac{a_1}{3a_0} - \frac{2a_1^3 - a_0a_1a_2 + 3a_0^2a_3}{a_0(3a_0a_2 - a_1^2)} = -\frac{4a_1^3 + 6a_0a_1a_2 + 9a_0^2a_3}{a_0(3a_0a_2 - a_1^2)}.$$

Если кроме условия $D = 0$ выполнено и условие $b = 0$, то

$$y_0 = y_1 = y_2 = 0, \qquad x_0 = x_1 = x_2 = -\frac{a_1}{3a_0},$$

т. е. в этом и только в этом случае существует тройной корень. Условие $D = 0$ здесь можно заменить условием $a = 0$, т. е. получаем такие условия для тройного корня:

$$3a_0a_2 - a_1^2 = 0, \qquad 2a_1^3 - 9a_0a_1a_2 + 27a_0^2a_3 = 0;$$

последнее условие можно заменить таким: $27a_0^2a_3 - a_1^3 = 0$.

§ 125. Пусть все коэфициенты a_0, a_1, a_2, a_3, а следовательно, и a, b вещественны. Разберем вопрос о вещественности корней.

1. При $D = 0$ все корни вещественны, ибо, как мы видели, они выражаются рационально через коэфициенты.

2. При $D < 0$, $\frac{b^2}{4} + \frac{a^3}{27} > 0$, т. е. корень квадратный в u и v вещественен и, таким образом, вещественны количества $-\frac{b}{2} \pm \sqrt{\frac{b^2}{4} + \frac{a^3}{27}}$; в этом случае для u и v можно взять вещественные кубические корни, ибо при них условие (5) удовлетворится. Следовательно, y_0 вещественно, а

$$y_1 = -\frac{u+v}{2} + \frac{i\sqrt{3}}{2}(u - v), \qquad = y_1 = -\frac{u+v}{2} - \frac{i\sqrt{3}}{2}(u - v)$$

сопряженно комплексны. Точно так же x_0 вещественно, а x_1, x_2 сопряженно комплексны.

3. При $D > 0$, $\frac{b^2}{4} + \frac{a^3}{27} < 0$, т. е. $\sqrt{\frac{b^2}{4} + \frac{a^3}{27}}$ — мнимое число, и $-\frac{b}{2} \pm \sqrt{\frac{b^2}{4} + \frac{a^3}{27}}$ — сопряженные комплексные числа; u и v тоже сопряженно комплексны [ибо по (5) их произведение вещественно); точно так же ωu и $\omega^2 v$ сопряженно комплексны, и $\omega^2 u$ и ωv тоже. Следовательно, y_0, y_1, y_2 вещественны; именно, если $u = \alpha + \beta i$, $v = \alpha - \beta i$, то $y_0 = 2\alpha$, $y_1 = -\alpha - \beta\sqrt{3}$, $y_2 = -\alpha + \beta\sqrt{3}$. Конечно, и x_0, x_1, x_2 в этом случае тоже вещественны.

Но в этом случае формула Кардано совершенно неприменима: приходится извлекать кубический корень из комплексного числа $\alpha_1 + \beta_1 i$; мы докажем, что это извлечение сводится опять к решению уравнения (4), т. е. получается порочный круг. Именно, пусть

$$\sqrt[3]{\alpha_1 + \beta_1 i} = \rho(\cos\varphi + i\sin\varphi);$$

тогда $\alpha_1^3 + \beta_1^3 = \rho^3(\cos 3\varphi + \sin 3\varphi)$; отсюда

$$\rho^3 = \sqrt{\alpha_1^2 + \beta_1^2}, \qquad \cos 3\varphi = \frac{\alpha_1}{\rho^3};$$

итак, ρ мы находим простым извлечением корня; посмотрим, как найти φ. Имеем $\cos 3\varphi = 4\cos^3\varphi - 3\cos\varphi$ (§ 11), $\cos\varphi = \xi$; получаем для ξ уравнение:

$$4\xi^3 - 3\xi - \frac{\alpha_1}{\rho^3} = 0, \quad \text{но} \quad \alpha_1 = -\frac{b}{2}, \qquad \beta_1 = \sqrt{-\frac{b^2}{4} - \frac{a^3}{27}},$$

$$\alpha_1^2 + \beta_1^2 - \frac{a^3}{27} = \rho^6;$$

следовательно:

$$\cos 3\varphi = \frac{\alpha_1}{\rho^3} = -\frac{b}{2} : \sqrt{-\frac{a^3}{27}} = \frac{b}{2} : \left(\frac{a}{3}\sqrt{-\frac{a}{3}}\right).$$

Таким образом получаем для ξ уравнение:

$$4\xi^3 - 3\xi - \frac{b}{2} : \left(\frac{a}{3}\sqrt{-\frac{a}{3}}\right) = 0,$$

или

$$-8\,\frac{a}{3}\sqrt{-\frac{a}{3}}\,\xi^3 + 2a\sqrt{-\frac{a}{3}}\,\xi + b = 0;$$

сделаем подстановку:

$$2\sqrt{-\frac{a}{3}}\,\xi = t;$$

тогда:

$$-8\,\frac{a}{3}\sqrt{-\frac{a}{3}}\,\xi^3 = t^3,$$

и наше уравнение принимает вид: $t^3 + at + b = 0$, т. е. мы опять возвратились к уравнению (4). В этом случае применяется так называемое тригонометрическое решение. Имеем:

$$y_0 = 2\rho\cos\varphi = 2\sqrt{-\frac{a}{3}}\cos\varphi,$$

$$y_1 = -\rho\cos\varphi - \rho\sqrt{3}\sin\varphi = 2\sqrt{-\frac{a}{3}}\,\cos\left(\varphi + \frac{4\pi}{3}\right),$$

$$y_2 = -\rho\cos\varphi + \rho\sqrt{3}\sin\varphi = 2\sqrt{-\frac{a}{3}}\,\cos\left(\varphi + \frac{2\pi}{3}\right),$$

угол φ определяется из уравнения

$$\cos(3\varphi) = -\frac{b}{2} : \sqrt{-\frac{a^3}{27}}$$

и вычисляется при помощи логарифмов. Этот случай называется «*неприводимым*».

Пример 1. Уравнение $x^3 - x - 1 = 0$; здесь $a = -1$, $b = -1$;

$$\frac{b^2}{4} + \frac{a^3}{27} = \frac{1}{4} - \frac{1}{27} = \frac{23}{4\cdot 27} > 0,$$

т. е. здесь имеется один вещественный и два комплексных корня. Имеем:

$$u = \sqrt[3]{\frac{1}{2} + \frac{1}{2}\sqrt{\frac{23}{27}}}, \qquad v = \sqrt[3]{\frac{1}{2} - \frac{1}{2}\sqrt{\frac{23}{27}}};$$

пусть

$$N = \frac{1}{2}\sqrt{\frac{23}{27}},$$

тогда

$$\lg N = \frac{1}{2}\lg 23 - \frac{1}{2}\lg 27 - \lg 2, \qquad \lg 23 = 1,3617278, \qquad \lg 27 = 1,4313638,$$

$$\lg 2 = 0,3010300, \qquad \frac{1}{2}\lg 23 = 0,6808639, \qquad -\frac{1}{2}\lg 27 == \overline{1},2843181,$$

$$-\lg 2 = \overline{1},6989700;$$

следовательно:

$$\lg N = \overline{1},6641520, \quad N = 0,46148\ldots, \quad \frac{1}{2} + N = 0,96148, \quad \frac{1}{2} - N = 0,03852,$$

$$\lg 0,96148 = \overline{1},9829403, \quad \lg 0,03852 = \overline{2},5856863, \quad \lg u = \frac{1}{3}\lg 0,96148 = \overline{1},9943134,$$

$$\lg v = \frac{1}{3}\lg 0,03852 = \overline{1},5285621, \quad u = 0,98699, \quad v = 0,33772;$$

отсюда $x_0 = u + v = 1,32471\ldots$ — это верно с точностью до $0,001$; далее, найдем:

$$x_1 = \frac{u+v}{2} + i\frac{\sqrt{3}(u-v)}{2} = -0,662 + i \cdot 0,562,$$

$$x_2 = \frac{u+v}{2} - i\frac{\sqrt{3}(u-v)}{2} = -0,662 - i \cdot 0,562,$$

(x_1 и x_2 вычисляем тоже при помощи логарифмов).

Пример 2. Уравнение $x^3 - 4x^2 - 11x + 30 = 0$; здесь

$$a_0 = 1, \qquad a_1 = -4, \qquad a_2 = -11, \qquad a_3 = 30;$$

найдем

$$a = -\frac{49}{3}, \qquad b = \frac{486}{27};$$

уравнение для y:

$$y^3 - \frac{49}{3}y + \frac{286}{27} = 0, \qquad x = y + \frac{4}{3}.$$

Здесь

$$\frac{b^2}{4} + \frac{a^3}{27} = -\frac{97\,200}{27^2} < 0,$$

т. е. все три корня вещественны, и формула Кардано неприменима.

Берем тригонометрическое решение:

$$\cos(3\varphi) = -\frac{b}{2} : \sqrt{-\frac{a^3}{27}} = -\frac{143}{7^3},$$

$\lg \dfrac{147}{7^3} = \lg 143 - 3\lg 7 = 2,1553860 - 3 \cdot 0,8450980 = 2,1553860 - 2,5352940 = \overline{1},6200420$; пусть $\overline{1},6200420 = \cos\varphi_1$; тогда $\varphi_1 = 65°21'30''$; но $\cos(3\varphi) = -\cos\varphi_1$; следовательно, $3\varphi = 180° - \varphi_1$, $3\varphi = 114°38'30''$, $\varphi = 38°12'50''$;

$$\varphi + 240° = 278°12'50'' = 360° - 81°47'10'',$$
$$\varphi + 120° = 158°12'50'' = 180° - 21°47'10''.$$

Далее, имеем:

$$y_0 = 2\sqrt{-\frac{a}{3}}\cos\varphi = \frac{2\cdot 7}{3}\cos 38°12'50'',$$

точно так же:

$$y_1 = \frac{2\cdot 7}{3}\cos 81°47'10', \qquad y_2 = -\frac{2\cdot 7}{3}\cos 21°47'10''.$$

Находим:

$$\begin{array}{lll} \lg 2 = 0,3010300, & \lg\cos 38°12'50'' = \overline{1},8952606, & \lg y_0 = 0,5652673, \\ \lg 7 = 0,8450980 & \lg\cos 81°47'10'' = \overline{1},1549376, & \lg y_1 = \overline{1},8239443, \\ -\lg 3 = \overline{1},5228787, & \lg\cos 21°47'10'' = \overline{1},9678174, & \lg(-y_2) = 0,6368241, \end{array}$$

$y_0 = 3,675$, $y_1 = 0,667$, $y_2 = -4,333$. Далее, $x = y + 1,333$; следовательно, $x_0 = 5,008$, $x_1 = 2,000$, $x_2 - 3,000$.

Можно непосредственно убедиться, что числа 5, 2, -3 действительно являются корнями данного уравнения.

Упражнения

Исследовать и решить кубические уравнения:

153) $x^3 - 4x^2 + 3x - 12 = 0$.

Отв. $4, \pm i\sqrt{3}$ (корни).

154) $x^3 + 3x^2 + 7x + 5 = 0$.

Отв. -1, $-1 \pm 2i$ (корни).

155) $x^3 + 3x^2 - 2x - 6 = 0$.

Отв. -3, $\pm\sqrt{2}$ (корни).

156) $x^3 - 10x^2 + 12x + 72 = 0$.

Отв. -2, 6, 6 (корни).

157) $8x^3 - 60x^2 + 150x - 125 = 0$.

Отв. $2\dfrac{1}{2}$ (корень тройной).

§ 126. Уравнения четвертой степени. Способ Феррари. Общий вид уравнения четвертой степени:

$$a_0x^4 + a_1x^3 + a_2x^2 + a_3x + a_4 = 0; \tag{7}$$

его корни x_0, x_1, x_2, x_3; $a_0 \neq 0$; делим обе части на a_0 и делаем подстановку: $x = y - \dfrac{a_1}{4a_0}$; тогда получим:

$$y^4 + ay^2 + by + c = 0, \tag{8}$$

где

$$a = \frac{a_2}{a_0} - \frac{3}{8}\frac{a_1^2}{a_0^2},$$

$$b = \frac{a_3}{a_0} - \frac{1}{2}\frac{a_1 a_2}{a_0^2} + \frac{1}{8}\frac{a_1^3}{a_0^3},$$

$$c = \frac{a_4}{a_0} - \frac{1}{4}\frac{a_1 a_3}{a_0^2} + \frac{1}{16}\frac{a_1^2 a_2}{a_0^3} - \frac{3}{256}\frac{a_1^4}{a_0^4}.$$

Существует много способов решения уравнений четвертой степени; изложим три мы изложим три из них.

Способ Феррари (Ferrari). Преобразовываем левую часть (8) следующим образом:

$$y^4 + ay^2 \quad + \quad by + c = \left(y^2 + \frac{a}{2} + r\right)^2 - 2y^2 r +$$

$$+ \quad by - \frac{a^2}{4} - ar - r^2 + c = 0;$$

выбираем неопределенную величину r так, чтобы левая часть уравнения превратилась в разность квадратов двух целых функций от y; для этого должно быть:

$$b^2 - 4 \cdot 2r\left(r^2 + ar + \frac{a^2}{4} - c\right) = 0,$$

или

$$8r^3 + 8ar^2 + (2a^2 - 8c)r - b^2 = 0. \tag{9}$$

Это — уравнение для r; оно называется *разрешающим кубическимуравнением* или *кубической резольвентой* данного уравнения четвертой степени. Мы увидим, что это же самое уравнение встречается и в других способах; его вообще нельзя избежать при решении уравнения четвертой степени.

Найдя один его корень r, получим:

$$\left(y^2 + \frac{a}{2} + r\right)^2 - 2r\left(y - \frac{b}{4r}\right)^2 = 0,$$

т. е. уравнение (5) распадается на два квадратных:

$$y^2 + \sqrt{2r} \cdot y + \frac{a}{2} + r - \frac{b}{2\sqrt{2r}} = 0$$

и

$$y^2 - \sqrt{2r} \cdot y + \frac{a}{2} + r + \frac{b}{2\sqrt{2r}} = 0.$$

§ 127. Способ Декарта. Постараемся левую часть уравнения (7) разложить на два квадратных множителя:

$$a_0 x^4 + a_1 x^3 + a_2 x^2 + a_3 x + a_4 = a_0(x^2 + px + q)(x^2 + p'x + q');$$

перемножая в правой части и сравнивая коэфициенты, найдем:

$$p + p' = \frac{a_1}{a_0}, \qquad q + q' + pp' = \frac{a_2}{a_0}, \qquad pq' + qp' = \frac{a_3}{a_0}, \qquad qq' = \frac{a_4}{a_0};$$

обозначим еще $q+q'=\sigma$, тогда по второму из написанных уравнений $pp'=\dfrac{a_2}{a_0}-\sigma$. Берем теперь произведение:

$$\begin{vmatrix}1 & 1 & 0\\ p & p' & 0\\ q & q' & 0\end{vmatrix}\cdot\begin{vmatrix}1 & 1 & 0\\ p' & p & 0\\ q' & q & 0\end{vmatrix}=\begin{vmatrix}2 & p+p' & q+q'\\ p+p' & 2pp' & pq'+qp'\\ q+q' & pq'+qp' & 2qq'\end{vmatrix}=0,$$

ибо оба сомножителя равны нулю.

Иначе

$$\begin{vmatrix}2 & \frac{a_1}{a_0} & \sigma\\ \dfrac{a_1}{a_0} & 2\left(\dfrac{a_1}{a_0}-\sigma\right) & \dfrac{a_3}{a_0}\\ a_0\sigma & a_3 & 2a_4\end{vmatrix}=0$$

или, наконец,

$$\begin{vmatrix}2a_0 & a_1 & a_0\sigma\\ a_1 & 2a_2-2a_0\sigma & a_3\\ a_0\sigma & a_3 & 2a_4\end{vmatrix}=0.$$

Это — кубическое уравнение для σ; мы докажем позже, что это — то же самое уравнение, что и (9). Пусть $a_0\sigma=t$; тогда получим:

$$t^3-a_2t^2+(a_1a_3-4a_0a_4)t+4a_0a_2a_4a_0a_3^2-a_1^2a_4=0. \tag{10}$$

Положим $t=u+\dfrac{a_2}{3}$; тогда (10) перейдет в уравнение:

$$u^3-4g_2u+16g_3=0,$$

где

$$a_1a_3-4a_0a_4-\frac{a_2^2}{3}=-4g_2,$$

$$\frac{8}{9}a_0a_2a_4-8a_0a_3^2-a_1^2a_4+\frac{1}{3}a_1a_2a_3-\frac{2}{27}a_2^3=16g_3;$$

$g)2$ и g_3 — так называемые инварианты функций четвертой степени.

Положим еще $u=-4s$; тогда получим:

$$4s^3-g_2s-g_3=0 \tag{11}$$

нормальную форму кубического разрешающего уравнения.

Корни этого уравнения обозначим через e_1, e_2, e_3. Найдем дискриминант уравнения (11):

$$4^4(e_2-e_3)^2(e_3-e_1)^2(e_1-e_20^2=16(g_2^3-27g_3^2).$$

Найдя один корень уравнения (11) или (10), мы найдем и σ; после этого получим:

$$p+p'=\frac{a_1}{a_0},\qquad pp'==\frac{a_2}{a_0}-\sigma,$$

т. е. p и p' — корни квадратного уравнения:

$$z^2-\frac{a_1}{a_0}z+\frac{a_2}{a_0}-\sigma=0;$$

далее, $q+q'=\sigma$, $qq'=\dfrac{a_4}{a_0}$, т. е. q и q' — корни уравнения

$$z^2-\sigma z+\frac{a_4}{a_0}=0,$$

и данное уравнение (7) распадается на два уравнения: $x^2+px+q=0$ и $x^2+p'x+q'=0$; пусть x_0, x_1 — корни первого, x_2, x_3 — корни второго уравнения, тогда

$$x_0+x_1=-p, \qquad x_0x_1=q, \qquad x_2+x_3=-p], \qquad x_2x_3=q';$$

отсюда

$$q+q'=x_0x_1+x_2x_3=\sigma=\frac{a_2}{3a_0}-\frac{4s}{a_0},$$

где s один из корней уравнения (11); пусть это будет e_1; итак,

$$\left.\begin{aligned} x_0x_1+x_2x_3 &= \frac{a_2}{3a_0}-\frac{4e_1}{a_0}; \\ \text{подобным же образом найдем:} & \\ x_0x_2+x_1x_3 &= \frac{a_1}{3a_2}-\frac{4e_2}{a_0}, \\ x_0x_3+x_1x_2 &= \frac{a_0}{3a_2}-\frac{4e_3}{a_0}. \end{aligned}\right\} \tag{12}$$

Действительно, если мы вместо корня e_1 возьмем, например, корень e_2, то аналогично разложим наше уравнение четвертой степени на два квадратных уравнения, только распределение корней x_0, x_1, x_2, x_3 в них будет иное; пусть тогда одно квадратное уравнение имеет, например, корни x_0, x_2, а другое x_1, x_3. Точно так же корню e_3 соответствует распределение: x_0, x_3, и x_1, x_2. Заметим, что иных распределений нет.

Вычитая уравнения (12) друг из друга, получаем:

$$\left.\begin{aligned} 4(e_2-e_3)&=a_0(x_1-x_0)(x_2-x_3), \\ 4(e_3-e_1)&=a_0(x_2-x_0)(x_3-x_1), \\ 4(e_1-e_2)&=a_0(x_3-x_0)(x_1-x_2). \end{aligned}\right\} \tag{13}$$

Отсюда получаем дискриминант уравнения четвертой степени:

$$\begin{aligned} D &= a_0^6(x_1-x_0)^2(x_2-x_3)^2(x_2-x_0)^2(x_3-x_1)^2(x_3-x_0)^2(x_1-x_2)^2 \\ &= 4^6(e_2-e_3)^2(e_3-e_1)^2(e_1-e_20^2=16^2(g_2^3-27g_3^20, \end{aligned} \tag{14}$$

т. е. если D_1 — дискриминант уравнения (11), то имеем:

$$D=16D_1. \tag{14a}$$

Согласно (11) имеем: $e_1+e_2+e_3=0$ или $3e_1=(e_1-e_2)+(e_1-e_3)$; отсюда по (13) найдем:

$$\left.\begin{aligned} 12e_1 &= a_0[(x_3-x_0)(x_1-x_2)-(x_2-x_0)(x_3-x_1)], \\ \text{точно так же} & \\ 12e_2 &= a_0[(x_1-x_0)(x_2-x_3)-(x_3-x_0)(x_1-x_2)], \\ 12e_3 &= a_0[(x_2-x_0)(x_3-x_1)-(x_1-x_0)(x_2-x_3)], \end{aligned}\right\} \tag{15}$$

т. е. корни разрешающего кубического уравнения выражаются рационально через корни данного уравнения четвертой степени.

§ 128. Способ Эйлера. В уравнении (8) положим:

$$2y = u + v + w;$$

обозначим еще

$$S = u^2 + v^2 + w^2, \qquad T = v^2w^2 + w^2u^2 + u^2v^2.$$

Имеем:

$$4y^2 = S + 2(vw + wu + uv),$$
$$16y^4 = S^2 + 4S(vw + wu + uv) + 4T + 8uvw(u + v + w);$$

подставляя это в (8), получаем:

$$S^2 + 4T + 4aS + 16c + 8(uvw + b)(u + v + w) +$$
$$+4(S + 2a)(vw + wu + uv) = 0.$$

Установим теперь следующие зависимости между u, v и w:

$$S + 2a = 0, \qquad uvw + b = 0; \tag{16}$$

тогда уравнение (8) превратится в уравнение:

$$S^2 + 4T + 4aS + 16c = 0,$$

или вместо S подставляя ^-2a [по первому уравнению (16)]:

$$T = a^2 - 4c. \tag{17}$$

Формулы (16) и (17) показывают, что u^2, v^2, w^2 — корни уравнения:

$$z^3 + 2az^2 + (a^2 - 4c)z - b^2 = 0; \tag{18}$$

легко видеть, что это — то же уравнение, что и (9); именно, $z = 2r$; если положим $a_0\left(\frac{z}{4} + \frac{a}{6}\right) = -s$ или $z = \frac{4s}{a_0} - \frac{2}{3}a$, то получим уравнение (11). Таким образом уравнения (9), (10) и (18) линейными подстановками преобразовываются в одно и то же уравнение (11), т. е. все эти уравнения по своему существу равносильны: решив одно из них, мы тем самым решим и все остальные.

Решив уравнение (18), т. е. найдя u^2, v^2 и w^2, мы извлечением квадратного корня найдем u, v и w; комбинируя различные знаки у корней, найдем восемь различных комбинаций u, v и w; но из них годны только четыре: именно, второе уравнение (16) дает: $uvw = -b$; если u, v и w — одна комбинация, удовлетворяющая этому условию, то другие комбинации будут u, $-v$, $-w$; $-u$, v, $-w$; $-u$, $-v$, w. Итак, получаем:

$$2y_0 = u + v + w, \qquad 2y_1 = u - v - w,$$
$$2y_2 = -u + v - w, \qquad 2y_3 = -u - v + w,$$

или для корней уравнения (7):

$$\left.\begin{aligned} x_0+\frac{a_1}{4a_0}&=\frac{u+v+w}{2}, \qquad x_2+\frac{a_1}{4a_0}=\frac{-u+v-w}{2},\\ x_1+\frac{a_1}{4a_0}&=\frac{u-v-w}{2}, \qquad x_3+\frac{a_1}{4a_0}=\frac{-u-v+w}{2}. \end{aligned}\right\} \tag{19}$$

Из (19) и (15) выводим:

$$-\frac{e_1}{a_0}=\frac{u^2}{4}+\frac{a}{6}, \qquad -\frac{e_2}{a_0}=\frac{v^2}{4}+\frac{a}{6}, \qquad -\frac{e_3}{a_0}=\frac{w^2}{4}+\frac{a}{6}. \tag{20}$$

§ 129. Кратность корней. Относительно кратности корней в уравнении четвертой степени могут быть пять случаев: 1) один четырехкратный корень; 2) один тройной корень и один простой; 3) два двойных корня; 4) один двойной и два простых корня; 5) все корни простые.

1. Пусть $x_0=x_1=x_2=x_3$; тогда по (15) $e_1=e_2=e_3=0$; далее, по (19) $v+w=0$, $w+u=0$, $u+v=0$, т. е. $v=-w=u$, $v=-u$, $u=-u=0$, $v=0$, $w=0$; следовательно, по (20) и $a=0$, или $8a_0a_2-3a_1^2=0$, и из (11) $g_2=0$, $g_3=0$.

Условия $a=0$, $g_2=0$, $g_3=0$ достаточны для существования четырехкратного корня, ибо если они выполнены, то $e_1=e_2=e_3=0$, $u=v=w=0$, т. е. $x_0=x_1=x_2=x_3$. Заметим, что уравнения $g_2=0$, $g_3=0$ влекут за собою и $D=0$ [по (14)], но не обратно. Условия $a=0$, $g_2=0$, $g_3=0$ равносильны условиям $a=0$, $b=0$, $c=0$ [по (18)]. Искомый корень есть $-\dfrac{a_1}{4a_0}$.

2. Пусть $x_0\neq x_1=x_2=x_3$; следовательно, по [(19)] $u-v-w=-u+v-w=-u-v+w$, откуда $u=v=w\neq 0$, иначе все x были бы равны, но из (15) заключаем: $e_1=e_2=e_3=0$. Следовательно, по (20) $u^2=v^2=w^2=-\dfrac{2}{3}a$, т. е. $a\neq 0$, или $8a_0a_2-3a_1^2\neq 0$, но $g_2=g_3=0$.

Обратно, если $_2=0$, $g_3=0$, $a\neq 0$, то уравнение имеет один тройной корень и один простой: именно, тогда $e_1=e_2=e_3=0$, $u^2=v^2=w^2\neq 0$; следовательно, $\pm u=\pm v=\pm w$; здесь может быть одна из четырех комбинаций:

$$\begin{aligned} &a)\quad u=v=w, && \text{тогда} && x_0\neq x_1=x_2=x_3,\\ &b)\quad u=-v=w, && \text{''} && x_2\neq x_0=x_1=x_3,\\ &c)\quad u=v=-w, && \text{''} && x_3\neq x_0=x_1=x_2,\\ &d)\quad -u=v=w, && \text{''} && x_4\neq x_0=x_2=x_3. \end{aligned}$$

Условия $g_2=0$, $g_3=0$ можно заменить такими:

$$a^2+12c=0, \qquad 8a^3+27b^2=0;$$

эти равенства (см. конец § 124) говорят, что уравнение (18) имеет тройной корень, т. е. $u^2=v^2=w^2$; При $a\neq 0$ этот корень не равен нулю; но e_1, e_2, e_3 при этом равны нулю.

3. Пусть $x_0=x_1\neq x_2\neq x_3$; тогда по (15) $e_1=e_2\neq e_3$. Далее, по (19):

$$u+v+w=u-v-w, \qquad -u+v-w=-u-v+w;$$

следовательно, $v+w=0$, $v-w=0$, т. е. $v=w=0\neq u$ (иначе был бы случай 1). Итак, уравнение (18) имеет двойной корень, равный нулю, т. е. $a^2-4c=0$, $b=0$, но $a\neq 0$. Далее, $g_2\neq 0$, $g_3\neq 0$, но $D=0$.

Обратно, если $a\neq 0$, но $b=0$, $a^2-4c=0$, то уравнение имеет два двойных корня. Именно, тогда (18) имеет два корня, равных нулю, и может иметь место один из трех случаев:

$$\begin{array}{lllll} a) & v=w=0\neq u & \text{тогда} & x_0=x_1\neq x_2=x_3, \\ b) & w=u=0\neq v & '' & x_0=x_2\neq x_1=x_3 \\ c) & u=v=0\neq w & '' & x_0=x_3\neq x_1=x_2. \end{array}$$

4. Пусть $x_2=x_3$, но x_0, x_2 все различны; тогда по (14): $e_2=e_3\neq e_1$. Далее, по [(16)]: $-u+v-w=-u-v+w$; $v=w\neq u$ (иначе был бы случай 1 или 2), и $v\neq w\neq 0$ (иначе был бы случай 3); следовательно, a_2-4c и b не равны одновременно нулю. Далее, здесь тоже $g_2\neq 0$, $g_3\neq 0$, но $D=0$.

Обратно, если $D=0$, но a_2-4c и b не равны одновременно нулю и $g_2\neq 0$, $g_3\neq 0$, то уравнение имеет один двойной корень и два простых. Именно, тогда уравнение (18) имеет один двойной корень, не равный нулю, и один простой.

Имеем здесь три случая:

a) $\pm v=w\neq u$, тогда $x_2=x_3$, но x_0, x_1, x_2 различны; или $x_0=x_1$, но x_1, x_2, x_3 различны;

b) $\pm w=u\neq v$, тогда $x_1=x_3$, но x_0, x_1, x_2 различны; или $x_0=x_2$, но x_0, x_1, x_3 различны;

c) $\pm u=v\neq w$, тогда $x_0=x_3$, но x_0, x_1, x_2 различны; или $x_1=x_2$, x_0, x_1, x_3 различны.

5. Как известно из общей теории, все корни различны тогда и только тогда, если $D\neq 0$.

§ 130. Вещественность корней при вещественных коэфициентах. Пусть все коэфнциенты нашего уравнения вещественны. Тогда могут быть следующие три случая: 1) все корни вещественны, 2) два корня вещественны, а два сопряженно комплексны, 3) все корни мнимы (попарно сопряженны).

Из (14) видно, что в случаях 1 и 3 $D>0$, а в случае 2 $D<0$. Разберем подробнее случаи 1 и 3. В случае 1 $u^2, v^2, w^2>0$, т. е. уравнение (18) имеет все три корня положительные (один из них может быть равен нулю); из (14a) следует, что все три корня уравнения (15) должны быть вещественны; чтобы они были и положительными, мы по теореме Декарта (§ 89) заключаем, что должно быть: $a<0$, $a^2-4c>0$, чтобы в ряду $1, 2a, a^2-4c, -b^2$ были три перемены знака. Это условие необходимо и достаточно, ибо при нем отрицательных корней уравнение (18) иметь не может. В случае, если один из корней уравнения (18) равен нулю, то $b=0$ и два остальных корня удовлетворяют квадратному уравнению: $z^2+2az+(a^2-4c)=0$; оба корня этого уравнения положительны опять-таки при $a<0$, $a^2-4c>0$.

Итак, при $D\neq 0$:

1) $D>0$, $a<0$, $a_2-4c>0$ — все корни вещественны.

2) $D<0$, — два корня вещественны и два мнимы.

3) $D>0$, но не выполняется одновременно $a<0$, $a_2-4c>0$ — все корни мнимы.

Пусть теперь $D = 0$. В случаях 1 и 2 § 129 не может быть мнимых корней; эти случаи характеризуются тем, что $g_2 = 0$, $g_3 = 0$ или $a^2 + 12c = 0$, $8a^3 + 27b^2 = 0$. Заметим, что при $a \neq 0$ также и $b \neq 0$ и $c \neq 0$, при этом $a < 0$, $a^2 - 4c > 0$.

В случае 3 § 129 или все корни вещественны, или все мнимы (т. е. имеется два двойных мнимых корня), смотря по тому, какой знак имеет единственный неравный нулю корень уравнения (18), или какой знак имеет a. Если $a < 0$, то все корни вещественны; если же $a > 0$, то все корни мнимы.

В случае 4 § 129 или все корни вещественны, или двойной корень вещественен, а два остальные мнимы. Вещественны все корни тогда и только тогда, если все корни уравнения (18) положительны (один простой корень может быть равен нулю), для чего необходимо и достаточно, чтобы было $a < 0$, $a^2 - 4c > 0$. Если это не выполнено, то имеем два мнимых корня. Итак, получаем следующую таблицу:

1. Все корни вещественны:

a) При $D > 0$, $a < 0$, $a_2 - 4c > 0$.

b) " $D = 0$, $a \leq 0$, $a_2 - 4c = 0$, $b = 0$.

2. Два корня вещественны и два мнимы:

a) При D < 0.

b) " $D = 0$, если не выполнены условия $a_2 - 4c = b = 0$, или $a < 0$, $a_2 - 4c > 0$.

3. Все корни мнимы:

a) При $D > 0$, если не выполнены условия $a < 0$, $a^2 - 4c > 0$.

b) " $D = 0$, $a > 0$, $a_2 - 4c = 0$, $b = 0$.

Пример 1. Дано уравнение $x^4 - 8x^3 + 18x^2 - 27 = 0$; берем $x = y + 2$ и находим уравнение для y:

	1	−8	18	0	−27
2	1	−6	6	12	−3
2	1	−4	−2	8	
2	1	−4	−2	7	
2	1	−2	−6		
2	1	0			
	1				

так что получаем $y^4 - 6y^2 + 8y - 3 = 0$, здесь $a = -6$, $b = 8$, $c = -3$. Далее находим уравнение с корнями u^2, v^2, w^2, [уравнение (18)]: $z^3 - 12z^2 + 48z - 64 = 0$ легко видеть, что левая часть этого уравнения есть $(z - 4)^3$, т. е. $u^2 = v^2 = w^2 = 4$ и мы имеем здесь случай 2 § 129: один тройной корень и один простой. Имеем по формулам (19), если считать, что $u = v = w = -2$ [согласно второму уравнению (16)

$$x_0 = 2 + \frac{-6}{2} = 2 - 3 = -1, \qquad x_1 = x_2 = x_3 = 2 + \frac{2}{2} = 3.$$

Пример 2. Дано уравнение $x^4 + 2x^3 + 5x^2 + 4x + 4 = 0$. Находим $x = y - \frac{1}{2}$.

$$\begin{array}{r|ccccc} & 1 & 2 & 5 & 4 & 4 \\ -\frac{1}{2} & 1 & \frac{3}{2} & \frac{17}{4} & \frac{15}{8} & \frac{49}{16} \\ -\frac{1}{2} & 1 & 1 & \frac{15}{4} & 0 & \\ -\frac{1}{2} & 1 & \frac{1}{2} & \frac{7}{2} & & \\ -\frac{1}{2} & 1 & 0 & & & \\ & 1 & & & & \end{array}$$

$y^4 + \frac{7}{2}y^2 + \frac{49}{16} = 0$; уравнение (18): $z^3 + 3z^2 = 0$, т. е. можно взять $u^2 = -7$, $v^2 = w^2 = 0$; здесь мы имеем случай 3 § 129. Пусть $u = i\sqrt{7}$; тогда

$$x_0 = x_1 = \frac{-1 + \sqrt{7}}{2}, \qquad x_2 = x_3 = \frac{-1 - \sqrt{7}}{2}.$$

Упражнения

Решить и исследовать уравнения четвертой степени:

158) $x^4 - 2x^3 - 13x^2 + 38x - 24 = 0$.

Отв. Корни 1, ?2, 3, -4.

159) $x^4 - 3x^3 + x^2 + 4 = 0$.

Отв. Корни 2 — двойной, $\frac{-1 \pm i\sqrt{3}}{2}$.

160) $x^4 + 3x^3 + x^2 + 15x - 20 = 0$.

Отв. Корни 1, -4, $\pm i\sqrt{5}$.

161) $256x^4 - 768x^3 + 864x^2 - 432x + 81 = 0$.

Отв. $\frac{3}{4}$ — 4-кратный корень.

162) $x^4 + 3x^3 + 6x^2 + 6x + 4 = 0$.

Отв. Корни $-1 \pm i\sqrt{3}$, $\frac{-1 \pm i\sqrt{7}}{2}$.

§ 131. Общие замечания. В предыдущих параграфах было изложено так называемое «алгебраическое» решение уравнений третьей и четвертой степеней, т. е. решение этих уравнений в радикалах или при помощи извлечения корней. Уравнения степени выше четвертой в общем виде, как уже было сказано выше (§ 102), не решаются в радикалах, но существуют специальные классы уравнений высших степеней, которые решаются в радикалах. Один такой весьма обширный класс уравнений нашел Абель, а вполне исследовал этот вопрос Галуа, давший теорию алгебраических уравнений, носящую его имя (глава XII).

Впрочем, решения уравнений третьей и четвертой степеней в радикалах, важные теоретически, практического значения не имеют: они слишком громоздки и гораздо сложнее, чем вычисление корней по одному из общих способов, указанных в главе V.

Наконец, в так называемом «неприводимом случае» (§ 125) у кубических уравнений решение в радикалах вообще неприменимо, т. е. совершенно никакого практического значения не имеет.

ГЛАВА ВОСЬМАЯ

СИММЕТРИЧЕСКИЕ ФУНКЦИИ

§ 132. Определения. Основная теорема. Целая рациональная функция n переменных $x_1, x_2, \ldots, x_n$ есть многочлен вида:

$$\sum A_{\alpha_1,\alpha_2,\ldots,\alpha_n} x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}, \tag{1}$$

здесь $A_{\alpha_1,\alpha_2,\ldots,\alpha_n}$ — постоянные, т. е. независимые от $x_1, x_2, \ldots, x_n$ коэфициенты; сумма берется для значений:

$$\alpha_1 = 0, 1, 2, \ldots, m_1, \qquad \alpha_1 = 0, 1, 2, \ldots, m_2, \quad \ldots, \quad \alpha_n = 0, 1, 2, \ldots, m_n,$$

причем каждое значение α_1 комбинируется с каждым значением α_2, — с каждым значением α_3 и т. д. Таким образом в сумме (1) имеется всего

$$(m_1 + 1)(m_2 + 1) \cdots (m_n + 1)$$

слагаемых, хотя, конечно, некоторые из них могут быть равны нулю. Эту сумму (1) можно представить как ц. р. функцию только от x_1; коэфициенты этой функции будут ц. р. функциями от $x_2, x_3, \ldots, x_n$; степень функции (1) как ц. р. функции от x_1 есть m_1 точно так же относительно x_2 функция (1) m_2-й степени и т. д. Вообще функцию (1) можно представить как ц. р. функцию от любых k из n переменных.

Сумма показателей при переменных $\alpha_1 + \alpha_2 + \ldots + \alpha_n$ в данном члене называется *измерением* этого члена. В одном или в нескольких из членов функции (1) измерение — наибольшее; это наибольшее измерение есть *степень* функции (1) от n переменных. Если все члены функции одного и того же измерения, то функция — *однородная*. Очевидно, что всякая ц. р. функция от n переменных представляется как сумма однородных функций.

Пример 1. $5x_1^2x_2x_3 - 2x_1x_3^2 + x_2^4 + \dfrac{3}{4}x_1x_2x_3x_4 - 3x_1^2x_4^2 - \dfrac{2}{3} - x_1x_2x_4^2$ — однородная функция четвертого измерения.

Пример 2. $8x_1^3x_2 - 2x_1x_2x_4 + 6x_1x_2^2x_3^2 - 4x_1^2x_2 + 2x_1x_3 - 6x_1^2x_2^3 + x_1^2$ неоднородная функция пятой степени; она представляется как сумма четырех однородных функций:

$$2x_1x_3 + x_1^2, \qquad -5x_3^3 - 4x_1^2x_2 - 2x_1x_2x_4, \qquad 8x_1^3x_2, \qquad 6x_1x_2^2x_3^2 - 6x_1^2x_2^3.$$

§ 133. Существуют ц. р. функции нескольких переменных, не меняющие своего вида от любой перестановки этих переменных; такие функции называются симметрическими. Такова, например, функция:

$$x_1^2x_3 + x_1^2x_3 + x_2^2x_1 + x_2^2x_3 + x_3^2x_1 + x_3^2x_2 + 3(x_1 + x_2 + x_3).$$

Если $a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \ldots + a_n = 0$ данное алгебраическое уравнение с корнями $x_1, x_2, \ldots, x_n$, то как известно, связь между корнями и коэфициентами уравнения дается формулами § 50.

Это — формулы Вьета; они позволяют по данным корням составить уравнение.

Правые их части — симметрические функции от $x_1, x_2, \ldots, x_n$, при этом *простейшие* симметрические функции: они — первой степени относительно каждого из переменных; называются они *элементарными симметрическими функциями.* Обозначим их:

$$\left.\begin{array}{c} x_1 + x_2 + \ldots + x_n = \sum x_\lambda = f_1, \qquad \sum x_\lambda x_\mu = f_2, \\ \sum x_\lambda x_\mu x_\nu = f_3, \quad \ldots, \quad x_1x_2\cdots x_nf_n. \end{array}\right\} \tag{2}$$

Тогда уравнение с корнями $x_1, x_2, \ldots, x_n$ можно представить в виде:

$$x^n - f_1x^{n-1} + f_2x^{n-2} - \ldots + (-1)^n f_n = 0. \tag{3}$$

При произвольных $x_1, x_2, \ldots, x_n$ всегда существуют $f_1, f_2, \ldots, f_n$; но и обратно: при произвольных $f_1, f_2, \ldots, f_n$ всегда существуют $x_1, x_2, \ldots, x_n$, именно, корни уравнения (3), т. е. $f_1, f_2, \ldots, f_n$, так же независимы друг от друга, как и $x_1, x_2, \ldots, x_n$.

Если $\varphi(z_1, z_2, \ldots, z_n)$ — любая ц. р. функция от $z_1, z_2, \ldots, z_n$, и мы подставим $z_1 = f_1$, $z_2 = f_2$, $\ldots$, $z_n = f_n$, то получим $\varphi(f_1, f_2, \ldots, f_n) = \psi(x_1, x_2, \ldots, x_n)$ — целую рациональную функцию и при этом симметрическую функцию от $x_1, x_2, \ldots, x_n$, ибо, если как-нибудь переставим $x_1, x_2, \ldots, x_n$, то ведь $f_1, f_2, \ldots, f_n$ не изменятся, т. е. не изменится и φ. Но важно то, что и обратная теорема верна:

Основная теорема теории симметрических функций. *Всякая целая рациональная симметрическая функция $F(x_1, x_2, \ldots, x_n)$ от $x_1, x_2, \ldots, x_n$ представляется как целая рациональная функция от элементарных симметрических функций: $F(x_1, x_2, \ldots, x_n) = G(f_1, f_2, \ldots, f_n)$ и притом только одним образом; при этом представлении над коэфициентами F совершаются только действия сложения, вычитания, умножения, т. е. если в F все коэфициенты — целые числа, то и в G все коэфициенты тоже целые числа.*

Мы дадим три доказательства этой теоремы.

§ 134. Суммы степеней. Формулы Ньютона. Рассмотрим еще один класс симметрических функций — это так называемые *степенные суммы*:

$$s_\alpha = x_1^\alpha + x_2^\alpha + \ldots + x_n^\alpha; \qquad \alpha = 1, 2, 3, \ldots;$$

при $\alpha = 0$ имеем $s_0 = n$. При данном числе n переменных, степенных сумм бесчисленное множество, тогда как элементарных симметрических функций всего только n.

Выведем *формулы Ньютона*, выражающие зависимость степенных сумм и элементарных симметрических функций друг от друга.

Пусть $f(x) = x^n - f_1x^{n-1} + f_2x^{n-2} - \ldots + (-1)^n f_n$. По § 56 (10) имеем:

$$f'(x) = \sum_{\varkappa=1}^{n} \frac{f(x)}{x - x_\varkappa};$$

далее, по способу Горнера (§ 51) находим:

$$\frac{f(x)}{x-x_\varkappa}=x^{n-1}+f_1(x_\varkappa)x^{n-2}+f_2(x_\varkappa)x^{n-3}+\ldots+f_{n-1}(x_\varkappa),$$

где

$$f_\lambda(x)=x^\lambda-f_1x^{\lambda-1}+f_2x^{\lambda-2}-\ldots+(-1)^\lambda f_\lambda;$$

подставляя сюда вместо x $x_1,x_2,\ldots,x_n$, и складывая, получаем:

$$\sum_{\varkappa=1}^{n}f_\lambda(x_\varkappa)=s_\lambda-f_1s_{\lambda-1}+f_2s_{\lambda-2}-\ldots+(-1)^\lambda nf_\lambda;$$

отсюда

$$f'(x)=\sum_{\varkappa=1}^{n}[x^{n-1}+f_1(x_\varkappa)x^{n-2}+\ldots+f_{n-1}(x_\varkappa)]=$$
$$=nx^{n-1}+\sum_{\varkappa=1}^{n}f_1(x_\varkappa)x^{n-2}+\sum_{\varkappa=1}^{n}f_1(x_\varkappa)x^{n-3}+\ldots+\sum_{\varkappa=1}^{n}f_{n-1}(x_\varkappa),$$

или, сравнивая коэфициенты при x в обеих частях, найдем:

$$(-1)^\lambda(n-\lambda)f_\lambda=\sum_{\varkappa=1}^{n}f_\lambda(x_\varkappa)=s_\lambda-f_1s_{\lambda-1}+f_2s_{\lambda-2}-\ldots+(-1)^\lambda nf_\lambda;$$

отсюда

$$s_\lambda-f_1s_{\lambda-1}+f_2s_{\lambda-2}-\ldots+(-1)^\lambda\lambda f_\lambda=0. \tag{4}$$

Это — *первая формула Ньютона*, годная для $\lambda=1,2,\ldots,n-1$.

Имеем, далее:

$$f(x_\varkappa)=0,\qquad x_\varkappa^\lambda f(x_\varkappa)=0,\qquad \sum_{\varkappa=1}^{n}x_\varkappa^\lambda f(x_\varkappa)=0,$$

или

$$s_{n+\lambda}-f_1s_{n+\lambda-1}+f_2s_{n+\lambda-2}-\ldots+(-1)^nf_ns_\lambda=0. \tag{5}$$

Это — *вторая формула Ньютона*, годная для $\lambda=0,1,2,3,\ldots$ Эти две формулы дают возможность выразить последовательно $s_1,s_2,s_3,\ldots$ через $f_1,f_2,\ldots,f_n$, и обратно — $f_1,f_2,\ldots,f_n$ через $s_1,s_2,s_3,\ldots$ Легко убедиться, что s_λ зависит только от $f_1,f_2,\ldots,f_\lambda$ при $\lambda\geq n$; при $\lambda\geq n$ s_λ зависит от $f_1,f_2,\ldots,f_n,\ldots$, f_λ зависит только от $s_1,s_2,\ldots,s_\lambda$. В выражении для s_λ через $f_1,f_2,\ldots,f_\lambda$ все коэфициенты целые; в выражении же f_λ через $s_1,s_2,\ldots,s_\lambda$ все коэфициенты дробные. Формулы (5) получаются из (4), если положить $f_{n+1}=0$, $f_{n+2}=0,\ldots$; поэтому, если мы вычислим s_λ для случая n переменных и захотим найти s_λ для случая m переменных $(m<n)$, то нам следует только в найденном выражении для s положить

$$f_{m+1}=f_{m+2}=\ldots=f_n=0.$$

Формулы (4) и (5) применяются не только в том случае, когда $x_1,x_2,\ldots,x_n$ независимые переменные; они, например, позволяют вычислить сумму данных степеней корней данного уравнения.

Пример. По формулам (4) находим:

$$s_1 = f_1,$$
$$s_2 = f_2^2 - 2f_2,$$
$$s_3 = f_1^3 - 3f_1f_2 + 3f_3,$$
$$s_4 = f_1^4 - 4f_1^2f_2 + 4f_1f_3 + 2f_2^2 - 4f_4.$$

Обратно:

$$f_1 = s_1,$$
$$f_2 = \frac{1}{2}(s_1^2 - s_2),$$
$$f_3 = \frac{1}{6}(s_1^3 - 3s_1s_2 + 2s_3),$$
$$f_4 = \frac{1}{24}(s_1^4 - 6s_1^2s_2 + 8s_1s_3 + 3s_2^2 - 6s_4).$$

Упражнения

163) Дано уравнение $x^4 - 5x^2 + 2x + 1 = 0$; найти сумму третьих степеней его корней.

Отв. -6.

164) Дано уравнение $x^3 + x - 1 = 0$; найти сумму пятых степеней его корней.

Отв. -5.

165) Найти уравнение третьей степени, для которого сумма корней равна единице, сумма квадратов корней равна единице и сумма кубов корней равна единице.

Отв. $x^3 - x^2 = 0$.

166) Найти уравнение второй степени, для которого сумма корней равна 4, а сумма квадратов корней равна 5.

Отв. $2x^2 - 8x + 11$.

§ 135. Формулы Варинга (Waring). Формулы Ньютона принадлежат к так называемым *рекурентным формулам* или *формулам приведения*: они позволяют последовательно вычислять — сначала s_1, затем s_2, затем s_3 и т. д. в зависимости от f_λ или сначала f_1, затем f_2, f_3 и т. д. в зависимости от s_λ. Но существуют формулы, выражающие непосредственно s_k — при любом k от функций f_λ, и, обратно, f_λ при любом k — от функций s_λ; это — так называемые *формулы Варинга*, которые мы сейчас и выведем. Для этого воспользуемся известным бесконечным рядом для функции $\ln(1+z)$ (где ln означает натуральный логарифм) [61]:

$$\ln(1+z) = z - \frac{z^2}{2} + \frac{z^3}{3} - \frac{z^4}{4} + \ldots; \tag{6}$$

этот ряд сходится абсолютно при $|z| < 1$.

Пусть $x_1, x_2, \ldots, x_n$ — наши переменные, а x — новое переменное, причем мы берем значения x большими по абсолютной величине, чем значения $x_1, x_2, \ldots, x_n$, т. е. $|x| > |x_1|$, $|x| > |x_2|$, $\ldots$, $|x| > |x_n|$.

[61] Формула (6) для вещественных z выводится в любом учебнике анализа бесконечно малых, а для комплексного z — в любом учебнике теории функций комплексного переменного.

При $z = \dfrac{x_k}{x}$ получаем из (6):

$$\ln\left(1+\frac{x_k}{x}\right) = \frac{x_k}{x} - \frac{1}{2}\,\frac{x_k^2}{x^2} + \frac{1}{3}\,\frac{x_k^3}{x^3} = -\sum_{\lambda}^{\infty} \frac{(-1)^\lambda}{\lambda}\,\frac{x_k^\lambda}{x^\lambda}; \tag{7}$$

положим здесь $k = 1, 2, \ldots, n$ и, написав n получаемых из (7) таким образом равенств, сложим их почленно [иначе, просуммируем обе части (7) по k] [62], в левой части мы получим сумму логарифмов, т. е. логарифм произведения; в правой же части найдем суммы:

$$\frac{(-1)^\lambda}{\lambda}\,\frac{x_1^\lambda}{x^\lambda} + \frac{(-1)^\lambda}{\lambda}\,\frac{x_2^\lambda}{x^\lambda} + \ldots + \frac{(-1)^\lambda}{\lambda}\frac{x_n^\lambda}{x^\lambda} = \frac{(-1)^\lambda}{\lambda}\,\frac{s_\lambda}{x^\lambda};$$

итак, получим:

$$\ln\left\{\left(1+\frac{x_1}{x}\right)\left(1+\frac{x_2}{x}\right)\cdots\left(1+\frac{x_n}{x}\right)\right\} = -\sum_{\lambda=1}^{\infty}\frac{(-1)^\lambda}{\lambda}\,\frac{s_\lambda}{x^\lambda}. \tag{8}$$

С другой стороны, перемножение дает:

$$\left(1+\frac{x_1}{x}\right)\left(1+\frac{x_2}{x}\right)\cdots\left(1+\frac{x_n}{x}\right) = 1 + \frac{f_1}{x}\frac{f_2}{x^2} + \ldots + \frac{f_n}{x^n} = 1 + y,$$

где

$$y = \frac{f_1}{x} + \frac{f_2}{x^2} + \ldots + \frac{f_n}{x^n}.$$

По (6) имеем:

$$\ln(1+y) = -\sum_{\lambda=1}^{\infty}\frac{(-1)^\lambda \cdot y^\lambda}{\lambda}. \tag{6a}$$

Мы должны вычислить y^λ при любом λ; здесь мы воспользуемся формулой для степени полинома (алгебраической суммы), являющейся обобщением элементарной формулы бинома Ньютона и легко доказываемой на основании этой последней методом полной индукции:

$$(z_1 + z_2 + \ldots + z_n)^\lambda = \sum \frac{\lambda!}{\mu_1!\mu_2!\cdots\mu_n!}\, z_1^{\mu_1} z_2^{\mu_2}\cdots z_n^{\mu_n}, \tag{9}$$

где сумма берется по всем целым положительным или равным нулю значениям $\mu_1, \mu_2, \ldots, \mu_n$, при условии:

$$\mu_1 + \mu_2 + \ldots + \mu_n = \lambda.$$

Из (9) имеем $\left(\text{при } z_1 = \dfrac{f_1}{x},\ z_2 = \dfrac{f_2}{x^2},\ \ldots,\ z_n = \dfrac{f_n}{x^n}\right)$:

$$y^\lambda = \sum \frac{\lambda!}{\mu_1!\mu_2!\cdots\mu_n!} f_1^{\mu_1} f_2^{\mu_2!}\cdots f_n^{\mu_n}\, x^{-(\mu_1+2\mu_2+\ldots+n\mu_n)},$$

[62] В теории бесконечных рядов доказывается, что сходящиеся бесконечные ряды можно почленно складывать друг с другом.

где опять ставится условие: $\mu_1 + \mu_2 + \ldots + \mu_n = \lambda$.

Далее, имеем:

$$\frac{(-1)^\lambda y^\lambda}{\lambda} = \sum \frac{(-1)^\lambda (\lambda-1)!}{\mu_1!\mu_2!\cdots\mu_n!} f_1^{\mu_1} f_1^{\mu_1} f_2^{\mu_2} \cdots f_n^{\mu_n} x^{-(\mu_1+2\mu_2+\ldots+n\mu_n)}$$

или

$$\frac{(-1)^\lambda y^\lambda}{\lambda} = \sum \frac{(-1)^\lambda (\lambda-1)!}{\mu_1!\mu_2!\cdots\mu_n!} f_1^{\mu_1} f_2^{\mu_2} \cdots f_n^{\mu_n} x^{-(\mu_1+2\mu_2+\ldots+n\mu_n)}$$

при условии

$$\mu_1 + \mu_2 + \ldots + \mu_n = \lambda.$$

Подставляя теперь для $\lambda = 1, 2, 3, \ldots$ эти выражения в (6a), принимая во внимание, что левые, а следовательно, и правые части в (6a) и (8) одинаковы, сравниваем коэфициенты при x^λ в правых частях (8) и (6a) [63]:

$$\frac{(-1)^\lambda s_\lambda}{\lambda} = \sum \frac{(-1)^{\mu_1+\mu_2\ldots+\mu_n}(\mu_1+\mu_2+\ldots+\mu_n-1)!}{\mu_1!\mu_2!\cdots\mu_n!} f_1^{\mu_1} f_2^{\mu_2} \cdots f_n^{\mu_n} \qquad (10)$$

при условии $\mu_1 + 2\mu_2 + \ldots + n\mu_n = \lambda$; что касается условия $\mu_1 + \mu_2 + \ldots + \mu_n = \lambda$, то в (10) оно не имеет места, ибо в (6a) λ может равняться любому натуральному числу, а различные слагаемые правой части (10) могут соответствовать различным значениям λ. Число слагаемых правой части (10) конечно, ибо как λ, так и все μ_μ — целые положительные (или равные нулю) числа, и, следовательно, разложение λ в сумму $\mu_1 + 2\mu_2 + \ldots + n\mu_n$ возможно только конечным числом способов.

Формула (10) и есть первая *формула Варинга*. Заметим, что условие $\mu_1 + 2\mu_2 + \ldots + n\mu_n = \lambda$ можно заменить таким

$$\mu_1 + 2\mu_2 + \ldots + \lambda\mu_\lambda = \lambda,$$

ибо при $\lambda < n$ имеем $(\lambda+1)\mu_{\lambda+1} + \ldots n\mu_n = 0$, а при $\lambda > n$ будет $(n+1)\mu_{n+1} + \ldots + \lambda\mu_\lambda = 0$, так как $f_{n+1} = f_{n+2} = \ldots = 0$. Заметим еще, что

$$(-1)^\lambda = (-1)^{\mu_1+2\mu_2+\ldots+\lambda\mu_\lambda} = (-1)^{\mu_1+\mu_3+\mu_5+\ldots},$$

ибо четные слагаемые в показателе при -1 можно отбросить. Следовательно, разделив обе части (10) на $(-1)^\lambda$ и помножив на λ, получим:

$$s_\lambda = \sum \frac{(-1)^{\mu_2+\mu_4++\mu_6+\ldots}(\mu_1+\mu_2++\mu_n-1)!}{\mu_1!\mu_2!\cdots\mu_n!} f_1^{\mu_1} f_2^{\mu_2} \cdots f_n^{\mu_n}. \qquad (10a)$$

Пример 1. При $\lambda = 2$ имеем: $\mu + 1 + 2m_2 = 2$; это условие дает два решения: $\mu_1 = 2$, $\mu_2 = 0$ и $\mu_1 = 0$, $\mu_2 = 1$; т. е. сумма в (10a) имеет два слагаемых. Итак:

$$s_2 = 2 \cdot \left(\frac{1}{2!} f_1^2 - \frac{1}{1!} f_2 \right) = f_1^2 - 2f_2.$$

[63] Здесь мы основываемся на теореме, доказываемой в теории функций, о том, что аналитическая функция только одним образом разложима в степенной ряд.

Пример 2. При $\lambda = 3$ имеем: $\mu_1 + 2\mu_2 + 3\mu_3 = 3$; это дает три решения: $\mu_1 = 3$, $\mu_2 = \mu_3 = 0$, $\mu_1 = \mu_2 = 1$, $\mu_3 = 0$, $\mu_1 = \mu_2 = 0$, $\mu_3 = 1$, и, следовательно, три слагаемых в (10a); имеем:

$$s_3 = 3\left(\frac{2!}{3!}f_1^3 - f_1 f_2 + f_3\right) = f_1^3 - 3f_1 f_2 + 3f_3.$$

Пример 3. При $\lambda = 4$ имеем: $\mu_1 + 2\mu_2 + 3\mu_3 + 4\mu_4 = 4$, что дает пять решений: $\mu_1 = 4$, $\mu_2 = \mu_3 = \mu_4 = 0$, $\mu_1 = 2$, $\mu_2 = 1$, $\mu_3 = \mu_4 = 0$, $\mu_1 = \mu_3 = 1$, $\mu_2 = \mu_4 = 0$, $\mu_2 = 2$, $\mu_1 = \mu_3 = 0$, $\mu_2 = 2$, $\mu_1 = \mu_3 = \mu_4 = 0$, $\mu_1 = \mu_2 = \mu_3 = 0$, $\mu_4 = 1$; следовательно:

$$s_4 = 4\left(\frac{3!}{4!}f_1^4 - \frac{2!}{2!}f_1^2 f_2 + f_1 f_3 + \frac{1}{2!}f_2^2 - f_4\right) = f_1^4 - 4f_1^2 f_2 + 4f_1 f_3 + 2f_2^2 - 4f_4.$$

§ 136. Выведем теперь зависимость функций f_λ от s_μ. Имеем, заменив в (8) x на $-x$:

$$\ln\left\{\left(1 - \frac{x_1}{x}\right)\left\{\left(1 - \frac{x_2}{x}\right)\cdots\left\{\left(1 - \frac{x_n}{x}\right)\right\}\right\} = -\sum_{k=1}^{\infty}\frac{s_k}{kx^k} = -\frac{s_1}{x} - \frac{s_2}{2x^2} - \frac{s_3}{3x^3} - \ldots;$$

отсюда, переходя от логарифмов к числам:

$$\left(1 - \frac{x_1}{x}\right)\left(1 - \frac{x_2}{x}\right)\cdots\left(1 - \frac{x_n}{x}\right) = e^{-\frac{s_1}{x}}e^{-\frac{s_2}{2x^2}}e^{-\frac{s_3}{3x^3}}\ldots; \tag{11}$$

но [64]

$$\left.\begin{aligned} e^{\frac{s_1}{x}} &= \sum_{\lambda=0}^{\infty}(-1)^\lambda\frac{s_1^\lambda}{\lambda! x^\lambda}, \\ e^{\frac{s_2}{2x^2}} &= \sum_{\lambda=0}^{\infty}(-1)^\lambda\frac{s_2^\lambda}{\lambda! 2^\lambda}x^{-2\lambda}, \\ e^{\frac{s_3}{3x^3}} &= \sum_{\lambda=0}^{\infty}(-1)^\lambda\frac{s_3^\lambda}{\lambda! 3^\lambda}x^{-3\lambda}, \\ &\cdots\cdots\cdots\cdots\cdots\cdots \end{aligned}\right\}$$

Перемножаем теперь почленно эти ряды и подставляем в правую часть (11) [65], в

[64] Мы применяем известный ряд для показательной функции, выводимый в диференциальном исчислении:

$$e^z = 1 + z + \frac{z^2}{2!} + \frac{z^3}{3!} + \ldots = \sum_{\lambda=0}^{\infty}\frac{z^\lambda}{\lambda!}.$$

[65] Мы имеем право перемножать почленно абсолютно сходящиеся ряды (ряд для показательной функции — абсолютно сходящийся); что касается того, что тут бесконечное произведение, то оно определяется как предел произведения первых его m сомножителей, при $m \to \infty$; можно доказать, что этот предел существует; но при выводе формулы (15) мы пользуемся только конечным числом сомножителей этого бесконечного произведения.

левой части (11) производим перемножение; получаем:

$$1 - f_1 x^{-1} + f_2 x^{-2} - \ldots + (-1)^k f_k x^{-k} + \ldots + (-1)^n f_n x^{-n} = \\ = \sum \frac{(-1)^{\lambda_1+\lambda_2+\lambda_3+\ldots} s_1^{\lambda_1} s_2^{\lambda_2} s_3^{\lambda_3} \cdots x^{-(\lambda_1+2\lambda_2+3\lambda_3+\ldots)}}{1^{\lambda_1} \cdot 2^{\lambda_2} \cdot 3^{\lambda_3} \cdots \ \lambda_1!\lambda_2!\lambda_3! \cdots}. \tag{13}$$

Слагаемые правой части в (13) мы располагаем по степеням x, так что, полагая $\lambda_1 + 2\lambda_2 + 3\lambda_3 + \ldots = k$, мы берем последовательно $k = 0, 1, 2, 3, \ldots$ и для каждого k подбираем $\lambda_1, \lambda_2, \lambda_3, \ldots$, так, чтобы выполнялось условие $\lambda_1 + 2\lambda_2 + 3\lambda_3 + \ldots = k$; тут в левой части — бесконечная сумма, но очевидно, что, начиная с $(k+1)$-го слагаемого, все дальнейшие равны нулю (ибо $\lambda_1, \lambda_2, \lambda_3, \ldots$ целые числа ≥ 0); таким образом для данного k мы имеем условие:

$$\lambda_1 + 2\lambda_2 + 3\lambda_3 + \ldots = k. \tag{14}$$

Это условие для данного k дает конечное число систем решений $\lambda_1, \lambda_2, \ldots, \lambda_k$. Таким образом, вычисляя слагаемые в правой части (13), соответствующие одному и тому же данному k, мы используем для этого только конечное число (именно k) рядов (12), ибо непременно $\lambda_{k+1} = \lambda_{k+2} = \ldots = 0$, что соответствует тому, что в $(k+1)$-м, $(k+2)$-м и т. д. рядах (12) мы берем сомножителями только первые члены, равные единице.

Сравнивая теперь в тождестве (13) коэфициенты при x^{-k} в обеих частях, получим:

$$(-1)^k f_k = \sum \frac{(-1)^{\lambda_1+\lambda_2+\ldots+\lambda_k} s_1^{\lambda_1} s_2^{\lambda_2} \cdots s_k^{\lambda_k}}{1^{\lambda_1} \cdot 2^{\lambda_2} \cdots k^{\lambda_k} \lambda_1!\lambda_2! \cdots \lambda_k!} \tag{15}$$

при условии (14). Это и есть *вторая формула Варинга*.

Пример 1. $k = 2$; условие $\lambda_1 + 2\lambda_2 = 2$ дает два решения: $\lambda_1 = 2$, $\lambda_2 = 0$, $\lambda_1 = 0$, $\lambda_2 = 1$; следовательно, сумма в (15) имеет два слагаемых:

$$f_2 = \frac{s_1^2}{2!} - \frac{s_2}{2!} = \frac{1}{2}(s_1^2 - s_2).$$

Пример 2. $k = 3$; условие $\lambda_1 + 2\lambda_2 + 3\lambda_3 = 3$ дает три решения:

$$\lambda_1 = 3,\ \lambda_2 = \lambda_3 = 0, \qquad \lambda_1 = \lambda_2 = 1,\ \lambda_3 = 0, \qquad \lambda_1 = \lambda_2 = 0,\ \lambda_3 = 1;$$

получаем из (15):

$$-f_3 = -\frac{s_1^3}{3!} + \frac{s_1 s_2}{2} - \frac{s_3}{3} = \frac{1}{3!}(s_1^3 - 3s_1 s_2 + 2s_3).$$

Упражнения

167) По формуле (10) найти s_5, s_6.

Отв. $s_5 = f_1^5 - 5f_1^3 f_2 + 5f_1^2 f_3 - 5f_1 f_4 - 5f_2 f_3 + 5f_5$, $s_6 = f_1^6 - 6f_1^4 f_2 + 6f_1^3 f_3 + 9f_1^2 f_2^2 - 6f_1^2 f_4 - 12f_1 f_2 f_3 + 6f_1 f_5 - 2f_2^3 + 6f_2 f_4 + 3f_3^2 - 6f_6$.

168) По формуле (15) найти f_5.

Отв. $f_5 = \frac{1}{5!}(s_1^5 - 10s_1^3 s_2 + 20s_1^2 s_3 + 15s_1 s_2^2 - 30s_1 s_4 - 20s_2 s_3 + 24s_5)$.

§ 137. Некоторые приложения. В формуле (10a) положим $n = 2$; тогда

$$s_\lambda = \lambda \sum \frac{(-1)^{\mu_2}(\mu_1 + \mu_2 - 1)!}{\mu_1!\mu_2!} f_1^{\mu_1} f_2^{\mu_2} \tag{16}$$

при условии $\mu_1 + 2\mu_2 = \lambda$. Пусть $\mu_2 = \mu$; тогда $\mu_1 = \lambda - 2\mu$?; $\mu \geq 0$ и $\mu \leq \frac{\lambda}{2}$, т. е. μ принимает целые значения от нуля до $\frac{\lambda}{2}$ при λ четном или до $\frac{\lambda - 1}{2}$ при λ нечетном, т. е. вообще до $\left[\frac{\lambda}{2}\right]$ включительно. И (16) дает:

$$s_\lambda = \lambda \sum \frac{(-1)^{\mu}(\lambda - \mu - 1)!}{\mu!(\lambda - 2\mu)!} f_1^{\lambda - 2\mu} f_2^{\mu}. \tag{16a}$$

Пусть наши переменные будут: $x_1 = x$, $x_2 = \frac{1}{x}$; тогда $f_1 = x + \frac{1}{x}$, $f_2 = 1$. Заменим λ через n; тогда (16a) даст:

$$s_n = x^n + \frac{1}{x^n} = n \sum_{\mu=0}^{\left[\frac{n}{2}\right]} \frac{(-1)^{\mu}(\lambda - \mu - 1)!}{\mu!(\lambda - 2\mu)!} \left(x + \frac{1}{x}\right)^{n-2\mu}. \tag{17}$$

Диференцируем обе части (17) по x:

$$nx^{n-1} - \frac{n}{x^{n+1}} = n \sum \frac{(-1)^{\mu}(\lambda - \mu - 1)!}{\mu!(\lambda - 2\mu)!} (n - 2\mu) \left(x + \frac{1}{x}\right)^{n-2\mu-1} \left(1 - \frac{1}{x^2}\right)$$
$$\left(\mu = 0, 1, 2, \ldots, \frac{n-1}{2} \quad \text{или} \quad \frac{n}{2} - 1\right)^{66}$$

деля обе части на $1 - \frac{1}{x^2}$ и принимая во внимание, что $1 - \frac{1}{x^2} = \frac{1}{x}\left(x - \frac{1}{x}\right)$ и $\frac{(n-\mu-1)!}{\mu!(n-2\mu)!}(n - 2\mu) = \frac{(n-\mu-1)!}{\mu!(n-2\mu-1)!} = \binom{n-\mu-1}{\mu}$, получим

$$\frac{x^n - x^{-n}}{x - x^{-1}} = \sum (-1)^{\mu} \binom{n-\mu-1}{\mu} \left(x + \frac{1}{x}\right)^{n-2\mu-1}$$
$$\left(\mu = 0, 1, 2, \ldots, \frac{n-1}{2} \quad \text{или} \quad \frac{n}{2} - 1\right). \tag{18}$$

В формулах (17), (18) положим $x = e^{i\varphi}$; тогда

$$\frac{1}{x} = e^{-i\varphi}, \quad x^{\pm n} = e^{\pm in\varphi}, \quad x + \frac{1}{x} = 2\cos\varphi,$$
$$x - \frac{1}{x} = 2i\sin\varphi, \quad x^n + \frac{1}{x^n} = 2\cos n\varphi, \quad x^n - \frac{1}{x^n} = 2i\sin n\varphi^{67}$$

и получаем:

$$2\cos n\varphi = n \sum_{\mu=0}^{\left[\frac{n}{2}\right]} \frac{(-1)^{\mu}(n - \mu - 1)!}{\mu!(n - 2\mu)!} (2cos\varphi)^{n-2\mu}, \tag{19}$$

$$\frac{\sin n\varphi}{\sin\varphi} = \sum (-1)^{\mu} \binom{n-\mu-1}{\mu} (2\cos\varphi)^{n-2\mu-1} \quad \left(\mu = 0, 1, 2, \ldots, \frac{n-1}{2} \text{ или } \frac{n}{2} - 1\right). \tag{20}$$

Эти формулы можно было бы вывести и из формулы Муавра (§ 12).

Упражнения

169) По формуле (19) найти $\cos 2\varphi$, $\cos 3\varphi$, $\cos 4\varphi$.
Отв. $2\cos^2\varphi - 1$, $4\cos^3\varphi - 3\cos\varphi$, $8\cos^4\varphi - 8\cos^2\varphi + 1$.
170) По формуле (20) найти $\sin 3\varphi$, $\sin 4\varphi$.
Отв. $(4\cos^2\varphi - 1)\sin\varphi$, $(8\cos^3\varphi - 4\cos\varphi)\sin\varphi$.

§ 138. Доказательство Жирара (Girard) основной теоремы. Так как степенные суммы представляются по формулам Ньютона как целые рациональные функции от элементарных симметрических функций, то нам достаточно доказать, что всякая целая рациональная симметрическая функция представляется как целая рациональная функция от степенных сумм. Это мы и докажем.

Пусть в данную симметрическую функцию входит член:

$$Ax_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n};$$

тогда туда входят и все члены, получающиеся из этого путем всевозможных перестановок в этом члене $x_1, x_2, \ldots, x_n$. Сумму всех таких членов (взятых по одному разу) обозначим через

$$A \cdot S(x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n});$$

$S(x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n})$ есть тоже симметрическая функция — при этом простейшая симметрическая функция, содержащая член $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$, она вполне определяется этим своим членом. Такая функция называется *моногенной* (или *однотипной*); она однородна.

Очевидно, что всякая симметрическая функция представляется как сумма моногенных; поэтому достаточно доказать основную теорему для моногенных функций. Заметим, что некоторые из показателей $\alpha_1, \alpha_2, \ldots, \alpha_n$, могут быть равны нулю; мы их не будем писать, т. е. будем ставить например, $S(x_1^{\alpha_1} x_2^{\alpha_2})$ вместо $S(x_1^{\alpha_1} x_2^{\alpha_2} x_3^0 \cdots x_n^0)$ и т. п.

Начнем с простейших моногенных функций.

$$S(x_1^{\alpha}) = s_{\alpha}, \qquad S(x_1^{\alpha} x_2^{\beta}) = s_{\alpha} s_{\beta} - s_{\alpha+\beta}$$

при $\alpha \neq \beta$, ибо очевидно, что в произведение $s_{\alpha} s_{\beta}$ входят все члены из $S(x_1^{\alpha} x_2^{\beta})$ и, кроме этого, члены $x_1^{\alpha+\beta}, x_2^{\alpha+\beta}, \ldots$, составляющие функцию $s_{\alpha+\beta}$. При $\alpha = \beta$ члены $x_{\varkappa}^{\alpha} x_{\lambda}^{\alpha}$ и $x_{\varkappa}^{\alpha} x_{\lambda}^{\alpha}$ одинаковы, т. е. в выражении $s_{\alpha}^2 - s_{2\alpha}$ каждый член из $S(x_1^{\alpha} x_2^{\alpha})$ встречается два раза, т. е.

$$S(x_1^{\alpha} x_2^{\alpha}) = \frac{1}{2}(s_{\alpha}^2 - s_{2\alpha}).$$

Подобным же образом найдем, при различных α, β, γ:

$$S(x_1^{\alpha} x_2^{\beta} x_3^{\gamma}) = S(x_1^{\alpha} x_2^{\beta}) s_{\gamma} - S(x_1^{\alpha+\gamma} - x_2^{\beta}) - S(x_1^{\alpha} x_2^{\beta+\gamma}),$$

или

$$S(x_1^\alpha x_2^\beta x_3^\gamma) = s_\alpha s_\beta s_\gamma - s_{\alpha+\beta}s_\gamma - s_{\alpha+\gamma}s_\beta - s_\alpha s_{\beta+\gamma} + 2s_{\alpha+\beta+\gamma}.$$

Если же α, β, γ не все различны, то подобно предыдущему выведем:

$$S(x_1^\alpha x_2^\beta x_3^\gamma) = \frac{1}{2}\,(s_\alpha^2 s_\gamma - s_{2\alpha}s_\gamma - 2s_\alpha s_{\alpha+\gamma} + 2s_{2\alpha+\gamma}),$$

$$S(x_1^\alpha x_2^\beta x_3^\gamma) = \frac{1}{6}\,(s_\alpha^3 - 3s_{2\alpha}s_\alpha + 2s_{3\alpha}).$$

Общий случай:

$$S(x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_k^{\alpha_k} x_{k+1}^{\alpha_{k+1}} = S(x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_k^{\alpha_k}) s_{\alpha_{k+1}} -$$
$$-S(x_1^{\alpha_1+\alpha_{k+1}} x_2^{\alpha_2} \cdots x_k^{\alpha_k}) - S(x_1^{\alpha_1} x_2^{\alpha_2+\alpha_{k+1}} \cdots x_k^{\alpha_k}) - \ldots - S(x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_k^{\alpha_k+\alpha_{k+1}}).$$

Если мы умеем выразить через степенные суммы моногенную функцию $S(x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_k^{\alpha_k})$, содержащую k сомножителей в каждом члене, то по выведенной формуле, сумеем выразить и функцию

$$S(x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_k^{\alpha_k} x_{k+1}^{\alpha_{k+1}}).$$

В случае, если из показателей $\alpha_1, \alpha_2, \ldots, \alpha_k, \alpha_{k+1}$, имеется p равных друг другу, затем q равных друг другу и т. д., то выражение функции $S(x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_k^{\alpha_k} x_{k+1}^{\alpha_{k+1}}$ через степенные суммы надо еще разделить на $p!q!\cdots$

Пример 1. $S(x_1^2 x_2) = s_1 s_2 - s_3 = f_1 f_2 - 3f_3$.

Пример 2. $S(x_1^3 x_2 x_3) = \frac{(}{s_1}^2 s_3 - s_2 s_3 - 2s_1 s_4 + 2s_5)$. Формулы для s_1, s_2, s_3, s_4 имеются в § 134; вычислим по формулам Ньютона и выражение для s_5 [68]:

$$s_5 = f_1^5 - 5f_1^3 f_2 + 5f_1^2 f_3 + 5f_1 f_2^2 - 5f_1 f_4 - 5f_2 f_3 + 5f_5;$$

подставляя и вычисляя, найдем: $S(x_1^3 x_2 x_3) = f_1^2 f_3 - 2f_2 f_3 - f_1 f_4 + 5f_5$.

Пример 3. $n = 3$, $F(x_1, x_2, x3) = (x_1 - x_2)^2 (x_1 - x_3)^2 (x_2 - x_3)^2$ (дискриминант кубического уравнения);

$$\begin{aligned} F(x_1, x_2, x3) &= S(x_1^4 x_2^2) + 2S(x_1^3 x_2^2 x_3) - \\ &- 2S(x_1^4 x_2 x_3) - 2S(x_1^3 x_2^3) - 6S(x_1^2 x_2^2 x_3^2) = \\ &= s_2 s_4 - s_6 + 2(s_1 s_2 s_3 - s_2 s_4 - s_1 s_5 - s_3^2 + 2s_6) - \\ &- (s_1^2 s_4 - s_2 s_4 - 2s_1 s_5 + 2s_6) - (s_3^2 - s_6) - (s_2^3 - 3s_2 s_4 + 2s_6) = \\ &= 2s_1 s_2 s_3 - 3s_3^2 - s_1^2 s_4 - s_2^3 + 3s_2 s_4; \end{aligned}$$

подставляя значения для s_1, s_2, s_3, s_4 (§ 134; в выражении для s_4 следует положить $f_4 = 0$), получим после упрощений:

$$F(x_1, x_2, x3) = f_1^2 f_2^2 - 4f_1^3 f_3 - 27f_3^2 - 4f_2^3 + 18f_1 f_2 f_3.$$

Из этих примеров видно, что практически таким путем представлять симметрическую функцию как ц. р. функцию от элементарных симметрических функций

[68] См. также упражнение 167) в § 136.

неудобно, ибо требует больших вычислений и представляет, можно сказать, окольный путь.

Упражнения

Представить как функции от $f_1, f_2, \ldots, f_n$, следующие функции:

171) $S(x_1^2 x_2 x_3)$.

Отв. $\frac{1}{2}(s_1^2 s_2 - s_2^2 - 2s_1 s_2 + 2s_4) = f_1 f_3 - 4f_3$.

172) $S(x_1^3 x_2)$.

Отв. $s_1 s_3 - s_4 = f_1^2 f_1 - f_1 f_3 - 2f_2^2 + 4f_4$.

173) Найти $S(x_1^4 x_2^2)$, где x_1, x_2, x_3 корни уравнения $x^3 - x + 2 = 0$.

Отв. -2.

174) Найти $S(x_1^2 x_2^2 x_3)$, где x_1, x_2, x_3, x_4, корни уравнения $x^4 + x^3 + x^2 + x + 1 = 0$.

Отв. $+2$.

§ 139. Доказательство Гаусса основной теоремы. Нам достаточно доказать основную теорему для однородных симметрических функций, ибо (§ 132) всякая симметрическая ц. р. функция представляется как сумма однородных функций, которые, очевидно, тоже симметрические.

Во всякой ц. р. функции от n переменных мы можем расположить члены следующим образом: из двух членов

$$Ax_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n} \quad \text{и} \quad Bx_1^{\beta_1} x_2^{\beta_2} \cdots x_n^{\beta_n}$$

мы считаем первый стоящим выше, чем второй, если 1) $\alpha_1 > \beta_1$ или 2) $\alpha_1 = \beta_1$, $\alpha_2 > \beta_2$ или 3) $\alpha_1 = \beta_1$, $\alpha_2 = \beta_2$, $\alpha_3 > \beta_3$ и т. д. По этому принципу располагаются слова в словарях; поэтому такое расположение называется *лексикографическим*.

Лемма 1. *Высший член произведения двух функций, расположенных лексикографически, равен произведению высших членов сомножителей.*

Доказательство. Пусть

$$Ax_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$$

высший, а

$$A' x_1^{\alpha'_1} x_2^{\alpha'_2} \cdots x_n^{\alpha'_n}$$

какой-нибудь член первого сомножителя; тогда или

$$\alpha_1 > \alpha'_1,$$

или

$$\alpha_1 = \alpha_1, \qquad \alpha_2 > \alpha'_2,$$

или

$$\alpha_1 = \alpha'_1, \qquad \alpha_2 = \alpha'_2, \qquad \alpha_3 > \alpha'_3,$$

и т.д.

Подобно же пусть

$$Bx_1^{\beta_1} x_2^{\beta_2} \cdots x_n^{\beta_n}$$

высший, а

$$B' x_1^{\beta'_1} x_2^{\beta'_2} \cdots x_n^{\beta'_n}$$

какой-нибудь член второго сомножителя; тогда или

$$\beta_1 > \beta'_1,$$

или

$$\beta_1 = \beta'_1, \qquad \beta_2 > \beta'_2,$$

и т. д. Докажем, что в произведении член

$$ABx_1^{\alpha_1+\beta_1}x_2^{\alpha_2+\beta_2}\cdots x_n^{\alpha_n+\beta_n}$$

выше, чем член

$$A'B'x_1^{\alpha'_1+\beta'_1}x_2^{\alpha'_2+\beta'_2}\cdots x_n^{\alpha'_n+\beta'_n}.$$

Именно

$$\alpha_1 \geq \alpha'_1, \qquad \beta_1 \geq \beta'_1,$$

т. е.

$$\alpha_1 + \beta_1 \geq \alpha'_1 + \beta'_1;$$

если

$$\alpha_1 + \beta_1 = \alpha'_1 + \beta'_1,$$

тогда

$$\alpha_1 = \alpha'_1, \qquad \beta_1 = \beta'_1;$$

но тогда

$$\alpha_2 \geq \alpha'_2, \qquad \beta_2 \geq \beta'_2,$$

т. е.

$$\alpha_2 + \beta_2 \geq \alpha'_2 + \beta'_2$$

и т. д.

Лемма 2. *Если*

$$Ax_1^{\alpha_1}x_2^{\alpha_2}\cdots x_n^{\alpha_n}$$

высший член симметрической функции, то

$$\alpha_1 \geq \alpha_2 \geq \alpha_3 \geq \ldots$$

Доказательство. Пусть $\alpha_2 > \alpha_1$; так как функция симметрическая, то в ней имеется член

$$Ax_1^{\alpha_1}x_2^{\alpha_2}x_3^{\alpha_3}\cdots x_n^{\alpha_n},$$

который при $\alpha_2 > \alpha_1$ выше, чем

$$Ax_1^{\alpha_1}x_2^{\alpha_2}x_3^{\alpha_3}\cdots x_n^{\alpha_n}.$$

Подобным же образом убедимся, что α_3 не больше, чем α_2 и т. д.

Пусть $F(x_1, x_2, \ldots, x_n)$ данная симметрическая функция, расположенная лексикографически, и

$$Ax_1^{\alpha_1}x_2^{\alpha_2}\cdots x_n^{\alpha_n} \quad —$$

ее высший член. Возьмем функцию

$$Af_1^{\alpha_1-\alpha_2}f_2^{\alpha_2-\alpha_3}\cdots f_n^{\alpha_n};$$

ее высший член по лемме 1 есть:

$$Ax_1^{\alpha_1-\alpha_2}(x_1^{\alpha_2-\alpha_3}x_2^{\alpha_2-\alpha_3})\cdots(x_1^{\alpha_n}x_2^{\alpha_n}\cdots x_n^{\alpha_n})$$

(ибо, очевидно, в f_1 высший член есть x_1, в f_2 высший член есть x_1x_2 и т. д.).

Следовательно, в разности

$$F(x_1,x_2,\ldots,x_n)-Af_1^{\alpha_1-\alpha_2}f_2^{\alpha_2-\alpha_3}\cdots f_n^{\alpha_n}=F_1(x_1,x_2,\ldots,x_n)$$

член $Ax_1^{\alpha_1}x_2^{\alpha_2}\cdots x_n^{\alpha_n}$ сократится, и высший член этой разности

$$Bx_1^{\beta_1}x_2^{\beta_2}\cdots x_n^{\beta_n}$$

будет ниже. Теперь отнимаем от F_1 функцию $Bf_1^{\beta_1-\beta_2}f_2^{\beta_2-\beta_3}\cdots f_n^{\beta_n}$, у которой высший член тот же, что и у F_1, и т. д.; в конце концов после такого отнятия получим нуль, ибо в однородной функции число членов, которые ниже данного члена, — конечно. Итак, получаем:

$$F(x_1,x_2,\ldots,x_n)=Af_1^{\alpha_1-\alpha_2}f_2^{\alpha_2-\alpha_3}\cdots f_n^{\alpha_n}+Bf_1^{\beta_1-\beta_2}f_2^{\beta_2-\beta_3}\cdots f_n^{\beta_n};$$

это и есть искомое представление функции F. Из самого хода его видно, что мы не вводим дробных коэфициентов: если в F все коэфициенты целые, то и после указанного представления они останутся целыми.

Докажем теперь, что это представление функции возможно только одним образом. Пусть возможны два представления: $F(x_1,x_2,\ldots,x_n)=G(f_1,f_2,\ldots,f_n)=G_1(f_1,f_2,\ldots,f_n)$; мы видели, что при независимых $x_1,x_2,\ldots,x_n$ и $f_1,f_2,\ldots,f_n$, независимы; далее, при всех значениях $f_1,f_2,\ldots,f_n$, функции G и G_1 равны, т. е. $G-G_1=0$. Итак, дело сводится к теореме: если при всех значениях независимых переменных $z_1,z_2,\ldots,z_n$ ц. р. функция $f(z_1,z_2,\ldots,z_n)=0$, то все ее коэфициенты должны быть равны нулю. В § 50 эта теорема была доказана для целых рациональных функций одного переменного; но ее легко распространить на случай нескольких переменных. Именно, пусть для функций $n-1$ переменных она верна; расположим $f(z_1,z_2,\ldots,z_n)$ по переменному z_n (§ 132); коэфициенты будут ц. р. функциями от $z_1,z_2,\ldots,z_{n-1}$. При любых данных значениях $z_1,z_2,\ldots,z_{n-1}$ и при всяком z_n $f=0$; следовательно (по § 50), все эти коэфициенты равны нулю; но ведь значения $z_1,z_2,\ldots,z_{n-1}$ — любые; следовательно, эти коэфициенты, которые суть ц. р. функции от $z_1,z_2,\ldots,z_{n-1}$ равны нулю при всяких значениях $z_1,z_2,\ldots,z_{n-1}$, т. е. по нашему условию они тождественно равны нулю, и теорема доказана. Итак, $G-G_1\equiv 0$, $G\equiv G_1$ и основная теорема доказана во всех частях.

Пример 1. Имеем $S(x_1^2x_2)$; здесь высший член — $x_1^2x_2$; берем произведение $f_1^{2-1}f_2^{1-0}f_3^0\cdots f_n^0=f_1f_2$ и находим: $S(x_1^2x_2)-f_1f_2$; но $f_1f_2=(x_1+x_2+\ldots+x_n)(x_1x_2+x_1x_3+\ldots)=S(x_1^2x_2)+3S(x_1x_2x_3)=S(x_1^2x_2)+3f_3$; у f_3 здесь имеется коэфициент 3, ибо каждый член встречается три раза: например, $x_1\cdot x2x_3+x_2\cdot x_1x_3+x_3\cdot x_1x_2$. Итак, $S(x_1^2x_2)-f_1f_2=-3f_3$; следовательно, $S(x_1^2x_2)=f_1f_2-3f_3$.

Но в таком виде применять этот способ довольно неудобно; гораздо проще применить способ неопределенных коэфициентов, заранее высчитав, какие члены

будут в функции G; это довольно легко, если известен высший член функции F; именно, тогда можно найти все члены, низшие, чем этот высший, а по ним — и соответственные члены для G. Неопределенные коэфициенты определятся, если давать переменным $x_1, x_2, \ldots, x_n$ частные значения.

Пример 2. $S(x_1^3 x_2 x_3)$; здесь высший член — $x_1^3 x_2 x_3$, выписываем все члены $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$ — ниже члена $x_1^3 x_2 x_3$ и с условием $\alpha_1 \geq \alpha_2 \geq \ldots \geq \alpha_n$. Получаем всего четыре комбинации показателей:

$$\begin{array}{llll}
1) & 3\ 1\ 1\ 0\ 0\ 0 & \text{соответственно} & f_1^{3-1} f_2^{1-1} f_3^{1-0} = f_1^2 f_3, \\
2) & 2\ 2\ 1\ 0\ 0\ 0 & \text{''} & f_1^{2-2} f_2^{2-1} f_3^{1-0} = f_2 f_3, \\
3) & 2\ 1\ 1\ 1\ 0\ 0 & \text{''} & f_1^{2-1} f_2^{1-1} f_3^{1-1} f_4^{1-0} = f_1 f_4, \\
4) & 1\ 1\ 1\ 1\ 1\ 0 & \text{''} & f_1^{1-1} f_2^{1-1} f_3^{1-1} f_3^{1-1} f_4^{1-1} f_5^{1-0} = f_5.
\end{array}$$

Итак, искомая функция G будет иметь четыре члена; коэфициент высшего члена, очевидно, равен единице. Следовательно:

$$S(x_1^3 x_2 x_3) = f_1^3 f_2 + A f_2 f_3 + B f_1 f_4 + C f_5.$$

Коэфициенты A, B, C найдем, давая $x_1, x_2, x_3, \ldots$ частные значения.

1) При $x_1 = x_2 = x_3 = 1$, $x_4 = \ldots = x_n = 0$: $S(x_1^3 x_2 x_3) = 3$, $f_1 = 3$, $f_2 = 3$, $f_3 = 1$, $f_4 = f_5 = 0$; следовательно, $3 = 9 + 3A$.

2) При $x_1 = x_2 = x_3 = x_4 = 1$, $x_5 = \ldots = x_n 0$: $S(x_1^3 x_2 x_3) = 12$, $f_1 = 4 f_2 = 6$, $f_3 = 4$, $f_4 = 1$, $f_5 = 0$; следовательно, $12 = 64 + 24A + 4B$.

3) При $x_1 x_2 = x_3 = x_4 = x_5 = 1$, $x_6 = \ldots = x_n = 0$: $S(x_1^3 x_2 x_3 = 30$, $f_1 = 5$, $f_2 = f_3 = 10$, $f_4 = 5$, $f_5 = 1$; следовательно, $30 = 250 + 100A + 25B + C$.

Итак, для определения A, B, C имеем:

$$1 = 3 + A, \qquad 3 = 16 + 6A + B, \qquad 30 = 250 + 100A + 25B + C.$$

Отсюда $A = -2$, $B = -1$, $C = 5$. Следовательно,

$$S(x_1^2 x_2 x^3) = f_1^2 f_3 - 2 f_2 f_3 - f_1 f_4 + 5 f_5.$$

Пример 3. Дискриминантом кубического уравнения называется выражение:

$$F(x_1 - x_2)^2 (x_1 - x_3)^2 (x_2 - x_3)^2.$$

Здесь высший член есть — $x_1^4 x_2^2$; имеем пять комбинаций показателей:

$$\begin{array}{llll}
1) & 4\ 2\ 0 & \text{соответственно} & f_1^2 f_2^2, \\
2) & 4\ 1\ 1 & \text{''} & f_1^3 f_3, \\
3) & 3\ 3\ 1 & \text{''} & f_2^2, \\
4) & 3\ 2\ 1 & \text{''} & f_1 f_2 f_3 \\
5) & 2\ 2\ 2 & \text{''} & f_3^1.
\end{array}$$

Высший коэфициент здесь равен единице. Итак:

$$= F(x_1, x_2, x_3) = f_1^2 f_2^2 + A f_1^3 f_3 + B f_2^2 + C f_1 + D f_3^2.$$

При $x_1 = x_2 = 1,\ x_3 = 0:$ $\quad F = 0,\ f_1 = 2,\ f_2 = 1,\ f_3 = 0;$

″ $x_1 = x_2 = x_3 = 1:$ $\quad F = 0,\ f_1 = 3,\ f_2 = 3,\ f_3 = 1;$

″ $x_1 = x_2 = 1,\ x_3 = -1:$ $\quad F = 0,\ f_1 = 1,\ f_2 = -1,\ f_3 = -1;$

″ $x_1 = 2,\ x_2 = x_3 = -1:$ $\quad F = 0,\ f_1 = 0,\ f_2 = -3,\ f_3 = -2;$

следовательно:

$$0 = 4 + B$$
$$0 = 81 + 27A + 27B + 9C + D,$$
$$0 = 1 - A - B + C + d,$$
$$0 = -27B + 4D.$$

Отсюда найдем:

$$A = -4, \qquad B = -4, \qquad C = 18, \qquad D = -27,$$

т. е.

$$F = f_1^2 f_2^2 - 4f_1^3 f_3 - 4f_2^2 + 18 f_1 f_2 f_3 - 27 f_3^2.$$

Упражнения

Выразить как функции от $f_1, f_2, \ldots, f_n$ следующие функции:

175) $S(x_1^3 x_2^3$

Отв. $f_2^3 - 3f_1 f_2 f_3 + 3f_3^4 - 8f_1 f_5 + 3f_6$.

176) $n = 4$, $(x_1x_2 + x_3x_4)(x_1x_3 + x_2x_4)(x_1c_4 + x_2x_3)$.

Отв. $f_1^2 f_4 + f_3^2$.

177) Выразить через $f_1, f_2, \ldots, f_n$, посредством способа Гаусса s_3, s_4, s_5.

178) x_1, x_2, x_3 — корни уравнения $x^3 - x - 2 = 0$; вычислить $S(x_1^4 x_2$.

Отв. 10.

179) $S(x_1^3 x_2^2 x_3)$.

Отв. $f_1 f_2 f_3 - 3f_3^2$.

§ 140. Доказательство Коши (Cauchy) основной теоремы. Пусть $f_1, f_2, \ldots, f_n$, элементарные симметрические функции от $x_1, x_2, \ldots, x_n$, тогда как $g_1, g_2, \ldots, g_{n-1}$ элементарные симметрические функции от $n-1$ переменных $x_1, x_2, \ldots, x_{n-1}$. Найдем зависимость между $f_\varkappa$ и g_λ.

Имеем:

$$\begin{aligned} f_1 &= g_1 + x_n, \\ f_2 &= g_2 + x_n g_1, \\ f_3 &= g_3 + x_n g_2, \\ &\ldots\ldots\ldots\ldots\ldots, \\ f_{n-1} &= g_{n-1} + x_n g_{n-2}, \\ f_n &= x_n g_{n-1}. \end{aligned} \tag{21}$$

Отсюда

$$\begin{aligned} g_1 &= f_1 - x_n, \\ g_2 &= f_2 - x_n f1 + x_n^2, \\ g_3 &= f_3 - x_n f_2 + x_n^2 f_1 - x_n^3, \qquad (22) \\ &\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots, \\ g_{n-1} &= f_{n-1} - x_n f_{n-2} + \dots + (-1)^{n-1} x^{n-1}. \end{aligned}$$

Докажем теперь основную теорему для случая двух переменных. Пусть $F(x_1, x_2)$ данная симметрическая функция; имеем $x_2 = f_1 - x_1$; следовательно $F(x_1, x_2) = F(x_1, f_1 - x_1) = \Phi(x_1) = A_0 x_1^m + A_1 x_1^{m-1} + \dots + A_m$; обозначим: $f(x) = x^2 - f_1 x + f_2$; очевидно, что $f(x_1) = 0$, $f(x_2) = 0$. Делим $\Phi(x)$ на $f(x)$; пусть $Q(x)$ — частное; остаток будет первой степени; обозначим его $A + Bx$; заметим, что A и B ц. р. функции от f_1, f_2. Итак, $\Phi(x) = f(x)Q(x) + A + Bx$; при $x = x_1$ $\Phi(x_1) = A + Bx_1$. Итак, $F(x_1, x_2) = A + Bx_1$; переставим x_1 и x_2; от этого не изменится ни $F(x_1, x_2)$, ни f_1, ни f_2, т. е. ни A, ни B, значит $ABx_1 = A + Bx_2$, т. е. $B = 0$; $F = A$, и теорема доказана.

Общий случай. Пусть $F(x_1, x_2, \dots, x_n)$ данная симметрическая функция; располагаем ее по степеням переменного x_n: $F(x_1, x_2, \dots, x_n) = F_0 x_n^{\mu-1} + F_1 x_n^{\mu-2} + \dots + F_\mu$; $F_0, F_1, \dots, F_\mu$ симметрические функции от $x_1, x_2, \dots, x_{n-1}$. Для $n = 2$ теорема доказана; пусть она верна для симметрических функций от $n-1$ переменных; тогда $F_0, F_1, \dots, F_\mu$ представляются как ц. р, функции от $g_1, g_2, \dots, g_{n-1}$; но $g_1, g_2, \dots, g_{n-1}$ мы можем по (22) выразить через $f_1, f_2, \dots, f_{n-1}$ и x_n; расположив полученную после этого функцию снова по степеням x_n, получим:

$$F = A_0 x_n^\nu + A_1 x^{\nu-1} + \dots + A_\nu,$$

где $A_0, A_1, \dots, A_\nu$ ц. р. функции от $f_1, f_2, \dots, f_{n-1}$. Обозначив эту функцию через $\Phi(x_n)$, делим $\Phi(x)$ на $f(x) = x^n - f_1 x^{n-1} + f_2 x^{n-2} - \dots + (-1)^n f_n$: $\Phi(x) = Q(x)f(x) + C_0 x^{n-1} + C_1 x^{n-2} + \dots + C_{n-1}$; $C_0, C_1, \dots, C_{n-1}$ — ц. р. функции от $f_1, f_2, \dots, f_n$. При $x = x_n$ $\Phi(x_n) = C_0 x_n^{n-1} + C_1 x_n^{n-2} + \dots + C_{n-1}$, ибо $f(x_n) = 0$. Итак $F(x_1, x_2, \dots, x_n) = C_0 x_n^{n-1} + C_1 x_n^{n-2} + \dots + C_{n-1}$, или $C_0 x_n^{n-1} + C_1 x_n^{n-2} + \dots + C_{n-1} - F = 0$.

От любой перестановки $x_1, x_2, \dots, x_n$ не изменяются ни C_0, ни C_1, …, ни C_{n-1}, ни F. Следовательно, имеем: уравнение $C_0 x_n^{n-1} + C_1 x_n^{n-2} + \dots + C_{n-1} - F = 0$ $(n-1)$-й степени имеет n различных корней: $x_1, x_2, \dots, x_n$, т. е. (по § 50) все коэфициенты равны нулю: $C_0 = 0$, $C_1 = 0$, …, $C_{n-2} = 0$, $C_{n-1} = F$, и теорема доказана.

Из хода доказательства видно, что в C_{n-1} как функции от $f_1, f_2, \dots, f_n$, все коэфициенты целые, раз они целые в функции F.

Пример. Пусть $n = 3$ и дана функция $S(x_1^2 x_2) = x_1^2 x_2 + x_2^2 x_1 + x_1^2 x_3 + x_3^2 x_1 + x_2^2 x_3 + x_3^2 x_2$. Имеем:

$$\begin{aligned} S(x_1^2 x_2) &= (x_1 + x_2)x_3^2 + (x_1^2 + x_2^2)x_3 + x_1 x_2 (x_1 + x_2) = \\ &= g_1 x_3^2 + (g_1^2 - 2g_2)x_3 + g_1 g_2; \end{aligned}$$

или, подставляя по (22) $f_\varkappa$ вместо $g_\varkappa$: $S(x_1^2 x_2) = -3x_3^3 + 3f_1 x_3^2 - 3f_2 x_3 + f_1 f_2$; деля это на $x_3^3 - f_1 x_3^2 + f_2 x_3 - f_3$, находим остаток: $f_1 f_2 - 3f_3$; итак, согласно общей теории:

$$S(x_1^2 x_2) = f_1 f_2 - 3f_3.$$

§ 141. Функции, зависящие от разностей переменных. Пусть данная ц. р. функция $F(x_1, x_2, \ldots, x_n)$ зависит только от разностей переменных; т. е. другими словами, от одновременного прибавления к x_1, к x_2, ..., к x_n одного и того же числа t функция F не изменяется; иными словами, функция F не зависит от t. Тогда ее полная производная по t равна нулю [69]; найдем эту производную:

$$\frac{dF}{dt} = \frac{\partial\partial}{\partial x_1} + \frac{\partial F}{\partial x_2} + \ldots + \frac{\partial F}{\partial x_n} = 0.$$

Обратно: пусть для функции F верно диференциальное уравнение:

$$\frac{\partial F}{\partial x_1} + \frac{\partial F}{\partial x_2} + \ldots + \frac{\partial F}{\partial x_n} = 0. \tag{23}$$

Заменив $x_1, x_2, \ldots, x_n$ через $x_1+t, x_2+t, \ldots, x_n+t$, мы по (23) заключаем, что F не зависит от t, т. е. F зависит только от разностей переменных $x_1, x_2, \ldots, x_n$. Итак:

Теорема. *Необходимое и достаточное условие для того, чтобы функция $F(x_1, x_2, \ldots, x_n)$ зависела только от разностей переменных, таково: она должна удовлетворять диференциальному уравнению* (23).

Пусть теперь $F(x_1, x_2, \ldots, x_n)$ — симметрическая функция, и пусть $F(x_1, x_2, \ldots, x_n) = G(f_1, f_2, \ldots, f_n)$, где G ц. р. функция от $f_1, f_2, \ldots, f_n$. Тогда

$$\sum_{\lambda=1}^{n} \frac{\partial F}{\partial x_\lambda} = \sum_{\varkappa=1}^{n} \left(\frac{\partial G}{\partial f_\varkappa} \sum_{\lambda=1}^{n} \frac{\partial f_\varkappa}{\partial x_\lambda} \right) = \sum_{\varkappa=1}^{n} (n - \varkappa + 1) f_{\varkappa-1} \frac{\partial G}{\partial f_\varkappa}.$$

В самом деле, обозначим через $f_\varkappa^{(\lambda)}$ $\varkappa$-ю элементарную симметричную функцию от $x_1, x_2, \ldots, x_{\lambda-1}, x_{\lambda+1}, \ldots, x_n$; тогда

$$\frac{\partial f_\varkappa}{\partial x_\lambda} = f_{\varkappa-1}^{(\lambda)}, \qquad \sum_{\lambda=1}^{n} \frac{\partial f_\varkappa}{\partial x_\lambda} = f_{\varkappa-1}^{(1)} + f_{\varkappa-1}^{(2)} + \ldots + f_{\varkappa-1}^{(n)};$$

каждое произведение $x_{\alpha_1} x_{\alpha_2} \cdots x_{\alpha_{\varkappa-1}}$ (где $\alpha_1, \alpha_2 \ldots, \alpha_{\varkappa-1}$ некоторые $\varkappa - 1$ из чисел $1, 2, \ldots, n$) здесь встречается $n - \varkappa + 1$ раз, ибо это произведение не встречается в $f_{\varkappa-1}^{(\alpha_1)}, f_{\varkappa-1}^{(\alpha_2)}, \ldots, f_{\varkappa-1}^{(\alpha_{\varkappa-1})}$. Итак:

$$f_{\varkappa-1}^{(1} + f_{\varkappa-1}^{(2)} + \ldots + f_{\varkappa-1}^{(n)} = (n - \varkappa + 10 f_{\varkappa-1}.$$

При $\varkappa = 1$ имеем:

$$\frac{\partial f_1}{\partial x_\lambda} = 1, \qquad \sum_{\lambda=1}^{n} \frac{\partial f_1}{\partial x_\lambda} = n.$$

Если $F(x_1, x_2, \ldots, x_n)$ зависит только от разностей переменных, то по (23) получим:

$$\sum_{\varkappa=1}^{n} (n - \varkappa + 1) f_{\varkappa-1} \frac{\partial G}{\partial f_\varkappa} = 0,$$

[69] Эта теорема, равно как и последующие формулы, применяемые в этом параграфе, взята из диференциального исчисления; мы не имеем возможности их здесь выводить.

или

$$n\frac{\partial G}{\partial f_1}+(n-1)f_1\frac{\partial G}{\partial f_2}+(n-2)f_2\frac{\partial G}{\partial f_3}+\ldots+f_{n-1}\frac{\partial G}{\partial f_n}=0. \qquad (24)$$

Итак:

Теорема. *Если, симметрическая функция $F(x_1,x_2,\ldots,x_n)$ зависит только от разностей переменных и $G(f_1,f_2,\ldots,f_n)$ — ее представление через $f_1,f_2,\ldots,f_n$, то G удовлетворяет уравнению* (24). *Обратно, если G удовлетворяет уравнению* (24), *то $F(x_1,x_2,\ldots,x_n)$ зависит только от разностей переменных.*

Этой теоремой удобно пользоваться при вычислении неопределенных коэфициентов в G, если находить G по способу Гаусса (§ 139); именно, найдя (24), мы можем приравнять нулю все коэфициенты в (24) и получим ряд линейных уравнений для определения наших неопределенных коэфициентов.

Пример. $F(x_1,x_2,x_3)=(x_1-x_2)^2(x_2-x_3)^2(x_3-x_10^2$; имеем (пример 3, в § 139): $G=f_1^2f_2^2+Af_1^3f_3+Bf_2^3+Cf_1f_2f_3+Df+3^2$.

Уравнение (24) здесь имеет вид:

$$3\frac{\partial G}{\partial f_1}+2f_1\frac{\partial G}{\partial f_2}+f_2\frac{\partial G}{\partial f_3}=0, \qquad \frac{\partial G}{\partial f_1}=2f_1f_2^2+3Af_1^2f_3+Cf_2f_3,$$
$$\frac{\partial G}{\partial f_2}=2f_1^2f_2+3Bf_2^2+Cf_1f_3, \qquad \frac{\partial G}{\partial f_3}=Af_1^3+Cf_1f_2+2Df_3;$$

подставляя, найдем:

$$6f_1f_2^2+9Af_1^2f_3+3Cf_2f_3+4f_1^3f_2+6Bf_1f_2^2+2Cf_1^2f_3+$$
$$+Af_1^3f_2+Cf_1f_2^2+2Df_2f_3=0;$$

отсюда $6+6B+C=0$, $9A+2C=0$, $3V+2D=0$, $4+A=0$; отсюда $A=-4$, $B=-4$, $C=18$, $D=-27$, как мы и нашли раньше.

Упражнения

Выразить через f_λ следующие функции:

180) $(x_1-x_2)^2(x_2-x_3)^2+(x_2-x_3)^2(x_3-x_1)^2+(x_3-x_1)^2(x_1-x_2)^2$.

Отв. $f_1^4-6f_1^2f_2+18f_2^2$.

181) $(x_1-x_20^2+(x_2-x_3)^2++(x_3-x_1)^2$.

Отв. $2f_1^2-6f_2$.

§ 142. Обобщения основной теоремы. Основная теорема теории симметрических функций легко обобщается и на дробные симметрические функции. Пусть $\dfrac{f(x_1,x_2,\ldots,x_n)}{g(x_1,x_2,\ldots,x_n)}$ — дробная симметрическая функция; f и g — ц. р. функции, не имеющие общих множителей (т. е. дробь несократима). От любой перестановки переменных $x_1,x_2,\ldots,x_n$ эта дробь, конечно, не перестанет быть несократимой; с другой стороны, она от этой перестановки не изменится; следовательно, от всякой такой перестановки f и g могут получить только некоторый постоянный множитель a. По теореме § 23 каждая перестановка может быть произведена путем нескольких (например λ) транспозиций; если от первой из этих транспозиций f и g приобретают множитель a_1 от второй — множитель a_2 и т. д. — от λ-й — множитель a_λ, то, очевидно, $a=a_1a_2\cdots a_\lambda$, т. е. нам достаточно найти множители

a только для транспозиций. Но произведя два раза одну и ту же транспозицию, мы совсем не изменим ни f, ни g; следовательно, должно быть $a_2 = 1$, $a = \pm 1$ [70]. Далее, можно убедиться, что достаточно определить множители a только для транспозиций, где одно определенное переменное, например x_1 переставляется с каждым из остальных. Действительно, для того чтобы переставить $x_\varkappa$ с x_λ, можно сначала x_1 переставить с $x_\varkappa$, затем x_1 с x_λ и опять x_1 с $x_\varkappa$; это мы запишем символически так:

$$(\varkappa, \lambda) = (1, \varkappa)(1, \lambda)(1, \varkappa).$$

Следовательно, нам нужно только определить множители a для транспозиций, которые символически выражаются так: $(1, 2), (1, 3), \ldots, (1, n)$.

Докажем, что или для всех этих транспозиций $a = +1$, или для всех $a = -1$. Пусть для $(1, \varkappa)$ $a = +1$, а для $(1, \lambda)$ $a = -1$; тогда для транспозиции $(\varkappa, \lambda)$ найдем, что $a = -1$; но с другой ведь стороны: $(\varkappa, \lambda) = (1, \lambda)(1, \varkappa)(1, \lambda)$, и мы найдем также, что для той же транспозиции $a = +1$; это противоречие, которое устраняется только тем, что для всех $(1, \varkappa)$ и $(1, \lambda)$ [а следовательно и $(\varkappa, \lambda)$] a имеет одно и то же значение: или для всех =! или для всех -1.

Если $a = +1$, то и для всех перестановок вообще $a = 1$ и f и g — симметрические функции. Если же для транспозиций $a = -1$, то для одних перестановок (четных, ср. § 24) $a = +1$, для других (нечетных) $a = -1$, т. е. четные перестановки не изменяют f и g, нечетные — меняют знак у f и g; такие функции f и g называются полусимметрическими (иначе *знакопеременными*, *альтернирующими*). Но мы докажем, что этого случая не может быть, если дробь — несократима. Именно:

Лемма. *Всякая ц. р. полусимметрическая функция $f(x_1, x_2, \ldots, x_n)$ имеет множителем произведение разностей:*

$$P(x_1, x_2, \ldots, x_n) = \prod_{\varkappa<\lambda}(x_\varkappa - x_\lambda) = (x_1 - x_2)(x_1 - x_3)\cdots(x_{n-1} - x_n),$$

и частное $f : P$ есть симметрическая функция.

Доказательство. Легко доказать эту лемму для $n = 2$: пусть $f(x_1, x_2)$ ц. р. функция и $f(x_2, x_1) = -f(x_1, x_2)$; следовательно, если f имеет член $Ax_1^\alpha x_2^\beta$ то она имеет и член $Ax_1^\beta x_2^\alpha$ и алгебраическая сумма их $A(x_1^\alpha x_2^\beta - x_1^\beta x_1^\alpha)$ делится на $(x_1 - x_2)$, т. е. и вся функция $f(x_1, x_2)$ делится на $x_1 - x_2$.

Пусть теперь $f(x_1, x_2, \ldots, x_n)$ ц. р. полусимметрическая функция от n переменных; ее можно рассматривать как полусимметрическую функцию от всяких двух переменных $x_\varkappa$, x_λ, т. е. она делится на $x_\varkappa - x_\lambda$ при всяких $\varkappa$ и λ (причем брать $\varkappa < \lambda$), т. е. она делится на

$$P(x_1, x_2, \ldots, x_n).$$

Но $P(x_1, x_2, \ldots, x_n)$ тоже полусимметрическая функция; следовательно, частное — симметрическая функция от $x_1, x_2, \ldots, x_n$.

[70] Если, например, при перестановке x_1 с x_2 функция f получит множитель f, то при новой перестановке x_1 с x_2 функция f еще раз получит тот же самый множитель a. Можно подумать, что переход от $f(x_1, x_2, \ldots)$ к $f(x_2, x_1, \ldots)$ не тот же, что переход от $f(x_2, x_1, \ldots)$ к $f(x_1, x_2, \ldots)$, являющийся обратным к первому. Но по существу тут оба раза переставляются первое и второе место, а обозначения переменных, занимающих эти места, роли не играют; ведь множитель a не зависит от них.

Итак, если несократимая дробь $\dfrac{f(x_1, x_2, \ldots, x_n)}{g(x_1, x_2, \ldots, x_n)}$ является симметрической функцией, то ее числитель и знаменатель тоже симметрические функции; применяя к ним основную теорему, мы найдем, что и для дробной рациональной симметрической функции эта теорема верна; такая функция представляется как дробная рациональная функция от элементарных симметрических функций $f_1, f_2, \ldots, f_n$ причем при этом над коэфициентами производятся только действия сложения, вычитания, умножения.

До сих пор мы предполагали, что $x_1, x_2, \ldots, x_n$ — независимые переменные, и симметрические функции от них были симметрическими функциями по виду, т. е. не меняли своего внешнего вида, как бы мы ни переставляли $x_1, x_2, \ldots, x_n$. Но в дальнейшем нам часто придется иметь дело с функциями от *корней данного уравнения*, т. е. там $x_1, x_2, \ldots, x_n$ уже не будут независимыми переменными, а могут быть даже вполне определенными числами. В этом случае функция от $x_1, x_2, \ldots, x_n$ может быть симметрической только *по значению*, т. е. принимать одно и то же значение, как бы ни переставляли числа $x_1, x_2, \ldots, x_n$. Например, при $n = 2$, если x_1, x_2 корни уравнения $x^2 - 2x + 3 = 0$, функция $x_1^2(x_1 + x_2) - 2(2x_1 - 5)$ будет симметрической *по значению*, которое равно 4, но не по виду; тогда как функция, симметрическая по виду, будет всегда симметрическая и по значению (какие бы значения мы ни придавали ее аргументам).

Основная теорема была доказана для функций, симметрических по виду. Но легко доказать, что она верна и для функций, симметрических по значению (как целых, так и дробных). Пусть $\varphi_1(x_1, x_2, \ldots, x_n)$ функция, симметрическая по значению ($x_1, x_2, \ldots, x_n$ не независимые переменные, а корни какого-то уравнения). Докажем, что функцию φ_1 можно заменить функцией, симметрической по виду. Пусть

$$\varphi_1(x_1, x_2, \ldots, x_n) = k;$$

будем переставлять $x_1, x_2, \ldots, x_n$ всеми возможными способами; получим от этих перестановок функции $\varphi_2, \varphi_3, \ldots, \varphi_{n!}$; их вид будет вообще разниться от φ_1 и друг от друга, но значение каждой из них равно k. Тогда

$$\Phi(x_1, x_2, \ldots, x_n) = \frac{1}{n!}\,(\varphi_1 + \varphi_2 + \varphi_3 + \ldots + \varphi_{n!})$$

есть симметрическая функция по виду, и значение ее тоже равно k; ею можно заменить функцию φ_1 и применив к ней основную теорему.

Пример 1. Рассмотренную уже функцию $x_1^2(x_1 + x_2) - 2(2x_1 - 5)$, симметрическую по значению, если x_1 и x_2 корни уравнения $x^2 - 2x - 3 = 0$, можно заменить следующей функцией, симметрической по виду:

$$F = \frac{1}{2}\,[x_1^2(x_1 + x_2) - 2(2x_1 - 5) + x_2^2(x_1 + x_2) - 2(2x_2 - 5)],$$

или, принимая во внимание, что $x_1 + x_2 = 2$:

$$F = x_1^2 + x_2^2 - 2(x_1 + x_2) + 10 = x_1^2 + x_2^2 + 6;$$

легко видеть, что значение F остается равным 4.

Пример 2. Функцию $\varphi = (x_1 - 1)x_2^3x_3^3$, симметрическую по значению, если x_1, x_2, x_3 корни уравнения $x^3 - x + 1 = 0$, можно заменить функцией, симметрической по виду:

$$F = \frac{1}{3}\left[(x_1 - 1)x_2^3x_3^3 + (x_2 - 1)x_3^3x_1^3 + (x_3 - 1)x_1^3x_2^3\right];$$

но ту же функцию можно заменить и такою:

$$F_1 = x_1^3x_2^3x_3^3,$$

ибо данное уравнение дает при $x = x_1$:

$$x_1 - 1 = x_1^3 =,$$

на основании чего и получаем из сразу F_1. Все три функции φ, F и F_1 имеют одно и то же численное значение -1. Заметим, что функции F и F_1 как функции от независимых переменных x_1, x_2, x_3, не сводятся одна к другой. Это показывает, что функцию, симметрическую по значению, можно заменить функцией, симметрической по виду, разными способами, и способ, изложенный выше, есть только один из способов, — не всегда самый простой.

§ 143. Рассмотрим теперь (целую или дробную) рациональную функцию, зависящую от нескольких рядов переменных: $x_1, x_2, \ldots, x_n$, $y_1, y_2, \ldots, y_m$, $z_1, z_2, \ldots, z_k$, $\ldots$, и симметрическую относительно каждого из этих рядов в отдельности:

$$u = F(x_1, x_2, \ldots, x_n,\ y_1, y_2, \ldots, y_m,\ z_1, z_2, \ldots, z_k).$$

Обозначим через $f_1, f_2, \ldots, f_n$ элементарные симметрические функции от x_1, x_2, $\ldots, x_n$ через $g_1, g_2, \ldots, g_m$ — от $y_1, \ldots, y_m$, через $h_1, h_2, \ldots, h_k$ — от $z_1, z_2, \ldots, z_k$ и т. д.

Рассматриваем F как функцию от $x_1, x_2, \ldots, x_n$ с коэфициентами, зависящими от $y_1, \ldots, y_m$, $z_1, \ldots, z_k$, $\ldots$ Эти коэфициенты — симметрические функции от $y_1, \ldots, y_m$, $z_1, \ldots, z_k$, $\ldots$ Представляем теперь F в зависимости от $f_1, f_2, \ldots, f_n$, получаем:

$$u = F_1(f_1, f_2, \ldots, f_n,\ y_1, \ldots, y_m,\ z_1, \ldots, z_k,\ \ldots).$$

Но при переходе от F к F_1 мы над коэфициентами функции F произвели только действия сложения, вычитания и умножения; новые коэфициенты (в F_1) останутся симметрическими функциями от $y_1, \ldots, y_m$, $z_1, \ldots, z_k$, $\ldots$

Теперь рассматриваем F_1 как функцию от $y_1, \ldots, y_m$, она симметрическая относительно $y_1, \ldots, y_m$, коэфициенты ее при этом — рациональные функции от $f_1, f_2, \ldots, f_n$, и симметрические функции от $z_1, \ldots, z_k$, $\ldots$ Представляем F_1 как функцию от $g_1, \ldots, g_m$ и т. д.; в конце концов получим:

$$u = G(f_1, f_2, \ldots, f_n,\ g_1, g_2, \ldots, g_m,\ h_1, h_2, \ldots, h_k,\ \ldots).$$

Итак:

Теорема. *Если целая (дробная) рациональная функция от нескольких рядов переменных — симметрическая относительно каждого ряда этих переменных,*

то ее можно представить, как целую (дробную) рациональную функцию от элементарных симметрических функций каждого из рядов наших переменных, причем при этом представлении над коэфициентами нашей функции совершаются лишь действия сложения, вычитания и умножения.

Следствие. Целая или дробная рациональная функция с рациональными коэфициентами (или с коэфициентами, принадлежащими данному телу P от корней уравнений с рациональными (или с принадлежащими телу P) коэфициентами имеет рациональное значение (или значение из тела P).

Пример.

$$\begin{aligned} F &= x_1^2y_1 + x_2^2y_1 + x_1^2y_2 + x_2^2y_2 + x_1^2y_3 + x_2^2y_3 = \\ &= (x_1^+x_2^2)(y_1 + y_2 + y_3) = (f_1^2 - 2f_2)g_1. \end{aligned}$$

§ 144. Уничтожение иррациональности в знаменателе. Пусть $\dfrac{\varphi(x)}{\psi(x)}$ рациональная функция с рациональными коэфициентами (φ и ψ — целые функции), и x_1 корень уравнения $f(x) = 0$ n-й степени; остальные корни этого уравнения: $x_2, x_3, \ldots, x_n$. Задача наша в том, чтобы функцию $\dfrac{\varphi(x_1)}{\psi(x_1)}$ заменить равной ей целой функцией от x_1 с рациональными коэфициентами. При этом мы предполагаем, что ни один из корней $x_1, x_2, \ldots, x_n$ не удовлетворяет уравнению $\psi(x) = 0$, т. е. функции $f(x)$ и $\psi(x)$ взаимно простые. Это всегда выполнено, если уравнение $f(x) = 0$ неприводимо (§ 110, следствия I и II), ибо $\psi(x_1) \neq 0$; теоретически мы всегда это можем предположить.

Способ 1. Умножаем числитель и знаменатель нашей дроби на $\psi(x_2)\psi(x_3)\cdots\psi(x_n)$:

$$\frac{\varphi(x)1)}{\psi(x_1)} = \frac{\varphi(x_1)\psi(x_2)\cdots\psi(x_n)}{\psi(x_1)\psi(x_2)\cdots\psi(x_n)}$$

теперь знаменатель у нас — симметрическая функция от $x_1, x_2, \ldots, x_n$, и значит выражается рационально через $f_1, f_2, \ldots, f_n$, т. е. через коэфициенты уравнения $f(x) = 0$; следовательно, равен рациональному числу a. В числителе же $\psi(x_2)\cdots\psi(x_n)$ есть рациональная функция от $g_1, g_2, \ldots, g_{n-1}$ (если $g_1, g_2, \ldots, g_{n-1}$ — элементарные симметрические функции от $x_2, \ldots, x_n$, т. е. выражается рационально через $f_1, f_2, \ldots, f_{n-1}$, и x_1 [§ 140 (22)]; значит весь числитель есть ц. р. функция от x_1 с рациональными коэфициентами, т. е. вся дробь есть ц. р. функция от x_1 с рациональными коэфициентами: $\dfrac{\varphi(x_1)}{\psi(x_1)} = \Phi(x_1)$; если степень $\Phi(x_1) \geq n$, то делим $\Phi(x)$ на $f(x)$: $\Phi(x) = f(x)Q(x) + R(x)$, где степень $R(x) \leq n^-1$; при $x = x_1$ $f(x_1) = 0$, т. е. $\Phi(x_1) = R(x_1)$ и значит $\dfrac{\varphi(x_1)}{\psi(x_1)} = R(x_1)$. Итак:

Теорема. *Если $\dfrac{\varphi(x)}{\psi(x)}$ — рациональная функция с рациональными коэфициентами, а x_1 — корень неприводимого уравнения $f(x) = 0$ n-й степени, и $\psi(x_1) \neq 0$, то $\dfrac{\varphi(x_1)}{\psi(x_1)}$ представляется как целая рациональная функция от x_1 с рациональными коэфициентами степени $\leq n - 1$. Это представление возможно только одним образом.*

Докажем вторую часть теоремы. Пусть имеем два различных представления:

$$c_0 + c_1x_1 + c_2x_1^2 + \ldots + c_{n-1}x_1^{n-1} = c'_0 + c'_1x_1 + c'_2x_1^2 + \ldots + c'_{n-1}x_1^{n-1};$$

отсюда

$$F(x_1) = (c_0 - c'_0) + (c_1 - c'_1)x_1 + (c_2 - c'_2)x_1^2 + \ldots + (c_{n-1} - c'_{n-1})x_1^{n-1} = 0,$$

т. е. x_1 есть корень уравнения $F(x) = 0$, степень которого $\leq n-1$: но x_1 корень неприводимого уравнения n-й степени; следовательно, по следствию 5 § 110, все коэфициенты в $F(x)$ равны нулю, т. е.

$$c_0 = c'_0, \quad c_1 = c'_1, \ \ldots, \ c_{n-1} = c'_{n-1}.$$

Способ 2. Так как $f(x)$ и $\psi(x)$ взаимно простые, то можно (по § 52) найти такие ц. р. функции $f_1(x)$ и $\psi_1(x)$, что будет: $f(x)f_1(x) + \psi(x)\psi_1(x) = 1$, причем $f_1(x)$ и $\psi_1(x)$ находятся рациональным путем, т. е. все их коэфициенты тоже рациональны. При $x = x_1$ получаем: $f(x_1) = 0$, следовательно, $\psi(x)\psi_1(x_1) = 1$;

$$\frac{1}{\psi(x_1)} = \psi_1(x_1), \qquad \frac{\varphi(x_1)}{\psi(x_1)} = \varphi(x_1)\psi(x_1);$$

если степень $\varphi(x)\phi(x)$, то ее можно понизить, как и в способе 1.

Пример. Дана дробь $\dfrac{1}{x_1 - 1}$, где x_1 — корень уравнения $x^3 - x + 1 = 0$.

Способ 1.

$$\frac{1}{x_1 - 1} = \frac{(x_2 - 1)(x_3 - 1)}{(x_1 - 1)(x_2 - 1)(x_3 - x_1)};$$

$(x_1 - 1)(x_2 - 1)(x_3 - x_1) = f_3 - f_2 + f_1 - 1 = -1 + 1 - 1 = -1$, ибо $f_1 = 0$, $f_2 = -1$, $f_3 = -1$; далее, $(x_2 - 1)(x_3 - 1) = g_2 - g_1 + 1 = f_2 - x_1f_1 + x_1^2 - f_1 + x_1 + 1 = -1 + x_1^2 + x_1 + 1 = x_1(x_1 + 1)$; итак:

$$\frac{1}{x_1 - 1} = -x_1(x_1 + 1).$$

Способ 2. Делим $x^3 - x + 1$ на $x - 1$:

$$\begin{array}{r|l} x^3 - x + 1 & x - 1 \\ \cline{2-2} x^3 - x^2 & x^2 + x \\ \hline x^2 - x & \\ x^2 - x & \\ \hline +1 & \end{array}$$

итак $x^4 - x + 1 = (x - 1)(x_2 + x) + 1$, $(x^3 - x + 1) - (x - 1)(x^2 + x) = 1$; при $x = x_1$

$$-x_1(x_1 - 1)(x_1^2 + x_1) = 1, \qquad \frac{1}{x_1 - 1} = -x_1(x_1 + 1).$$

Упражнения

Уничтожить иррациональность в знаменателях:

182) $\dfrac{x_1}{x_1-1}$, где x_1 — корень уравнения $x^4+x^2+1=0$.

Отв. $-\dfrac{1}{3}(x_1+1)(x_1^2+2)$.

183) $\dfrac{2x_1}{x_1+1}$, где x_1 — корень уравнения x^4+x-1.

Отв. $2x_1^2(x_1^2-x_1+1)$.

184) $\dfrac{2x_1+1}{x_1^2+2}$, где x_1 — корень уравнения $x^3+3x^2-2x-1=0$.

Отв. $-\dfrac{1}{81}(10x_1^2+53x_1+29)$.

185) $\dfrac{2\sqrt{5}-1}{\sqrt[3]{25}+4\sqrt[3]{5}+1}$.

Отв. $\dfrac{1}{22}(13-3\sqrt[3]{5}-\sqrt[3]{25})$.

§ 145. Резольвенты. § 145. Пусть $f(x)\equiv x^n-f_1x^{n-1}+f_2x^{n-2}-\ldots+(-1)^nf_n=0$ — данное уравнение с корнями $x_1,x_2,\ldots,x_n$. Пусть $v_1=\varphi(x_1,x_2,\ldots,x_n)$ — некоторая рациональная функция от корней с рациональными коэфициентами. Пусть при всевозможных перестановках $x_1,x_2,\ldots,x_n$ функция v_1 принимает' только m значений $v_1,v_2,\ldots,v_m$; очевидно, что $1\leq m\leq n!$; $m=n!$ мы имеем тогда, если при всякой перестановке корней $x_1,x_2,\ldots,x_n$ функция v_1 меняет свое значение; $m=1$, если функция v_1 симметрична относительно $x_1,x_2,\ldots,x_n$. Возьмем функцию от переменного v:

$$\begin{aligned}F(v) &= (v-v_1)(v-v_2)\cdots(v-v_m)=\\ &= v^m-F_1v^{m-1}+F_2v^{m-2}-\ldots+(-1)^mF_m.\end{aligned}$$

От перестановки $x_1,x_2,\ldots,x_n$ меняются местами и $v_1,v_2,\ldots,v_m$; но $F_1,F_2,\ldots,F_m$ от этого не изменяются, ибо они симметрические функции от $v_1,v_2,\ldots,v_m$. Итак, $F_1,F_2,\ldots,F_m$ суть также и симметрические функции от $x_1,x_2,\ldots,x_n$, т. е. выражаются рационально через $f_1,f_2,\ldots,f_n$; в частном случае, при $f_1,f_2,\ldots,f_n$, рациональных, и $F_1,F_2,\ldots,F_m$ — рациональные числа. Но уравнению $F(v)=0$ удовлетворяет корень $v=v_1$. Итак:

Теорема. *Всякая рациональная функция φ от корней $x_1,x_2,\ldots,x_n$ уравнения $f(x)=0$, имеющая m значений при всевозможных перестановках корней, удовлетворяет алгебраическому уравнению m-й степени с коэфициентами, рационально зависящими от коэфициентов уравнения $f(x)=0$.* (В частности при $m=1$ сама функция φ рационально зависит от козфициентов уравнения $f(x)=0$.)

Пример. $v_1=(x_1-x_2)^2$; функция не изменяется при всевозможных перестановках корней, при которых x_1 и x_2 переставляются только друг с другом; таких перестановок всего $2\cdot(n-2)!$. Если в данной перестановке x_1 переходит в $x_\varkappa$, x_2 — в x_λ, то v_1 перейдет в $v_\mu=(x_\varkappa-x_\lambda)^2$; таких перестановок, переводящих v_1 в v_μ всего тоже $2\cdot(n-2)!$, т. е., всего различных значений функции v_1 мы имеем $\dfrac{n!}{2(n-2)!}=\dfrac{n(n-1)}{2}$, и значит уравнение, которому удовлетворяет v_1, будет степени $\dfrac{n(n-1)}{2}$.

Упражнения

186) $n = 3$, $v_1 = x_1 + x_2$; найти уравнение для v_1.

Отв. $v^3 - 2f_1v^2 + (f_1^2 + f_2)v - (f_1f_2 - f_3) = 0 = 0$.

187) $n = 4$, $v_1 = x_1x_2 + x_3x_4$; найти уравнение для v_1.

Отв. $v^3 - f_2v^2 + (f_1f_3 + 4f_4)v - (f_1^2f_4 + f_3^2) = 0$.

188) Решить предыдущий пример, если x_1, x_2, x_3, x_4 корни уравнения $x_4 - x + 1$.

Отв. $v^3 - 4v - 1 = 0$.

Заметим, что уравнение для v_1 $F(v) = 0$ называется *резольвентой* (*разрешающим*) для уравнения $f(x) = 0$, ибо при подходящем выборе функции v_1 его решение облегчает решение данного уравнения $f(x) = 0$ [71]. Некоторые авторы называют резольвентой самую функцию v_1.

§ 146. Преобразование Чирнгаузена (Tschirnhausen). Пусть опять $f(x) = x^n - f_1x^{n-1} + f_2x^{n-2} - \ldots + (-1)^n f_n = 0$ данное уравнение с корнями $x_1, x_2, \ldots, x_n$, и пусть $v_1 =$ — данная рациональная функция от корня x_1 с рациональными коэфициентами. Для всевозможных перестановок корней эта функция имеет только n значений: v_1, $v_2 = \varphi(x_2)$, $\ldots$, $v_n = \varphi(x_n)$. Мы знаем (§ 144), что функцию φ всегда можно заменить целой рациональной функцией от x_1 степени $\leq n - 1$ с коэфициентами, рационально зависящими от $f_1, f_2, \ldots, f_n$. Нахождение уравнения для v_1 называется *преобразованием Чирнгаузена* данного уравнения. Мы укажем два способа этого преобразования.

Способ 1. Итак, пусть $v = a_0 + a_1x + a_2x^2 + \ldots + a_{n-1}x^{n-1}$; найдем v^2 и при помощи данного уравнения сделаем степень $v^2 \leq n - 1$ [т. е. делим v^2 на $f(x)$ и берем остаток]; получаем:

$$v^2 = b_0 + b_1x + b_2x^2 + \ldots + b_{n-1}x^{n-1}.$$

Подобным же образом найдем:

$$v^3 = c_0 + c_1x + c_2x^2 + \ldots + c_{n-1}x^{n-1},$$
$$\ldots$$
$$v^n = k_0 + k_1x + k_2x^2 + \ldots + k_{n-1}x^{n-1}.$$

Подставляя в эти равенства вместо x $x_1, x_2, \ldots, x_n$ и получая в левых частях $v_1, v_2, \ldots, v_n$, складываем получающиеся таким образом равенства:

$$S_1 = na_0 + a_1s_1 + a_2s_2 + \ldots + a_{n-1}s_{n-1},$$
$$S_2 = nb_0 + b_1s_1 + b_2s_2 + \ldots + b_{n-1}s_{n-1}$$
$$\ldots$$
$$S_n = nk_0 + k_1s_1 + k_2s_2 + \ldots + k_{n-1}s_{n-1}.$$

Здесь $s_1, s_2, \ldots$ степенные суммы для $x_1, x_2, \ldots, x_n$, а $S_1, S_2, \ldots$ — степенные суммы для $v_1, v_2, \ldots, v_n$. Найдя $S_1, S_2, \ldots, S_n$, вычисляем коэфициенты уравнения для $v_1, v_2, \ldots, v_n$:

$$v^n - P_1v^{n-1} + P_2v^{n-2} - \ldots + (-1)^n P_n = 0$$

[71] Ср. главу XII.

по формулам Ньютона (§ 134): $S_1 - P_1 = 0$, $S_2 - P_1S_1 + 2P_2 = 0$, ...

Большую роль в этой теории играет коэфициент P_2; он называется *безуниант* (по имени французского математика Bézout).

Пример. Дано уравнение $x^3-2x+3=0$; $v = 1-x+x^2$; находим $v^2 = 7-9x+5x^2$, $v^3 = 49-49x+31x^2$; далее, $S_1 = 3-s_1+s_2$, $S_2 = 21-9s_1+5s_2$, $S_3 = 147-49s_1+31s_2$; здесь $f_1 = 0$, $f_2 = -2$, $f_3 = -3$; $s_1 = 0$, $s_2 = f_1^2-2f_2 = 4$; следовательно, $S_1 = 7$, $S_2 = 41$, $S_3 = 271$. Далее, $P_1 = 7$, $P_2 = 4$, $P_3 = 4$, и уравнение для v: $v^3-7v^2+4v-4=0$.

Способ 2 Эрмита (Hermite). Умножаем v на x и вместо x^n подставляем $f_1x^{n-1}-f_2x^{n-2}+\ldots-(-1)f_n$; тогда vx представится как ц. р. функция от x степени $\leq n-1$. Подобно же находим $vx^2, \ldots, vx^{n-1}$; получаем (коэфициенты b_λ, c_λ, ..., k_λ имеют теперь уже не те значения, что в способе 1):

$$\begin{aligned} v &= a_0 + a_1x + a_2x^2 + \ldots + a_{n-1}x^{n-1}, \\ vx &= b_0 + b_1x + b_2x^2 + \ldots + b_{n-1}x^{n-1}, \\ vx^2 &= c_0 + c_1x + c_2x^2 + \ldots + c_{n-1}x^{n-1}, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ vx^{n-1} &= k_0 + k_1x + k_2x^2 + \ldots + k_{n-1}x^{n-1}, \end{aligned}$$

Или

$$\begin{gathered} (a_0 - v) + a_1x + a_2x^2 + \ldots + a_{n-1}x^{n-1} = 0, \\ b_0 + (b_1 - v)x + b_2x^2 + \ldots + b_{n-1}x^{n-1} = 0, \\ c_0 + c_1x + (c_2 - v)x^2 + \ldots + c_{n-1}x^{n-1} = 0, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ k_0 + k_1x + k_2x^2 + \ldots + (k_{n-1} - v)x^{n-1} = 0. \end{gathered}$$

Эти уравнения можно рассматривать как систему n однородных линейных уравнений с n неизвестными, причем эта система удовлетворяется, если неизвестные имеют значения: $1, x, x^2, \ldots, x^{n-1}$; так как эти значения не все равны нулю (именно, 1), то (по § 33, следствию II) детерминант, составленный из коэфициентов этой системы, равен нулю, т. е.

$$\begin{vmatrix} a_0 - v & a_1 & a_2 & \ldots & a_{n-1} \\ b_0 & b_1 - v & b_2 & \ldots & b_{n-1} \\ c_0 & c_1 & c_2 - v & \cdots & c_{n-1} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ k_0 & k_1 & k_2 & \ldots & k_{n-1} - v \end{vmatrix} = 0.$$

Это и есть искомое уравнение для v.

Пример. Возьмем то же уравнение: $x^2 - 2x + 3 = 0$ и ту же функцию $v = 1 + x + x^2$. Имеем:

$$\begin{aligned} v &= 1 - x + x^2 \\ vx &= -3 + 3x - x^2, \\ vx^2 &= 3 - 5x + 3x^2; \end{aligned}$$

отсюда

$$\begin{vmatrix} 1 - v & -1 & 1 \\ -3 & 3 - v & -1 \\ 3 & -5 & 3 - v \end{vmatrix} = 0,$$

или $-v^3+7v^2-4v+4=0$, то же уравнение, что и раньше.

Упражнения

Преобразовать по способу Чирнгаузена следующие уравнения:
189) $x^2-3x^2-2=0$, $v=2-2x+x^2$.
Отв. $v^3-9v^2+24v-32=0$.
190) $x^4-x^3+2x-1=0$, $v=1-x+2x^2$.
Отв. $v^4-5v^3+5v^2-25v+25=0$.
191) $x^4+x^3+x^2+x+1=0$, $v=1+x+x^2+x^3$.
Отв. $v^4-v^3+v^2-v+1=0$.
192) $x^5-1=0$, $v=-1+x^4$.
Отв. $v^5+5v^4+10v^3+10v^2+5v=0$.

§ 147. Результант. Пусть имеем уравнение $f(x)=a_0x^n+a_1x^{n-1}+\ldots+a_n=0$ с корнями $x_1,x_2,\ldots,x_n$ и уравнение $g(x)=b_0x^m+b_1x^{m-1}+\ldots+b_m=0$ с корнями $y_1,y_2\ldots,y_m$. *Результант уравнений* $f=0$ и $g=0$, или функций f и g, есть следующее выражение: $R(f,g)=b_0^nf(y_1)f(y_2)\cdots f(y_m)$. Но $f(x)=a_0(x-x_1)(x-x_2)\cdots(x-x_n)$; следовательно:

$$\begin{aligned} R(f,g) &= a_0(y_1-x_1)(y_1-x_2)\cdots(y_1-x_n)\times \\ &\times\ a_0(y_2-x_1)(y_2-x_2)\cdots(y_2-x_n)\times \\ &\quad\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ &\times\ a_0(y_m-x_1)(y_m-x_2)\cdots(y_m-x_n)\times \\ &\times\ b_0\cdot b_0\cdots b_0 \end{aligned}$$

или

$$R(f,g)=a_0^mb_0^n\prod_{r,s}(y_r-x_s)\qquad(r=1,2,\ldots,m;\ s=1,2,\ldots,n).\tag{25}$$

Соединяя множителей по колоннам, получим:

$$\begin{aligned} R(f,g) &= a_0^m(-1)^mg(x_1)(-1)^mg(x_2)\cdots(-1)^mg(x_n)= \\ &= (-1)^{mn}\cdot a_0^mg(x_1)g(x_2)\cdots g(x_n), \end{aligned}$$

т. е.

$$R(f,g)=(-1)^{mn}\cdot R(g,f).$$

Из определения результанта следует, что он — симметрическая функция от $y_1,y_2,\ldots,y_m$ с коэфициентами, рационально зависящими от $a_0,a_1,\ldots,a_n$, или — симметрическая функция от $x_1,x_2,\ldots,x_n$ с коэфициентами, рационально зависящими от $b_0,b_1\ldots,b_m$. Другими словами, $R(f,g)$ есть рациональная (и при этом целая) функция от $a_0,a_1\ldots,a_n$ и от $b_0,b_1\ldots,b_m$. Далее, из определения $R(f,g)$ следует:

Теорема. *Необходимое и достаточное условие для того, чтобы уравнения* $f(x)=0$ *и* $g(x)=0$ *имели общий корень, следующее: результант этих уравнений должен быть равен нулю.*

Если уравнения $f(x)=0$ и $g(x)=0$ имеют общий корень, то между их коэфициентами должна быть известная зависимость; уравнение $R(f,g)=0$ и выражает

эту зависимость. Другими словами, $R(f,g)=0$ есть результат исключения x из уравнений $f(x)=0$ и $g(x)=0$.

Укажем способы вычисления $R(f,g)$ как функции от коэфициентов.

Способ 1. Пусть степень $f \geq$ степени g; делим f на g: $f=gq+f_1$; степень $f_1 = n_1 \leq m-1$; для $x=y_\lambda$: $f(y_\lambda)=f_1(y_\lambda)$; отсюда следует: $R(f,g)=b_0^{n-n_1}R(f_1,g)$; теперь делим g на f_1 и подобно же продолжаем далее, пока не дойдем до остатка, который равен постоянному количеству. Если же, например, $f(x)=k=\text{const}$, то $f(y_1)=f(y_2)=\ldots=f(y_m)=k$, т. е. $R(f,g)=b_0^0\cdot k^m=k^m$.

Способ 2. Возьмем, например, $n=3$, $m=2$ (хотя наши рассуждения будут общими); пусть x — общий корень уравнений $f(x)=0$, $g(x)=0$ имеем:

$$\begin{aligned}
f(x) &= a_0x^3+a_1x^2+a_2x+a_3=0,\\
xf(x) &= a_0x^4+a_1x^3+a_2x^2+a_3x=0,\\
g(x) &= b_0x^2+b_1x+b_2=0,\\
xg(x) &= b_0x^3+b_1x^2+b_2x=0,\\
x^2g(x) &= b_0x^4+b_1x^3+b_2x^2=0.
\end{aligned}$$

Эти уравнения можно рассматривать как пять линейных однородных уравнений с пятью неизвестными, удовлетворяющихся при значениях неизвестных 1, x, x^2, x^3, x^4; эти значения не все равны нулю; следовательно (§ 33, следствие II), детерминант из коэфициеитов этой системы равен нулю:

$$D=\begin{vmatrix} a_0 & a_1 & a_2 & a_3 & 0\\ 0 & a_0 & a_1 & a_2 & a_3\\ b_0 & b_1 & b_2 & 0 & 0\\ 0 & b_1 & b_1 & b_2 & 0\\ 0 & 0 & b_0 & b_1 & b_2 \end{vmatrix}=0.$$

Это уравнение есть результат исключения x из уравнений $f(x)=0$, $g(x)=0$; отсюда можно предвидеть, что левая часть его, т. е. D, отличается от R разве только постоянным множителем. Докажем, что $D=R(f,g)$. Имеем[72]:

$$\begin{vmatrix} a_0 & a_1 & a_2 & a_3 & 0\\ 0 & a_0 & a_1 & a_2 & a_3\\ b_0 & b_1 & b_2 & 0 & 0\\ 0 & b_1 & b_1 & b_2 & 0\\ 0 & 0 & b_0 & b_1 & b_2 \end{vmatrix}\cdot\begin{vmatrix} y_1^4 & y_1^3 & y_1^2 & y_1 & 1\\ y_2^4 & y_2^3 & y_2^2 & y_2 & 1\\ x_1^4 & x_1^3 & x_1^2 & x_1 & 1\\ x_2^4 & x_2^3 & x_2^2 & x_2 & 1\\ x_3^4 & x_3^3 & x_3^2 & x_3 & 1 \end{vmatrix}=$$

$$=\begin{vmatrix} y_1f(y_1) & y_2f(y_2) & 0 & 0 & 0\\ f(y_1) & f(y_2) & 0 & 0 & 0\\ 0 & 0 & x_1^2g(x_1) & x_2^2g(x_2) & x_3^2g(x_3)\\ 0 & 0 & x_1g(x_1) & x_2g(x_2) & x_3g(x_3)\\ 0 & 0 & g(x_1) & g(x_2) & g(x_3) \end{vmatrix}=$$

$$=\begin{vmatrix} y_1f(y_1) & y_2fy_2) \\ f(y_1) & f(y_2) \end{vmatrix}\cdot\begin{vmatrix} x_1g(x_1) & x_2^2g(x_2) & x_3g(x_3)\\ x_1g(x_1) & x_2g(x_2) & x_3g(x_3)\\ g(x_1) & g(x_2) & g(x_3) \end{vmatrix}$$

[72] См. § 34.

$$= f(y_1)f(y_2)g(x_1)g(x_2)g(x_3)\cdot\begin{vmatrix} y_1 & y_2 \\ 1 & 1 \end{vmatrix}\cdot\begin{vmatrix} x_1^2 & x_2^2 & x_3^2 \\ x_1 & x_2 & x_3 \\ 1 & 1 & 1 \end{vmatrix}$$

или (пример 3 в § 30):

$$\begin{aligned} D \quad &\cdot \quad (-1)^{10}(y_2-y_1)(x_1-y_1)(x_2-y_1)(x_3-y_1)(x_1-y_2)(x_2-y_2)(x_3-y_3)\times \\ &\times \quad (x_3-y_2)(x_2-x_1)(x_3-x_1)(x_3-x_2) = f(y_1)f(y_2)g(x_1)g(x_2)g(x_3)\times \\ &\times \quad g(x_3)(-1)(y_2-y_1)(-1)^3(x_2-x_1)(x_3-x_1)(x_3-x_2), \end{aligned}$$

или $D = b_0^3 f(y_1)f(y_2) = R(f,g)$, что и требовалось доказать.

Пример. Найдем результант двух квадратных уравнений:

$$f(x) = ax^2 + a_1x + a_2 = 0, \qquad g(x) = b_0x^2 + b_1x + b_2 = 0.$$

Имеем по второму способу:

$$\begin{aligned} R(f,g) &= \begin{vmatrix} a_0 & a_1 & a_2 & 0 \\ 0 & a_0 & a_1 & a_2 \\ b_0 & b_1 & b_2 & 0 \\ 0 & b_0 & b_1 & b_3 \end{vmatrix} = \\ &= \begin{vmatrix} a_0 & a_1 & a_2 & 0 \\ 0 & a_0 & a_1 & a_2 \\ 0 & b_1 - \dfrac{a_1b_0}{a_0} & b_2 - \dfrac{a_2b_0}{a_0} & 0 \\ 0 & b_0 & b_1 & b_2 \end{vmatrix} = a_0\cdot\begin{vmatrix} a_0 & a_1 & a_2 \\ b_1 - \dfrac{a_1b_0}{a_0} & b_2 - \dfrac{a_2b_0}{a_0} & 0 \\ b_0 & b_1 & b_2 \end{vmatrix} = \\ &= (a_0b_2 - a_2b_0)^2 - 9a_1b_2 - a_2b_1)(a_0b_1 - a_1b_0). \end{aligned}$$

Упражнения

Найти результант следующих уравнений:

193) $x^4 - 2x^2 + 3 = 0$ и $x^2 - x + 1 = 0$.

Отв. 19.

194) $x^3 - 3x^2 + x + 2 = 0$ и $x^3 - x^2 - 4 = 0$.

Отв. 0.

§ 148. Уравнения с двумя неизвестными. Пусть $f(x,y)$ и $g(x,y)$ два алгебраических уравнения с двумя неизвестными; первое n-й степени, второе m-й степени.

Расположим левые их части по степеням y:

$$f(x,y) = a_0(x)y^n + a_1(x)y^{n-1} + \ldots + a_n(x),$$
$$g(x,y) = b_0(x)y^m + b_1(x)y^{m-1} + \ldots + b_m(x);$$

здесь $a_\varkappa(x)$ ц. р. функция от x степени $\leq \varkappa$; то же самое и $b_\varkappa$. Пусть x_1, y_1 — решение этой системы уравнений; тогда уравнения с неизвестным y:

$$f(x_1,y) = 0, \qquad g(x_1,y) = 0$$

имеют общее решение $y = y_1$, т. е. их результант должен быть равен нулю; обозначим его через $R(x)$; следовательно, уравнение $R(x) = 0$ имеет решение $x = x_1$. Итак, чтобы решить нашу систему уравнений, надо решить уравнение $R(x) = 0$; пусть $x = x_1$ одно из его решений; подставляем x_1 вместо x в функции $f(x, y)$ и $g(x, y)$; тогда $f(x_1, y)$ и $g(x_1, y)$ будут иметь общего делителя степени ≥ 1. Находим его: пусть этот делитель равен $h(y)$; решив уравнение $h(y) = 0$, мы получим искомые значения y. Если $h(y)$ линейная функция, то при данном x_1 корень y_1 уравнения $h(y) = 0$ находится рациональным путем, и значению x_1 соответствует только одно значение y_1 дающее решение (x_1, y_1) данной системы.

Определим, какой степени функция $R(x)$ относительно x. По выражению (10) для $R(f, g)$ видно, что $R(f, g)$ однородная функция от $x_1, x_2, \ldots, x_n$, $y_1, \ldots, y_m$ степени nm. Выразим $R(f, g)$ через коэфициенты $a_{\varkappa}$ и b_λ; пусть

$$R(f, g) = \sum A a_0^{\alpha_0} a_1^{\alpha_1} a_2^{\alpha_2} \cdots a_n^{\alpha_n} b_0^{\beta_0} b_1^{\beta_1} b_2^{\beta_2} \cdots b_m^{\beta_m},$$

где A — -целые числа; из (25) очевидно, что $R(f, g)$ — целая функция от $a_{\varkappa}$ и b_λ. Если мы, обратно, вместо $a_{\varkappa}$ и b_λ подставим $x_{\varkappa}$ и y_λ, мы должны получить однородную функцию от $x_{\varkappa}$ и y_λ степени $n \cdot m$. Но a_0 0-й степени относительно $x_{\varkappa}$, a_1 — первой степени; a_2 — второй степени, $\ldots$, a_n — n-й степени; подобно же b_0 — 0-й степени относительно y_λ, b_1 — первой степени, b_2 — второй степени, $\ldots$, b_m — m-степени: следовательно:

$$A a_0^{\alpha_0} a_1^{\alpha_1} a_2^{\alpha_2} \cdots a_n^{\alpha_n} b_0^{\beta_0} b_1^{\beta_1} b_2^{\beta_2} \cdots b_m^{\beta_m}$$

есть ц. р. функция степени:

$$0 \cdot \alpha_0 + 1 \cdot \alpha_1 + 2 \cdot \alpha_2 + \ldots + n\alpha_n + 0 \cdot \beta_0 + 1 \cdot \beta_1 + 2 \cdot \beta_2 + \ldots m\beta_m$$

от $x_1, x_2, \ldots, x_n$, $y1$,...,ут, но в каждом члене это выражение должно быть равно nm, ибо $R(f, g)$ однородная функция степени nm от $x_1, \ldots, x_n$, $y_1, \ldots, y_m$, т. е. в каждом члене в $R(f, g)$:

$$0 \cdot \alpha_0 + 1 \cdot \alpha_1 + 2 \cdot \alpha_2 + \ldots + n\alpha_n + 0 \cdot \beta_0 + 1 \cdot \beta_1 + 2 \cdot \beta_2 + \ldots m\beta_m = n \cdot m. \quad (26)$$

Заметим, что эта сумма называется *весом* члена; мы доказали, что в функции $R(f, g)$ вес каждого члена один и тот же: $n \cdot m$; такая функция называется *изобаричной*.

Из (26) следует для случая, когда $a_{\varkappa}$ и $b_{\varkappa}$ ц. р. функции от x степени $\varkappa$, что $R(x)$ ц. р. функция от x степени $\leq n \cdot m$ (ибо высшие члены могут и сократиться). Итак:

Теорема. *Если из системы, уравнений $f(x, y) = 0$ n-й степени и $g(x, y) = 0$ m-й степени исключим одно из неизвестных, то в результате получим уравнение с другим неизвестным степени $n \cdot m$ (в частных случаях и ниже).*

Сколько же систем решений x, y имеет наша система уравнений $f(x, y) = 0$ и $g(x, y) = 0$? Найдя один из корней x_1 уравнения $R(x) = 0$ и подставив его в данные уравнения, мы находим уравнение для y $h(y) = 0$; вопрос в том, какой степени будет функция $h(y)$, т. е. будет ли найденному значению $x = x_1$ соответствовать только одно значение y, или несколько таких значений? Более глубокое

исследование дает следующий результат [73]. Степень функции $h(y)$ равна кратности найденного корня x_1 уравнения $R(x) = 0$; в частности, если x_1 — простой корень, то и $h(y)$ будет первой степени.

Если в частном случае окажется, что $R(x)$ будет ниже, чем $(n \cdot m)$-й степени, то в этом случае, как обычно в алгебре, считают, что один или несколько корней x равны ∞. Таким образом получаем следующую общую теорему:

Теорема. *Система двух алгебраических уравнений $f(x, y) = 0 = 0$ и $g(x, y) = 0$ n-й и m-й степени, имеет всегда $m \cdot n$ (различных или равных) систем решений x, y, если только функции $f(x, y)$ и $g(x, y)$ не имеют общих множителей, содержащих переменные x, y.*

Эту теорему первый высказал Безу (Bézout), и при этом в геометрической форме:

Две алгебраические кривые n-го и m-то порядков, не имеющие общих частей, пересекаются в $m \cdot n$ точках (причем некоторые из этих точек пересечения могут сливаться, некоторые же могут лежать в ∞).

В формулировке этой теоремы упоминается один исключительный случай, которого мы еще не разбирали: может случиться, что результант $R(x)$ будет тождественно равен нулю, — независимо от x. Это значит, что функции $f(x, y)$ и $g(x, y)$ в этом случае имеют общего делителя $h(x, y)$, содержащего по крайней мере одно из переменных x, y. Очевидно, что для всяких x, y, для которых $h(x, y)$ обратится в 0, и $f(x, y)$ и $g(x, y)$ будут равны нулю, т. е. наши уравнения имеют в этом случае бесчисленное множество пар решений x, y, именно, все системы x, y, которые удовлетворяют уравнению $h(x, y) = 0$. Говоря геометрическим языком, в этом случае кривые $f(x, y) = 0$ и $g(x, y) = 0$ имеют общую часть: $h(x, y) = 0$.

Нахождение уравнения $R(x) = 0$ по двум данным уравнениям $f(x, y) = 0$ и $g(x, y) = 0$ называется *исключением* (*элиминацией*) y из уравнений $f = 0$, $g = 0$.

Пример. Исключить y из уравнений:

$$\begin{cases} 2x^2 - 3xy + y^2 + 4x - 5 = 0 \\ x^2 - y^2 + 2x + 3y + 1 = 0. \end{cases}$$

Располагая по степени y найдем:

$$\begin{cases} y^2 - 3xy + (2x^2 + 4x - 5) = 0, \\ -y^2 + 3y + (x^2 + 2x + 1) = 0. \end{cases}$$

Имеем для результанта два квадратных уравнения (см. пример в § 147):

$$R = (a_0 b_2 - a_2 b_0)^2 - 9a_1 b_2 - a_2 b_1)(a_0 b_1 - a_1 b_0);$$

здесь

$$a_0 = 1, \quad a_1 = -3x, \quad a_2 = 2x^2 + 4x - 5; \quad b_0 = -1, \quad b_1 = 3, \quad b_2 = x^2 + 2x + 1;$$

следовательно:

$$\begin{aligned} R(x) &= [((x^2 + 2x + 1) \cdot 1 + (2x^2 + 4x - 5) \cdot 1]^2 - \\ &- [-3x((x^2 + 2x + 1) - 3(x^2 + 4x + 5)](3 - 3x) = \\ &= 9x^3 + 3x^2 + 42x - 29. \end{aligned}$$

[73] См., например, Weber, Lehrbuch der Algebra, Bd. 1, § 54, 55.

Итак, результат исключения:

$$9x^3 + 3x^2 + 42x - 29 = 0;$$

здесь он третьей степени.

Упражнения

195) Исключить y из уравнений: $x^2+xy+y^2-3=0$, $2x^2+2xy-3y^2+x-y+2=0$.

Отв. $25x^4 - 107x^2 + 9x + 46 = 0$.

196) Исключить y из уравнений: $x^2 + xy - 2y^2 - 2x + 5y - 3 = 0$, $2x^2 - 2xy - 3x + 5y - 5 = 0$.

Отв. Нуль, так как левые части наших уравнений имеют общего множителя $x - y + 1$.

197) Исключить x из уравнений: $x^3 - 3y^3 + 1 = 0$, $x^2 + y^2 - 6 = 0$.

Отв. $10y^6 - 18y^4 - 6y^3 + 108y^2 - 215 = 0$.

§ 149. Дискриминант. Пусть $f(x) = 0$ данное уравнение n-й степени с корнями $x_1, x_2, \ldots, x_n$. Дискриминантом его называется следующее выражение:

$$D = (-1)^{\frac{n(n-1)}{2}}\, a_0^{-1} R(f', f).$$

Но

$$R(f', f) = a_0^{n-1} f'(x_1) f'(x_2) \cdots f'(x_n);$$

по § 56 (9):

$$f(x_\varkappa) = a_0(x_\varkappa - x_1)(x_\varkappa - x_2)\cdots(x_\varkappa - x_{\varkappa-1})(x_\varkappa - x_{\varkappa+1})\cdots(x_\varkappa - x_n);$$

следовательно:

$$R(f', f) = a_0^{n-1} a_0^{-1} \cdot a_0^n \prod_{\alpha>\beta} (x_\alpha - x_\beta)^2 (-1)^{\frac{n(n-1)}{2}};$$

значит

$$D = a_0^{2n-2} \prod_{\alpha>\beta} (x_\alpha - x_\beta)^2. \tag{27}$$

По § 57, теореме 1 заключаем:

Теорема. *Необходимое и достаточное условие существования кратных корней у уравнения $f(x) = 0$ следующее: дискриминант уравнения должен быть равен нулю.*

Дискриминант, как видно из уравнения (27), есть симметрическая функция корней, т. е. выражается рационально через коэфициенты, при этом он — целая функция от $a_0, a_1, \ldots, a_n$. Вычислить его как функцию от $a_0, a_1, \ldots, a_n$ можно общими способами, указанными и § 138–141. Укажем еще на один способ вычисления D.

Имеем (см. § 30, пример 3):

$$\begin{vmatrix} 1 & 1 & \ldots & 1 \\ x_1 & x_2 & \ldots & x_n \\ \ldots & \ldots & \ldots & \ldots \\ x_1^{n-1} & x_2^{n-1} & \ldots & x_n^{n-1} \end{vmatrix} = \prod_{\alpha>\beta} (x_\alpha - x_\beta).$$

Умножаем этот детерминант на самого себя, комбинируя строки со строками. Получаем:

$$\prod_{\alpha>\beta}(x_\alpha - x_\beta)^2 = \begin{vmatrix} s_0 & s_1 & s_2 & \dots & s_{n-1} \\ s_1 & s_2 & s_3 & \dots & s_n \\ s_2 & s_3 & s_4 & \dots & s_{n+1} \\ \dots & \dots & \dots & \dots & \dots \\ s_{n-1} & s_n & s_{n+1} & \dots & s_{2n-2} \end{vmatrix}. \tag{28}$$

D получается, если этот детерминант умножим на a_0^{2n-2}.

Пример 1. Пусть $n = 2$; найдем дискриминант квадратного уравнения $ax^2 + bx + c = 0$.

Имеем:

$$D = a^2 \cdot \begin{vmatrix} 2 & s_1 \\ s_1 & s_2 \end{vmatrix} = a^2(2s_2 - s_1)^2 = a^2\left[\left(\frac{b}{a}\right)^2 - 4\frac{c}{a}\right] = b_2 - 4ac,$$

как известно из элементарной алгебры.

Пример 2. Пусть $n = 3$; наше уравнение:

$$a_0x^3 + a_1x^2 + a_2x + a_3 = 0.$$

Имеем:

$$\begin{vmatrix} 3 & s_1 & s_2 \\ s_1 & s_2 & s_3 \\ s_2 & s_3 & s_4 \end{vmatrix} = 3s_2s_4 + 2s_1s_2s_3 - s_3^2 - s_1^2s_4 - 3s_3^2 =$$

$$= f_1^2f_2^2 - 4f_1^3f_3 + 18f_1f_2f_3 - 4f_2^3 - 27f_3^2.$$

(Ср. §§ 138, 139 и 141). Но $f_1 = -\frac{a_1}{a_0}$; $f_2 = \frac{a_2}{a_0}$; $f_3 - \frac{a_3}{a_0}$; кроме того, найденное выражение надо еще умножить на $a_0^{2\cdot3-2} = a_0^4$; от этого дроби уничтожаются. Итак:

$$D = a_1^2a_2^2 - 4a_1^3a_3 + 18a_0a_1a_2a_3 - 4a_0a_2^3 - 27a_0^2a_3^2. \tag{29}$$

В частном случае для уравнения $x^3 + ax + b = 0$ получаем:

$$D = -4a^3 - 27b^2 = -4 \cdot 27\left(\frac{b^2}{4} + \frac{a^3}{27}\right). \tag{30}$$

§ 150. Способ Коши отделения корней. Пусть наш дискриминант $D \neq 0$. Имеем: $+\sqrt{|D|} = \prod|x_\varkappa - x_\lambda|$; пусть $(x_\alpha - x_\beta|$ одна из этих разностей; тогда

$$\frac{\sqrt{|D|}}{|x_\alpha - x_\beta|} = \prod{}'|x_\varkappa - x_\lambda|,$$

где штрих возле $\prod$ означает, что в произведении нет одного сомножителя, именно, $|x_\alpha - x_\beta|$, т. е. всего имеется $\frac{n(n-1)}{2} - 1$ сомножителей. Пусть $g = \alpha + 1$ высший предел абсолютной величины корней (см. § 65); тогда

$$|x_\varkappa - x_\lambda| \leq |x_\varkappa| + |x_\lambda| < 2g,$$

следовательно:

$$\frac{\sqrt{|D|}}{|x_\alpha - x_\beta|} < (2g)^{\frac{n(n-1)}{2}-1};$$

отсюда

$$|x_\alpha - x_\beta| > \frac{\sqrt{|D|}}{2g^{\frac{n(n-1)}{2}-1}}.$$

На этом основан способ Коши отделения корней.

Обозначим:

$$\frac{\sqrt{|D|}}{2g^{\frac{n(n-1)}{2}-1}} = h;$$

тогда для всяких двух корней x_α и x_β: $|x_\alpha - x_\beta| > h$, т, е. в интервале длины h или нет ни одного корня, или имеется только один корень. Так как $D \neq 0$, то все корни нашего уравнения — простые. Пусть g_1 и g_2 — нижний и верхний пределы вещественных корней данного уравнения; берем значения: g_1, $g_1 + h$, $g_1 + 2h$, $\ldots$, $g_1 + (m-1)h$, g_2, предполагая, что $g_1 + (m-1)h < g_2 \leq g_1 + mh$.

Находим теперь соответственные значения левой части уравнения:

$$f(g_1), \quad f(g_1 + h), \quad f(g_1 + 2h), \ \ldots, \ f(g_2)$$

и обращаем внимание на их знаки; если

$$\operatorname{sign} f(g_1 + \lambda h) = \operatorname{sign} f[g_1 + (\lambda + 1)h],$$

то в интервале $[g_1 + \lambda h, g_1 + (\lambda + 1)_h]$ нет ни одного корня нашего уравнения; если же

$$\operatorname{sign} f(g_1 + \lambda h) = -\operatorname{sign} f[g_1 + (\lambda + 1)h],$$

то в интервале $[g_1 + \lambda h, g_1 + (\lambda + 1)_h]$ лежит один и только один корень нашего уравнения. Таким образом все вещественные корни нашего уравнения будут отделены. Этот способ при всей его теоретической простоте не имеет практического значения вследствие того, что получаемая в нем величина h очень мала, т. е. число наших испытаний m очень велико.

Пример. Дано уравнение $f(x) = x^3 - 3x + 1 = 0$; здесь

$$g = \alpha + 1 = 4; \qquad D = -4 \cdot 27\left(\frac{1}{2} - 1\right) = 2 \cdot 27 = 54;$$

$$\frac{n(n-1)}{2} - 1 = 2; \qquad h = \frac{\sqrt{54}}{8^2} > 0,1,$$

т. е. мы можем взять для простоты $h = 0,1$ (очевидно, что мы имеем право уменьшить h). По способу Ньютона (§ 83) легко найдем, что здесь $g_1 = -2$, $g_2 = +2$; таким образом $m = 40$.

Вычисляем теперь:

$$f(-2), \quad f(-1,9), \quad f(-1,8), \ \ldots, \ f(2);$$

найдем:

$$\begin{aligned} &f(-1,9) = -0,159, && f(-1,8) = +0,568, \\ &f(0,3) = +0,127, && f(0,4) = -0,136, \quad . \\ &f(1,5) = -0,125, && f(1,6) = +0,296. \end{aligned}$$

Итак, три вещественных корня нашего уравнения лежат в интервалах:

$$(-1,9-1,8), \qquad (0,3;0,4), \qquad (1,5;1,6).$$

§ 151. Общие замечания о рациональных функциях нескольких переменных. Очевидно, что сумма, разность и произведение целых (или дробных) рациональных функций — тоже целые (или дробные) рациональные функции; частное рациональных функций — тоже рациональная функция, при этом предполагается, что все это — функции от одних и тех же n переменных. При сложении, вычитании и умножении рациональных функций над их коэфициентами совершаются тоже только действия сложения, вычитания и умножения; при делении над коэфициентами может совершаться и действие деления. Отсюда следует:

Все рациональные функции одних и тех же n переменные составляют тело (§ 13); *все рациональные функции с коэфициентами из данного числового тела составляют тело.*

Все целые рациональные функции одних и тех же переменных составляют область целости (§ 13); *все целые рациональные функции с коэфициентами из данной области целости тоже составляют область целости.*

Для полного доказательства последнего предложения следует еще показать, что область рациональных функций не имеет нулевых делителей (§ 5), т. е. что произведение целых рациональных функций тождественно равно нулю только тогда, если один из сомножителей тождественно равен нулю. Для функций одного переменного это легко следует из теоремы § 50, а для функций нескольких переменных это легко доказывается методом полной индукции.

Заметим, что если мы рассматриваем функции от n переменных $x_1, x_2, \ldots, x_n$, то функции от некоторых из этих переменных, равно как и постоянные количества, рассматриваются как частные случаи функций от всех n переменных $x_1, x_2, \ldots, x_n$.

Как и для целых рациональных функций одного переменного (§ 47), определяется делимость для целых рациональных функций нескольких переменных и строится теория их делимости. И здесь мы можем брать функции либо с любыми числовыми коэфициентами, либо в данном теле P (т. е. с коэфициентами из P, ср. § 111). Как и для функций одного переменного, определяется *приводимость* и *неприводимость* целых рациональных функций в теле P.

Если целая рациональная функция неприводима в теле всех комплексных чисел, то она называется неразложимой; в противном случае — разложимой. Но в то время как для функций одного переменного единственными неразложимыми целыми рациональными функциями были линейные, неразложимые целые рациональные функции нескольких переменных могут быть какой угодно степени. Например, целая рациональная функция двух переменных

$$x^n + y$$

неразложима. Но основная теорема о разложении всякой целой рациональной функции на неразложимые (или в данном теле — на неприводимые) множители и об однозначности этого разложения (с точностью до постоянных множителей) здесь верна (ср. § 50 и § 100).

Переходя теперь к симметрическим функциям, заметим, что основная теорема теории симметрических функций и обратная к ней теорема (§ 133) дает возможность сопоставить со всякой целой или дробной рациональной симметрической функцией от n переменных (вообще, или в данном теле, или в данной области целости) единственную целую же или дробную же рациональную функцию от новых n переменных, именно, от элементарных симметрических функций от старых переменных (тоже вообще, или в том же теле, или в той же области целости), и обратно. Иными словами, симметрической функции

$$F(x_1, x_2, \ldots, x_n)$$

соответствует (целая или дробная) рациональная функция:

$$G(z_1, z_2, \ldots, z_n),$$

если при $z_1 = f_1$, $z_2 = f_2$, $\ldots$, $z_n = f_n$ мы имеем:

$$F(x_1, x_2, \ldots, x_n) \equiv G(f_1, f_2, \ldots, f_n).$$

Далее, очевидно, что сумме, разности, произведению и частному симметрических функций соответствует сумма, разность, произведение и частное соответствующих функций G. Дробные и целые рациональные симметрические функции (вообще или в данном теле P) образуют тело, а целые рациональные симметрические функции (вообще, или в данной области целости) образуют область целости. Предыдущие выводы выражают в такой форме:

Тело рациональных симметрических функций от n переменных (вообще, или в данном теле P) изоморфно телу всех рациональных функций от n переменных (тоже вообще, или в том же теле P).

Область целости целых рациональных симметрических функций от n переменных (вообще, или в данной области целости Z) изоморфна области целости всех целых рациональных функций от n переменных (тоже вообще, или в той же области целости Z).

Это- — интересная теорема, говорящая о том, что тело всех рациональных функций от n переменных изоморфно своей части, ибо симметрические рациональные функции от n переменных составляют только часть всех рациональных функций от n переменных. Аналогично — для области целости целых рациональных функций.

Отсюда вытекает теория делимости целых рациональных симметрических функций, понятие о неразложимости (или о неприводимости) симметрической функции, именно как симметрической, наконец, основная теорема о представлении всякой ц. р. симметрической функции в виде произведения неразложимых (или неприводимых) симметрических функций и об единственности такого представления.

Заметим, что элементарные симметрические функции неразложимы как симметрические функции.

§ 152. Подстановки, допускаемые данной функцией. Переставляя переменные в данной функции, мы производим с ними *подстановку* (§ 26). Симметрическую функцию можно определить как такую, которая допускает все подстановки своих переменных; если n число переменных, то число всех подстановок

этих переменных есть $n!$ (§ 26). Обобщим теперь понятие о симметрической функции, рассматривая функции, допускающие не все, а некоторые подстановки своих переменных.

В § 142 мы встретились с одним таким обобщением — полусимметрическими функциями, допускающими все четные подстановки (§ 28). Всякая функция n переменных всегда допускает тождественную подстановку (§ 26).

Пусть $f = f(x_1, x_2, \ldots, x_n)$ — данная функция, а A — некоторая подстановка ее аргументов $x_1, x_2, \ldots, x_n$; сделав в f эту подстановку A, мы обозначим результат так: f_A.

Пусть f — функция от независимых переменных $x_1, x_2, \ldots, x_n$; под выражением: «f допускает подстановку A» мы понимаем, что от подстановки A эта функция совсем не меняет своего вида, т. е. имеет место тождество:

$$f \equiv f_A. \tag{31}$$

Пусть эта же функция допускает и подстановку B; это значит

$$f \equiv f_B.$$

Но тождество (31) не нарушится, если в обеих его частях мы произведем подстановку B, ибо это сведется только к иной нумерации переменных; итак, получим:

$$f_B \equiv f_{AB},$$

где AB есть, как обычно, результат композиции подстановок A и B (§ 26). С другой стороны, (32) и (33) дают:

$$f \equiv f_{AB},$$

т. е. функция f допускает и подстановку AB. Это говорит следующее:

Все подстановки, допускаемые данной функцией f от n независимых переменных, образуют группу (§ 27).

Здесь важно, что переменные *независимые*; иначе из (31) нельзя было бы вывести (33). В теории Галуа (гл. XII) рассматриваются рациональные функции (в данном теле) от корней данного уравнения (в том же теле); там аргументы функций не независимые переменные, и, следовательно, выведенная теорема не верна.

Коснемся вкратце и обратной задачи: найти целую рациональную функцию от n переменных $x_1, x_2, \ldots, x_n$, которая допускала бы данные подстановки $A_1, A_2, \ldots, A_k$ этих переменных. Для этого мы, первым делом, всячески «перемножаем» эти подстановки, т. е. находим всевозможные «произведения»

$$A_1A_2,\ \ A_2A_1,\ \ A_1A_3,\ \ldots,\ A_1^2,\ \ A_1^3,\ \ldots,\ A_2^2,\ \ \ldots, A_1^2A_2,\ \ldots,\ A_1A_2A_1,\ \ldots;$$

эти произведения частью будут равны уже данным подстановкам $A_1, \ldots, A_k$, а частью будут новыми подстановками; мы это перемножение продолжаем до тех пор, пока не перестанем получать новых подстановок, что непременно должно случиться, ибо число всех подстановок наших n переменных $x_1, x_2, \ldots, x_n$ конечно (равно $n!$); тогда все эти полученные произведения вместе с данными подстановками $A_1, A_2, \ldots, A_k$ составят замкнутую систему подстановок, содержащую всевозможные их произведения, т. е. группу (§ 27); говорят, что эта группа «порождается»

подстановками $A_1, A_2, \ldots, A_k$, которые являются ее «генераторами»; обозначают эту группу так:

$$\{A_1, A_2, \ldots, A_k\}.$$

Мы сокращенно обозначим ее буквою $\mathfrak{A}$. Если окажется, что $\mathfrak{A}$ есть группа всех n подстановок количеств $x_1, x_2, \ldots, x_n$, то только любая симметрическая функция является решением нашей задачи, т. е. такой функцией, которая допускает подстановки $A_1, A_2, \ldots, A_k$.

Если же группа $\mathfrak{A}$ не состоит из всех подстановок количеств $x_1, \ldots, x_n$, а только из части их (т. е. если $\mathfrak{A}$ есть «подгруппа» группы всех этих подстановок), то поступаем следующим образом. Берем такую целую рациональную функцию $\varphi(x_1, x_2, \ldots, x_n)$, которая меняла бы свой вид от *каждой* из $n!$ подстановок количеств $x_1, x_2, \ldots, x_n$ (кроме тождественной). Пусть группа $\mathfrak{A}$ состоит из подстановок: E (тождественная), $B_2, B_3, \ldots, B_m$ (конечно, среди них находятся и данные подстановки $A_1, A_2, \ldots, A_k$). Тогда

$$\varphi_E \equiv \varphi, \varphi_{B_2}, \varphi_{B_3}, \ldots, \varphi_{B_m}$$

будут m целых рациональных различных функций и любая симметрическая функция от $\varphi, \varphi_{B_2}, \ldots, \varphi_{B_m}$ решает нашу задачу: она — целая рациональная функция от $x_1, x_2, \ldots, x_n$, допускающая все подстановки группы $\mathfrak{A}$, в частности $A_1, A_2, \ldots, A_k$. Действительно, возьмем, например:

$$f \equiv \varphi + \varphi_{B_2} + \varphi_{B_3} + \ldots + \varphi_{B_m};$$

применим к f какую-нибудь подстановку B из $\mathfrak{A}$ (т. е. B одна из подстановок E, $B_2, \ldots, B_m$); получим:

$$f_B \equiv \varphi_B + \varphi_{B_2B} + \varphi_{B_3B} + \ldots + \varphi_{B_mB};$$

но $B, B_2B, B_3B, \ldots, B_mB$ все тоже подстановки из $\mathfrak{A}$ и все они различны (по закону однозначной обратимости, — см. § 26), т. е. эти произведения $B, B_2B, \ldots, B_mB$ отличаются от $E, B_2, \ldots, B_mB$ только порядком, в каком они стоят; а следовательно:

$$f_B \equiv B,$$

и наше утверждение доказано.

Возникает вопрос: а если мы к f применим какую-нибудь подстановку количеств $x_1, \ldots, x_n$, не принадлежащую к группе $\mathfrak{A}$, изменится ли от этого f или нет? Заранее на этот вопрос нельзя ответить; но можно выбрать функцию f так, чтобы она непременно менялась от всякой подстановки, не принадлежащей к $\mathfrak{A}$; например, если взять

$$f \equiv (t - \varphi)(t - \varphi_{B_2})(t - \varphi_{B_3}) \cdots (t - \varphi_{B_m})$$

и подобрать подходящим образом целое число t (ср. гл. XII, § 214).

Остается еще показать, как выбрать функцию φ, чтобы она менялась при всякой подстановке $x_1, x_2, \ldots, x_n$ (кроме тождественной). Можно, например, взять

$$\varphi = a_1x_1 + a_2x_2 + \ldots + a_nx_n,$$

где $a_1, a_2, \ldots, a_n$ — любые (например, целые) различные числа.

Пример. Пусть $n = 3$; найдем целую рациональную функцию от x_1, x_2, x_3, которая допускала бы подстановку $A = \begin{pmatrix} x_1 & x_2 & x_3 \\ x_2 & x_1 & x_3 \end{pmatrix} = (x_1, x_2)$, эта подстановка A вместе с тождественной подстановкой E уже образует группу, т. е. $\mathfrak{A} = E + A$.

Берем теперь функцию $\varphi \equiv a_1x_1 + a_2x_2 + a_3x_3$, где a_1, a_2, a_3 — различные постоянные; имеем: $\varphi_a = a_2x_1 + a_1x_2 + a_3x_3$; и можно взять:

$$f = \varphi + \varphi_A = (a_1 + a_2)(x_1 + x_2) + 2a_3x_3.$$

Обозначим: $a_1 + a_2 = a$, $2a_3 = b$; тогда

$$f = a(x_1 + x_2) + bx_3.$$

При $a \neq b$ функция f будет меняться при всякой подстановке, кроме E и A (т. е. f «принадлежит» к группе $\mathfrak{A}$). Другое решение будет такое:

$$f = (t - \varphi)(t - \varphi_A),$$

где t — подходящим образом подобранное целое число.

ЧАСТЬ ВТОРАЯ

ГЛАВА ДЕВЯТАЯ

ТЕОРИЯ МАТРИЦ

§ 153. Основные понятия. Ранг матрицы. Понятие матрицы нам уже встречалось (§ 38, 40); можно определить матрицу как рассматриваемую как нечто целое *таблицу чисел, расположенных прямоугольником* (в частном случае — *квадратом*) *по строкам и столбцам*. Если в матрице m строк и n столбцов, то она состоит из mn чисел; при $m \neq n$ она называется *прямоугольной*, и именно, *mn-матрицей*; при $m = n$ она называется *квадратной*, и именно, n-го *порядка*. Числа, из которых состоит матрица, мы будем называть ее *элементами* и обозначать малыми латинскими или греческими буквами; располагая их в m строк и n столбцов, мы будем всю таблицу брать в скобки, чтобы показать, что она образует матрицу; сокращенно мы будем обозначать матрицы большими латинскими буквами.

Так,

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix} \tag{1}$$

есть mn-матрица в общем виде; два индекса у ее элементов дают: первый — номер строки, второй — номер столбца.

Пример 1.

$$\begin{pmatrix} 4 & 3 & -1 & 2 \\ -1 & 0 & 5 & -2 \\ 3 & 3 & 4 & 0 \end{pmatrix}$$

есть числовая $(3, 4)$-матрица.

Пример 2.

$$\begin{pmatrix} 8 & 1 & 0 & 1 & 5 \\ 4 & -1 & 2 & -2 & 0 \\ 1 & 2 & 2 & 5 & 1 \\ 4 & 2 & -1 & 2 & -1 \\ 1 & 0 & -2 & 3 & 1 \end{pmatrix}$$

есть квадратная матрица 5-го порядка.

Пример 3.

$$\begin{pmatrix} 4 & 1 \\ 2 & 6 \\ 1 & 0 \\ 3 & 2 \end{pmatrix}$$

есть $(4, 2)$-матрица.

Пример 4. $(a_1, a_2, \ldots, a_n)$ есть общая $(1, n)$-матрица («строка»).

Пример 5. $\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_m \end{pmatrix}$ есть общая $(m, 1)$-матрица («столбец»).

Пример 6. (a) есть квадратная матрица 1-го порядка; она состоит из одного числа, которое мы будем в дальнейшем писать без скобок, рассматривая, таким образом, числа как частные случаи матриц (как квадратные матрицы 1-го порядка).

Примечание. Хотя в приведенных выше примерах мы брали в качестве элементов целые числа, но вообще элементы матрицы могут быть любыми комплексными числами. Можно даже рассматривать матрицы, элементы которых сами являются тоже матрицами.

Потребность во введении и исследовании матриц возникла в различных областях математики и ее приложений. Мы с этим уже встречались в первой части нашего курса: детерминант дает квадратную матрицу его элементов; система линейных уравнений и система линейных функций дают нам матрицы их коэфициентов. Позже мы познакомимся еще с иными источниками матриц. Но везде, где рассматриваются матрицы, первостепенную роль играет их *ранг*, уже определенный нами в § 40. Мы там видели, что ранг mn-матрицы есть целое положительное число, не превосходящее наименьшего из чисел m и n. Наименьшее значение для ранга есть 1, если в матрице есть хоть один элемент, отличный от нуля. Ранг 0 имеют только матрицы, состоящие из нулей («нулевые» матрицы). Для квадратной матрицы n-го порядка ранг меньше или равен n; этот ранг равен n, если единственный детерминант n-го порядка, а именно, составленный из всех элементов матрицы, отличен от нуля; такую квадратную матрицу (т. е., у которой ранг равен порядку) мы будем называть неособенной; если же у квадратной матрицы ранг ниже порядка, т. е. ее детерминант (составленный из всех ее элементов) равен нулю, то мы ее назовем особенной.

Если A — квадратная матрица n-го порядка, то ее детерминант (тоже n-го порядка) обозначают через $|A|$ [74]. Итак, квадратная матрица A неособенная, если $|A| \neq 0$.

Из приведенных выше примеров в 1) мы имеем матрицу ранга 2, в 2) — неособенную квадратную матрицу ранга 5, в 3) матрицу ранга 2.

Со всякой mn-матрицей $[(1)]$ можно сопоставить две системы линейных форм, а именно:

$$y_\alpha = \sum_{\beta=1}^{n} a_{\alpha\beta} x_\beta \qquad (\alpha = 1, 2, \ldots, m) \tag{2}$$

$$y'_\beta = \sum_{\alpha=1}^{m} a_{\alpha\beta} x'_\alpha \qquad (\beta = 1, 2, \ldots, n). \tag{3}$$

Формы (2) составляются «по строкам», формы (3) — «по столбцам». По теореме 3 § 42 мы заключаем, что ранг r матрицы (1) есть число линейно независимых

[74] Это обозначение не следует смешивать с обозначением абсолютной величины числа.

форм в системе (2) или в системе (3). Это выражают иначе, говоря, что ранг r есть *число линейно независимых строк* в матрице (1) или *число линейно независимых столбцов* в той же матрице. Это дает вместе с тем два новых определения ранга матрицы. Отсюда также следует, что в матрице *число линейно независимых строк всегда равно числу линейно независимых столбцов*.

Наконец, в теории матриц часто пользуются и языком векторов: матрицу (1) можно рассматривать как систему m векторов $a_1, a_2, \ldots, a_m$ в n-мерном пространстве, причем составляющими для вектора a_λ служат числа $a_{\lambda 1}, a_{\lambda 2}, \ldots, a_{\lambda n}$, — или как систему n векторов $a'_1, a'_2, \ldots, a'_n$ в m-мерном пространстве с составляющими $a_{1\varkappa}, a_{2\varkappa}, \ldots, a_{m\varkappa}$ для вектора $a'_\varkappa$. Ранг матрицы (1) есть не что иное, как число линейно независимых векторов каждой из этих двух систем.

§ 154. Элементарные преобразования матрицы. Конечно, матрица — не детерминант, и те преобразования, которые не меняют величины детерминанта, тем не менее меняют матрицу: даже от перестановки строк со столбцами матрица совершенно меняется. Но все же рассматриваются такие операции над матрицами, которые, изменяя сами матрицы, не меняют их ранга; эти операции называются «*элементарными преобразованиями*» матриц; их три, а именно:

1. Перестановка двух строк или двух столбцов.

2. Умножение всех элементов строки (или столбца) на один и тот же, отличный от нуля, множитель.

3. Прибавление к элементам данной строки (или столбца) соответствующих элементов другой строки (или столбца), умноженных на один и тот же произвольный множитель.

Эти три преобразования обладают свойством симметрии, т. е. если от матрицы A к матрице B можно перейти одним из этих преобразований, то и от B к A можно перейти таким же преобразованием.

Назовем две матрицы *эквивалентными*, если от одной из них можно перейти к другой посредством конечного числа элементарных преобразований.

Понятие эквивалентности, очевидно, удовлетворяет трем основным законам равенств — *симметрии*, *транзитивности*, *рефлективности* (§ 2, примечание 1).

Эквивалентные матрицы имеют один и тот же ранг.

Это следует из того, что от преобразований 1, 2 и 3 ранг матрицы не меняется; для преобразований 1 и 2 это очевидно; что касается преобразования 3, то легко видеть, что оно не может повысить ранга матрицы, ибо каждый данный детерминант k-го порядка рассматриваемой матрицы оно может в крайнем случае заменить суммой двух детерминантов k-го порядка той же матрицы; но оно не может и понизить ранг матрицы, ибо тогда, переходя подобным же преобразованием от новой матрицы к старой, мы получили бы повышение ранга, чего не может быть.

Скоро мы увидим, что и обратно: mn-матрицы, имеющие одни и тот же ранг, эквивалентны, т. е. от одной из них можно перейти к другой посредством конечного числа элементарных преобразований.

Следствие. Данная матрица перейдет в эквивалентную ей, если мы к одной из ее строк (или столбцов) прибавим линейную комбинацию других ее строк (или столбцов).

Это сводится к нескольким применениям преобразования 3.

Пусть матрица (1) имеет ранг r; преобразованием 1, т. е. перестановкою строк и перестановкою столбцов, мы можем заменить матрицу (1) такою, эквивалентною ей, у которой детерминант, составленный из первых r строк и первых r столбцов, будет отличен от нуля. Пусть это преобразование уже проделано, и значит

$$\begin{vmatrix} a_{11} & a_{12} & \dots & a_{1r} \\ a_{21} & a_{22} & \dots & a_{2r} \\ \dots & \dots & \dots & \dots \\ a_{r1} & a_{r2} & \dots & a_{rr} \end{vmatrix} \neq 0. \tag{4}$$

Возьмем элементы λ-й строки матрицы (1): $a_{\lambda 1}, a_{\lambda 2}, \dots, a_{\lambda n}$ $(\lambda > r)$ и заменим их, согласно преобразованию 3, такими:

$$a'_{\lambda 1} = a_{\lambda 1} - \sum_{\mu=1}^{r} a_{\mu 1} x_\mu, \quad a'_{\lambda 2} = a_{\lambda 2} - \sum_{\mu=1}^{r} a_{\mu 2} x_\mu, \quad \dots, \quad a'_{\lambda n} = a_{\lambda n} - \sum_{\mu=1}^{r} a_{\mu n} x_\mu.$$

$x_1, x_2, \dots, x_n$ — пока неопределенные величины, но мы их выберем так, чтобы было $a'_{\lambda 1} = a'_{\lambda 2} = \dots = a'_{\lambda n} = 0$; это сводится к решению системы n линейных уравнений

$$\sum_{\mu=1}^{r} a_{\mu\nu} x_\mu = a_{\lambda\mu}, \qquad (\nu = 1, 2, \dots, n)$$

с r неизвестными $x_1, x_2, \dots, x_r$; ранг этой системы равен r, причем необходимое и достаточное условие разрешимости этой системы здесь выполнено (§ 40, теорема 1). Таким образом мы достигнем того, что все элементы λ-й строки $\lambda > r$ обратятся в нуль. Эту операцию мы можем проделать для $\lambda = r+1, r+2, \dots, m$; тогда матрица (1) заменится такой эквивалентной ей:

$$\left.\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ \dots & \dots & \dots & \dots \\ a_{r1} & a_{r2} & \dots & a_{rn} \\ 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 \end{pmatrix}\right\} m - r \text{ строк}$$

Теперь берем λ-й столбец $(\lambda > r)$: $a_{1\lambda}, a_{2\lambda}, \dots, a_{r\lambda}, 0, \dots, 0$, заменяем ее такою:

$$a'_{1\lambda} = a_{1\lambda} - \sum_{\mu=1}^{r} a_{1\mu} x_\mu, \quad \dots, \quad a'_{r\lambda} = a_{r\lambda} - \sum_{\mu=1}^{r} a_{r\mu} x_m, \quad 0, \ \dots, \ 0,$$

и выбираем $x_1, x_2, \dots, x_r$ так, чтобы было $a'_{1\lambda} = a'_{2\lambda} = \dots = a'_{r\lambda} = 0$, что сводится к решению системы r уравнений

$$\sum_{\mu=1}^{r} a_{\nu\mu} x_\mu = a_{\varkappa\lambda} \qquad (\nu = 1, 2, \dots, r)$$

с r неизвестными $x_1 x_2, , \dots, x_r$, причем эта система разрешима, так как детерминант ее отличен от нуля. Проделывая это для $\lambda = r+1, r+2, \dots, n$, мы заменим

(1) эквивалентною ей матрицей:

$$A_1 = \left.\begin{pmatrix} a_{11} & \dots & a_{1r} & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ a_{r1} & \dots & a_{rr} & 0 & \dots & 0 \\ 0 & \dots & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & \underbrace{0 \quad \dots \quad 0}_{n-r \text{ столбцов}} \end{pmatrix}\right\} m-r \text{ строк} \tag{5}$$

причем выполнено условие (4), в силу чего в детерминанте (4) в каждой строке и в каждом столбце есть элементы, отличные от нуля. Вследствие этого преобразованием 1 мы можем всегда достигнуть того, чтобы было $a_{11} \neq 0$. В таком случае прибавляем ко 2-му столбцу 1-й, умноженный на $-\dfrac{a_{12}}{a_{11}}$, к 3-му столбцу 1-й, умноженный на $-\dfrac{a_{13}}{a_{11}}$, и т. д., — к r-му столбцу 1-й, умноженный на $-\dfrac{a_{1r}}{a_{11}}$; этим мы достигнем того, что 1-я строка примет вид: $a_{11}\ 0\ 0\ \dots\ 0$. Если теперь окажется, что $a_{22} = 0$ [причем новое a_{22}, а не то, которое было в (5); в обозначениях (5) это будет $a_{22} - \dfrac{a_{12}}{a_{11}}a_{21}$] то ведь во 2-м столбце есть какой-то элемент $a_{\lambda 2} \neq 0$ ($\lambda > 2$), и мы можем применить преобразование 1 и переставить 2-ю строку с λ-й. Таким образом, не нарушая общности, можно положить, что новое $a_{22} \neq 0$. Теперь прибавляем к 3-му столбцу 2-й, умноженный на $-\dfrac{a_{23}}{a_{22}}$, к 4-му столбцу 2-й, умноженный на $-\dfrac{a_{24}}{a_{22}}$ и т. д., к r-му столбцу 2-й, умноженный на $-\dfrac{a_{2r}}{a_{22}}$; этим мы достигнем того, что 2-я строка примет вид: $a_{21}\ a_{22}\ 0\ \dots\ 0$. Продолжая, далее, этот процесс, мы заменим матрицу (5) эквивалентною ей:

$$A_2 = \begin{pmatrix} a_{11} & 0 & \dots & 0 & 0 & \dots & 0 \\ a_{21} & a_{22} & \dots & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ a_{r1} & a_{r2} & \dots & a_{rr} & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \end{pmatrix}, \tag{6}$$

причем здесь все диагональные элементы $a_{11}, a_{22}, \dots, a_{rr}$ отличны от нуля. Теперь проделываем аналогичную операцию со строками: прибавляем ко 2-й строке 1-ю, умноженную на $-\dfrac{a_{21}}{a_{11}}$, к 3-й строке 1-ю, умноженную на $-\dfrac{a_{31}}{a_{11}}$ и т. д., к r-й строке 1-ю, умноженную на $-\dfrac{a_{r1}}{a_{11}}$; после этого прибавляем к 3-й строке 2-ю, умноженную на $-\dfrac{a_{32}}{a_{22}}$ и т. д., к r-й строке 2-ю, умноженную на $-\dfrac{a_{r2}}{a_{22}}$ и т. д. В результате матрицу

A_2 мы заменим эквивалентною ей матрицею:

$$A_3 = \begin{pmatrix} a_{11} & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & a_{22} & \dots & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & a_{rr} & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \end{pmatrix}. \tag{7}$$

Здесь $a_{11}, a_{22}, \dots, a_{rr}$ все отличны от нуля. Применяем теперь к (7) преобразование 2: 1-ю строку умножаем на $\dfrac{1}{a_{11}}$, 2-ю — на $\dfrac{1}{a_{22}}$ и т. д., r — на $\dfrac{1}{a_{rr}}$; этим мы матрицу A_3 заменим такою ей эквивалентною:

$$A_4 = \left.\begin{pmatrix} 1 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \end{pmatrix}\right\} \begin{matrix} r \text{ строк} \\ \\ \\ \\ \\ \\ m-r \text{ строк} \end{matrix} \tag{8}$$

$$\underbrace{}_{r \text{ столбцов}} \quad \underbrace{}_{\substack{n-r \\ \text{столбцов}}}$$

Итак, мы пришли к следующему результату:

Теорема. *Всякая mn-матрица ранга r эквивалентна матрице* (8).

Назовем матрицу (8) *нормальной mn*-матрицей ранга r заметим, что эта матрица — вполне определенная. Отсюда следует:

Теорема. *mn-матрицы, имеющие один и тот же ранг, эквивалентны друг другу.*

§ 155. Линейные подстановки. Композиция матриц. *Подстановкой* вообще называется замена одних переменных другими в данной функции или в данной формуле. Пусть, например, $F(x_1, x_2, \dots, x_n)$ данная функция от n переменных, и требуется переменные $x_1, x_2, \dots, x_n$ заменить переменными $y_1, y_2, \dots, y_n$, связанными с $x_1, x_2, \dots, x_n$ некоторыми соотношениями. Наиболее простым является случай, когда одни из переменных прямо заданы как функции других, например, $x_1, x_2, \dots, x_n$ заданы как функции от $y_1, y_2, \dots, y_n$:

$$x_1 = \varphi_1(y_1, y_2, \dots, y_n), \quad x_2 = \varphi_2(y_1, y_2, \dots, y_n), \ \dots,$$
$$x_n = \varphi_n(y_1, y_2, \dots, y_n).$$

Такой вид соотношений самый удобный, ибо он позволяет прямо подставить в F вместо x_k функции φ_k и сразу получить выражение F в виде функции от $y_1, y_2, \dots, y_n$. Заметим, что в предыдущих главах настоящего курса нам уже встречались различные частные случаи подстановок: например, преобразование Горнера (§ 55) есть подстановка $y = x - a$; преобразование Чирнгаузена (§ 146) есть

тоже подстановка: $v = a_0 + a_1 x + \ldots + a_{n-1} x^{n-1}$; наконец, выражение симметрической функции через элементарные симметрические функции (§ 138–140) есть тоже подстановка — переменных $f_1, x_2, \ldots, f_n$ вместо $x_1, x_2, \ldots, x_n$.

Мы рассмотрим частный случай подстановок, представляющий особый интерес, именно, случай, когда все функции $\varphi_1, \varphi_2, \ldots, \varphi_n$ являются линейными однородными функциями от $y_1, y_2, \ldots, y_n$; это — так называемые *линейные подстановки*. Общий вид линейной подстановки таков:

$$x_\lambda = \sum_{\lambda=1}^{n} a_{\varkappa\lambda} y_\lambda \qquad (\varkappa = 1, 2, \ldots, n). \tag{9}$$

Таким образом линейная подстановка n переменных представляет собою систему n линейных форм (9); их коэфициенты образуют квадратную матрицу n-го порядка:

$$A = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{pmatrix}. \tag{10}$$

Матрица (10) служит символом линейной подстановки (9); она вполне определяет линейную подстановку, ибо в последней важны значения коэфициентов, а обозначения переменных роли не играют. Если матрица A неособенная, т. е. если ее детерминант $|A| \neq 0$, то подстановка (9) называется *собственной*; в этом и только в этом случае все n форм (9) линейно независимы (§ 42), и уравнения (9) разрешимы относительно $y_1, y_2, \ldots, y_n$, т. е. можно, обратно, выразить $y_\varkappa$ через x_λ, причем, очевидно, $y_\varkappa$ будут тоже линейными формами от x_λ. Если же $|A| = 0$, то подстановка (9) *несобственная*, уравнения (9) вообще неразрешимы относительно $y_\varkappa$, эти уравнения связывают $x_1, x_2, \ldots, x_n$ друг с другом линейной зависимостью (§ 42), т. е. накладывают на них новое условие.

Предположим, что, произведя подстановку (9), мы заменяем $y_1, x_2, \ldots, y_n$ через новые переменные $z_1, z_2, \ldots, z_n$ посредством новой линейной подстановки:

$$y_\lambda = \sum_{\mu=1}^{n} b_{\lambda\mu} z_\mu \qquad (\lambda = 1, 2, \ldots, n); \tag{11}$$

матрицу ее коэфициентов обозначим через B, написав сокращенно:

$$B = (b_{\lambda\mu}).$$

Но если мы значения y_λ из (11) подставим в (9), то тем самым мы выразим $x_\varkappa$ непосредственно через z_μ:

$$x_\varkappa = \sum_{\lambda=1}^{n} a_{\varkappa\lambda} \sum_{\mu=1}^{n} b_{\lambda\mu} z_\mu = \sum_{\mu=1}^{n} z_\mu \sum_{\lambda=1}^{n} a_{\varkappa\lambda} b_{\lambda\mu},$$

или

$$x_\varkappa = \sum_{\mu=1}^{n} c_{\varkappa\mu} z_\mu \qquad (\varkappa = 1, 2, \ldots, n), \tag{12}$$

где

$$c_{\varkappa\mu} = \sum_{\lambda=1}^{n} = a_{\varkappa 1}b_{1\mu} + a_{\varkappa 2}b_{2\mu} + \ldots + a_{\varkappa n}b_{n\mu} \qquad (\varkappa, \mu = 1, 2, \ldots, n). \tag{13}$$

Формула (12) показывает, что $x_{\varkappa}$ — линейные формы от z_{μ}, коэфициенты которых даются формулой (13). Таким образом подстановка переменных z вместо x есть тоже линейная; она является, таким образом, композицией линейных подстановок (9) и (11). Матрица коэфициентов $c_{\varkappa\mu}$

$$C = (c_{\varkappa\mu})$$

является результатом композиции матриц A и B и обозначается символически как их «произведение»:

$$C = AB.$$

Формула (13) дает нам правило выполнения этого символического умножения; это — то же, что и закон составления произведения детерминантов по третьему способу § 31: комбинирование строк со столбцами. Остальные три способа составления произведения детерминантов, указанные в § 31, для нашего символического произведения матриц неверны, ибо в матрице мы не имеем права переставлять строки со столбцами. Из той же формулы (13) вытекает:

$$|C| = |A| \cdot |B|;$$

следовательно: *произведение неособенных матриц есть тоже неособенная матрица*, ибо при $|A| \neq 0$, $|B| \neq 0$ будет и $|C| \neq 0$.

Вообще же перемножать мы можем и особенные матрицы, лишь бы они были одного и того же порядка.

На примерах легко убедиться, что коммутативный закон вообще неверен для нашего умножения матриц:

$$AB \neq BA.$$

Но ассоциативный закон для умножения матриц, как мы сейчас докажем, верен:

$$(AB)C = A(BC) = ABC. \tag{14}$$

Пусть $A = (a_{\alpha\beta})$, $B = (b_{\alpha\beta})$, $C = (c_{\alpha\beta})$— три любые матрицы n-го порядка; обозначим

$$AB = P = p_{\alpha\beta}), \qquad BC = Q = q_{\alpha\beta}), \qquad (AB)C = PC = R = (r_{\alpha\beta}),$$

$$A(BC) = AQ = S = (s_{\alpha\beta}.$$

Тогда по (13)

$$p_{\alpha\beta} = \sum_{\varkappa=1}^{n} a_{\alpha\varkappa}b_{\varkappa\beta}, \qquad q_{\alpha\beta} = \sum_{\lambda=1}^{n} b_{\alpha\lambda}c_{\lambda\beta},$$

$$r_{\alpha\beta} = \sum_{\lambda=1}^{n} p_{\alpha\lambda}c_{\lambda\beta} = \sum_{\varkappa,\lambda} a_{\alpha\varkappa}b_{\varkappa\lambda}c_{\lambda\beta},$$

$$a_{\alpha\beta} = \sum_{\varkappa=1}^{n} a_{\alpha\varkappa}q_{\varkappa\beta} = \sum_{\varkappa,\lambda} a_{\alpha\varkappa}b_{\varkappa\lambda}c_{\lambda\beta},$$

т. е. $r_{\alpha\beta} = s_{\alpha\beta}$ при всех α и β; следовательно, $R = S$, и ассоциативный закон доказан.

§ 156. Понятие о композиции матриц распространяется и на случай прямоугольных матриц; однако не всякие две прямоугольные матрицы могут быть компонированы («перемножены») друг с другом: формула (13) требует, чтобы число столбцов множимого равнялось числу строк множителя; это условие, очевидно, и достаточно для возможности композиции двух матриц; результат этой композиции есть прямоугольная (в частном случае — квадратная) матрица, число строк которой то же, что и у множимого, а число столбцов — то же, что и у множителя. Таким образом, если A — mn-матрица, B — np-матрица, то ABВ — mp-матрица. Заметим, что из существования AB вовсе не следует существование BA; это последнее существует только при $m = p$; но тогда и AB и BA — квадратные матрицы, AВ — m-го порядка, BA — n-го порядка.

Пример.

$$\begin{pmatrix} 1 & 3 & 2 & -1 \\ 5 & -1 & 6 & 2 \\ -3 & 1 & 0 & 4 \end{pmatrix} \cdot \begin{pmatrix} 5 & 3 \\ 1 & 0 \\ 2 & -1 \\ 3 & 4 \end{pmatrix} = \begin{pmatrix} 9 & -3 \\ 42 & 17 \\ -2 & 7 \end{pmatrix}.$$

Ассоциативный закон, очевидно, верен и для композиции прямоугольных матриц; его здесь можно формулировать так:

Если A, B, C — прямоугольные (в частности квадратные) матрицы и если существуют AB и BC, то существуют и $(AB)C$ и $A(BC)$, причем

$$(AB)C = A(BC),$$

так что можно писать просто без скобок ABC.

Доказывается это совершенно так же, как и для квадратных матриц, так что мы это доказательство опускаем.

Рассмотрим частный случай умножения mn-матрицы на $(n, 1)$-матрицу (или на «столбец»); пусть

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots\dots\dots\dots\dots\dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}, \qquad (x) = \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix};$$

в результате перемножения получается $(m, 1)$-матрица $(y) = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_m \end{pmatrix}$; но по формуле (13)

$$y_\alpha = \sum_{\beta=1}^{n} = a_{\alpha\beta} x_\beta, \qquad \alpha = 1, 2, \dots, m.$$

Таким образом матричная формула:

$$(y) = A(x) = \tag{15}$$

выражает совокупность m линейных форм от n переменных. При mn формула (15) выражает просто линейную подстановку, только обычно мы выражаем x через y, т. е. (меняя обозначение) берем эту подстановку в виде:

$$(x) = A(y);$$

если в свою очередь $(y) = B(z)$, где B — тоже матрица n-го порядка, то, подставляя, найдем:

$$(x) = A(B(z)) = AB(z);$$

эта формула, определяющая «произведение» матриц AB, выражает в сущности частный случай ассоциативного закона.

Докажем теперь следующую теорему:

Теорема. *Ранг произведения нескольких матриц не может быть выше ранга каждого из сомножителей.*

Эта теорема относится как к квадратным, так и к прямоугольным матрицам.

Доказательство. Достаточно доказать теорему для произведения двух сомножителей. Пусть $A = (a_{\alpha\beta})$, $B = (b_{\alpha\beta})$, $C = AB = (c_{\alpha\beta})$; A — mn-матрица, B — np-матрица; тогда C — mp-матрица и по (13):

$$c_{\alpha\beta} = \sum_{\lambda=1}^{n}, a_{\alpha\lambda} b_{\lambda\beta} \qquad , \alpha = 1, 2, \ldots, m,\ \beta = 1, 2, \ldots, p.$$

Возьмем некоторый детерминант k-го порядка детерминанта C:

$$\mathbf{\Gamma} = \begin{vmatrix} c_{\alpha_1\beta_1} & c_{\alpha_1\beta_2} & \ldots & c_{\alpha_1\beta_k} \\ c_{\alpha_1\beta_1} & c_{\alpha_2\beta_2} & \ldots & c_{\alpha_2\beta_k} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ c\alpha_k\beta_1 & c_{\alpha_k\beta_2} & \ldots & c_{\alpha_k\beta_k} \end{vmatrix};$$

здесь $\alpha_1, \alpha_2, \ldots, \alpha_k$ — некоторые k из номеров $1, 2, \ldots, m$, а $\beta_1, \beta_2, \ldots, \beta_k$, — некоторые k из номеров $1, 2, \ldots, p$. Рассмотрим теперь также две матрицы:

$$\mathbf{A} = \begin{pmatrix} a_{\alpha_1 1} & a_{\alpha_1 2} & \ldots & a_{\alpha_1 n} \\ a_{\alpha_2 1} & a_{\alpha_2 2} & \ldots & s_{\alpha_2 n} \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ a_{\alpha_k 1} & a_{\alpha_k 2} & \ldots & a_{\alpha_k n} \end{pmatrix}, \qquad \mathbf{B} = \begin{pmatrix} b_{1\beta_1} & b_{2\beta_1} & \ldots & b_{n\beta_1} \\ b_{1\beta_2} & b_{2\beta_2} & \ldots & b_{n\beta_n} \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ b_{1\beta_k} & b_{2\beta_k} & \ldots & b_{n\beta_k} \end{pmatrix}.$$

Применив к детерминанту $\mathbf{\Gamma}$ и к матрицам $\mathbf{A}$ и $\mathbf{B}$ обобщенную теорему умножения (§ 38), мы убедимся, что $\mathbf{\Gamma}$ представится как сумма произведений детерминантов k-го порядка матрицы $\mathbf{A}$ на соответствующие детерминанты k-го порядка матрицы $\mathbf{B}$; но детерминанты k-го порядка матрицы $\mathbf{A}$ являются в то же время детерминантами k-го порядка и матрицы A, а детерминанты k-го порядка матрицы $\mathbf{B}$ — детерминантами и матрицы B, если только переставить строки со столбцами, отчего численные их значения не меняются. Если теперь k больше ранга матрицы A или матрицы B, то детерминанты k-го порядка матрицы A или B равны нулю, но тогда и $\Gamma = 0$, т. е. и все детерминанты k-го порядка матрицы C равны нулю. Этим наша теорема доказана.

Упражнения

198) Перемножить подстановки $A = \begin{pmatrix} 2 & 3 \\ 1 & 5 \end{pmatrix}$, $B = \begin{pmatrix} 4 & 2 \\ 1 & 3 \end{pmatrix}$.

Отв. $AB = \begin{pmatrix} 11 & 13 \\ 9 & 17 \end{pmatrix}$, $BA = \begin{pmatrix} 10 & 22 \\ 5 & 18 \end{pmatrix}$.

199) Перемножить подстановки

$$A = \begin{pmatrix} 5 & -1 & 2 \\ 3 & 5 & 0 \\ 1 & 4 & 1 \end{pmatrix}, \qquad B = \begin{pmatrix} 5 & 9 & -10 \\ -3 & 3 & 6 \\ 7 & -21 & 28 \end{pmatrix}.$$

Отв. $AB = BA = \begin{pmatrix} 42 & 0 & 0 \\ 0 & 42 & 0 \\ 0 & 0 & 42 \end{pmatrix}$.

200) Перемножить подстановки $A = \begin{pmatrix} 5 & 1 & 0 & 3 \\ 2 & 4 & 5 & 3 \end{pmatrix}$, $B = \begin{pmatrix} 4 & 2 \\ -2 & 4 \\ 1 & 3 \\ 1 & -5 \end{pmatrix}$.

Отв. $AB = \begin{pmatrix} 21 & -1 \\ 8 & 12 \end{pmatrix}$, $BA = \begin{pmatrix} 24 & 12 & 10 & 18 \\ -2 & 14 & 20 & 6 \\ 11 & 13 & 15 & 12 \\ -5 & -19 & -25 & -12 \end{pmatrix}$.

201) На матрицах

$$A = \begin{pmatrix} 3 & -1 & 5 \\ 1 & 2 & 4 \\ 3 & 2 & -1 \end{pmatrix}, \qquad B = \begin{pmatrix} 4 & 3 & 1 \\ 3 & 1 & 2 \\ -1 & -2 & 1 \end{pmatrix}, \qquad C = \begin{pmatrix} 4 & 3 & 2 \\ -2 & 1 & -1 \\ 3 & 1 & 1 \end{pmatrix}$$

проверить ассоциативный закон [т. е. выяснить, что $(AB)C = A(BC)$].

202) Проверить ассоциативный закон на матрицах

$$A = \begin{pmatrix} 4 & 1 & 2 & -1 \\ 2 & 3 & 1 & 0 \end{pmatrix}, \qquad B = \begin{pmatrix} 4 & 2 & -1 \\ -1 & 2 & 5 \\ 1 & 1 & 3 \\ -5 & 3 & 0 \end{pmatrix}, \qquad C = \begin{pmatrix} -1 & 0 \\ 2 & 5 \\ 0 & 3 \end{pmatrix}.$$

Отв. $ABC = \begin{pmatrix} -4 & 66 \\ 16 & 103 \end{pmatrix}$.

§ 157. Обратные подстановки и матрицы. Если линейная подстановка (9) собственная (§ 155), т. е. матрица (10) неособенная, то мы можем систему уравнений (9) решить относительно y, т. е. выразить эти новые переменные y через старые переменные x . По § 33 находим:

$$y_\lambda = \frac{1}{|A|} \sum_{\varkappa=1}^{n} A_{\varkappa\lambda} x_\lambda \qquad (\lambda = 1, 2, \ldots, n); \tag{16}$$

здесь $|A|$ — детерминант матрицы $A = (a_{\varkappa\lambda})$; он не равен нулю; $A_{\varkappa\lambda}$ — миноры $(n-1)$-го порядка детерминанта $|A|$. Мы видим, что y_λ в свою очередь тоже линейные формы от $x_\varkappa$, т. е. (16) дает новую линейную подстановку, так называемую

обратную к (9). Ее матрица называется *обратной матрицей* к A и обозначается A^{-1}. Имеем:

$$A^{-1} = \begin{pmatrix} \frac{A_{11}}{|A|} & \frac{A_{21}}{|A|} & \dots & \frac{A_{n1}}{|A|} \\ \frac{A_{12}}{|A|} & \frac{A_{22}}{|A|} & \dots & \frac{A_{n2}}{|A|} \\ \dots\dots\dots\dots\dots\dots\dots\dots \\ \frac{A_{1n}}{|A|} & \frac{A_{2n}}{|A|} & \dots & \frac{A_{nn}}{|A|} \end{pmatrix}. \tag{17}$$

По формуле для взаимного детерминанта (§ 32) находим:

$$|A^{-1} = \frac{1}{|A|^n} \begin{pmatrix} A_{11} & A_{21} & \dots & A_{n1} \\ A_{12} & A_{22} & \dots & A_{n2} \\ \dots\dots\dots\dots\dots\dots\dots\dots \\ A_{1n} & A_{2n} & \dots & A_{nn} \end{pmatrix} = \frac{|A|^{n-1}}{|A|^n} = \frac{1}{|A|}.$$

Заметим, что обратная матрица существует только у неособенной, матрицы, и сама она тоже неособенная, ибо $\dfrac{1}{|A|} \neq 0$.

Если мы в данной функции сделаем подстановку (9), а затем обратную к ней подстановку (16), то снова вернемся к первоначальным переменным, т. е. ничего не изменим, или сделаем тождественную подстановку $x_1 = x_1$, $x_2 = x_2$, …, $x_n = x_n$; ее матрица обычно обозначается буквою E и имеет вид:

$$E = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \dots\dots\dots\dots\dots \\ 0 & 0 & \dots & 1 \end{pmatrix}, \tag{18}$$

т. е. у нее вдоль диагонали стоят единицы, а остальные элементы все равны нулю; она называется *единичной* матрицей, ибо, как мы увидим ниже, при композиции матриц она играет роль единицы. Матрица E — неособенная; очевидно, $|E| = 1$. Очевидно, также, что $E^{-1} = E$.

Непосредственным перемножением по формулам (13) проверяем, что действительно:

$$AA^{-1} = E \tag{19}$$

для всякой неособенной матрицы A. Это равенство также может служить для определения A^{-1} для данной (неособенной) матрицы A; позже мы увидим, что при данном A обратная к A матрица определяется однозначно.

Далее, легко проверить для всякой (т. е. в том числе и особенной) матрицы A [75], что

$$AE = EA = A. \tag{20}$$

Это и показывает, что E играет роль единицы при нашем умножении матриц. Мы видим, кроме того, что при умножении на E верен также и коммутативный закон;

[75] С точки зрения линейных подстановок формула (20) совершенно очевидна: ведь произвести тождественную подстановку E значит ничего не изменить, а следовательно, подстановка AE, равно как и EA, сводится к одной только подстановке A.

это выражают, говоря, что матрица E переместима со всякой другой квадратной матрицей того же порядка.

Пусть опять A — неособенная, а B и C — любые матрицы n-го порядка, и мы имеем:

$$BA = CA;$$

умножая обе части этого равенства справа на A^{-1} и применяя ассоциативный закон, получим:

$$B(AA^{-1}) = C(AA^{-1}),$$

и по (19) $BE = CE$, или по (20)

$$B = C.$$

Мы вывели не что иное, как левую сторону закона однозначной обратимости (§ 191). Умножим теперь обе части равенства (19) слева на A^{-1}:

$$A^{-1}(AA^{-1}) = A^{-1}E;$$

на основании (20) и ассоциативного закона можно написать:

$$(A^{-1}A)A^{-1} = EA^{-1},$$

а так как A^{-1} — неособенная матрица, то на основании доказанной левой стороны закона однозначной обратимости

$$A^{-1}A = E,$$

или, в соединении с (19)

$$AA^{-1} = A^{-1}A = E. \qquad (19a)$$

Это говорит, во-первых, что всякая неособенная матрица переместима со своей обратной; во-вторых, что свойство обратимости — взаимное, т. е. обратная матрица к A^{-1} есть снова A, или

$$(A^{-1})^{-1} = A.$$

В-третьих, (19а) позволяет доказать и правую сторону закона однозначной обратимости; именно, пусть

$$AB = AC;$$

отсюда

$$(A^{-1}A)B = (A^{-1}A)C, \qquad EB = EC, \quad \text{или} \quad B = C.$$

Докажем теперь, что для неособенных матриц верен и закон неограниченной обратимости (§ 4, гл. 1). Пусть A — неособенная, а B — любая матрица; легко видеть, что уравнения

$$AX = B \quad \text{и} \quad YA = B$$

имеют решения:

$$X = A^{-1}B, \qquad Y = BA^{-1};$$

что эти решения единственные, следует из закона однозначной обратимости.

Мы видим, что законы неограниченной и однозначной обратимости распространимы без ограничений только на неособенные матрицы.

Из всего предыдущего видно, что для композиции неособенных матриц данного порядка верны все основные законы групп (§ 27); так как, кроме того, произведение неособенных матриц всегда есть тоже неособенная матрица (§ 155), то все неособенные матрицы данного порядка образуют группу относительно своего символического умножения; конечно, эта группа бесконечна. Но внутри этой общей группы имеется еще бесчисленное множество подгрупп.

Так, все неособенные матрицы данного порядка, элементы которых вещественны, образуют группу;

все неособенные матрицы данного порядка, элементы которых рациональны, образуют группу;

все неособенные матрицы данного порядка, элементы которых принадлежат данному телу P, образуют группу;

все неособенные матрицы данного порядка с детерминантами, равными единице, составляют группу и т. д.

Упражнения

203) Найти обратную к матрице $\begin{pmatrix} 3 & -1 & 2 \\ 1 & 4 & -3 \\ 2 & 2 & 1 \end{pmatrix}$.

Отв. $\begin{pmatrix} \frac{2}{5} & \frac{2}{5} & -\frac{1}{5} \\ -\frac{7}{25} & -\frac{1}{25} & \frac{11}{25} \\ -\frac{6}{25} & -\frac{8}{25} & \frac{13}{25} \end{pmatrix}$.

204) Найти обратную к матрице $\begin{pmatrix} 1 & -2 & -1 \\ 3 & 1 & 2 \\ 1 & 2 & 2 \end{pmatrix}$.

Отв. $\begin{pmatrix} -2 & 2 & -3 \\ -4 & 3 & -5 \\ 5 & -4 & 7 \end{pmatrix}$.

205) Решить уравнения $AX = B$, $YA = B$, где $A = \begin{pmatrix} 3 & 4 \\ 1 & 8 \end{pmatrix}$, $B = \begin{pmatrix} 2 & 1 \\ 3 & 6 \end{pmatrix}$.

Отв. $X = \frac{1}{20}\begin{pmatrix} 4 & -16 \\ 7 & 17 \end{pmatrix}$, $Y = \frac{1}{20}\begin{pmatrix} 15 & -5 \\ 18 & 6 \end{pmatrix}$.

§ 158. Степени матрицы. Переместимые матрицы. Умножая квадратную матрицу на самое себя, мы получаем степени: $AA = A^2$, $A^2A = A^3$, $\dots A^{m-1}A = A^m$; таких степеней вообще бесчисленное множество. Естественно положить по определению $A^1 = A$. На основании ассоциативного закона имеем:

$$A^m = \underbrace{AA\cdots A}_{m \text{ раз}};$$

далее:

$$A^\alpha A^\beta = A^\beta A^\alpha = A^{\alpha+\beta}, \tag{21}$$

т. е. *две степени одной и той же матрицы всегда переместимы*; здесь коммутативный закон является следствием ассоциативного. Из (21) легко следует:

$$(A^\alpha)^\beta = A^{\alpha\beta}.$$

Переходя специально к рассмотрению неособенных матриц, докажем следующую формулу:

$$(ABC\cdots)^{-1} = (\cdots C^{-1}B^{-1}A^{-1}, \tag{22}$$

т. е. *матрица, обратная произведению, равна произведению матриц, обратных сомножителям, взятых в обратном порядке.*

Действительно, например, для трех сомножителей:

$$(ABC)(C^{-1}B^{-1}A^{-1}) = (AB)(CC^{-1})(B^{-1}A^{-1}) = ABEB^{-1}A^{-1} =$$
$$= ABB^{-1}A^{-1} = AEA^{-1} = AA^{-1} = E;$$

следовательно:

$$C^{-1}B^{-1}A^{-1} = (ABC)^{-1}.$$

Из (22) при $A = B = C = \ldots$, если число сомножителей m, получаем:

$$(A^m)^{-1} = (A^{-1})^m;$$

естественно обозначить:

$$(A^m)^{-1} = (A^{-1})^m = A^{-m}. \tag{23}$$

Так определяются отрицательные степени неособенной матрицы. Наконец, естественно определить

$$A^0 = E \tag{24}$$

для неособенной матрицы A.

Докажем теперь, что формулы (21) и (22) верны для любых целых показателей ($\neq 0$). Пусть α и $\beta > 0$; имеем:

$$(A^{-1})^\alpha (A^{-1})^\beta = (A^{-1})^\beta (A^{-1})^\alpha = (A^{-1})^{\alpha+\beta}$$

или по (23)

$$A^{-\alpha}A^{-\beta} = A^{-\beta}A^{-\beta} = A^{-\alpha-\beta}.$$

Пусть $\alpha > \beta$; имеем:

$$A^\alpha A^{-\beta} = A^{\alpha-\beta}(A^\beta A^{-\beta}) = A^{\alpha-\beta}E = A^{\alpha-\beta},$$

$$A^{-\beta}A^\alpha = A^{-\beta}A^\beta A^{\alpha-\beta} = EA^{\alpha-\beta} = A^{\alpha-\beta};$$

если $\alpha < \beta$, то вместо A берем A^{-1}.

Далее по (23):

$$(A^\alpha)^\beta = [(A^{-1})^\alpha]^\beta = (A^{-1})^{\alpha\beta} = A^{-\alpha\beta},$$
$$(A^\alpha)^{-\beta} = [(A^\alpha)^\beta]^{-1} = (A^{\alpha\beta})^{-1} = A^{-\alpha\beta},$$
$$(A^{-\alpha})^{-\beta} = \{[(A^{-1})^\alpha]^\beta\}^{-1} = [(A^{-1})^{\alpha\beta}]^{-1} = [(A^{-1})^{-1}]^\alpha\beta = A^{\alpha\beta}.$$

Заметим еще, что $E^2 = E$ к вообще $E^\alpha = E$ при любом целом α.

Из предыдущего следует, что все (положительные, нулевая и отрицательные) степени неособенной матрицы A образуют группу (вообще бесконечную); эта группа называется *циклической*. Заметим, что одни только положительные степени матрицы группы не составляют, несмотря на свойство (21); совокупность всех положительных степеней матрицы образуют *полугруппу* (§ 211).

Рассмотрим теперь переместимые матрицы [76].

Теорема. *Если неособенные матрицы A и B переместимы, то A переместимо с B^{-1}, A^{-1} — с B, A^{-1} — с B^{-1}, и уравнения $AX = B$ и $YA = B$ имеют одно и то же решение.*

Доказательство. Обе части равенства $AB = BA$ умножаем слева и справа на B^{-1}:

$$B^{-1}ABB^{-1} = B^{-1}BAB^{-1},$$

или

$$B^{-1}AE = EAB^{-1},$$

$$B^{-1}A = AB^{-1}.$$

Подобным же образом докажем, что A^{-1} переместимо с B и с B^{-1}. В § 157 мы имели $X = A^{-1}B$, $Y = BA^{-1}$; теперь мы видим, что $X = y$. Можно просто обозначить

$$X = Y = \frac{B}{A}.$$

Упражнения

206) $A = \begin{pmatrix} 1 & 3 \\ 5 & -2 \end{pmatrix}$; найти A^2, A^3, A^{-1}, A^{-2}.

Отв. $\begin{pmatrix} 16 & -3 \\ -5 & 19 \end{pmatrix}$, $\begin{pmatrix} 1 & 54 \\ 90 & -53 \end{pmatrix}$, $\begin{pmatrix} \frac{2}{17} & \frac{3}{17} \\ \frac{5}{17} & -\frac{1}{17} \end{pmatrix}$, $\begin{pmatrix} \frac{19}{289} & \frac{3}{289} \\ \frac{5}{289} & \frac{16}{289} \end{pmatrix}$.

207) Найти степени матрицы $I = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

Отв. Их только четыре различных:

$$I, \qquad I^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad I^3 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \qquad I^4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

208) Найти степени матрицы $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.

Отв. $A^\alpha = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$ при $\alpha \neq 0$.

209) Даны матрицы $A = \begin{pmatrix} 1 & 2 & -1 \\ 0 & 1 & 3 \\ 3 & 2 & 4 \end{pmatrix}$ и $B = \begin{pmatrix} -6 & -6 & 5 \\ 9 & 3 & 3 \\ 3 & 8 & 4 \end{pmatrix}$; проверить, что они переместимы, а также, что A переместимо с B^{-1}, B — с A^{-1}, и A^{-1} с B^{-1}.

[76] Если матрицы переместимы, то говорят также, что они коммутируют друг с другом.

§ 159. Обобщения для прямоугольных матриц. Будем индексом при обозначении единичной матрицы указывать ее порядок; так, E_n есть единичная матрица n-го порядка.

Непосредственной проверкой легко убедиться, что *для mn-матрицы E_m есть левая единица, а E_n — правая единица.*

Пусть K nm-матрица ранга n; в таком случае можно бесчисленным множеством способов найти такую mn-матрицу L ранга n, что будет

$$KL = E_n. \tag{25}$$

Обратно, при данном L (ранга n) K определяется бесконечно многозначно. (Из того, что K ранга n, следует, конечно, что $m > n$.)

Пусть $K = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1m} \\ a_{21} & a_{22} & \dots & a_{2m} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nm} \end{pmatrix}$; обозначим $L = \begin{pmatrix} x_{11} & x_{12} & \dots & x_{1n} \\ x_{21} & x_{22} & \dots & x_{2n} \\ \dots & \dots & \dots & \dots \\ x_{m1} & x_{m2} & \dots & x_{mn} \end{pmatrix}$, где $x_{\alpha\beta}$ пока неизвестны. Условие (25) дает (по (13))

$$\sum_{\lambda=1}^{m} a_{\alpha\lambda} x_{\lambda\beta} = e_{\alpha\beta} \qquad (\alpha, \beta = 1, 2, \dots, n), \tag{26}$$

(как и в § 32) означает единицу при $\alpha = \beta$ и нуль при $\alpha \neq \beta$. При данном индексе β (26) представляет систему n уравнений с m неизвестными $x_{1\beta}, x_{2\beta}, \dots, x_{m\beta}$; ранг этой системы n, поэтому она имеет решения (§ 40). Такую систему мы имеем при каждом β. Так как $m > n$, то степень неопределенности системы $m - n \geq 1$ (§ 41), т. е. при каждом β мы имеем бесчисленное множество систем решений; следовательно, матрица L в (25) определяется при всяком данном K и при этом бесконечным множеством способов.

Совершенно аналогично, считая $x_{\alpha\beta}$ данными, а $a_{\alpha\beta}$ искомыми, мы докажем, что, при данном L, K определяется бесконечно многозначно.

Обобщим теперь доказанную теорему. Пусть A_n — любая матрица n-го порядка; $A_n K$ существует и есть mn-матрица; точно так же LA_n существует и есть mn-матрица, и из (25), так как $A_n E_n = E_n A_n = A_n$, получаем:

$$(A_n K)L = K(LA_n) = A_n,$$

или *при данной матрице n-го порядка A_n и при данной nm-матрице (или mn-матрице) K (или L) ранга n можно всегда найти бесчисленным множеством способов mn-матрицу L_1 (или nm-матрицу K_1) так, что будет*

$$KL_1 = A_n \qquad (\textit{или} \quad K_1 L = A_n).$$

Пример. Пусть $n = 2$, $m = 3$, $K = \begin{pmatrix} 5 & 1 & -2 \\ 1 & 0 & -3 \end{pmatrix}$; найдем L согласно (25). Здесь $E_2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$; пусть

$$L = \begin{pmatrix} x_1 & y_1 \\ x_2 & y_2 \\ x_3 & y_3 \end{pmatrix},$$

тогда имеем по (26):

$$\begin{cases} 5x_1 + x_2 - 2x_3 = 1, \\ x_1 - 3x_3 = 0, \end{cases} \qquad \begin{cases} 5y_1 + y_2 - 2y_3 = 0, \\ y_1 - 3y_3 = 1. \end{cases}$$

Эти системы дают решения:

$$x_1 = 3u, \qquad x_2 = 1 - 13u, \qquad x_3 = u,$$
$$y_1 = 1 + 3v, \quad y_2 = -5 - 13v, \quad y_3 = v,$$

где u и v произвольные параметры. Взяв, например, $u = 0$, $v = 1$, получим:

$$L = \begin{pmatrix} 0 & 4 \\ 1 & -18 \\ 0 & 1 \end{pmatrix}.$$

Предыдущая теорема может быть еще более обобщена: *пусть K данная mn-матрица n-го ранга, а A — любая np-матрица; в таком, случае можно бесчисленным множеством способов найти mp-матрицу L_1 так, что будет*

$$KL_1 = A.$$

Если L -—- данная mn-матрица ранга n $(m > n)$, а B — любая pn-матрица, то можно бесчисленным множеством способов найти pm-матрицу K_1, так, что будет

$$K_1 L = B.$$

Практически, как мы сейчас покажем на примере, находя L_1 или K_1 , нам нет надобности исходить из уравнения (25) и умножать найденное решение L справа на A или найденное решение K слева на B.

Пример. Пусть $m = 4$, $n = 2$, $p = 3$, $L = \begin{pmatrix} 6 & 1 \\ 3 & 2 \\ -1 & 3 \\ 5 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 2 & 5 \\ 4 & 10 \\ -2 & -5 \end{pmatrix}$; найдем K_1 так, чтобы было $K_1 L = B$.

Пусть $K_1 = \begin{pmatrix} x_1 & x_2 & x_3 & x_4 \\ y_1 & y_2 & y_3 & y_4 \\ z_1 & z_2 & z_3 & z_4 \end{pmatrix}$; тогда, находя по (13) произведение K_1 на L и приравнивая его B, найдем такие системы уравнений:

$$\begin{cases} 6x_1 + 3x_2 - x_3 + 5x_4 = 2, \\ x_1 + 2x_2 + 3x_3 = 5, \end{cases} \qquad \begin{cases} 6y_1 + 3y_2 - y_3 + 5y_4 = 4, \\ y_1 + 2y_2 + 3y_3 = 10, \end{cases}$$

$$\begin{cases} 6z_1 + 3z_2 - z_3 + 5z_4 = -2, \\ z_1 + 2z_2 + 3z_3 = -5. \end{cases}$$

Первая система дает $x_1 = 5 - 2x_2 - 3x_3$, $x_4 = \frac{1}{5}(9x_2 + 19x_3 - 28)$; x_2 и x_3 произвольны; точно так же, вторая и третья системы дадут: $y_1 = 10 - 2y_2 - 3y_3$, $y_4 = \frac{1}{5}(9y_2 +$

$19y_3 - 56$); y_2 и y_3 произвольны; $z_1 = -5 - 2z_2 - 3z_3$, $z_4 = \frac{1}{5}(9z_2 + 19z_3 + 28)$; z_2 и z_3 произвольны.

Берем, например, $x_2 = x_3 = 1$, $y_2 = -2$, $y_3 = 1$, $z_2 = 1$, $z_3 = 2$; тогда получим: $x_1 = x_4 = 0$, $y_1 = 11$, $y_4 = -11$, $z_1 = -13$, $z_4 = 15$, откуда

$$K_1 = \begin{pmatrix} 0 & 1 & 1 & 0 \\ 11 & -2 & 1 & -11 \\ -13 & 1 & 2 & 15 \end{pmatrix}.$$

§ 160. Транспонированная матрица. Если мы в данной матрице A переставим строки с колоннами, то получим новую матрицу A'; *транспонированную* относительно A [77]. Очевидно, что транспонированная для A' будет снова A, т. е. $(A')' = A$. Если A mn-матрица, то A' — nm-матрица; обе матрицы A и A' имеют один и тот же ранг. Если A квадратная матрица n-го порядка, то и A' тоже, и очевидно

$$|A'| = |A|;$$

в частности A и A' одновременно неособенные или одновременно особенные.

Теорема. *Если A компонируется с B, то B' компонируется с A' и $(AB)' = B'A'$.*

Доказательство. Пусть A mn-матрица, B np-матрица;

$$A = (a_{\alpha\beta} \qquad (\alpha = 1, 2, \ldots, m,\ \beta = 1, 2, \ldots, n),$$

$$B = (b_{\varkappa\lambda}) \qquad (\varkappa = 1, 2, \ldots, n,\ \lambda = 1, 2, \ldots, p);$$

тогда B' — pn-матрица, A' — nm-матрица, т. е. B' действительно компонируется с A'. Пусть, далее:

$$AB = (c_{\alpha\beta}) \qquad (\alpha = 1, 2, \ldots, m,\ \beta = 1, 2, \ldots, p),$$

$$B/A/ = (d_{\alpha\beta}) \qquad (\alpha = 1, 2, \ldots, p,\ \beta = 1, 2, \ldots, m);$$

тогда по (12)

$$c_{\alpha\beta} = \sum_{\lambda=1}^{m} a_{\alpha\lambda} b_{\lambda\beta},$$

$$d_{\beta\alpha} = \sum_{\lambda=1}^{m} b_{\lambda\beta} a_{\alpha\lambda},$$

т. е. действительно $c_{\alpha\beta} = d_{\beta\alpha} =$, что и показывает, что $B'A'$ получается из AB перестановкой строк со столбцами.

Выведенная формула, конечно, непосредственно обобщается и на несколько сомножителей:

$$(ABC\cdots)' = \cdots C'B'A'.$$

Следствие 1. Если $KL = E_n$, где E_n — единичная матрица n-го порядка, то $L'K' = E_n$. Это следует из того очевидного факта, что $E_n' = E_n$. В частности, если A — квадратная неособенная матрица, то

$$(A')^{-1} = (A^{-1})', \tag{27}$$

[77] Некоторые авторы называют матрицу A' сопряженною с матрицей A.

ибо раз $AA^{-1} = E$, то и $(A^{-1})'A' = E$, откуда и следует (27).

Следствие 2. Если A и B квадратные переместимые матрицы, то и A' и B' переместимы, и $(AB)' = A'B'$, $\left(\frac{B}{A}\right)' = \frac{B'}{A'}$ (причем в последнем случае предполагается, что матрица A — неособенная).

Это следует из того, что $(AB)' = B'A'$, $(BA)' = A'B'$, а так как $AB = BA$, то и $A'B' = B'A'$. Но тогда переместимы и B с A^{-1} (см. теорему в конце § 158); следовательно, $(BA^{-1})' = B'(A^{-1})' = B'(A')^{-1}$, т. е. $\frac{B}{A} = \frac{B'}{A'}$.

§ 161. Связь матриц с подстановками n символов. В § 26 мы ввели понятие о подстановках n символов и об их композиции. Сейчас мы покажем, что эти подстановки n символов можно рассматривать как частные случаи линейных подстановок, а следовательно, и матриц. Действительно, подстановку n символов можно рассматривать как перестановку наших переменных $x_1, x_2, \ldots, x_n$, или как перемену их нумерации. Так, например, подстановку $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 4 & 3 \end{pmatrix}$ можно толковать так, что x_1 получает теперь 5-й номер, x_2 — 1-й номер, x_3 — 2-й номер, x_4 остается со своим номером 4-м, x_5 получает 3-й номер; иными словами, мы делаем такую линейную подстановку:

$$\begin{aligned}
x_1 = y_5 &= 0 \cdot y_1 + 0 \cdot y_2 + 0 \cdot y_3 + 0 \cdot y_4 + 1 \cdot y_5, \\
x_2 = y_1 &= 1 \cdot y_1 + 0 \cdot y_2 + 0 \cdot y_3 + 0 \cdot y_4 + 0 \cdot y_5, \\
x_3 = y_2 &= 0 \cdot y_1 + 1 \cdot y_2 + 0 \cdot y_3 + 0 \cdot y_4 + 0 \cdot y_5, \\
x_4 = y_4 &= 0 \cdot y_1 + 0 \cdot y_2 + 0 \cdot y_3 + 1 \cdot y_4 + 0 \cdot y_5, \\
x_5 = y_3 &= 0 \cdot y_1 + 0 \cdot y_2 + 1 \cdot y_3 + 0 \cdot y_4 + 0 \cdot y_5,
\end{aligned}$$

ей соответствует матрица:

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

В этой матрице, как мы видим, в каждой строке и в каждой колонне все элементы равны нулю кроме одного, который равен единице. Детерминант такой матрицы сводится к одному члену — произведению этих единиц, взятому со знаком $+$ или $-$, смотря по тому, образуют ли номера мест этих единиц по строкам четную или нечетную перестановку. Например, в данном случае эти номера

$$5 \quad 1 \quad 2 \quad 4 \quad 3$$

образуют перестановку, совпадающую с нижней строкой данной подстановки $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 4 & 3 \end{pmatrix}$ это, конечно, будет и в общем случае; но четность или нечетность нижнего расположения совпадает с четностью или нечетностью самой подстановки; следовательно, можно заключить: *детерминант матрицы, представляющей данную подстановку n символов, равен $+1$, если подстановка четная, и -1, если подстановка нечетная.*

(В данном примере этот детерминант равен -1).

Что произведению подстановок соответствует произведение соответствующих матриц, совершенно очевидно: ведь матрица есть символ линейной подстановки, а подстановки n символов мы и толковали, как частный случай линейной подстановки, и композиция двух подстановок n символов сведется к композиции соответствующих линейных подстановок, т. е. их матриц.

Укажем еще, какая матрица соответствует транспозиции $(\varkappa, \lambda)$ (§ 23); это будет, именно, матрица

$$F_{\varkappa\lambda} = \begin{pmatrix} 1 & 0 & \dots & 0 & \dots & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 & \dots & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & \dots & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & \dots & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & \dots & 0 & \dots & 1 \end{pmatrix} \begin{matrix} \\ \\ \\ \varkappa\text{-я строка} \\ \\ \lambda\text{-я строка} \\ \\ \\ \end{matrix} \tag{28}$$

$$\begin{matrix} \varkappa\text{-й} & \lambda\text{-й} \\ \text{столбец} & \text{столбец;} \end{matrix}$$

иными словами, эта матрица получается из E, если в E переставим друг с другом $\varkappa$-ю и λ-ю строки (или, что то же, $\varkappa$-й и λ-й столбцы).

§ 162. Новое истолкование элементарных преобразований. Мы докажем, что введенные в § 154 «элементарные преобразования» матрицы получаются от умножения этой матрицы справа и слева на подходящим образом выбранные неособенные квадратные матрицы.

1. Перестановку двух строк мы получим, помножив данную матрицу слева на матрицу типа (28); перестановку столбцов, — помножив ее справа на матрицу того же типа (28).

2. Все элементы $\varkappa$-й строки умножатся на множитель a, если данную матрицу помножить слева на матрицу вида:

$$M_{\varkappa a} = \begin{pmatrix} 1 & 0 & \dots & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & a & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & \dots & 1 \end{pmatrix} \begin{matrix} \\ \\ \\ \varkappa\text{-я строка} \\ \\ \\ \end{matrix} \tag{29}$$

$$\begin{matrix} \varkappa\text{-й} \\ \text{столбец.} \end{matrix}$$

В этой матрице все элементы равны нулю кроме диагональных, которые все равны единице за исключением стоящего на $\varkappa$-м месте, который равен a.

Все элементы $\varkappa$-й колонны данной матрицы умножатся на a, если ее помножить справа на матрицу вида (29).

3. К элементам $\varkappa$-й строки данной матрицы прибавятся соответствующие элементы λ-й строки, умноженные на a, если данную матрицу помножить слева на

матрицу вида:

$$N^{(a)}_{\varkappa\lambda} = \begin{matrix}\begin{pmatrix} 1 & 0 & \dots & 0 & \dots & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 & \dots & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & \dots & a & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & \dots & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & \dots & 0 & \dots & 1 \end{pmatrix} \\ \begin{matrix} \varkappa\text{-й} & & \lambda\text{-й} \\ \text{столбец} & & \text{столбец;} \end{matrix}\end{matrix} \quad \begin{matrix} \varkappa\text{-я строка} \\ \\ \lambda\text{-я строка} \end{matrix} \tag{30}$$

Эта матрица отличается от E тем, что на пересечении $\varkappa$-й строки с λ-м столбцом стоит не нуль, а a.

К элементам $\varkappa$-го столбца данной матрицы прибавятся соответствующие элементы λ-го столбца, умноженные на a, если данную матрицу умножить справа на *транспонированную* к матрице (30).

Все эти утверждения легко проверяются непосредственно. Матрицы (28), (29) (при $a \neq 0$) и (30) неособенные, ибо

$$|F_{\varkappa\lambda}| = -1, \qquad |M_{\varkappa a}| = a \neq 0, \qquad |N^{(a)}_{\varkappa\lambda}| = +1.$$

Заметим еще формулы:

$$F^{-1}_{\varkappa\lambda} = F_{\varkappa\lambda}; \qquad F_{\varkappa\lambda} = F_{1\varkappa}F_{1\lambda}F_{1\varkappa} = F_{1\lambda}F_{1\varkappa}F_{1\lambda};$$

последнее следует из того, что для транспозиций имеем (§ 142):

$$(\varkappa, \lambda) = (1, \varkappa)(1, \lambda)(1, \varkappa) = (1, \lambda)(1, \varkappa)(1, \lambda).$$

Далее:

$$M^{-1}_{\varkappa a} = M_{\varkappa, \frac{1}{a}}, \qquad = M_{\varkappa a} = F_{1\varkappa}M_{1a}F_{1\varkappa};$$

$$(N^{(a)}_{\varkappa\lambda})^{-1} = N^{(-a)}_{\varkappa\lambda}, \qquad (N^{(a)}_{\varkappa\lambda})' = N^{(a)}_{\lambda\varkappa}, \qquad N^{(a)}_{\varkappa\lambda} = F_{1\varkappa}F_\lambda N^{(a)}_{12}F_{2\lambda}F_{1\varkappa},$$

$$N^{(a)}_{12} = M_{1a}N^{(1)}_{12}M_{1,\frac{1}{a}}.$$

Таким образом обратные подстановки к (28), (29), (30) того же типа, т. е. дают того же типа элементарные преобразования.

Заметим, что данную матрицу A мы можем не предполагать непременно квадратной: она может быть любой mn-матрицей; только в этом случае следует умножать A слева на матрицы m-го порядка, а справа — на матрицы n-го порядка типов (28), (29) и (30).

Если A — квадратная неособенная матрица n-го порядка, то «нормальная» матрица для A, которая в § 154 (8) обозначена через A_4, есть одиночная матрица E_n. Но ведь идя от E_n назад, — умножениями на обратные матрицы, — мы в конце концов снова придем к A; при этом множитель E_n, как единицу, можно откинуть. Введя еще обозначения: $F_{1\varkappa} = F_\varkappa$, $M_{1a} = M_a$, $N^{(1)}_{12} = N$, и принимая во внимание приведенные выше формулы, получим:

Теорема. *Всякую неособенную квадратную матрицу можно представить как произведение матриц $F_\varkappa$, M_a, N.*

Разберем подробнее случай $n = 2$, т. е. случай матриц второго порядка. Пусть $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ данная неособенная матрица, т. е. $\varepsilon = ad - bc \neq 0$. Не нарушая общности, положим, что $a \neq 0$ иначе мы помножили бы предварительно нашу матрицу на $F_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Следуем рецепту, указанному в § 154 для перехода от A_1 к A_4. Для этого умножаем $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ справа на $N_{12}^{\left(-\frac{b}{a}\right)}$ и слева на $N_{21}^{\left(-\frac{c}{a}\right)}$;

$$\begin{pmatrix} 1 & 0 \\ -\dfrac{c}{a} & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & -\dfrac{b}{a} \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & \dfrac{\varepsilon}{a} \end{pmatrix};$$

полученную матрицу умножаем на $M_{2,\frac{a}{\varepsilon}}$ справа и на $M_{1,\frac{1}{a}}$ слева:

$$\begin{pmatrix} \dfrac{1}{a} & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & \dfrac{\varepsilon}{a} \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & \dfrac{a}{\varepsilon} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = E.$$

Теперь, идя от E назад, т. е. умножая на обратные матрицы, мы придем к $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$; получим:

$$N_{21}^{\left(\frac{c}{a}\right)} M_{1a} M_{2,\frac{\varepsilon}{a}} N_{12}^{\left(\frac{b}{a}\right)} = \begin{pmatrix} 1 & 0 \\ \dfrac{c}{a} & 1 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & \dfrac{\varepsilon}{a} \end{pmatrix} \begin{pmatrix} 1 & \dfrac{b}{a} \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Пример. $\begin{pmatrix} 5 & -3 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ \dfrac{2}{5} & 1 \end{pmatrix} \begin{pmatrix} 5 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & \dfrac{11}{5} \end{pmatrix} \begin{pmatrix} 1 & -\dfrac{3}{5} \\ 0 & 1 \end{pmatrix}$.

Из примененных здесь матриц M_{1a}, M_{2a}, $N_{12}^{(a)}$ и $N_{21}^{(a)}$ не все независимы; если обозначим $V = F_2 \cdot M_{2,-1} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, то $V^{-1} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ и $V^{-1} N_{12}^{(-a)} V = N_{21}^{(a)}$, $V^{-1} M_{2a} V = M_{1a}$, т. е. *всякая неособенная матрица второго порядка есть произведение матриц типов* $V = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $M_{2a} = S_a = \begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix}$ *и* $N_{12}^{(a)} = T_a = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$. (Из предыдущей теоремы мы знаем, что и T_a может быть сведено к T_1 формулой $T_a = V^{-1} S_a V T_1 V^{-1} S_{\frac{1}{a}} V$.)

§ 163. Билинейные формы. Сумма матриц. Укажем еще на одно конкретное представление матриц, которое приведет нас к определению «суммы» матриц.

Рассмотрим такую функцию:

$$F = \sum_{\beta=1}^{n} \sum_{\alpha=1}^{n} a_{\alpha\beta} x_\alpha y_\beta;$$

по отношению к каждому из двух рядов переменных $x_1, x_2, \ldots, x_n$ и $y_1, y_2, \ldots, y_n$ F является линейной однородной функцией, коэфициенты которой суть линейные формы от переменных другого ряда; по отношению же ко всем $2n$ переменным F является функцией второй степени, однородной и не содержащей квадратов переменных. Такая функция называется *билинейной формой*. В билинейной форме обозначения переменных роли не играют; важны коэфиииенты, которые составляют квадратную матрицу:

$$A = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots\ldots\ldots\ldots\ldots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{pmatrix};$$

строки в ней соответствуют переменным x_α, а столбцы — переменным y_β. Пусть k — любое число; имеем:

$$F \cdot k = k \cdot F = k \cdot \sum_{\alpha,\beta} a_{\alpha\beta} x_\alpha y_\beta = \sum_{\alpha,\beta} k a_{\alpha\beta} x_\alpha y_\beta;$$

отсюда мы определяем:

$$A \cdot k = k \cdot A = k \cdot \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots\ldots\ldots\ldots\ldots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{pmatrix} = \begin{pmatrix} ka_{11} & ka_{12} & \ldots & ka_{1n} \\ ka_{21} & ka_{22} & \ldots & ka_{2n} \\ \ldots\ldots\ldots\ldots\ldots \\ ka_{n1} & ka_{n2} & \ldots & ka_{nn} \end{pmatrix}, \tag{31}$$

т. е. чтобы *умножить матрицу на некоторое число, надо каждый ее элемент умножить на это число*. Такой численный множитель k называется *скалярным множителем*.

Пусть

$$G = \sum_{\alpha,\beta} b_{\alpha\beta} x_\alpha y_\beta$$

другая билинейная форма от тех же $2n$ переменных; ее матрица:

$$B = (b_{\alpha\beta}).$$

Сумма

$$F + G = \sum_{\alpha,\beta} (a_{\alpha\beta} + b_{\alpha\beta}) x_\alpha y_\beta$$

есть также билинейная форма; ее матрицу мы определим как сумму матриц A и B, а именно:

$$A + B = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots\ldots\ldots\ldots\ldots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} & \ldots & b_{1n} \\ b_{21} & b_{22} & \ldots & b_{2n} \\ \ldots\ldots\ldots\ldots\ldots \\ b_{n1} & b_{n2} & \ldots & b_{nn} \end{pmatrix} =$$

$$= \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} & \ldots & a_{1n} + b_{1n} \\ a_{21} + b_{21} & a_{22} + b_{22} & \ldots & a_{2n} + b_{2n} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{n1} + b_{n1} & a_{n2} + b_{n2} & \ldots & a_{nn} + b_{nn} \end{pmatrix}. \tag{32}$$

Замечание. Обращаем внимание на то, что формулы (31) и (32) для матриц совершенно не совпадают со свойствами III и IV детерминантов в § 30.

Формула (32) обобщается и на несколько слагаемых. Очевидно, что для суммы матриц верны коммутативный и ассоциативный законы. Докажем, что для суммы и символического произведения матриц верен и дистрибутивный закон:

$$(A+B)C = AC + BC, \qquad C(A+B) = CA + CB. \tag{33}$$

Пусть

$$A = (a_{\alpha\beta}), \qquad B = (b_{\alpha\beta}), \qquad C = (c_{\alpha\beta});$$

тогда

$$A + B = A = (a_{\alpha\beta} + A = (b_{\alpha\beta}), \qquad (A+B)C = \left(\sum_{\varkappa=1}^{n}(a_{\alpha\varkappa} + b_{\alpha\varkappa})c_{\varkappa\beta}\right),$$

$$AC = \left(\sum_{\varkappa=1}^{n} a_{\alpha\varkappa}c_{\varkappa\beta}\right), \qquad BC = \left(\sum_{\varkappa=1}^{n} b_{\alpha\varkappa}c_{\varkappa\beta}\right),$$

$$AC + BC = \left(\sum_{\varkappa=1}^{n} a_{\alpha\varkappa}c_{\varkappa\beta} + \sum_{\varkappa=1}^{n} b_{\alpha\varkappa}c_{\varkappa\beta}\right) = \left(\sum_{\varkappa=1}^{n}(a_{\alpha\varkappa}c_{\varkappa\beta} + b_{\alpha\varkappa})c_{\varkappa\beta}\right) =$$

$$= \left(\sum_{\varkappa=1}^{n}(a_{\alpha\varkappa} + b_{\alpha\varkappa})c_{\varkappa\beta}\right) = (A+B)C.$$

Так же убедимся и в верности второй формулы (33). (Обе формулы здесь не зависят друг от друга, ибо коммутативный закон для нашего произведения неверен.)

Из (31) и (32) выводим, что если p, q, r скалярные множители, то

$$pA + qB + rC = (pa_{\alpha\beta} + qb_{\alpha\beta} + rc_{\alpha\beta});$$

отсюда при $p = 1$, $q = -1$, $r = 0$

$$A - B = (a_{\alpha\beta} - b_{\alpha\beta}),$$

т. е. разность матриц находится аналогично сумме.

Определим еще

$$-A = -(a_{\alpha\beta}) = (-a_{\alpha\beta}),$$

тогда

$$A - B = A + (-B).$$

Легко убедиться, что формулы (33) верны для алгебраической суммы (т. е. для суммы и для разности) скольких угодно слагаемых. А отсюда следует, что обычное правило умножения многочленов верно для матриц, например:

$$(A + B + C)(P + Q) = AP + BP + CP + AQ + BQ + CQ.$$

Как частные случаи получаем правила возвышения многочленов в степени, например:

$$(A+B)^2 = (A+B)(A+B) = A^2 + AB + BA + B^2,$$

но два средних члена мы не можем соединить в один, так как вообще $AB \neq BA$.

Отметим еще формулу:

$$(pA + qB + rC)' = pA' + qB' + rC'.$$

Обобщение. Можно рассматривать билинейные формы, где число переменных x_α не равно числу переменных y_β; общий вид такой формы:

$$F = \sum_{\beta=1}^{n} \sum_{\alpha=1}^{m} a_{\alpha\beta} x_\alpha y_\beta; \tag{34}$$

ей соответствует прямоугольная тп-матрица:

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots\dots\dots\dots\dots\dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}.$$

Умножение такой матрицы на скалярный множитель, сложение и вычитание таких матриц определяется, как и для квадратных матриц. Две прямоугольные матрицы можно складывать тогда и только тогда, если у обеих число строк одно и то же. Наконец, для сложения и умножения прямоугольных матриц (если умножение возможно) верен дистрибутивный закон (33) со всеми следствиями из него.

Заметим, что ранг матрицы A называется также рангом соответствующей билинейной формы.

§ 164. Приведение билинейных форм. Возьмем билинейную форму в общем виде (34); наиболее важный случай, когда число переменных x_α то же, что и число переменных y_β, мы получаем из результатов этого параграфа как частный случай, при $m = n$. Произведем над переменными x_α линейную подстановку:

$$x_\alpha = \sum_{\varkappa=1}^{m} p_{\alpha\varkappa} u_\varkappa$$

с матрицей $P = (p_{\alpha\varkappa})$; P — квадратная матрица m-то порядка. Тогда форма F примет вид:

$$\sum_{\beta=1}^{n} \sum_{\alpha=1}^{m} \sum_{\varkappa=1}^{m} a_{\alpha\beta} p_{\alpha\varkappa} u_\varkappa y_\beta = \sum_{\beta=1}^{n} \sum_{\varkappa=1}^{m} r_{\varkappa\beta} u_\varkappa y_\beta,$$

где

$$r_{\varkappa\beta} = \sum_{\alpha=1}^{m} p_{\alpha\varkappa} a_{\alpha\beta} \qquad (\varkappa = 1, 2, \dots, m,\ \beta = 1, 2, \dots, n).$$

Если мы обозначим через R mn-матрицу:

$$R = (r_{\varkappa\beta}),$$

то последняя формула показывает, что

$$R = P'A.$$

Итак, от этой подстановки наша билинейная форма перешла в билинейную же с матрицей R. Введем теперь и вместо переменных y_β новые переменные v_λ посредством линейной подстановки:

$$y_\beta = \sum_{\lambda=1}^{n} q_{\beta\lambda} v_\lambda,$$

матрица которой $Q = (q_{\beta\lambda})$ есть квадратная матрица n-го порядка. От этого наша билинейная форма перейдет в

$$\sum_{\beta=1}^{n}\sum_{\varkappa=1}^{m}\sum_{\lambda=1}^{n} r_{\varkappa\beta} q_{\beta\lambda} u_\varkappa v_\lambda = \sum_{\lambda=1}^{n}\sum_{\varkappa=1}^{m} b_{\varkappa\lambda} u_\varkappa v_\lambda,$$

где

$$b_{\varkappa\lambda} = \sum_{\beta=1}^{n} r_{\varkappa\beta} q_{\beta\lambda} \qquad (\varkappa = 1, 2, \ldots, m,\ \lambda = 1, 2, \ldots, n).$$

Отсюда видно, что mn-матрица $B = (b_{\varkappa\lambda})$представляется в виде:

$$B = RQ = P'AQ. \tag{35}$$

Итак, *посредством этих двух линейных подстановок P и Q билинейная форма F перейдет в билинейную же форму*

$$G = \sum_{\lambda=1}^{n}\sum_{\varkappa=1}^{m} b_{\varkappa\lambda} u_\varkappa v_\lambda$$

того же типа. Между матрицами A и B этих форм имеется зависимость (35); а между детерминантами — в случае $m = n$:

$$|B| = |P|\,|A|\,|Q|.$$

Если r — ранг A, а s — ранг B, то по теореме § 156 заключаем, что $s \leq r$. Мы говорим: форма G *содержится* в форме ?; форма F *содержит* форму G. Это означает, что F двумя линейными подстановками может быть преобразована в G. Если и обратно, форма F содержится в G, то формы F и G называются *эквивалентными*; в этом случае и $r \leq s$, т. е. $r = s$. Итак:

Теорема 1. *Если формы F и G эквивалентны, то ранги их матриц одинаковы.*

Если в (35) $|P| \neq 0$ и $|QQ \neq 0$, то существуют Q^{-1} и $(P')^{-1}$; тогда из (27) следует:

$$A = (P^{-1})' B Q^{-1},$$

т. е. и F содержится в G и значит F и G эквивалентны. Следовательно:

Теорема 2. *Формы F и G эквивалентны, если одна из них может быть преобразована в другую посредством двух линейных подстановок, детерминанты которых не равны нулю.*

Мы увидим, что и обратные теоремы к теоремам 1 и 2 верны. Именно мы докажем следующее:

Теорема 3. *Всякая билинейная форма ранга r может быть двумя линейными подстановками с детерминантами, не равными нулю, преобразована в так называемую нормальную форму:*

$$H = x_1 y_1 + x_2 y_2 + \ldots + x_r y_r.$$

Предварительно докажем следующую лемму. Пусть F — данная Форма,

$$X_\beta = \frac{\partial F}{\partial y_\beta} = \sum_{\alpha=1}^{m} a_{\alpha\beta} x_\alpha, \qquad Y_\alpha = \frac{\partial F}{\partial x_\alpha} = \sum_{\beta=1}^{n} a_{\alpha\beta} y_\beta,$$

$$R_k = \begin{pmatrix} a_{11} & \dots & a_{1k} & Y_1 \\ \dots & \dots & \dots & \dots \\ a_{k1} & \dots & A_{kk} & Y_k \\ X_1 & \dots & X_k & F \end{pmatrix};$$

тогда:

Лемма. *R_k есть билинейная форма, совершенно независящая ни от $x_1, x_2, \dots, x_k$, ни от $y_1, y_2, \dots, y_k$; если ранг $F \leq k$, то R_k тождественно равно нулю.*

Доказательство. Разложив, по § 36 R_k по элементам последней строки и последнего столбца, получим:

$$R_k = CF - \sum_{\alpha,\beta=1}^{k} C_{\alpha\beta} Y_\alpha X_\beta,$$

где

$$C = \begin{pmatrix} a_{11} & \dots & a_{1k} \\ \dots & \dots & \dots \\ a_{k1} & \dots & a_{kk} \end{pmatrix}$$

и $C_{\alpha\beta}$ — миноры $(k-1)$-го порядка детерминанта C. Отсюда видно, что R_k — билинейная форма от $x_\varkappa$ и y_λ. Положим $R_k = \sum_{\varkappa,\lambda=1}^{n} b_{\varkappa\lambda} x_\varkappa y_\lambda$; коэфициент $b_{\varkappa\lambda}$ мы найдем, положив $x_\varkappa = y_\lambda = 1$, а остальные переменные равными нулю; тогда R_k обратится в $b_{\varkappa\lambda}$. Но тогда будет $Y_\alpha = a_{\alpha\lambda}$, $X_\beta = a_{\varkappa\beta}$, $F = a_{\varkappa\lambda}$; следовательно:

$$b_{\varkappa\lambda} = \begin{pmatrix} a_{11} & \dots & a_{1k} & a_{1\lambda} \\ \dots & \dots & \dots & \dots \\ a_{k1} & \dots & a_{kk} & a_{k\lambda} \\ a_{\varkappa 1} & \dots & a_{\varkappa k} & a_{\varkappa\lambda} \end{pmatrix}.$$

Отсюда заключаем:

1) При $\varkappa \leq k$ или $\lambda \leq k$, $b_{\varkappa\lambda} = 0$, т. е. R_k не зависит ни от $x_1, \dots, x_k$, ни от $y_1, \dots, y_k$.

2) Если ранг $F \leq k$, то все $b_{\varkappa\lambda} = 0$, как детерминанты $(k+1)$-порядка матрицы формы F. Тем самым лемма доказана.

Доказательство теоремы 3. Пусть, например, $a_{\alpha\beta} \neq 0$; тогда перенумеровываем наши переменные так, чтобы $a_{\alpha\beta}$ оказалось на первом месте, или, другими словами, переставляем x_1 с x_α и y_1 с y_β. Таким образом, не нарушая общности, можно положить $a_{11} \neq 0$. По предыдущей лемме при $k = 1$ получаем, что

$$\begin{pmatrix} a_{11} & Y_1 \\ X_1 & F \end{pmatrix} = R_1$$

не зависит ни от x_1 ни от y_1. Имеем:

$$a_{11} F - X_1 Y_1 = R_1,$$

следовательно:

$$F = \frac{1}{a_{11}} X_1 Y_1 + \frac{1}{a_{11}} R_1;$$

мы этим сделали подстановки:

$$X_1 = a_{11}x_1 + a_{21}x_2 + \ldots + a_{m1}x_m, \quad x_2 = x_2, \ldots, x_m = x_m,$$
$$Y_1 = a_{11}y_1 + a_{21}y_2 + \ldots + a_{n1}y_n, \qquad y_2 = y_2, \ldots, y_n = y_n.$$

Детерминанты этих подстановок равны $a_{11} \neq 0$. Обозначим

$$\frac{1}{a_{11}} X_1 Y_1 = u_1 v_1, \qquad \frac{1}{a_{11}} R_1 = F',$$

где F' — билинейная форма от $x_2, \ldots, x_m$, $y_2, \ldots, y_n$. Если все коэфициенты в F' равны нулю, то мы уже у цели; если нет, то к ней применяем такое же преобразование. Найдем:

$$F = u_1 v_1 + F',$$
$$F' = u_2 v_2 + F'',$$
$$F'' = u_3 v_3 + F''',$$
$$\ldots\ldots\ldots\ldots\ldots$$

Число переменных в формах F', F'', ... каждый раз уменьшается на два; таким образом после конечного числа таких преобразований мы придем к форме, тождественно равной нулю. Следовательно, F преобразуется в

$$H = u_1 v_1 + u_2 v_2 + \ldots + u_r v_r.$$

Каждое из этих отдельных преобразований сводится к двум линейным подстановкам с детерминантами, не равными нулю; соединив их все, получим две линейные подстановки с детерминантами, не равными нулю, которые прямо преобразовывают F в H. Следовательно, по теореме 2 формы F и H эквивалентны и значит имеют один и тот же ранг (по теореме 1); но ранг H, очевидно, равен r; следовательно, и ранг F есть r. Тем самым теорема 3 доказана.

Если формы F и G (с матрицами A и B) имеют один и тот же ранг r, то по доказанному, они могут быть преобразованы в одну и ту же нормальную форму H с матрицей C; следовательно:

$$C = R'AS, \quad |R| \neq 0, \quad |S| \neq 0$$
$$C = T'BU, \quad |T| \neq 0, \quad |U| \neq 0.$$

Из второго выражения получаем:

$$B = (T^{-1})' C U^{-1};$$

подставляя сюда первое выражение для C, находим:

$$B = (T^{-1})' R' A S U^{-1} = (RT^{-1})' A (SU^{-1}),$$

причем

$$|RT^{-1}| \neq 0, \qquad |SU^{-1}| \neq 0.$$

Следовательно (по теореме 2), формы F и G эквивалентны. Этим доказана теорема, обратная к теореме 1:

Теорема 4. *Если две билинейные формы имеют один и тот же ранг, то они эквивалентны.*

А отсюда непосредственно следует и обратная к теореме 2:

Теорема 5. *Если две формы эквивалентны, то каждая из них преобразовывается в другую линейными подстановками, детерминанты, которых не равны нулю.*

Таким образом теоремы 2 и 5 дают новое определение эквивалентности билинейных форм.

Собственно всю теорию эквивалентности билинейных форм мы могли бы вывести из результатов § 154 и 162. Назовем эквивалентными формы одних и тех же переменных, имеющие один и тот же ранг; тогда по последней теореме § 154 матрицы этих форм могут быть получены одна из другой путем конечного числа элементарных преобразований; но по § 162 элементарные преобразования сводятся к умножениям данной mn-матрицы справа и слева на квадратные матрицы с детерминантами, отличными от нуля, а эти умножения — на преобразование данной билинейной формы собственными линейными подстановками.

Преобразование билинейной формы в нормальную, указанное в теореме 3, называется *приведением* (редукцией) билинейной формы. Метод доказательства теоремы 3, приведенный выше, есть вместе с тем и практический метод действительного приведения данной формы.

Пример. $F = 3x_1y_1 - 5x_1y_2 - x_1y_3 + 2x_2y_1 + 2x_2y_2 - 4x_2y_3$. Здесь $m = 2$,

$$A = \begin{pmatrix} 3 & -5 & -1 \\ 2 & 2 & -4 \end{pmatrix},$$

$$X_1 = \frac{\partial F}{\partial y_1} = 3x_1 + 2x_2, \qquad Y_1 = \frac{\partial F}{\partial x_1} = 3y_1 - 5y_2 - y_3,$$

$$F' = F - \frac{1}{3}X_1Y_1 = \frac{16}{3}x_2y_2 - \frac{10}{3}x_2y_3.$$

Обозначим теперь

$$X_2 = \frac{\partial F'}{\partial y_2} = \frac{16}{3}x_2, \qquad Y_2 = \frac{\partial F'}{\partial x_2} = \frac{16}{3}y_2 - \frac{10}{3}y_3;$$

тогда

$$F' - \frac{3}{16}X_2Y_2 \equiv 0.$$

Итак:

$$F = \frac{1}{3}X_1Y_1 + \frac{3}{16}X_2Y_2.$$

Обозначим еще

$$u_1 = \frac{1}{3}X_1 = x_1 + \frac{2}{3}x_2, \qquad u_2 = \frac{3}{16}X_2 = x_2,$$

$$v_1 = Y_1 = 3y_1 - 5y_2 - y_3, \qquad v_2 = y_2 = \frac{16}{3}y_2 - \frac{10}{3}y_3, \qquad v_3 = y_3;$$

тогда получим: $F = u_1v_1 + u_2v_2$; это и есть искомая нормальная форма. Найдем подстановки, переводящие F в эту форму. Для этого выразим x_1, x_2 через u_1, u_2 и y_1, y_2, y_3 через v_1, v_2, v_3. Найдем:

$$\begin{cases} x_1 = u_1 - \dfrac{2}{3}u_2, \\ x_2 = u_2, \end{cases} \qquad \begin{cases} y_1 = \dfrac{1}{3}v_1 + \dfrac{5}{16}v_2 + \dfrac{11}{8}v_3, \\ y_2 = \dfrac{3}{16}v_2 + \dfrac{5}{8}v_3, \\ y_3 = v_3. \end{cases}$$

Итак, искомые подстановки:

$$P = \begin{pmatrix} 1 & -|D\frac{2}{3} \\ 0 & 1 \end{pmatrix}, \qquad Q = \begin{pmatrix} \dfrac{1}{3} & \dfrac{5}{16} & \dfrac{11}{8} \\ 0 & \dfrac{3}{16} & \dfrac{5}{8} \\ 0 & 0 & 1 \end{pmatrix}.$$

И действительно:

$$P'AQ = \begin{pmatrix} 1 & 0 \\ -\dfrac{2}{3} & 1 \end{pmatrix} \begin{pmatrix} 3 & -5 & -1 \\ 2 & 2 & -4 \end{pmatrix} \begin{pmatrix} \dfrac{1}{3} & \dfrac{5}{16} & \dfrac{11}{8} \\ 0 & \dfrac{3}{16} & \dfrac{5}{8} \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Упражнения

210). Привести к нормальному виду форму:

$$F = 5x_1y_1 - 4x_1y_2 + 3x_2y_1 - 2x_2y_2$$

и найти соответствующие подстановки

Отв. $u_1v_1 + u_2v_2$, $P = \begin{pmatrix} 1 & -3 \\ 0 & 5 \end{pmatrix}$, $Q = \begin{pmatrix} \dfrac{1}{5} & \dfrac{2}{5} \\ 0 & \dfrac{1}{2} \end{pmatrix}$.

211). То же самое для формы:

$$F = x_1y_1 + x_1y_2 + x_1y_3 + x_1y_4 + x_2y_1 - x_2y_2 + x_2y_3 + x_2y_3 - x_2y_4 + \\ + x_3y_1 + x_3y_3 + x_4y_2 + x_4y_4.$$

Отв. $u_1v_1 + u_2v_2$, $P = \begin{pmatrix} 4 & -1 & -\dfrac{1}{2} & -\dfrac{1}{2} \\ 0 & 1 & -\dfrac{1}{2} & \dfrac{1}{2} \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$, $Q = \begin{pmatrix} 1 & \dfrac{1}{2} & -1 & 0 \\ 0 & -\dfrac{1}{2} & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$.

§ 165. Нулевые матрицы. Нулевыми называются матрицы (прямоугольные и квадратные), все элементы которых равны нулю. При сложении и умножении такие матрицы играют роль нуля; поэтому мы и будем обозначать их через нуль.

Выясним теперь, при каких условиях произведение двух матриц равно нулю, причем будем рассматривать общий случай прямоугольных матриц (рассматривая квадратные матрицы как частный случай). Итак, пусть $A = (a_{\alpha\beta})$ mn-матрица, $B = (b_{\alpha\beta})$ np-матрица и

$$AB = 0. \tag{36}$$

Это сводится к mp равенствам:

$$\sum_{\lambda=1}^{n} a_{\alpha\lambda} b_{\lambda\beta} = 0, \qquad \alpha = 1, 2, \ldots, m, \ \beta = 1, 2, \ldots, p. \tag{37}$$

Конечно, (36) удовлетворяется, если $A = 0$ или $B = 0$, т. е. если все $a_{\alpha\lambda} = 0$ или все $b_{\lambda\beta} = 0$. Отбросим пока этот тривиальный случай. Предположим, что матрица A — данная, а B — искомая; тогда при данном β (37) есть система m линейных однородных уравнений с n неизвестными; для существования у нее нетривиальных решений ранг r матрицы A должен быть меньше, чем n (§ 44); в этом случае существует $n - r$ независимых решений; находя $b_{\lambda\beta}$ при различных β, мы можем использовать все эти независимые решения или только часть их; таким образом в матрице B не больше, чем $n - r$ линейно независимых строк, и значит ранг матрицы $B \leq n - r$. Если матрица B данная, а A искомая, то рассуждения будут аналогичны. Итак:

Теорема. *Равенство* (36)*, где A — mn-матрица, B — np-матрица, и обе отличны от нуля, возможно только в том случае, если сумма рангов A и $B \leq n$. Если одна из матриц A, B данная, а другая — искомая, то уравнение (36) имеет нетривиальные решения тогда и только тогда, если ранг данной матрицы меньше n, и в этом случае — бесчисленное множество решений; при этом при данном A число p столбцов у B произвольно; при данном B число m строк у A произвольно.*

Переходя к случаю квадратных матриц, получаем:

Следствие 1. Уравнения $AX = 0$, $YA = 0$ имеют нетривиальные решения тогда и только тогда, если A — особенная матрица (т. е. $|A| = 0$.

Следствие 2. Произведение неособенных квадратных матриц равно нулю тогда и только тогда, если по крайней мере один из сомножителей равен нулю.

Полученные результаты можно выразить еще следующим образом: mn-матрица есть *левый нулевой делитель* тогда и только тогда, если ее ранг меньше n, и *правый нулевой делатель* тогда и только тогда, если ее ранг меньше m; если ранг mn-матрицы меньше наименьшего из чисел m и n, то тогда (и только в этом случае) она — *двусторонний нулевой делитель*.

Квадратная матрица тогда и только тогда нулевой делитель (и при этом всегда двусторонний), если она особенная. В области неособенных матриц данного порядка нет нулевых делителей.

Пример. Найти общее решение уравнения:

$$AX = 0,$$

где $A = \begin{pmatrix} 2 & 1 & 5 & -3 \\ 1 & 3 & -1 & 2 \\ 3 & 5 & 1 & 4 \end{pmatrix}$, а X должно быть $(4, 2)$-матрицей.

A ранга 3; следовательно, X должно быть ранга $\leq 4 - 3 = 1$. Пусть

$$X = \begin{pmatrix} x_1 & y_1 \\ x_2 & y_2 \\ x_3 & y_3 \\ x_4 & y_4 \end{pmatrix};$$

имеем по (37):

$$2x_1 + x_2 + 5x_3 - 3x_4 = 0,$$
$$x_1 + 3x_2 - x_3 + 2x_4 = 0,$$
$$3x_1 + 5x_2 + x_3 + 4x_4 = 0,$$

и совершенно такую же систему имеем для y_1 y_2, y_3, y_4. Находим: $x_1 = -20u$, $x_2 = 7u$, $x_3 = 9u$, $x_4 4u$, где u — произвольный параметр. Для y_λ имеем то же решение, только вместо u берем другой параметр v: $y_1 = -20v$, $y_2 = 7v$, $y_3 = 9v$, $y_4 = 4v$. Итак:

$$X = \begin{pmatrix} -20u & -20v \\ 7u & 7v \\ 9u & 9v \\ 4u & 4v \end{pmatrix}.$$

Упражнения

212). Найти общее решение уравнения $AX = 0$, где $A = \begin{pmatrix} 3 & 2 & 1 \\ 1 & 4 & 5 \\ 15 & 5 & -2 \end{pmatrix}$.

Отв. $\begin{pmatrix} 3u & 3v & 3w \\ -7u & -7v & -7w \\ 5u & 5v & 5w \end{pmatrix}$.

213) То же для уравнения $YA = 0$, где $A = \begin{pmatrix} 4 & 1 & 2 & -1 \\ 1 & 3 & -1 & 0 \\ 5 & 4 & 1 & -1 \\ 2 & -5 & 4 & -1 \end{pmatrix}$.

Отв. $\begin{pmatrix} -u_1 - v_1 & -u_1 + 2v_1 & u_1 & v_1 \\ -u_2 - v_2 & -u_2 + 2v_2 & u_2 & v_2 \\ -u_3 - v_3 & -u_3 + 2v_3 & u_3 & v_3 \\ -u_4 - v_4 & -u_4 + 2v_4 & u_4 & v_4 \end{pmatrix}$.

§ 166. Взаимная матрица. Скалярные, диагональные и квази-диагональные матрицы. *Взаимная* матрица для данной квадратной матрицы A n-го порядка определяется, аналогично взаимному детерминанту (§ 32), как матрица n-го же порядка, элементами которой служат миноры $(n-1)$-го порядка матрицы A'. Если через $a_{\alpha\beta}$ обозначим элементы матрицы A, а через $A_{\alpha\beta}$ соответствующие им миноры $(n-1)$-го порядка, которые находятся по известному элементарному

правилу (§ 30), то взаимная матрица будет:

$$\widetilde{A} = \begin{pmatrix} A_{11} & A_{21} & \dots & A_{n1} \\ A_{12} & A_{22} & \dots & A_{n2} \\ \dots\dots\dots\dots\dots\dots \\ A_{1n} & A_{2n} & \dots & A_{nn} \end{pmatrix};$$

для ее детерминанта имеем (§ 30): $|\widetilde{A}| = |A|^{n-1}$.

Если $|A| = 0$, то и $|\widetilde{A}| = 0$, и обратно; т. е. данная матрица и ее взаимная одновременно или обе неособенные, или обе особенные.

Если ранг матрицы A меньше $n-1$, то $\widetilde{A} = 0$.

На основании формул § 32 легко найдем:

$$A\widetilde{A} = \widetilde{A}A = \begin{pmatrix} |A| & 0 & \dots & 0 \\ 0 & |A| & \dots & 0 \\ \dots\dots\dots\dots\dots\dots \\ 0 & 0 & \dots & |A| \end{pmatrix};$$

на основании формулы (31) § 163 это можно представить так:

$$A\widetilde{A} = \widetilde{A}A = |A|E. \tag{38}$$

Отсюда следует, что при $|A| = 0$ будет:

$$A\widetilde{A} = \widetilde{A}A = 0, \tag{38a}$$

т. е. $\widetilde{A}$ является в этом случае решением уравнений $AX = 0 = 0$ и $YA = 0$. При $|A| \neq$ формула (38) есть следствие из формул (17), (19а) § 157, ибо из (17) легко следует [по (31) § 163]:

$$A^{-1} = \frac{1}{|A|}\widetilde{A}. \tag{39}$$

В правой части формулы (38) стоит матрица такого вида:

$$aE = Ea = \begin{pmatrix} a & 0 & \dots & 0 \\ 0 & a & \dots & 0 \\ \dots\dots\dots\dots \\ 0 & 0 & \dots & a \end{pmatrix},$$

у которой вдоль диагонали стоит число a, а все остальные элементы равны нулю; такая матрица называется *скалярной*; она переместима со всякой другой матрицей того же порядка и при умножении дает тот же результат, что и скалярный множитель [см. (31) § 163], т. е. умножение всех элементов другого множителя на a. Подстановка, соответствующая скалярной матрице aE, имеет вид:

$$x_\lambda = ay_\lambda \qquad (\lambda = 1, 2, \dots, n). \tag{40}$$

Если считать наши переменные $x_1, x_2, \dots, x_n$ координатами точки в n-мерном пространстве, то (40) дает преобразование подобия в этом пространстве.

Рассмотрим теперь более общую матрицу:

$$A = \begin{pmatrix} a_1 & 0 & \dots & 0 \\ 0 & a_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & a_n \end{pmatrix},$$

где вдоль диагонали стоят числа $a_1, a_2, \dots, a_n$, а остальные элементы равны нулю; такая матрица называется *диагональной* и обозначается

$$A = [a_1, a_2, \dots, a_n]^{78}$$

Очевидно, $|A| = a_1 a_2 \cdots a_n$. Скалярная матрица — частный случай диагональной, когда $a_1 = a_2 = \dots = a_n$. Всякие две диагональные матрицы (одного и того же порядка) переместимы друг с другом; если $B = [b_1, b_2, \dots, b_n]$, то

$$AB = BA = [a_1 b_1, a_2 b_2, \dots, a_n b_n],$$

т. е. произведение диагональных матриц — тоже диагональная матрица [79]. Наконец, и сумма диагональных матриц — тоже диагональная матрица:

$$A + B = [a_1 + b_1, a_2 + b_2, \dots, a_n + b_n].$$

Введем еще понятие о квази-диагональной матрице, являющейся обобщением диагональной; приведем сначала пример такой матрицы:

$$\begin{pmatrix} 4 & 1 & 2 & 0 & 0 & 0 & 0 \\ 5 & 3 & -1 & 0 & 0 & 0 & 0 \\ 1 & 2 & 6 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 3 & 7 & 0 & 0 \\ 0 & 0 & 0 & -2 & 4 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 5 \\ 0 & 0 & 0 & 0 & 0 & 4 & 3 \end{pmatrix}$$

Мы видим, что вдоль диагонали как бы нанизаны детерминанты разных порядков (в данном примере третьего, второго, и еще второго), а остальные элементы равны нулю. Общая схема квази-диагональной матрицы такая: вдоль диагонали идут разной величины квадраты, заполненные числами (на рисунке они заштрихованы), а остальные элементы (вне этих квадратов) равны нулю. В зависимости от числа этих квадратов, от их величин и от их последовательности квази-диагональные матрицы даже одного и того

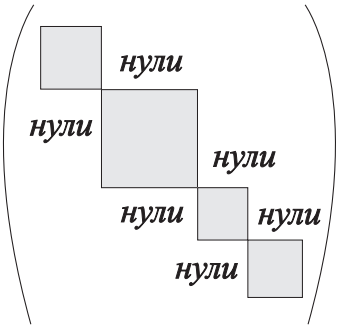


Схема квази-диагональной матрицы

[78] Это обозначение не следует смешивать с символом Кронекера (§ 25).

[79] Отсюда следует, что все неособенные диагональные матрицы данного порядка образуют группу относительно умножения.

же порядка могут иметь различную структу-
ру. Мы будем считать, что две квази-диагональные матрицы имеют одну и ту же структуру, если обе они образованы по одной и той же схеме (т. е. вдоль диагоналей обеих матриц идут квадраты одинаковой величины и в одинаковой последовательности). Если A — квази-диагональная матрица, то обозначим через $A_1, A_2, \ldots, A_k$ матрицы, стоящие в заштрихованных квадратах схемы матрицы A (пусть k — их число); мы будем обозначать:

$$A = [A_1, A_2, \ldots, A_k].$$

Так, в приведенном выше примере $k = 3$, $A_1 = \begin{pmatrix} 4 & 1 & 2 \\ 5 & 3 & -1 \\ 1 & 2 & 6 \end{pmatrix}$, $A_2 = \begin{pmatrix} 3 & 7 \\ -2 & 4 \end{pmatrix}$, $A_3 = \begin{pmatrix} 15 & \\ 4 & 3 \end{pmatrix}$.

Пусть $B = [B_1, B_2, \ldots, B_k]$ матрица той же структуры, что и A, т. е. B_1 того же порядка, что и A_1, B_2 — того же порядка, что и A_2 и т. д., B_k того же порядка, что и A_k. Тогда легко убедиться, что

$$A + B = [A_1 + B_1, A_2 + B_2, \ldots, A_k + B_k]$$
$$AB = [A_1B_1, A_2B_2, \ldots, A_kB_k].$$

Но $AB \neq BA$, ибо вообще, $A_1B_1 \neq B_1A_1$ и т. д. Итак, чтобы сложить или перемножить квази-диагональные матрицы одной и той же структуры, надо сложить или перемножить их составные части, соответствующие друг другу. Наконец, по теореме § 34 убеждаемся, что:

$$|A| = |A_1|\,|A_2| \cdots |A_k|. \tag{41}$$

Пусть A — неособенная матрица n-го порядка, а A_λ матрицы n_λ-го порядка ($\lambda = 1, 2, \ldots, k$); по (41) все A_λ также являются неособенными матрицами и $n_1 + n_2 + \ldots + n_k = n$. Линейная подстановка, соответствующая матрице A, такова, что первые n_1 переменных преобразовываются в новые n_1 переменных, следующие n_2 переменных — отдельно в новые n_2 переменных, и т. д. Будем рассматривать линейную подстановку как преобразование координат в n-мерном пространстве с оставлением того же начала; тогда в случае, когда матрица подстановки квази-диагональная, дело можно представить так, что отдельно преобразовываются координаты в $_1$-мерном пространстве, отдельно — в n_2-мерном, и т. д., отдельно в n_k-мерном, где все эти k пространств лежат в данном n-мерном, переходят через точку 0 и кроме этой точки никакая пара этих пространств не имеет общих точек, — всякая же точка всего n-мерного пространства вполне определяется своими проекциями в эти k пространств.

§ 167. Подобные матрицы. Когредиентные и контрагредиентные преобразования. В этом параграфе мы рассматриваем квадратные матрицы одного и того же порядка n.

Матрицы A и B называются *подобными*, если существует такая неособенная матрица P, что

$$AP = PB \qquad \text{или} \qquad P^{-1}AP = B.$$

Говорят иначе, что A переходит в B *преобразованием посредством* P.

Для этого понятия подобия верны три основных закона равенств (§ 2, примечание 1): 1) если A подобно B, то и B подобно A, ибо из $P^{-1}AP = B$ следует $(P^{-1})^{-1}BP^{-1} = A$, и P^{-1}, как и P, неособенная матрица; 2) если A подобна B, а B подобна C, то и A подобна C, ибо из $P^{-1}AP = B$, $Q^{-1}BQ = C$ следует: $(PQ)^{-1}A(PQ) = C$, и PQ неособенная матрица; 3) A всегда подобна A, ибо $E^{-1}AE = A$.

Имеем, далее: если $B = P^{-1}AP$, то

$$|B| = |P|^{-1}|A|\,|P| = |A|,$$

ибо для произведения детерминантов коммутативный закон верен. Следовательно, *подобные неособенные матрицы имеют один и тот же детерминант; если же одна из подобных матриц особенная, то и другая тоже.* Из последней теоремы § 156 следует, что *подобные матрицы имеют один и тот же ранг*, ибо из $B = P^{-1}AP$ следует, что ранг $\leq$ рангу , а из $A = PBP^{-1}$ следует, что ранг $A \leq$ рангу B.

Будем обозначать подобие знаком $\sim$. Имеем:

1) *Если* $A \sim B$, *то и* $A^{-1} \sim B^{-1}$. Действительно, если $B = P^{-1}AP$, то, переходя к обратным матрицам, по (22) § 158 имеем:

$$B^{-1} = P^{-1}A^{-1}P;$$

при этом видим, что B получается из A преобразованием посредством того же элемента P, посредством которого и B получается из A.

2) *Если* $A \sim B$, *то и* $A' \sim B'$. Ибо из $B = P^{-1}AP$, переходя к транспонированным матрицам, получаем по теореме и следствию 1 § 160: $B' = P'A'(P')^{-1}$.

3) *Если* $A \sim B$, *то и* $A^\lambda \sim B^\lambda$ *при любом целом* $\lambda \neq 0$. Пусть $B = P^{-1}AP$; тогда при $\lambda > 0$

$$B^\lambda = \underbrace{P^{-1}APP^{-1}AP\cdots P^{-1}AP}_{\lambda \text{ раз}} = P^{-1}AEAE\cdots EAP =$$
$$= P^{-1}\underbrace{AA\cdots A}_{\lambda \text{ раз}}P = P^{-1}AP.$$

При $\lambda < 0$ это же получается из 2).

4) *Если* A, B *посредством* P *преобразовывается в* A_1, B_1, *то* $A + B$ *и* AB *посредством* P *преобразовываются в* $A_1 + B_1$ *и* A_1B_1. Ибо

$$P^{-1}(A + B)P = P^{-1}AP + P^{-1}BP = A_1 + B_1,$$
$$P^{-1}(AB)P = P^{-1}APP^{-1}BP = A_1B_1.$$

Обратимся теперь к самим линейным подстановкам, причем будем пользоваться символическим обозначением § 156, а именно, будем обозначать через (x) совокупность (столбец) переменных $x_1, x_2, \ldots, x_n$, а через

$$(x) = A(y) \tag{42}$$

саму линейную подстановку с матрицей A. Пусть $P^{-1}AP = A_1$, $(x) = P(\xi)$, $(y) = P(\eta)$; тогда $(\xi) = P^{-1}(x)$; подставляя сюда $A(y)$ вместо (x) и $P(\eta)$ вместо (y), получим:

$$(\xi) = P^{-1}AP(\eta) = A_1(\eta). \tag{43}$$

Переменные (x), (y), с одной стороны, и (ξ), (η) — с другой, называются *когредиентными*, а преобразования (42) и (43) — *когредиентними преобразованиями.* Преобразование (42) можно рассматривать геометрически как преобразование n-мерного пространства, или как отображение одного n-мерного пространства на другое; подстановку же $(x) = P(\xi)$ можно рассматривать как преобразование координат в данном n-мерном пространстве, а именно — переход от координат (x) к координатам (ξ); аналогично, $(y) = P(\eta)$ есть то же самое преобразование координат, только в другом пространстве. Тогда когредиентные преобразования (42) и (43) дают одно и то же отображение одного пространства на другое, только в разных системах координат.

Рассматриваются еще *контрагредиентные* преобразования; это — два таких преобразования:

$$(x) = A(y), \qquad (\eta) = A'(\xi), \tag{44}$$

где A' матрица, транспонированная по отношению к A (§ 160). Напишем (44) подробнее:

$$x_\lambda = \sum_{\mu=1}^{n} a_{\lambda\mu} y_\mu \qquad (\lambda = 1, 2, \ldots, n),$$
$$\eta_\mu = \sum_{\lambda=1}^{n} a_{\lambda\mu} \xi_\lambda \qquad (\mu = 1, 2, \ldots, n).$$

Умножим обе части первого из этих уравнений на ξ_λ, просуммируем по λ и примем во внимание второе уравнение; получим:

$$\sum_{\lambda=1}^{n} x_\lambda \xi_\lambda = \sum_{\lambda=1}^{n} \sum_{\mu=1}^{n} a_{\lambda\mu} y_\mu \xi_\lambda = \sum_{\mu=1}^{n} y_\mu \sum_{\lambda=1}^{n} a_{\lambda\mu} \xi_\lambda = \sum_{\mu=1}^{n} y_\mu \eta_\mu.$$

Итак, между контрагредиентными переменными (x), (y) и (ξ), (η) существует соотношение:

$$x_1\xi_1 + x_2\xi_2 + \ldots + x_n\xi_n = y_1\eta_1 + y_2\eta_2 + \ldots + y_n\eta_n. \tag{45}$$

Обратно, если (45) существует, и $(x) = A(y)$, причем (y) — независимые переменные, то и $(\eta) = A'(\xi)$.

§ 168. Рациональные функции от матрицы. Пусть A — данная квадратная матрица n-го порядка и

$$g(r) = a_0 + a_1 r + a_2 r^2 + \ldots + a_m r^m$$

данная целая рациональная функция от переменной r с численными коэфициентами; выражение:

$$g(A) = a_0 E + a_1 A + a_2 A^2 + \ldots + a_m A^m$$

есть некоторая квадратная матрица n-го порядка; если $A = (a_{\alpha\beta})$, то элементы матрицы $g(A)$ будут [§ 163, (31) и (32)]:

$$a_0 e_{\alpha\beta} + a_1 a^{(1)}_{\alpha\beta} + a_2 a^{(2)}_{\alpha\beta} + \ldots + a_m a^{(m)}_{\alpha\beta},$$

где мы вообще через $a_{\alpha\beta}^{(k)}$ обозначаем элементы матрицы A^k; для них имеет место следующая формула приведения:

$$a_{\alpha\beta}^{(k)} = \sum_{\lambda=1}^{n} a_{\alpha\lambda}^{(k-1)} a_{\lambda\beta}, \qquad k = 2, 3, 4, \ldots; \tag{46}$$

при этом $a_{\alpha\beta}^{(1)} = a_{\alpha\beta}$.

Матрица $g(A)$ называется *целой рациональной функцией от матрицы* A. Заметим, что A может быть и особенной матрицей, равно как и $g(A)$ может оказаться неособенной или особенной.

Пусть $h(A) = b_0E + b_1A + b_2A^2 + \ldots + b_kA^k$ — другая целая рациональная функция той же матрицы A. Легко видеть, что всякие две целые рациональные функции одной и той же матрицы всегда переместимы, ибо всякие две степени одной и той же матрицы переместимы. Если детерминант

$$|h(A)| \neq 0,$$

т. е. матрица $h(A)$ неособенная (что между прочим может случиться и при особенной A), то существует матрица:

$$f(A) = g(A) \cdot h(A)^{-1} = h(A)^{-1} \cdot g(A) = \frac{f(A)}{g(A)};$$

назовем ее *дробной рациональной функцией матрицы* A. Заметим, что $f(A)$ особенная или неособенная одновременно с $g(A)$.

На основании результатов § 160 и 163 выводим:

$$f(A)' = f(A').$$

Далее, на основании 3) и 4) § 167 выводим для целой рациональной функции:

$$P^{-1}g(A)P = g(P^{-1}AP).$$

Пример. Пусть $f(r) = \dfrac{5 + r - r^2}{1 + r^2}$, $A = \begin{pmatrix} 1 & 4 \\ 2 & 9 \end{pmatrix}$; имеем:

$$A^2 = \begin{pmatrix} 9 & 40 \\ 20 & 89 \end{pmatrix}, \qquad E + A^2 = \begin{pmatrix} 10 & 40 \\ 20 & 90 \end{pmatrix},$$

$$\begin{pmatrix} 10 & 40 \\ 20 & 90 \end{pmatrix}^{-1} = \begin{pmatrix} 90 & -40 \\ -20 & 10 \end{pmatrix} \cdot \frac{1}{100} = \frac{1}{10} \begin{pmatrix} 9 & -4 \\ -2 & 1 \end{pmatrix},$$

$$5E + A - A^2 = -2 \begin{pmatrix} 6 & 38 \\ 19 & 82 \end{pmatrix},$$

$$f(A) = \frac{5E + A - 2A^2}{1 + A^2} = -2 \begin{pmatrix} 6 & 38 \\ 19 & 82 \end{pmatrix} \cdot \frac{1}{10} \begin{pmatrix} 9 & -4 \\ -2 & 1 \end{pmatrix} = -\frac{1}{5} \begin{pmatrix} -22 & 14 \\ 5 & -6 \end{pmatrix}.$$

Упражнения

214) Вычислить $g(A)$, где $A = \begin{pmatrix} 3 & 5 & -1 \\ 0 & 1 & 2 \\ 2 & -1 & 0 \end{pmatrix}$, $g(r) = 4 - 2r + r^3$.

Отв. $\begin{pmatrix} 33 & 39 & 37 \\ 16 & 19 & -10 \\ 6 & 45 & 16 \end{pmatrix}$.

215) Вычислить $\dfrac{A+E}{A-2E}$, где $A = \begin{pmatrix} 0 & 1 & 2 \\ 2 & 3 & 4 \\ 1 & 0 & 1 \end{pmatrix}$.

Отв. $\begin{pmatrix} \frac{1}{2} & \frac{1}{2} & 1 \\ 3 & 1 & 6 \\ -\frac{1}{2} & \frac{1}{2} & -1 \end{pmatrix}$.

§ 169. Характеристическое уравнение. Пусть $x_1, x_2, \ldots, x_n$ — декартовы координаты точек в n-мерном пространстве [80]. Тогда линейную подстановку $(x) = A(y)$ (при $|A| \neq 0$) можно рассматривать как взаимно однозначное отображение этого пространства на самоё себя; при этом точка O (начало координат) остается неподвижной (т. е. отображается сама на себя). При этом отображении всякая линейная функция от $x_1, x_2, \ldots, x_n$ переходит в линейную же функцию от $y_1, y_2, \ldots, y_n$, т. е. геометрические образы, выражаемые линейными уравнениями, переходят в образы того же рода; в частности прямая (выражаемая в n-мерном пространстве $n-1$ линейными уравнениями) переходит в прямую же, при этом, если одна из этих прямых проходит через точку O, то и другая тоже проходит через O. Но если прямая проходит через O, то ее уравнения — однородны, т. е. мы имеем систему $n-1$ однородных уравнений с n неизвестными. Такая система вообще точно определяет отношения неизвестных, т. е. проходящая через точку O прямая вполне определяется отношениями координат ее точек:

$$x_1 : x_2 : \ldots : x_n = \xi_1 : \xi_2 : \ldots : \xi_n,$$

где $\xi_1, \xi_2, \ldots, \xi_n$ — данные числа.

Поставим такую задачу: найти прямые, проходящие через точку O, которые преобразованием $(x) = A(y)$ переводятся сами в себя; это — так называемые *инвариантные* прямые относительно данного преобразования. Для такой прямой переменные (x) должны быть пропорциональны переменным (y); это можно выразить так:

$$x_1 = \omega y_1, \quad x_2 = \omega y_2, \ \ldots, \ x_n = \omega y_n,$$

где ω — неравный нулю множитель пропорциональности. Подставив сюда выражения x_λ через y_μ [согласно подстановке $(x) = A(y)$] и заменив опять букву y буквою x, получим:

$$\sum_{\beta=1}^{n} a_{\alpha\beta} x_\beta = \omega x_\alpha \qquad (\alpha = 1, 2, \ldots, n),$$

[80] В геометрических представлениях мы не исключаем из рассмотрения и мнимые элементы.

или, перенеся члены ωx_α в левую часть:

$$\left.\begin{aligned}
&(a_1 1-\omega)x_1+a_{12}x_2+\ldots+a_{1n}x_n=0,\\
&a_2 1x_1+(a_{22}-\omega)x_2+\ldots+a_{2n}x_n=0,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&a_n 1x_1+a_{n2}x_2+\ldots+(a_{nn}-\omega)x_n=0
\end{aligned}\right\} \tag{47}$$

Это — система n линейных однородных уравнения для $x_1, x_2, \ldots, x_n$, имеющая решения $x_1, x_2, \ldots, x_n$, не все равные нулю (ибо x_λ — координаты всякой точки на искомой инвариантной прямой, а все $x_\lambda = 0$ только для точки O). Следовательно (§ 33, следствие 2), детерминант системы равен нулю, и мы имеем уравнение для ω:

$$\begin{vmatrix}
a_{11}-\omega & a_{12} & \ldots & a_{1n}\\
a_{21} & a_{22}-\omega & \ldots & a_{2n}\\
\ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots\\
a_{n1} & a_{n2} & \ldots & a_{nn}-\omega
\end{vmatrix}=0. \tag{48}$$

Это — так называемое *характеристическое уравнение* матрицы A; оно n-й степени; его корни называются *характеристическими числами* [81], а его левая часть — *характеристической функцией* матрицы A; обозначив ее через $\varphi(r)$ так, чтобы ее высший коэфициент был равен единице, имеем:

$$\varphi(r)=(-1)^n\begin{vmatrix}
r-a_{11} & -a_{12} & \ldots & -a_{1n}\\
-a_{21} & r-a_{22} & \ldots & -a_{2n}\\
\ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots\\
-a_{n1} & -a_{n2} & \ldots & r-a_{nn}
\end{vmatrix}=(-1)^n|A-rE|, \tag{49}$$

или

$$\varphi(r)=|rE-A|, \tag{49a}$$

ибо для умножения детерминанта n-го порядка на $(-1)^n$ достаточно умножить на -1 каждую его строку, т. е. изменить у всех его элементов знаки на обратные.

Характеристические числа матрицы A обозначим через $r_1, r_2, \ldots, r_n$; тогда

$$\varphi(r)=(r-r_1)(r-r_2)\cdots(r-r_n). \tag{49b}$$

Положив $r=0$, получим из (49) и (496):

$$r_1 r_2\cdots r_n=|A|, \tag{50}$$

т. е. произведение характеристических чисел равно детерминанту матрицы A. Мы предположили, что $|A|\neq 0$; тогда из (50) следует, что ни одно из характеристических чисел не равно нулю; взяв любое из них за ω, мы из (47) найдем отношения $x_1 : x_2 : \ldots : x_n$, т. е. искомую инвариантную прямую. Мы видим, что таких прямых вообще (если все r_λ различны) имеется n.

Но мы можем формально [формулами (48), (49)] определить характеристические функцию, уравнение и числа и в том случае, когда $|A|=0$, т. е. когда A особенная матрица; только тогда, как показывает (50), одно или несколько характеристических чисел равны нулю.

[81] Иначе собственными значениями матрицы A.

Если мы развернем детерминант $rE - A$, то коэфициент при r^{n-1} окажется равным $-(a_{11} + a_{22} + \ldots + a_{nn})$; следовательно [по формулам Вьета, § 50], сумма характеристических чисел

$$\chi(A) = r_1 + r_2 + \ldots + r_n = a_{11} + a_{22} + \ldots + a_{nn}. \tag{51}$$

Эта сумма чисел r_λ или диагональных коэфициентов матрицы A называется *следом* или *характером* матрицы A. Характеры играют очень большую роль в теории групп.

Уравнения типа (48) очень часто встречаются в разных областях математики и ее приложений; они называются еще *вековыми уравнениями*, ибо к уравнению такого типа приводит в небесной механике исследование вековых возмущений планет.

Пусть

$$g(r) = b_0 r^m + b_1 r^{m-1} + \ldots + b_m = b_0(r - s_1)(r - s_2)\cdots(r - s_m)$$

какая-нибудь целая рациональная функция от r m-степени с корнями $s_1, s_2, \ldots, s_m$. Подставляя A вместо r и E вместо единицы, получим:

$$g(A) = b_0(A - s_1E)(A - s_2E)\cdots(A - s_mE)^{82}.$$

Переходя к детерминантам и принимая во внимание, что детерминант произведения матриц равен произведению детерминантов этих матриц, а также что $|cA| = c^n|A|$, если A матрица n-го порядка и c — скалярный множитель, получим:

$$|g(A)| = b_0^n|A - s_1E|\,|(A - s_2E|\,\cdots\,|A - s_mE|;$$

но

$$|A - rE| = (-1)^n\varphi(r),$$

следовательно:

$$\begin{aligned} |g(A)| &= (-1)^{mn}b_0^n\varphi(s_1)\varphi(s_2)\cdots\varphi(s_m) = \\ &= (-1)^{mn}b_0^n(s_1 - r_1)(s_1 - r_2)\cdots(s_1 - r_n)\cdot \\ &\qquad (s_2 - r_1)(s_2 - r_2)\cdots(s_2 - r_n)\cdot \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ &\qquad (s_m - r_1)(s_m - r_2)\cdots(s_m - r_n)\cdot \end{aligned}$$

или

$$|g(A)| = g(r_1)g(r_2)\cdots g(r_n). \tag{52}$$

Мы видим, что $|g(A)|$ есть не что иное, как результант функций $g(r)$ и $\varphi(r)$.

Пусть $h(A)$ — другая целая рациональная функция матрицы A и $|h(A)| \neq 0$; имеем также:

$$|h(A)| = h(r_1)h(r_2)\cdots h(r_n);$$

[82]Такую подстановку мы имеем право сделать, ибо, перемножив двучлены в правой части и применив формулы Вьета, мы получим $g(A)$, как она определена в § 168. И вообще, если $g(r) = g_1(r)g_2(r)$, то $g(A) = g_1(A) + g_2(A)$.

тогда $f(A)=\dfrac{g(A)}{h(A)}$ — дробная рациональная функция от A, и мы имеем:

$$|f(A)|=\frac{|g(A)|}{|h(A)|}=\frac{g(r_1)g(r_2)\cdots g(r_n)}{h(r_1)h(r_2)\cdots h(r_n)}=f(r_1)f(r_2)\cdots f(r_n),$$

т. е. формула (52) верна и для дробных рациональных функций от A.

Если $f(s)$ — рациональная функция, то $f(s)-r$ — тоже рациональная функция от s; применяя к ней формулу (52), найдем:

$$|f(A)-rE|=[f(r_1)-r][f(r_2)-r]\cdots[f(r_n)-r]. \tag{53}$$

Эта формула показывает, что для матрицы $f(A)$ характеристические числа будут $f(r_1), f(r_2), \ldots, f(r_n)$. Итак:

Теорема. *Если $r_1, r_2, \ldots, r_n$ характеристические числа матрицы A, то $f(r_1)$, $f(r_2), \ldots, f(r_n)$, — характеристические числа $f(A)$, где $f(r)$ — любая рациональная функция.*

Заметим, что у подобных матриц (§ 167) характеристические функции, а следовательно, и характеристические числа одинаковы.

§ 170. Формула Кэли. Обозначим через $F=\widetilde{rE-A}=f_{\alpha\beta}$ матрицу, взаимную с $rE-A$; элементы ее $f_{\alpha\beta}$ — целые рациональные функции (-1)-й степени от r:

$$_{\alpha\beta}=b_{\alpha\beta}+{}_{\alpha\beta}r+d_{\alpha\beta}r^2+\ldots+l_{\alpha\beta}r^{n-1}.$$

Обозначим матрицы:

$$A_0=(b_{\alpha\beta}),\quad A_1=(c_{\alpha\beta}),\quad A_2=(d_{\alpha\beta}),\quad \ldots,\quad A_{n-1}=(l_{\alpha\beta}).$$

Тогда по формулам (31), (32) § 163

$$F=A_0r+A_1r+A_2r^2+\ldots+A_{n-1}r^{n-1}.$$

По формуле (38) § 166

$$\widetilde{rE-A}(rE-A)=\varphi(r)E,$$

так как $|Er-A|=\varphi(r)$. Пусть

$$\varphi(r)=a_0+a_1r+a_2r^2+\ldots+a_nr^n$$

(причем $a_n=1$); тогда

$$\begin{gathered}(A_0r+A_1r+A_2r^2+\ldots+A_{n-1}r^{n-1})(-A+rE)=\\=(a_0+a_1r+a_2r^2+\ldots+a_nr^n)E.\end{gathered}$$

Это — тождество; следовательно коэфициенты при одинаковых степенях r должны быть равны:

$$\begin{aligned}-A_0A &= a_0E,\\ -A_1A+A_0, &= a_1E\\ -A_2A+A_1, &= a_2E\\ \cdots\cdots&\cdots\cdots\\ -A_{n-1}A+A_{n-2}, &= a_{n-1}E\\ +A_{n-1} &= a_nE.\end{aligned}$$

Умножаем первое из этих равенств на E, второе на A, третье на A^2 и т. д., последнее на A^n и складываем; получаем:

$$0 = a_0E + a_1A + a_2A^2 + \ldots + a_nA^n$$

или

$$\varphi(A) = 0.$$

Итак:

Теорема. *Если $\varphi(r) = 0$ характеристическая функция матрицы A, то тождественно*

$$\varphi(A) = 0. \tag{54}$$

Это так называемое *соотношение Кэли* (Cayley). Оно показывает, что матрицы $E, A, A^2, \ldots, A^n$ *линейно зависимы*. Вообще следует заметить, что линейно независимых матриц n-го порядка существует только n^2. Именно, обозначим через $C_{\varkappa\lambda}$ матрицу, у которой элемент $a_{\varkappa\lambda} = 1$ (при определенных $\varkappa$ и λ), а остальные элементы равны нулю. Таких матриц $C_{\varkappa\lambda}$ всего существует n^2, и все они, очевидно, линейно независимы. Всякая же другая матрица $A = (a_{\alpha\beta})$ зависит линейно от $C_{\varkappa\lambda}$, именно:

$$A = \sum_{\varkappa,\lambda} a_{\varkappa\lambda}C_{\varkappa\lambda}.$$

Таким образом и линейно независимых степеней матрицы A может существовать не больше n^2; но соотношение Кэли показывает, что их не больше n; на самом же деле их может быть и еще меньше.

Обозначим через $\theta(r)$ общий наибольший делитель всех элементов $f_{\alpha\beta}$ матрицы F; $\theta(r)$ — целая рациональная функция от r; тогда $F = \theta(r) \cdot G$, где G тоже матрица n-го порядка, элементы которой целые рациональные функции от r. Но F — взаимная матрица с $rE - A$, т. е. элементы $f_{\alpha\beta}$ матрицы F — миноры $(n-1)$-го порядка матрицы $rE - A$ или детерминанта $|rE - A| = \varphi(r)$. Разложив этот детерминант по элементам какого-либо ряда, получим в качестве коэфициентов $f_{\alpha\beta}$; а так как все $f_{\alpha\beta}$ делятся на $\theta(r)$, то и $\varphi(r)$ раздедится на $\theta(r)$:

$$\varphi(r) = \theta(r)\psi(r),$$

где $\psi(r)$ тоже целая рациональная функция от r. Но мы ведь имеем:

$$F \cdot (rE - A) = \varphi(r)E;$$

мы видим, что обе части делятся на $\theta(r)$; сократив на ?(г), получим:

$$G \cdot (rE - A) = \psi(r)E.$$

Отсюда выводим, что

$$\psi(A) \equiv 0, \tag{55}$$

совершенно аналогично тому, как мы из предыдущего равенства вывели (54). Если функция $\theta(r)$ степени ≥ 1, то $\psi(r)$ будет степени низшей, чем степень $\varphi(r)$.

Докажем теперь, что *если* $\Phi(r)$ *целая рациональная функция, и* $\Phi(A) \equiv 0$, *то* $\Phi(r)$ *делится на* $\psi(r)$, *откуда следует, что (55) есть уравнение наинизшей степени, которому удовлетворяет матрица* A.

Пусть s неопределенное количество; по теореме Декарта (§ 49) $\Phi(r) - \Phi(s)$ делится на $r - s$:

$$\Phi(r) - \Phi(s) \equiv (r - s)\Phi(r, s),$$

где $\Phi(r, s)$ — некоторая целая рациональная функция от r и s. Подставляем в последнем равенстве A вместо s и принимаем во внимание, что по условию $\Phi(A) \equiv 0$; получаем:

$$\Phi(r)E = (rE - A)\Phi(r, A). \tag{56}$$

С другой стороны, мы имели $\psi(r)e = G(rE - A)$. Умножая первое из этих равенств на G, а второе — на $\Phi(r, A)$, и вычитая второе из первого, получим

$$\Phi(r)G = \psi(r)\Phi(r, A).$$

Правая часть делится на $\psi(r)$, следовательно, и левая делится на $\psi(r)$; но элементы матрицы G — частные от деления элементов матрицы F на их общий наибольший делитель $\theta(r)$:

$$g_{\alpha\beta} = \frac{f_{\alpha\beta}}{\theta(r)},$$

т. е. эти элементы $g_{\alpha\beta}$ — взаимно простые, и значит все они не могут делиться на $\psi(r)$; следовательно, $\Phi(r)$ делится на $\psi(r)$, и наше предложение доказано.

Полагая $\Phi(r) = \varphi(r)$, имеем из (56):

$$\varphi(r)E = (rE - A)\Phi(r, A),$$

где $\Phi(r, s)$ какая-то целая рациональная функция от r и s. Умножая полученное равенство на F и принимая во внимание, что $F \cdot (rE - A) = \varphi(r)E$, получим, сократив:

$$F = \Phi(r, A).$$

Но F — взаимная матрица к $rE - A$ при всяком r; положим $r = 0$; тогда F обратится во взаимную матрицу к $-A$, т. е. в $\widetilde{(-A)}$; но $\widetilde{(-A)} = -\widetilde{A}$; итак, получим:

$$\widetilde{A} = -\Phi(0, A),$$

или

Следствие. Взаимная матрица к данной матрице A есть целая рациональная функция от A.

Пример. При $n = 2$ имеем:

$$A = \begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix}, \qquad \varphi(r) = \begin{vmatrix} \alpha - r & \beta \\ \gamma & \delta - r \end{vmatrix} = (\alpha\delta - \beta\gamma) - r(\alpha + \delta) + r^2;$$

формула Кэли дает:

$$\varphi(A) = (\alpha\delta - \beta\gamma)E - (\alpha + \delta)A + A^2 \equiv 0.$$

Имеем:

$$A^2 = \begin{vmatrix} \alpha^2+\beta\gamma & \beta(\alpha+\delta) \\ \gamma(\alpha+\delta) & \beta\gamma+\delta^2 \end{vmatrix};$$

следовательно:

$$\varphi(A) = \begin{vmatrix} \alpha\delta-\beta\gamma-\alpha(\alpha+\delta)+\alpha^2+\beta\gamma & -\beta(\alpha+\delta)+\beta(\alpha+\delta) \\ -\gamma(\alpha+\delta)+\gamma(\alpha+\delta) & \alpha\delta-\beta\gamma-\delta(\alpha+\delta)+\beta\gamma+\delta^2 \end{vmatrix};$$

все четыре элемента в этой матрице действительно равны нулю.

Упражнения

216) Проверить формулу Кэли для матрицы $A = \begin{vmatrix} 3 & 1 & 2 \\ 4 & 1 & 3 \\ 1 & 2 & 1 \end{vmatrix}$.

217) Пусть $A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$; выразить взаимную матрицу $\widetilde{A}$ как целую рациональную функцию от A.

Отв. $\widetilde{A} = (\alpha+\delta)E - A$.

§ 171. Преобразование Крылова и Лузина. Формулы (50) и (51) § 169 дают для характеристического или векового уравнения свободный член и коэфициент при r; но остальные его коэфициенты весьма трудно вычислить вследствие того, что неизвестное r входит только в диагональные элементы детерминанта $A - rE$. Поэтому практически весьма важно так преобразовать вековое уравнение, чтобы неизвестное r вместо диагональных элементов входило в элементы одного какого-нибудь ряда (строки или столбца). Такое преобразование выполнил акад. А. Н. Крылов [83] на основании свойств системы линейных уравнений; акад. Н. Н. Лузин [84] выполнил то же преобразование чисто алгебраическими средствами и подробно исследовал все возможные здесь случаи. Исследования Лузина сильно упростил одесский математик Гантмахер [85].

Обозначим, как и в § 168, через $a^{(k)}_{\alpha\beta}$ элементы матрицы A^k; имеем для них формулу приведения (46). Пусть $x_1, x_2, \ldots, x_n$ независимые друг от друга произвольные параметры; обозначим:

$$x'_\alpha = \sum_{\lambda=1}^{n} a_{\lambda\alpha}x_\lambda = a_{1\alpha}x_1 + a_{2\alpha}x_2 + \ldots + a_{n\alpha}x_n,$$
$$x''_\alpha = \sum_{\lambda=1}^{n} a^{(2)}_{\lambda\alpha}x_\lambda = a^{(2)}_{1\alpha}x_1 + a^{(2)}_{2\alpha}x_2 + \ldots + a^{(2)}_{n\alpha}x_n,$$

и вообще

$$x^{(k)}_\alpha = \sum_{\lambda=1}^{n} a^{(k)}_{\lambda\alpha}x_\lambda = a^{(k)}_{1\alpha}x_1 + a^{(k)}_{2\alpha}x_2 + \ldots + a^{(k)}_{n\alpha}x_n; \qquad (57)$$

[83] А. Н. Крылов, О численном решении уравнения, которым в технических вопросах определяются частоты малых колебаний материальных систем, Известия Академии наук СССР, 1931.

[84] Н. Н. Лузин, О методе академика А. Н. Крылова составления векового уравнения, Известия Академии наук СССР, 1931.

[85] Работа Гантмахера печатается в «Известиях Академии наук СССР».

для всякого целого $k > 0$, $\alpha = 1, 2, \ldots, n$. Подставив в (57) выражение для $a_{\lambda\alpha}^{(k)}$ из (46) (изменив там немного обозначения), получим:

$$x_\alpha^{(k)} = \sum_{\lambda=1}^{n} \left(\sum_{\mu=1}^{n} a_{\lambda\mu}^{(k-1)} a_{\mu\alpha} \right) = \sum_{\mu=1}^{n} \left(\sum_{\lambda=1}^{n} a_{\mu\alpha} \sum_{\lambda=1}^{n} a_{\lambda\mu}^{(k-1)} x_\lambda \right).$$

Но по (57)

$$\sum_{\lambda=1}^{n} a_{\lambda\mu}^{(k-1)} x_\lambda = x_\mu^{(k-1)};$$

следовательно:

$$x_\alpha^{(k)} = \sum_{\mu=1}^{n} a_{\mu\alpha} x_\mu^{(k-1)}. \tag{58}$$

Теперь составим следующее произведение:

$$\begin{vmatrix} x_1 & x_2 & \ldots & x_n \\ x_1' & x_2' & \ldots & x_n' \\ \ldots & \ldots & \ldots & \ldots \\ x_1^{(n-1)} & x_2^{(n-1)} & \ldots & x_n^{(n-1)} \end{vmatrix} \cdot \begin{vmatrix} a_{11} - r & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} - r & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{n1} & a_{n2} & \ldots & a_{nn} - r \end{vmatrix},$$

где второй сомножитель — левая часть нашего векового уравнения. Комбинируя строки множимого со столбцами множителя и применяя формулу (58), найдем, что это произведение равно

$$\begin{pmatrix} x_1' - rx_1 & x_2' - rx_2 & \ldots & x_n' - rx_n \\ x_1'' - rx_1' & x_2'' - rx_2' & \ldots & x_n'' - rx_n 1 \\ \ldots & \ldots & \ldots & \ldots \\ x_1^{(n)} - rx_1^{(n-1)} & x_2^{(n)} - rx_2^{(n-1)} & \ldots & x_n^{(n)} - rx_n^{(n-1)} \end{pmatrix}.$$

Этот детерминант (§ 30, VI) можно представить в виде:

$$\begin{pmatrix} 1 & x_1 & x_2 & \ldots & x_n \\ 0 & x_1' - rx_1 & x_2' - rx_2 & \ldots & x_n' - rx_n \\ 0 & x_1'' - rx_1' & x_2'' - rx_2' & \ldots & x_n'' - rx_n' \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & x_1^{(n)} - rx_1^{(n-1)} & x_2^{(n)} - rx_2^{(n-1)} & \ldots & x_n^{(n)} - rx_n^{(n-1)} \end{pmatrix};$$

в этом новом детерминанте прибавим к элементам 2-й строки элементы 1-й, умноженные на r (§ 30, V, следствие 2); после этого прибавим к элементам 3-й строки элементы 2-й, умноженные на r; после этого прибавим к элементам 4-й строки элементы 3-й, умноженные на r, и т. д.; получим:

$$\begin{pmatrix} 1 & x_1 & x_2 & \ldots & x_n \\ r & x_1' & x_2' & \ldots & x_n' \\ r^2 & x_1'' & x_2'' & \ldots & x_n'' \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ r^n & x_1^{(n)} & x_2^{(n)} & \ldots & x_n^{(n)} \end{pmatrix} = \Phi(r).$$

Итак, вековое уравнение можно заменить уравнением $\Phi(r) = 0$. Его левая часть — детерминант $(n+1)$-го порядка, но неизвестное r входит только в первый столбец.

Это преобразование возможно, если только детерминант

$$\begin{vmatrix} x_1 & x_2 & \dots & x_n \\ x_1' & x_2' & \dots & x_n' \\ \dots & \dots & \dots & \dots \\ x_1^{(n-1)} & x_2^{(n-1)} & \dots & x_n^{(n-1)} \end{vmatrix}$$

отличен от нуля; таким образом значения наших параметров $x_1, x_2, \dots, x_n$ следует выбрать так, чтобы названный детерминант не обратился в нуль. Это возможно всегда за исключением случая, когда он тождественно равен нулю. Однако этого случая мы здесь разбирать не будем.

Пример. Преобразовать уравнение

$$\begin{vmatrix} 3-r & 2 & 1 \\ -1 & 2-r & 2 \\ 2 & 1 & 1-r \end{vmatrix} = 0$$

способом Крылова и Лузина.

Здесь $n = 3$, $A = \begin{vmatrix} 3 & 2 & 1 \\ -1 & 2 & 2 \\ 2 & 1 & -1 \end{vmatrix}$; находим

$$A^2 = \begin{vmatrix} 9 & 11 & 8 \\ -1 & 4 & 5 \\ 7 & 7 & 5 \end{vmatrix}, \qquad A^3 = \begin{vmatrix} 32 & 48 & 39 \\ 3 & 11 & 12 \\ 24 & 33 & 26 \end{vmatrix}.$$

Пусть $x_1 = 1$, $x_2 = x_3 = 0$; тогда по (57) $x_\alpha^{(k)} = a_{1\alpha}^{k)}$, или $x_1' = 3$, $x_2' = 2$, $x_3' = 1$, $x_1'' = 9$, $x_2'' = 11$, $x_3'' = 8$, $x_1''' = 32$, $x_2''' = 48$, $x_3''' = 39$. Следовательно, преобразованное уравнение будет

$$\begin{vmatrix} 1 & 1 & 0 & 0 \\ r & 3 & 2 & 1 \\ r^2 & 9 & 11 & 8 \\ r^3 & 32 & 48 & 39 \end{vmatrix} = 0.$$

Замечание. Мы видим, что при таком выборе значений x_1, x_2, x_3 нам достаточно знать только первые строки в A^2 и A^3.

Упражнения

218) Преобразовать способом Крылова и Лузина уравнение:

$$\begin{vmatrix} 2-r & -8 \\ 4 & 5-r \end{vmatrix} = 0.$$

Отв.

$$\begin{vmatrix} 1 & 1 & 0 \\ r & 2 & -8 \\ r^2 & -28 & -56 \end{vmatrix} = 0.$$

§ 172. Некоторые частные виды матриц. *Симметрической матрицей* называется такая матрица, которая не изменяется от перестановки строк со столбцами, т. е. которая тождественна со своей транспонированной (§ 160):

$$A = A'.$$

Иными словами, симметрическая матрица симметрична относительно своей диагонали; если $A = (a_{\alpha\beta})$, то для симметрической матрицы $a_{\alpha\beta} = a_{\beta\alpha}$ для всех α и β.

Полусимметрической (иначе — *косой симметрической*, *альтернирующей*) матрицей называется матрица, меняющая знак от перестановки строк со столбцами; иными словами, это такая матрица B, что:

$$B' = -B.$$

Если $B = (b_{\alpha\beta})$, то $b_{\alpha\beta} = -b_{\beta\alpha}$ для всех α и β; отсюда, в частности, следует при $\alpha = \beta$, что $b_{\alpha\alpha} = -b_{\alpha\alpha} = 0$, т. е. *в полусимметрической матрице все диагональные элементы равны нулю.*

Пусть P — любая квадратная матрица, P' — ее транспонированная; тогда легко видеть, что $A = P + P'$ есть симметрическая, а $B = P - P'$ — полусимметрическая матрица. Но отсюда, обратно:

$$P = \frac{1}{2}(A + B) = \frac{1}{2}A + \frac{1}{2}B.$$

Очевидно, что $\frac{1}{2}A$ тоже симметрическая, а $\frac{1}{2}B$ — полусимметрическая матрицы. Следовательно, *всякая квадратная матрица представляется в виде суммы симметрической и полусимметрической матриц.*

Докажем однозначность этого представления. Пусть

$$P = S + T,$$

где S — симметрическая (т. е. $S' = S$), а T — полусимметрическая (т. е. $T' = -T$). Тогда мы имеем:

$$P' = S - T.$$

Отсюда

$$S = \frac{1}{2}(P + P' = \frac{1}{2}A, \qquad T = \frac{1}{2}(P - P') = \frac{1}{2}B,$$

что и доказывает однозначность представления,

До сих пор мы не ставили никаких условий для элементов наших матриц: эти элементы могли быть любыми комплексными числами. Нами мы в данной матрице A заменим все ее элементы $a_{\alpha\beta}$ сопряженными комплексными числами $\overline{a}_{\alpha\beta}$ (если в частности $a_{\alpha\beta}$ вещественна, то, конечно, $\overline{a}_{\alpha\beta} = a_{\alpha\beta}$), то получим *сопряженную* с A матрицу $\overline{A}$.

Эрмитовой матрицей [86] называется такая матрица, которая при перестановке строк со столбцами переходит в свою сопряженную; иначе, это такая матрица A, для которой транспонированная совпадает с сопряженной, т. е.

$$A' = \overline{A}.$$

[86] По фамилии французского математика Эрмита (Hermite), который ввел в рассмотрение такие матрицы.

Таким образом для нее $a_{\alpha\beta} = \overline{a}_{\beta\alpha}$; в частности, при $\alpha = \beta$ $a_{\alpha\alpha} = \overline{a}_{\alpha\alpha}$, и, следовательно, все ее диагональные элементы вещественны.

Заметим, что если все элементы эрмитовой матрицы вещественны, то такая эрмитова матрица является симметрической.

§ 173. Ортогональные матрицы. Так называются матрицы $A = a_{\alpha\beta}$, отличающиеся свойством

$$AA' = E, \tag{59}$$

иными словами:

$$A' = A^{-1}. \tag{59a}$$

Уравнение (59) равносильно таким уравнениям:

$$\sum_{\lambda=1}^{n} a_{\alpha\lambda} a_{\beta\lambda} = e_{\alpha\beta}, \tag{59b}$$

где, как и раньше, $e_{\alpha\beta} = 1$ при $\alpha = \beta$ и $e_{\alpha\beta} = 0$ в остальных случаях. Уравнений (59б) всего $\dfrac{n(n+1)}{2}$; их выражают словами, говоря, что строки матрицы A образуют нормирование-ортогональную систему. Но из (59) следует также:

$$A/A = E, \tag{59}$$

и обратно. Уравнение (59в) дает:

$$\sum_{\lambda=1}^{n} a_{\lambda\alpha} a_{\lambda\beta} = e_{\alpha\beta}, \tag{59}$$

эти $\dfrac{n(n+1)}{2}$ уравнений показывают, что и столбцы матрицы A образуют нормированно-ортогональную систему. Итак, мы видим, что ортогональность столбцов матрицы вытекает из ортогональности строк, и обратно.

Далее, из (59) и из того, что $|A'| = |A|$, следует:

$$|A|^2 = 1, \qquad \text{т. е. } = \pm 1.$$

Если $|A| = +1$, то ортогональная матрица A называется *собственно ортогональной*; если $|A| = -1$, то A — *несобственно ортогональная* матрица.

Пусть A и B две ортогональные матрицы, т. е. $A^{-1} = A'$; $B^{-1} = B'$; тогда $B^{-1}A^{-1} = B'A'$; по (22) § 158 и по теореме § 160 это дает:

$$(AB)^{-1} = (AB)',$$

т. е. произведение двух ортогональных матриц — тоже ортогональная матрица. Очевидно, далее, что произведение двух собственно ортогональных или двух несобственно ортогональных матриц — собственно ортогональная матрица, а произведение собственно ортогональной на несобственно ортогональную, или, обратно, — несобственно ортогональная матрица. Единичная матрица E собственно ортогональная, ибо $E^{-1} = E' = E$, $|E| = 1$. Наконец, совершенно очевидно, что если A — ортогональная матрица, то и A^{-1} тоже, ибо $(A^{-1})^{-1} = (A')' = A$.

Из всего этого следует, что все ортогональные матрицы данного порядка составляют группу, а из них собственно ортогональные составляют подгруппу этой группы.

Рассмотрим теперь *ортогональную подстановку*; т. е. линейную подстановку с ортогональной матрицей A. Соотношение (59) показывает, что такая подстановка контрагредиентна к своей обратной [§ 167, (44)], а отсюда и из (45) следует, что если $(x) = A(y)$, то

$$x_1^2 + x_2^2 + \ldots + x_n^2 = y_1^2 + y_2^2 + \ldots + y_n^2. \tag{60}$$

Это легко проверить непосредственно:

$$x_\alpha = \sum_{\beta=1}^{n} a_{\alpha\beta} y_\beta, \qquad \sum_{\alpha=1}^{n} x_\alpha^2 = \sum_{\alpha=1}^{n} \left(\sum_{\beta=1}^{n} a_{\alpha\beta} y_\beta \right)^2 = \sum_{\alpha=1}^{n} \sum_{\beta,\gamma=1}^{n} a_{\alpha\beta} a_{\alpha\gamma} y_\beta y_\gamma,$$

или

$$\sum_{\alpha=1}^{n} x_\alpha^2 = \sum_{\beta,\gamma=1}^{n} y_\beta y_\gamma \sum_{\alpha=1}^{n} a_{\alpha\beta} a_{\alpha\gamma}.$$

Но по (59г) $\sum\limits_{\alpha=1}^{n} a_{\alpha\beta} a_{\alpha\gamma} = e_{\beta\gamma}$; следовательно:

$$\sum_{\alpha=1}^{n} x_\alpha^2 = \sum_{\beta,\gamma=1}^{n} e_{\beta\gamma} y_\beta y_\gamma = \sum_{\beta=1}^{n} y_\beta^2,$$

и равенство (60) доказано. Равенство (60) показывает, что выражение $x_1^2 + x_2^2 + \ldots + x_n^2$ есть *инвариант* для группы ортогональных подстановок. Обратно, пусть нам дано теперь (60), и мы ищем все линейные подстановки, для которых (60) выполнено; пусть

$$x_\alpha = \sum_{\beta=1}^{n} a_{\alpha\beta} y_\beta \qquad (\alpha = 1, 2, \ldots, n)$$

такая подстановка; подставляя в (60) вместо x_α эти выражения, найдем:

$$\sum_{\alpha=1}^{n} \sum_{\beta,\gamma=1}^{n} a_{\alpha\beta} a_{\alpha\gamma} y_\beta y_\gamma = \sum_{\beta=1}^{n} y_\beta^2,$$

или

$$\sum_{\beta,\gamma=1}^{n} y_\beta y_\gamma \sum_{\alpha=1}^{n} a_{\alpha\beta} a_{\alpha\gamma} = \sum_{\beta,\gamma=1}^{n} e_{\beta\gamma} y_\beta y_\gamma,$$

а так как y_λ — независимые переменные, то коэфициенты при $y_\beta y_\gamma$ должны быть равны, т. е. $\sum\limits_{\alpha=1}^{n} a_{\alpha\beta} a_{\alpha\gamma} = e_{\beta\gamma}$. Но это равносильно условию (59в), и значит наша подстановка или матрица $A = (a_{\alpha\beta})$ должна быть ортогональна.

Название «ортогональная» подстановка имеет геометрическое происхождение: пусть $x_1, x_2, \ldots, x_n$ координаты точки в n-мерном пространстве при *ортогональной*

системе координат; тогда ортогональная подстановка преобразовывает эту систему координат в ортогональную же. Так, в случаях $n = 2$ и $n = 3$ формулы (59) (59г) обращаются в известные из аналитической геометрии формулы преобразования прямоугольных координат. При этом при $|A| = +1$ мы имеем просто вращение системы координат из старого положения в новое, а в случае $|A| = -1$ мы имеем вращение вместе с отражением (при $n = 2$ — от прямой, при $n = 3$ — от плоскости). Выражение

$$x_1^2 + x_2^2 + \ldots + x_n^2$$

есть расстояние точки $(x_1, x_2, \ldots, x_n)$ от точки 0; естественно, что при перемене координат оно не должно меняться.

Унитарная матрица находится в таком же соотношении с ортогональной, в каком эрмитова матрица — с симметрической. Определяется унитарная матрица $A = (a_{\alpha\beta})$ формулой:

$$A\overline{A}' = E \tag{61}$$

или

$$\overline{A}' = A^{-1} \qquad \text{или} \qquad A' = \overline{A}^{-1} \tag{61}$$

или

$$\sum_{\lambda=1}^{n} a_{\alpha\lambda}\overline{a}_{\beta\lambda} = e_{\alpha\beta} =; \tag{61}$$

в частности при $\alpha = \beta$

$$\sum_{\lambda=1}^{n} |a_{\alpha\beta}|^2 = 1.$$

Равенств (61б) и здесь всего $\dfrac{n(n+1)}{2}$. Формула (61) равносильна такой:

$$\overline{A}'A = E \tag{61}$$

или

$$\sum_{\lambda=1}^{n} a_{\lambda\alpha}\overline{a}_{\lambda\beta} = e_{\alpha\beta}; \tag{61}$$

в частности

$$\sum_{\lambda=1}^{n} |a_{\lambda\alpha}|^2 = 1.$$

Абсолютная величина детерминанта $|A|$ и здесь равна единице; произведение двух унитарных матриц тоже унитарная матрица. Для унитарных преобразований выражение

$$x_1\overline{x}_1 + x_2\overline{x}_2 + \ldots + x_n\overline{x}_n = |x_1|^2 + |x_2|^2 + \ldots + |x_n|^2$$

является инвариантом (предлагается читателю проверить это вычислением — совершенно аналогично выводу подобного же свойства ортогональных преобразований).

Если элементы унитарной матрицы все вещественны, то она совпадает с ортогональной.

Упражнение

219) Доказать, что матрица $\frac{1}{22}\begin{pmatrix}12 & 4 & 18\\ 12 & -18 & -4\\ 14 & 12 & -12\end{pmatrix}$ ортогональна.

§ 174. Квадратичные формы. Квадратичная форма есть однородная функция второй степени от n переменных $x_1, x_2, .., x_n$; обозначим ее так:

$$F = a_{11}x_1^2 + a_{22}x_2^2 + \ldots \quad + \quad a_{nn}x_n^2 + 2a_{12}x_1x_2 + 2a_{13}x_1x_3 + \\ + \quad 2a_{23}x_2x_3 + \ldots = \sum_{\alpha,\beta=1}^{n} a_{\alpha\beta}x_\alpha x_\beta,$$

причем предполагаем, что $a_{\alpha\beta} = a_{\beta\alpha}$.

Матрица этой формы $A = (a_{\alpha\beta})$ — симметрическая (§ 172).

Мы видим, что квадратичная форма получается из билинейной, если в последней оба ряда переменных тождественны друг другу: $y_\alpha = x_\alpha$.

Произведем в нашей форме линейную подстановку $P = (p_\alpha)$:

$$x_\alpha = \sum_{\varkappa=1}^{n} p_{\alpha\varkappa}u_\varkappa;$$

получим:

$$x_\alpha x_\beta = \sum_{\varkappa,\lambda=1}^{n} p_{\alpha\varkappa}p_{\beta\lambda}u_\varkappa u_\lambda$$

и наша форма перейдет в форму:

$$G = \sum_{\alpha,\beta,\varkappa,\lambda} a_{\alpha\beta}p_{\alpha\varkappa}p_{\beta\lambda}u_\varkappa u_\lambda = \sum_{\varkappa,\lambda} b_{\varkappa\lambda}u_\varkappa u_\lambda,$$

где

$$b_{\varkappa\varkappa} = \sum_{\alpha,\beta} a_{\alpha\beta}p_{\alpha\varkappa}p_{\beta\varkappa},$$

а коэфициент при $u_\varkappa u_\lambda$ $(\varkappa \neq \lambda)$ есть

$$2b_{\varkappa\lambda} = \sum_{\alpha,\beta} a_{\alpha\beta}p_{\alpha\varkappa}p_{\beta\lambda} \quad + \quad \sum_{\alpha,\beta} a_{\alpha\beta}p_{\alpha\lambda}p_{\beta\varkappa} = \sum_{\alpha,\beta} a_{\alpha\beta}p_{\alpha\varkappa}p_{\beta\lambda} + \\ + \quad \sum_{\alpha,\beta} a_{\beta\alpha}p_{\beta\lambda}p_{\alpha\varkappa} = 2\sum_{\alpha,\beta} a_{\alpha\beta}p_{\alpha\varkappa}p_{\beta\lambda},$$

ибо

$$a_{\beta\alpha} = a_{\alpha\beta}.$$

Следовательно, и при $\varkappa \neq \lambda$

$$b_{\varkappa\lambda} = \sum_{\alpha,\beta} a_{\alpha\beta}p_{\alpha\varkappa}p_{\beta\lambda}.$$

Если обозначим $B = (b_{\varkappa\lambda})$, то $B = P'AP$; матрица B тоже симметрическая, ибо $B' = B$. Далее

$$|B| = |A| \cdot |P|^2. \tag{62}$$

Если $|A| \neq 0$, то и $|B| \neq 0$; ранг $\leq$ ранга A. Говорят, что G *заключается* или *содержится* в F; F *содержит* G. Если и G содержит F, то F и G *эквивалентны*; в этом случае ранги матриц A и B равны. Если $|P| \neq 0$, то находим: $A = (P^{-1})'BP^{-1}$, т. е. A и B эквивалентны. Следовательно, теоремы 1 и 2 § 164 верны [87] и для квадратичных форм. Мы докажем, что и теоремы 4 и 5 верны для квадратичных форм. Для этого докажем теорему, аналогичную теореме 3 § 164.

Теорема. *Всякую квадратичную форму ранга r можно линейной подстановкой с детерминантом, не равным нулю, преобразовать к нормальной форме:* $H = x_1^2 + x_2^2 + \ldots + x_r^2$.

Воспользуемся леммой § 164.

Здесь

$$R_k = \begin{vmatrix} a_{11} & \ldots & a_{1k} & F_1 \\ \ldots\ldots & \ldots & \ldots\ldots & \ldots\ldots \\ a_{k1} & \ldots & a_{kk} & F_k \\ F_1 & \ldots & F_k & F \end{vmatrix},$$

где

$$F_\alpha = X_\alpha - Y_\alpha = \frac{1}{2}\frac{\partial F}{\partial x_\alpha} = \sum_{\beta=1}^{n} a_{\alpha\beta}x_\beta.$$

R_k — квадратичная форма, зависящая от $x_{k+1}, \ldots, x_n$; если ранг $F = r \leq k$, то $R_k \equiv= 0$. Например, при $k = 1$

$$R_1 = \begin{vmatrix} a_{11} & F_1 \\ F_1 & F \end{vmatrix} = a_{11}F - F_1^2 = a_{11}\sum_{\alpha,\beta=1}^{n} a_{\alpha\beta}x_\alpha x_\beta - \left[\sum_{\alpha,\beta=1}^{n} a_{\alpha\beta}x_\beta\right]^2; \tag{63}$$

отсюда видно, что члены с x_1 действительно сокращаются.

Различим два случая:

1. Не все диагональные элементы в A равны нулю, например $a_{\alpha\alpha} \neq 0$; тогда переставляем x_1 с x_α и достигаем того, что $a_{\alpha\alpha}$ будет стоять на первом месте. Таким образом, не нарушая общности, можно положить $a_{11} \neq 0$. Применяя формулу (63), имеем $a_{11}F = F_1^2 + R_1$. Вводим F_1 вместо x_1, т. е. производим подстановку:

$$F_1 = a_{11}x_1 + a_{12}x_2 + + \ldots + a_{1n}x_n, \quad x_2 = x_2, \quad \ldots, \quad x_n = x_n;$$

ее детерминант:

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & \ldots & a_{1n} \\ 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots \\ 0 & 0 & 0 & \ldots & 1 \end{pmatrix} = a_{11} \neq 0.$$

Теперь подставляем $\dfrac{F_1}{\sqrt{a_{11}}} = u_1$ и получаем: $F = u_1^2 + \dfrac{1}{a_{11}}R_1$, где $\dfrac{1}{a_{11}}R_1$ — форма от $x_2, \ldots, x_n$.

[87] Только здесь преобоазование совершается не двумя, а одной линейной подстановкой.

2. Все диагональные элементы $a_{\alpha\alpha} = 0$. В этом случае рассмотрим детерминанты второго порядка такого вида:

$$\begin{vmatrix} a_{\alpha\alpha} & a_{\alpha\beta} \\ a_{\beta\alpha} & a_{\beta\beta} \end{vmatrix} = -a_{\alpha\beta}^2$$

(это — так называемые «главные» детерминанты второго порядка); они не все равны нулю, так как иначе все элементы $a_{\alpha\beta}$ в A были бы равны нулю. В таком случае, не нарушая общности, можно положить:

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} \neq 0.$$

Берем тогда:

$$R_2 = \begin{vmatrix} 0 & a_{12} & F_1 \\ a_{21} & 0 & F_2 \\ F_1 & F_2 & F \end{vmatrix} = -a_{12}^2 F + 2a_{12}F_1F_2.$$

(Это — квадратичная форма от $x_3, \ldots, c_n$; следовательно:

$$F = \frac{2}{a_{12}} F_1F_2 - \frac{1}{a_{12}^2} R_2.$$

Мы ввели F_1 и ? вместо x_1 и x_2, т. е. сделали подстановку:

$$\begin{aligned} F_1 &= 0 \cdot x_1 + a_{12}x_2 + a_{13}x_3 + \ldots, \\ F_2 &= a_{21}x_1 + 0 \cdot x_2 + a_{23}x_3 + \ldots, \\ x_3 &= x_3, \\ &\ldots\ldots, \\ x_n &= x_n. \end{aligned}$$

Детерминант ее:

$$\begin{vmatrix} 0 & a_{12} & a_{13} & a_{14} & \ldots & a_{1n} \\ a_{21} & 0 & a_{23} & a_{24} & \ldots & a_{2n} \\ 0 & 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 0 & 1 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & 0 & \ldots & 1 \end{vmatrix} = \begin{vmatrix} 0 & a_{12} \\ a_{21} & 0 \end{vmatrix} \cdot \begin{vmatrix} 1 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & 1 \end{vmatrix} = -a_{12}^2 \neq 0.$$

Можно написать:

$$F = \frac{1}{2a_{12}}(F_1 + F_2)^2 - \frac{1}{2a_{12}}(F_1 - F_2)^2 + F_1', \tag{64}$$

где

$$F_1' = -\frac{1}{a_{12}^2} R_2.$$

Обозначим

$$\frac{F_1 + F_2}{\sqrt{2a_{12}}} = u_1, \qquad \frac{F_1 - F_2}{\sqrt{-2a_{12}}} = u_2^2;$$

тогда

$$F = u_1^2 + u_2^2 + F',$$

где F' — форма от $x_3, \ldots, x_n$, с которой мы поступаем также одним из двух указанных способов. Таким образом в конце концов мы преобразуем форму F в $H = u_1^2 + u_2^2 + \ldots + u_r^2$.

Из этой теоремы, как уже было указано, вытекают теоремы, аналогичные теоремам 4 и 5 § 164.

§ 175. Закон инерции квадратичных форм. В предыдущих рассуждениях коэфициенты как самых форм, так и применяемых подстановок предполагались любыми комплексными числами, равно как и наши переменные могли принимать комплексные значения. В настоящем параграфе мы ограничиваемся областью вещественных чисел. Этим мы суживаем понятие эквивалентности форм: формы с вещественными коэфициентами мы считаем эквивалентными, если каждая из них может быть преобразована в другую посредством линейной подстановки с вещественными же коэфициентами. В этом смысле формы, имеющие один и тот же ранг, могут не быть эквивалентными. Выясним, какое же будет здесь необходимое и достаточное условие эквивалентности форм.

В случае первом § 174 мы брали $\dfrac{F_1}{\sqrt{a_{11}}} = u_1$; теперь мы можем так положить только при $a_{11} > 0$; если же $a_{11} < 0$, то мы положим $\dfrac{F_1}{\sqrt{-a_{11}}} = u_1$ и тогда получим $F_1 = -u_1^2 + \dfrac{1}{a_{11}} R_1$.

В случае втором § 174 мы имели (64), где первые два члена в правой части имеют разные знаки, т. е. F в этом случае всегда представляется в виде $F = u_1^2 - u_2^2 + F'$.

Следовательно, форма F всегда преобразовывается в следующую нормальную форму:

$$\varepsilon_1 u_1^2 + \varepsilon_2 u_2^2 + \ldots + \varepsilon_r u_r^2,$$

где $\varepsilon_\lambda = \pm 1$, причем детерминант применяемой подстановки не равен нулю.

Предположим, что из всех ε_λ p равны $+1$, а q равны -1. Конечно, $p + q = r$ (в частных случаях p или q может быть равно нулю). Перенумеровав иначе наши временные, мы получим нормальную форму в таком виде:

$$H = u_1^2 + u_2^2 + \ldots + u_p^2 - u_{p+1}^2 - u_{p+2}^2 - \ldots - u_{p+q}^2.$$

Пусть G другая квадратичная форма с тем же рангом r, которая преобразовывается в такую нормальную форму:

$$H' = v_1^2 + v_2^2 + \ldots + v_{p'}^2 - v_{p'+1}^2 - v_{p'+2}^2 - \ldots - v_{p'+q'}^2,$$

где тоже $p' + q' = r$. Если $p' = p$, $q' = q$; то F и G, очевидно, эквивалентны.

Возникает вопрос: могут ли F и G быть эквивалентными при $p' \neq p$ и, следовательно, $q' \neq q$? Докажем следующее:

Теорема. *Если форма H содержит H'; то должно быть $p \geq p'$, $q \geq q'$.*

Доказательство. Пусть $p < p'$. Если H содержит H'; то существует подстановка:

$$u_\alpha = \sum_{\beta=1}^{n} k_{\alpha\beta} v_\beta \qquad (\alpha = 1, 2, \ldots, n),$$

переводящая H в H' [88]; т. е., сделав эту подстановку, мы должны получить тождество:

$$\begin{gathered} u_1^2 + u_2^2 + \ldots + u_p^2 - u_{p+1}^2 - u_{p+2}^2 - \ldots - u_{p+q}^2 = \\ = v_1^2 + v_2^2 + \ldots + v_{p'}^2 - v_{p'+1}^2 - v_{p'+2}^2 - \ldots - v_{p'+q'}^2, \end{gathered}$$

или

$$\begin{gathered} u_1^2 + u_2^2 + \ldots + u_p^2 + v_{p'+1}^2 + v_{p'+2}^2 + \ldots + v_{p'+q'}^2 = \\ v_1^2 + v_2^2 + \ldots + v_{p'}^2 + u_{p+1}^2 + u_{p+2}^2 + \ldots + u_{p+q}^2; \end{gathered} \tag{65}$$

если $p < p'$, то $p + q' + (n - p' - q') < p' + q' + (n - p' - q') = n$.

Следовательно, число переменных:

$$u_1,\ \ldots,\ u_p,\ v_{p'+1},\ \ldots,\ v_{p'+q'},\ v_{p'+q'+1},\ \ldots,\ v_n$$

меньше, чем n. Но эти переменные можно рассматривать как линейные однородные функции от $v_1, v_2 \ldots, v_n$. Берем систему линейных однородных уравнений:

$$u_1 = 0,\ \ldots,\ u_p = 0,\ v_{p'+1} = 0,\ \ldots,\ v_n = 0 \tag{66}$$

с n неизвестными $v_1, v_2, , \ldots, v_n$; число уравнений меньше n; следовательно, ранг матрицы коэфициентов этой системы меньше n; следовательно, эта система имеет решения, в которых не все неизвестные равны нулю [§ 41 (14)], и при этом, конечно, вещественные решения. Подставим эти решения $v_1, v_2, \ldots, v_n$ в (65); в таком случае левая, а следовательно, и правая часть (65) обратятся в нуль; но правая часть есть сумма квадратов вещественных чисел; следовательно, каждый квадрат будет равен нулю, и мы получим:

$$v_1 = 0,\ \ldots,\ v_{p'} = 0;$$

но мы уже имеем по (66) $v_{p'+1} = 0, \ldots, v_n = 0$; следовательно, все количества $v_1, v_2, \ldots, v_n$ будут равны нулю, тогда как мы только что вывели, что они не все равны нулю. Следовательно наше предположение о том, что $p < p'$; неверно: $p \geq p'$. Совершенно так же мы докажем, что $q \geq q'$.

Следствие. Если H и H' эквивалентны, то $p' = p$, $q' = q$.

Отсюда непосредственно следует, что F н G тогда и только тогда эквивалентны, если у них $p' = p$, $q' = q$. Или:

Каким бы вещественным образом мы ни преобразовывали нашу (вещественную) квадратичную форму F в алгебраическую сумму квадратов, числа получающихся при этом положительных квадратов (p) и отрицательных квадратов (q) одни и те же для всех способов преобразований.

Эта теорема известна под именем *закона инерции квадратичных форм.* Числа p и q являются, таким образом, инвариантами относительно всех вещественных

[88] Хотя H и H' фактически зависят от меньшего, чем n, числа переменных, но мы должны помнить, что общее число переменных у нас n.

линейных преобразований. Число p называется *положительным индексом инерции*, q называется *отрицательным индексом инерции*; $p - q = s$ — *сигнатура* квадратичной формы.

Пример. Привести к нормальному виду форму:

$$F = 3x_1^2 - x_2^3 + 2x_3^2 + 4x_1x_2 - 2x_1x_3 - 6x_2x_3.$$

Имеем здесь $F_1 = \dfrac{1}{2}\dfrac{\partial F}{\partial x_1} = 3x_1 + 2x_2 - x_3$; найдем вычислением:

$$3F - F_1^2 = F' = -7x_2^2 + 5x_3^2 - 14x_2x_3.$$

Следовательно:

$$3F = F_1^2 - 7x_2^2 + 5x_3^2 - 14x_2x_3;$$

этим мы произвели подстановку:

$$x_1 = \frac{1}{3}F_1 - \frac{2}{3}x_2 + \frac{1}{3}x_3, \quad = x_2 = x_2, \quad x_3 = x_3,$$

или

$$\begin{pmatrix} \dfrac{1}{3} & -\dfrac{2}{3} & \dfrac{1}{3} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Берем теперь

$$F' = -7x_2^2 + 5x_3^2 - 14x_2x^3;$$

обозначим

$$F_2 = \frac{1}{2}\frac{\partial F}{\partial x_2} = -7x_2 - 7x_3;$$

вычисляем

$$-7F' - F_2^2 = -84x_3^2;$$

следовательно:

$$F = \frac{1}{3}F_1^2 - \frac{1}{21}F_2^2 + 4x_3^2;$$

этим мы произвели подстановку:

$$F_1 = F_1, \qquad x_2 = -\frac{1}{7}F_2 - x_3, \qquad x_3 = x_3,$$

или

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & -\dfrac{1}{7} & -1 \\ 0 & 0 & 1 \end{pmatrix};$$

теперь вводим

$$F_1 = \sqrt{3}\cdot u_1, \qquad F_2 = \sqrt{21}\cdot u_2, \qquad x_3 = \frac{1}{2}u_3;$$

тогда

$$F = u_1^2 - u_2^2 + u_3^2;$$

этим мы произвели подстановку:

$$\begin{vmatrix} \sqrt{3} & 0 & 0 \\ 0 & \sqrt{21} & 0 \\ 0 & 0 & \frac{1}{2} \end{vmatrix}.$$

Теперь найдем подстановку, которая прямо переводит F в нормальный вид $u_1^2 - u_2^2 + u_3^2$; это

$$\begin{vmatrix} \frac{1}{3} & -\frac{2}{3} & \frac{1}{3} \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{vmatrix} \begin{vmatrix} 1 & 0 & 0 \\ 0 & -\frac{1}{7} & -1 \\ 0 & 0 & 1 \end{vmatrix} \begin{vmatrix} \sqrt{3} & 0 & 0 \\ 0 & \sqrt{21} & 0 \\ 0 & 0 & \frac{1}{2} \end{vmatrix} =$$

$$= \begin{vmatrix} \frac{1}{\sqrt{3}} & \frac{2}{\sqrt{21}} & \frac{1}{2} \\ 0 & -\sqrt{\frac{3}{7}} & -\frac{1}{2} \\ 0 & 0 & \frac{1}{2} \end{vmatrix},$$

или

$$x_1 = \frac{u_1}{\sqrt{3}} + \frac{2u_2}{\sqrt{21}} + \frac{u_3}{2}, \qquad x_2 = -\sqrt{\frac{3}{7}}u_2 - \frac{u_3}{2}, \qquad x_3 = \frac{u_3}{2}.$$

Рекомендуем произвести фактически эту подстановку в форме F, проверив тем самым наши вычисления.

В данном, случае $p = 2$, $q = 1$, $r = 3$, $s = 1$.

Обратим внимание на вещественные квадратичные формы, у которых отрицательный индекс инерции равен нулю; такие формы преобразовываются в сумму квадратов: следовательно, они ни при каких вещественных значениях переменных не могут быть отрицательными. Если кроме этого ранг формы равен числу ее переменных n, то такая форма преобразовывается в сумму n квадратов; она при всяких вещественных значениях своих аргументов положительна и равна нулю, если только все ее аргументы равны нулю. Такая форма называется *определенной положительной*.

Упражнения

220) Привести к нормальному виду форму:

$$F = 4x_1^2 + 2x_2^2 - 6x_3^2 + 6x_1x_2 + 10x_1x_3 + 4x_2x_3$$

и найти соответствующую подстановку.

Отв. $u_1^2 - u_2^2$, $\begin{vmatrix} \frac{1}{2} & \frac{3}{2} & 4 \\ 0 & -2 & -7 \\ 0 & 0 & 1 \end{vmatrix}$.

221) То же самое для формы:

$$F = ax_1x_2 - 2x_1x_3 + 2x_2x_3.$$

Отв. $u_1^2 - u_2^2 + u_3^2$, $\begin{vmatrix} \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ 0 & 0 & \frac{1}{\sqrt{2}} \end{vmatrix}$.

§ 176. Эрмитовы формы. Так называются формы вида:

$$F = \sum_{\alpha,\beta=1}^{n} a_{\alpha\beta} x_\alpha \overline{x}_\beta,$$

коэфициенты которых удовлетворяют условию

$$a_{\alpha\beta} = \overline{a}_{\beta\alpha}.$$

Матрица такой формы — эрмитова (§ 172). По существу эрмитова форма есть билинейная форма с эрмитовой матрицей, причем оба ряда переменных всегда имеют значения, сопряженные (как комплексные числа) друг другу (число переменных первого ряда и второго ряда — одинаково). Если давать переменным вещественные значения, то форма Эрмита обращается в квадратичную; если, кроме того, все коэфициенты формы вещественны, то матрица ее — симметрическая, и такая форма ничем не отличается от вещественных квадратичных форм.

Все, что говорилось о квадратичных формах, можно почти дословно применить к эрмитовым формам. Сделаем, например, в данной эрмитовой форме линейную подстановку

$$P = (p_{\alpha\beta} \quad \text{или} \quad x_\alpha = \sum_{\alpha=1}^{n} p_{\alpha\varkappa} u_\varkappa \qquad (\alpha = 1, 2, \ldots, n).$$

Тогда $\overline{x}_\beta = \sum_{\lambda=1}^{n} a_{\alpha\beta} p_{\alpha\varkappa} \overline{p}_\lambda = b_{\varkappa\lambda}$ и подставляя это в данную форму, найдем:

$$\sum_{\alpha,\beta=1}^{n} a_{\alpha\beta} \left(\sum_{\varkappa=1}^{n} p_{\alpha\varkappa} u_\varkappa \right) \left(\sum_{\lambda=1}^{n} \overline{p}_{\beta\lambda} \overline{u}_\lambda \right) = \sum_{\varkappa,\lambda=1}^{n} u_\varkappa \overline{u}_\lambda \sum_{\alpha,\beta=1}^{n} a_{\alpha\beta} p_{\alpha\varkappa} \overline{p}_{\beta\lambda}.$$

Обозначим: $\sum_{\alpha,\beta=1}^{n} a_{\alpha\beta} p_{\alpha\varkappa} \overline{p}_{\beta\lambda} = b_{\varkappa\lambda}$; это — коэфициент при $u_\varkappa \overline{u}_\lambda$; тогда коэфициент при $u_\lambda \overline{u}_\varkappa$ будет:

$$\sum_{\alpha,\beta=1}^{n} a_{\alpha\beta} p_{\alpha\lambda} \overline{p}_{\beta\varkappa} = \sum_{\alpha,\beta=1}^{n} \overline{a}_{\beta\alpha} \overline{p}_{\beta\varkappa} p_{\alpha\lambda} = \overline{b}_{\varkappa\lambda},$$

ибо $a_{\alpha\beta} = \overline{a}_{\beta\alpha}$. Таким образом матрица $B = (b_{\alpha\beta})$ тоже эрмитова, т. е. и новая форма, в которую перейдет F:

$$G = \sum_{\varkappa,\lambda=1}^{n} b_{\varkappa\lambda} u_{\varkappa} \overline{u}_{\lambda}$$

эрмитова. Если обозначим $A = (a_{\alpha\beta})$, то между матрицами A к B существует, как показывает формула для $b_{\varkappa\lambda}$, соотношение:

$$B = P' A \overline{P}.$$

Эквивалентность эрмитовых форм определяется совершенно так же, как и квадратичных. Далее, совершенно так же, как и для квадратичных форм, доказывается, что эрмитова форма приводится к нормальному виду; только здесь мы определяем:

$$X_\beta = \frac{\partial F}{\partial \overline{x}_\beta} = \sum_{\alpha=1}^{n} a_{\alpha\beta} x_\alpha;$$

тогда

$$\overline{X} = \frac{\partial F}{\partial x_\alpha} = \sum_{\beta=1}^{n} a_{\alpha\beta} \overline{x}_\beta = \sum_{\beta=1}^{n} \overline{a}_{\beta\alpha} \overline{x}_\beta.$$

Если не все диагональные элементы равны нулю, то, не нарушая общности, можно положить: $a_{11} \neq 0$. В таком случае берем: $a_{11} F = X_1 \overline{X}_1 + a_{11} F'$, где F' эрмитова форма, зависящая только от $x_2, \ldots, x_n$, $\overline{x}_2, \ldots, \overline{x}_n$. Если же все диагональные элементы равны нулю, то, не нарушая общности, можно положить:

$$\begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = \begin{vmatrix} 0 & a_{12} \\ a_{21} & 0 \end{vmatrix} = -a_{12}\overline{a}_{12} = -|a_{12}|^2 \neq 0.$$

В таком случае берем:

$$R_2 = \begin{vmatrix} 0 & a_{12} & \overline{X}_1 \\ a_{21} & 0 & \overline{X}_2 \\ X_1 & X_2 & F \end{vmatrix} = -|a_{12}|^2 F + a_{12} X_1 \overline{X}_2 + \overline{a}_{12} \overline{X}_1 X_2;$$

отсюда

$$F = \frac{1}{\overline{a}_{12}} X_1 \overline{X}_1 + \frac{1}{a_{12}} \overline{X}_1 X_2 - \frac{1}{|a_{12}|^2} R_2,$$

причем R_2 эрмитова форма, зависящая только от $x_3, \ldots, x_n$, $\overline{x}_3, \ldots, \overline{x}_n$.

Положим теперь:

$$\sqrt{2} X_1 = u_1 + u_2, \qquad \frac{\sqrt{2}}{a_{12}} X_2 = u_1 - u_2;$$

тогда:

$$F = u_1 \overline{u}_1 - u_2 \overline{u}_2 - \frac{1}{|a_{12}|^2} R_2.$$

Отсюда легко следует, что линейной подстановкой с детерминантом, отличным от нуля, мы эрмитову форму F переведем в «нормальную»:

$$H = \varepsilon_1 u_1 \overline{u}_1 + \varepsilon_2 u_2 \overline{u}_2 + \ldots + \varepsilon_r u_r \overline{u}_r = \varepsilon_1 |u_1|^2 + \varepsilon_2 |u_2|^2 + \ldots + \varepsilon_r |u_r|^2,$$

где $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_r$ равны частью $+1$, частью -1, r есть ранг формы F (т. е. матрицы A).

Далее, совершенно так же, как и для вещественных квадратичных форм, доказывается для эрмитовых форм *закон инерции*.

Если $r = n$ и все $\varepsilon_\lambda = +1$, то эрмитова форма называется *определенной положительной*; она имеет положительные значения при всех значениях переменных, кроме того случая, когда все переменные равны нулю: тогда и только тогда и значение формы есть нуль.

Пример. Привести к нормальному виду форму:

$$F = x_1\overline{x}_1 + (1+i)x_1\overline{x}_2 - 3ix_1\overline{x}_3 + (1-i)x_2\overline{x}_1 + 3ix_3\overline{x}_1 + 2x_2\overline{x}_2.$$

Имеем:

$$\begin{aligned}
&X_1 = x_1 + (1-i)x_2 + 3ix_3,\\
&F' = F - X_1\overline{X}_1 = 9x_3\overline{x}_3 - 3(1+i)x_2\overline{x}_3 - 3(1-i)x_3\overline{x}_2,\\
&X_2 = 9x_3 - 3(1+i)x_2,\\
&F'' = F' - \frac{1}{9}X_2\overline{X}_2 = 2x_2\overline{x}_2.
\end{aligned}$$

Итак:

$$F = X_1\overline{X}_1 + \frac{1}{9}X_2\overline{X}_2 + 2x_2\overline{x}_2.$$

Положим теперь $X_1 = u_1$, $\dfrac{1}{3}X_2 = u_2$, $\sqrt{2}\,x_2 = u_3$; тогда F примет вид:

$$H = u_1\overline{u}_1 + u_2\overline{u}_2 + u_3\overline{u_3}.$$

Подстановка, примененная нами, имеет вид:

$$\begin{vmatrix} 1 & -i & 0 \\ 0 & 0 & \dfrac{1}{\sqrt{2}} \\ 0 & \dfrac{1}{3} & \dfrac{1+i}{3\sqrt{2}} \end{vmatrix}.$$

§ 177. Ортогональное преобразование квадратичной формы. Итак, квадратичная вещественная форма преобразовывается линейной подстановкой к такому виду:

$$r_1u_1^2 + r_2u_2^2 + \ldots + r_nu_n^2. \tag{67}$$

В § 175 мы видели, что $r_\lambda = \pm 1$, а если ранг формы меньше n, то некоторые из r_λ равняются нулю. Будем считать r_λ какими-то вещественными числами (не обязательно равными ± 1) и докажем, что *всякая вещественная квадратичная форма может быть приведена к виду (67) посредством вещественной линейной ортогональной подстановки*. На языке матриц это значит, что всякая вещественная симметрическая матрица подобна диагональной матрице (§ 166), причем преобразовывается в эту диагональную матрицу посредством вещественной ортогональной

матрицы. Это следует из того, что матрица формы (67) — диагональная, именно: $[r_1, r_2, \ldots, r_n]$, и что если P — ортогональная матрица, то $P' = P^{-1}$ [§ 173 (59а)].

Если $A = (a_{\alpha\beta})$ матрица данной квадратичной формы (т. е. $a_{\alpha\beta} = a_{\beta\alpha}$), а $P = (p_{\alpha\beta})$— искомая ортогональная матрица, преобразовывающая матрицу A в диагональную, то имеем:

$$P^{-1}AP = [r_1, r_2, \ldots, r_n],$$

или

$$AP = P \cdot [r_1, r_2, \ldots, r_n]. \tag{68}$$

Это дает уравнения:

$$\sum_{\beta=1}^{n} a_{\alpha\beta}p_\beta = p_{\alpha\gamma}r_\gamma \qquad (\alpha, \gamma = 1, 2, \ldots, n), \tag{68}$$

или, иначе:

$$\left.\begin{array}{l} (a_{11} - r_\gamma)p_{1\gamma} + a_{12}p_{2\gamma} + \ldots + a_{1n}p_{n\gamma} = 0, \\ a_{21}p_{1\gamma} + (a_{22} - r_\gamma)p_{2\gamma} + \ldots + a_{2n}p_{n\gamma} = 0, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{n1}p_{1\gamma} + a_{n2}p_{2\gamma} + \ldots + (a_{nn} - r_\gamma)p_{n\gamma} = 0. \end{array}\right\} \tag{68}$$

Но при данном γ это — те же уравнения, что и (47) в § 169; так как P — неособенная матрица (ибо $|P| = \pm 1$, как для всякой ортогональной матрицы), то $p_{1\gamma}, p_{2\gamma}, \ldots, p_{n\gamma}$ ни при каком γ не могут все равняться нулю; следовательно (§ 33), детерминант системы (68б) должен равняться нулю; а это нам дает характеристическое уравнение (§ 169) для r_γ, следовательно, r_γ — характеристическое число матрицы A. Докажем предварительно следующее:

Теорема. *Все характеристические числа вещественной симметрической матрицы вещественны.*

Доказательство. Найдя одно из характеристических числел r_γ, мы найдем из (68а) и $p_{1\gamma}, p_{2\gamma}, \ldots, p_{n\gamma}$ (мы еще не знаем, вещественны ли они). Умножаем теперь уравнения (68а) на $\overline{p}_{\alpha\gamma}$ и суммируем по α:

$$\sum_{\alpha,\beta=1}^{n} a_{\alpha\beta}\overline{p}_{\alpha\gamma}p_{\beta\gamma} = r_\gamma \sum_{\alpha=1}^{n} p_{\alpha\gamma}\overline{p}_{\alpha\gamma} = r_\gamma \sum_{\alpha=1}^{n} |p_{\alpha\gamma}|^2.$$

Правая сумма в полученном равенстве вещественна; докажем, что и левая часть вещественна; в самом деле, она равна своей сопряженной:

$$\sum_{\alpha,\beta=1}^{n} a_{\alpha\beta}p_{\alpha\gamma}\overline{p}_{\beta\gamma},$$

ибо $a_{\alpha\beta} = a_{\beta\alpha}$. Но отсюда следует, что и r_γ вещественно, что и требовалось доказать.

Замечание. Совершенно тем же способом можно доказать, что и у эрмитовой матрицы все характеристические числа вещественны.

Пусть теперь r_γ и r_δ — два различных корня характеристического уравнения для A, и мы нашли соответственно им два ряда чисел:

$$p_{1\gamma},\ p_{2\gamma},\ \ldots,\ p_{n\gamma}, \quad \text{и} \quad p_{1\delta},\ p_{2\delta},\ \ldots,\ p_{n\delta}.$$

Мы теперь знаем, что все эти числа вещественны, ибо r_γ и r_δ вещественны; докажем, что эти два ряда ортогональны друг к другу. Для этого уравнение (68а) умножаем на $p_{\alpha\delta}$ и суммируем по α; точно так же уравнение, аналогичное (68а), только со значком не γ, а δ, умножаем на $p_{\alpha\gamma}$ и суммируем по α; получаем:

$$\sum_{\alpha,\beta=1}^{n} a_{\alpha\beta}p_{\beta\gamma}p_{\alpha\delta} = r_\gamma \sum_{\alpha=1}^{n} p_{\alpha\gamma}p_{\alpha\delta},$$
$$\sum_{\alpha,\beta=1}^{n} a_{\alpha\beta}p_{\beta\delta}p_{\alpha\gamma} = r_\delta \sum_{\alpha=1}^{n} p_{\alpha\delta}p_{\alpha\gamma}.$$

Левые части этих равенств одинаковы, ибо $a_{\alpha\beta} = a_{\beta\alpha}$; значит и правые тоже одинаковы, откуда

$$(r_\gamma - r_\delta)\sum_{\alpha=1}^{n} p_{\alpha\gamma}p_{\alpha\delta} = 0;$$

так как $r_\gamma \neq r_\delta$, то, следовательно:

$$\sum_{\alpha=1}^{n} p_{\alpha\gamma}p_{\alpha\delta} = 0,$$

а это и есть условие ортогональности вышеприведенных рядов.

Если $\sum_{\alpha=1}^{n} p_{\alpha\gamma}^2 = k \neq 1$ (и, конечно, $k > 0$), то делим все $p_{\alpha\gamma}$ (при $\alpha = 1, 2, \ldots, n$) на $\sqrt{k}$; это не нарушает ни уравнения (69б), ни условия ортогональности с $p_{\alpha\delta}$, но теперь новые $p_{\alpha\gamma}$ дают $\sum_{\alpha=1}^{n} p_{\alpha\gamma}^2 = 1$. Говорят, что мы *нормировали* ряд $p_{\alpha\gamma}$ ($\alpha = 1, 2, \ldots, n$). Так мы можем нормировать и каждый наш ряд $p_{1\delta}, p_{2\delta}, \ldots, p_{n\delta}$.

Если все n характеристических чисел $r_1, r_2, \ldots, r_n$ матрицы A различны, то мы имеем и n различных, ортогональных друг к другу и нормированных рядов $p_\gamma, p_{2\gamma}, \ldots, p_{n\gamma}$ ($\gamma = 1, 2, \ldots, n$); считая эти ряды столбцами, строим матрицу $P = (p_{\alpha\beta})$, которая будет ортогональна и удовлетворит равенству (68).

В случае кратных характеристических чисел преобразование усложняется; покажем, как его вести в этом случае. Пусть r_1 — какое-нибудь характеристическое число матрицы A; найдем из (68б) (при $\gamma = 1$) $p_{11}, p_{21}, \ldots, p_{n1}$ (и нормируем их). Построим теперь какую-нибудь ортогональную матрицу с первым столбцом $p_{11}, p_{21}, \ldots, p_{n1}$ [89], обозначим ее через Q; тогда

$$B = Q^{-1}AQ$$

тоже будет симметрической матрицей. Иначе:

$$AQ = QB.$$

[89] Я не останавливаюсь на довольно простом доказательстве возможности этого построения.

Но по (68a) первый столбец левого (а значит и правого) произведения есть: $p_{11}r_1$, $p_{21}r_1, \ldots, p_{n1}r_1$, а в правой части, в Q первый столбец есть $p_{11}, p_{21}, \ldots, p_{n1}$. Таким образом, комбинируя строки в Q с первым столбцом в B, мы получаем каждый раз $p_{11}r_1 + 0 + 0 + \ldots$, $p_{21}r_1 + 0 + 0 + \ldots$, $\ldots$; следовательно, в B первый столбец таков: $r_1, 0, 0, \ldots, 0$; а так как B — симметрическая матрица, то и первая строка в B такая же: $r_1,), 0, \ldots, 0$. Таким образом B имеет вид:

$$B = \begin{pmatrix} r & 0 & 0 & \ldots & 0 \\ 0 & b_{22} & b_{23} & \ldots & b_{2n} \\ 0 & b_{32} & b_{33} & \ldots & b_{3n} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & b_{n2} & b_{n3} & \ldots & b_{nn} \end{pmatrix}.$$

Матрица $(n-1)$-го порядка:

$$B_1 = \begin{pmatrix} b_{22} & b_{23} & \ldots & b_{2n} \\ b_{32} & b_{33} & \ldots & b_{3n} \\ \ldots & \ldots & \ldots & \ldots \\ b_{n2} & b_{n3} & \ldots & b_{nn} \end{pmatrix}$$

также симметрическая. Проделывая с ней то же самое, мы постепенно превратим ее в диагональную матрицу. Но это сводится к тому, что мы к A применяем последовательно несколько ортогональных подстановок; а так как произведение ортогональных подстановок — тоже ортогональная подстановка, то этим наше предложение доказано.

Эти ортогональные преобразования квадратичных форм для случаев $n = 2$ и $n = 3$ приходится делать в аналитической геометрии, когда мы, перенося начало координат в центр кривой или поверхности 2-го порядка, желаем повернуть прямоугольные оси координат так, чтобы в уравнении этой кривой или поверхности уничтожались члены, содержащие произведения координат. Вращение осей прямоугольных координат выражается аналитически ортогональной линейной подстановкой, при помощи которой мы и сводим наше уравнение к виду $Ax^2 + By^2 = F$ в случае кривой 2-го порядка, или к виду $Ax^2 + By^2 + Cz^2 = F$ в случае поверхности 2-го порядка.

§ 178. Одновременное приведение двух квадратичных форм. Мы предполагаем, что одна из двух наших форм F и G положительная определенная; пусть это, например, F. В таком случае мы можем преобразовать F в сумму n квадратов (см. конец § 175):

$$F_1 = x_1^2 + x_2^2 + \ldots + x_n^2;$$

форма G от этого преобразования перейдет в некоторую квадратичную форму G_1. Теперь преобразовываем форму G_1 посредством *ортогональной* подстановки к виду:

$$r_1x_1^2 + r_2x_2^2 + \ldots + r_nx_n^2;$$

форма F_1 при этом не изменит своего вида, ибо сумма квадратов переменных есть инвариант относительно ортогональных подстановок. Соединяя теперь в одно два

произведенных преобразования, мы видим, что при помощи одного этого комбинированного преобразования обе формы F и G приводятся к нормальному виду. Это преобразование имеет большое значение в математической физике.

§ 179. Матрицы с целыми элементами. Рассматривая матрицы и соответствующие им билинейные формы с целыми коэфициентами, мы будем применять к ним и линейные преобразования исключительно с целыми коэфициентами. Для простоты мы будем рассматривать только квадратные матрицы, т. е. билинейные формы, в которых оба ряда состоят из одинакового числа переменных. Вместо самих форм мы будем брать их матрицы и будем говорить, что матрица A *содержит* матрицу B, если существуют две матрицы P и Q с целыми коэфициентами (так же, как и A и B), — такие, что

$$B = PAQ. \tag{69}$$

Если не только A содержит B, но и B содержит A, то A и B называются *эквивалентными*. Но это понятие эквивалентности уже, чем в § 164: если P и Q неособенные матрицы, т. е. существуют P^{-1} и Q^{-1}, то из этого еще не следует, что A и B эквивалентны: надо еще чтобы у P^{-1} и Q^{-1} все элементы были целыми (как и у P и Q). Точно так же, одинаковость рангов матриц A и B является условием необходимым, но не достаточным для эквивалентности этих матриц. Целью настоящего параграфа и является вывод необходимых и достаточных условий эквивалентности «целочисленных» (как мы будем их называть) матриц.

Теорема. *Если P — целочисленная матрица, то P^{-1} — тогда и только тогда будет тоже целочисленной матрицей, если $|P| = \pm 1$.*

Целочисленные матрицы с детерминантами ± 1 называются *унимодулярными*; они, очевидно, составляют группу (§ 27).

Доказательство. Если и P и P^{-1} — целочисленны, то P и $|P^{-1}| = \frac{1}{|P|}$ целые числа, что возможно только при $|P| = \pm 1$. Обратно, если $|P| = \pm 1$, то P^{-1} целочисленна, что следует из формулы (17) § 157.

Обозначим через d_1 общий наибольший делитель всех элементов матрицы A; в таком случае [(31) § 163]

$$A = d_1 A_1,$$

где A_1 — целочисленная матрица, все элементы которой взаимно простые; такая матрица называется *первообразной*. Заметим, что всякая *унимодулярная матрица первообразна*.

Составим всевозможные детерминанты k-го порядка нашей целочисленной матрицы A; все они имеют целые значения; обозначим через d_k их общий наибольший делитель; d_k называется *детерминантным делителем* k-го порядка; при $k = 1$ он совпадает с определенным выше числом d_1. Если r — ранг матрицы A, то условимся считать $d_k = 0$ при $k > r$. Для $r = n$, $d_n = |A|$.

Так как всякий детерминант k-го порядка можно расположить по элементам какого-нибудь ряда (§ 32), и коэфициентами этого разложения являются детерминанты $(k-1)$-го порядка, то, следовательно, все детерминанты k-го порядка, а значит и их общий наибольший делитель d_k делятся на d_k. Итак, каждый из детерминантных делителей является делителем всех последующих детерминантных делителей.

Формула (69) показывает, что все элементы матрицы B делятся на d_1, а из доказательства последней теоремы § 156 заключаем, что детерминанты k-го порядка матрицы B, являясь суммами произведений детерминантов k-го порядка матриц P, A и Q, все делятся на d_k; отсюда следует:

Теорема. *Если матрица A содержит матрицу B* [90]*, то детерминантные делители матрицы B делятся на соответствующие детерминантные делители матрицы A.*

Следствие. Эквивалентные матрицы имеют одинаковые детерминантные делители.

В дальнейшем мы увидим, что одинаковость детерминантных делителей есть и достаточное условие для эквивалентности целочисленных матриц.

§ 180. Элементарные делители. Аналогично § 154 будем преобразовывать целочисленные матрицы к «нормальному» виду при помощи элементарных преобразований, причем последние будем понимать в более узком смысле, нежели в § 154, а именно, этими элементарными преобразованиями теперь будут:

1. Перестановка двух строк или двух столбцов.

2. Умножение всех элементов строки или столбца на -1.

3. Прибавление к элементам строки или столбца соответствующих элементов другой строки или столбца, умноженных на одно и то же целое число.

Легко видеть (из § 162), что эти преобразования достигаются умножением данной матрицы справа и слева на *унимодулярные* матрицы.

При помощи этих преобразований будем нашу целочисленную матрицу A трансформировать следующим образом: переставляя строки и столбцы, поставим на первое место наименьший по абсолютной величине элемент и с помощью преобразования 2 сделаем его положительным. Это теперь будет наше a_{11}. Если какой-нибудь элемент первой строки (или столбца) $a_{1\lambda}$ (или $a_{\lambda 1}$) не делится на a_{11} и $a_{1\lambda} = a_{11}t + a'_{1\lambda}$, (или $a_{\lambda 1} = a_{11}t + a'_{\lambda 1}$, где t — неполное частное, а $a'_{1\lambda} < a_{11}$ (или $a'_{\lambda 1} < a_{11}$) остаток, то к λ-му столбцу (или к λ-й строке) прибавляем первый, умноженный на $-t$, и вместо $a_{1\lambda}$ получаем $a'_{1\lambda}$ (или вместо $a_{\lambda 1}$ получаем $a'_{\lambda 1}$). Теперь переставляем λ-й столбец (или строку) с первым, ибо $a'_{1\lambda}$ (или $a'_{\lambda 1}$) меньше, чем a_{11} и больше нуля. Затем опять смотрим, есть ли в первой строке (или столбце) элемент, не делящийся на новое a_{11} и, если есть, снова проделываем ту же операцию. Число этих операций будет конечно, ибо с каждой из них a_{11} уменьшается, оставаясь целым и $\geq d_1$ (общий наибольший делитель всех $a_{\alpha\beta}$); т. е. рано или поздно мы достигнем того, что все элементы первой строки и первого столбца будут делиться на a_{11}; тогда, отнимая от строк и столбцов первые строку и столбец, умноженные на частные от делений $a_{1\lambda}$ и $a_{\lambda 1}$ на a_{11}, мы обратим в нуль все элементы первой строки и первого столбца кроме a_{11} и наша матрица примет вид

$$\begin{pmatrix} a_{11} & 0 & \dots & 0 \\ 0 & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ 0 & a_{n2} & \dots & a_{nn} \end{pmatrix}. \tag{70}$$

[90] Во всех этих исследованиях мы имеем в виду исключительно целочисленные матрицы, и понятия «содержания» и «эквивалентности» в том смысле, как мы определили в начале этого параграфа.

Теперь мы можем аналогичным путем достигнуть того, чтобы все $a_{\alpha\beta}$ делились на a_{11}, ибо если $a_{\alpha\beta}$ не делится на a_{11}, то мы прибавим к первой строке α-ю, так чтобы первая строка стала составлена из элементов $a_{11}, a_{\alpha 2}, \ldots, a_{\alpha n}$, и вновь произведем указанную выше операцию. В конце концов мы достигнем того, что в (70) все $a_{\alpha\beta}$ будут делиться на a_{11}; тогда, очевидно, будет: $a_{11} = d_1$, ибо от всех этих операций общий наибольший делитель d_1 всех элементов матрицы A не изменится (см. следствие в конце § 179).

Теперь то же самое проделываем с матрицей

$$\begin{pmatrix} a_{22} & \ldots & a_{2n} \\ \ldots\ldots\ldots\ldots \\ a_{n2} & \ldots & a_{nn} \end{pmatrix}$$

и т. д. Таким образом мы в конце концов преобразуем нашу матрицу в матрицу такого вида:

$$\begin{pmatrix} e_1 & 0 & \ldots & 0 \\ 0 & e_2 & \ldots & 0 \\ \ldots\ldots\ldots\ldots \\ 0 & 0 & \ldots & e_n \end{pmatrix} = [e_1, e_2, \ldots, e_n]. \tag{71}$$

Если ранг r данной матрицы меньше n, то $e_{r+1} = \ldots = e_n = 0$. Каждое e_k делится на e_{k-1}. Данная матрица A преобразовалась в «нормальную» матрицу (71) элементарными преобразованиями, т. е. умножением справа и слева на унитарные матрицы; т. е. A эквивалентна матрице (71).

Числа $e_1, e_2, \ldots, e_n$ называются *элементарными делителями* матрицы A; каждый из них есть делитель всех последующих. Мы уже видели, что $e_1 = d_1$. Легко видеть, что:

$$d_k = e_1 e_2 \cdots e_k. \tag{72}$$

Действительно, взяв детерминант k-го порядка из первых k строк и k столбцов матрицы (71), мы увидим, что он равен $e_1 e_2 \cdots e_k$; всякий же иной детерминант k-го порядка этой матрицы или равен нулю, или равен $e_{\alpha_1} e_{\alpha_2} \cdots e_{\alpha_k}$, где $\alpha_1 \geq 1$, $\alpha_2 \geq 2$, $\ldots$, $\alpha_k \geq k$, т. е. e_{α_1} делится на e_1, e_{α_2} делится на e_2 и т. д., e_{α_k} делится на e_k, и значит $e_{\alpha_1} e_{\alpha_2} \cdots e_{\alpha_k}$ делится на $e_1 e_2 \cdots e_k$. Итак:

$$e_k = \frac{d_k}{d_{k-1}}, \qquad e_1 = d_1. \tag{72}$$

Это — новое определение элементарных делителей.

Две (целочисленные) матрицы, имеющие одинаковые элементарные делители, очевидно, эквивалентны, ибо каждая из них преобразовывается в одну и ту же нормальную матрицу (71). Обратно, две эквивалентные матрицы имеют одинаковые детерминантные делители (см. следствие в конце § 179), а следовательно, по (72а), и одинаковые элементарные делители. Итак:

Необходимое и достаточное условие эквивалентности двух целочисленных матриц состоит в одинаковости их детерминантных или элементарных делителей.

Мы видим также, что эквивалентные целочисленные матрицы всегда преобразовываются одна в другую посредством унимодулярных матриц, ибо каждая из них преобразовывается посредством таких матриц в нормальную форму (71).

Если матрица A только содержит матрицу B, то, как мы видели в § 179, детерминантные делители матрицы B делятся на соответствующие детерминантные делители матрицы A, но обратное тут неверно. Однако существует теорема о том, что необходимым и достаточным условием того, чтобы матрица A содержала матрицу B, является делимость элементарных делителей матрицы B на соответственные элементарные делители матрицы A.

§ 181. λ-матрицы. Рассмотрим еще матрицы, элементами которых служат целые рациональные функции от одного переменного λ с любыми числовыми коэфициеитами; будем для краткости называть такие матрицы *λ-матрицами.* Их теория совершенно аналогична теории целочисленных матриц. Только роль чисел ± 1 теперь играют все постоянные (т. е. независимые от λ) количества. *Унимодулярной* теперь назовем λ-матрицу, детерминант которой равен $\text{const} \neq 0$. И здесь имеем теорему. *Если P — λ-матрица, то P^{-1} тогда и только тогда тоже λ-матрица, если P унимодулярна* (откуда следует, что и P^{-1} тоже унимодулярна). *Первообразной* назовем теперь λ-матрицу, у которой общий наибольший делитель всех элементов есть const, (или функция нулевой степени).

Аналогично тому, как в § 179, определяем случай, когда λ-матрица A *содержит* λ-матрицу B, и когда λ-матрицы эквивалентны. Далее, аналогично определяем *детерминантные делители* λ-матрицы: $d_1(\lambda), d_2(\lambda), \ldots, d_n(\lambda)$ и здесь $d_k(\lambda)$ делится на $d_{k-1}(\lambda)$ и верна теорема: *если матрица A содержит матрицу B, то детерминантные делители B делятся на соответствующие детерминантные делители матрицы A; и, наконец, следствие: эквивалентные λ-матрицы имеют одинаковые детерминантные делители.*

Элементарные преобразования λ-матриц следующие: 1 — как в § 154; 2 — умножение строки или столбца на отличный от нуля постоянный множитель; 3 — прибавление к элементам одного ряда соответствующих элементов другого, умноженных на одну и ту же целую рациональную функцию от λ. Этими преобразованиями можно данную λ-матрицу привести к виду:

$$\begin{pmatrix} e_1(\lambda) & 0 & \ldots & 0 \\ 0 & e_2(\lambda) & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & e_n(\lambda) \end{pmatrix} = [e_1(\lambda), e_2(\lambda), \ldots, e_n(\lambda)]. \tag{73}$$

И здесь $e_k(\lambda)$ делится на $e_{k-1}(\lambda)$, $e_k(\lambda) = \dfrac{d_k(\lambda)}{d_{k-1}(\lambda)}$, $e_1(\lambda) = d_1(\lambda)$; если r — ранг матрицы, то при $k > r$ $e_k(\lambda) = d_k(\lambda) = 0$.

Необходимое и достаточное условие эквивалентности λ-матриц состоит в одинаковости у них функций $d_k(\lambda)$ или $e_k(\lambda)$.

Но элементарными делителями λ-матрицы (по Вейерштрассу) называются не сами функции $e_k(\lambda)$, а их линейные множители с соответствующими показателями. Так, если:

$$e_k(\lambda) = (\lambda - \alpha)^{\varepsilon_k}(\lambda - \alpha')^{\varepsilon'_k}(\lambda - \alpha'')^{\varepsilon''_k} \cdots,$$

то элементарными делителями матрицы A будут:

$$(\lambda-\alpha)^{\varepsilon_1},\ (\lambda-\alpha')^{\varepsilon'_1},\ (\lambda-\alpha'')^{\varepsilon''_1},\ \ldots,$$
$$(\lambda-\alpha)^{\varepsilon_2},\ (\lambda-\alpha')^{\varepsilon'_2},\ (\lambda-\alpha'')^{\varepsilon''_2},\ \ldots,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

очевидно, что $0 \le \varepsilon_1 \le \varepsilon_2 \le \ldots$, $0 \le \varepsilon'_1 \le \varepsilon'_2 \le \ldots$, $0 \le \varepsilon''_1 \le \varepsilon''_2 \le \ldots$, функции же $e_k(\lambda)$ называются *инвариантными множителями* матрицы A. Очевидно, что эти функции $e_k(\lambda)$ вполне определены элементарными делителями.

ГЛАВА ДЕСЯТАЯ

ИНВАРИАНТЫ И КОВАРИАНТЫ

§ 182. Основные понятия и примеры. Понятие *инвариантности* (неизменности) широко распространено во всей математике и в ее приложениях; чтобы выяснить это понятие, приведем предварительно несколько примеров.

В аналитической геометрии, как известно, свойства линий и фигур исследуются *алгебраическим путем* посредством системы координат, хотя бы прямоугольной; положение осей этой системы координат по отношению к данной линии или фигуре существенной роли не играет, но обусловливает большую или меньшую сложность вычислений. Поэтому часто необходимо преобразовывать координаты, меняя положения осей, чтобы достигнуть возможной простоты вычислений. При этих преобразованиях сама линия или фигура, конечно, не меняется, а следовательно, не меняются и числовые соотношения между ее частями; говорят, что эти соотношения инвариантны относительно совокупности данных преобразований. Как простейший пример приведем расстояние между двумя данными точками в плоскости:

$$d = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2}, \tag{1}$$

где (x_1, y_1), (x_2, y_2) — координаты наших точек. Введя новую прямоугольную же систему координат соотношениями:

$$\left.\begin{aligned} x &= x' \cos\varphi - y' \sin\varphi + a, \\ y &= x' \sin\varphi + y' \cos\varphi + b, \end{aligned}\right\} \tag{2}$$

где (x, y) — старые, (x', y') — новые координаты точки, (a, b) — старые координаты нового начала, и подставив в (1) вместо x_1, x_2, y_1, y_2 их выражения согласно формулам (2), мы получим для расстояния d точно такое же выражение, что и (1), в новых координатах:

$$d = \sqrt{(x'_1 - x'_2)^2 + (y'_1 - y'_2)^2}.$$

Говорят, что выражение (1) есть *инвариант* (правильнее даже *ковариант*) относительно преобразований (2).

В качестве второго примера возьмем две прямые линии в плоскости, выражаемые, как известно, уравнениями:

$$\left.\begin{aligned} A_1 x + B_1 y + C_1 &= 0, \\ A_2 x + B_2 y + C_2 &= 0. \end{aligned}\right\} \tag{3}$$

Угол α между ними дается формулой:

$$\operatorname{th}\alpha = \frac{A_1B_2 - A_2B_1}{A_1A_2 + B_1B_2}. \tag{4}$$

При преобразовании координат (2) уравнения (3) наших прямых примут вид:

$$\left.\begin{aligned} A_1'x' + B_1'y' + C_1' = 0, \\ A_2'x' + B_2'y' + C_2' = 0, \end{aligned}\right\} \tag{3}$$

где $A_1', \ldots, C_2'$ — уже новые коэфициенты, зависящие линейно от старых, а также зависящие от a, b, φ. Но прямые ведь остались те же, а следовательно, и угол между ними не изменился, т. е., составив из новых коэфициентов выражение:

$$\frac{A_1'B_2' - A_2'B_1'}{A_1'A_2' + B_1'B_2'},$$

мы заключаем, что оно будет равно тому же самому $\operatorname{tg}\alpha$. Следовательно, это выражение (4) является *инвариантом* относительно преобразований (2). Вычислениями можно проверить, что числитель и знаменатель в (4) в отдельности являются инвариантами, т. е. что

$$\begin{aligned} A_1'B_2' - A_2'B_1' &= A_1B_2 - A_2B_1, \\ A_1'A_2' + B_1'B_2' &= A_1A_2 + B_1B_2. \end{aligned}$$

Заметим, что равенства $A_1B_2 - A_2B_1 = 0$, $A_!A_2 + B_1B_2 = 0$ являются выражениями параллельности и перпендикулярности наших прямых.

Преобразование (2) мы толковали как перемену положения прямоугольных осей координат на плоскости; но его можно толковать и как преобразование самой плоскости, при котором точка (x, y) переходит в точку (x', y'); при этом не изменяются ни расстояние между двумя точками, ни угол между двумя прямыми. Такое преобразование называется *движением* плоскости в самой себе. Совокупность всевозможных преобразований типа (2) (при различных действительных φ, a, b) образует группу движений плоскости (§ 27). Всякое такое движение есть одно-однозначное преобразование, т. е. при нем каждой точке (x, y) соответствует всегда одна и только одна точка (x', y'), и обратно. Для каждого преобразования (2) существует *обратное*, переводящее (x', y'), в (x, y). Наконец как частный случай (2) (при $\varphi = 0$, $a = 0$, $b = 0$) получаем *тождественное преобразование* $x = x'$; $y = y'$.

Заметим, что при $a = b = 0$ и при любом φ формулы (2) дают *группу вращений* плоскости вокруг точки 0; это — линейные однородные подстановки двух переменных, или матрицы 2-го порядка, и именно ортогональные матрицы (§ 173).

В геометрии рассматриваются и более общие преобразования, например, *аффинные*, в которых старые координаты заменяются линейными (неоднородными) функциями от новых координат. Для плоскости аффинные преобразования выражаются формулами:

$$\left.\begin{aligned} x = a_1x' + b_1y' + c_1, \\ y = a_2x' + b_2y' + c_2 \end{aligned}\right\} \tag{5}$$

при условии $a_1b_2 - a_2b_1 \neq 0$.

При этом преобразовании изменяется и расстояние между двумя точками, и угол между двумя прямыми, но параллельность прямых сохраняется. Если мы наши прямые (3) подвергнем преобразованию (5), то они перейдут в прямые же, уравнения которых будут вида (3а); но составив из новых коэфициентов выражение $A'_1B'_2 - A'_2B'_1$, мы увидим, что оно вообще не равно выражению $A_1B_2 - A_2B_1$, а именно, имеет место следующее соотношение:

$$A'_1B'_2 - A'_2B'_1 = (a_1b_2 - a_2b_1)(A_1B_2 - A_2B_1). \tag{6}$$

Неравный нулю множитель $a_1b_2 - a_2b_1$ есть детерминант преобразования (5). Формула (6) показывает, что $A_1B_2 - A_2B_1$ и $A'_1B'_2 - A'_2B'_1$ всегда равны нулю или не равны нулю *одновременно*, т. е. если прямые (3) параллельны, то и прямые (3а) параллельны, и если (3) не параллельны, то и (3а) — тоже. Таким образом здесь выражение $A_1B_2 - A_2B_1$ указывает на инвариантное свойство нашей фигуры (параллельность прямых), но инвариантом в предыдущем смысле не является: при преобразовании (5) оно изменяется — получает множителя $a_1b_2 - a_2b_1$. Целесообразно и тут считать выражение $A_1B_2 - A_2B_1$ инвариантом, и именно *относительным инвариантом*, — в отличие от *абсолютного*, который совершенно не меняется при данных преобразованиях.

Более общими, чем аффинные преобразования, являются *проективные преобразования* или *коллинеации*; для плоскости они выражаются формулами:

$$\left.\begin{aligned} x &= \frac{a_1x' + b_1y' + c_1}{a_3x' + b_3y' + c_3}, \\ y &= \frac{a_2x' + b_2y' + c_2}{a_3x' + b_3y' + c_3}. \end{aligned}\right\} \tag{7}$$

Чтобы такое преобразование было одноднозначным, должно выполняться условие:

$$\begin{vmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{vmatrix} \neq 0. \tag{7}$$

При этих преобразованиях прямые остаются прямыми, но параллельность их вообще нарушается. Вообще *порядок* кривой (или поверхности) при этом не меняется, хотя форма кривой может измениться (например, эллипс может перейти в гиперболу). Таким образом порядок данной кривой является абсолютным инвариантом относительно проективных преобразований; такие инварианты, которые, по своему существу являются целыми числами, носят название *арифметических инвариантов*. В качестве других примеров арифметических инвариантов приведем ранг билинейной формы относительно собственных линейных подстановок (§ 164), ранг и сигнатуру, или положительный и отрицательный индексы инерции вещественных квадратичных форм — относительно собственных линейных вещественных преобразований (§ 175), наконец, детерминантные и элементарные делители целочисленных матриц — относительно унимодулярных преобразований (§ 180).

Название «проективные преобразования» объясняется тем, что при них данная и преобразованная фигуры находятся в проективном соотношении, а это для

прямых и пучков лучей выражается в том, что *ангармоническое* или *двойное* отношение четырех точек прямой или четырех лучей пучка при этом преобразовании не изменяется, т. е. является абсолютным инвариантом относительно этих преобразований [91].

При рассмотрении коллинеаций удобно пользоваться однородными координатами, полагая (в плоскости) $x = \frac{x_1}{x_3}$, $y = \frac{x_2}{x_3}$; тогда преобразование (7) примет вид:

$$\left.\begin{aligned} x_1 &= a_1x_1 + b_1x_2' + c_1x_3', \\ x_2 &= a_2x_1 + b_2x_2' + c_2x_3', \\ x_3 &= a_3x_1 + b_3x_2' + c_3x_3'. \end{aligned}\right\} \tag{8}$$

Но это — при условии (7a) — есть собственная линейная подстановка. Заметим, что левые части уравнений поверхностей и линий в однородных координатах являются однородными, функциями от координат.

§ 183. Определения. Некоторые частные случаи. Переходя к систематическому изложению алгебраической теории инвариантов и ковариантов, мы будем рассматривать исключительно собственные линейные преобразования n переменных, т. е. те, которые мы ввели в § 155; эти преобразования являются обобщением проективных преобразований в геометрии, которые как частные случаи включают в себя и аффинные преобразования и движения. Мы будем брать как заданные нам одну или несколько целых рациональных однородных функций от наших n переменных, преобразовывать их нашими линейными подстановками и находить их инварианты и коварианты.

Целая рациональная однородная функция от n переменных называется *формой*; в зависимости от числа переменных различают формы *бинарные* (двоичные), *тернарные* (троичные) и т. д.; в зависимости от степени различают формы *линейные*, *квадратичные*, *кубичные* и т. д.

Пусть $f(x_1, x_2, \ldots, x_n)$ форма m-й степени от n переменных; ее коэфициенты мы обозначим буквою a со значками. Пусть $P = (p_{\alpha\beta})$, $x_\alpha = \sum_{\beta=1}^{n} p_{\alpha\beta}x_\beta'$ — линейная подстановка, посредством которой переменные x_α заменяются через x_β', вследствие чего форма $f(x_1, x_2, \ldots, x_n)$ перейдет в $F(x_1', x_2', \ldots, x_n')$. Очевидно, что F тоже форма m-й степени от $x_1', x_2', \ldots, x_n'$; коэфициенты ее мы обозначим буквою A со значками. Очевидно, что F имеет тот же вид, что и f, только всюду вместо коэфициентов a стоят коэфициенты A, а вместо переменных x_α — переменные x_β.

Пусть $K(a, x)$ — функция от коэфициентов a и переменных x_α, обладающая следующим свойством:

$$K(A, x') = |P|^\lambda \cdot K(a, x), \tag{9}$$

где $|P|$ — детерминант подстановки P, а λ вполне определенное число, не зависящее от взятой подстановки P. Такая функция $K(a, x)$ называется *ковариантом* (*соизменяющейся*) данной формы f *веса* λ. Мы будем брать за $K(a, x)$ только целые рациональные функции от a и от x, т. е. будем рассматривать целые рациональные коварианты. Если при этом $K(a, x)$ — неоднородная функция от a и

[91] Ангармоническое отношение точек A, B, C, D на прямой есть выражение $\frac{AC}{BC} : \frac{AD}{BD}$.

от x_α, то (§ 132) она может быть представлена как сумма однородных функций; а так как посредством линейной подстановки однородная функция переходит и однородную же, то очевидно, что неоднородный ковариант представляется как сумма однородных ковариантов, так что мы можем ограничиться рассмотрением однородных ковариантов. В частном случае K может совсем не зависеть от x_α, а быть функцией только коэфициентов a: $I(a)$; в таком случае $I(a)$ есть *инвариант* (*неизменяющаяся*) формы f. Если $I(A) = |P|^\lambda \cdot I(a)$, то λ — *вес* инварианта.

Пусть теперь нам дано несколько форм от одних и тех же переменных $x_1, x_2, \ldots, x_n$; именно, $f_1, f_2, \ldots, f_k$, с коэфициентами a, b, c, ...

Пусть посредством линейной подстановки P эти формы переходят в формы $F_1, F_2, \ldots, F_k$ от $x'_1, x'_2, \ldots, x'_n$ с коэфициентами $A, B, C, \ldots$ Функция $K(a, b, c, \ldots, x)$ от $x_1, x_2, \ldots, x_n$ и от коэфициентов этих форм, обладающая свойством

$$K(A, B, C, \ldots, x') = |P|^\lambda \cdot K(a, b, c, \ldots, x), \tag{10}$$

называется *совокупным ковариантом* форм $f_1, f_2, \ldots, f_k$ *веса* λ. В частности, если K совсем не зависит от x_α, то она называется *совокупным инвариантом* тех же форм. И здесь мы можем ограничиться рассмотрением только однородных ковариантов и инвариантов. Если вес инварианта или ковариантa равен нулю, то такой инвариант или ковариант называется *абсолютным* (§ 182).

Иногда бывает целесообразно рассматривать коварианты, зависящие не от переменных $x_1, x_2, \ldots, x_n$, а от переменных $\xi_1, \xi_2, \ldots, \xi_n$, которые подвергаются той же линейной подстановке, что и x_α; такие переменные называются *когредиентными* с x_α, (§ 167). Может случиться, что ковариант зависит и от x_α, и от ξ_α, или даже от нескольких рядов когредиентных переменных.

Пример 1. Всякая форма есть абсолютный ковариант самой себя.

Пример 2. Система n линейных форм от n переменных $y_\alpha = \sum_{\beta=1}^{n} a_{\alpha\beta} x_\beta$ посредством подстановки P переходит в систему форм:

$$y_\varkappa = \sum_{\lambda=1}^{n} a'_{\varkappa\lambda} x'_\lambda, \quad \text{где} \quad a'_{\varkappa\lambda} = \sum_{\beta=1} a_{\varkappa\beta} p_{\beta\lambda}.$$

Отсюда видно, что

$$\begin{vmatrix} a'_{11} & a'_{12} & \ldots & a'_{1n} \\ a'_{21} & a'_{22} & \ldots & a'_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a'_{n1} & a'_{n2} & \ldots & a'_{nn} \end{vmatrix} = \begin{vmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{vmatrix} \cdot |P|,$$

т. е. детерминант системы

$$\Delta = \begin{vmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{vmatrix}$$

есть совокупный инвариант наших форм веса 1.

Пример 3. Формула (62) § 174 показывает, что для квадратичной формы детерминант, составленный из ее коэфициентов, есть инвариант веса 2.

Пример 4. Пусть формы $f_1, f_2, \ldots, f_n$, посредством линейной подстановки P переходят в $F_1, F_2, \ldots, F_n$; пусть $\xi_1, \xi_2, \ldots, \xi_n$ — новые переменные, которые мы подвергаем той же линейной подстановке P, отчего они переходят в $\xi_1', \xi_2', \ldots, \xi_n'$. Тогда посредством той же линейной подстановки P, произведенной и над x_α и над ξ_α, формы

$$\sum_{i=1}^{n} \xi_i \frac{\partial f_\alpha}{\partial x_i}$$

перейдут в формы:

$$\sum_{i=1}^{n} \xi_i' \frac{\partial F_\alpha}{\partial x_i'}.$$

Действительно, заменив x_i через $x_i = t\xi_i$ мы получим по формуле Тэйлора (§ 54):

$$f_\alpha(x_1 + t\xi_1, x_2 + t\xi_2, \ldots, x_n + t\xi_n) =$$

$$= f_\alpha + t\sum_{i=1}^{n} \xi_i \frac{\partial f_\alpha}{\partial x_i} + \frac{t^2}{2!} \sum_{i,k=1}^{n} \xi_i \xi_k \frac{\partial^2 f_\alpha}{\partial x_i \partial x_k} + \ldots, \tag{11}$$

где через f_α без указания аргументов мы обозначаем ту же функцию от аргументов $x_1, x_2, \ldots, x_n$.

Произведя над x_α и ξ_α подстановку P, мы получим:

$$F_\alpha(x_1' + t\xi_1', x_2' + t\xi_2', \ldots, x_n' + t\xi_n') =$$

$$= F_\alpha + t\sum_{i=1}^{n} \xi_i' \frac{\partial F_\alpha}{\partial x_i'} + \frac{t^2}{2!} \sum_{i,k=1}^{n} \xi_i' \xi_k' \frac{\partial^2 F_\alpha}{\partial x_i' \partial x_k'} + \ldots \tag{12}$$

Но подстановка P не изменяет t; следовательно, коэфициенты при одинаковых степенях t должны быть равны; сравнивая коэфициенты при t, найдем:

$$\sum_{i=1}^{n} \xi_i \frac{\partial f_\alpha}{\partial x_i} = \sum_{i=1}^{n} \xi_i' \frac{\partial F_\alpha}{\partial x_i'},$$

что и требовалось доказать. Это верно при $\alpha = 1, 2, \ldots, n$; таким образом мы имеем преобразование n линейных форм

$$\sum_{i=1}^{n} \xi_i \frac{\partial f_\alpha}{\partial x_i}$$

и, следовательно, по 2, эти формы имеют совокупный инвариант веса 1:

$$\Delta = \begin{vmatrix} \frac{\partial f_1}{\partial x_1} & \frac{\partial f_1}{\partial x_2} & \cdots & \frac{\partial f_1}{\partial x_n} \\ \frac{\partial f_2}{\partial x_1} & \frac{\partial f_2}{\partial x_2} & \cdots & \frac{\partial f_2}{\partial x_n} \\ \cdots\cdots & \cdots\cdots & \cdots & \cdots\cdots \\ \frac{\partial f_n}{\partial x_1} & \frac{\partial f_n}{\partial x_2} & \cdots & \frac{\partial f_n}{\partial x_n} \end{vmatrix} = D\left(\frac{f_1, f_2, \ldots, f_n}{x_1, x_2, \ldots, x_n}\right).$$

Это так называемый *функциональным детерминант* или *якобиан* [по имени математика Якоби (Jacobi)] форм $f_1, f_2, \ldots, f_n$; он является совокупным, ковариантом этих форм веса 1.

Пример 5. Из тех же формул (11) и (12), примененных к *одной* только форме f, найдем, сравнивая коэфициенты при t^2, что

$$\sum_{i,k=1}^{n} \xi_i \xi_k \frac{\partial^2 f}{\partial x_i \partial x_k}$$

посредством P перейдет в

$$\sum_{i,k=1}^{n} \xi'_i \xi'_k \frac{\partial^2 F}{\partial x'_i \partial x'_k};$$

это — квадратичная форма от $\xi_1, \xi_2, \ldots, \xi_n$; следовательно, по 3, заключаем, что она имеет инвариант веса 2:

$$H = \begin{vmatrix} \dfrac{\partial^2 f}{\partial x_1^2} & \dfrac{\partial^2 f}{\partial x_1 \partial x_2} & \cdots & \dfrac{\partial^2 f}{\partial x_1 \partial x_n} \\ \dfrac{\partial^2 f}{\partial x_2 \partial x_1} & \dfrac{\partial^2 f}{\partial x_2^2} & \cdots & \dfrac{\partial^2 f}{\partial x_2 \partial x_n} \\ \cdots\cdots & \cdots\cdots & \cdots\cdots & \cdots\cdots \\ \dfrac{\partial^2 f}{\partial x_n \partial x_1} & \dfrac{\partial^2 f}{\partial x_n \partial x_2} & \cdots & \dfrac{\partial^2 f}{\partial x_n^2} \end{vmatrix}.$$

Это так называемый *детерминант Гессе* (Hesse) или *гессиан* формы f; для f он является ковариантом веса 2. Легко видеть, что H есть якобиан для $\dfrac{\partial f}{\partial x_1}, \dfrac{\partial f}{\partial x_2}, \ldots, \dfrac{\partial f}{\partial x_n}$:

$$H = D\left(\frac{\dfrac{\partial f}{\partial x_1}, \dfrac{\partial f}{\partial x_2}, \ldots, \dfrac{\partial f}{\partial x_n}}{x_1, x_2, \ldots, x_n}\right).$$

Пример 6. Заметим, что всякую неоднородную ц. р. функцию мы можем превратить в однородную, введя еще новое переменное t и приписав к каждому члену множителем некоторую степень t так, чтобы после этого все члены получили одно и то же измерение. Таким образом мы можем ц. р. функцию одного переменного

$$f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_n$$

превратить в бинарную форму n-й степени:

$$f(x, y) = a_0 x^n + a_1 x^{n-1} y + a_2 x^{n-2} y^2 + \ldots + a_n y^n; \tag{13}$$

это самый общий вид бинарной формы. Обозначим через $\alpha_1, \alpha_2, \ldots, \alpha_n$ корни функции $f(x)$; тогда $f(x) = a_0(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n)$; заменим $\alpha_1, \alpha_2, \ldots, \alpha_n$, отношениями $\dfrac{\alpha_1}{\beta_1}, \dfrac{\alpha_2}{\beta_2}, \ldots, \dfrac{\alpha_n}{\beta_n}$; тогда получим:

$$f(x, y) = a(x\beta_1 - y\alpha_1)(x\beta_2 - y\alpha_2) \cdots (x\beta_n - y\alpha_n),$$

где $a\beta_1\beta_2\cdots\beta_n = a_0$. Произведя теперь над x, y подстановку

$$P = \begin{pmatrix} p_1 & q_1 \\ p_2 & q_2 \end{pmatrix},$$

мы увидим, что α_λ, β_λ испытают подстановку:

$$\alpha'_\lambda = q_2\alpha_\lambda - q_1\beta_\lambda, \qquad \beta'_\lambda = p_1\beta_\lambda - p_2\alpha_\lambda;$$

действительно:

$$\begin{aligned} x\beta_\lambda - y\alpha_\lambda &= (p_1x' + q_1y')\beta_\lambda - (p_2x' + q_2y')\alpha_\lambda = \\ &= x'(p_1\beta_\lambda - p_2\alpha_\lambda) - y'(q_2\alpha_\lambda = q_1\beta_\lambda) = x'\beta'_\lambda - y'\alpha'_\lambda; \end{aligned}$$

отсюда видно, что $x\beta_\lambda - y\alpha_\lambda$ (при $\lambda = 1, 2, \ldots, n$) являются ковариантами формы (13), и при этом *иррациональными* ковариантами (ибо α_λ и β_λ иррациональны). Находим, далее:

$$\alpha'_\varkappa\beta'_\lambda - \alpha'_\lambda\beta'_\varkappa = \begin{vmatrix} \alpha'_\varkappa & \beta'_\varkappa \\ \alpha'_\lambda & \beta'_\lambda \end{vmatrix} = \begin{vmatrix} q_2\alpha_\varkappa q_1\beta_\varkappa & p_1\beta_\varkappa - p_2\alpha_\varkappa \\ q_2\alpha_\lambda - q_1\beta_\lambda & p_1\beta_\lambda - p_2\alpha_\lambda \end{vmatrix} =$$

$$= \begin{vmatrix} q_2 & -q_1 \\ -p_2 & p_1 \end{vmatrix} \cdot \begin{vmatrix} \alpha_\varkappa & \beta_\varkappa \\ \alpha_\lambda & \beta_\lambda \end{vmatrix} = |P| \cdot (\alpha_\varkappa\beta_\lambda - \alpha_\lambda\beta_\varkappa).$$

Следовательно, $\alpha_\varkappa\beta_\lambda - \alpha_\lambda\beta_\varkappa$? (при $\varkappa\lambda = 1, 2, \ldots, n$, $\varkappa \neq \lambda$) суть (иррациональные) инварианты формы (13) веса 1.

Пример 7. Из 6 следует, что от подстановки P

$$D = \prod_{\varkappa\neq\lambda} (\alpha_\varkappa\beta_\lambda - \alpha_\lambda\beta_\varkappa)^2$$

перейдет в

$$D = \prod_{\varkappa\neq\lambda} (\alpha'_\varkappa\beta'_\lambda - \alpha'_\lambda\beta'_\varkappa)^2 = D = \prod_{\varkappa\neq\lambda} (\alpha_\varkappa\beta_\lambda - \alpha_\lambda\beta_\varkappa)^2|P|^2 = |P|^{n(n-1)} \cdot D,$$

ибо в D как раз $\dfrac{n(n-1)}{2}$ квадратных сомножителей. Но D по существу есть не что иное, как дискриминант формы (13). Итак, дискриминант бинарной формы n-й степени есть инвариант веса $n(n-1)$.

Пример 8. Пусть имеем теперь две бинарные формы: (13) и

$$g(x, y) = b_0x^m + b_1x^{m-1}y + \ldots + b_my^m = b(x\delta_1 - y\gamma_1)\cdots(x\delta_m - y\gamma_m).$$

Применяем и к $f(x, y)$, и к $g(x, y)$ одну и ту же линейную подстановку P. Тогда, как и в 6, найдем:

$$\gamma'_\varkappa\beta'_\lambda - \alpha'_\lambda\delta'_\varkappa = |P| \cdot (\gamma_\varkappa\beta_\lambda - \alpha_\lambda\delta_\varkappa),$$

а отсюда

$$\prod_{\substack{\varkappa = 1, 2, \ldots, m \\ \lambda = 1, 2, \ldots, n}} (\gamma'_\varkappa\beta'_\lambda - \alpha'_\lambda\delta'_\varkappa) = |P|^{mn} \cdot \prod_{\substack{\varkappa = 1, 2, \ldots, m \\ \lambda = 1, 2, \ldots, n}} (\gamma_\varkappa\beta_\lambda - \alpha_\lambda\delta_\varkappa),$$

т. е. результант двух бинарных форм есть совокупный инвариант этих форм веса mn.

§ 184. Теорема. *Если n — число переменных, m — степень данной формы, ν — степень ее коварианта относительно переменных x_α, μ — степень коварианта относительно коэфициентов a данной формы, λ — вес коварианта, то*

$$m\mu = n\lambda + \nu. \tag{14}$$

Доказательство. Эту формулу мы выведем, сравнив в обеих частях равенства (9) степени этих частей относительно коэфициентов p_{ik}. Заметим, что x^α первой степени относительно p_{ik}, $|P|$ n-й степени относительно p_{ik}, A m-й степени относительно p_{ik}; отсюда и получается формула (14). Она легко обобщается на случай совокупного ковариант k форм:

$$\sum_{i=1}^{k} m_i\mu_i = n\lambda + \nu, \tag{14a}$$

где m_i — степень формы f_i, μ_i — степень коварианта относительно коэфициентов формы f_i. Для инвариантов получаем соответственные формулы, полагая $\nu = 0$, а именно:

$$m\mu = n\lambda, \qquad \sum_{i=1}^{k} m_i\mu_i = n\lambda. \tag{14}$$

§ 185. Бинарные формы. В § 162 мы видели, что всякая неособенная матрица 2-го порядка представляется как произведение матриц $V = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $T_a = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ и $S_a = \begin{pmatrix} 1 & 0 \\ 0 & a \end{pmatrix}$. При переводе на язык подстаковок это значит, что всякая собственная бинарная линейная подстановка сводится на ряд подстановок типов:

$$V)\ \ x = -y',\ y = x', \qquad T_a)\ \ x = x' + ay',\ y = y', \qquad S_a)\ \ x = x',\ y = ay'.$$

Следовательно, чтобы убедиться, будет ли данная функция K ковариантом бинарной формы, достаточно проверить формулу (9) для подстановок V, T_a, S_a.

В теории инвариантов и ковариантов удобно к каждому члену бинарной формы приписывать биномиальный коэфициент, что, очевидно, не нарушает общности.

Итак, пусть данная форма:

$$f(x,y) = a_0x^n + na_1x^{n-1}y + \ldots + \binom{n}{i} a_ix^{n-i}y^i + \ldots + a_ny^n.$$

Пусть

$$K = \sum_{\alpha=0}^{k} S_\alpha(a)x^{k-\alpha}y^\alpha$$

ковариант формы $f(x,y)$ степени k, веса λ. Произведя подстановку S_m, т. е, $x = x'$; $y = my'$; получим:

$$\sum_{\alpha=0}^{k} S_\alpha(A) x'^{k-\alpha} y'^{\alpha} = m^\lambda = \sum_{\alpha=0}^{k} S_\alpha(a) x^{k-\alpha} y^\alpha, \tag{15}$$

так как по условию K — ковариант веса λ, а $|S_m| = m$. Но легко проверить, что $A_i = a_i m^i$.

Пусть $S_a(a) = \sum c a_0^{l_0} a_1^{l_1} \cdots a_n^{l_n}$; вес члена $c a_0^{l_0} a_1^{l_1} \cdots a_n^{l_n}$ (в смысле § 148) есть $\omega = l_1 + 2l_2 + \ldots + nl_n$. Подстановка S_m заменяет $S_\alpha(a)$ через $S_\alpha(A)$, и члену $c a_0^{l_0} a_1^{l_1} \cdots a_n^{l_n}$ соответствует в $S_\alpha(A)$ член

$$c A_0^{l_0} A_1^{l_1} \cdots A_n^{l_n} = c a_0^{l_0} a_1^{l_1} \cdots a_n^{l_n}\ m^\omega.$$

Но (15) есть тождество; подставив в правой части x' вместо x и my' вместо y, мы должны получить, что члены, содержащие одно и то же произведение $a_0^{l_0} a_1^{l_1} \cdots a_n^{l_n}$ $x'^{k-\alpha} y'^{\alpha}$ в обеих частях (15), должны быть одинаковы. Это дает:

$$c a_0^{l_0} a_1^{l_1} \cdots a_n^{l_n}\, m^\omega\, x'^{k-\alpha} y'^{\alpha} = m^\lambda\, c a_0^{l_0} a_1^{l_1} \cdots a_n^{l_n} x'^{k-\alpha} y'^{\alpha} m^\alpha,$$

откуда

$$\omega = l_1 + 2l_2 + \ldots + nl_n = \lambda + \alpha,$$

т. е. $S_\alpha(a)$ — изобаричная функция веса $\lambda + \alpha$ (в смысле § 148).

Обратно, если это условие выполнено для каждого $S_\alpha(a)$ $(\alpha = 1, 2, \ldots, k)$, то K — ковариант относительно подстановок S_m. В частности $S_0(a)$ должна быть изобаричной функцией веса λ, т. е. веса самого ковариант (в смысле § 183); $S_0(a)$ называется *ведущим членом ковариант*.

Однородная изобаричная ц. р. функция от коэфициентов бинарной формы называется *полуинвариантом*, если она инвариантна относительно подстановок $T_r = \begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix}$; от такой подстановки коэфициенты формы $a_0, a_1, \ldots$ перейдут в $A_0 = a_0$, $A_1 A = a_1 + r a_0$, $A_2 = a_2 + 2ra_1 + r^2 a_0$, … Следовательно, a_0 есть полуинвариант данной формы.

Далее, $A_0 A_2 - A_1^2 = a_0 a_2 - a_1^2$, т. е. и $a_0 a_2 - a_1^2$ тоже полуинвариант данной формы. Заметим, что a_0 есть ведущий член самой формы f, а $a_0 a_2 - a_1^2$ ведущий член ковариант Гессе для f.

Теорема. *Ведущий член ковариант бинарной формы есть полуинвариант этой формы.*

Доказательство. Нам нужно доказать, что $S_0(a)$ инвариантно относительно подстановки T_r, или $x = x' + ry'$, $y = y'$; или $x' = x - ry$, $y' = y$; $|T_r| = 1$. Так как K ковариант, то

$$\sum_{\alpha=1}^{k} S_\alpha(A)(x - ry)^{k-\alpha} y^\alpha = \sum_{\alpha=1}^{k} S_\alpha(a) x^{k-\alpha} y^\alpha;$$

отсюда $S_0(A) = S_0(a)$, что и требовалось доказать.

§ 186. Посредством подстановки T_r каждый корень уравнения

$$f\left(\frac{x}{y},1\right)=0$$

уменьшается на r, а следовательно, разность двух корней не изменяется. При $r=-\dfrac{a_1}{a_0}$ мы получаем A_1 и f посредством $T_{-\frac{a_1}{a_0}}$ переходит в

$$g(x',y')=a_0x'^n+\binom{n}{2}b_2x'^{n-2}y'^2+\binom{n}{3}b_3x'^{n-3}y'^3+\ldots+b_ny'^n;$$

здесь

$$b_2=a_2-\frac{a_1^2}{a_0},\quad b_3=a_3-3\frac{a_1a_3}{a_0}+2\frac{a_1^3}{a_0^2},\quad \ldots;$$

если $x_1,x_2,\ldots,x_n$ корни уравнения $f\left(\dfrac{x}{y},1\right)=0$, то корни уравнения $g\left(\dfrac{x'}{y'},1\right)=0$ будут $x_\alpha+\dfrac{a_1}{a_0}$ $(\alpha=1,2,\ldots,n)$. Но

$$\begin{aligned}x_\alpha+\frac{a_1}{a_0} &= x_\alpha-\frac{1}{n}(x_1+x_2+\ldots+x_n)=\\ &= \frac{1}{n}[(x_\alpha-x_1)+(x_\alpha-x_2)+\ldots+(x_\alpha-x_n)]\end{aligned}$$

$\left(\text{ибо}x_1+x_2+\ldots+x_n=-\dfrac{na_1}{a_0}\right)$. Это показывает, что корни уравнения $g\left(\dfrac{x'}{y'},1\right)=0$ инвариантны относительно подстановок T_r, а следовательно, и симметрические функции от них $\dfrac{b_2}{a_0}$, $\dfrac{b_3}{a_0}$, $\ldots$ тоже инвариантны относительно T_r. Следовательно, однородные изобаричные полиномы:

$$\left.\begin{aligned}S_2&=a_0b_2=a_0a_2-a_1^2,\\ S_3&=a_0^2b_3=a_0^2a_3-3a_0a_1a_2+2a_1^3,\\ S_4&=a_0^3b_4=a_0^3a_4-4a_0^1a_1a_3+6a_0a_1^2-3a_1^4\end{aligned}\right\}\qquad(16)$$

и т. д. до S_n включительно все — полуинварианты формы f. Если $S(a_0,a_1,a_2,\ldots,a_n)$ любой полуинвариант для f, то он допускает и подстановку $T_{-\frac{a_1}{a_0}}$, т. е. имеем:

$$S(a_0,a_1,a_2,\ldots,a_n)=S(a_0,0,b_2,\ldots,b_n)=S\left(a_0,0,\frac{S_2}{a_0},\ldots,\frac{S_n}{a_0^{n-1}}\right),$$

т. е.

Теорема. *Всякий полуинвариант формы f есть полином от $a_0,S_2,\ldots,S_n$, делений на некоторую степень a_0.*

Мы видели, что ведущий член коварианта формы f есть полуинвариант для f. Возникает вопрос: всякий ли полуинвариант для f может быть ведущим членом некоторого коварианта? Ответ на этот вопрос утвердительный. Но мы докажем здесь только следующую теорему:

Теорема. *Если S полуинвариант формы f веса λ степени d, то существует не больше одного ковариантa формы f с ведущими членом S, и этот ковариант K имеет степень $k = nd - 2\lambda$.*

Доказательство. Вес K (как ковариантa) равен весу S (в смысле § 148); формула (14) § 184 дает $nd = 2\lambda + k$; следовательно, $k = nd - 2\lambda$. Пусть существуют два ковариантa с ведущим членом S: K и K_1; они одного и того же веса λ, и их разность (в которой ведущие члены сокращаются) имеет множителя y: она равна $y \cdot \varphi(a_0, a_1, \ldots, a_n, x, y)$; посредством любой подстановки P эта функция перейдет в функцию $y'\varphi(A_0, A_1, \ldots, A_n, x', y')$, и мы будем иметь:

$$y'\varphi(A_0, A_1, \ldots, A_n, x', y') = |P|^\lambda y\varphi(a_0, a_1, \ldots, a_n, x, y);$$

отсюда видно, что функция $y\varphi$ содержит совершенно произвольный линейный множитель $\dfrac{y'}{|P|^\lambda}$, ибо y' может быть произвольной линейной функцией от x и y. Но это, конечно, невозможно.

В этой теореме инварианты рассматриваются как частные случаи ковариантов; полуинвариант S инвариантен относительно подстановок T_r и S_m; если он, кроме того, допускает и подстановку V, то он (см. начало § 185) инвариант; в таком случае он сам является своим ведущим членом, и другого ковариантa с тем же ведущим членом у формы f не существует.

Если мы допустим, что существуют коварианты $K_1, K_2, \ldots, K_n$ с ведущими членами $a_0, S_2, \ldots, S_n$ [см. (16)], то легко доказать, что *для данной бинарной формы f существует только конечное число независимых ковариантов, так что всякий ее ковариант представляется как целая рациональная функция с численными коэфициентами от этих независимых ковариантов.* Эти независимые коварианты составляют так называемую *полную систему ковариантов формы f*. (И здесь инварианты рассматриваются как частные случаи ковариантов.)

Действительно, пусть S есть ведущий член данного ковариантa K; S — полуинвариант; следовательно:

$$S = F(a_0, S_2, S_3, \ldots, S_n) = \sum c a_0^\alpha S_2^\beta S_3^\gamma \cdots ;$$

все члены в S должны иметь один и тот же вес (ибо S изобарична): $\lambda = \beta\lambda_2 + \gamma\lambda_3 + \ldots$, где $\lambda_2, \lambda_3, \ldots$ веса $S_2, S_3, \ldots$ (вес $a_0 = 0$); следовательно, и K имеет (как ковариант) тот же вес λ; с другой стороны, $K_1^\alpha K_2^\beta K_3^\gamma \cdots$ тоже ковариант того же веса λ и $F(K_1, K_2, \ldots, K_n)$ — ковариант веса λ с ведущим членом $F(a_0, S_2, \ldots, S_n)$; по предыдущей теореме такой ковариант может быть только один; следовательно:

$$K = F(K_1, K_2, \ldots, K_n).$$

§ 187. Пусть опять

$$F(x', y') = \sum_{i=0}^{n} \binom{n}{i} a_i x^{n-i} y^i \tag{17}$$

данная бинарная форма, к которой мы применим подстановку T_m, т. е. $x = x' + my'$, $y = y'$; отчего наша форма примет вид:

$$F(x', y') = \sum_{i=0}^{n} \binom{n}{i} A_i x'^{n-i} y'^i, \tag{18}$$

где A_i — некоторые полиномы от m, $a_0, \ldots, a_n$. Диференцируем обе части тождества $f(x,y) = F(x',y')$ по m; в левой части будем иметь нуль, ибо $f(x,y)$ не зависит от m. Итак, получим:

$$0 \equiv \sum_{i=0}^{n} \binom{n}{i} \left\{ \frac{\partial A_i}{\partial m} x'^{n-i} y'^{i} - A_i (n-i)(x'^{n-i-1} y'^{i+1} \right\},$$

ибо $x' = x - my$, $y' = y$, следовательно, $\dfrac{\partial x'}{\partial m} = -y$. Так как правая часть тождественно равна нулю, то коэфициент при $x'^{n-i} y'^{i}$ должен обращаться в нуль, т. е.

$$\binom{n}{i} \frac{\partial A_i}{\partial m} - \binom{n}{i-1} (n-i+1) A_{i-1} = 0$$

(при $i = 0$ второй член левой части отсутствует). Но

$$\binom{n}{i} = \binom{n}{i-1} \frac{n-i+1}{i};$$

подставляя это в предыдущее равенство, найдем:

$$\frac{\partial A_0}{\partial m} = 0, \qquad \frac{\partial A_i}{\partial m} = i A_{i-1} \quad (i = 1, 2, \ldots, n). \tag{19}$$

Это — соотношения между коэфициентами A_i и m.

Пусть нам дан ковариант $K(a_0, \ldots, a_n; x, y)$ формы (17); обозначим $K_0 = K(a_0, \ldots, a_n; x, y)$, $K = K(A_0, \ldots, A_n; x, y)$. Мы применяем опять подстановку T_m и имеем тождество:

$$K_0 \equiv K.$$

Но K_0 не зависит от m; следовательно, и K — тоже, т. е.

$$\frac{\partial K}{\partial m} \equiv 0.$$

Обратно, из последнего тождества следует, что K не зависит от m, т. е. имеет при каком-нибудь m то же значение, что и при $m = 0$, т. е. $K \equiv K_0$, т. е. K — инвариант относительно T_m. Имеем:

$$\frac{\partial K}{\partial m} = \sum_{i=0}^{n} \frac{\partial K}{\partial A_i} \frac{\partial A_i}{\partial m} + \frac{\partial K}{\partial x'} \frac{\partial x'}{\partial m} \sum_{i=1}^{n} i A_{i-1} \frac{\partial K}{\partial A_i} - y' \frac{\partial K}{\partial x'}. \tag{20}$$

Так как это при всяком m тождественно равно нулю, то в частности и при $m = 0$, т. е.

$$\Omega K_0 - y \frac{\partial K_0}{\partial x} \equiv 0, \tag{21}$$

где

$$\Omega = \sum_{i=1}^{n} i a_{i-1} \frac{\partial}{\partial a_i} = a_0 \frac{\partial}{\partial a_1} + 2 a_1 \frac{\partial}{\partial a_2} + \ldots + n a_{n-1} \frac{\partial}{\partial a_n}. \tag{22}$$

Но тождество (21) остается в силе, если вместо x, y, $a_0, \ldots, a_n$ подставить x', y', $A_0, \ldots, A_n$; т. е. выполнение этого тождества (21) есть необходимое и достаточное условие того, чтобы K был ковариантом относительно подстановок T_m.

Переменим ролями x и y, а также a_i и a_{n-i} $(i = 0, 1, \ldots, n)$; тогда вместо T_m получим подстановку R_m: $x = x'$; $y = y' + mx'$, и мы можем сказать, что K тогда и только тогда ковариант относительно подстановки R_m, если

$$OK_0 - x\frac{\partial K_0}{\partial y} \equiv 0, \tag{21}$$

где

$$O = \sum_{i=1}^{n} i a_{n-i+1}\frac{\partial}{\partial a_{n-i}} = a_n\frac{\partial}{\partial a_{n-1}} + 2a_{n-1}\frac{\partial}{\partial a_{n-2}} + \ldots + na_1\frac{\partial}{\partial a_0}. \tag{22}$$

Относительно подстановок S_m K ковариант, если он изобаричен, причем вес x считается равным единице, а вес y считается равным нулю; это следует из результата § 185, состоящего в том, что при $K = \sum_{\alpha=0}^{k} S_\alpha(a)x^{k-\alpha}y^\alpha$ для подстановок S_m K тогда и только тогда ковариант, если $S_\alpha(a)$ изобаричная функция веса $\lambda + \alpha$ $(\alpha = 0, 1, 2, \ldots, k)$. Отсюда и следует, что K должен быть изобаркчным веса $\lambda + k$.

Но $V = T_{-1}R_1T_{-1}$; следовательно (ср. § 162), всякая бинарная собственная подстановка может быть рассматриваема как композиция подстановок типа T_m, R_m, S_m. Отсюда следует:

Теорема. *Полином $K(a_0, \ldots, a_n; x, y)$ тогда и только тогда ковариант бинарной формы (17), если он изобаричен и обращается в нуль операторами $\Omega - y\frac{\partial}{\partial x}$ и $O - x\frac{\partial}{\partial y}$.*

Напоминаем, что инвариант тут рассматривается как частный случай ковариантa, именно, когда K не зависит от x и y; там операторы будут просто Ω и O.

Однородный изобаричный полином от $a_0, \ldots, a_n$ тогда и только тогда полуинвариант, если он обращается в нуль оператором Ω.

§ 188. Коммутаторы. Мы имеем:

$$\left.\begin{aligned}\Omega &= \sum_{i=1}^{n} i a_{i-1}\frac{\partial}{\partial a_i} = \sum_{k=0}^{n-1}(k+1)a_k\frac{\partial}{\partial a_{k+1}},\\ O &= \sum_{i=1}^{n}(n-i+1)a_i\frac{\partial}{\partial a_{i-1}} = \sum_{k=0}^{n-1}(n-k)a_{k+1}\frac{\partial}{\partial a_k};\end{aligned}\right.$$

отсюда

$$\Omega O = \sum_{i=0}^{n} i a_{i-1}\left[(n-i+1)\frac{\partial}{\partial a_{i-1}} + \sum_{k=0}^{n-1}(n-k)a_{k+1}\frac{\partial^2}{\partial a_i \partial a_k}\right],$$
$$O\Omega = \sum_{k=0}^{n-1}(n-k)a_{k+1}\left[(k+1)\frac{\partial}{\partial a_{k+1}} + \sum_{i=1}^{n} i a_{i-1}\frac{\partial^2}{\partial a_k \partial a_i}\right].$$

Оператор $\Omega O - O\Omega$ называется коммутатором Ω и O; он содержит только первые производные (ибо вторые сокращаются). В первых членах ΩO положим $i+1$ вместо

i, а в первых членах $O\Omega$ положим $i-1$ вместо k; тогда

$$\begin{aligned}\Omega O - O\Omega &= \sum_{i=0}^{n-1}(i+1)a_i(n-i)\frac{\partial}{\partial a_i} - \sum_{i=1}^{n}(n-i+1)a_i i\frac{\partial}{\partial a_i} = \\ &= \sum_{i=0}^{n}(n-2i)a_i\frac{\partial}{\partial a_i}.\end{aligned} \tag{23}$$

Пусть S однородная функция от $a_0,\ldots,a_n$ степени μ; тогда по известной теореме Эйлера об однородных функциях

$$\sum_{i=0}^{n} a_i\frac{\partial S}{\partial a_i} \equiv \mu S.$$

Если S, кроме того, изобарична веса w, то, как легко проверить непосредственно для каждого члена функции S:

$$\sum_{i=0}^{n} i a_i\frac{\partial S}{\partial a_i} \equiv wS.$$

Подвергая S действию оператора (23) и применив указанные формулы, найдем:

Теорема. *Если S однородная (степени μ) и изобаричная (веса w) функция от $a_0,\ldots,a_n$, то*

$$(\Omega O - O\Omega)S \equiv (n\mu - 2w)S, \tag{24}$$

$$\Omega O^r - O^r\Omega)S \equiv r(n\mu - 2w - r + 1)O^{r-1}S. \tag{25}$$

Последнюю формулу доказываем методом полной индукции: полагая, что она правильна для r, докажем ее для $r+1$. Заметим, что функция OS — степени μ и веса $w+1$; поэтому, заменив в (25) S через OS, получим:

$$(\Omega O^r - O^r\Omega)OS \equiv r(n\mu - 2w - r - 1)O^{r-1}OS;$$

отсюда

$$\begin{aligned}(\Omega O^{r+1} - O^{r-1}\Omega)S &\equiv (\Omega O^r - O^r\Omega)OS + O^r(\Omega O - O\Omega)S \equiv \\ &\equiv r(n\mu - 2w - r - 1)O^rS + (n\mu - 2w)O^rS \equiv \\ &\equiv (r+1)(n\mu - 2w - r)O^rS,\end{aligned}$$

т. е. формула (25) верна и для $r+1$, т. е. доказана, вполне.

Таким же образом докажем формулу:

$$(O\Omega^r - \Omega^r O)S \equiv r(-n\mu + 2w - r + 1))\Omega^{r-1}S, \tag{26}$$

принимая во внимание, что ΩS степени μ и веса $w-1$.

§ 189. Существование ковариант с данным ведущим членом.

Лемма. *Если S не равный тождественно нулю полуинвариант степени μ веса w бинарной формы n-й степени, то $n\mu - 2w \geq 0$.*

Пусть $m\mu - 2w < 0$; так как $\Omega S \equiv 0$, то из (25) следует:

$$\Omega O^r S = r(n\mu - 2w - r + 1)O^{r-1}S \quad \text{для} \quad r = 1, 2, \ldots; \tag{27}$$

при этом $n\mu - 2w - r + 1 < 0$. Но вес OP на единицу больше, чем вес P, и наибольший вес полинома от $a_0, \ldots, a_n$ степени μ есть μn. С другой стороны, положив $r = n\mu - w + 1$, мы увидим, что вес $O^{n\mu-w+1}S$ будет $n\mu + 1$, т. е. больше, чем $n\mu$, где μ — степень S, а следовательно, и $O^{n\mu-w+1}S$. Отсюда следует:

$$O^{n\mu-w+1}S \equiv 0.$$

Но тогда (27) при $r = n\mu - w + 1$ даст:

$$O^{n\mu-w}S \equiv 0.$$

Положив теперь в (27) $r = n\mu - w$, найдем: $O^{n\mu-w-1}S \equiv 0$ и т. д., в конце концов найдем $OS \equiv 0$, $S \equiv 0$, что противоречит нашему условию. Этим лемма доказана.

Пусть дан ковариант с ведущим членом S:

$$K = Sx^\nu + S_1 x^{\nu-1}y + S_2 x^{\nu-2}y^2 + \ldots + S_\nu y^\nu.$$

По (14) § 184, где вместо m мы пишем n, вместо n пишем 2 и вместо λ пишем w, найдем для степени ν ковариантa:

$$\nu = n\mu - 2w.$$

Применяя к K формулу (21a), получим:

$$\begin{aligned}(OS - S_1)x^\nu \quad &+ \quad (OS_1 - 2S_2 0 x^{\nu-1}y + \ldots + \\ &+ \quad (OS_{\nu-1} - \nu S_\nu)xy^{\nu-1} + OS_\nu y^\nu \equiv 0.\end{aligned}$$

Но это имеет место тогда и только тогда, если

$$K = Sx^\nu + OSx^{\nu-1}y + \frac{1}{2!}O^2 S x^{\nu-2}y^2 + \ldots + \frac{1}{nu!}O^\nu S y^\nu, \tag{28}$$

и кроме того

$$O^{\nu+1}S \equiv 0. \tag{29}$$

Это последнее тождество нам и остается доказать. Заметим, что (27) при $r = \nu + 1 = n\mu - 2w + 1$ дает:

$$\Omega O^{\nu+1}S \equiv 0.$$

А так как $O^{\nu+1}S$ степени μ веса $W = w + \nu + 1 = n\mu - w + 1$ и обращается в нуль оператором Ω, то по § 187 (в конце) это — полуинвариант; но тогда по доказанной лемме он $\equiv 0$, ибо $n\mu - 2W = -(n\mu - 2w) - 2 < 0$. Следовательно, (29) выполнено, и (21a) выполнено для K, где K дается формулою (28). Но легко доказать, что и (21) для K выполнено, ибо, взяв ΩK, найдем в нем коэфициент при $x^{\nu-r}y^r$:

$$\frac{1}{r!}\Omega O^r S - \frac{1}{(r-1)!}(\nu - r + 1)O^{r-1}S,$$

а это по (27) $\equiv 0$. Отсюда по теореме § 187 заключаем, что (28) есть действительно ковариант данной формы. Итак:

Теорема. *Существует всегда и (по третьей теореме* § 185*) только один ковариант бинарной формы, ведущий член которого есть данный полуинвариант этой формы.*

Отсюда же следует, что существуют коварианты с ведущими членами $a_0, S_2, S_3, \ldots$ [см. (16) § 185], а следовательно, оправдывается и последнее заключение § 185 о том, что эти коварианты $K_1, K_2, K_3, \ldots, K_n$ образуют полную систему ковариантов данной бинарной формы n-й степени.

§ 190. Бинарные формы низших степеней.

1) $n = 1$; $f = a_0x + a_1y$. Здесь имеется только один независимый полуинвариант a_0 — ведущий член самой формы. Следовательно, f и составляет свою собственную полную систему ковариантов; всякий ковариант формы f есть целая рациональная функция от f.

2) $n = 2$; $f = a_0x^2 + 2a_1xy + a_2y^2$. Полная система полуинвариантов здесь: a_0 и $S_2 = a_0a_2 - a_1^2$; a_0 — ведущий член самой формы f; S_2 — инвариант для f (дискриминант). Следовательно, всякий ковариант формы f есть целая рациональная функция от f и S_2

3) n =3; $f = a_0x^3 + 3a_1x^2y + 3a_2xy^2 + a_3y^3$. Полная система полуинвариантов здесь a_0, S_2, S_3 [см. (16) § 185]; члены в S_2 и S_3, не содержащие a_0: $T_2 = -a_1^2$, $T_3 = 2a_1^3$, так что $4T_2^3 + T_3^2 = 0$; отсюда следует, что $4S_2^3 + S_3^2$ имеет множителем a_0; вычисляя, найдем:

$$\begin{aligned} 4S_2^3 + S_3^2 = &- a_0^3D, \quad \text{где} \quad D = 3a_1^2a_2^2 - 4a_1^3a_3 + \\ &+ 6a_0a_1a_2a_3 - 4a_0a_2^3 - a_0^2a_3^2; \end{aligned}$$

$27D$ — не что иное, как дискриминант кубической формы [ср. (29) § 149, приняв во внимание, что коэфициенты формы ? у нас a_0, $3a_1$, $3a_2$, a_3]. S_2 — ведущий член коварианта Гессе нашей формы:

$$H = (a_0a_2 - a_1^2)x^2 + (a_0a_3 - a_1a_2)xy + (a_1a_3 - a_2^2)y^3$$

(точнее, ковариант Гессе для f есть $36H$). Наконец, $S_3 = a_0^2a_3 - 3a_0a_1a_2 + 2a_1^3$ есть ведущий член функционального детерминанта G функций f и H, который тоже есть ковариант для f веса 3 (точнее, этот функциональный детерминант равен $3G$). Всякий ковариант формы f представляется как целая рациональная функция от f, D, H и G, причем G входит не выше чем в первой степени, так как существует следующее *соотношение Кэли*:

$$4H^3 + G^2 \equiv -f^2D.$$

4) $n = 4$; $f = a_0x^4 + 4a_1x^3y + 6a_2x^2y^2 + 4a_3xy^3 + a_4y^4$. Здесь полная система полуинвариантов: a_0, S_2, S_3, S_4; выделяя в этих полуинвариантах члены, не содержащие a_0, найдем: $4T_2^3 + T_3^2 = 0$, $3T_2^2 + T_4 = 0$; следовательно, $4S_2^3 + S_3^2$ и $3S_2^2 + S_4$ имеют множителем a_0; можно вычислить: $3S_2^2 + S_4 = a_0^2g_2$, где $g_2 = a_0a_4 - 4a_1a_3 + 3a_2^2$; далее $4S_2^3 + S_3^2 = a_0^2(S_2g_2 - a_0g_3)$, где $g_3 = a_0a_2a_4 - a_0a)3^2 + 2a_1a_2a_3 - a_1^2a_4 - a_2^3$. S_2 есть ведущий член формы H, где $144H$ — гессиан для f; S_3 — ведущий член формы

G, где $8G$ — якобиан для f и H; H и G — коварианты, а g_2 и g_3 — инварианты формы f. Дискриминант формы четвертой степени есть: $D = g_2^3 - 27g_3^2$.

Всякий ковариант формы f есть целая рациональная функция от f, g_2, g_3, H, G; между этими формами существует зависимость:

$$f^3 g_3 - f^2 H g_2 + 4H^3 + G^2 \equiv 0.$$

Упражнения

222) Найти полную систему ковариантов для формы $f = x^3 + 6x^2y - 3xy^2 + 2y^3$.
Отв. $D = -76$, $H = -5x^2 + 4xy + 3y^2$, $G = 24x^3 - 6x^2y + 48xy^2 - 14y^3$.
223) То же для формы $f = (x - y)^4$.
Отв. $g_2 \equiv g_3 \equiv H \equiv G \equiv 0$.

ГЛАВА ОДИННАДЦАТАЯ

ТЕОРИЯ ГРУПП

§ 191. Введение. Основные постулаты. В предыдущих главах мы уже не раз сталкивались с понятием *группы*; мы встречались и с группами подстановок данных символов (§ 26—28, 152), и с группами матриц (§ 157, 173, 179), и с группами геометрических преобразований (§ 182). Несмотря на разнообразие конкретных объектов («элементов»), из которых составляются эти группы, действие над этими объектами в различных конкретных примерах было подчинено одним и тем же основным законам; эти законы мы перечисляли в § 27. Теперь мы построим абстрактную теорию групп, причем ограничимся конечными группами, особенно важными для алгебры, ибо они имеют большие приложения в теории алгебраических уравнений (главы XII и XIII). Только в конце этой главы мы скажем несколько слов и о бесконечных группах.

В абстрактной теории групп природа тех объектов, над которыми мы совершаем наше действие, для нас безразлична; мы будем их называть *элементами* и обозначать большими латинскими буквами: A, B, C, A_1, P, ... Известно только, что над всякими двумя взятыми в определенном порядке элементами (необязательно отличными друг от друга) можно совершить некоторое «действие» (которое мы обозначаем, как обычное умножение, точкой, или просто ставя элементы рядом), в результате которого мы получаем некоторый третий элемент (необязательно отличный от первых двух). Для этого действия должны быть верны все законы, перечисленные в § 27 и верные для подстановок данных символов. Но, определяя действие абстрактной группы, нам нет надобности перечислять все эти законы, ибо они не независимы: одни вытекают из других. Достаточно формулировать только независимые законы, выставить их как данные постулаты, определяющие действие абстрактной группы, и выводить из них остальные законы как теоремы. Так мы получаем *систему постулатов*, определяющую группу. Разные авторы давали разные системы постулатов. Мы приведем систему постулатов Фробениуса (Frobenius), одну из самых ранних по времени и одну из наиболее простых; эта система состоит из четырех следующих постулатов:

I. Действие наше однозначно и применимо ко всяким двум элементам.

II. Действие однозначно-обратимо, т, е. из $AC = BC$ или из $CA = CB$ следует $A = B$.

III. Для него верен ассоциативный закон:

$$(AB)C = A(BC) = ABC. \tag{1}$$

(Закон этот непосредственно обобщается на несколько сомножителей: сомножители произведения можно соединять в какие угодно группы, лишь бы не изменялся порядок, в котором они стоят).

IV. Множество всех наших элементов конечно.

В теории матриц постулат IV не выполнен: там могут быть и бесконечные группы. Мы вводим постулат IV, желая ограничиться конечными группами, которые сейчас нас только и интересуют [92]. Заметим, что коммутативный закон мы вообще не предполагаем верным.

Наши элементы мы будем соединять в совокупности, которые назовем «комплексами», и будем обозначать большими готическими буквами; тот факт, что данные элементы A, B, C, ... объединяются в комплекс $\mathfrak{A}$ мы обозначим, соединяя A, B, C, ... знаками $+$:

$$\mathfrak{A} = A + B + C + \ldots \tag{2}$$

Точно так же два и больше комплексов мы можем объединить в более обширный комплекс; пусть, например $\mathfrak{B} = P + Q + R + \ldots$, тогда

$$\mathfrak{C} = \mathfrak{A} + \mathfrak{B} = A + B + C + \ldots + P + Q + R + \ldots \tag{3}$$

Конечно, для этой символической суммы верны и коммутативный и ассоциативный законы, ибо здесь фактически нет никакого «действия» в смысле получения новых элементов, а просто объединение в совокупность. В таком обозначении, как (2), необязательно все элементы A, B, C ... должны быть различны; например, если $\mathfrak{A}$ и $\mathfrak{B}$ содержат общие элементы, то в правой части (3) необходимо попадутся равные элементы. Число различных элементов в комплексе назовем *порядком* комплекса. Один элемент можно рассматривать как комплекс первого порядка.

Произведение комплекса на комплекс (и комплекса на элемент) мы определяем по правилу произведения обычных сумм:

$$\mathfrak{A}\mathfrak{B} = (A + B + C + \ldots)(P + Q + R + \ldots) =$$
$$= AP + AQ + \ldots + BP + BQ + + \ldots;$$
$$\mathfrak{A}P = AP + BP + CP + \ldots;$$

конечно, вообще $\mathfrak{A}\mathfrak{B} \neq \mathfrak{B}\mathfrak{A}$, но ассоциативный закон верен. Что касается постулата II, то он вообще неверен для произведений комплексов: из $\mathfrak{A}\mathfrak{C} = \mathfrak{B}\mathfrak{C}$, или из $\mathfrak{C}\mathfrak{A} = \mathfrak{C}\mathfrak{B}$ вообще не следует, что $\mathfrak{A} = \mathfrak{B}$. В одном только случае постулат II верен: если два комплекса, будучи умножены на один и тот же элемент, дают равные результаты, то и эти два комплекса равны: из $\mathfrak{A}P = \mathfrak{B}P$ или $P\mathfrak{A} = P\mathfrak{B}$ следует $\mathfrak{A} = \mathfrak{B}$.

Пусть, например, $\mathfrak{A} = A + B + C + \ldots$, $\mathfrak{B} = K + L + M + \ldots$, тогда $\mathfrak{A}P = \mathfrak{B}P$ дает

$$AP + BP + CP + \ldots = KP + LP + MP + \ldots;$$

элемент AP стоит в левой части, значит, в правой есть равный ему элемент, например, KP; $AP = KP$, откуда по постулату II заключаем: $A = K$. Так мы докажем, что всякий элемент из $\mathfrak{A}$ встречается и в $\mathfrak{B}$, и обратно. Заметим, что, когда

[92] Заметим, что для бесконечных групп недостаточно было бы просто отбросить постулат IV: надо было бы вместо постулата об однозначной обратимости ввести постулат о неограниченной обратимости, т. е. о том, что уравнения $AX = B$ и $YA = B$ всегда имеют решения.

говорится о равенстве комплексов, принимаются во внимание только различные элементы в каждом комплексе.

Если элемент P входит в комплекс $\mathfrak{A}$, то мы будем писать $P \subset \mathfrak{A}$. Если все (различные) элементы из $\mathfrak{B}$ входят также и в $\mathfrak{A}$, то мы будем обозначать $\mathfrak{B} \subset \mathfrak{A}$. Из $\mathfrak{B} \subset \mathfrak{A}$ и $\mathfrak{A} \subset \mathfrak{B}$ следует $\mathfrak{A} = \mathfrak{B}$.

Все наши элементы составляют группу. Но обычно уже часть всех элементов составляет группу; как мы эту часть охарактеризуем? Эта часть есть некоторый комплекс $\mathfrak{A}$, отличающийся следующим свойством: если $A \subset \mathfrak{A}$ и $B \subset \mathfrak{A}$, то и $AB \subset \mathfrak{A}$ (это так называемое «групповое» свойство). Или короче это можно выразить так: $\mathfrak{A}\mathfrak{A} \subset \mathfrak{A}$; обычно обозначают: $\mathfrak{A}\mathfrak{A} = \mathfrak{A}^2$. Следовательно, группа $\mathfrak{A}$ определяется следующей формулой: $\mathfrak{A}^2 \subset \mathfrak{A}$.

§ 192. Следствия из основных постулатов. Теорема 1. *Если $\mathfrak{A}$ группа и элемент $P \subset \mathfrak{A}$, то*

$$\mathfrak{A}P = P\mathfrak{A} = \mathfrak{A}.$$

Доказательство. Если $\mathfrak{A} = A_1 + A_2 + \ldots + A_n$ и P — один из элементов $A_\varkappa$, то $A_1P, A_2P, \ldots, A_nP$ — все элементы из $\mathfrak{A}$, и все они различны (по постулату II); следовательно, это все элементы $A_1, A_2, \ldots, A_n$ (только в другом порядке) и $\mathfrak{A}P = \mathfrak{A}$. Подобным же образом докажем, что $P\mathfrak{A} = \mathfrak{A}$.

Следствие 1. Если $\mathfrak{B}$ комплекс элементов из $\mathfrak{A}$, то $\mathfrak{A}\mathfrak{B} = \mathfrak{B}\mathfrak{A} = \mathfrak{A}$.

Следствие 2. При $\mathfrak{B} = \mathfrak{A}$ получим $\mathfrak{A}^2 = \mathfrak{A}$; это — новое определение группы.

Итак, при $P \subset \mathfrak{A}$ $\mathfrak{A}P = \mathfrak{A}$; следовательно, одно из произведений $A_\varkappa P$ равно P; пусть это будет $EP = P$, где E — один из элементов $\subset \mathfrak{A}$. Если X — любой из наших элементов (необязательно $X \subset \mathfrak{A}$), то имеем $X(EP) = XP$; но по постулату III $(XE)P = X(EP) = XP$ и по постулату II $XE = X$; далее, $(XE)X = XX$, $X(EX) = XX$ и опять по постулату II $EX = X$. Такой элемент E единственный; если F тоже отличается свойством, что для всякого X $XF = FX = X$, то найдем, с одной стороны, $FE = E$, а с другой, $FE = F$, т. е. $F = E$. Далее, $E^2 = E$ и этим равенством E вполне определяется: если и $F^2 = F$, то, перемножив, найдем $E^2F = EF^2$, $E^2F = (EF)F$; по постулату II $E^2 = EF$ и еще раз по постулату II $E = F$. Итак:

Теорема 2. *Среди наших элементов имеется один элемент E, характеризуемый следующим свойством: $E^2 = E$; этот элемент E переместим со всяким другим элементом X, причем $XE = EX = X$. Этот же элемент E непременно входит во всякую группу, которую можно образовать из наших элементов. Он один также составляет группу, — единственную группу первого порядка.*

Этот элемент E называется *главным* элементом или *единицей* [93], а группа, им одним образуемая, — *главной* или *единичной* группой.

Возвратимся опять к равенству $\mathfrak{A}P = \mathfrak{A}$ при $P \subset \mathfrak{A}$. Так как $E \subset \mathfrak{A}$, то для некоторого Q будет $QP = E$; отсюда $(QP)Q = EQ = QE$, $Q(PQ) = QE$ и по постулату II $PQ = E$. По постулату II легко заключить, что такой элемент Q — единственный для данного P; он называется *обратным* к P элементом и обозначается P^{-1}. Итак:

[93] Некоторые авторы обозначают его просто через единицу; я не ввожу этого обозначения во избежание путаницы с обычной единицей.

Теорема 3. *Для каждого из наших элементов P существует единственный обратный к P элемент P^{-1}, отличающийся следующим свойством: $PP^{-1} = P^{-1}P = E$. Если в данную группу входит P, то туда непременно входит и P^{-1}.*

Свойство обратности взаимное: P есть обратный элемент к P^{-1}.

Теорема 4. $(AB)^{-1} = B^{-1}A^{-1}$*; это же обобщается и на несколько сомножителей.*

Теорема 5. *Если $\mathfrak{A}$ — группа и $\mathfrak{A}P = \mathfrak{A}$ (или $P\mathfrak{A} = \mathfrak{A}$), то P — элемент из $\mathfrak{A}$* (это — теорема, обратная к теореме 1).

Доказательство. В $\mathfrak{A}$ имеется элемент E; из $\mathfrak{A}P = \mathfrak{A}$ заключаем, что $EP = P \subset \mathfrak{A}$.

Теорема 6. *При всяких данных A и B уравнения $AX = B$ и $YA = B$ имеют решения, принадлежащие ко всякой группе, куда входят A и B.*

Доказательство. Легко убедиться, что $X = A^{-1}B$, $Y = BA^{-1}$ являются искомыми решениями, принадлежащими к той же группе, куда входят A и B: по постулату II эти решения единственные.

§ 193. Степени элемента. Если A данный элемент, то мы определяем:

$$A^2 = AA, \quad A^3 = A^2A, \ \ldots, \ A^n = A^{n-1}A = \underbrace{AA\cdots A}_{n \text{ раз}}, \quad A^0 = E,$$

$$A^{-n} = (A^{-1})^n = (A^n)^{-1}$$

(из теоремы 4 § 192 следует, что оба эти выражения равны). Для всяких целых $\varkappa$ и $\lambda \neq 0$ имеем:

$$A^{\varkappa}A^{\lambda} = A^{\lambda}A^{\varkappa} = A^{\varkappa+\lambda}. \tag{4}$$

Так как число всех наших элементов конечно, то степени одного элемента A не могут быть все различны: для некоторых целых k и $l > 0$ будем иметь: $A^{k+l} = A^k$ или $A^{k+l-1}A = A^{k-1}A$; а отсюда по постулату II $A^{k+l-1} = A^{k-1}$; дальше точно так же найдем $A^{k+l-2} = A^{k-2}$ и т. д., наконец, $A^{l+1} = A$.

Таким образом первая из повторяющихся степеней есть первая степень A. Пусть m — наименьшее число, большее нуля, для которого $A^{m+1} = A$; это число называется *порядком* элемента A; имеем $A^mA = EA$; а отсюда по постулату II $A^m = E$. Степени $A, A^2, \ldots, A^m$ все различны; дальнейшие же степени суть повторения этих в том же порядке:

$$A^{m+1} = A, \quad A^{m+2} = A^2, \ \ldots$$

Это же периодическое повторение идет и в обратную сторону:

$$A^0 = E = A^m, \quad A^{-1} = A^{m-1}, \quad A^{-2} = A^{m-2}, \ \ldots$$

Вообще $A^{\varkappa} = A^{\lambda}$ тогда и только тогда, если $\varkappa - \lambda$ делится на m, или в обозначениях теории чисел, если $\varkappa = \lambda (\mathrm{mod}\, m)$.

Формула (4) показывает, что все степени элемента A образуют группу; эта группа m-го порядка называется *циклической* группой и обозначается $\{A\}$; как показывает (4), для нее верен и коммутативный закон (который в случае степеней является следствием ассоциативного); такая группа называется *коммутативной* или *абелевой* [по имени норвежского математика Абеля (Abel)].

Если в некоторую группу $\mathfrak{C}$ входит элемент A, то туда входят и все степени A, т. е. и вся циклическая группа $\{A\}$, являющаяся, таким образом, *делителем* или *подгруппой* группы $\mathfrak{C}$.

§ 194. Теорема Лагранжа. Лемма. *Если $\mathfrak{A}$ — группа, а R и S — два любых элемента, то или $\mathfrak{A}R = \mathfrak{A}S$ или комплексы $\mathfrak{A}R$ и $\mathfrak{A}S$ не имеют общих элементов; $\mathfrak{A}R = \mathfrak{A}S$ тогда и только тогда, если $RS^{-1} \subset \mathfrak{A}$.*

Доказательство. Пусть комплексы $\mathfrak{A}R$ и $\mathfrak{A}S$ имеют общий элемент $A_\varkappa R = A_\lambda S$, где $A_\varkappa$ и A_λ некоторые элементы из $\mathfrak{A}$; тогда, умножая равенство $A_\varkappa R = A_\lambda S$ на $\mathfrak{A}$ слева, получим: $\mathfrak{A}R = \mathfrak{A}S$, так как по теореме 1 § 192 $\mathfrak{A}A_\varkappa = \mathfrak{A}A_\lambda = \mathfrak{A}$; умножая обе части полученного равенства справа на S^{-1}, получим $\mathfrak{A}(RS^{-1}) = \mathfrak{A}$; отсюда по теореме 5 § 192 заключаем: $RS^{-1} \subset \mathfrak{A}$. Обратно: пусть $RS^{-1} \subset \mathfrak{A}$, тогда $\mathfrak{A}RS^{-1} = \mathfrak{A}$; умножая справа на S, найдем $\mathfrak{A}R = \mathfrak{A}S$, ибо $S^{-1}S = E$. Этим лемма доказана.

Пусть $\mathfrak{A}$ — группа, а $\mathfrak{B}$ какая-нибудь ее подгруппа. Имеем по следствию 1 теоремы 1 § 192:

$$\mathfrak{A} = \mathfrak{B}\mathfrak{A} = \mathfrak{B}E + \mathfrak{B}A_2 + \ldots + \mathfrak{B}A_n,$$

если $E, A_2, \ldots, A_n$ — все элементы из $\mathfrak{A}$ и n — порядок $\mathfrak{A}$. Но по предыдущей лемме комплексы $\mathfrak{B}E, \mathfrak{B}A_2, \ldots, \mathfrak{B}A_n$ или целиком совпадают друг с другом, или не имеют общих элементов; оставив только различные комплексы и отбросив равные оставленным, мы получим, меняя, в случае необходимости, нумерацию элементов A_i:

$$\mathfrak{A} = \mathfrak{B}E + \mathfrak{B}A_2 + \ldots + \mathfrak{B}A_t; \tag{5}$$

здесь в правой части все элементы различны; в каждом комплексе $\mathfrak{B}E, \mathfrak{B}A_2, \ldots$, $\mathfrak{B}A_t$, по m элементов, если m порядок $\mathfrak{B}$; всего же n элементов; следовательно $n = mt$. Таким образом:

Теорема Лагранжа. *Порядок группы делится на порядок всякой ее подгруппы.*

Число $t = \dfrac{n}{m}$ называется *индексом* подгруппы $\mathfrak{B}$ относительно $\mathfrak{A}$; обозначают: $t = (\mathfrak{A}, \mathfrak{B})$.

Следствие. Порядок группы делится на порядок всякого ее элемента.

Формула (5) представляет так называемое разложение $\mathfrak{A}$ на комплексы по *модулю* $\mathfrak{B}$, взятому слева. Мы могли бы, конечно, взять «модуль» $\mathfrak{B}$ и справа, доказав предварительно аналогичную лемму относительно комплексов $R\mathfrak{A}$ и $S\mathfrak{A}$. Получили бы разложение:

$$\mathfrak{A} = E\mathfrak{B} + A_2'\mathfrak{B} + A_3'\mathfrak{B} + \ldots + A_t'\mathfrak{B}. \tag{6}$$

Конечно, t в обеих формулах (5) и (6) одно и то же; точно так же первый комплекс и в (5) и в (6) есть группа $\mathfrak{B} = \mathfrak{B}E = E\mathfrak{B}$.

Что касается остальных комплексов, то они вообще в (5) и в (6) совершенно различны, — самые элементы из $\mathfrak{A}$ в (6) иначе распределены по комплексам, чем в (5).

§ 195. Пересечение и общее наименьшее кратное групп.

Теорема. *Элементы, общие двум или нескольким группам, образуют группу.*

Доказательство. Если P и Q принадлежат одновременно группам $\mathfrak{A}$ и $\mathfrak{B}$, то и PQ тоже принадлежит и к $\mathfrak{A}$ и к $\mathfrak{B}$, что и доказывает теорему.

Эта группа $\mathfrak{D}$ элементов, общих $\mathfrak{A}$ и $\mathfrak{B}$, называется *общим наибольшим делителем* или *пересечением* групп $\mathfrak{A}$ и $\mathfrak{B}$; мы ее обозначим: $\mathfrak{D} = \mathbf{D}(\mathfrak{A}, \mathfrak{B})$.

Группы, построенные из элементов данной системы, всегда непременно имеют общим главный элемент E; если кроме E данные группы не имеют общих элементов, то они называются *взаимно простыми*.

Теорема. *Если $\mathfrak{A}$ и $\mathfrak{B}$ — группы, то комплекс $\mathfrak{AB}$ тогда и только тогда является группой, если $\mathfrak{AB} = \mathfrak{BA}$.*

Примечание. Из равенства $\mathfrak{AB} = \mathfrak{BA}$, конечно, еще не следует, что каждый элемент из $\mathfrak{A}$ переместим с каждым элементом из $\mathfrak{B}$.

Доказательство. 1) Пусть $\mathfrak{AB} = \mathfrak{BA}$, тогда $(\mathfrak{AB})^2 = (\mathfrak{AB})(\mathfrak{AB}) = \mathfrak{A}(\mathfrak{BA})\mathfrak{B} = (\mathfrak{AA})(\mathfrak{BB}) = \mathfrak{A}^2\mathfrak{B}^2$; но $\mathfrak{A}^2 = \mathfrak{A}$, $\mathfrak{B}^2 = \mathfrak{B}$ (следствие 2 к теореме 1 § 192); следовательно $(\mathfrak{AB})^2 = \mathfrak{AB}$ и $\mathfrak{AB}$ есть группа.

2) Пусть $\mathfrak{AB}$ — группа; очевидно, что $\mathfrak{AB} \supset \mathfrak{A}$ и $\mathfrak{AB} \supset \mathfrak{B}$; следовательно, $\mathfrak{AB} \supset \mathfrak{BU}$. Пусть P — элемент из $\mathfrak{AB}$, тогда и $P^{-1} \subset \mathfrak{AB}$ (по теореме 3 § 192); следовательно $P^{-1} = AB$, где A элемент из $\mathfrak{A}$, B — из $\mathfrak{B}$, но тогда $P = (P^{-1})^{-1} = B^{-1}A^{-1}$; так как $B^{-1} \subset \mathfrak{B}$, $A^{-1} \subset \mathfrak{A}$, то $P = B^{-1}A^{-1} \subset \mathfrak{BA}$, т. е. всякий элемент из $\mathfrak{AB}$ находится также в $\mathfrak{BA}$, т. е. $\mathfrak{AB} \subset \mathfrak{BA}$. Следовательно, $\mathfrak{AB} = \mathfrak{BA}$, и теорема доказана.

Эта группа $\mathfrak{AB}$ (если она существует) называется *общим наименьшим кратным* групп $\mathfrak{A}$ и $\mathfrak{B}$; очевидно, что это наименьшая группа, содержащая $\mathfrak{A}$ и $\mathfrak{B}$, ибо всякая группа, содержащая $\mathfrak{A}$ и $\mathfrak{B}$, содержит также и комплекс $\mathfrak{AB}$ (а так же и $\mathfrak{BA}$). Если $\mathfrak{AB} \neq \mathfrak{BA}$, т. е. $\mathfrak{AB}$ не группа, то мы можем дополнить комплекс $\mathfrak{AB}$ новыми элементами, пока он не превратится в группу; тогда эта группа $\mathfrak{C}$ (которая таким образом $\supset \mathfrak{AB}$ и $\supset \mathfrak{BA}$) будет называться общим наименьшим кратным групп $\mathfrak{A}$ и $\mathfrak{B}$, или группой, *порождаемой* группами $\mathfrak{A}$ и $\mathfrak{B}$; она обозначается: $\mathfrak{C} = \{\mathfrak{A}, \mathfrak{B}\}$; это — наименьшая группа, содержащая $\mathfrak{A}$ и $\mathfrak{B}$. Подобно же определяется общее наименьшее кратное нескольких групп: $\{\mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_\mathfrak{k}\}$; это — наименьшая группа, содержащая $\mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_k$.

§ 196. Структура группы. Представление всякой группы в виде группы подстановок. Пуст $\mathfrak{A}$ -—- данная группа E, A, B, C, ... ее элементы; для того чтобы группа $\mathfrak{A}$ была нам вполне известна, нам необходимо знать, каким элементам (из группы же $\mathfrak{A}$) равняются всевозможные произведения элементов из $\mathfrak{A}$: EA, AB, AC, BC, BA, CA, ... То-есть группа только тогда *определена*, если все эти произведения нам даны. Это выражают, говоря, что нам дана *структура* групп. Обычно все эти произведения помещаются в квадратной таблице, которая строится аналогично пифагоровой таблице умножения; это так называемая *таблица Кэли* данной группы. Пусть, например, нам дана группа четвертого порядка с элементами E, A, B, C и с нижеследующей таблицей Кэли (табл. I). Здесь видно,

что $AB = C = \mathrm{C}$, $B = E$, $BC = A$ и т. п.

	E	A	B	C
E	E	A	B	C
A	A	E	C	B
B	B	C	E	A
C	C	B	A	E

Таблица I

	E	A_1	A_2	A_3	B	C
E	E	A_1	A_2	A_3	B	C
A_1	A_1	E	C	B	A_3	A_2
A_2	A_2	B	E	C	A_1	A_3
A_3	A_3	C	B	E	A_2	A_1
B	B	A_2	A_3	A_1	C	E
C	C	A_3	A_1	A_2	E	B

Таблица II

Таблица Кэли дает нам все, что относится к данной отвлеченной группе; все законы как общие законы действия, так и специальные свойства данной группы можно вывести из таблицы Кэли. Например, из табл. I видно, что для нашей группы четвертого порядка выполнен постулат II, ибо как в каждой строке, так и в каждом столбце таблицы стоят все различные элементы; из того, что таблица симметрична относительно главной диагонали (идущей слева — сверху направо — вниз), следует, что для нашей группы четвертого порядка верен и коммутативный закон; наконец, из таблицы видно, что в группе все элементы, кроме E, второго порядка, ибо $A^2 = B^2 = C^2 = E$. Это так называемая «*четверная*» группа.

Если нам даны конкретные элементы (например подстановки матрицы), действие над которыми производится по определенным правилам, то мы можем построить таблицу Кэли путем фактического выполнения нашего действия над всякими двумя из данных элементов. Например, табл. II представляет структуру симметрической группы 3-й степени, т. е. группы шестого порядка всех подстановок трех символов. Здесь

$$E = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad A_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad A_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$

$$B = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad C = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

Из табл. II видно, что эта группа не коммутативна; она имеет три элемента второго порядка A_1, A_2, A_3 и два элемента третьего порядка B, C; далее, она имеет три подгруппы второго порядка $E + A_1$, $E + A_2$, $E + A_3$ и одну подгруппу третьего порядка $E + B + C$; все эти подгруппы циклические.

Но если нам надо построить *абстрактную* группу, то мы, конечно, не можем написать в таблице Кэли элементы наобум, произвольно: надо построить таблицу так, чтобы основные постулаты действия оказались выполненными для строящейся группы. Труднее всего выполнить ассоциативный закон, который в таблице Кэли отражается весьма сложным образом.

Часто бывает, что мы из разных конкретных источников получаем группы, которые имеют одинаковую структуру; они с отвлеченной точки зрения представляют собой одно и то же, т. е. их таблицы Кэли отличаются друг от друга разве только обозначением элементов: если мы изменим это обозначение подходящим образом, то таблицы Кэли этих групп целиком совпадут друг с другом.

Такие группы называются *изоморфными* (точнее: *просто* или *однозначно изоморфными*) друг другу. Например, мы построили (табл. I) отвлеченно четверную

группу; но эту же таблицу Кэли мы будем иметь для группы таких четырех подстановок:

$$E=\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix},\quad A=\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix},\quad B=\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix},$$
$$C=\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}$$

(предлагается это проверить).

Следовательно, наша абстрактная четверная группа изоморфна группе этих четырех подстановок; она при помощи подстановок представилась в конкретном виде. Этот случай не исключительный; докажем следующее предложение:

Теорема. *Всякая абстрактная группа изоморфна некоторой группе подстановок.*

Доказательство. Пусть $\mathfrak{A}=E+A_2+\ldots+A_n$ данная абстрактная группа n-го порядка; мы имеем (теорема 1 § 192):

$$\mathfrak{A}=\mathfrak{A}A_\varkappa=EA_\varkappa+A_2A_\varkappa+\ldots+A_nA_\varkappa;$$

следовательно, $EA_\varkappa=A_\varkappa$, $A_2A_\varkappa,\ldots,A_nA_\varkappa$ — те же элементы $EA_2,A_2,\ldots,A_n$, только в другом порядке и

$$\overline{A}_\varkappa=\begin{pmatrix}E&A_2&\ldots&A_n\\A_\varkappa&A_2A_\varkappa&\ldots&A_nA_\varkappa\end{pmatrix}$$

есть некоторая подстановка n символов $EA_2,A_2,\ldots,A_n$. Точно так же имеем:

$$\overline{A}_\lambda=\begin{pmatrix}E&A_2&\ldots&A_n\\A_\lambda&A_2A_\lambda&\ldots&A_nA_\lambda\end{pmatrix};$$

но так как в подстановке верхнее расположение произвольно, то мы можем также взять:

$$\overline{A}_\lambda=\begin{pmatrix}A_\varkappa&A_2A_\varkappa&\ldots&A_nA_\varkappa\\A_\varkappa A_\lambda&A_2A_\varkappa A_\lambda&\ldots&A_nA_\varkappa A_\lambda\end{pmatrix};$$

(нижнее произведение мы пишем без скобок, ибо ассоциативный закон позволяет это); далее

$$\overline{A}_\varkappa\overline{A}_\lambda=\begin{pmatrix}E&A_2&\ldots&A_n\\A_\varkappa A_\lambda&A_2A_\varkappa A_\lambda&\ldots&A_nA_\varkappa A_\lambda\end{pmatrix};$$

с другой стороны

$$\overline{A_\varkappa A_\lambda}=\begin{pmatrix}E&A_2&\ldots&A_n\\A_\varkappa A_\lambda&A_2A_\varkappa A_\lambda&\ldots&A_nA_\varkappa A_\lambda\end{pmatrix};$$

следовательно, $\overline{A}_\varkappa\overline{A}_\lambda=\overline{A_\varkappa A_\lambda}$. Это показывает: каждому элементу $A_\varkappa$ нашей абстрактной группы соответствует подстановка $\overline{A}_\varkappa$; все эти подстановки образуют группу $\overline{\mathfrak{A}}$, изоморфную группе $\mathfrak{A}$, ибо подстановка, соответствующая произведению двух элементов, равна произведению подстановок соответствующих элементов.

Указанным способом абстрактная группа n-го порядка представляется как группа подстановок n-й степени (т. е. с n символами); это — далеко не единственный и не самый выгодный в практическом смысле способ представления абстрактный групп в виде групп подстановок, хотя теоретически он самый простой. Это конкретное представление абстрактных групп очень важно: оно показывает, что для того чтобы получить все возможные типы абстрактных групп, нам достаточно рассмотреть все типы групп подстановок, т. е. отвлеченную задачу оно сводит к конкретной.

Абстрактные группы могут быть изоморфными и друг другу, если элементы обеих групп только обозначением отличаются друг от друга. Интерес здесь представляет тот случай, когда две или несколько подгрупп одной и той же группы изоморфны друг другу; эти подгруппы и с абстрактной точки зрения приходится отличать друг от друга. Другой случай, когда одна и та же группа изоморфна самой себе, т. е. когда между ее элементами существует взаимно однозначное соответствие, причем, если A соответствует A_1, B соответствует B_1, то и AB соответствует A_1B_1. Эти изоморфизмы группы самой себе называются *автоморфизмами*, и их теория весьма важна для общей теории групп.

Упражнения

224) Найти все автоморфизмы четвертой группы (табл. I).

Отв. Их шесть; мы их все получим, если будем всевозможными способами переставлять друг с другом элементы A, B, C.

225) Группу шестого порядка, структура которой дана в табл. II, представить как группу подстановок шести символов (по теореме этого параграфа).

§ 197. Сопряженные элементы и группы. Инвариантные подгруппы. Пусть $\mathfrak{C}$ — —данная группа, A и P — два ее элемента. Возьмем элемент $B = P^{-1}AP$; он тоже из $\mathfrak{C}$ и называется элементом, *сопряженным* с A; а операция, посредством которой мы из A получаем B, называется *преобразованием элемента A посредством элемента P*. Сопряженность есть понятие, аналогичное равенству: оно симметрично, рефлективно и транзитивно, именно:

1. Если A сопряжено с B, то и B сопряжено с A; именно из $B = P^{-1}AP$ следует $A = PBP^{-1}$, т. е. A получается из B преобразованием посредством элемента P^{-1}. Следовательно, можно говорить о сопряженных элементах A и B вообще.

2. A сопряжено с A; действительно, $A = E^{-1}AE$, или $A = A^{-1}AA$.

3. Если A сопряжено с B, а B — с C, то и A сопряжено с C; именно: $B = P^{-1}AP$, $C = Q^{-1}BQ$; следовательно, $C = (PQ)^{-1}A(PQ)$.

Из понятия о сопряженных элементах вытекает понятие о сопряженных комплексах: если $\mathfrak{A} = A + B + C\ldots$, то

$$P^{-1}\mathfrak{A}P = P^{-1}AP + P^{-1}BP + P^{-1}CP + \ldots$$

Если один из сопряженных комплексов группа, то и другой тоже является группой. Пусть $\mathfrak{A}$ — группа; тогда в $\mathfrak{A}$ вместе с A и B входит и элемент AB; следовательно, в $P^{-1}\mathfrak{A}P$ входит элемент $P^{-1}ABP = P^{-1}AP \cdot P^{-1}BP$, ибо $P^{-1}P = E$; это показывает, что и $P^{-1}\mathfrak{A}P$ — группа и при этом изоморфная с $\mathfrak{A}$, ибо при

A, соответствующем $A' = P^{-1}AP$, и B, соответствующем $B' = P^{-1}BP$, мы имеем, что AB соответствует $A'B'$; в этом и заключается изоморфизм.

Пусть $\mathfrak{A}$ — подгруппа данной группы $\mathfrak{G} = E + G_2 + G_3 + G_4 + \ldots$; будем преобразовывать $\mathfrak{A}$ всеми элементами из $\mathfrak{G}$; получим подгруппы, сопряженные с $\mathfrak{A}$: $E^{-1}\mathfrak{A}E = \mathfrak{A}$, $G_2^{-1}\mathfrak{A}G_2$, $G_3^{-1}\mathfrak{A}G_3$, ... Может случиться, что эти подгруппы совпадут частью друг с другом, частью с $\mathfrak{A}$; мы выберем из них все различные и получим систему подгрупп, сопряженных с $\mathfrak{A}$. Особенно интересен случай, когда все подгруппы $\mathfrak{A}, G_2^{-1}\mathfrak{A}G_2, \ldots$ совпадут с $\mathfrak{A}$; в этом случае $\mathfrak{a}$ называется *инвариантной подгруппой* или *нормальным делителем* группы $\mathfrak{G}$. Следовательно, инвариантная подгруппа $\mathfrak{A}$ отличается следующим характерным свойством: если G — любой элемент из $\mathfrak{G}$, то $G^{-1}\mathfrak{A}G$, или $\mathfrak{A}G = G\mathfrak{A}$, т. е. подгруппа $\mathfrak{A}$ *переместила со всяким элементом* из $\mathfrak{G}$; обратно, если подгруппа $\mathfrak{A}$ переместима со всяким элементом из $\mathfrak{G}$, то она совпадает со всеми своими сопряженными, т. е. она инвариантна. Из этого, конечно, не следует, что каждый *элемент* из $\mathfrak{A}$ переместим с каждым элементом из $\mathfrak{G}$: если $G \subset \mathfrak{G}$ и $A \subset \mathfrak{A}$, то можно только утверждать, что в $\mathfrak{A}$ имеется такой элемент A', что $AG = GA'$. Это свойство можно принять за третье определение инвариантной подгруппы.

Теорема 1. *Общий наибольший делитель и общее наименьшее кратное всех сопряженных друг другу подгрупп группы $\mathfrak{G}$ являются, инвариантными подгруппами для $\mathfrak{G}$.*

Доказательство. Пусть $\mathfrak{A}, G_1^{-1}\mathfrak{A}G_1, G_2^{-1}\mathfrak{A}G_2, \ldots$ все сопряженные с $\mathfrak{A}$ подгруппы группы $\mathfrak{G}$; $\mathfrak{D}$ — их пересечение, $\mathfrak{C}$ — их общее наименьшее кратное. Если G — любой элемент из $\mathfrak{G}$, то легко видеть, что $G^{-1}\mathfrak{D}G$ и $G^{-1}\mathfrak{C}G$ будут, соответственно, пересечением и общим наименьшим кратным групп: $G^{-1}\mathfrak{A}G$, $(G_1G)^{-1}\mathfrak{A}(G_1G)$, $(G_2G)^{-1}\mathfrak{A}(G_2G)$, ... (это следует из изоморфизма получаемых преобразованием посредством G групп старым); но эти группы как сопряженные с $\mathfrak{A}$ совпадают с группами $\mathfrak{A}, G^{-1}\mathfrak{A}G_1, \ldots$ (разве только стоят в другом порядке); следовательно, и пересечение их, и общее наименьшее кратное не должны измениться: $G^{-1}\mathfrak{D}G = \mathfrak{D}$, $G^{-1}\mathfrak{C}G = \mathfrak{C}$, так как G — любой элемент $\subset \mathfrak{G}$, то следовательно, $\mathfrak{D}$ и $\mathfrak{C}$ инвариантны.

Теорема 2. *Общий наибольший делитель и общее наименьшее кратное инвариантных подгрупп группы $\mathfrak{G}$ суть тоже инвариантные подгруппы группы $\mathfrak{G}$.*

Доказательство. Пусть $\mathfrak{A}, \mathfrak{B}, \ldots$ инвариантные подгруппы группы $\mathfrak{G}$, $\mathfrak{D} = D(\mathfrak{A}, \mathfrak{B}, \ldots)$, $\mathfrak{C} = \{\mathfrak{A}, \mathfrak{B}? \ldots\}$; так как при любом $G \subset \mathfrak{G}$, $G^{-1}\mathfrak{A}G = \mathfrak{A}$, $G^{-1}\mathfrak{B}G = \mathfrak{B}$, ..., то и $G^{-1}\mathfrak{D}G = \mathfrak{D}$, $G^{-1}\mathfrak{C}G = \mathfrak{C}$, что и требовалось доказать.

Очевидно, что всякая подгруппа абелевой группы инвариантна.

Всякая группа $\mathfrak{G}$? является инвариантной подгруппой для самой себя; кроме того, главная группа, состоящая из одного только элемента E, является инвариантной подгруппой для всякой группы. Если кроме этих двух групп $\mathfrak{G}$ совсем не имеет инвариантных подгрупп, то она называется *простой*. Если группа совсем не имеет никаких подгрупп кроме E и самой себя, то она называется *простейшей*. Пусть $\mathfrak{G}$ — простейшая группа и A — один из ее элементов, неравный E; циклическая группа $\{A\}$ всех степеней элемента A является подгруппой для $\mathfrak{G}$; следовательно, должно быть $\mathfrak{G} = \{A\}$, т. е. простейшая группа — непременно циклическая. Пусть n — ее порядок; порядок элемента A тоже n. Если n — составное число, $n = kl$, то элемент A^k-го порядка, и циклическая группа $\{A^k\}$ 1-го порядка является подгруппой для $\mathfrak{G}$, не совпадающей с $\mathfrak{G}$, что противоречит тому, что $\mathfrak{G}$

— простейшая. Итак, $n = p$ — простое число. Обратно: всякая группа простого порядка p непременно простейшая: она кроме E и самой себя не имеет подгрупп и будет непременно циклической.

Простейшая группа, конечно, в то же время и простая; но существуют простые группы, не являющиеся, однако, простейшими; такие группы имеют подгруппы и кроме E и самой себя, только ни одна из этих подгрупп не инвариантна. Этих простых, но не простейших, групп бесчисленное множество, но если мы будем рассматривать все типы групп, начиная с низших порядков, то такие простые группы будут нам попадаться очень редко: наименьшая простая (но не простейшая) группа — это так называемая полусимметрическая группа 5-й степени и 60-го порядка. Очевидно, что абелева группа только тогда простая, если она простейшая.

Упражнение

226) Из подгрупп группы шестого порядка, структура которой дана в табл. II § 196, найти, какие сопряжены друг другу, и есть ли инвариантные.

Отв. $E + B + C$ инвариантна; $E + A_1$, $E + A_2$, $E + A_3$ сопряжены друг другу.

§ 198. Дополнительные группы. Если $\mathfrak{B}$ — инвариантная подгруппа для $\mathfrak{A}$, и мы разложим $\mathfrak{A}$ по модулю $\mathfrak{B}$ слева и справа [(5) и (6) § 194], то оба эти разложения здесь, очевидно, совпадут, ибо $\mathfrak{B}A_2 = A_2\mathfrak{B}$, …, $\mathfrak{B}A_t = A_t\mathfrak{B}$, так что из одного разложения непосредственно следует другое. Рассмотрим комплексы: $\mathfrak{B}E = \mathfrak{B}$, $\mathfrak{B}A_2$, …, $\mathfrak{B}A_t$; докажем, что для их произведений верны все основные четыре постулата § 191.

I. $\mathfrak{B}A_\varkappa \cdot \mathfrak{B}A_\lambda = \mathfrak{B}\mathfrak{B}A_\varkappa A_\lambda = \mathfrak{B}(A_\varkappa A_\lambda) = \mathfrak{B}A_\mu$, ибо $\mathfrak{B}$ переместимо со всяким $A_\varkappa$; $\mathfrak{B}\mathfrak{B} = \mathfrak{B}$ и $\mathfrak{B}A_\varkappa A_\lambda$ есть один из тех же комплексов $\mathfrak{B}A_\mu$.

II. Пусть $\mathfrak{B}A_\varkappa \cdot \mathfrak{B}A_\lambda = \mathfrak{B}_\varkappa \cdot \mathfrak{B}A_\mu$; отсюда $A_\varkappa\mathfrak{B}\mathfrak{B}A_\lambda = A_\varkappa\mathfrak{B}\mathfrak{B}A_\mu$, или $A_\varkappa(\mathfrak{B}A_\lambda) = A_\varkappa(\mathfrak{B}A_\mu)$; а это как раз тот случай (§ 191), когда для произведения комплексов верен постулат II; заключаем: $\mathfrak{B}A_\lambda = \mathfrak{B}A_\mu$.

Пусть теперь $\mathfrak{B}A_\lambda \cdot \mathfrak{B}A_\varkappa = \mathfrak{B}A_\mu \cdot \mathfrak{B}A_\varkappa$; отсюда $(\mathfrak{B}A_\lambda)A_\varkappa = (\mathfrak{B}A_\mu)A_\varkappa$; мы опять имеем тот же случай и опять заключаем, что $\mathfrak{B}A_\lambda = \mathfrak{B}A_\mu$.

III. Ассоциативный закон верен вообще для комплексов.

IV. Число наших комплексов, равное t, конечно.

Отсюда следует, что если эти комплексы $\mathfrak{B}A_\varkappa$ рассматривать как отдельные новые элементы, так сказать «высшего порядка», то они образуют группу; эта группа обозначается $\mathfrak{A}/\mathfrak{B}$ или $\dfrac{\mathfrak{A}}{\mathfrak{B}}$ и называется *дополнительной* к $\mathfrak{B}$ группой; ее порядок есть $t = \mathfrak{A}, \mathfrak{B}$ (и, значит равен индексу группы $\mathfrak{B}$ относительно $\mathfrak{A}$); роль главного элемента в ней играет $\mathfrak{B}$, ибо $\mathfrak{B}^2 = \mathfrak{B}$.

У абелевых групп всякая подгруппа инвариантна, а потому там для всякой подгруппы существует дополнительная группа, которая, очевидно, тоже абелева.

Теорема 1. *Если $\mathfrak{B}$ и $\mathfrak{C}$ — инвариантные подгруппы для $\mathfrak{A}$, причем $\mathfrak{B} \supset \mathfrak{C}$, то и $\dfrac{\mathfrak{B}}{\mathfrak{C}}$ инвариантная подгруппа для $\dfrac{\mathfrak{A}}{\mathfrak{C}}$ и индексы*

$$(\mathfrak{A}, \mathfrak{B}) = \left(\frac{\mathfrak{A}}{\mathfrak{C}}, \frac{\mathfrak{B}}{\mathfrak{C}}\right).$$

Доказательство. Очевидно, что $\mathfrak{C}$ будучи инвариантной подгруппой для $\mathfrak{A}$, будет также инвариантной подгруппой для $\mathfrak{B}$, т. е. дополнительная группа $\frac{\mathfrak{B}}{\mathfrak{C}}$ существует. Разложим $\mathfrak{A}$ и $\mathfrak{B}$ по модулю $\mathfrak{C}$ (здесь — все равно, справа или слева):

$$\mathfrak{A} = \mathfrak{C}P + \mathfrak{C}P' + \mathfrak{C}P'' + \mathfrak{C}P''' + \ldots; \quad \mathfrak{B} = \mathfrak{C}Q + \mathfrak{C}Q' + \mathfrak{C}Q'' + \ldots;$$

$Q, Q', Q'', \ldots$ некоторые элементы из $\mathfrak{B}$, а следовательно, и из $\mathfrak{A}$, так как $\mathfrak{B} \subset \mathfrak{A}$; следовательно, комплексы $\mathfrak{C}Q$, $\mathfrak{C}Q'$, $\mathfrak{C}Q''$, ... все встречаются среди комплексов $\mathfrak{C}P$, $\mathfrak{C}P'$, $\mathfrak{C}P''$, ...; но комплексы $\mathfrak{C}Q$, $\mathfrak{C}Q'$, $\mathfrak{C}Q''$, ... являются элементами группы $\frac{\mathfrak{B}}{\mathfrak{C}}$, а $\mathfrak{C}P$, $\mathfrak{C}P'$, $\mathfrak{C}P''$, ... — элементы группы $\frac{\mathfrak{A}}{\mathfrak{C}}$; следовательно, $\frac{\mathfrak{B}}{\mathfrak{C}} \subset \frac{\mathfrak{B}}{\mathfrak{C}}$. Пусть P — элемент из $\mathfrak{A}$, Q — элемент из $\mathfrak{B}$; так как $\mathfrak{B}$ — инвариантная подгруппа для $\mathfrak{A}$, то (§ 197, 3-е определение инвариантной подгруппы) в $\mathfrak{B}$ имеется такой элемент Q', что $QP = PQ'$; но тогда $\mathfrak{C}QP = \mathfrak{C}PQ'$, что можно представить в таком виде: $\mathfrak{C}Q \cdot \mathfrak{C}P = \mathfrak{C}P = \cdot\mathfrak{C}\mathfrak{Q}'$; так как $\mathfrak{C}P$ любой элемент из $\frac{\mathfrak{A}}{\mathfrak{C}}$, $\mathfrak{C}Q$ — любой элемент из $\frac{\mathfrak{B}}{\mathfrak{C}}$, а $\mathfrak{C}Q'$ тоже элемент из $\frac{\mathfrak{B}}{\mathfrak{C}}$, то отсюда (по тому же третьему определению) следует, что $\frac{\mathfrak{B}}{\mathfrak{C}}$ инвариантпая подгруппа для $\frac{\mathfrak{A}}{\mathfrak{C}}$.

Пусть n — порядок $\mathfrak{A}$, h — порядок $\mathfrak{B}$, k — порядок $\mathfrak{C}$; тогда порядок $\frac{\mathfrak{A}}{\mathfrak{C}} = (\mathfrak{A}\mathfrak{C} = \frac{n}{k}$, порядок $\frac{\mathfrak{B}}{\mathfrak{C}} = (\mathfrak{B}, \mathfrak{C}) = \frac{h}{k}$, $\left(\frac{\mathfrak{A}}{\mathfrak{C}}, \frac{\mathfrak{B}}{\mathfrak{C}}\right) = \frac{n}{k} : \frac{h}{k} = \frac{n}{h} = (\mathfrak{A}, \mathfrak{B})$, и наша теорема доказана.

Теорема 2. (обратная к теореме 1). *Если $\mathfrak{C}$ инвариантная подгруппа для $\mathfrak{A}$ и $\frac{\mathfrak{A}}{\mathfrak{C}}$ имеет подгруппу $\mathfrak{M}$, то $\mathfrak{A}$ имеет подгруппу $\mathfrak{B}$, содержащую в свою очередь подгруппу $\mathfrak{C}$, причем $\frac{\mathfrak{B}}{\mathfrak{C}} = \mathfrak{M}$. Если $\mathfrak{M}$ инвариантная подгруппа для $\frac{\mathfrak{A}}{\mathfrak{C}}$, то $\mathfrak{B}$ — инвариантная подгруппа для $\mathfrak{A}$. Порядок $\mathfrak{B}$ равен произведению порядков $\mathfrak{M}$ и $\mathfrak{C}$.*

Доказательство. Пусть, как и раньше, $\mathfrak{A} = \mathfrak{C}P + \mathfrak{C}P' + \mathfrak{C}P'' + \ldots$; комплексы $\mathfrak{C}P, \mathfrak{C}P'?, \ldots$ являются элементами группы $\frac{\mathfrak{A}}{\mathfrak{C}}$; рассматривая их как элементы, мы будем заключать их в скобки: $\frac{\mathfrak{A}}{\mathfrak{C}} = (\mathfrak{C}P) + (\mathfrak{C}P') + (\mathfrak{C}P'') + \ldots$ Часть их составляет группу $\mathfrak{M}$; пусть $\mathfrak{M} = (\mathfrak{C}Q) + (\mathfrak{C}Q') + (\mathfrak{C}Q'') + \ldots$, где все эти сложные элементы $(\mathfrak{C}Q), (\mathfrak{C}Q'), \ldots$ встречаются среди элементов $(\mathfrak{C}P), (\mathfrak{C}P'), \ldots$ Рассматривая теперь $\mathfrak{C}Q, \mathfrak{C}Q', \ldots$ снова как комплексы первоначальных элементов, обозначим:

$$\mathfrak{B} = \mathfrak{C}Q + \mathfrak{C}Q' + \mathfrak{C}Q'' + \ldots \tag{7}$$

Докажем, что комплекс $\mathfrak{B}$, есть группа первоначальных элементов. Возьмем два элемента из B: CQ и $C'Q'$; где C и C' — элементы из $\mathfrak{C}$; имеем $QC' = C''Q$, где C'' тоже элемент из $\mathfrak{C}$, ибо $\mathfrak{C}$ — инвариантная подгруппа для $\mathfrak{A}$. Следовательно, $CQ \cdot C'Q' = CC''QQ' = C'''QQ'$, где C''' тоже $\subset \mathfrak{C}$, но $C'''QQ'$ содержится в комплексе $\mathfrak{C}QQ' = \mathfrak{C}Q \cdot \mathfrak{C}Q'$, который входит в $\mathfrak{B}$, ибо элемент $(\mathfrak{C}Q) \cdot (\mathfrak{C}Q')$ входит в группу $\mathfrak{M}$. Следовательно, $CQ \cdot C'Q' \subset \mathfrak{B}$, что и доказывает, что B — группа. Если m порядок $\mathfrak{M}$, k порядок $\mathfrak{C}$, h порядок $\mathfrak{B}$, то из (7) очевидно, что $h = mk$. Очевидно, также, что $\frac{\mathfrak{B}}{\mathfrak{C}} = \mathfrak{M}$.

Пусть теперь $\mathfrak{M}$ — инвариантная подгруппа для $\frac{\mathfrak{A}}{\mathfrak{C}}$; тогда при данных $(\mathfrak{C}P)$ из $\frac{\mathfrak{A}}{\mathfrak{C}}$ и $(\mathfrak{C}Q)$ из $\mathfrak{M}$ можно найти в $\mathfrak{M}$ элемент $(\mathfrak{C}Q')$ так, чтобы было $(\mathfrak{C}Q)(\mathfrak{C}P) = (\mathfrak{C}P)(\mathfrak{C}Q')$; или (рассматривая $\mathfrak{C}P$, ..., снова как комплексы)

$$\mathfrak{C}Q\mathfrak{C}P = \mathfrak{C}P\mathfrak{C}Q',$$

или, так как $\mathfrak{C}$ (как инвариантная подгруппа) переместима и с Q' и с P:

$$QP\mathfrak{C} = PQ'\mathfrak{C};$$

в левой части этого равенства имеется элемент $QPE = QP$; следовательно, и в правой части имеется равный ему элемент $QP = PQ'C$, где C — некоторый элемент из $\mathfrak{C}$; но $Q'C = Q''$ есть элемент из $\mathfrak{B}$, ибо $Q' \subset \mathfrak{B}$ и $\mathfrak{C} \subset \mathfrak{B}$; итак,

$$QP = PQ'';$$

отсюда (§ 197, 3-е определение инвариантной подгруппы) следует, что $\mathfrak{B}$ — инвариантная подгруппа для $\mathfrak{A}$, и теорема 2 доказана полностью.

Определение. Инвариантная подгруппа $\mathfrak{C}$ группы $\mathfrak{A}$ называется *максимальной*, если $\mathfrak{A}$ не имеет инвариантной подгруппы $\mathfrak{B}$, которая в свою очередь содержала бы $\mathfrak{C}$.

Заметим, что максимальных инвариантных подгрупп у данной группы A может быть и несколько, и они могут быть различных порядков.

Следствие из теорем 1 и 2. Инвариантная подгруппа $\mathfrak{C}$ группы $\mathfrak{A}$ тогда и только тогда максимальна, если группа $\frac{\mathfrak{A}}{\mathfrak{C}}$ простая.

Замечание. Если $\mathfrak{B}$ и $\mathfrak{C}$ — две инвариантные подгруппы для $\mathfrak{A}$, то $\mathfrak{B}\mathfrak{C}$ всегда группа (ибо $\mathfrak{B}\mathfrak{C} = \mathfrak{C}\mathfrak{B}$) и притом тоже инвариантная подгруппа для $\mathfrak{A}$ (как общее наименьшее кратное групп $\mathfrak{B}$, $\mathfrak{C}$); если хоть одна из групп $\mathfrak{B}$, $\mathfrak{C}$ — максимальная инвариантная подгруппа для $\mathfrak{A}$, то $\mathfrak{B}\mathfrak{C} = \mathfrak{A}$ (иначе было бы $\mathfrak{A} \supset \mathfrak{B}\mathfrak{C} \supset \mathfrak{B}$, т. е. $\mathfrak{A}$ заключала бы инвариантную подгруппу $\mathfrak{B}\mathfrak{C}$, содержащую $\mathfrak{B}$ и $\mathfrak{C}$).

Теорема 3. *Если $\mathfrak{B}$, $\mathfrak{C}$ две максимальные инвариантные подгруппы группы $\mathfrak{A}$, $\mathfrak{D} = \mathbf{D}(\mathfrak{B}, \mathfrak{C})$, то $\mathfrak{D}$ — максимальная инвариантная подгруппа и для $\mathfrak{B}$ и для $\mathfrak{C}$, причем группа $\frac{\mathfrak{A}}{\mathfrak{B}}$ изоморфна $\frac{\mathfrak{C}}{\mathfrak{D}}$, $\frac{\mathfrak{A}}{\mathfrak{C}}$ изоморфна $\frac{\mathfrak{B}}{\mathfrak{D}}$.*

Доказательство. По теореме 2 § 197 $\mathfrak{D}$ — инвариантная подгруппа для $\mathfrak{A}$, а следовательно, и для $\mathfrak{B}$ и для $\mathfrak{C}$, т. е. $\frac{\mathfrak{B}}{\mathfrak{D}}$ и $\frac{\mathfrak{C}}{\mathfrak{D}}$ существуют. Разложим $\mathfrak{C}$ по модулю $\mathfrak{D}$:

$$\mathfrak{C} = \mathfrak{D} + \mathfrak{D}C' + \mathfrak{D}C'' + \ldots \tag{8}$$

Комплексы $\mathfrak{D}$, $\mathfrak{D}C'$, $\mathfrak{D}C''$, ... все различны. Умножив (8) на $\mathfrak{B}$ слева, найдем $\mathfrak{B}\mathfrak{C} = \mathfrak{B}\mathfrak{D} + \mathfrak{B}\mathfrak{D}C' + \mathfrak{B}\mathfrak{D}C'' + \ldots$; но $\mathfrak{B}\mathfrak{C} = \mathfrak{A}$ (см. предыдущее замечание), $\mathfrak{B}\mathfrak{D} = \mathfrak{B}$, ибо $\mathfrak{D} \subset \mathfrak{B}$, следовательно:

$$\mathfrak{A} = \mathfrak{B} + \mathfrak{B}C' + \mathfrak{B}C'' + \ldots; \tag{9}$$

докажем, что комплексы $\mathfrak{B}$, $\mathfrak{B}C'$, $\mathfrak{B}C''$, ... тоже все различны. Пусть $\mathfrak{B}C' = \mathfrak{B}C''$; следовательно (по лемме § 194), $C'C''^{-1} \subset \mathfrak{B}$; но ведь C' и C'' находятся в $\mathfrak{C}$;

следовательно $C'C''^{-1} \supset \mathfrak{C}$; будучи и в $\mathfrak{B}$ и в $\mathfrak{C}$, элемент $C'C''^{-1}$ находится и в $\mathfrak{D}$: $C'C''^{-1} \subset \mathfrak{D}$; тогда (по той же лемме § 194) $\mathfrak{D}C' = \mathfrak{D}C''$, а это неверно, ибо в (8) все комплексы различны. Следовательно, и в (9) все комплексы должны быть различны, и (9) представляет собою разложение $\mathfrak{A}$ по модулю $\mathfrak{B}$. Между комплексами (8) и (9) имеется взаимно однозначное соответствие: $\mathfrak{B}$ соответствует $\mathfrak{D}$, $\mathfrak{B}C'$ соответствует $\mathfrak{D}C'$ и т. д.; причем, если $\mathfrak{B}C'$ соответствует $\mathfrak{D}C'$, $\mathfrak{B}C''$ соответствует $\mathfrak{D}C''$, то и $\mathfrak{B}C' \cdot \mathfrak{B}C'' = \mathfrak{B}C'C''$ соответствует $\mathfrak{D}C' \cdot \mathfrak{D}C'' = \mathfrak{D}C'C''$, т. е. это соответствие дает изоморфизм групп $\frac{\mathfrak{A}}{\mathfrak{B}}$ и $\frac{\mathfrak{C}}{\mathfrak{D}}$. Совершенно так же докажем, что и $\frac{\mathfrak{A}}{\mathfrak{C}}$ и $\frac{\mathfrak{B}}{\mathfrak{D}}$ изоморфны. Но $\frac{\mathfrak{A}}{\mathfrak{B}}$ и $\frac{\mathfrak{A}}{\mathfrak{C}}$ простые группы (ибо $\mathfrak{B}$ и $\mathfrak{C}$ максимальные инвариантные подгруппы); следовательно, и изоморфные им группы $\frac{\mathfrak{C}}{\mathfrak{D}}$ и $\frac{\mathfrak{B}}{\mathfrak{D}}$ — простые; следовательно, $\mathfrak{D}$ — максимальная инвариантная подгруппа для $\mathfrak{C}$ и для $\mathfrak{B}$, и теорема 3 доказана.

§ 199. Композиционный ряд. Теорема Жордана – Гельдера. Пусть $\mathfrak{G}$ — данная группа, $\mathfrak{G}_1$ — какая-нибудь ее максимальная инвариантная подгруппа, $\mathfrak{G}_2$ — максимальная инвариантная подгруппа для $\mathfrak{G}_1$, $\mathfrak{G}_3$ — тоже для $\mathfrak{G}_2$ и т. д. Так как порядки групп $\mathfrak{G}$, $\mathfrak{G}_1$, $\mathfrak{G}_2$, $\mathfrak{G}_3$, ... убывают, то этот ряд должен окончиться главной группой E; пусть $\mathfrak{G}_n = E$. Такой ряд

$$\mathfrak{G}, \quad \mathfrak{G}_1, \quad \mathfrak{G}_2, \ \ldots, \ \mathfrak{G}_{n-1}, \quad \mathfrak{G}_n = E$$

называется *композиционным рядом* для группы $\mathfrak{G}$. Все дополнительные группы $\frac{\mathfrak{G}}{\mathfrak{G}_1}$, $\frac{\mathfrak{G}_1}{\mathfrak{G}_2}$, ..., $\frac{\mathfrak{G}_{n-1}}{\mathfrak{E}} = \mathfrak{G}_{n-1}$ — простые. Если данная группа $\mathfrak{G}$ простая, то единственная ее максимальная инвариантная подгруппа есть E и единственный ее композиционный ряд есть $\mathfrak{G}$, E. Если же группа $\mathfrak{G}$ не простая («составная»), то она вообще может иметь несколько совершенно различных композиционных рядов.

Теорема Жордана – Гельдера (Jordan, Hölder). *Если* $\mathfrak{G}$, $\mathfrak{G}_1$, ..., $\mathfrak{G}_n = E$ *и* $\mathfrak{G}$, $\mathfrak{H}_1$, $\mathfrak{H}_2$, ..., $\mathfrak{H}_m = E$ *два композиционных ряда группы* $\mathfrak{G}$, *то всегда* $n = m$, *и если не считать различными изоморфные друг другу, группы, то ряды дополнительных групп*

$$\frac{\mathfrak{G}}{\mathfrak{G}_1}, \quad \frac{\mathfrak{G}_1}{\mathfrak{G}_2}, \ \ldots, \mathfrak{G}_{n-1} \quad \text{и} \quad \frac{\mathfrak{G}}{\mathfrak{H}_1}, \quad \frac{\mathfrak{H}_1}{\mathfrak{H}_2}, \ldots, \mathfrak{H}_{n-1}$$

совпадают с точностью до порядка, т. е. каждая группа одного ряда изоморфна некоторой группе другого ряда, и обратно, и если в одном ряду имеется несколько изоморфных друг другу групп, то и в другом ряду имеется столько же групп, изоморфных первым; в частности и ряды индексов $(\mathfrak{G}, \mathfrak{G}_1)$, $(\mathfrak{G}_1, \mathfrak{G}_2)$, ..., $(\mathfrak{G}_{n-1}, \mathfrak{G}_n)$ *и* $(\mathfrak{G}, \mathfrak{H}_1)$, $(\mathfrak{H}_1, \mathfrak{H}_2)$, ..., $(\mathfrak{H}_{n-1}, \mathfrak{H}_n)$ *состоят из одних и тех же чисел, только может быть расположенных в разных порядках.*

Для рядов индексов эту теорему доказал Жордан; Гельдер обобщил ее и высказал в том виде, как мы ее приводим.

Доказательство. Для простых групп теорема тривиальна, ибо всякая простая группа только и имеет один композиционный ряд. Группы низших порядков (второго и третьего) простейшие, следовательно, и простые. Поэтому мы можем

применить метод полной индукции, приняв, что теорема верна для групп, порядки которых меньше порядка $\mathfrak{G}$.

Имеем $\mathfrak{G}_1\mathfrak{H}_1 = \mathfrak{H}_1\mathfrak{G}_1 = \mathfrak{G}$; пусть $\mathfrak{D} = \mathbf{D}(\mathfrak{G}_1, \mathfrak{H}_1)$; тогда по теореме 3 § 198 $\mathfrak{D}$ — максимальная инвариантная подгруппа и для $\mathfrak{G}_1$ и для $\mathfrak{H}_1$.

Пусть $\mathfrak{D}, \mathfrak{D}_1, \mathfrak{D}_2, \ldots, E$ — какой-нибудь композиционный ряд для $\mathfrak{D}$; тогда $\mathfrak{G}_1$, $\mathfrak{D}, \mathfrak{D}_1, \mathfrak{D}_2, \ldots, E$ и $\mathfrak{H}_1, \mathfrak{D}, \mathfrak{D}_1, \mathfrak{D}_2, \ldots, E$ — композиционные ряды для $\mathfrak{H}_1$ и $\mathfrak{G}_1$. Но так как $\mathfrak{G}_1$ и $\mathfrak{H}_1$ порядков низших, чем порядок $\mathfrak{G}$, то для них наша теорема предполагается верной. Так, например, для $\mathfrak{G}_1$, имеем два композиционных ряда:

$$\mathfrak{G}_1,\ \ \mathfrak{D},\ \ \mathfrak{D}_1,\ \ldots,\ E \quad \text{и} \quad \mathfrak{G}_1,\ \ \mathfrak{G}_2,\ \ \mathfrak{G}_3,\ \ldots, E; \tag{10}$$

отсюда заключаем, что число членов в них одинаково и что ряды дополнительных групп $\dfrac{\mathfrak{G}_1}{\mathfrak{D}}, \dfrac{\mathfrak{D}}{\mathfrak{D}_1}, \ldots$ и $\dfrac{\mathfrak{G}_1}{\mathfrak{G}_2}, \dfrac{\mathfrak{G}_2}{\mathfrak{G}_3}, \ldots$ отличаются друг от друга разве только порядком своих членов. Также и для $\mathfrak{H}_1$ имеем два композиционных ряда:

$$\mathfrak{H}_1,\ \ \mathfrak{D},\ \ \mathfrak{D}_1,\ \ldots,\ E \quad \text{и} \quad \mathfrak{H}_1,\ \ \mathfrak{H}_2,\ \ \mathfrak{H}_3,\ \ldots,\ E, \tag{11}$$

и заключаем то же самое. Отсюда уже следует, что число членов во вторых рядах (10) и (11) одинаково, а следовательно, и в данных рядах для $\mathfrak{G}$ число членов одинаково, т. е. $m = n$. Имеем теперь четыре ряда дополнительных групп для $\mathfrak{G}$:

$$\frac{\mathfrak{G}}{\mathfrak{G}_1},\quad \frac{\mathfrak{G}_1}{\mathfrak{G}_2},\quad \frac{\mathfrak{G}_2}{\mathfrak{G}_3},\ \ldots; \tag{12}$$

$$\frac{\mathfrak{G}}{\mathfrak{G}_1},\quad \frac{\mathfrak{G}_1}{\mathfrak{D}},\quad \frac{\mathfrak{D}}{\mathfrak{D}_1},\ \ldots; \tag{13}$$

$$\frac{\mathfrak{G}}{\mathfrak{H}_1},\quad \frac{\mathfrak{H}_1}{\mathfrak{D}},\quad \frac{\mathfrak{D}}{\mathfrak{D}_1},\ \ldots; \tag{14}$$

$$\frac{\mathfrak{G}}{\mathfrak{H}_1},\quad \frac{\mathfrak{H}_1}{\mathfrak{H}_2},\quad \frac{\mathfrak{H}_2}{\mathfrak{H}_3},\ \ldots; \tag{15}$$

Ряды (12) и (13), начиная со второго члена, как было уже выяснено, отличаются друг от друга только порядком членов; первые же члены у этих рядов одинаковы; то же самое верно и для рядов (14) и (15). Что касается (13) и (14), то эти ряды, начиная с третьего члена, вообще тождественны друг другу, и кроме того (по теореме 3 § 198), первый член (13) изоморфен второму члену (14), а второй член (13) изоморфен первому члену (14). Отсюда следует, что и ряды (12) и (15) отличаются друг от друга разве только порядком своих членов. Следовательно, для $\mathfrak{G}$ теорема Жордан – Гельдера доказана. Как простое следствие вытекает отсюда равенство рядов индексов.

Особенно интересен случай, когда для данной группы $\mathfrak{G}$ ряд индексов композиционного ряда состоит только из простых чисел; следовательно, все дополнительные группы (12) не только простые, но и простейшие. Такая группа $\mathfrak{G}$ называется *разрешимой* (по Фробениусу и Гельдеру) или *метациклической* (по Веберу). Например, абелева группа всегда разрешима.

§ 200. Гомоморфизм. Рассмотрим соотношение между данной группой $\mathfrak{G}$ и ее дополнительной группой $\dfrac{\mathfrak{G}}{\mathfrak{A}}$, где $\mathfrak{A}$ — какая-нибудь инвариантная подгруппа

для $\mathfrak{G}$. Пусть n — порядок $\mathfrak{G}$, m — порядок $\mathfrak{A}$, тогда порядок $\frac{\mathfrak{G}}{\mathfrak{A}}$ есть:

$$t = (\mathfrak{G}, \mathfrak{A}) = \frac{n}{m}.$$

Всякому элементу G из $\mathfrak{G}$ соответствует один определенный элемент из $\frac{\mathfrak{G}}{\mathfrak{A}}$, именно, комплекс $\mathfrak{A}G$, куда входит этот элемент G. При этом, если

	элементу	G	соответствует	$\mathfrak{A}G$,
	$''$	G'	$''$	$\mathfrak{A}G'$, , .
то	$''$	GG'	$''$	$\mathfrak{A}AA'$.

Но $\mathfrak{A}GG' = \mathfrak{A}^2GG' = \mathfrak{A}G \cdot \mathfrak{A}G'$. Следовательно, произведению элементов из $\mathfrak{G}$ соответствует произведение соответствующих элементов из $\frac{\mathfrak{G}}{\mathfrak{A}}$. Таким образом между группами $\mathfrak{G}$ и $\frac{\mathfrak{G}}{\mathfrak{A}}$ существует соответствие, похожее на изоморфизм, но отличающееся от последнего тем, что в то время как каждому элементу из $\mathfrak{G}$ соответствует только один элемент из $\frac{\mathfrak{G}}{\mathfrak{A}}$, — каждому элементу $\mathfrak{A}G$ из $\frac{\mathfrak{G}}{\mathfrak{A}}$ соответствует несколько элементов из $\mathfrak{G}$, — именно, все элементы комплекса $\mathfrak{A}G$; число их равно порядку группы $\mathfrak{A}$. Такое соответствие называется *гомоморфизмом* или *многозначным* (или *кратным*) изоморфизмом, — в отличие от ранее определенного (однозначного или простого) изоморфизма. Говорят, что группа $\mathfrak{G}$ *гомоморфна* группе $\frac{\mathfrak{G}}{\mathfrak{A}}$ (но не наоборот).

Вообще, *группа* $\mathfrak{A}$ *гомоморфна группе* $\mathfrak{B}$, если каждому элементу группы $\mathfrak{A}$ соответствует один и только один элемент группы $\mathfrak{B}$ (но не наоборот), причем если элементу A из $\mathfrak{A}$ соответствует элемент B из $\mathfrak{B}$, а элементу A_1 из $\mathfrak{A}$ — элемент B_1 из $\mathfrak{B}$, то элементу AA_1 соответствует BB_1.

Если группа $\mathfrak{A}$ гомоморфна группе $\mathfrak{B}$, а группа $\mathfrak{B}$ в свою очередь гомоморфна группе $\mathfrak{C}$, то и группа A гомоморфна группе $\mathfrak{C}$, т. е. для гомоморфизма верен закон транзитивности.

Теорема. *Если группа* $\mathfrak{A}$ *гомоморфна группе* $\mathfrak{B}$, *то в* $\mathfrak{A}$ *имеется такая инвариантная подгруппа* $\mathfrak{N}$, *что дополнительная группа* $\frac{\mathfrak{A}}{\mathfrak{N}}$ *просто изоморфна* $\mathfrak{B}$.

Доказательство. Пусть единице E' из $\mathfrak{B}$ соответствуют элементы P и Q из $\mathfrak{A}$; тогда по определению гомоморфизма элементу PQ из $\mathfrak{A}$ соответствует элемент $E'E' = E'$ из $\mathfrak{B}$. Это показывает, что все элементы из $\mathfrak{A}$, соответствующие единице из $\mathfrak{B}$, составляют, группу (а следовательно, между ними есть и единица из $\mathfrak{A}$); обозначим эту группу через $\mathfrak{N}$ и докажем, что она — инвариантная подгруппа для $\mathfrak{A}$. Заметим предварительно, что если элемент $A \subset \mathfrak{A}$ соответствует элементу $B \subset \mathfrak{B}$, то A^{-1} соответствует B^{-1}, действительно, если A^{-1} соответствует B'; то $AA^{-1} = E$ соответствует BB'; но единице E из $\mathfrak{A}$ соответствует только один элемент из $\mathfrak{B}$, именно единица E'; следовательно, $BB' = E'$; т. е. $B' = B^{-1}$.

Пусть теперь N — любой элемент из $\mathfrak{N}$, а A — любой элемент из $\mathfrak{A}$, причем A соответствует $B \subset \mathfrak{B}$; тогда элементу $A^{-1}NA$ соответствует $B^{-1}E'B = E'$; т. е. $A^{-1}NA = N_1 \subset \mathfrak{N}$, или $NA = A_1N$, а это и означает, что $\mathfrak{N}$ инвариантная подгруппа для $\mathfrak{A}$ (см. § 197, третье определение инвариантной подгруппы). Пусть

$$\mathfrak{A} = \mathfrak{N} + \mathfrak{N}A + \mathfrak{N}A' + \ldots$$

есть разложение группы $\mathfrak{A}$ по модулю $\mathfrak{N}$. Если элементу A соответствует элемент B из $\mathfrak{B}$, то каждому элементу NA из комплекса $\mathfrak{N}A$ соответствует один и тот же элемент $E'B = B$ из $\mathfrak{B}$. Обратно, если элементу $A_1 \subset \mathfrak{A}$ соответствует тоже элемент $B \subset \mathfrak{B}$, то элементу A_1A^{-1} соответствует $BB^{-1} = E'$; значит $A_1A^{-1} = N \subset \mathfrak{N}$, а следовательно, $A_1 = NA \subset \mathfrak{N}A$. То есть каждому элементу B из $\mathfrak{B}$ соответствуют все элементы некоторого комплекса $\mathfrak{N}A$, и только они. Таким образом между комплексами $\mathfrak{N}$, $\mathfrak{N}A$, $\mathfrak{N}A'$, ..., т. е. между элементами группы $\frac{\mathfrak{A}}{\mathfrak{N}}$, с одной стороны, и между элементами группы $\mathfrak{B}$, с другой стороны существует взаимно однозначное соответствие, причем если $\mathfrak{N}A$ соответствует B, а $\mathfrak{N}A'$ соответствует B'; то $\mathfrak{N}AA' = \mathfrak{N}A \cdot \mathfrak{N}A'$ соответствует BB'; т. е. это соответствие есть простой изоморфизм, и теорема доказана.

§ 201. В § 196 мы видели, что всякая абстрактная группа изоморфна некоторой группе подстановок. Обобщим теперь примененное при доказательстве этой теоремы построение. Пусть $\mathfrak{G}$ данная группа, $\mathfrak{H}$ — ее подгруппа и

$$G = \mathfrak{H} + \mathfrak{H}A_2 + \ldots + \mathfrak{H}A_k \tag{16}$$

разложение группы $\mathfrak{G}$ по модулю $\mathfrak{H}$, взятому слева. Пусть A_λ какой-нибудь элемент из $\mathfrak{G}$; тогда $\mathfrak{G}A_\lambda = \mathfrak{G}$ (см. § 192, теорему 1); но, с другой стороны:

$$\mathfrak{G} = \mathfrak{G}A_\lambda = \mathfrak{H}A_\lambda + \mathfrak{H}(A_2A_\lambda) + \ldots + \mathfrak{H}(A_kA_\lambda); \tag{16}$$

тут все комплексы правой части различны, ибо из

$$\mathfrak{H}A_\varkappa A_\lambda = \mathfrak{H}A_\mu A_\lambda$$

умножением справа на A_λ^{-1} получаем $\mathfrak{H}A_\varkappa = \mathfrak{H}A_\mu$; следовательно, комплексы в правой части (16а) те же, что и в правой части (16), только может быть расположены в ином порядке. Итак, элементу A_λ соответствует подстановка:

$$\overline{A}_\lambda = \begin{pmatrix} \mathfrak{H} & \mathfrak{H}A_2 & \ldots & \mathfrak{H}A_k \\ \mathfrak{H}A_\lambda & \mathfrak{H}A_2A_\lambda & \ldots & \mathfrak{H}A_kA_\lambda \end{pmatrix}.$$

Пусть A_μ другой элемент из $\mathfrak{G}$, ему соответствует подстановка:

$$\overline{A}_\mu = \begin{pmatrix} \mathfrak{H} & \mathfrak{H}A_2 & \ldots & \mathfrak{H}A_k \\ \mathfrak{H}A_\mu & \mathfrak{H}A_2A_\mu & \ldots & \mathfrak{H}A_kA_\mu \end{pmatrix} = \begin{pmatrix} \mathfrak{H}A_\lambda & \mathfrak{H}A_2A_\lambda & \ldots & \mathfrak{H}A_kA_\lambda \\ \mathfrak{H}A_\lambda A_\mu & \mathfrak{H}A_2A_\lambda A_\mu & \ldots & \mathfrak{H}A_kA_\lambda A_\mu \end{pmatrix};$$

тогда легко видеть, что элементу $A_\lambda A_\mu$ соответствует подстановка:

$$\overline{A_\lambda A}_\mu = \begin{pmatrix} \mathfrak{H} & \mathfrak{H}A_2 & \ldots & \mathfrak{H}A_k \\ \mathfrak{H}A_\lambda A_\mu & \mathfrak{H}A_2A_\lambda A_\mu & \ldots & \mathfrak{H}A_kA_\lambda A_\mu \end{pmatrix} = \overline{A}_\lambda \cdot \overline{A}_\mu,$$

т. е. произведению двух элементов из $\mathfrak{G}$ соответствует произведение подстановок, соответствующих сомножителям. Отсюда следует, что эти подстановки образуют группу $\overline{\mathfrak{G}}$, и что группа $\mathfrak{G}$ гомоморфна группе $\overline{\mathfrak{G}}$ (в частном случае быть может и просто изоморфна, но заранее мы этого не знаем).

Посмотрим, какие элементы A из $\mathfrak{G}$? соответствуют тождественной подстановке $\overline{E}$; это — такие элементы A, для которых $\mathfrak{H}A = \mathfrak{H}$ и $\mathfrak{H}A_\lambda A = \mathfrak{H}A_\lambda$ для всякого

$A_\lambda \subset \mathfrak{G}$. Из первого равенства (по теореме 5 § 192) следует: $A \subset \mathfrak{H}$; второе равенство дает: $(A_\lambda^{-1})\mathfrak{H}A_\lambda) = A_\lambda^{-1}\mathfrak{H}A_\lambda$, т. е. $A \subset A_\lambda^{-1}\mathfrak{H}A_\lambda$, при всяком A_λ из G. Таким образом элемент A — общий всем сопряженным с $\mathfrak{H}$ группам, т. е. A принадлежит их пересечению $\mathfrak{D}$. Обратно, если $A \subset \mathfrak{D}$, то, как легко убедиться, $\overline{A} = \overline{E}$ — тождественная подстановка. По теореме I § 197 $\mathfrak{D}$ — инвариантная подгруппа для $\mathfrak{G}$, а по теореме § 200 группа $\overline{\mathfrak{G}}$ просто изоморфна группе $\dfrac{\mathfrak{G}}{\mathfrak{D}}$. В частном случае, если $\mathfrak{D} = E$, т. е. если все сопряженные $\mathfrak{H}$ группы взаимно простые, то сама группа $\mathfrak{G}$ будет просто изоморфна группе $\overline{\mathfrak{G}}$, т. е. в этом случае группа подстановок $\overline{\mathfrak{G}}$ является представлением абстрактной группы $\mathfrak{G}$, причем представлением более выгодным, чем данное в § 196, ибо число k переставляемых символов (так называемая *степень* группы подстановок) меньше порядка группы, тогда как в доказательстве теоремы § 196 эта степень группы равна ее порядку. Этот выгодный для нас случай всегда имеет место, если $\mathfrak{G}$ — простая (но не простейшая) группа, ибо там всегда $\mathfrak{D} = E$: ведь простая группа не имеет инвариантных подгрупп кроме E и самоё себя. Другой предельный случай, когда сама подгруппа $\mathfrak{H}$ инвариантна; тогда $\mathfrak{D} = \mathfrak{H}$, и группа $\overline{\mathfrak{G}}$ просто изоморфна группе $\dfrac{\mathfrak{G}}{\mathfrak{H}}$; такой случай мы имеем в абелевых группах для всякой подгруппы $\mathfrak{H}$, ибо там всякая подгруппа инвариантна.

Пример. В § 196 рассматривается группа 6-го порядка перестановок трех символов (так называемая симметрическая группа третьей степени); по способу, данному в том же параграфе, она представляется как группа перестановок шести символов. Если же мы возьмем ее подгруппу $\mathfrak{H}_1 = E + A_1$, то из таблицы Кэли всей группы (таблица II в § 196) найдем такие сопряженные с $\mathfrak{H}_1$ подгруппы:

$$\mathfrak{H}_2 = E + A_2, \qquad \mathfrak{H}_3 = E + A_3;$$

они — взаимно простые. Следовательно, всю группу можно представить как группу подстановок трех символов. Имеем: $\mathfrak{H}_1 = \mathfrak{H}_1A_1 = E + A_1$, $\mathfrak{H}_1A_2 = \mathfrak{H}_1C = A_2 + C$, $\mathfrak{H}_1A_3 = \mathfrak{H}_1B = A_3 + B$; обозначив $\mathfrak{H}_1$ номером 1, $\mathfrak{H}_1A_2$ номером 2, $\mathfrak{H}_1A_3$ номером 3, мы получим:

$$\overline{E} = \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}, \quad \overline{A}_1 = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}, \quad \overline{A}_2 = \begin{pmatrix}3&2&1\\3&2&1\end{pmatrix}, \quad \overline{A}_3 = \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},$$
$$\overline{B} = \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}, \qquad \overline{C} = \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}$$

как раз те же самые подстановки, что и в § 196.

§ 202. Инвариантные комплексы. Пусть A элемент данной группы $\mathfrak{G}$; будем преобразовывать A (§ 197) всеми элементами из $\mathfrak{G}$; получим элементы $X^{-1}AX$ (где X пробегает все элементы из $\mathfrak{G}$), которые будут, конечно, не все различны; мы берем все различные элементы $X^{-1}AX$; пусть это будут $A_1, A_2, \ldots, A_{m-1}$; они образуют *класс сопряженных с A элементов*. Если элемент $B \subset \mathfrak{G}$ сопряжен с A, то он находится среди $A_1, A_2, \ldots, A_{m-1}$ и класс элементов, сопряженных с B, совпадает с классом $A_1, A_2, \ldots, A_{m-1}$. Таким образом мы можем все элементы из $\mathfrak{G}$ распределить по классам сопряженных элементов. Может случиться, что в данном классе будет только один элемент, т. е. один этот элемент составляет целый класс;

такой элемент называется *изолированным*. Если P — изолированный элемент, то это значит, что для всякого $X \subset \mathfrak{G}$ $X^{-1}PX = P$, или $PX = XP$, т. е. *изолированный элемент группы переместим с каждым элементом той же группы.* Единица E — всегда изолированный элемент.

Обозначим классы сопряженных элементов группы $\mathfrak{G}$ через $\mathfrak{A} = E, \mathfrak{A}_2, \mathfrak{A}_3, \ldots, \mathfrak{A}_k$; тогда

$$\mathfrak{G} = E + \mathfrak{A}_2 + \mathfrak{A}_3 + \ldots + \mathfrak{A}_k.$$

Очевидно, что никакие два класса не имеют общих элементов. Кроме E ни один из классов не составляет группы (ибо не содержит единицы E, которая должна быть во всякой группе).

Если X любой элемент из $\mathfrak{G}$, а $\mathfrak{A}_\lambda$ — какой-нибудь класс сопряженных элементов из $\mathfrak{G}$, то, очевидно:

$$X^{-1}\mathfrak{A}_\lambda X = \mathfrak{A}_\lambda,$$

ибо от преобразования посредством X элементов из $\mathfrak{A}_\lambda$ они только переставляются. В этом смысле системы $\mathfrak{A}_\lambda$ являются *инвариантными комплексами* группы $\mathfrak{G}$. Вообще комплекс $\mathfrak{A}$ элементов из $\mathfrak{G}$ называется *инвариантным*, если для всякого $X \subset \mathfrak{G}$

$$X^{-1}\mathfrak{A}X = \mathfrak{A}.$$

Очевидно, что всякий инвариантный комплекс, и в частности всякая инвариантная подгруппа группы G либо совпадает с одним из комплексов $\mathfrak{A}_\lambda$, либо есть сумма некоторых из них: $\mathfrak{A}_\varkappa + \mathfrak{A}_\lambda + \mathfrak{A}_\mu + \ldots$

Выясним теперь, сколько элементов имеется в данной системе $\mathfrak{A}_\lambda$. Пусть A — любой элемент из $\mathfrak{A}_\lambda$. Все элементы из $\mathfrak{G}$, переместимые с A, очевидно, составляют группу, ибо если $PA = AP$ и $PB = BP$, то и

$$P(AB) = (PA)B = (AP)B = A(PB) = A(BP) = (AB)P.$$

Эта группа переместимых с A элементов из $\mathfrak{G}$ называется *нормализатором* элемента A; обозначим ее через $\mathfrak{H}$ и разложим группу $\mathfrak{G}$ по модулю $\mathfrak{H}$, взятому слева:

$$\mathfrak{G} = \mathfrak{H} + \mathfrak{H}G + \mathfrak{H}G' + \ldots; \tag{17}$$

если $H \subset \mathfrak{H}$, то $HA = AH$, и, следовательно, $H^{-1}AH = A$; но если взят элемент не из $\mathfrak{H}$, то, преобразовывая им A, мы получим уже элемент из $\mathfrak{A}_\lambda$, отличный от A; например, $A_1 = G^{-1}AG \neq A$. Докажем, что при $G_1 \subset \mathfrak{H}G$ будет тоже $G_1^{-1}AG_1 = A_1$. Действительно, $G_1 = HG$, где $H \subset \mathfrak{H}$; следовательно:

$$G^{-1}AG_1 = (HG)^{-1}A(HG) = G^{-1}H^{-1}AHG = G^{-1}AG = A_1.$$

Обратно, пусть

$$G_1^{-1}AG_1 = A_1,$$

т. е.

$$G_1^{-1}AG_1 = G^{-1}AG;$$

умножая это слева на G_1; а справа на G^{-1}, найдем:

$$G_1G_1^{-1}AG_1G^{-1} = G_1G^{-1}AGG^{-1}$$

или

$$A(G_1G^{-1} = (G_1G^{-1}A.$$

Таким образом G_1G^{-1} переместимо с A, т. е. $G_1G^{-1} - H \subset \mathfrak{H}$; отсюда

$$G_1 = HG \subset \mathfrak{H}G.$$

Отсюда следует, что преобразовывая A различными элементами из G мы получим столько различных элементов $A, A_1, A_2, \ldots$, сопряженных с A, сколько имеется различных комплексов $\mathfrak{H}, \mathfrak{H}G, \mathfrak{H}G' \ldots$, в (17), а это число комплексов равно индексу $(\mathfrak{G}, \mathfrak{H})$. Итак:

Теорема. *Число различных элементов в классе сопряженных элементов $\mathfrak{A}_\lambda$ равно индексу нормализатора для любого элемента из $\mathfrak{A}_\lambda$.*

Отсюда следует, во-первых, что нормализаторы различных элементов из $\mathfrak{A}_\lambda$ имеют один и тот же порядок; можно доказать, что все эти нормализаторы являются сопряженными друг с другом, а следовательно, и изоморфными друг другу подгруппами группы $\mathfrak{G}$. Во-вторых, из доказанной теоремы следует, что *число различных элементов в $\mathfrak{A}_\lambda$ есть делитель порядка группы $\mathfrak{G}$.*

Теорема. *Все изолированные элементы данной группы $\mathfrak{G}$ образуют абелеву группу $\mathfrak{C}$, являющуюся инвариантной подгруппой для $\mathfrak{G}$.*

Доказательство. Очевидно, что произведение изолированных элементов — тоже изолированный элемент; все они переместимы и друг с другом, и со всяким иным элементом из $\mathfrak{G}$; это и доказывает нашу теорему.

Группа $\mathfrak{C}$ изолированных элементов называется *центром* группы $\mathfrak{G}$.

Для простой группы центр равен E.

Для абелевой группы всякий элемент изолированный,т. е. имеется столько классов сопряженных элементов, сколько самих элементов; центр абелевой группы есть сама эта группа.

Пример. У симметрической,группы третьей степени (6-го порядка; см. § 196) имеется три класса сопряженных элементов: $\mathfrak{A}_1 = E, \mathfrak{A}_2 = A_1+A_2+A_3, \mathfrak{A}_3 = B+C$.

Понятие о классах сопряженных элементов очень важно в так называемой теории характеров и представлений групп при помощи матриц.

§ 203. Теорема Силова (Sylow). В § 194 мы имели теорему Лагранжа о том, что порядок подгруппы есть делитель порядка всей группы. Возникает обратный вопрос: если порядок данной группы имеет делителем число m, то непременно ли существует у этой группы подгруппа m-го порядка. Оказывается, что, вообще говоря, это не непременно будет так. Например, группа всех четных подстановок четырех символов (так называемая полусимметрическая группа четвертой степени) 2-го порядка не имеет подгруппы 6-го порядка. Но в одном частном случае теорема Лагранжа обратима: именно, если делитель m порядка n группы есть степень простого числа. Тут имеет место такая теорема:

Теорема Силова. *Если порядок n данной группы $\mathfrak{G}$ делится на p^k, где p — простое число, то группа имеет подгруппу порядка p^k (при этом p^k может и не быть наивысшей степенью p, входящей в n).*

Например, группа 81-го порядка обязательно имеет подгруппу 3-го, 9-го, 27-го порядков. Силов домазал эту теорему для групп подстановок; Фробениус дал общее доказательство для абстрактных групп.

Лемма. *Если порядок n абелевой группы $\mathfrak{G}$ делится на простое число p, то в группе $\mathfrak{G}$ имеется элемент p-го порядка.*

Доказательство. Легко видеть, что во всякой, даже неабелевой, группе есть элемент простого порядка. Действительно, пусть $Q \subset \mathfrak{G}$; если порядок Q простое число, то высказанное предложение уже верно; если же этот порядок m — составное число, то он делится на простое число q; тогда $Q^m = (Q^{\frac{m}{q}})^q = E$, т. е. $Q^{\frac{m}{q}}$ есть элемент простого порядка.

Итак, пусть Q элемент абелевой группы G, и порядок Q есть q — простое число; пусть $q \neq p$ (иначе лемма была бы доказана). Циклическая группа $\{Q\} = \mathfrak{Q}$ является инвариантной подгруппой для $\mathfrak{G}$; следовательно, существует группа $\frac{\mathfrak{G}}{\mathfrak{Q}}$ порядка $\frac{n}{q}$, причем $\frac{n}{q}$ делится на p. Нашу лемму легко непосредственно проверить для групп 2, 3, 4 порядков. Следовательно, можно применить метод полной индукции, считая лемму доказанной для групп порядков, меньших n. Но $\frac{n}{q} < n$; следовательно, для группы $\frac{\mathfrak{G}}{\mathfrak{Q}}$ лемма считается доказанной, и в этой группе есть элемент p-го порядка; пусть это есть комплекс $\mathfrak{Q}A$; тогда имеем:

$$(\mathfrak{Q}A)^p = \mathfrak{Q}A^p = \mathfrak{Q},$$

а это (по теореме 5 § 192) означает, что $A^p \subset \mathfrak{Q}$. Но элементы из $D\mathfrak{Q}$ — различные степени Q; следовательно:

$$A^p = Q^t.$$

Определим число x из сравнения $px \equiv -t \pmod q$ [94] и возьмем элемент $Q^xA \subset \mathfrak{Q}A$; имеем:

$$(Q^xA)^p = Q^{px}A^p = Q^{px}Q^t = Q^{px+t} = E^{95},$$

так как $px + t$ делится на q, а $Q^q = E$. Итак, Q^xA и есть искомый элемент p-го порядка, и лемма доказана.

Переходим теперь к доказательству теоремы Силова. Она легко непосредственна проверяется для групп низших порядков, так что мы можем и здесь применить метод полной индукции, считая ее доказанной для групп порядков, меньших, чем n.

Разложим группу $\mathfrak{G}$ на классы сопряженных элементов; обозначим через c число изолированных элементов, а через $k_1, k_2, \ldots, k_\lambda$ — числа элементов в остальных λ классах; так как всего в группе n элементов, то имеем:

$$n = c + k_1 + k_2 + \ldots + k_\lambda.$$

Как мы видели в § 202, c и все k_μ — делители числа n. Пусть, например, k_ν не делится на p; тогда $\frac{n}{k_\nu}$ делится на p^k. Но $\frac{n}{k_\nu}$ есть порядок нормализатора (см. первую теорему § 202) для любого элемента из этого ν-го класса. Обозначим этот нормализатор через $\mathfrak{A}$; его порядок $\frac{n}{k_\nu} < n$ и делится на p^k; следовательно, для $\mathfrak{A}$

[94] Решить сравнение $px \equiv -t \pmod q$ — это значит найти такое целое число x, для которого $px + t$ делилось бы на q; иначе, решить в целых числах неопределенное уравнение $px + t = qy$. При $\mathbf{D}(p, q) = 1$ (а это здесь выполнено) решения всегда существуют.

[95] Для абелевых групп верна формула: $(AB)^m = A^mB^m$

теорема верна, т. е. $\mathfrak{A}$ имеет подгруппу $\mathfrak{P}$ порядка p^k; но $\mathfrak{P}$ ведь подгруппа и для $\mathfrak{G}$, т. е. для этого случая теорема Силова доказана.

Пусть теперь все k_ν делятся на p; тогда и c должно делиться на p, ибо n делится на p. Но c — порядок центра $\mathfrak{C}$ группы $\mathfrak{G}$, а центр — абелева группа. Следовательно, по лемме, в $\mathfrak{C}$ имеется элемент P порядка p. Обозначим через $\mathfrak{P} = \{P\}$ циклическую группу степеней P; $\mathfrak{P}$ — инвариантная подгруппа для $\mathfrak{G}$, так как $P \subset \mathfrak{G}$, т. е. P изолированный элемент. Группа $\dfrac{\mathfrak{G}}{\mathfrak{P}}$ порядка $\dfrac{n}{p} < n$; $\dfrac{n}{p}$ делится на p^{k-1} (а может быть и на p^k, если p не наивысшая степень p, входящая в n); следовательно, для группы $\dfrac{\mathfrak{G}}{\mathfrak{P}}$ теорема Силова имеет место, и эта группа имеет подгруппу порядка p^{k-1}; тогда, по теореме 2 § 198, мы можем обозначить эту подгруппу через $\dfrac{\mathfrak{U}}{\mathfrak{P}}$, где $\mathfrak{G} \supset \mathfrak{A} \supset \mathfrak{P}$. Так как порядок $\dfrac{\mathfrak{A}}{\mathfrak{P}}$ есть p^{k-1}, а порядок $\mathfrak{P}$ есть p, то, следовательно, порядок $\mathfrak{A}$ есть $p^{k-1}\,p = p^k$, т. е. группа $\mathfrak{G}$ имеет подгруппу $\mathfrak{A}$ порядка p^k, что и требовалось доказать.

Доказанная теорема называется первой теоремой Силова; есть еще вторая теорема, которую мы тут только сформулируем, не приводя доказательства.

Вторая теорема Силова. *Если группа $\mathfrak{G}$ n-го порядка имеет ровно x подгрупп порядка p^α, где p^α — наивысшая степень простого числа p, входящая в n, то $x \equiv 1 \pmod p$, или $x = 1 + mp$; все эти подгруппы порядка p^α сопряжены друг с другом; если $k < \alpha$, то всякая подгруппа группы $\mathfrak{G}$ порядка p^k содержится по крайней мере в одной из подгрупп порядка p^α.*

На этом мы заканчиваем теорию абстрактных групп и возвращаемся к группам подстановок.

§ 204. Разложение подстановок на циклы. Возьмем подстановку такого вида:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 1 & 6 & 2 & 5 \end{pmatrix};$$

здесь 1 заменяется на 4, 4 на 6, 6 на 5, 5 на 2, 2 на 3 и 3 на 1; эти замены, как мы видим, составляют цепь, последнее звено которой соединено с первым; такая подстановка называется *циклической*, или просто *циклом*, и обозначается в виде одной строки: $(1, 4, 6, 5, 2, 3)$, где каждый символ заменяется следующим за ним, а последний заменяется первым. Конечно, безразлично, с какого символа начать, лишь бы не нарушался порядок следования символов друг за другом. Так,

$$(1, 4, 6, 5, 2, 3) = (4, 6, 5, 2, 3, 1) = (2, 3, 1, 4, 6, 5) = \ldots$$

В общем случае подстановку можно «разложить» на циклы следующим образом:

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 2 & 1 & 0 & 3 & 5 & 9 & 8 & 6 & 7 \end{pmatrix} = (0, 4, 3)\ (1, 2)\ (5)\ (6, 9, 7, 8); \qquad (18)$$

здесь нуль переходит в 4, 4 — в 3, 3 — в нуль, следовательно, цикл замкнут; далее, 1 переходит в 2, а 2 снова в единицу; цикл опять замкнут; символ 5 переходит в самого себя; следовательно, он один составляет цикл; наконец, символы 6, 9, 7, 8 тоже составляют цикл. Никакая пара из этих четырех циклов, на которые

мы разложили нашу подстановку, не имеет общих символов; такие циклы, называются *независимыми*. Очевидно, что всякая подстановка может быть разложена таким же образом на независимые циклы; при этом, так как безразлично, с какого символа начать это разложение, то наши независимые циклы могли бы стоять и в каком-нибудь ином порядке, а в каждом из них символы могут тоже перемещаться, но в циклическом порядке, как было уже объяснено; в остальном же это разложение на независимые циклы однозначно: всегда, например, в подстановке (18) 0 будет находиться в тройном цикле вместе с 4 и 3: $(0, 4, 3)$, или $(4, 3, 0)$, или $(3, 0, 4)$; 2 будет находиться в двойном цикле вместе с 1 и т. п. Цикл, состоящий из одного символа, такой, как в (18) цикл (5) обычно не пишется; так что если в разложении подстановки на независимые циклы нет некоторых символов, то это значит, что эти символы не меняются в данной подстановке. В правой части (18) стоит символическое произведение циклов; это обычное произведение подстановок, ибо каждый цикл можно рассматривать как обычную подстановку, например:

$$(0, 4, 3) = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 1 & 2 & 0 & 3 & 5 & 6 & 7 & 8 & 9 \end{pmatrix}.$$

Таким образом независимые циклы, рассматриваемые как подстановки, всегда переместимы друг с другом.

Если приходится перемножать не независимые циклы, т. е. циклы, имеющие общие символы, то тут, конечно, коммутативный закон неверен; такое произведение зависимых циклов, всегда можно представить как произведение независимых циклов («действительно перемножить» данные зависимые циклы), например:

$$(0, 4, 6, 8, 5)\ (1, 3, 4, 7, 5, 6)\ (2, 0, 4, 3) = \\ = (0, 7, 5, 4, 1, 2)\ (6, 8)\ (3).$$

Рассуждаем так: в первом цикле 0 заменяется на 4, во втором цикле 4 заменяется на 7; третий цикл не меняет символа 7; следовательно 0 в конечном счете заменяется на 7; далее, 7 не меняется в первом цикле, во втором 7 переходит в 5, в третьем 5 не меняется; следовательно, 7 переходит в 5 и т. д. Когда первый цикл результата окажется замкнутым, берем один из символов, не вошедших в полученный первый цикл, и повторяем с ним то же рассуждение и т. д. Цикл (3), конечно, можно было бы и не писать.

Когда говорят о числе независимых циклов, на которые раскладывается данная подстановка, то принимаются во внимание и одночленные циклы.

Обратная к циклу подстановка, очевидно, есть тоже цикл, символы которого написаны в обратном порядке, например:

$$(1, 4, 2, 6, 5, 3)^{-1} = (3, 5, 6, 2, 4, 1).$$

Рассмотрим степени цикла, имеем, например:

$$(1, 2, 3, 4, 5)^2 = (1, 3, 5, 2, 4),$$

ибо 1 заменится на 2, а 2 сейчас же на 3 и т. д.; далее:

$$(1, 2, 3, 4, 5)^3 = (1, 4, 2, 5, 3),$$
$$(1, 2, 3, 4, 5)^4 = (1, 5, 4, 3, 2),$$
$$(1, 2, 3, 4, 5)^5 = (1)\ (2)\ (3)\ (4)\ (5) = E.$$

Возьмем еще:

$$(1,2,3,4,5,6)^2 = (1,3,5)\ (2,4,6),$$
$$(1,2,3,4,5,6)^3 = (1,4)\ (2,5)\ (3,6),$$
$$(1,2,3,4,5,6)^4 = (1,5,3)\ (2,6,4),$$
$$(1,2,3,4,5,6)^5 = (1,6,5,4,3,2), \quad (1,2,3,4,5,6)^6 = E.$$

Отсюда заключаем: *порядок цикла всегда равен числу символов, из которых состоит цикл. Степени цикла представляют собой или тоже циклы, или раскладываются на независимые циклы с одним и тем же числом символов; если цикл A m-го порядка, то A^{m-1} есть цикл, обратный к A* (как это и вытекает из общей теории).

Подстановка, которая раскладывается на независимые циклы с одним и тем же числом символов, называется *регулярной*; мы видели, что степени цикла — или циклы, или регулярные подстановки; можно было бы показать обратное: всякая регулярная подстановка есть степень цикла.

Упражнения

227) Разложить следующие подстановки на независимые циклы:

$$a)\ \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 9 & 8 & 5 & 4 & 6 & 0 & 1 & 2 & 7 \end{pmatrix}, \qquad b)\ \begin{pmatrix} \alpha & \beta & \gamma & \delta & \varepsilon & \zeta \\ \zeta & \delta & \beta & \gamma & \alpha & \varepsilon \end{pmatrix},$$
$$c)\ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 2 & 1 & 6 & 7 & 4 & 8 & 5 & 9 & 3 \end{pmatrix}.$$

Отв. a) $(0,3,5,6)\ (1,9,7)\ (2,8)$, b) $(\alpha,\zeta,\varepsilon)\ (\beta,\delta,\gamma)$, c) $(1,2)\ (3,6,8,9)\ (4,7,5)$.

228) «Перемножить» следующие циклы: a) $(0,4,3,2)\ (1,6,2,3)\ (4,5)$, b) $\alpha,\beta,\gamma)\ (\alpha,\delta,\varepsilon)\ (\alpha,\beta,\varepsilon)$, c) $(0,1)\ (0,1,2)\ (0,1,2,3)\ (0,1,2,3,4)$.

Отв. a) $(0,5,4,1,6,2)\ (3)$, b) $(\alpha,\varepsilon,\beta,\gamma,\delta)$, c) $(0,4)\ (1,3)\ (2)$.

229) Доказать, что обратная подстановка раскладывается на столько же независимых циклов, что и данная, и что в каждом из этих циклов столько символов и те же символы, что и в соответственных циклах данной подстановки, только эти символы идут в обратном порядке.

§ 205. Разложение подстановок на транспозиции. В § 28 уже было показано, что всякая подстановка представляется как произведение транспозиций, причем четность или нечетность числа этих транспозиций для данной подстановки вполне определена.

Докажем это иначе.

Легко видеть, что всякий цикл из m символов может быть разложен на $m-1$ транспозиций, например:

$$(1,2,3,4,5,6) = (1,2)\ (1,3)\ (1,4)\ (1,5)\ (1,6).$$

А так как всякая подстановка раскладывается на циклы, то она может быть разложена и на транспозиции, например:

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 2 & 1 & 5 & 0 & 8 & 7 & 9 & 4 & 6 \end{pmatrix} = (0,3,5,8,4)\ (1,2)\ (6,7,9) =$$
$$= (0,3)\ (0,5)\ (0,8)\ (0,4)\ (1,2)\ (6,7)\ (6,9).$$

Если число всех символов n, а число независимых циклов, на которые раскладывается подстановка (причем учитываются и одночленные циклы), есть s, то, как мы видим, подстановка раскладывается на $n - s$ транспозиций. Действительно, пусть эти s циклов содержат: первый a_1 символов, второй a_2 символов и т. д., s-й a_s символов; тогда первый раскладывается на $a_1 - 1$ транспозиций, второй — на $a_2 - 1$, ..., s-й — на $a_s - 1$, а всего подстановка разложится на $(a_1 - 1) + (a_2 - 1) + \ldots + (a_s - 1) = a_1 + a_2 + \ldots + a_s - s = n - s$ транспозиций, ибо совокупность всех циклов (в том числе и одночленных) включает все n символов и каждый по одному разу.

Разложение подстановки на транспозиции возможно многими способами с различным числом транспозиций; например, к данному разложению мы всегда можем написать еще две одинаковые транспозиции $(a, b)(a, b)$, которые не изменят результата. Но мы докажем, что найденное число $n - s$ есть наименьшее число транспозиций, на которые раскладывается данная подстановка.

Теорема. *Если подстановка n символов раскладывается на s независимых циклов, то наименьшее число транспозиций, на которые она может быть разложена, есть $n - s$; всякое другое число транспозиций, на которые она раскладывается, представляется в виде $n - s + 2p$, где p — целое число большее нуля.*

Предварительно докажем следующую лемму:

Лемма. *Если R данная, подстановка, а $T = (a, b)$ транспозиция, то в RT число независимых циклов или на единицу больше, или на единицу меньше, чем в R, смотря по тому, входят ли в R символы a и b в один и тот же или в разные циклы.*

Доказательство. В R мы должны учитывать только те циклы, куда входят a и b. Разберем два случая:

$$\begin{aligned} 1.\ R &= (a, a_1, a_2, \ldots, a_\alpha)\ (b, b_1, b_2, \ldots, b_\beta)\ \ldots, \\ RT &= (a, a_1, a_2, \ldots a_\alpha, b, b_1, b_2, \ldots, b_\beta)\ \ldots \end{aligned}$$

(остальные циклы не меняются); в самом деле, в R a_α переходит в a, а в T a переходит в b, следовательно, в RT a_α перейдет в b, т. е. в RT два цикла соединились в один.

$$\begin{aligned} 2.\ R &= (a, a_1, \ldots, a_\alpha, b, b_1, \ldots, b_\beta)\ \ldots, \\ RT &= (a, a_1, a_2, \ldots, a_\alpha)\ (b, b_1, \ldots, b_\beta)\ \ldots, \end{aligned}$$

т. е. RT один цикл расщепился на два.

Докажем теперь нашу теорему. Пусть данная подстановка A каким-нибудь образом разложена на t транспозиций, и пусть, например, $(1, 2)$ первая из них: $A = (1, 2)(a, b)(c, d)\ldots$ Имеем:

$$(1, 2) = (1, 2)(3)(4)\ldots(n),$$

т. е. подстановка $(1, 2)$ раскладывается на $n - 1$ независимых циклов; чтобы получить A, мы должны $(1, 2)$ умножить на (a, b), затем на $(, d)$ и т. д., всего $t - 1$ раз. Но по лемме от каждого такого умножения число независимых циклов изменяется на 1; в A же это число равно s. Обозначим: $\varepsilon_1 = -1$, $\varepsilon_2 = \pm 1$, ..., $\varepsilon_t = \pm 1$; тогда

$$n + \varepsilon_1 + \varepsilon_2 + \ldots + \varepsilon_t = s;$$

если из количеств $\varepsilon_\varkappa$ p равны $+1$, а $t-p$ равны -1, то получим:

$$n+p-(t-p)=s;$$

отсюда $t=n-s+2p$, и теорема доказана.

Отсюда следует, что числа транспозиций, на которые может быть разложена данная подстановка, всегда одной и той же четности, и все подстановки n символов разделяются на два класса: на *четные* подстановки (раскладывающиеся на четное число транспозиций) и *нечетные* подстановки (раскладывающиеся на нечетное число транспозиций). Очевидно, что произведение двух четных или двух нечетных подстановок всегда четная подстановка, а произведение четной на нечетную (или наоборот) — нечетная подстановка.

Теорема. *При всяком n существуют как четные, так и нечетные подстановки n элементов, причем число тех и других одинаково:* $\frac{1}{2}\,n!$.

Доказательство. Если n — четное, то, например, цикл $(1,2,\ldots,n)$ нечетная подстановка, а цикл $(1,2,\ldots,n-1)$ четная; если n — нечетное, то наоборот. Умножив все четные подстановки на какую-либо транспозицию, получим нечетные подстановки; умножив же все нечетные подстановки на транспозицию, получим четные подстановки. Отсюда следует, что число тех и других одинаково (и равно $\frac{1}{2}\,n!$, ибо всех подстановок $n!$).

Теорема. *Все четные подстановки n символов образуют группу, являющуюся инвариантной подгруппой (индекса 2) для симметрической группы n-й степени.*

Доказательство. Первая часть очевидна: произведение четных подстановок тоже четная подстановка. Вторая часть следует из того, что если R — четная, а S — любая подстановка, то $S^{-1}RS$ всегда тоже четная, ибо S всегда одинаковой четности с S (S^{-1} состоит из тех же транспозиций, что и S, только поставленных в обратном порядке).

Определение. Группа всех четных подстановок n символов называется *полусимметрической* [96] группой n-й степени.

Упражнения

230) Разложить на транспозиции подстановки;

$$a)\ \begin{pmatrix}0&1&2&3&4&5&6&7&8&9\\3&5&7&1&0&4&8&9&2&6\end{pmatrix},\qquad b)\ \begin{pmatrix}1&2&3&4&5&6&7\\3&6&1&7&2&5&4\end{pmatrix}$$

$$c)\ (3,5,7)\ (8,4,1,0,2).$$

Отв. a) $(0,3)\ (0,1)\ (0,5)\ (0,4)\ (2,7)\ (2,9)(2,6)\ (2,8)$, b) $(1,3)\ (2,6)\ (2,5)\ (4,7)$, c) $(3,5)\ (3,7)\ (8,4)\ (8,1)\ (8,0)\ (8,2)$.

231) Представить в виде произведений независимых циклов следующие произведения транспозиций: a) $(0,1)\ (1,3)\ (2,3)\ (3,4)\ (4,5)$, b) $(0,2)\ (3,6)\ (2,6)\ (0,3)$, c) $(0,1)\ (2,3)\ (1,2)\ (0,1)\ (1,2)$.

Отв. a) $(0,2,5,4,3,1)$, b) $(0,6)\ (2,3)$, c) $(0,1,2,3)$.

232) Если данная подстановка разложена на транспозиции, то как отсюда вывести разложение на транспозиции обратной подстановки?

[96] А также *знакопеременной* или *альтернирующей* группой.

Отв. Написать все транспозиции в обратном порядке.

§ 206. Подобные подстановки. Лемма. *Для того чтобы из подстановки A получить подстановку $P^{-1}AP$, надо в независимых циклах подстановки A сделать подстановку P.*

Доказательство. Этот способ составления $P^{-1}AP$ легче всего выясняется на примере:

$$A = (0,2,4,3,1)\ (5,6)\ (7,8,9), \qquad P = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 9 & 4 & 3 & 2 & 1 & 7 & 6 & 8 & 0 & 5 \end{pmatrix}$$

$$P^{-1}AP = (9,3,1,2,4)\ (7,6)\ (8,0,5).$$

Значит, берутся символы циклов A и вместо них ставятся те, которыми они заменяются в P: 9 вместо 0, 3 вместо 2, 1 вместо 4 и т. д.

Действительно, в P^{-1} 9 переходит в 0, в A 0 переходит в 2, в P 2 переходит в 3; следовательно, в $P^{-1}AP$ 9 перейдет в 3 и т. д.

Мы видим, что число независимых циклов в $P^{-1}AP$ то же, что и в P, и в каждом цикле по стольку же символов, что и в P. Такие подстановки называются *подобными*.

Упражнения

233) Преобразовать подстановку $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 1 & 2 & 8 & 4 & 7 & 6 & 5 \end{pmatrix}$ посредством подстановки $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 7 & 4 & 5 & 1 & 2 & 6 & 3 \end{pmatrix}$.

Отв. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 6 & 1 & 7 & 3 & 2 & 8 & 4 \end{pmatrix}$.

234) Найти подстановки, которые преобразовывают $(0,3,7)\ (2,5)\ (1,4,6)$ в $(0,6,2)\ (3,4)\ (1,7,5)$.

Отв. Их всего 1444; одна из них: $\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 0 & 1 & 3 & 6 & 7 & 4 & 5 & 2 \end{pmatrix}$.

§ 207. Простота полусимметрических групп степени $n > 4$. Обозначим симметрическую группу через $\mathfrak{S}$, полусимметрическую группу через $\mathfrak{R}$.

1. При $n = 2$ $\mathfrak{S}$ простейшая группа (2-го порядка); $\mathfrak{R} = E$.

2. При $n = 3$? $\mathfrak{S}$ 6-го порядка, $\mathfrak{R}$ 3-го порядка — простейшая группа.

3. При $n = 4$ $\mathfrak{S}$ 24-го порядка, $\mathfrak{R}$ 12-го порядка не простая: и $\mathfrak{S}$, и $\mathfrak{R}$ имеют инвариантную подгруппу, именно, четверную группу $\mathfrak{Q} = E + A + B + C$, где A =(0,1) (2,3), $B = (0,2)\ (1,3)$, $C = (0,3)\ (1,2)$. (Пример 1 § 196.) Действительно, если $S = \begin{pmatrix} 0 & 1 & 2 & 3 \\ \alpha & \beta & \gamma & \delta \end{pmatrix}$, где α, β, γ, δ — некоторая перестановка символов $0, 1, 2, 3$, то по лемме § 206, например, $S^{-1}AS = (\alpha,\beta)\ (\gamma,\delta)$ — одна из подстановок A, B, C. Как мы уже видели в § 196, группа $\mathfrak{Q}$ — абелева и имеет три подгруппы 2-го порядка $\mathfrak{Q}_1 = E + A$, $\mathfrak{Q}_2 = E + B$, $\mathfrak{Q}_3 = E + C$, инвариантные относительно $\mathfrak{Q}$, как всякие подгруппы абелевой группы. Следовательно, композиционный ряд для $\mathfrak{S}$ в этом случае: $\mathfrak{S}, \mathfrak{R}, \mathfrak{Q}, \mathfrak{Q}_\alpha$, E (где $\alpha = 1$ или 2, или 3); ряд индексов: 2, 3, 2, 2; следовательно, в этом (как и в двух предыдущих случаях) группа $\mathfrak{S}$ разрешима.

Теорема. *Полусимметричная группа $\mathfrak{R}$ n-й степени при $n > 4$ простая.*

Доказательство. Пусть $\mathfrak{R}$ имеет инвариантную подгруппу $\mathfrak{Q} \neq E$; докажем, что при $n > 4$ должно быть $\mathfrak{R} = \mathfrak{Q}$. Разберем несколько случаев.

1. В числе подстановок, содержащихся в $\mathfrak{Q}$, имеется тройной цикл: $Q = (0, 1, 2)$. Докажем, что тогда $\mathfrak{Q}$ содержит и все тройные циклы вида (α, β, γ).

Пусть $R = \begin{pmatrix} 0 & 1 & 2 & \dots \\ \alpha & \beta & \gamma & \dots \end{pmatrix}$ — четная подстановка (т. е. $\subset \mathfrak{R}$); тогда $R^{-1}QR = (\alpha, \beta, \gamma) \subset \mathfrak{D}$ (ибо $\mathfrak{D}$ — инвариантная подгруппа для $\mathfrak{R}$); R если же ? — нечетная, то $R' = \begin{pmatrix} 0 & 1 & 2 & \dots \\ \alpha & \gamma & \beta & \dots \end{pmatrix} = R \cdot (\beta, \gamma) =$ — четная, и $R'^{-1}QR' = (\alpha, \gamma, \beta) \subset \mathfrak{Q}$; но тогда и $(\alpha, \gamma, \beta)^2 = (\alpha, \beta, \gamma) \subset \mathfrak{Q}$.

Докажем теперь, что всякая четная подстановка раскладывается на тройные циклы; это следует из формул: $(\alpha, \beta)\ (\alpha, \gamma) = (\alpha, \beta, \gamma)$ и $(\alpha, \delta)\ (\beta, \gamma) = (\alpha, \beta, \gamma)\ (\alpha, \beta, \delta)$ и из того, что четная подстановка состоит из четного числа транспозиций. Таким образом $\mathfrak{Q}$, содержа все тройные циклы, содержит и всякую четную подстановку, т. е. $\mathfrak{Q} = \mathfrak{R}$.

Для дальнейшего заметим, что при $Q \subset \mathfrak{Q}$, $R \subset \mathfrak{R}$ имеем $PQR^{-1} \subset \mathfrak{Q}$ и $(Q^{-1}RQ)R^{-1} \subset \mathfrak{Q}$.

2. Пусть один из циклов подстановки $Q \subset \mathfrak{Q}$ содержит больше чем три символа: $Q = (0, 1, 2, 3, \dots)\ (\dots) \dots$; возьмем $R = (0, 1, 2)$; тогда $Q^{-1}RQ = (1, 2, 3)$, $(Q^{-1}RQ)R^{-1} = (1, 2, 3)\ (0, 2, 1) = (0, 2, 3) \subset \mathfrak{Q}$, и мы имеем уже разобранный случай 1, откуда снова заключаем: $\mathfrak{Q} = \mathfrak{R}$.

3. Пусть один из циклов подстановки $Q \subset \mathfrak{Q}$, содержит три символа:

$$Q = (0, 1, 2)\ (3, 4, \dots) \dots,$$

возьмем $R = (0, 1, 3)$, тогда

$$Q^{-1}RQ = (1, 2, 4), \qquad (Q^{-1}RQ)R^{-1} = (1, 2, 4)\ (0, 3, 1) = (0, 3, 1, 2, 4),$$

и мы имеем случай 2, так что снова заключаем: $\mathfrak{Q} = \mathfrak{R}$.

4. Пусть $Q \subset \mathfrak{Q}$ содержит не меньше трех двойных циклов:

$$Q = (0, 1)\ (2, 3)\ (4, 5) \dots;$$

берем $R = (0, 2, 4)$; тогда

$$Q^{-1}RQ = (1, 3, 5), \qquad (Q^{-1}RQ)R^{-1} = (1, 3, 5)(0, 4, 2),$$

и мы имеем случай 3; отсюда опять: $\mathfrak{Q} = \mathfrak{R}$.

5. Пусть Q имеет только два двойных цикла, а остальные одночленные: $Q = (0, 1)\ (2, 3)\ (4) \dots$; берем $R = (0, 1, 4)$; тогда $Q^{-1}RQ = (1, 0, 4)$, $(Q^{-1}RQ)R^{-1} = (1, 0, 4)\ (0, 4, 1) = (0, 1, 4)$, и мы опять имеем случай 3 и заключаем: $\mathfrak{Q} = \mathfrak{R}$.

Других случаев, не может быть, следовательно, теорема доказана. При $n = 4$ мы имеем исключение: там в случае 5 при $Q = (0, 1)\ (2, 3)$ нет символа 4 и мы не можем выбрать подходящим образом R и там действительно существует инвариантная подгруппа $\mathfrak{Q} \neq \mathfrak{R}$.

Следствие. Симметрическая группа $\mathfrak{S}$ n-й степени неразрешима при $n > 4$. Действительно, при $n > 4$ композиционный ряд для $\mathfrak{S}$ такой: $\mathfrak{S}, \mathfrak{R}, E$, ряд индексов: 2, $\frac{1}{2}n!$; но $\frac{1}{2}n!$ при $n > 4$ — составное число, т. е. $\mathfrak{R}$ — группа простая, но не простейшая.

Упражнения

235) Построить таблицу Кэли для симметрической группы четвертой степени (24-го порядка), найти все подгруппы этой группы и выяснить, какие из них инвариантные.

236) Построить таблицу Кэли для полусимметрической группы пятой степени (60-го порядка).

§ 208. Транзитивность и интранзитивность. Группа подстановок m символов называется *транзитивной*, если в ней имеются подстановки, переводящие каждый данный символ в каждый другой данный символ; в противном случае она называется *интранзитивной. Для того чтобы группа $\mathfrak{G}$ была транзитивной, необходимо и достаточно, чтобы в ней имелись подстановки, переводящие один определенный символ во все остальные.* Обозначим наши символы номерами: $1, 2, \ldots, m$, и пусть в G имеются подстановки, переводящие символ 1 во все остальные: пусть, например, A_k переводит 1 в k, а A_l переводит 1 в l, где k и l — любые заданные символы; тогда A_k^{-1} переведет k в 1, а $A_k^{-1}A_l$ переведет k в l. Этим наше предложение доказано.

Рассмотрим в данной транзитивной группе $\mathfrak{G}$ все подстановки, оставляющие данный символ, например 1, без изменения; в число их входит и тождественная подстановка E; если P и Q оставляют 1 без изменения, то и PQ и P^{-1} тоже не изменяют символа 1; т. е. все такие подстановки образуют группу $\mathfrak{A}_1$. Пусть подстановка A_2 переводит 1 в 2; тогда и все подстановки комплекса $\mathfrak{A}_1A_2$ переводят 1 в 2; обратно: если подстановка A' переводит 1 в 2, то A/A_2^{-1} оставляет 1 без изменения, т. е. $A'A_2^{-1} = P \subset \mathfrak{A}_1$, и, следовательно: $A' = PA_2 \subset \mathfrak{A}_1A_2$. Таким образом комплекс $\mathfrak{A}_1A_2$ состоит из всех подстановок, переводящих 1 в 2. Обозначим вообще через A_λ одну из подстановок, переводящих 1 в λ ($\lambda = 2, \ldots, m$), тогда все подстановки, переводящие 1 в λ, составляют комплекс $\mathfrak{A}_1A_\lambda$, и мы имеем разложение группы $\mathfrak{G}$ по модулю $\mathfrak{A}_1$, взятому слева:

$$\mathfrak{G} = \mathfrak{A}_1 + \mathfrak{A}_1A_2 + \mathfrak{A}_1A_3 + \ldots + \mathfrak{A}_1A_m.$$

Если k — порядок группы $\mathfrak{A}_1$; то $n = km$, т. е. *порядок транзитивной группы подстановок делится на ее степень.*

Рассмотрим подгруппы, сопряженные с $\mathfrak{A}_1$; легко видеть, что все подстановки группы $A_2^{-1}\mathfrak{A}_1A_2$ не изменяют символа 2, все подстановки группы $A_3^{-1}\mathfrak{A}_1A_3$, не изменяют символа 3 и т. д. Вообще, все подстановки группы $A_\lambda^{-1}\mathfrak{A}_1A_\lambda$ не изменяют символа λ. Обратно, пусть A не меняет символа λ; тогда $A_\lambda AA_\lambda^{-1} = P$ не изменит символа 1, т. е. $P \subset \mathfrak{A}_1$; но тогда $A = A_\lambda^{-1}PA_\lambda \subset A_\lambda^{-1}\mathfrak{A}_1A_\lambda$. Итак, группа $A_\lambda^{-1}\mathfrak{A}_1A_\lambda$ состоит из всех подстановок, не меняющих символа λ ($\lambda = 2, 3, \ldots, m$).

Легко видеть, что пересечение любых двух из групп $\mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_m$ состоит из одной только тождественной подстановки, т. е. все эти группы взаимно простые.

Рассмотрим случай, когда $\mathfrak{A}_1 = E$, т. е. когда E — единственная подстановка в группе G, не меняющая символ 1; но тогда $\mathfrak{A}_1 A_2 = A_2$, ..., $\mathfrak{A}_1 A_m = A_m$, и эти подстановки E, $A_2, \ldots, A_m$ исчерпывают всю группу $\mathfrak{G}$, порядок которой, таким образом, оказывается равным ее степени. Далее, $A_\lambda^{-1}\mathfrak{A}_1 A_\lambda = A_\lambda^{-1} E A_\lambda = E$; т. е. кроме E нет подстановок в $\mathfrak{G}$, которые бы оставляли хотя бы один символ без изменения. Итак, пусть подстановка A содержит символ 1 в α-членном цикле (§ 204); тогда A^α оставляет 1 без изменения, а следовательно, по-предыдущему: $A^\alpha = E$; так как A^α — наименьшая степень A, оставляющая 1 без изменения, то α — порядок подстановки A: но тогда в A все циклы α-членные, т. е. A *регулярная* (см. конец § 205), или циклическая подстановка. Итак, в этом случае группа $\mathfrak{G}$ состоит из регулярных подстановок; она называется также *регулярною*. Представление абстрактной группы в виде группы подстановок, данное в § 106, — *регулярное*, ибо получаемая там группа подстановок — *регулярная* (предлагается читателю проверить это).

Рассмотрим теперь интранзитивную группу; ее подстановками символ 1 переводится не во все остальные символы; предположим, что существуют в данной группе подстановки, переводящие символ 1 в символы $1, 2, 3, \ldots, k$, но не в иные; в таком случае подстановки данной группы переводят эти символы друг в друга, но не в остальные символы: пусть, например, A переводит 1 в $\varkappa$, а A_λ переводит 1 в λ, где $\varkappa$ и λ — символы из ряда $1, 2, 3, \ldots, k$; тогда $A_\varkappa^{-1} A_\lambda$ переводит $\varkappa$ в λ. С другой стороны, пусть подстановка A переводит $\varkappa$ в μ, тогда $A_\varkappa A$ переведет 1 в μ, т. е. μ — тоже из ряда $1, 2, \ldots, k$.

Взяв теперь символ $k+1$, мы убедимся, что никакая подстановка данной группы не переведет его ни в один из символов $1, 2, \ldots, k$, т. е. символ $k+1$ подстановками данной группы переводится в иные символы, скажем, в $k+1, k+2, \ldots, k+l$. Про эти символы можно сказать то же, что и про $1, 2, \ldots, k$: подстановки данной группы переводят их только друг в друга (причем любой из них в любой), но не в иные символы. Если $k+l < m$, то мы подобным же образом рассуждаем дальше. Итак, *в интранзитивкой группе переставляемые символы разделяются на транзитивные системы, так что все подстановки данной группы переводят символы одной и той же системы только друг в друга (причем любой из них в любой).*

Заметим, что понятие транзитивности и интранзитивности относится только к группам подстановок. Абстрактная группа может представляться конкретно вообще и в виде транзитивной, и в виде интранзитивной группы подстановок. Представления, данные нами в § 196 и 201, транзитивны.

§ 209. Примитивность и импримитивность. Пусть $\mathfrak{G}$ — данная транзитивная группа подстановок n-го порядка и m-й степени и $\mathfrak{A} - 1$ — подгруппа группы $\mathfrak{G}$, оставляющая один из символов, например 1, без изменения. Если $\mathfrak{G}$ не имеет такой подгруппы, которая содержала бы $\mathfrak{A}_1$ как свою подгруппу, то $\mathfrak{G}$ называется *примитивной* группой; в противном случае $\mathfrak{G}$ — *импримитивная* группа. Мы рассмотрим этот последний случай; итак, пусть $\mathfrak{H}$ — подгруппа группы $\mathfrak{G}$, содержащая в свою очередь $\mathfrak{A}_1$ своей подгруппой, т. е.

$$\mathfrak{G} \supset \mathfrak{H} \supset \mathfrak{A}_1.$$

Группа $\mathfrak{H}$ кроме подстановок из $\mathfrak{A}_1$ должна содержать еще иные подстановки; пусть одна из них есть A_2 (обозначения как в § 208), тогда $\mathfrak{H}$ содержит и весь

комплекс $\mathfrak{A}_1 A_2$, т. е. все подстановки, переводящие 1 в 2, а также A_2^{-1} и всю группу $A_2^{-1}\mathfrak{A}_1 A_2$ оставляющую символ 2 без изменения. Предположим для общности, что в $\mathfrak{H}$ входят подстановки, переводящие символ 1 в $1, 2, 3, \ldots, k$, но не в иные символы; это значит, что $\mathfrak{H}$ состоит из комплексов $\mathfrak{A}_1$, $\mathfrak{A}A_2, \mathfrak{A}_1 A_3, \ldots, \mathfrak{A}_1 A_k$:

$$\mathfrak{H} = \mathfrak{A}_1 + \mathfrak{A}_1 A_2 + \mathfrak{A}_1 A_3 + \ldots + \mathfrak{A}_1 A_k.$$

Легко доказать, что любые два символа из ряда $1, 2, \ldots, k$ переводятся подстановками из $\mathfrak{H}$ друг в друга, но ни один из них не переходит в этих подстановках ни в какой иной [97]. Разложим группу $\mathfrak{G}$ по модулю $\mathfrak{H}$ слева:

$$\mathfrak{G} = \mathfrak{H} + \mathfrak{H}H_2 + \ldots + \mathfrak{H}H_i. \tag{19}$$

Рассмотрим подстановку H_2; пусть она переводит символы $1, 2, \ldots, k$ в какие-то символы $a_1, a_2, \ldots, a_k$; докажем, что эти последние символы все отличны от $1, 2, \ldots, k$. То, что a_1 не равен $1, 2, \ldots, k$, — понятно; пусть теперь a_3 равно, например 3, т. е. H_2 переводит 2 в 3; но тогда $A_2 H_2$ переведет 1 в 3, что невозможно, ибо все подстановки, переводящие 1 в 3, содержатся в H, а $A_2 H_2$ не содержится в $\mathfrak{H}$.

Легко убедиться, что все подстановки комплекса $\mathfrak{H}H_2$ переводят $1, 2, \ldots, k$ в $a_1, a_2, \ldots, a_k$, и обратно: каждая подстановка, переводящая символы $1, 2, \ldots, k$ в $a_1, a_2, \ldots, a_k$, содержится в $\mathfrak{H}H_2$; группа же $H_2^{-1}\mathfrak{H}H_2$ переводит символы $a_1, a_2, \ldots, a_k$ в самих себя.

Точно так же убедимся, что все подстановки из комплекса $\mathfrak{H}H_3$ переводят символы $1, 2, \ldots, k$ в какую-то новую систему $b_1, b_2, \ldots, b_k$, отличную от $1, 2, \ldots, k$ и от $a_1, a_2, \ldots, a_k$ и т. д.

Таким образом все наши m символов разделяются на i систем по k символов ($ik = m$), причем подстановки данной группы $\mathfrak{G}$ переставляют между собою символы только внутри систем и самые системы друг с другом, но не «разъединяют» символы одной и той же системы: если, например, подстановка G разъединяет символы $a_1, a_2, \ldots, a_k$ (т. е. часть их переводит в одну систему, а другую часть — в иные системы), то подстановка $H_2 G$ разъединит систему $1, 2, \ldots, k$; а эти символы никакой подстановкой из $\mathfrak{G}$ не разъединяются, что можно заключить из разложения (19): если $H_2 G$ находится в комплексе $\mathfrak{H}H_\lambda$, то эта подстановка переводит $1, 2, \ldots, k$ в λ-ю систему.

Системы $1, 2, \ldots, k$; $a_1, a_2, \ldots, a_k$; $b_1, b_2, \ldots, b_k$, ... называются *системами импримитивности*.

Это распадение символов на системы импримитивности в импримитивных группах может служить определением импримитивных групп. Именно, мы докажем, что если оно имеется, то группа импримитивна. Итак, пусть в данной транзитивной группе $\mathfrak{G}$ подстановок m символов, эти символы распадаются на i систем по k символов ($ik = m$):

$$\begin{array}{ccccc} 1 & 2 & 3 & \ldots & k, \\ a_1 & a_2 & a_3 & \ldots & a_k, \\ b_1 & b_2 & b_3 & \ldots & b_k, \\ \ldots & \ldots & \ldots & \ldots & \ldots \end{array}$$

[97] То-есть $\mathfrak{H}$ — интранзитивная группа, и $1, 2, \ldots, k$ — одна из ее транзитивных систем.

так что все подстановки из $\mathfrak{G}$? переставляют эти системы целиком друг с другом и переставляют символы внутри каждой отдельной системы. Рассмотрим все подстановки из $\mathfrak{G}$, оставляющие первую систему на своем месте, т. е. переставляющие $1, 2, 3, \ldots, k$ только между собою; произведение двух таких подстановок, очевидно, такая же подстановка, т. е. все эти подстановки образуют группу $\mathfrak{H}$, — подгруппу группы $\mathfrak{G}$. Среди подстановок группы $\mathfrak{H}$ находятся и все такие, которые совсем не меняют символ $\mathfrak{1}$, т. е. все подстановки группы $\mathfrak{A}_1$; итак,

$$\mathfrak{G} \supset \mathfrak{H} \supset \mathfrak{A}_1,$$

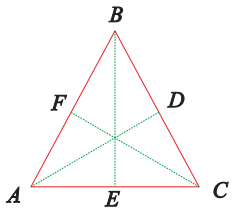
а это и показывает, что группа $\mathfrak{G}$ импримитивна.

Обращаем внимание на то, что понятие примитивности и импримитивности относится исключительно к транзитивным группам подстановок. Случается, что группу можно рассматривать как импримитивную несколькими способами, ибо может оказаться, что существует не одна подгруппа $\mathfrak{H}$, а несколько таких подгрупп группы $\mathfrak{G}$, содержащих своею подгруппою группу $\mathfrak{A}_1$.

§ 210. Другие примеры конкретных групп.

I. Группы вращений геометрических фигур.

Пример. Дан в плоскости равносторонний треугольник ABC (черт. 27); очевидно, что мы можем шестью способами привести его в совпадение с первоначальным положением: 1) оставить его неподвижным; 2) повернуть его вокруг его центра на 120° так, чтобы вершина B приняла положение A, C приняло положение B, A приняло положение C; 3) повернуть его вокруг центра на 240° (или же на 120° в обратную сторону), чтобы C приняло положение A, A — положение B, B — положение C; 4) повернуть его на 180° вокруг оси AD; 5) повернуть на 180° вокруг оси BE; 6) повернуть на 180° вокруг оси CF.



Черт. 27

Очевидно, что всякие два из этих шести вращения мы можем заменить одним из них же; например, произведенные последовательно вращения 2) и 5) можно заменить одним вращением 6). Таким образом, если рассматривать эти вращения как «элементы», а замену двух вращений одним равнодействующим как «действие» над этими элементами, то можно сказать, что эти шесть вращений составляют группу. Конечно, надо еще выяснить, выполнены ли для этого «действия» постулаты II и III § 191. Но здесь легко видеть, что получаемая группа 6-го порядка изоморфна группе всех шести подстановок трех символов, т. е. симметрической группе третьей степени (см. пример 2 § 196). Действительно, наши вращения по существу и являются подстановками трех вершин A, B, C треугольника, именно:

$$1)\ \begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix},\quad 2)\ \begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix},\quad 3)\ \begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix},\quad 4)\ \begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix},$$

$$5)\ \begin{pmatrix} A & B & C \\ C & B & A \end{pmatrix},\quad 6)\ \begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix}.$$

Более сложные примеры мы получим, если рассмотрим вращения правильных многогранников в пространстве, при которых они приходят в совпадение с

прежним положением. Здесь группа вращений тетраэдра изоморфна полусимметрической группе четвертой степени (12-го порядка); группа вращений октаэдра (а также и куба) изоморфна симметрической группе четвертой степени (24-го порядка); группа вращений икосаэдра (а также и додекаэдра) изоморфна полусимметрической группе пятой степени (60-го порядка).

II. Группы рациональных функций.

Пример. За «элементы» будем принимать такие шесть функций от x

$$\varphi_0 = x, \quad \varphi_1 = \frac{1}{x}, \quad \varphi_2 = 1 - x, \quad \varphi_3 = \frac{x}{x-1}, \quad \varphi_4 = \frac{x-1}{x}, \quad \varphi_5 = \frac{1}{1-x};$$

за «действие» над нашими элементами будем принимать подстановку в одну из функций другой функции вместо x; так, например: $\varphi_4\varphi_2 = \dfrac{(1-x)-1}{1-x} = \dfrac{-x}{1=x} = \dfrac{x}{x-1} = \varphi_3$. Легко убедиться, что эти шесть функций составляют группу, и при этом изоморфную той же симметрической группе третьей степени (пример 2 § 196). Можно показать также, что этой группе изоморфна группа матриц 2-го порядка:

$$E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad A_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix}, \quad A_3 = \begin{pmatrix} -1 & 0 \\ -1 & 1 \end{pmatrix},$$
$$B = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}, \quad C = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}.$$

Заметим, что эти шесть функций $\varphi_0, \ldots, \varphi_5$ представляют не что иное, как все шесть различных значений ангармонического отношения четырех точек на прямой, если всевозможными способами переставлять эти точки.

В приведенном примере x бы то независимым переменным. Ниже мы встретимся со случаями групп рациональных функций не от независимого переменного x, а от корней данного уравнения.

III. Примеры групп из теории чисел.

Пусть m — данный модуль; в качестве элементов рассматриваем классы чисел по модулю m, взаимно простых с m; число их равно $\varphi(m)$ (§ 120); в качестве действия рассматриваем обычное умножение: известно, что произведение чисел, взятых из двух определенных классов, есть число некоторого определенного третьего класса; следовательно, этим можно определить произведение самих классов. Для умножения верен не только ассоциативный, но и коммутативный закон; если мы берем только классы чисел, взаимно простых с m, то и постулат II § 191 верен для нашего умножения классов. Следовательно, эти $\varphi(m)$ классов составляют абвлеву группу. Роль главного элемента E здесь играет тот класс, к которому принадлежит число 1. Вместо того чтобы оперировать с классами, мы можем оперировать с числами, заменяя только знак равенства знаком сравнения. Следовательно, если a — число, взаимно простое с m, то его порядок (как элемента группы) есть такое наименьшее целое число $\mu > 0$, для которого $a^\mu = 1 (\mathrm{mod}\, m)$, т. е. μ — показатель, к которому принадлежит a по модулю m. Последствию из теоремы Лагранжа (§ 194) $\varphi(m)$ должно делиться на μ, а следовательно, $a^{\varphi(m)} \equiv 1 \pmod m$; это так называемая «*малая*» *теорема Ферма* (Fermat), которая, таким образом, весьма просто вытекает из теории групп.

IV. Группы матриц, или линейных подстановок.

О них уже упоминалось в главе IX, § 157. Наши подстановки n символов в сущности являются частным случаем матриц, как было уже выяснено в § 161. А отсюда и из § 196 следует, что всякая абстрактная конечная группа может быть представлена как группа матриц.

Эти представления очень важны и для самой абстрактной теории групп.

Можно было бы привести еще много различных примеров конкретных групп из всех областей математики; самые разнообразные «действия» в этих конкретных группах отвлеченно представляют собою одно и то же действие, подчиненное одним и тем же основным постулатам (§ 191). Возникает вопрос: возможны ли группы с другими действиями, подчиненными другим системам постулатов? Такие обобщения обычных групп действительно существуют; большинство их имеет также конкретные представления, позволяющие построить конкретно всевозможные типы этих групп; некоторые из них имеют и приложения, хотя эти приложения далеко не так значительны и многообразны, как приложения наших обычных групп.

Упражнения

237) Построить таблицу Кэли группы всех вращений тетраэдра, при которых он приходит в совпадение со своим прежним положением, н доказать, что эта группа изоморфна полусимметрической группе четвертой степени (12-го порядка).

,

238) Построить таблицу Кэли группы всех вращений квадрата в пространстве, при которых он приходит в совпадение со своим прежним положением, и представить эту группу как группу подстановок.

Отв. Искомая группа 8-го порядка, имеющая два элемента 4-го порядка и пять элементов 2-го порядка.

§ 211. Понятие о бесконечных группах. Обобщение понятия группы на случай, когда множество ее элементов бесконечно велико, принципиальных трудностей не представляет; но формально определить бесконечную группу теми четырьмя постулатами, которыми мы определяли конечный группы (§ 191), нельзя: в то время как для конечных групп закон однозначной обратимости и закон неограниченной обратимости являются следствиями один другого, в бесконечных группах только закон однозначной обратимости следует из закона неограниченной обратимости, но не обратно. Пусть, именно, для действия данной бесконечной группы верен закон неограниченной обратимости, т. е. уравнения $AX = B$, $YA = B$ при всяких A и B имеют решения X и Y. В таком случае пусть E — решение уравнения $AE = A$ при некотором данном A; но тогда

$$(XA)E = XA$$

при всяком X; по закону неограниченной обратимости можно выбрать X так, чтобы XA равнялось всякому элементу B; следовательно, будет

$$BE = B$$

для всякого B, т, е. E — правая единица для всех элементов группы. Пусть дано:

$$BA = CA;$$

выберем A' так, чтобы было

$$AA' = E$$

(это возможно по закону неограниченной обратимости); тогда

$$BAA' = CAA'$$

или $BE = CE$, т. е.

$$B = C.$$

Этим доказана левая сторона закона однозначной обратимости; аналогично докажем и правую сторону.

Что для бесконечных групп закон неограниченной обратимости не вытекает из закона однозначной обратимости, следует хотя бы из примера § 158 (гл. IX): положительные степени матрицы вообще образуют бесконечную систему, замкнутую в себе в том смысле, что произведение двух таких степеней одной и той же матрицы есть тоже степень той же матрицы; но эта система не есть группа; в ней неверен закон неограниченной обратимости, хотя закон однозначной обратимости верен.

Поэтому, определяя бесконечную группу, мы за постулат II берем закон неограниченной обратимости. Если же в бесконечной системе элементов с действием верны четыре постулата § 191, т. е. вместо закона неограниченной обратимости верен только закон однозначной обратимости, то такая система называется *полугруппой*. Поэтому, если мы в данной бесконечной группе выделили такую замкнутую в себе часть, что произведение всяких двух элементов этой части тоже принадлежит к этой части, то такая часть может оказаться еще не подгруппой данной группы, а только полугруппой; чтобы доказать, что она — группа, нужно выявить существование у нее единицы и обратного элемента ко всякому ее элементу.

Основные теоремы теории конечных групп вообще переносятся и на бесконечные группы — с некоторыми изменениями. Например, теорема Лагранжа (§ 194), конечно, не может быть формулирована в том же виде, как для конечных групп, но разложение группы по ее подгруппе («модулю»), взятой справа или слева, существует:

$$\mathfrak{A} = \mathfrak{B} + \mathfrak{B}A_2 + \mathfrak{B}A_3 + \dots;$$

здесь $\mathfrak{A}$ — данная бесконечная группа, $\mathfrak{B}$ — ее (конечная или бесконечная) подгруппа; но множество комплексов $\mathfrak{B}A_2$, $\mathfrak{B}A_3$, ... может быть конечным, а может быть и бесконечным (исчислимым или даже неисчислимым; в этом последнем случае индексы $2, 3, \dots$ имеют, конечно, только условный характер). Понятие инвариантной подгруппы, а также дополнительной группы, здесь тоже имеется, как и для конечных групп. Но композиционного ряда бесконечная группа может вообще и не иметь.

Рассмотрение групп геометрических преобразований привело к понятию о так называемых *непрерывных группах преобразований*, изучаемых в геометрии; их ввел первый Софус Ли (Sophus Lie). В настоящее время разработана также абстрактная теория непрерывных групп.

ГЛАВА ДВЕНАДЦАТАЯ

ОСНОВЫ ТЕОРИИ ГАЛУА

§ 212. Вводные замечания. Приступая к теоретическому исследованию алгебраических уравнений, нам важно с самого начала установить нашу точку зрения и наметить дальнейшие задачи. Мы будем исходить из четырех рациональных действий — сложения, вычитания, умножения и деления, считая их за основные. Вместе с данными числами, например $c_1, c_2, \ldots, c_m$, мы будем считать известными и все числа, получающиеся из этих данных посредством четырех рациональных действий, т. е., другими словами, и все рациональные функции от них с рациональными коэфициентами. Все такие функции составляют *область рациональности* (или *тело*, или *поле*, § 13), про которую мы скажем, что она *порождается* числами $c_1, c_2, \ldots, c_m$; обозначим эту область рациональности одною буквою $\mathbf{P}$. Пусть $\dfrac{f(c_1, c_2, \ldots, c_m)}{g(c_1, c_2, \ldots, c_m)}$ — такая рациональная функция от $c_1, c_2, \ldots, c_m$ с рациональными коэфициентами (где f и g — целые рациональные функции); ее значение при данных $c_1, c_2, \ldots, c_m$ вычислить легко. Гораздо труднее обратная задача: пусть известно значение C нашей функции, но неизвестно значение одного из ее аргументов, например c_1, т. е. пусть нам дано: $\dfrac{f(x, c_2, \ldots, c_m)}{g(x, c_2, \ldots, c_m)} = C$; это равенство представляет собою уравнение для x, которое мы всегда сможем привести к обычному виду, освободившись от знаменателя, раскрыв скобки, и т. п. Таким образом решение уравнения есть самое общее обратное действие к совокупности рациональных действий. С этой точки зрения мы и будем его рассматривать. Займемся изучением свойств этого действия. Первым делом следует заметить, что при решении уравнения мы выходим вообще из нашей основной области $\mathbf{P}$: если и $c_2, \ldots, c_m$ и C — числа из области $\mathbf{P}$, то решения x нашего уравнения вообще не будут принадлежать к области $\mathbf{P}$.

В частном случае, конечно, может случиться, что один или несколько корней нашего уравнения тоже принадлежат к области $\mathbf{P}$, т. е. выражаются рационально (т. е. как целые рациональные функции с рациональными коэфициентами) через данные количества $c_2, \ldots, c_m$, C; такие корни мы будем считать известными, хотя бы практически найти эти корни и было очень трудно. Если все корни нашего уравнения выражаются рационально через данные количества $c_2, \ldots, c_m$, C или через коэфициенты данного уравнения, то мы будем считать наше уравнение решенным. Итак, вместе с данным уравнением мы считаем за данное и некоторое тело $\mathbf{P}$, к которому принадлежат все коэфициенты данного уравнения; мы говорим, что нам дано уравнение в теле $\mathbf{P}$. Это тело $\mathbf{P}$ может быть телом, порождаемым всеми коэфициентами нашего уравнения, но может быть и шире его; мы

имеем право его еще больше расширять, т. е. присоединять к нему новые количества, но только так, чтобы оно не переставало быть телом. Количества из этого основного тела $\mathbf{P}$ мы будем называть *рациональными* (точнее — *относительно рациональными* в отличие от обычных абсолютно рациональных чисел). Задача наша состоит в том, чтобы так расширить это тело $\mathbf{P}$, чтобы в это расширенное тело попали все корни нашего уравнения, т. е. чтобы все корни нашего уравнения *сделались рациональными*. В этом случае мы будем считать уравнение решенным; левая часть данного уравнения должна в этом расширенном теле раскладываться на линейные множители (ср. § 76).

§ 213. Алгебраическое тело. Пусть $\mathbf{P}$ — данное тело; посмотрим, каким образом оно может быть расширено; для этого мы должны присоединить к $\mathbf{P}$ по крайней мере одно количество α, не принадлежащее к $\mathbf{P}$; но присоединяя α, мы должны одновременно присоединить к $\mathbf{P}$ и все рациональные функции от α с коэфициентами из $\mathbf{P}$ (для того чтобы после расширения снова получить тело); но все эти рациональные функции от α с коэфициентами из $\mathbf{P}$ составляют уже тело, содержащее само тело $\mathbf{P}$ делителем (ибо количество из $\mathbf{P}$ есть «целая рациональная функция нулевой степени от α»); это тело мы обозначим через $\mathbf{P}(\alpha)$ и будем его рассматривать как результат присоединения к $\mathbf{P}$ количества α. Подобно этому можно присоединить к $\mathbf{P}$ и несколько количеств $\alpha, \beta, \gamma, \ldots$, т. е. присоединить все рациональные функции от них с коэфициентами из $\mathbf{P}$; получим тело $\mathbf{P}(\alpha, \beta, \gamma, \ldots)$, причем, очевидно, что результат получится один и тот же, будем ли мы присоединять $\alpha, \beta, \gamma, \ldots$ последовательно (в каком угодно порядке) или присоединим все сразу.

Особенно интересен и важен случай, когда присоединяемое к телу $\mathbf{P}$ количество α есть корень алгебраического уравнения $f(x) = 0$ в теле $\mathbf{P}$ (т. е. с коэфициентами из $\mathbf{P}$). Такое количество α называется *алгебраическим количеством, происходящим из области рациональности* $\mathbf{P}$ [98]; по следствиям § 110 оно является корнем одного и только одного неприводимого уравнения $g(x) = 0$ в теле $\mathbf{P}$; пусть n — степень этого уравнения, а количества $\alpha, \alpha', \alpha'', \ldots, \alpha^{(n-1)}$ — его корни (все различные по следствию в § 110); эти корни называются *сопряженными* друг с другом алгебраическими количествами; n — степень каждого из количеств $\alpha, \alpha', \ldots, \alpha^{(n-1)}$.

Из основной теоремы теории симметрических функций (§ 133) следует, что всякая симметрическая функция от $\alpha, \alpha', \ldots, \alpha^{(n-1)}$ есть рациональное количество (т. е. находится в теле $\mathbf{P}$).

Например, если $\mathbf{P}$ — тело всех вещественных чисел, то сопряженные алгебраические количества здесь — обычные сопряженные комплексные числа $a + bi$ и $a - bi$; вещественное же количество (как количество из $\mathbf{P}$) не имеет сопряженных или сопряжено само с собой.

Если мы присоединяем к телу $\mathbf{P}$ алгебраическое количество n-й степени α, происходящее из области рациональности $\mathbf{P}$, то получаемое тело $\mathbf{P}(\alpha)$ называется *алгебраическим телом* n-й *степени* над $\mathbf{P}$; как мы видим, это понятие относительное зависит от выбора тела $\mathbf{P}$. Всякое количество из $\mathbf{P}(\alpha)$ есть рациональная

[98] Это понятие является обобщением понятия об алгебраическом числе; последнее мы имеем, если $\mathbf{P}$ — абсолютная область рациовальности (ср. § 75).

функция от α, т. е. имеет вид: $\dfrac{\varphi(\alpha)}{\psi(\alpha)}$, где φ и ψ — целые рациональные взаимно простые функции, причем если $g(x) = 0$ — неприводимое уравнение, которому удовлетворяет α, то функция ψ — взаимно простая с g последнее вытекает из § 110, следствия II. Из § 144 следует, что всякое количество из $\mathbf{P}(\alpha)$ представляется и только одним образом как целая рациональная функция от α степени не выше $n-1$ (ибо все выводы § 99, как легко убедиться, остаются верными, если вместо абсолютно рациональных чисел брать количества из любого данного тела $\mathbf{P}$).

§ 214. Теорема Абеля. Лемма. *Если нам дано несколько целых рациональных функций от n переменных: $f_1(x_1, x_2, \ldots, x_n)$, $f_2(x_1, x_2, \ldots, x_n)$, $\ldots$, $f_m(x_1, x_2, \ldots, x_n)$, то можно всегда дать переменным такие целые значения, при которых ни одна из этих функций не будет равна нулю.*

Доказательство. Для целых рациональных функций одного переменного эта теорема очевидна, так как целая рациональная функция одного переменного обращается в нуль при конечном числе значений своего аргумента (§ 50). Применим метод полной индукции: пусть для целых рациональных функций $n-1$ переменных эта теорема верна; расположим каждую из наших функций f_λ по переменному x_n: $f_\lambda = g_{\lambda 0}x_n^k + g_{\lambda 1}x_n^{k-1} + \ldots + g_{\lambda k}$; $g_{\lambda\mu}$ — целые рациональные функции от $n-1$ переменных $x_1, x_2, \ldots, x_{n-1}$; следовательно, по нашему предположению мы можем дать для $x_1, x_2, \ldots, x_{n-1}$ такие целые значения, при которых ни одна из функций $g_{\lambda\mu}$ не будет равна нулю; для этих значений $x_1, x_2, \ldots, x_{n-1}$ наши функции f_λ обращаются в целые рациональные функции от одного переменного x_n, не равные тождественно нулю. Следовательно, можно дать для x_n такое целое значение, при котором ни одна из функций f_λ не обратится в нуль, и лемма доказана.

Теорема Абеля. *Присоединение к телу $\mathbf{P}$ нескольких алгебраических количеств $\alpha, \beta, \gamma, \ldots$ равносильно присоединению некоторого одного алгебраического количества ω, или: $\mathbf{P}(\alpha, \beta, \gamma, \ldots) = \mathbf{P}(\omega)$.*

Иными словами, если $\alpha, \beta, \gamma, \ldots$ — несколько алгебраических количеств (относительно области $\mathbf{P}$), то можно всегда найти такую рациональную функцию от них в $\mathbf{P}$ (т. е. с коэфициентами из $\mathbf{P}$): $\omega = \Phi(\alpha, \beta, \gamma, \ldots)$, чтобы, обратно, $\alpha, \beta, \gamma, \ldots$ были рациональными функциями в $\mathbf{P}$ от ω: $\alpha = \varphi(\omega)$, $\beta = \psi(\omega)$, $\gamma = \chi(\omega)$, $\ldots$

Доказательство. Пусть α — алгебраическое количество a-й степени и пусть $\alpha, \alpha', \alpha'', \ldots$ — все сопряженные с α количества; пусть, далее, β b-й степени и $\beta, \beta', \beta'', \ldots$ — сопряженные с β количества; γ c-й степени и $\gamma, \gamma', \gamma'', \ldots$ — сопряженные с γ количества и т. д. Возьмем теперь $\omega = p\alpha + q\beta + r\gamma + \ldots$, где p, q, r, $\ldots$ — пока неопределенные коэфициенты; подставим сюда вместо α значения $\alpha, \alpha', \alpha'', \ldots$, вместо β значения $\beta, \beta', \beta'', \ldots$, вместо γ значения $\gamma, \gamma', \gamma'', \ldots$ и т. д., и будем комбинировать каждое значение для α с каждым значением для β, для γ, $\ldots$; получим всего $m = abc\cdots$ значений ω: $\omega, \omega', \omega'', \ldots, \omega^{(m-1)}$. Докажем, что можно дать коэфициентам p, q, r, $\ldots$ такие целые значения, при которых все эти от количеств будут различны между собой. Действительно, $\dfrac{m(m-1)}{2}$ разностей $\omega - \omega', \omega - \omega'', \omega' - \omega'', \ldots$ суть линейные функции от $p, q, r, \ldots$, не равные тождественно нулю. В таком случае по доказанной лемме можно дать для $p, q, r, \ldots$ такие целые значения, чтобы ни одна из наших разностей не обратилась в нуль;

ω как линейная комбинация величин $\alpha, \beta, \gamma, \ldots$ принадлежит полю $\mathbf{P}(\alpha, \beta, \gamma, \ldots)$:

$$\omega \subset \mathbf{P}(\alpha, \beta, \gamma, \ldots).$$

Количества $\omega, \omega', \omega'', \ldots$ служат корнями алгебраического уравнения

$$F(t) = (t-\omega)(t-\omega')(t-\omega'')\cdots(t-\omega^{(n-1)}) = 0,$$

коэфициенты которого, являясь симметрическими функциями от $\omega, \omega', \omega'', \ldots$, будут тем самым симметрическими функциями от $\alpha, \alpha', \alpha'', \ldots$, от $\beta, \beta', \beta'', \ldots$, от $\gamma, \gamma', \gamma'', \ldots$ и т. д., т. е. выразятся рационально через коэфициенты уравнений для α, для β, для γ и т. д., т. е. будут количествами из $\mathbf{P}$. Следовательно, и ω будет алгебраическим количеством относительно $\mathbf{P}$.

Пусть теперь θ — некоторая рациональная функция от $\alpha, \beta, \gamma, \ldots$ в теле $\mathbf{P}$; подставив вместо α значения $\alpha, \alpha', \alpha'', \ldots$, вместо β значения $\beta, \beta', \beta'', \ldots$ и т. д., мы получим кроме θ еще значения $\theta', \theta'', \ldots, \theta^{(m-1)}$; пусть при этом обозначения выбраны так, что θ' соответствует тем же подстановкам для α, для β, для γ и т. д., что и в ω', θ'' — тем же, что и в ω'', и т. д. Количества $\theta, \theta', \theta'', \ldots, \theta^{(m-1)}$ могут оказаться и не все различными. Возьмем теперь функцию

$$F(t)\cdot\left\{\frac{\theta}{t-\omega}+\frac{\theta'}{t-\omega'}+\ldots+\frac{\theta^{(m-1)}}{t-\omega^{(m-1)}}\right\} = \Psi(t).$$

Очевидно, что $\Psi(t)$ — целая рациональная функция от t, коэфициенты которой симметрические функции от $\alpha, \alpha', \alpha'', \ldots$, от $\beta, \beta', \beta'', \ldots$ и т. д., т. е. все эти коэффициенты из $\mathbf{P}$. Положив $t = \omega$, получим:

$$\theta \cdot F'(\omega) = \Psi(\omega); \quad \text{откуда} \quad \theta = \frac{\Psi(\omega)}{F'(\omega)}.$$

[$F'(\omega) \neq 0$, так как ω — -простой корень уравнения $F(t) = 0$, которое вообще не имеет кратных корней.] Итак, всякая рациональная функция от $\alpha, \beta, \gamma, \ldots$ в теле $\mathbf{P}$ есть рациональная функция от ω в теле $\mathbf{P}$; в частности сами количества $\alpha, \beta, \gamma, \ldots$ суть рациональные функции от ω, и теорема доказана.

Пример. Дано $\mathbf{P}(\sqrt{2}, \sqrt{3}) = \mathbf{P}(\omega)$, найти ω, т. е. найти такую рациональную функцию от $\sqrt{2}$ и $\sqrt{3}$, чтобы через нее $\sqrt{2}$ и $\sqrt{3}$ тоже выражались рационально. Здесь имеем: $\alpha = \sqrt{2}$, $\alpha' = -\sqrt{2}$, $\beta = \sqrt{3}$, $\beta' = -\sqrt{3}$. За ω можно взять $\omega = \sqrt{2}+\sqrt{3}$; тогда $\omega' = \sqrt{2}-\sqrt{3}$, $\omega'' = -\sqrt{2}+\sqrt{3}$, $\omega''' = -\sqrt{2}-\sqrt{3}$. Вычисляем:

$$\begin{aligned} F(t) &= (t-\sqrt{2}-\sqrt{3})(t-\sqrt{2}+\sqrt{3})(t+\sqrt{2}-\sqrt{3})(t+\sqrt{2}+\sqrt{3}) = \\ &= t^4 - 10t^2 + 1, \end{aligned}$$

$$F(t)\cdot\left\{\frac{\sqrt{2}}{t-\omega}+\frac{\sqrt{2}}{t-\omega'}-\frac{\sqrt{2}}{t-\omega''}-\frac{\sqrt{2}}{t-\omega'''}\right\} = \Psi(t) = 8(t^2+1);$$

отсюда при $t = \omega$

$$\sqrt{2} = \frac{2(\omega^2+1)}{\omega^3-5\omega}.$$

Чтобы найти формулу для $\sqrt{3}$, можно поступить так же; но можно и проще найти

$$\sqrt{3} = \omega - \sqrt{2} = \frac{\omega^4-7\omega^2-2}{\omega^3-5\omega} = \frac{3(\omega^2-1)}{\omega^3-5\omega}.$$

Предлагаете проверить формулы для $\sqrt{2}$ и $\sqrt{3}$, подставив вместо ω его значение $\sqrt{2}+\sqrt{3}$ и действительно вычислив правые части.

§ 215. Свойства алгебраических тел. Теорема 1. *Всякое количество из алгебраического тела* $\mathbf{P}(\alpha)$ *есть алгебраическое количество (относительно* $\mathbf{P}$*).*

Доказательство. Пусть $\mathbf{P}(\alpha)$ n-й степени и $\alpha, \alpha', \alpha'', \ldots, \alpha^{(n-1)}$ — сопряженные с α количества. Пусть $\theta \subset \mathbf{P}(\alpha)$; θ — радиональная функция от α в теле $\mathbf{P}$: $\theta = \varphi(\alpha)$; возьмем: $\theta' = \varphi(\alpha')$, $\ldots \theta^{(n-1)} = \varphi(\alpha^{(n-1)}$; эти количества $\theta, \theta', \ldots, \theta^{(n-1)}$ (которые могут и не быть все различны, в то время как $\alpha, \alpha', \ldots, \alpha^{(n-1)}$ все различны) назовем тоже *сопряженными* (относительно тела $\mathbf{P}$). Уравнение

$$F(t) = (t-\theta)(t-\theta')\cdots(t-\theta^{(n-1)}) = 0$$

есть уравнение в теле $\mathbf{P}$, ибо коэфициенты его — симметрические функции от $\theta, \theta', \ldots, \theta^{(n-1)}$, а значит, и от $\alpha, \alpha', \alpha'', \ldots, \alpha^{(n-1)}$; один из его корней θ. Следовательно, θ — алгебраическое количество относительно $\mathbf{P}$.

Уравнение $F(t) = 0$ может быть и приводимым; пусть $\Phi(t)$ — неприводимый в $\mathbf{P}$ делитель $F(t)$, одним из корней которого является θ; следовательно, $\Phi(\theta) = 0$, или $\Phi(\varphi(\alpha)) = 0$; но $\Phi(\varphi(x))$ — целая рациональная функция в теле $\mathbf{P}$, и уравнение $\Phi(\varphi(x)) = 0$ имеет общий корень α с неприводимым уравнением $f(x) = 0$ для α; по § 110, следствию II и все корни уравнения $f(x) = 0$, т. е. все количества $\alpha, \alpha', \alpha'', \ldots, \alpha^{(n-1)}$, должны удовлетворять тому же уравнению $\Phi(\varphi(x)) = 0$, т. е. и $\Phi(\varphi(\alpha')) = 0$, $\ldots$, $\Phi(\varphi(\alpha^{(n-1)}) = 0$, или $\Phi(\theta') = 0$, $\ldots$, $\Phi(\theta^{(n-1)} = 0$. Но тогда по следствию III § 110 заключаем: $F(t) = \Phi(t)^k$ (высшие коэфициенты мы берем равными единице). Следовательно:

Теорема 2. *Все сопряженные относительно тела* $\mathbf{P}(\alpha)$ *количества* $\theta, \theta', \ldots, \theta^{(n-1)}$*, или различны, или распадаются на* l *систем по* k *равных количеств, где* $kl = n$*.*

Следствие. Если все сопряженные количества равны:

$$\theta = \theta' = \ldots = \theta^{(n-1)},$$

то θ — рациональное количество (т. е. $\theta \subset \mathbf{P}$).

Доказательство. Тогда $k = n$; следовательно, $l = 1$, т. е. θ удовлетворяет уравнению 1-й степени в $\mathbf{P}$.

Теорема 3. *Если все сопряженные количества* $\theta, \theta', \ldots, \theta^{(n-1)}$*, различны (т. е.* $k = l$*,* $l = n$*), то и* α *выражается рационально через* θ *и* $\mathbf{P}(\theta) = \mathbf{P}(\alpha)$*.*

Доказательство. Возьмем функцию:

$$F(t)\cdot\left\{\frac{\alpha}{t-\theta} + \frac{\alpha'}{t-\theta'} + \ldots + \frac{\alpha^{(n-1)}}{t-\theta^{(n-1)}}\right\} = \Psi(t);$$

как и в теореме Абеля, выводим, что $\Psi(t)$ — целая рациональная функция от t в теле $\mathbf{P}$; отсюда при $t = \theta$; $\alpha = \dfrac{\Psi(\theta)}{F'(\theta)}$, т. е. α (а следовательно, и всякая рациональная функция от α) выражается рационально через θ. Так как, и обратно, θ есть рациональная функция от α, то получаем $\mathbf{P}(\theta) = \mathbf{P}(\alpha)$.

Такое количество θ, через которое все количества из тела $\mathbf{P}(\alpha)$ выражаются рационально (в $\mathbf{P}$), называется *первообразным* количеством тела $\mathbf{P}(\alpha)$. Само количество α — первообразное для тела $\mathbf{P}(\alpha)$. Мы видим: количество θ тогда и только

тогда первообразное количество алгебраического тела $\mathbf{P}(\alpha)$ n-й степени, если все сопряженные [относительно $\mathbf{P}(\alpha)$] с θ количества различны.

Следствие. Алгебраическое тело n-й степени над $\mathbf{P}$ не может иметь делителем тоже алгебраическое тело n-й степени над $\mathbf{P}$ кроме самого себя.

Доказательство. Если θ первообразное количество такого делителя, то θ удовлетворяет неприводимому уравнению n-й степени в $\mathbf{P}$; но тогда θ — первообразное количество самого данного тела.

Теорема 4. *Всякий делитель $\mathbf{P}'$ алгебраического тела $\mathbf{P}(\alpha)$, заключающий тело $\mathbf{P}$, есть тоже алгебраическое тело (над $\mathbf{P}$).*

Доказательство. Пусть $\theta \in \mathbf{P}'$; следовательно, $\theta \subset \mathbf{P}(\alpha)$, т. е. (по теореме 1) θ — алгебраическое количество (относительно $\mathbf{P}$); $\mathbf{P}(\theta)$ — алгебраическое тело; если $\mathbf{P}(\theta) = \mathbf{P}'$, то теорема доказана. Если $\mathbf{P}(\theta) \subset \mathbf{P}'$, то пусть $\theta_1 \subset \mathbf{P}'$, но не заключается в $\mathbf{P}(\theta)$; берем $\mathbf{P}(\theta, \theta_1)$ по теореме Абеля это алгебраическое тело; если оно равно $\mathbf{P}'$, то теорема доказана. Если же $\mathbf{P}(\theta, \theta_1) \subset \mathbf{P}'$, то пусть θ_2 — количество из $\mathbf{P}'$, но не из $\mathbf{P}(\theta, \theta_1)$; берем $\mathbf{P}(\theta, \theta_1, \theta_2)$ и т. д. Имеем: $\mathbf{P}(\theta) \subset \mathbf{P}(\theta, \theta_1) \subset \mathbf{P}(\theta, \theta_1, \theta_2) \subset \ldots$; степени этих алгебраических тел целые числа, которые увеличиваются, но остаются меньше степени тела $\mathbf{P}(\alpha)$; следовательно, их ряд конечен, и при некотором λ мы найдем: $\mathbf{P}(\theta, \theta_1, \theta_2, \ldots, \theta_\lambda) = \mathbf{P}'$, т. е. $\mathbf{P}'$ — алгебраическое тело.

Тело $\mathbf{P}(\alpha)$, совсем, не имеющее делителей, содержащих $\mathbf{P}$, называется *первообразным* (*примитивным*); в таком теле все количества за исключением рациональных (т. е. количеств из $\mathbf{P}$) первообразны. Очевидно, что всякое алгебраическое тело простой степени первообразно; но обратное заключение неверно.

Пример. Пусть $\mathbf{P}$ — абсолютная область рациональности, $\alpha = \sqrt[4]{2}$; α удовлетворяет неприводимому в $\mathbf{P}$ уравнению $x^4 - 2 = 0$; сопряженные с α количества: $\alpha' = -\sqrt[4]{2}$, $\alpha'' = i\sqrt[4]{2}$, $\alpha''' = -i\sqrt[4]{2}$. Тело $\mathbf{P}(\alpha)$ не первообразно; действительно, для $\theta = \alpha^2 = \sqrt{2}$ имеем $\theta' = \sqrt{2} = \theta$, $\theta'' = \theta''' = -\sqrt{2}$, т. е. здесь $k = l = 2$. Тело $\mathbf{P}(\sqrt{2})$ есть делитель данного тела $\mathbf{P}(\sqrt[4]{2}$; для этого последнего $\theta = \sqrt{2}$ — не первообразное количество. Но количество $\eta = \alpha^2 + \alpha = \sqrt{2} + \sqrt[4]{2}$ — первообразное для тела $\mathbf{P}(\sqrt[4]{2})$, так как здесь все сопряженные с η количества различны: $\eta' = \sqrt{2} - \sqrt[4]{2}$, $\eta'' = -\sqrt{2} + i\sqrt[4]{2}$, $\eta''' = -\sqrt{2} - i\sqrt[4]{2}$. Выразим α через η по способу, указанному в теореме 3; имеем:

$$F(t) = (t-\eta)(t-\eta')(t-\eta'')(t-\eta''') = t^4 - 4t^2 - 8t + 2,$$

$$\Psi(t) = F(t) \cdot \left\{ \frac{\alpha}{t-\eta} + \frac{\alpha'}{t-\eta'} + \frac{\alpha''}{t-\eta''} + \frac{\alpha'''}{t-\eta'''} \right\} = 8(2t+1);$$

$$F'(t) = 4t^3 - 8t - 8 = 4(t^2 - 2t - 2);$$

следовательно,

$$\alpha = \frac{\Psi(\eta)}{F'(\eta)} = \frac{2(2\eta+1)}{\eta^3 - 2\eta - 2}.$$

§ 216. Нормальное тело. Резольвента Галуа. Если $\alpha, \alpha', \ldots, \alpha^{(n-1)}$ сопряженные алгебраические количества (относительно $\mathbf{P}$), то тела $\mathbf{P}(\alpha)$, $\mathbf{P}(\alpha')$, …, $\mathbf{P}(\alpha^{(n-1)})$ называются *сопряженными алгебраическими телами*, они вообще различны; $\mathbf{P}(\alpha) = \mathbf{P}(\alpha')$ тогда и только тогда, если α' рациональная функция в $\mathbf{P}$ от α, а α — рациональная функция в $\mathbf{P}$ от α'; но одно из этих двух условий влечет

за собою и другое: пусть α' — рациональная функция от α; тогда, следовательно, $\mathbf{P}(\alpha') \subset \mathbf{P}(\alpha)$; но оба эти тела n-й степени, значит, по следствию из теоремы 3 $\mathbf{P}(\alpha') = \mathbf{P}(\alpha)$.

Особенно интересен случай, когда все сопряженные алгебраические тела совпадают: $\mathbf{P}(\alpha) = \mathbf{P}(\alpha') = \ldots = \mathbf{P}(\alpha^{(n-1)})$; такое тело $\mathbf{P}(\alpha)$ называется *нормальным*, и соответственно неприводимое уравнение — *нормальное*; каждый из его корней $\alpha, \alpha', \ldots, \alpha^{(n-1)}$ выражается рационально через каждый другой из этих корней; для этого необходимо и достаточно, чтобы все корни $\alpha, \alpha', \ldots, \alpha^{(n-1)}$ выражались рационально через некоторый один из них, например через α.

Пример 1. Квадратное уравнение $ax^2 + bx + c = 0$ в любой области рациональности $\mathbf{P}$ всегда нормально: если α_1 и α_2 — его корни, то всегда $\alpha_2 = -\dfrac{b}{a} - \alpha_1$, т. е. α_2 выражается рационально через α_1 и, конечно, обратно.

Пример 2. В абсолютной области рациональности уравнение деления окружности $\Phi_m(x) = 0$ (§ 120) нормально: оно неприводимо, и все его корни являются степенями одного из них (§ 120–122).

Теорема. *Если $F(x) = 0$ уравнение в $\mathbf{P}$ m-й степени без кратных корней, то, присоединив к $\mathbf{P}$ все корни $\alpha_1, \alpha_2, \ldots, \alpha_m$ этого уравнения $F(x) = 0$, мы получим нормальное тело $\mathbf{P}(\alpha_1, \alpha_2, \ldots, \alpha_m)$.*

Заметим, что при этом $F(x) = 0$ не предполагается непременно неприводимым.

Доказательство. Возьмем некоторую рациональную функцию $\theta_1 = \Phi(\alpha_1, \alpha_2, \ldots, \alpha_m)$ в теле $\mathbf{P}$; переставляя в функции Φ всевозможными способами $\alpha_1, \alpha_2, \ldots, \alpha_m$, мы получим соответственно этим $m!$ перестановкам $m!$ количеств: $\theta_1, \theta_2, \ldots, \theta_{m!}$. Как и при доказательстве теоремы Абеля, мы убедимся, что функцию Φ можно выбрать так, чтобы все эти $m!$ количеств были различны. Имеем

$$G(x) = (x - \theta_1)(x - \theta_2) \cdots (x - \theta_{m!}) = 0$$

— уравнение в $\mathbf{P}$, которому удовлетворяет θ_1). Пусть $\omega_1 = \Omega(\alpha_1, \alpha_2, \ldots, \alpha_m)$— любая рациональная функция от $\alpha_1, \alpha_2, \ldots, \alpha_m$ в теле $\mathbf{P}$; пусть $\omega_2, \omega_3, \ldots, \omega_{m!}$ получаются из ω_1 тем же путем, что и $\theta_2, \theta_3, \ldots, \theta_{m!}$ из θ_1.

Возьмем

$$G(x) \cdot \left\{ \frac{\omega_1}{x - \theta_1} + \frac{\omega_2}{x - \theta_2} + \ldots + \frac{\omega_{m!}}{x - \theta_{m!}} \right\} = \Psi(x);$$

как и в § 214 и 215, убедимся, что $\Psi(x)$ — целая рациональная функция в теле $\mathbf{P}$. Это показывает, что При $x = \theta_1$ получаем: $\omega_1 = \dfrac{\Psi(\theta_1)}{G'(\theta_1)}$. Это показывает, что θ — первообразное количество в теле $\mathbf{P}(\alpha_1, \alpha_2, \ldots, \alpha_m)$, т. е.

$$\mathbf{P}(\alpha_1, \alpha_2, \ldots, \alpha_m) = \mathbf{P}(\theta_1),$$

а так как $\theta_2, \ldots, \theta_{m!}$ тоже находятся в этом теле (ибо они — рациональные функции от $\alpha_1, \alpha_2, \ldots, \alpha_m$), то они выражаются рационально через θ_1. Уравнение $G(x) = 0$ может быть и приводимо; пусть $g(x)$ — тот неприводимый множитель полинома $G(x)$, который имеет корнем θ_1; уравнение $g(x) = 0$ нормально (ибо его корни — часть всех корней $\theta_1, \theta_2, \ldots$, и все они выражаются рационально через θ_1), и тело $\mathbf{P}(\theta_1)$ нормально, что и требовалось доказать.

Уравнение $g(x) = 0$ называется *резольвентой Галуа* (Galois) данного уравнения $F(x) = 0$; оно нормально; степень $g(x)$ $\nu \leq m$. Нормальное уравнение является своей собственной резольвентой Галуа.

Теорема. *Уравнение $g(x) = 0$ тогда и только тогда является резольвентой Галуа данного уравнения $F(x) = 0$ (без кратных корней), если: 1) $g(x)$ неприводимо (в $\mathbf{P}$); 2) все корни уравнения $F(x) = 0$ выражаются рационально (в $\mathbf{P}$) через один какой-нибудь корень уравнения $g(x) = 0$; 3) один из корней уравнения $g(x) = 0$ есть рациональная функция (в $\mathbf{P}$) от корней уравнения $F(x) = 0$.*

Доказательство. Пусть $\alpha_1, \alpha_2, \ldots, \alpha_m$ — корни уравнения $F(x) = 0$, а $\theta_1, \theta_2, \ldots$, θ_ν — корни уравнения $g(x) =$Q; пусть $\alpha_1 = \varphi_1(\theta_1)$, $\alpha_2 = \varphi_2(\theta_1)$, $\ldots \alpha_m = \varphi_m(\theta_1)$, $\theta_2 = \Psi(\alpha_1, \alpha_2, \ldots, \alpha_m)$; по 2) $\mathbf{P}(\alpha_1, \alpha_2, \ldots, \alpha_m) \subset \mathbf{P}(\theta_1)$, по 3) $\mathbf{P}(\alpha_1, \alpha_2, \ldots, \alpha_m) \supset P(\theta_2)$; но так как степени тел $\mathbf{P}(\theta_1)$ и $\mathbf{P}(\theta_2)$ равны, то должно быть:

$$\mathbf{P}(\alpha_1, \alpha_2, \ldots, \alpha_m) = \mathbf{P}(\theta_1);$$

следовательно, по предыдущей теореме, $\mathbf{P}(\theta_1)$ — нормальное тело, т. е. оно совпадает со всеми своими сопряженными, и значит $g(x) = 0$ нормальное уравнение, — резольвента Галуа уравнения $F(x) = 0$. Обратное очевидно.

Мы видим, что с выставленной нами в § 212 точки зрения решение уравнения $F(x) = 0$ и решение уравнения $g(x) = 0$ — одна и та же задача: решив одно из них, мы найдем корни другого рациональны путем. Но уравнение $g(x) = 0$ имеет то преимущество, что для его решения достаточно найти только один его корень; остальные определятся рациональным путем.

Пример. Дано уравнение $x^3 - 3x + 3 = 0$. Найти его резольвенту Галуа. По § 124 заключаем, что уравнение наше не имеет кратных корней. Пусть α_1, α_2, α_3 — его корни; построим функцию θ_1 («функцию Галуа») следующим образом: $\theta_1 = \alpha_1 - \alpha_2$; тогда: $\theta_2 = \alpha_1 - \alpha_3$, $\theta_3 = \alpha_2 - \alpha_3$, $\theta_4 = \alpha_2 - \alpha_1$, $\theta_5 = \alpha_3 - \alpha_1$, $\theta_6 = \alpha_3 - \alpha_2$; все эти количества различны;

$$\begin{aligned}
G(x) &= (x-\theta_1)(x-\theta_2)\cdots(x-\theta_6) = \\
&= (x-\alpha_1+\alpha)(x-\alpha_1+\alpha_3)(x-\alpha_2+\alpha_3)(x-\alpha_2+\alpha_1)(x-\alpha_3+\alpha_1)(x-\alpha_3+\alpha_2) = \\
&= [x^2-(\alpha_1-\alpha_2)^2][x^2-(\alpha_1-\alpha_3)^2][x^2-(\alpha_2-\alpha_3)^2] = \\
&= x^6 - [(\alpha_1-\alpha_2)^2+(\alpha_1-\alpha_3)^2+(\alpha_2-\alpha_3)^2]x^4 + \\
&+ [(\alpha_1-\alpha_2)^2(\alpha_1-\alpha_3)^2+(\alpha_1-\alpha_2)^2(\alpha_2-\alpha_3)^2+(\alpha_1-\alpha_3)^2(\alpha_2-\alpha_3)^2]x^2 - \\
&- (\alpha_1-\alpha_2)^2(\alpha_1-\alpha_3)^2(\alpha_2-\alpha_3)^2 = x^6 - 18x^4 + 162x^2 - 135.
\end{aligned}$$

Этот полином неприводим; таким образом уравнение $x^6 - 18x^4 + 162x^2 - 135 = 0$ есть резольвента Галуа данного уравнения.

§ 217. Группа Галуа и ее свойства. Займемся теперь нормальным уравнением $g(x) = 0$ ν-й степени с корнями $\theta_1, \theta_2, \ldots, \theta_\nu$; в теле $\mathbf{P}$ все эти корни выражаются рационально через один из них: $\theta_2 = \varphi_2(\theta_1)$, $\theta_3 = \varphi_3(\theta_1)$, $\ldots$, $\theta_\nu = \varphi_\nu(\theta_1)$; $\varphi_2, \varphi_3, \ldots, \varphi_\nu$ — некоторые рациональные функции в $\mathbf{P}$. Обозначим еще $\theta_1 = \varphi_1(\theta_1)$; φ_1 есть так называемая «тождественная» функция. Имеем: $g(\theta_\nu) = 0$, или $g(\varphi_\lambda(\theta_1)) = 0$, но $g(\varphi_\lambda(x))$ есть некоторая рациональная функция в $\mathbf{P}$, т. е. $g(\varphi_\lambda(x)) = 0$ — алгебраическое уравнение в $\mathbf{P}$ (если оно имеет дробные члены, то можно, как обычно, избавиться в нем от дробей), которое имеет корень θ_1; значит,

по § 110, следствию II, и все корни $\theta_\varkappa$ неприводимого уравнения $g(x)=0$ также удовлетворяют уравнению $g(\varphi_\lambda(x))=0$, т. е. $g(\varphi_\lambda(\theta_\varkappa))=0$, т. е. $\varphi_\lambda(\theta_\varkappa)$ — один из корней уравнения $g(x)=0$, например, $\varphi_\lambda(\theta_\varkappa)=\theta_\mu$, или $\varphi_\lambda(\varphi_\varkappa(\theta_1))=\varphi_\mu(\theta_1)$. Таким образом результат подстановки в одну из функций φ_λ вместо θ_1 другой функции $\varphi_\varkappa(\theta_1)$ дает некоторую третью функцию $\varphi_\mu(\theta_1)$ из тех же ν функций. По тому же следствию II в § 110 получаем, что и для всякого θ_ρ $(\rho=1,2,\dots,\nu)$ будет $\varphi_\lambda(\varphi_\varkappa(\theta_\rho))=\varphi_\mu(\theta_\rho)$; но для любого числа x это равенство вообще неверно: оно — не тождество. Таким образом, если за аргументы наших функций брать только количества $\theta_1,\theta_2,\dots,\theta_\nu$ и рассматривать наши функции как данные «элементы», а подстановку одной в другую — как «действие» над ними, то групповой постулат I для них выполнен (§ 191); постулат IV тоже выполнен, ибо множество наших элементов конечно. Докажем, что и постулаты II и III выполнены. Равенство $\varphi_\varkappa(\varphi_\lambda(\theta_\rho))=\varphi_\mu(\theta_\rho)$ можно переписать так: $\varphi_\varkappa(\varphi_\lambda(\theta_\rho))=(\varphi_\varkappa\varphi_\lambda)(\theta_\rho)$, если функцию φ_μ обозначим через $\varphi_\varkappa\varphi_\lambda$ как результат композиции $\varphi_\varkappa$ и φ_λ. Далее, $\theta_\rho=\varphi_\rho(\theta_1)$; следовательно, $\varphi_\varkappa(\varphi_\lambda\varphi_\rho(\theta_1))=(\varphi_\varkappa\varphi_\lambda)\varphi_\rho(\theta_1)$; по § 110, следствию II это равенство верно и для любого из корней $\theta_1,\theta_2,\dots,\theta_\nu$; следовательно, можно вообще написать (без аргументов) $\varphi_\varkappa(\varphi_\lambda\varphi_\rho)=(\varphi_\varkappa\varphi_\lambda)\varphi_\rho$ для любых $\varkappa,\lambda,\rho$; это и есть ассоциативный закон, или постулат III. Для доказательства постулата II заметим, что, так как $\varphi_1(\theta_1),\varphi_2(\theta_1),\dots,\varphi_\nu(\theta_1)$, все различны, то и $\varphi_1(\theta_\lambda),\varphi_2(\theta_\lambda),\dots,\varphi_\nu(\theta_\lambda)$, при любом $\lambda=1,2,\dots,\nu$ будут все различны. Именно, из $\varphi_\varkappa(\theta_\lambda)=\varphi_\mu(\theta_\lambda)$ мы заключаем (по тому же следствию II § 110), что и $\varphi_\varkappa(\theta_1)=\varphi_\mu(\theta_1)$. Но равенство $\varphi_\varkappa\varphi_\lambda=\varphi_\nu\varphi_\lambda$ можно иначе написать так: $\varphi_\varkappa\varphi_\lambda(\theta_1)=\varphi_\mu\varphi_\lambda(\theta_1)$ или (без аргумента) $\varphi_\varkappa\varphi_\lambda=\varphi_\mu\varphi_\lambda$; таким образом из этого равенства следует: $\varphi_\varkappa=\varphi_\mu$, и одна сторона постулата II доказана. Так как количества $\varphi_1(\theta_\lambda),\varphi_2(\theta_\lambda),\dots,\varphi_\nu(\theta_\lambda)$ все различны и число их равно ν, то они представляют собою все корни $\theta_1,\theta_2,\dots,\theta_\nu$, только в другом порядке; среди них, например, имеется корень θ_1, т. е. для некоторого σ $\varphi_\sigma(\theta_\lambda)=\theta_1$, или $\varphi_\sigma\varphi_\lambda(\theta_1)=\varphi_1(\theta_1)$, или просто $\varphi_\sigma\varphi_\lambda=\varphi_1$; эта функция φ_σ является, таким образом, «обратной» к φ_λ (опять-таки напоминаем, — только для значений $\theta_1,\theta_2,\dots,\theta_\nu$ аргумента); обозначим ее через φ_λ^{-1}; следовательно, $\varphi_\lambda^{-1}\varphi_\lambda=\varphi_1$. Можно доказать, что и $\varphi_\lambda\varphi_\lambda^{-1}=\varphi_1$. Пусть теперь: $\varphi_\lambda\varphi_\varkappa=\varphi_\lambda\varphi_\mu$, тогда $\varphi_\lambda^{-1}\varphi_\lambda\varphi_\varkappa=\varphi_\lambda^{-1}\varphi_\lambda\varphi_\mu$, или $\varphi_1\varphi_\varkappa=\varphi_1\varphi_\mu$; но, очевидно, $\varphi_1\varphi_\varkappa=\varphi_\varkappa$, $\varphi_1\varphi_\mu=\varphi_\mu$; следовательно, $\varphi_\varkappa=\varphi_\mu$, и другая сторона постулата II тоже доказана.

Таким образом наши «элементы» $\varphi_1,\varphi_2,\dots,\varphi_\nu$ образуют группу. Эта группа и есть *группа Галуа* уравнения $g(x)=0$, или данного уравнения

Пример 1. Возьмем уравнение деления окружности на пять равных частей (§ 120): $\Phi_5(x)=x^4+x^3+x^2+x+1=0$; его корни θ_1, θ_2, θ_3, θ_4 находятся в следующей связи: $\theta_2=\theta_1^2$, $\theta_3=\theta_1^3$, $\theta_4=\theta_1^4$ (заметим, что $\theta_1^5=1$); следовательно, $\varphi_1(x)=x$, $\varphi_2(x)=x^2$, $\varphi_3(x)=x^3$, $\varphi_4(x)=x^4$; эти функции φ_1, φ_2, φ_3, φ_4 составляют группу, если за их аргумент брать θ_1 или θ_2, или θ_3, или θ_4; но для любого x они, конечно, не составляют группы, например, $\varphi_2(\varphi_4(x))=(x^4)^2=x^8$ уже новая функция, тогда как $\varphi_2(\varphi_4(\theta_1))=(\theta_1^4)^2=\theta_1^8=\theta_1^3=\varphi_3(\theta_1)$, ибо $\theta_1^5=1$.

Пример 2. Возьмем уравнение $g(x)=(x^2-x+1)^3-a(x^2-x)^2=0$; перепишем его в таких двух формах:

$$\left(x+\frac{1}{x}-1\right)^3-a\left(x+\frac{1}{x}-2\right)^2=0, \qquad (a)$$

$$-[x(1-x)-1]^2-a[x(1-x)]^2=0. \qquad (b)$$

Из формы (a) видно, что, если x — корень нашего уравнения, то и $\dfrac{1}{x}$ — тоже его корень; а форма (b) говорит, что и $1-x$ тоже будет его корнем. Таким образом, если один из корней нашего уравнения обозначим через θ_0, то корнями будут также:

$$\theta_1 = \frac{1}{\theta_0}, \quad \theta_2 = 1 - \theta_0, \quad \theta_5 = \frac{1}{1-\theta_0}, \quad \theta_4 = 1 - \frac{1}{\theta_0} = \frac{\theta_0 - 1}{\theta_0},$$

$$\theta_3 = \frac{1}{\dfrac{\theta_0 - 1}{\theta_0}} = \frac{\theta_0}{\theta_0 - 1}.$$

Количество a можно подобрать так, чтобы уравнение было неприводимым; все эти шесть корней будут различны. Мы видим, что наше уравнение нормально и его группа Галуа состоит из функций:

$$\varphi_0 = x, \quad \varphi_1 = \frac{1}{x}, \quad \varphi_2 = 1 - x, \quad = \varphi_3 = \frac{x}{x-1}, \quad \varphi_4 = \frac{x-1}{x}, \quad \varphi_5 = \frac{1}{1-x}.$$

Эти функции (ср. § 210, II) составляют группу при любом x.

§ 218. Возвратимся теперь к нашему уравнению $F(x) = 0$ m-й степени с корнями $\alpha_1, \alpha_2, \ldots, \alpha_m$, для которого $g(x) = 0$ является резольвентой Галуа. Мы имели (§ 216, доказательство первой теоремы): $\theta_1 = \Phi(\alpha_1, \alpha_2, \ldots, \alpha_m)$; остальные количества $\theta_2, \ldots, \theta_\nu$ получались из θ_1 посредством некоторых ν перестановок корней $\alpha_1, \alpha_2, \ldots, \alpha_m$, т. е. функциям $\varphi_1, \varphi_2, \ldots, \varphi_\nu$ соответствуют некоторые ν подстановок m корней $\alpha_1, \alpha_2, \ldots, \alpha_m$; подстановку, соответствующую функции φ_λ, мы обозначим через

$$A_\lambda = \begin{pmatrix} \alpha_1 & \alpha_2 & \ldots & \alpha_m \\ \alpha_1^{(\lambda)} & \alpha_2^{(\lambda)} & \ldots & \alpha_m^{(\lambda)} \end{pmatrix},$$

где $\alpha_1^{(\lambda)}, \alpha_2^{(\lambda)}, \ldots, \alpha_m^{(\lambda)}$ — некоторая перестановка количеств $\alpha_1, \alpha_2, \ldots, \alpha_m$. Очевидно, что функции φ_1 соответствует тождественная подстановка E. Посмотрим, какая подстановка соответствует переходу от $\theta_\varkappa$ к $\varphi_\lambda(\theta_\varkappa)$; очевидно, это та же подстановка A_λ; но в ней целесообразно верхнее расположение взять не в виде $\alpha_1, \alpha_2, \ldots, \alpha_m$, а в виде $\alpha_1^{(\varkappa)}, \alpha_2^{(\varkappa)}, \ldots, \alpha_m^{(\varkappa)}$; тогда нижнее расположение будет уже некоторое новое: $\alpha_1^{(\rho)}, \alpha_2^{(\rho)}, \ldots, \alpha_m^{(\rho)}$, т. е.

$$A_\lambda = \begin{pmatrix} \alpha_1^{(\varkappa)} & \alpha_2^{(\varkappa)} & \ldots & \alpha_m^{(\varkappa)} \\ \alpha_1^{(\rho)} & \alpha_2^{(\rho)} & \ldots & \alpha_m^{(\rho 0)} \end{pmatrix}.$$

Но $\varphi_\lambda(\theta_\varkappa) = \varphi_\lambda\varphi_\varkappa(\theta_1) = \varphi_\mu(\theta)_1$, где $\varphi_\mu = \varphi_\lambda\varphi_\varkappa$. С другой стороны,

$$A_\varkappa A_\lambda = \begin{pmatrix} \alpha_1 & \alpha_2 & \ldots & \alpha_m \\ \alpha_1^{(\varkappa)} & \alpha_2^{(\varkappa)} & \ldots & \alpha_m^{(\varkappa)} \end{pmatrix} \begin{pmatrix} \alpha_1^{(\varkappa)} & \alpha_2^{(\varkappa)} & \ldots & \alpha_m^{(\varkappa)} \\ \alpha_1^{(\rho)} & \alpha_2^{(\rho)} & \ldots & \alpha_m^{(\rho)} \end{pmatrix} = \begin{pmatrix} \alpha_1 & \alpha_2 & \ldots & \alpha_m \\ \alpha_1^{(\rho)} & \alpha_2^{(\rho)} & \ldots & \alpha_m^{(\rho)} \end{pmatrix};$$

мы видим, что эта последняя подстановка должна как раз быть равна A_μ, т. е. должно быть $\varrho = \mu$. Итак, между функциями $\varphi_1, \varphi_2, \ldots, \varphi_\nu$, и подстановками

$A_1, A_2, \ldots, A_\nu$ существует взаимнооднозначное соответствие, причем если $\varphi_\varkappa$ соответствует $A_\varkappa$, а φ_λ соответствует A_λ, то $\varphi_\lambda\varphi_\varkappa$ соответствует $A_\varkappa A_\lambda$. Таким образом подстановки $A_1, A_2, \ldots, A_\nu$ тоже составляют группу (обозначим ее через $\mathfrak{G}$), которая изоморфна группе функций $\varphi_1, \varphi_2, \ldots, \varphi_\nu$; правда, у нас $\varphi_\lambda\varphi_\varkappa$ соответствует $A_\varkappa A_\lambda$, а не $A_\lambda A_\varkappa$, как должно быть по определению изоморфизма, но легко видеть, что по существу мы здесь как раз имеем изоморфизм, — все дело в наших обозначениях: подстановки производятся в порядке слева направо, а функции берутся в порядке справа налево [99]. Обычно *группой Галуа* нашего уравнения $F(x) = 0$ называют именно группу $\mathfrak{G}$ подстановок $A_\varkappa$.

Пусть $\Psi(\alpha_1, \alpha_2, \ldots, \alpha_m)$ — рациональная функция от $\alpha_1, \alpha_2, \ldots, \alpha_m$ в теле $\mathbf{P}$; произведем над $\alpha_1, \alpha_2, \ldots, \alpha_m$ в функции Ψ подстановку A; от этого функция Ψ получит новое значение, которое мы обозначим Ψ_A; если окажется, что $\Psi_A = \Psi$, т. е. что от подстановки A функция Ψ не изменилась, то мы говорим, что функция Ψ допускает подстановку A. Точно так же, если уравнение $\Psi(\alpha_1, \alpha_2, \ldots, \alpha_m) = 0$ не нарушилось от подстановки A, то мы говорим, что уравнение $\Psi = 0$ *допускает* подстановку A.

Примечание. Если рассматривается функция от корней данного численного уравнения, то, конечно, речь идет об изменении численного значения этой функции. Но нам может быть дана функция и от независимых переменных (например, если наше уравнение с произвольными буквенными коэфициентами, то корни его — независимые переменные); в таком случае, говоря о том, что такая функция допускает данную подстановку, мы подразумеваем, что самый вид функции от этой подстановки не изменяется. Например, функция $2(x_1 + x_2) + x_3^2$ допускает подстановку $\begin{pmatrix} x_1 & x_2 & x_3 \\ x_2 & x_1 & x_3 \end{pmatrix}$, но не допускает подстановки $\begin{pmatrix} x_1 & x_2 & x_3 \\ x_2 & x_3 & x_1 \end{pmatrix}$.

Симметрическая функция от m переменных допускает всякую подстановку этих переменных; поэтому группа всех подстановок m символов и называется симметрической.

Полусимметрическая функция (§ 142) допускает все четные подстановки, группа которых поэтому и называется полусимметрической (§ 205).

Теорема 1. *Рациональная функция в P $\Psi(\alpha_1, \alpha_2, \ldots, \alpha_m)$ тогда и только тогда имеет рациональное значение (из $\mathbf{P}$), если она допускает все подстановка группы $\mathfrak{G}$.*

Доказательство. Так как $\mathbf{P}(\alpha_1, \alpha_2, \ldots, \alpha_m) = \mathbf{P}(\theta_1)$, то, следовательно, $\Psi(\alpha_1, \alpha_2, \ldots, \alpha_m) = \psi(\theta_1)$, где ψ — тоже рациональная функция от θ_1 в $\mathbf{P}$. Подстановка $A_\varkappa$ будет соответствовать замене θ_1 на $\theta_\varkappa$. Пусть сначала $\Psi = \Psi_{A_2} = \ldots = \Psi_{A_\nu}$ ($A_1 = E$, $\Psi_E = \Psi$); тогда

$$\psi(\theta_1) = \psi(\theta_2) = \ldots = \psi(\theta_\nu) = \frac{1}{\nu}\{\psi(\theta_1) + \psi(\theta_2) + \ldots + \psi(\theta_\nu)\};$$

но это — симметрическая функция от $\theta_1, \theta_2, \ldots, \theta_\nu$; следовательно (по § 133), она выражается рационально через коэфициенты уравнения $g(x) = 0$, т. е. является количеством из $\mathbf{P}$, т. е. $\Psi(\alpha_1, \alpha_2, \ldots, \alpha_m) = \varepsilon \subset \mathbf{P}$.

[99] На самом деле и при наших обозначениях мы имеем обычный изоморфизм группы подстановок $A_\varkappa$ и группы функций $\varphi_\varkappa$; надо только, чтобы $A_\varkappa$ соответствовало не $\varphi_\varkappa$, а $\varphi_\varkappa^{-1}$ (при $\varkappa = 1, 2, \ldots, \nu$).

Обратно, пусть $\Psi(\alpha_1, \alpha_2, \ldots, \alpha_m) = \varepsilon subset \mathbf{P}$, т. е. $\psi(\theta_1) = \varepsilon \subset \mathbf{P}$; но тогда это количество равно всем своим сопряженным (§ 215), т. е. $\psi(\theta_1) = \psi(\theta_2) = \ldots = \psi(\theta_\nu)$, или $\Psi = \Psi_{A_2} = \ldots = \Psi_{A_\nu}$, и теорема доказана.

Теорема 2. *Подстановка A корней $\alpha_1, \alpha_2, \ldots, \alpha_m$ данного уравнения тогда и только тогда принадлежит к группе Галуа $\mathfrak{G}$, если она допускается всеми уравнениями между корнями $\alpha_1, \alpha_2, \ldots, \alpha_m$ в теле $\mathbf{P}$.*

Доказательство. Если $A \subset \mathfrak{G}$, то ясно, что всякое уравнение $\Psi(\alpha_1, \alpha_2, \ldots, \alpha_m) = 0$ в теле $\mathbf{P}$ допускает A, ибо Ψ есть рациональная функция от $\alpha_1, \alpha_2, \ldots, \alpha_m$ в $\mathbf{P}$, имеющая рациональное значений (теорема 1). Обратно, пусть A допускается всеми уравнениями между $\alpha_1, \alpha_2, \ldots, \alpha_m$ в $\mathbf{P}$. Возьмем уравнение $g(x) = 0$, имеющее корни $\theta_1, \theta_2, \ldots, \theta_\nu$ и никаких других; итак, $g(\theta_1) = 0$, но $\theta_1 = \Phi(\alpha_1, \alpha_2, \ldots, \alpha_m)$ — рациональная функция от $\alpha_1, \alpha_2, \ldots, \alpha_m$ в теле $\mathbf{P}$ (см. доказательство теоремы 1 в § 216); всевозможными перестановками корней $\alpha_1, \alpha_2, \ldots, \alpha_m$ мы из θ_1, получим $m!$ количеств, среди которых будут и $\theta_2, \ldots, \theta_\nu$, (получающиеся, если мы в Φ произведем ν подстановок из группы $\mathfrak{G}$). Подставив в $g(\theta_1) = 0$ вместо θ_1 функцию Φ, мы получим $g(\Phi(\alpha_1, \alpha_2, \ldots, \alpha_m)) = 0$; это — уравнение между $\alpha_1, \alpha_2, \ldots, \alpha_m$ в теле $\mathbf{P}$; по условию оно допускает подстановку A; но, с другой стороны, оно допускает только подстановки группы $\mathfrak{G}$, ибо только при них Φ переходит в $\theta_1, \theta_2, \ldots, \theta_\nu$; следовательно, $A \subset \mathfrak{G}$, что и требовалось доказать.

Теорема 2 приводит нас к новому определению группы Галуа, как *группы подстановок корней $\alpha_1, \ldots, \alpha_m$, которые допускаются всяким уравнением между этими корнями в теле $\mathbf{P}$. Заметим, что отдельные уравнения между корнями в теле $\mathbf{P}$ могут допускать кроме подстановок группы $\mathfrak{G}$ и другие подстановки; но все эти подстановки вообще не образуют группы; группу — именно, группу $\mathfrak{G}$ — образуют те подстановки, которые допускаются всеми уравнениями между корнями в теле $\mathbf{P}$.*

Порядок ν группы Галуа есть делитель числа $m!$ порядка симметрической группы подстановок m символов (§ 194, теорема Лагранжа). Наибольшее значение для ν есть $m!$, в этом случае говорят, что данное уравнение не имеет *аффекта*; в общем случае частное $\dfrac{m!}{\nu}$ называется *степенью аффекта* данного уравнения.

Случай, когда $\nu = m!$, представляется, если уравнение дано «в общем виде», т. е. если коэфициенты его — независимые переменные (буквы); в этом случае и корни уравнения — независимые переменные, и следовательно, единственные «уравнения» между корнями, которые существуют, суть тождества (никаких соотношений между независимыми переменными не может быть); а тождества допускают всякую подстановку корней, т. е., по теореме 2, всякая подстановка принадлежит к группе Галуа. Но следует заметить, что этот случай далеко не единственный, когда уравнение не имеет аффекта: существуют и уравнения с числовыми коэфициентами всякой степени без аффекта, т. е. имеющие группой Галуа всю симметрическую группу соответственной степени.

Другой «предельный» случай, когда $\nu = 1$, т. е. когда группа Галуа состоит из одной только тождественной подстановки E. В этом случае каждый корень α_λ в отдельности допускает все подстановки группы Галуа (т. е. тождественную подстановку $\mathbf{P}$); следовательно, по теореме 1, все корни нашего уравнения рациональны (т. е. находятся в области $\mathbf{P}$), а следовательно, наше уравнение уже решено (§ 212). Обратно, если все корни уравнения рациональны, то мы имеем

ряд таких уравнений $\alpha_\lambda = \alpha_\lambda$ $(\lambda = 1, 2, \ldots, m)$, где $\alpha_\lambda \subset \mathbf{P}$; эти уравнения только и допускают одну тождественную подстановку E, т. е. вся группа Галуа и состоит из одной только подстановки E.

Разберем теперь общий случай: пусть дано уравнение $F(x) = 0$ в области $\mathbf{P}$, и $\mathfrak{G}$ — его группа Галуа. Расширим область $\mathbf{P}$, т. е. возьмем имеете $\mathbf{P}$ более обширное тело $\mathbf{P}' \supset \mathbf{P}$. Уравнение $\psi(\alpha_1, \alpha_2, \ldots, \alpha_m) = 0$ в области $\mathbf{P}$ есть также и уравнение в области $\mathbf{P}'$; но не обратно: могут существовать уравнения между корнями $\alpha_1, \alpha_2, \ldots, \alpha_m$ с коэфициентами из $\mathbf{P}'$; но не из $\mathbf{P}$, т. е. в теле $\mathbf{P}'$ вообще существует больше уравнений между корнями, чем в теле $\mathbf{P}$. Эти новые уравнения в теле $\mathbf{P}'$ могут не допускать всех подстановок группы $\mathfrak{G}$, т. е. в теле $\mathbf{P}'$ группа Галуа может состоять только из некоторых подстановок группы $\mathfrak{G}$, т. е. быть подгруппой $\mathfrak{G}$.

Итак, от расширения области $\mathbf{P}$ группа $\mathfrak{G}$ вообще уменьшается; если при таком расширении группа $\mathfrak{G}$ обратится в главную группу E, то, следовательно, в расширенной области все корни сделаются рациональными, и уравнение будет решено. Следовательно, решение уравнения состоит в сведении его группы Галуа к главной группе E. Чем ниже порядок группы Галуа, тем проще уравнение, тем мы, так сказать, ближе к его решению.

§ 219. Естественные и побочные иррациональности. Таким образом вопрос состоит в том, какие количества надо присоединить к области $\mathbf{P}$, чтобы от такого присоединения группа Галуа нашего уравнения уменьшилась.

Мы будем присоединять к $\mathbf{P}$ исключительно алгебраические количества, происходящие из области $\mathbf{P}$ (§ 213). Пусть ρ — такое количество, т. е. корень некоторого неприводимого в $\mathbf{P}$ уравнения $\Phi(x) = 0$. Если в теле $\mathbf{P}(\rho)$ группа Галуа будет уже не ν-го, а μ-го порядка $(\mu < \nu)$, то это значит, что в этом теле резольвента Галуа данного уравнения $g(x) = 0$ сделалась приводимой: в теле $\mathbf{P}(\rho)$ от $g(x)$ отделился неприводимый множитель μ-й степени $g_1(x, \rho)$ (буквою ρ в скобках мы обозначим, что коэфициенты g_1 зависят от ρ), и $g_1(x, \rho) = 0$ — новая резольвента Галуа данного уравнения, — уже в теле $\mathbf{P}(\rho)$. Из множителей, на которые распадается $g(x)$, мы выберем множитель g_1 так, чтобы уравнению $g_1(x, \rho) = 0$ как раз удовлетворял корень θ_1; остальные его корни пусть будут $\theta_2, \theta_3, \ldots, \theta_\mu$ (это — часть всех корней $\theta_1, \theta_2, \ldots, \theta_\nu$). Соответствующие функции $\varphi_1, \varphi_2, \ldots, \varphi_\mu$ и здесь составляют группу (мы сохраняем обозначения § 217), — подгруппу всей группы $\varphi_1, \varphi_2, \ldots, \varphi_\nu$; следовательно, ν делится на μ: $\nu = \mu j$.

Возьмем такое выражение (где t — пока неопределенное количество):

$$\begin{aligned} \omega_1 &= (t - \theta_1)(t - \theta_2) \cdots (t - \theta_\mu) = \\ &= (t - \varphi_1(\theta_1))(t - \varphi_2(\theta_1)) \cdots (t - \varphi_\mu(\theta_1)) \quad =; \end{aligned} \tag{1}$$

ω_1 не изменится, если вместо θ_1 подставить θ_2 или θ_3, .. , или θ_μ, например:

$$\begin{aligned} &(t - \varphi_1(\theta_2))(t - \varphi_2(\theta_2)) \cdots (t - \varphi_\mu(\theta_2)) = \\ &= (t - \varphi_1\varphi_2(\theta_1))(t - \varphi_2\varphi_2(\theta_1)) \cdots (t - \varphi_\mu\varphi_2(\theta_1)), \end{aligned} \tag{2}$$

а это то же самое, что и ω_1, ибо $\varphi_1\varphi_2, \varphi_2\varphi_2, \ldots, \varphi_\mu\varphi_2$ суть те же функции $\varphi_1, \varphi_2, \ldots,$ φ_μ, только в другом порядке (по свойству группы, см. § 192, теорема 1). Но если мы вместо θ_1 подставим одно из количеств $\theta_{\mu+1}, \ldots \theta_\nu$, то получим уже нечто иное,

например:

$$\begin{aligned}\omega_2 &= (t-\varphi_1(\theta_{\mu+1}))(t-\varphi_2(\theta_{\mu+1}))\cdots(t-\varphi_\mu(\theta_{\mu+1})) = \\ &= (t-\theta_{\mu+1})(t-\theta_{\mu+2})\cdots(t-\theta_{2\mu}),\end{aligned}$$

если выбрать нумерацию так, чтобы:

$$\varphi_2(\theta_{\mu+1}) = \varphi_2\varphi_{\mu+1}(\theta_1) = \theta_{\mu+2},\ \ldots,\ \varphi_\mu(\theta_{\mu+1}) = \varphi_\mu\varphi_{\mu+1}(\theta_1) = \theta_{2\mu}.$$

И здесь, если мы вместо $\theta_{\mu+1}$ подставим $\theta_{\mu+2}$ или $\theta_{\mu+3}$, ..., или $\theta_{2\mu}$, то ω_2 не изменится, так как, например, подставить в ω_2 вместо $\theta_{\mu+1}$ количество $\theta_{\mu+2}$ означает то же самое, что подставить $\theta_{\mu+1}$ вместо θ_1 в выражение (2), которое равно ω_1. Рассуждая так дальше, мы найдем, что от подстановки вместо θ_1 количеств θ_2, θ_3, ..., θ_ν в (1) мы получим всего j разных выражений: $\omega_1, \omega_2, \ldots, \omega_j$, от этих подстановок выражения эти только меняются местами. Можно (§ 214, доказательство теоремы Абеля) дать для t такое целое значение, чтобы получившиеся j количеств $\omega_1, \omega_2, \ldots, \omega_j$ оказались все различными. Очевидно при этом, что ω_1 есть количество из $\mathbf{P}(\rho)$ (§ 218, теорема 1), т. е. $\omega_1 = \chi(\rho)$, где χ — рациональная функция в теле $\mathbf{P}$.

Пусть теперь $\tau_1 = \psi(\theta_1)$ есть количество из $\mathbf{P}(\theta_1)$ (т. е. ψ — рациональная функция в $\mathbf{P}$) и одновременно из $\mathbf{P}(\rho)$, так что, по теореме 1, § 218:

$$\tau_1 = \psi(\theta_1) = \psi(\theta_2) = \ldots = \psi(\theta_\mu)$$

или

$$\tau_1 = \psi(\varphi(\theta_1)) = \psi(\varphi_2(\theta_1)) = \ldots = \psi(\varphi_\mu(\theta_1)). \tag{3}$$

Но мы знаем, что равенства (3) остаются верными, если вместо θ_1 подставим одно из количеств θ_2, θ_3, ..., θ_ν; при этом, если мы будем заменять θ_1 через $\theta_2, \ldots, \theta_\mu$, то, как мы уже знаем, τ_1 не изменится; если же заменим θ_1, например, через $\theta_{\mu+1}$, то получим $\tau_2 = \psi(\varphi_1(\theta_{\mu+1})) = \psi(\varphi_2(\theta_{\mu+1})) = \ldots = \psi(\varphi_\mu(\theta_{\mu+1}))$ или (по прежнему обозначению) $\tau_2 = \psi(\theta_{\mu+1}) = \psi(\theta_{\mu+2}) = \ldots = \psi(\theta_{2\mu})$.

Вообще мы видим, что от замены θ_1 через $\theta_2, \ldots, \theta_\mu$ мы получим всего j количеств $\tau_1, \tau_2, \ldots, \tau_j$, (причем здесь они могут и не быть все различными); при этом, например, τ_λ получается от тех же замен, что и ω_λ. Возьмем теперь функции:

$$(x-\omega_1)(x-\omega_2)\cdots(x-\omega_j) = \Omega(x), \tag{4}$$

$$\Omega(x)\cdot\left\{\frac{\tau_1}{x-\omega_1} + \frac{\tau_2}{x-\omega_2} + \ldots + \frac{\tau_j}{x-\omega_j} = \Psi(x). \right. \tag{5}$$

Обе эти функции — целые рациональные в теле $\mathbf{P}$, ибо от замены θ_1 через $\theta_2, \ldots, \theta_\nu$, количества $\omega_1, \omega_2, \ldots, \omega_j$ только меняются местами, и $\tau_1, \tau_2, \ldots, \tau_j$ совершенно так же меняются местами, т. е. симметрические функции от них не изменяются. .Из (5) при $x = \omega_1$ получим: $\tau_1 = \dfrac{\Psi(\omega_1)}{\Omega'(\omega_1)}$, т. е. τ_1 есть рациональная функция от ω_1 в теле $\mathbf{P}$, или $\tau_1 \subset \mathbf{p}(\omega_1)$. Таким образом всякое количество τ_1, одновременно принадлежащее и к телу $\mathbf{P}(\theta_1)$ и к телу $\mathbf{P}(\rho)$, принадлежит и к телу $\mathbf{P}(\omega_1)$; $\mathbf{P}(\omega_1)$ есть *общий наибольший делитель*, или *пересечение* тел $\mathbf{P}(\theta_1)$

и $\mathbf{P}(\rho)$. Но тогда и коэфициенты функции $g_1(x,\rho)$, являясь одновременно количествами из $\mathbf{P}(\rho)$ и из $\mathbf{P}(\theta_1)$ [последнее потому, что они — симметрические функции от $\theta_1, \theta_2 = \varphi_2(\theta_1), \ldots, \theta_\mu = \varphi_\mu(\theta_1)$], принадлежат также и к телу $\mathbf{P}(\omega_1)$, т. е. $g_1(x,\rho) \equiv g_2(x,\omega_1)$ и уравнение $g_1(x,\rho) = 0$, или, что то же самое, $g_2(x,\omega_1) = 0$ есть уравнение в теле $\mathbf{P}(\omega_1)$. Очевидно, что уравнение $g_2(x,\omega_1) = 0$ и в теле $\mathbf{P}(\omega_1)$ неприводимо, раз оно неприводимо в более обширном теле $\mathbf{P}(\rho)$. Итак, присоединение к $\mathbf{P}$ количества ρ дает то же снижение группы Галуа, что и присоединение к $\mathbf{P}$ количества ω_1; но ω_1 есть рациональная функция от θ_1, или, что то же самое, рациональная функция от корней $\alpha_1, \alpha_2, \ldots, \alpha_m$ в теле $\mathbf{P}$; такое количество a называется *естественной иррациональностью* данного уравнения $F(x) = 0$. Количество же ρ, не являющееся рациональной функцией от корней данного уравнения в теле $\mathbf{P}$, называется *побочной иррациональностью*. Итак:

Теорема. *Всякое возможное снижение группы Галуа может быть достигнуто присоединением к* $\mathbf{P}$ *естественных иррациональностей.*

В этом смысле присоединение побочной иррациональности ρ равносильно присоединению некоторой естественной иррациональности ω, являющейся рациональной функцией от ρ в теле $\mathbf{P}$; $\mathbf{P}(\omega_1)$ есть пересечение тел $\mathbf{P}(\rho)$ и $\mathbf{P}(\alpha_1, \alpha_2, \ldots, \alpha_m)$.

Заметим, что на практике иногда приходится присоединять к $\mathbf{P}$ и побочные иррациональности, если от этого достигаются какие-нибудь практические упрощения.

§ 220. Соотношения между алгебраическими телами и подгруппами группы Галуа. Итак, рассмотрим естественные иррациональности; пусть $\omega_1 = f(\theta_1) = \psi(\alpha_1, \alpha_2, \ldots, \alpha_m)$ — такая иррациональность, где f и ψ — рациональные функции от своих аргументов в теле $\mathbf{P}$.

Теорема 1. *Подстановки из группы Галуа* $\mathfrak{G}$ *данного уравнения, которые допускаются естественной иррациональностью* ω_1*, образуют группу* $\mathfrak{H}$ *(подгруппу для* $\mathfrak{G}$*).*

Доказательство. Пусть $A_\varkappa$ и A_λ — подстановки из $\mathfrak{G}$, которые допускаются функцией ψ; тогда $\psi_{A_\varkappa} = \psi$, но это есть уравнение между корнями в теле $\mathbf{P}$; по теореме 2 (§ 218) оно допускает подстановку A_λ , т. е. $\psi_{A_\varkappa A_\lambda} = \psi_{A_\lambda}$; с другой стороны, $\psi_{A_\lambda} = \psi$; следовательно, $\psi_{A_\varkappa A_\lambda} = \psi$, т. е. $A_\varkappa A_\lambda$ — тоже подстановка, допускаемая функцией ψ, а это и доказывает нашу теорему.

Если $\rho_1 = \chi(\omega_1)$, где χ — тоже рациональная функция в $\mathbf{P}$, то, очевидно, что все подстановки, допускаемые функцией ω_1, допускаются и функцией ρ_1, т. е. подгруппа группы Галуа тех подстановок, которые допускаются функцией ρ_1 заключает в себе подгруппу подстановок, допускаемых функцией ω_1. Если и $\omega_1 = \chi_1(\rho_1)$(где χ_1 — тоже рациональная функция в $\mathbf{P}$), то обе эти подгруппы совпадают, но в этом и только в этом случае и $\mathbf{P}(\rho_1) = \mathbf{P}(\omega_1)$.

Таким образом имеется соответствие между подгруппами группы Галуа и алгебраическими телами над $\mathbf{P}$ — делителями тела $\mathbf{P}(\theta_1)$. Из доказательства теоремы § 219 легко следует, что всякой подгруппе группы $\mathfrak{G}$ соответствует естественная иррациональность — именно функция ω_1 [§ 219 (1)], где $\varphi_1, \varphi_2, \ldots, \varphi_\mu$ составляют данную подгруппу группы $\mathfrak{G}$, если ее рассматривать как группу рациональных функций $\theta_1, \theta_2, \ldots, \theta_\nu$.

При этом подгруппе $\mathfrak{H}$ группы $\mathfrak{G}$ соответствует не одна, а бесчисленное множество естественных иррациональностей, именно, все первообразные количества

тела $\mathbf{P}(\omega_1)$. Из предыдущего легко следует, что, и обратно, — всякое количество, соответствующее подгруппе $\mathfrak{H}$, есть первообразное количество тела $\mathbf{P}(\omega_1)$; ибо, если ρ_1 допускает все подстановки из $\mathfrak{H}$, то ρ_1 — рациональная функция от ω_1 (см. доказательство теоремы § 219), а если кроме подстановок из $\mathfrak{H}\rho_1$ не допускает ни одной подстановки из $\mathfrak{G}$, то и ω_1 — рациональная функция от ρ_1 и $\mathbf{P}(\rho_1) = \mathbf{P}(\omega_1)$, т. е. каждой подгруппе группы $\mathfrak{G}$ соответствует одно и только одно тело. Итак:

Теорема 2. *Между подгруппами группы Галуа и алгебраическими телами над* $\mathbf{P}$*, делителями тела* $\mathbf{P}(\theta_1)$*, существует взаимно однозначное соответствие: всякой подгруппе* $\mathfrak{H}$ *соответствует одно и только одно тело* $\mathbf{P}(\omega_1)$*, и обратно. Группа* $\mathfrak{H}$ *состоит из подстановок группы* $\mathfrak{G}$*, допускаемых всеми количествами из* $\mathbf{P}(\omega_1)$ *как функциями от корней* $\alpha_1, \alpha_2, \ldots, \alpha_m$*; тело* $\mathbf{P}(\omega_1)$ *состоит из рациональных функций от* $\alpha_1, \alpha_2, \ldots, \alpha_m$*, допускающих все подстановки из группы* $\mathfrak{H}$*.*

Заметим, что телу $\mathbf{P}$ соответствует вся группа Галуа $\mathfrak{G}$; телу $\mathbf{P}(\theta_1)$ соответствует главная группа E.

Теорема 3. *Если подгруппе* $\mathfrak{H}$ *соответствует тело* $\mathbf{P}(\omega_1)$*, а подгруппе* $\mathfrak{R}$ *— тело* $\mathbf{P}(\rho_1)$*, то соотношение* $\mathfrak{H} \supset \mathfrak{R}$ *влечет за собою* $\mathbf{P}(\omega_1) \subset \mathbf{P}(\rho_1)$*, и обратно.*

Отсюда легко следует:

Теорема 4. *Если подгруппе* $\mathfrak{H}$ *соответствует тело* $\mathbf{P}(\omega_1)$*, а подгруппе* $\mathfrak{R}$ *— тело* $\mathbf{P}(\rho_1)$*, то подгруппе* $\mathfrak{D} = \mathbf{D}(\mathfrak{H}, \mathfrak{R})$ *соответствует тело* $\mathbf{P}(\omega_1, \rho_1)$*, а подгруппе* $\{\mathfrak{H}, \mathfrak{R}\}$ *—пересечение тел* $\mathbf{P}(\omega_1)$ *и* $\mathbf{P}(\rho_1)$*, и обратно.*

Эта теорема непосредственно обобщается на несколько подгрупп и тел.

Доказательство. Пусть $\mathfrak{D}$ — подгруппа, соответствующая телу $\mathbf{P}(\omega_1, \rho_1)$. Так как $\mathbf{P}(\omega_1) \subset \mathbf{P}(\omega_1, \rho_1)$ и $\mathbf{P}(\rho_1) \subset \mathbf{P}(\omega_1, \rho_1)$, то, следовательно, $\mathfrak{D} \subset \mathfrak{H}$ и $\mathfrak{D} \subset \mathfrak{R}$; с другой стороны, если подстановка $A \subset \mathfrak{H}$ и $A \subset \mathfrak{R}$, то A допускается и функцией ω_1, и функцией ρ_1, т. е. и всякой функцией от ω_1 и ρ_1, т. е. $A \subset \mathfrak{D}$, т. е. $\mathfrak{D} = \mathbf{D}(\mathfrak{H}, \mathfrak{R})$. Подобным же образом доказывается и вторая часть теоремы

Теорема 5. *Если подгруппе* $\mathfrak{H}$ *группы Галуа* $\mathfrak{G}$ *соответствует тело* $\mathbf{P}(\omega_1)$*, то* $\mathfrak{H}$ *есть группа Галуа нашего уравнения в теле* $\mathbf{P}(\omega_1)$*.*

Доказательство. Это, собственно, уже следует из доказательства теоремы § 219. Докажем это непосредственно. Всякое уравнение $f(\alpha_1, \alpha_2, \ldots, \alpha_m, \omega_1) = 0$ между корнями в теле $\mathbf{P}(\omega_1)$ допускает все подстановки из $\mathfrak{H}$ (так как для них ω_1 не изменяется); с другой стороны, равенство $\omega_1 = \psi(\alpha_1, \alpha_2, \ldots, \alpha_m)$ есть тоже уравнение между корнями $\alpha_1, \alpha_2, \ldots, \alpha_m$ в теле $\mathbf{P}(\omega_1)$; но оно кроме подстановок из $\mathfrak{H}$ не допускает никаких других подстановок. Следовательно, по теореме 2 (§ 218) $\mathfrak{H}$ и есть группа Галуа данного уравнения в теле $\mathbf{P}(\omega_1)$.

Если мы в функции ω_1 будем над $\alpha_1, \alpha_2, \ldots, \alpha_m$ производить все подстановки группы $\mathfrak{G}$, то это сведется к тому, что мы вместо корня θ_1 резольвенты Галуа будем подставлять корни $\theta_2, \theta_3, \ldots, \theta_\nu$; от этого (доказательство теоремы 1, § 216) ω_1 перейдет в *сопряженные* в теле $\mathbf{P}(\theta_1)$ количества $\omega_1, \omega_2, \ldots, \omega_j$, где $j = \dfrac{\nu}{\mu}$ (μ — порядок группы $\mathfrak{H}$). Разложим $\mathfrak{G}$ по модулю $\mathfrak{H}$ слева (§ 194):

$$\mathfrak{G} = \mathfrak{H} + \mathfrak{H}A_2 + \mathfrak{H}A_3 + \ldots + \mathfrak{H}A_j.$$

От применения к ω_1 подстановок одного и того же комплекса $\mathfrak{H}A_\lambda$ оно перейдет в одно и то же количество, например, ω_λ; обратно, если $A \subset \mathfrak{G}$ и $(\omega_1)_A = \omega_\lambda$, то $(\omega_1)_{AA_\lambda^{-1}} = \omega_1$, т. е. $AA_\lambda^{-1} = A' \subset \mathfrak{H}$; следовательно, $A = A'A_\lambda \subset \mathfrak{H}A_\lambda$.

Посмотрим, какая группа соответствует количеству ω_λ.

Пусть A — подстановка этой группы, т. е. $(\omega_\lambda)_A = \omega_\lambda$; следовательно, $(\omega_1)_{A_\lambda A} = (\omega_1)_{A_\lambda}$; $(\omega_1)_{A_\lambda A A_\lambda^{-1}} = \omega_1$, т. е. $A_\lambda A A_\lambda^{-1} \subset \mathfrak{H}$; $A \subset A_\lambda^{-1}\mathfrak{H}A_\lambda$.

Обратно, если $A = A_\lambda^{-1}HA_\lambda$, где $H \subset \mathfrak{H}$, то, очевидно: $(\omega_\lambda)_A = (\omega_\lambda)_{A_\lambda^{-1}HA_\lambda} = \omega_\lambda$. Итак, количеству ω_λ [и телу $\mathbf{P}(\omega_\lambda)$] соответствует группа $A_\lambda^{-1}\mathfrak{H}A_\lambda$. Если $A_\lambda^{-1}\mathfrak{H}A_\lambda = \mathfrak{H}$, то это значит, что $\mathbf{P}(\omega_\lambda) = \mathbf{P}(\omega_1)$. Если $A_\lambda^{-1}\mathfrak{H}A_\lambda = \mathfrak{H}$ при всяком λ, то, следовательно, $\mathbf{P}(\omega_1) = \mathbf{P}(\omega_2) = \ldots = \mathbf{P}(\omega_j)$, и обратно. Следовательно:

Теорема 6. *Сопряженным подгруппам группы Галуа соответствуют сопряженные тела; инвариантной подгруппе соответствует нормальное тело, и обратно.*

Теорема 7. *Если функции ω_1 соответствует подгруппа $\mathfrak{H}$ группы Галуа $\mathfrak{G}$, то группа Галуа неприводимого уравнения $\Omega(x) = 0$, которому удовлетворяет ω_1 в теле $\mathbf{P}$, изоморфна дополнительной группе $\frac{\mathfrak{G}}{\mathfrak{D}}$, где $\mathfrak{D}$ — пересечение всех сопряженных с $\mathfrak{H}$ подгрупп.*

Доказательство. $\Omega(x) = (x-\omega_1)(x-\omega_2)\cdots(x-\omega_j)$ (§ 219). Пусть $f(\omega_1, \omega_2, \ldots, \omega_j) = 0$ — любое уравнение в $\mathbf{P}$ между $\omega_1, \omega_2, \ldots, \omega_j$, подставив вместо $\omega_1, \omega_2, \ldots, \omega_j$ их выражения через $\alpha_1, \alpha_2, \ldots, \alpha_m$, получим уравнение для $\alpha_1, \alpha_2, \ldots, \alpha_m$ в P: $\Phi(\alpha_1, \alpha_2, \ldots, \alpha_m) = 0$, допускающее все подстановки из $\mathfrak{G}$; от этих подстановок количеств $\alpha_1, \alpha_2, \ldots, \alpha_m$ будут испытывать подстановки, которые и составят искомую группу Галуа $\mathfrak{G}$ уравнения $\Omega(x) = 0$.

Посмотрим, от каких подстановок из $\mathfrak{G}$ расположение $\omega_1, \omega_2, \ldots, \omega_j$ совсем не изменится; очевидно — от всех подстановок из $\mathfrak{D}$, где $\mathfrak{D}$ — пересечение всех групп, сопряженных с $\mathfrak{H}$; ибо, если A такая подстановка, то, не изменяя ω_1, A должна принадлежать к $\mathfrak{H}$, не изменяя ω_2 она должна одновременно принадлежать и к $A_2^{-1}\mathfrak{H}A_2$ и т. д. Итак, всей группе $\mathfrak{D}$ соответствует тождественная подстановка E из $\overline{\mathfrak{G}}$. Пусть теперь подстановки A' и A'' из $\mathfrak{G}$ производят одну и ту же подстановку количеств $\omega_1, \omega_2, \ldots, \omega_j$; тогда $A'A''^{-1}$ не изменят расположения $\omega_1, \omega_2, \ldots, \omega_j$, т. е. $A'A''^{-1} = A \subset \mathfrak{D}$, т. е. $\mathfrak{D}A' = \mathfrak{D}A''$. Обратно, все подстановки одного и того же комплекса $\mathfrak{D}A'$ производят одну и ту же подстановку количеств $\omega_1, \omega_2, \ldots, \omega_j$, т. е. соответствуют одной и той же подстановке A' из $\overline{\mathfrak{G}}$. Итак, между подстановками группы $\overline{\mathfrak{G}}$ и комплексами $\mathfrak{D}A$ имеется взаимно однозначное соответствие, причем, если $\mathfrak{D}A$ соответствует $\overline{A}$, $\mathfrak{D}A'$ соответствует $\overline{A}'$; то $\mathfrak{D}A \cdot \mathfrak{D}A' = \mathfrak{D}AA'$ соответствует $\overline{AA}'$; отсюда следует, что группа $\overline{\mathfrak{G}}$ изоморфна группе $\frac{\mathfrak{G}}{\mathfrak{D}}$, и наша теорема доказана.

§ 221. Полные и частные резольвенты. Итак, если мы решим уравнение $\Omega(x) = 0$ и присоединим к $\mathbf{P}$ все его корни, то группа Галуа данного уравнения обратится в $\mathfrak{D}$. Такие уравнения $\Omega(x) = 0$ называются *резольвентами* данного уравнения (ср. § 145). Если $\mathfrak{D} = E$, т. е. если все группы $A^{-1}\mathfrak{H}A$ взаимно простые, то $\overline{\mathfrak{G}}$ изоморфна $\mathfrak{G}$, и уравнение $\Omega(x) = 0$ называется *полной резольвентой* данного уравнения; присоединив к $\mathbf{P}$ все его корни, мы сведем группу Галуа данного уравнения к E, т. е. решим и данное уравнение. Таким образом решение данного уравнения и решение его полной резольвенты — одна и та же задача (теоретически), хотя бы степени их и были различны. Например, резольвента Галуа данного уравнения (§ 216) всегда является его полной резольвентой. Если группа Галуа $\mathfrak{G}$ простая, то существуют только полные резольвенты, так как $\mathfrak{D}$ — инвариантная

подгруппа для $\mathfrak{G}$ (по теореме 1 в § 197) и, следовательно, для простой группы $\mathfrak{G}$ должно быть $\mathfrak{D} = E$. В этом случае и данное уравнение называется *простым*. Если же группа $\mathfrak{G}$ составная, то и данное уравнение называется *составным*. Если $\mathfrak{D}$ не главная группа (т. е. $\mathfrak{D} \neq E$), то уравнение $\Omega(x) = 0$ называется *частной резольвентой*; частные резольвенты существуют только у составных уравнений.

Если группа Галуа абелева, то и данное уравнение называется *абелевым*; если группа Галуа циклическая, то и уравнение *циклическое*; если группа Галуа простейшая, то и уравнение *простейшее*.

Теорема. *Неприводимое циклическое уравнение всегда нормально.*

Доказательство. Группа Галуа циклического уравнения состоит из степеней подстановки A корней $\alpha_1, \alpha_2, \ldots, \alpha_m$ данного уравнения; докажем, что если данное циклическое уравнение неприводимо, то подстановка A представляет собою один цикл (§ 204).

Действительно, пусть $B = (\alpha_1, \alpha_2, \ldots, \alpha_\mu)$ — один из независимых циклов, на которые раскладывается A: в подстановках $A^2, A^3, \ldots$ будут содержаться соответствующие степени этого цикла $B_2, B^3, \ldots$; возьмем функцию

$$f(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_\mu);$$

ее коэфициенты — симметрические функции от $\alpha_1, \alpha_2, \ldots, \alpha_\mu$ и, следовательно, допускают подстановку B и ее степени, а следовательно, и подстановку A, куда B входит как часть, и все степени A, т. е. всю группу Галуа данного уравнения; значит, все коэфициенты функции $f(x)$ рациональны (в данном теле $\mathbf{P}$); но $f(x)$ является множителем левой части нашего уравнения $F(x) = 0$, ибо

$$F(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_\mu) \cdots (x - \alpha_m).$$

Так как наше уравнение неприводимо, то должно быть $\mu = m$, т. е. $B = A$. Но как цикл, так и все его степени (пример в конце § 204) перемещают все входящие в этот цикл символы за исключением той его степени, которая равна E. Таким образом, если мы найдем какой-нибудь один из корней нашего уравнения, например, α_1, и присоединим α_1 к телу $\mathbf{P}$, то в теле $\mathbf{P}(\alpha_1)$ группа нашего уравнения должна свестись к E, ибо (теорема 5, § 220) подгруппа $\mathfrak{H}$ группы Галуа, соответствующая функции α_1 от корней, состоит из подстановок, не изменяющих α_1, т. е. в данном случае из одной только подстановки E. Но тогда мы заключаем, что в теле $\mathbf{P}(\alpha_1)$ содержатся и остальные корни нашего уравнения (§ 218), т. е. все корни выражаются рационально через α_1 (в теле $\mathbf{P}$), т. е. уравнение наше нормальное (§ 216), и теорема доказана.

В дальнейшем мы будем рассматривать исключительно только неприводимые циклические уравнения, которые мы просто будем называть циклическими.

§ 222. Сведение решения уравнения к цепи простых уравнений. Пусть $\mathfrak{G}, \mathfrak{G}_1, \mathfrak{G}_2, \ldots, \mathfrak{G}_{n-1}, E$ — композиционный ряд (§ 199) для группы Галуа $\mathfrak{G}$ нашего уравнения $F(x) = 0$ в области $\mathbf{P}$. Найдем иррациональность η_1, принадлежащую к группе $\mathfrak{G}_1$, η_1 есть корень некоторого неприводимого уравнения $\Phi_1(x) = 0$ в теле $\mathbf{P}$ с группой Галуа $\dfrac{\mathfrak{G}}{\mathfrak{G}_1}$ (§ 220, теорема 7). Решив это уравнение, присоединим все его корни к $\mathbf{P}$; получим область $\mathbf{P}_1$, в которой группа Галуа нашего уравнения будет $\mathfrak{G}_1$.

Теперь в области $\mathbf{P}_1$ найдем рациональную функцию от корней нашего уравнения η_2, принадлежащую к группе $\mathfrak{G}_2$; η_2 есть корень неприводимого уравнения $\Phi_2(x) = 0$ в теле $\mathbf{P}_1$ с группой Галуа $\dfrac{\mathfrak{G}_1}{\mathfrak{G}_2}$. Решим это уравнение и присоединим все его корни к $\mathbf{P}_1$; получим тело $\mathbf{P}_2$, в котором группа Галуа нашего уравнения будет уже $\mathfrak{G}_2$, и т. д.

Когда мы решим последнее уравнение в этой цепи, а именно, некоторое неприводимое уравнение $\Phi_n(x) = 0$ в теле $\mathbf{P}_{n-1}$ с группой Галуа $\dfrac{\mathfrak{G}_{n-1}}{E} = \mathfrak{G}_{n-1}$, и присоединим его корни к $\mathbf{P}_{n-1}$, то получим тело $\mathbf{P}_n$, в котором группа Галуа нашего уравнения будет E, т. е. все корни $\alpha_1, \alpha_2, \ldots, \alpha_m$ нашего уравнения будут находиться в этим теле $\mathbf{P}_n$, и наше уравнение будет, таким образом, решено.

Итак, решение нашего уравнения свелось к решению цепи уравнений: $\Phi_1(x) = 0$, $\Phi_2(x) = 0$, $\ldots$, $\Phi_n(x) = 0$ с группами Галуа $\dfrac{\mathfrak{G}}{\mathfrak{G}_1}$, $\dfrac{\mathfrak{G}_1}{\mathfrak{G}_2}$, $\ldots$, $\mathfrak{G}_{n-1}$; все эти группы простые, т. е. и все эти уравнения простые. Наша группа ? может иметь несколько различных композиционных рядов, но по теореме Жордана – Гельдера (§ 199) число членов в различных рядах одно и то же и дополнительные группы $\dfrac{\mathfrak{G}}{\mathfrak{G}_1}$, $\dfrac{\mathfrak{G}_1}{\mathfrak{G}_2}$, $\ldots$ (рассматриваемые как абстрактные группы) одни и те же в различных рядах, разве только стоят в другом порядке. Т. е. для различных композиционных рядов уравнения $\Phi_1(x) = 0$, $\Phi_2(x) = 0$, $\ldots$ могут быть различны, различной степени, в различных областях рациональности, но число их одно и то же, и группы Галуа у них одни и те же, т. е. для различных рядов эти уравнения, так сказать, той же самой трудности. Итак:

Теорема. *Решение всякого уравнения сводится к решению цепи простых уравнений, причем число n этих уравнений и структура их групп Галуа для данного уравнения вполне определены.*

Особенно важен случай, когда группа $\mathfrak{G}$ разрешима (метациклическая, § 199); в этом случае все группы $\dfrac{\mathfrak{G}}{\mathfrak{G}_1}$, $\dfrac{\mathfrak{G}_1}{\mathfrak{G}_2}$, $\ldots$ — простейшие, следовательно, и уравнения $\Phi_1(x) = 0$, $\Phi_2(x) = 0$, $\ldots$ — простейшие, т. е. циклические уравнения простых степеней. Ниже мы увидим, что такие и только такие уравнения разрешимы в радикалах (поэтому и группа $\mathfrak{G}$ называется разрешимой). В частности, как мы заключаем из того же § 199, все абелевы уравнения (а также и все циклические, как частный случай абелевых) имеют разрешимые группы.

Решить уравнение в радикалах — это значит свести его решение к решению цепи двучленных уравнений вида $x^k = a$. Нашей дальнейшей целью является показать, с одной стороны, что простейшее уравнение всегда решается в радикалах, с другой стороны, — что решение двучленного уравнения сводится к решению цепи простейших уравнений.

§ 223. Сведение двучленных уравнений к цепи простейших уравнений. В главе седьмой уже были выведены многие свойства двучленных уравнений. Заметим, что нам достаточно рассмотреть только двучленные уравнения простой степени p, ибо, если $k = pqr\ldots$, где p, q, r, $\ldots$ — простые числа (может быть, и не все различные), то, как известно, $x = \sqrt[k]{a}\ldots\sqrt[r]{\sqrt[q]{\sqrt[p]{a}}}$, т. е. решение уравнения $x^k = a$ сводится к решению цепи уравнений: $y^p = a$, $z^q = y$, $t^r = z$, $\ldots$

Про уравнение же $x^p = a$ мы знаем следующее:

1. Оно или неприводимо в области $\mathbf{P}$, или имеет рациональный корень (т. е. корень, принадлежащий к области $\mathbf{P}$); в § 116 эта теорема была доказана для абсолютной области рациональности $\mathbf{P}$; но доказательство, приведенное там, не требует никаких специальных условий для тела $\mathbf{P}$, которое может быть таким образом любым.

2. Если α — один корень уравнения $x^p = a$, то другие найдутся умножением α на все корни ρ уравнения $x^p = 1$ (§ 114).

3. Уравнение $x^p = 1$ имеет один непервообразный корень 1; остальные $p-1$ его корней первообразны и служат корнями уравнения деления окружности $\Phi_p(x) = 0$, неприводимого в абсолютной области рациональности (§ 120, 122).

Легко доказать еще следующее:

4. Уравнение $\Phi_p(x) = 0$ нормальное и при этом циклическое (но не простейшее, так как $p-1$ не простое число).

Доказательство. Из § 216 следует, что $\Phi_p(x) = 0$ нормальное уравнение: оно неприводимо (§ 122) и все его корни выражаются рационально через один из них; если ρ — один его корень, то остальные его корни $\rho^2, \rho^3, \ldots, \rho^{p-1}$.

Из теории чисел известно, что для всякого простого числа p существуют так называемые «первообразные корни», т. е. такие числа g, для которых никакая пара степеней $g, g^2, g^3, \ldots, g^{p-2}, g^{p-1}$ несравнима друг с другом по модулю p, а $g^{p-1} \equiv 1 \pmod p$; следовательно, по модулю p числа $g, g^2, g^3, \ldots, g^{p-1}$ представляют ряд чисел $1, 2, 3, \ldots, p-1$, только в другом порядке. Следовательно, $\rho, \rho^g, \rho^{g^2}, \rho^{g^3}, \ldots, \rho^{g^{p-2}}$, представляют собою наши корни $\rho, \rho^2, \rho^3, \ldots, \rho^{p-1}$, только в другом порядке; при этом $\rho^{g^2} = (\rho^g)^g$ $\rho^{g^3} = (\rho^{g^2})^g$ и т. д., т. е. каждый следующий корень ряда $\rho, \rho^g, \rho^{g^2}, , \ldots$ представляет собою одну и ту же функцию (g-ю степень) предыдущего, и, кроме того, $\rho = \rho^{g^{p-1}} = (\rho^{g^{p-2}})^g$, т. е. первый корень представляет собою ту же самую функцию от последнего. Если мы обозначим $\varphi(x) = x^g$, и вместо $\varphi(\varphi(x))$, $\varphi(\varphi(\varphi(x)))$ будем писать φ^2, φ^3, …, то наши корни будут $\rho, \chi(\rho), \varphi^2(\rho), \ldots, \varphi^{p-2}(\rho)$. Но $\varphi^{p-1}(\rho) = \rho$; это и показывает, что группа наших рациональных функций $\varphi, \varphi^2, \ldots$ — циклическая, т. е. группа Галуа нашего уравнения циклическая.

5. Если к нашей области $\mathbf{P}$ присоединить один из корней ρ уравнения $\Phi_p(x) = 0$, то в теле $\mathbf{P}(\rho)$ уравнение $x^p = a$ становится нормальным, а следовательно, и простейшим.

Доказательство. Действительно, если α — один из корней уравнения $x^p = a$, то по свойству 2 другие его корни будут $\alpha\rho, \alpha\rho^2, \ldots, \alpha\rho^{p-2}$; они все выражаются рационально через α (в теле $\mathbf{P}(\rho)$, следовательно, уравнение $x^p = a$ нормальное, а следовательно, его степень p есть и порядок его группы Галуа; но p — простое число, т. е. эта группа — простейшая.

Итак, решение уравнения $x^p = a$ сводится к решению уравнения $\Phi_p(x) = 0$ (которое, как циклическое, и значит абелево, сводится к решению цепи простейших уравнений) и присоединению корня этого уравнения ρ к области $\mathbf{P}$, в которой само уравнение $x^p = a$ становится простейшим. Итак:

Теорема. *Решение двучленных уравнений (т. е. извлечение корней) сводится к решению цепи простейших уравнений.*

§ 224. Решение циклических уравнений в радикалах. Теперь нам предстоит доказать, что простейшие уравнения решаются в радикалах. Мы докажем,

что вообще всякое циклическое уравнение решается в радикалах.

Итак, пусть $F(x) = 0$ циклическое уравнение m-й степени с корнями $\alpha, \varphi(\alpha)$, $\varphi(\varphi(\alpha)) = \varphi^2(\alpha), \ldots, \varphi^{m-1}(\alpha)$ [тогда как $\varphi^m(\alpha) = \alpha$]. Решим сначала уравнение $x^m = 1$ и присоединим к $\mathbf{P}$ все его корни; пусть ρ — один из этих корней; возьмем выражение:

$$\psi(\alpha) = (\rho, \alpha) + \alpha + \rho \cdot \varphi(\alpha) + \rho^2\varphi^2(\alpha) + \ldots + \rho^{m-1}\varphi^{m-1}(\alpha);$$

это — так *называемая резольвента Лагранжа* [100]. Подставив $\varphi(\alpha)$ вместо α, получим:

$$\psi(\varphi(\alpha)) = \varphi(\alpha) + \rho\varphi^2(\alpha) + \rho^2\varphi^3(\alpha) + \ldots + \\ + \rho^{m-2}\varphi^{m-1}(\alpha) + \rho^{m-1} \cdot \alpha = \rho^{-1}\psi(\alpha),$$

ибо

$$\rho^{m-1} = \rho^{-1} \qquad (\rho^m = 1).$$

Точно так же найдем $\psi(\varphi^2(\alpha)) = \rho^{-2}\psi(\alpha)$ и т. д. Возьмем $v = [\psi(\alpha)]^m$; имеем $\psi[\varphi(\alpha)]^m = \rho^{-m}[\psi(\alpha)]^m = v$, точно так же $[\psi(\varphi^2(\alpha))]^m = v$ и т. д. Отсюда по теореме 1 § 218 заключаем, что v — рациональное количество [т. е. из нашей области $\mathbf{P}(\rho)$. Имеем $\psi(\alpha) = \sqrt[m]{v}$.

За ρ можно взять любой из m корней уравнения $x^m = 1$; пусть эти корни $\rho_1 = 1, \rho_2, \rho_3, \ldots, \rho_m$; подставив в $\psi(\alpha)$ каждый из этих корней, получим:

$$\left.\begin{array}{lcl} \alpha + \varphi(\alpha) + \varphi^2(\alpha) + \ldots + \varphi^{m-1}(\alpha) & = & u_0, \\ \alpha + \rho_2\varphi(\alpha) + \rho_2^2\varphi^2(\alpha) + \ldots + \rho_2^{m-1}\varphi^{m-1}(\alpha) & = & \sqrt[m]{v_2}, \\ \alpha + \rho_3\varphi(\alpha) + \rho_3^2\varphi^2(\alpha) + \ldots + \rho_3^{m-1}\varphi^{m-1}(\alpha) & = & \sqrt[m]{v_3}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & & \\ \alpha + \rho_m\varphi(\alpha) + \rho_m^2\varphi^2(\alpha) + \ldots + \rho_m^{m-1}\varphi^{m-1}(\alpha) & = & \sqrt[m]{v_m}, \end{array}\right\} \qquad (6)$$

где $v_2, v_3, \ldots, v_m$ — количества из $\mathbf{P}(\rho)$; очевидно, $u_0 \subset \mathbf{P}(\rho)$. Сложив почленно эти равенства и применив вторую теорему § 119, найдем:

$$m\alpha = u_0 + \sqrt[m]{v_2} + \sqrt[m]{v_3} + \ldots + \sqrt[m]{v_m}. \qquad (7)$$

Умножив же уравнения (6), соответственно, на единицу, на ρ_2^{-k}, на ρ_3^{-k}, …, на ρ_m^{-k} и сложив, найдем:

$$m\alpha_k = m\varphi^k(\alpha) = u_0 + \rho_2^{-k}\sqrt[m]{v_2} + \rho_3^{-k}\sqrt[m]{v_3} + \ldots + \rho_m^{-k}\sqrt[m]{v_m}. \qquad (8)$$

Формулы (7) и (8) дают решение циклического уравнения в радикалах, если мы сможем найти корни $\rho_2, \rho_3, \ldots, \rho_m$ в радикалах; это — корни уравнения $x^m = 1$, решение которого, как мы видели, сводится к решению цепи простейших, т. е. циклических уравнений, но степеней меньших m. Поэтому здесь применим метод полной индукции: если доказано, что циклические уравнения степени меньших m решаются в радикалах, то формулы (7) и (8) доказывают, что циклическое уравнение m-й степени решается в радикалах. Но уравнения второй степени решаются все в радикалах; следовательно, доказана такая теорема:

[100] Здесь резольвентой называется не уравнение, как в § 145, а сама функция от корней данного уравнения.

Теорема. *Всякое циклическое (а, следовательно, и всякое простейшее) уравнение разрешимо в радикалах.*

Замечание. Формулы (7) и (8), важные теоретически, так сказать, принципиально, практического значения не имеют, так как неизвестно, какие значения радикалов $\sqrt[m]{v_2}$, $\sqrt[m]{v_3}$, ... надо брать. Относительно этого существуют известные дополнения, по поводу которых здесь распространяться не будем.

§ 225. Условие разрешимости уравнения в радикалах. Теорема Руффини – Абеля. Теоремы предыдущего параграфа говорят, что уравнение решается в радикалах тогда и только тогда, если его решение может быть сведено к решению цепи простейших уравнений. Таким образом на основании результата § 222 мы можем сказать, что всякое уравнение с разрешимой группой решается в радикалах. Докажем теперь обратное: если уравнение решается в радикалах, то группа его разрешима или если решение данного уравнения сводится к решению цепи простейших уравнений, то группа его разрешима.

Пусть $F(x) = 0$ данное уравнение, решение которого сводится к решению цепи простейших уравнений. Вначале группа Галуа этого уравнения $\mathfrak{G}$; после решения всех простейших уравнений, корни которых мы последовательно присоединяем к данной области рациональности, эта область так расширится, что группа Галуа данного уравнения будет E (уравнение будет решено). Следовательно, эта группа $\mathfrak{G}$ постепенно должка уменьшаться (может быть, и не после решения каждого уравнения). Рассмотрим случай, когда после решения одного из простейших уравнений $\psi(x) = 0$ нашей цепи группа Галуа уменьшается. Пусть до решения этого уравнения наша область $\mathbf{P}$ и группа $\mathfrak{A}$; после решения — область $\mathbf{P}(\eta)$ и группа $\mathfrak{B}$; η — один из корней этого решенного простейшего уравнения, $\psi(x) = 0$ степени p (простое число); так как простейшее уравнение — нормальное, то достаточно найти и присоединить к $\mathbf{P}$ только один его корень η); если η — побочная иррациональность, то (по теореме § 219) мы можем заменить η естественной иррациональностью (на самом деле η и не может здесь быть побочной иррациональностью), т. е. мы можем предполагать, что η — естественная иррациональность. Тело $\mathbf{P}(\eta)$ — нормальное, а следовательно, $\mathfrak{B}$ — инвариантная подгруппа для $\mathfrak{A}$ (§ 220, теорема 6); группа Галуа уравнения $\psi(x) = 0$ p-го порядка изоморфна группе $\frac{\mathfrak{A}}{\mathfrak{B}}$; следовательно, $(\mathfrak{A}, \mathfrak{B}) = p$.

Выберем теперь из нашей цепи простейших уравнений те, решение которых уменьшает группу Галуа данного уравнения; пусть эта группа вначале $\mathfrak{G}$, потом сводится к $\mathfrak{H}$, затем к $\mathfrak{R}$ и т. д. Тогда по доказанному заключаем, что $\mathfrak{G}$ — инвариантная подгруппа для $\mathfrak{G}$, $\mathfrak{R}$ — инвариантная подгруппа для $\mathfrak{G}$ и т. д., и группы $\frac{\mathfrak{G}}{\mathfrak{H}}, \frac{\mathfrak{H}}{\mathfrak{R}}, \ldots$ — простейшие. Но это значит, что ряд $\mathfrak{G}$, $\mathfrak{H}$, $\mathfrak{R}$, ... есть композиционный ряд для $\mathfrak{G}$, и группа $\mathfrak{G}$ разрешима. Таким образом доказана следующая теорема:

Теорема. *Уравнение разрешимо в радикалах тогда и только тогда, если его группа Галуа разрешима (метациклическая).*

Следствие. Абелево уравнение всегда разрешимо в радикалах.

Мы видели (§ 218), что группа Галуа общего (т. е. с любыми буквенными коэфициентами) уравнения m-й степени есть симметрическая группа m-й степени. В § 207 мы видели, что симметрические группы второй, третьей и четвертой степе-

ней разрешимы, но при $m > 4$ симметрическая группа m-й степени неразрешима. Следовательно, уравнения второй, третьей и четвертой степеней разрешимы в радикалах в общем виде, тогда как:

Теорема Руффини – Абеля (Ruffini – Abel). *Уравнение степени выше четвертой в общем виде неразрешимо в радикалах.*

§ 226. Общие замечания. Сделаем некоторые замечания. Настоящая глава представляет собою только введение в теорию Галуа, так сказать, теоретические основы этой теории; при этом мы рассматривали только главнейшее, совершенно не касаясь деталей. Для желающих продолжать изучение теории алгебраических уравнений можно рекомендовать список литературы по этой теории, помещенный в конце настоящей книги, в особенности же капитальный труд Вебера, «Lehrbuch der Algebra», в трех томах.

Мы оставили также без рассмотрения практические вопросы, которые возникают при изучении теории алгебраических уравнений: например, если дано уравнение, как практически найти, решается ли это уравнение в радикалах, и в случае утвердительного ответа, как найти формулу его решения в радикалах. Или более общий вопрос: как найти группу Галуа данного уравнения? Можно сказать, что принципиально мы группу всякого уравнения всегда можем найти путем конечного числа операций: действительно, надо только проделать на частном примере данного уравнения все те построения, какие мы провели при доказательстве первой теоремы § 215, найти резольвенту Галуа для данного уравнения, найти рациональные функции $\varphi_1, \varphi_2, \ldots, \varphi_\nu$ и затем построить группу этих функций. А затем, исследуя эту группу, мы ответим и на вопрос, решается ли в радикалах данное уравнение. Но практически, конечно, это построение даже для совсем простых случаев не выполнимо. Имеются только частные виды уравнений, для которых вопрос об их разрешимости в радикалах определенно решен. Например, как мы видели, все абелевы уравнения разрешимы в радикалах, ибо абелева группа всегда разрешима. Но вообще следует сказать, что чисто практического, так сказать, прикладного значения вопрос о разрешимости уравнения в радикалах не имеет: даже на примере кубических уравнений и уравнений четвертой степени мы видим, что получаемые формулы их решения в радикалах слишком громоздки, — гораздо проще вычислять корни этих уравнений одним из общих приемов вычисления корней. Кроме того, уже в теории кубических уравнений нам встретился «неприводимый случай», когда мы вообще не можем воспользоваться выведенной формулой для вычисления корней; такие случаи встречаются и у уравнений высших степеней, решаемых в радикалах.

ГЛАВА ТРИНАДЦАТАЯ

НЕКОТОРЫЕ ЧАСТНЫЕ ВИДЫ УРАВНЕНИЙ

§ 227. Приводимость и неприводимость. Уравнение $F(x) = 0$ m-й степени, являвшееся предметом исследования в предыдущей главе (§ 216 и ел.), могло быть как неприводимым, так и приводимым: требовалось лишь, чтобы оно не имело кратных корней. Исследуем, как его неприводимость или приводимость (в данной области $\mathbf{P}$) отражаются на его группе Галуа.

Если оно приводимо, то пусть в области $\mathbf{P}$

$$F(x) = F_1(x) \cdot F_2(x),$$

и пусть $\alpha_1, \alpha_2, \ldots, \alpha_k$ — корни уравнения $F_1(x) = 0$ k-й степени ($k < m$) в области $\mathbf{P}$. Равенство

$$F_1(\alpha_1) = 0$$

можно рассматривать как рациональное уравнение в $\mathbf{P}$ между корнями $\alpha_1, \alpha_2, \ldots, \alpha_m$ данного уравнения $F(x) = 0$; оно должно допускать все подстановки группы Галуа; но кроме значения α_1 уравнение $F_1(x) = 0$ удовлетворится еще только корнями $\alpha_2, \alpha_3, \ldots, \alpha_k$. Следовательно, все подстановки группы Галуа переводят $\alpha_1, \alpha_2, \ldots, \alpha_k$ только друг в друга, но не переводят ни один из этих корней ни в один из остальных корней $\alpha_{k+1}, \ldots, \alpha_m$. Это показывает, что группа Галуа в этом случае интранзитивна (§ 208).

Обратно, пусть группа Галуа данного уравнения в $\mathbf{P}$ интранзитивна, и пусть $\alpha_1, \alpha_2, \ldots, \alpha_k$ одна из ее транзитивных систем (§ 208); в таком случае подстановки группы Галуа только переставляют $\alpha_1, \alpha_2, \ldots, \alpha_k$ между собою, симметрические же функции от $\alpha_1, \alpha_2, \ldots, \alpha_k$ не меняются, т. е. являются рациональными количествами (из $\mathbf{P}$; § 218, теорема 1); следовательно, функция $F_1(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_k)$ есть функция в теле $\mathbf{P}$, но $F(x)$ делится на $F_1(x)$, т. е. $F(x)$ приводима в теле $\mathbf{P}$. Итак:

Теорема. *Если уравнение приводимо, то его группа Галуа интранзитивна; если же уравнение неприводимо, то его группа Галуа транзитивна.*

Заметим, что здесь имеется в виду группа Галуа как группа *подстановок*; на группе же рациональных функций корней резольвенты Галуа приводимость и неприводимость данного уравнения не отражается, ибо одна и та же резольвента Галуа может быть и у неприводимого, и у приводимого уравнения (сама она всегда неприводима). Существенную роль играет здесь также область рациональности $\mathbf{P}$: с расширением $\mathbf{P}$ неприводимое уравнение может сделаться приводимым, т. е. транзитивная группа Галуа может свестись к своей интранзитивной подгруппе.

§ 228. Примитивные и импримитивные уравнения. В § 215 было дано определение первообразного (примитивного) алгебраического тела $\mathbf{P}(\alpha)$ над $\mathbf{P}$: это такое алгебраическое тело над $\mathbf{P}$, которое не имеет делителей над $\mathbf{P}$, т. е. нет такого (алгебраического же — по теореме 4 § 215) тела $\mathbf{P}(\theta)$ над $\mathbf{P}$, чтобы было

$$\mathbf{P}(\alpha) \supset \mathbf{P}(\theta) \supset \mathbf{P}.$$

Неприводимое уравнение $F(x) = 0$ в теле $\mathbf{P}$, которому удовлетворяет α, тоже называется *первообразным* или *примитивным*. Если же тело $\mathbf{P}(\alpha)$ не первообразно, то и неприводимое уравнение для α $F(x) = 0$ в $\mathbf{P}$ называется *непервообразным* или *импримитивным*. Рассмотрим этот последний случай. Пусть θ — непервообразное (нерациональное) количество из тела $\mathbf{P}(\alpha)$, т. е. некоторая рациональная функция от α в теле $\mathbf{P}$:

$$\theta = \varphi(\alpha),$$

такая, что α не есть рациональная функция от θ в $\mathbf{P}$. Пусть тело $\mathbf{P}(\alpha)$ n-й степени, и $\alpha, \alpha', \alpha'', \ldots, \alpha^{(n-1)}$ — сопряженные с α количества, т. е. корни неприводимого в $\mathbf{P}$ уравнения $F(x) = 0$. В таком случае количества $\theta^\lambda = \varphi(\alpha^{(\lambda-1)})(\lambda = 1, 2, \ldots, n-1)$ распадаются на m систем по k равных друг другу количеств (§ 215, теорема 2); пусть, например:

$$\begin{aligned}
\theta &= \varphi(\alpha) = \varphi(\alpha_1) = \ldots = \varphi(\alpha_{k-1}),\\
\theta' &= \varphi(\alpha') = \varphi(\alpha'_1) = \ldots = \varphi(\alpha'_{k-1}),\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
\theta^{(m-1)} &= \varphi(\alpha^{(m-1)}) = \varphi(\alpha_1^{(m-1)}) = \ldots = \varphi(\alpha_{k-1}^{(m-1)}),
\end{aligned}$$

где $\alpha, \alpha_1, \ldots, \alpha_{k-1}$; $\alpha', \alpha'_1, \ldots, \alpha'_{k-1}$; $\ldots$; $\alpha^{(m-1)}, \alpha_1^{(m-1)}, \ldots, \alpha_{k-1}^{(m-1)}$ — иные обозначения для тех же количеств $\alpha, \alpha', \ldots, \alpha^{(n-1)}$; $n = km$.

Возьмем уравнение $\varphi(x) - \theta = 0$; ему удовлетворяют k количеств $\alpha, \alpha_1, \ldots, \alpha_{k-1}$, но не удовлетворяет никакое другое $\alpha_\mu^{(\lambda)}$, ибо $\varphi(\alpha_\mu^{(\lambda)} - \theta = \theta^\lambda - \theta \neq 0$, поскольку все $\theta, \theta', \ldots, \theta^{(m-1)}$, различны. Следовательно, $\alpha, \alpha_1, \ldots, \alpha_{k-1}$ — единственные общие корни уравнений $F(x) = 0$ и $\varphi(x) - \theta = 0$, и общий наибольший делитель функций $F(x)$ и $\varphi(x) - \theta$ есть [101]:

$$\Phi(x, \theta) = (x - \alpha)(x - \alpha_1) \cdots, (x - \alpha_{k-1}).$$

Так как функция $F(x)$ в теле $\mathbf{P}$, а функция $\varphi(x) - \theta$ — в теле $\mathbf{P}(\theta)$, то функция $\Phi(x, \theta)$ тоже в теле $\mathbf{P}(\theta)$, при этом θ не входит в знаменатель (в чем легко убедиться); таким образом $\Phi(x, \theta)$ есть целая рациональная функция от x и θ в теле $\mathbf{P}$. Докажем, что эта функция $\Phi(x, \theta)$ неприводимая функция от x в теле $\mathbf{P}(\theta)$. Пусть она делится на целую рациональную функцию от x тоже в теле $\mathbf{P}(\theta)$, с корнем α:

$$\Psi(x, \theta).$$

Эту функцию Ψ мы можем считать целою функцией) и от x и от θ (по § 144); возьмем уравнение:

$$\Psi(x, \varphi(x)) = 0;$$

[101] Мы предположили, что $\varphi(x)$ — рациональная функция в $\mathbf{P}$; но ведь мы знаем (§ 144), что ее можно всегда заменить целой рациональной, при этом даже степени большей или равной $n - 1$.

это—уравнение в $\mathbf{P}$, которому удовлетворяет корень α неприводимого в $\mathbf{P}$ уравнения $F(x) = 0$; следовательно, ему удовлетворяют и остальные корни того же неприводимого уравнения (§ 110, следствие II), в частности корни $\alpha, \alpha_1, \ldots, \alpha_{k-1}$, т. е.

$$\Psi(\alpha, \theta) = \Psi(\alpha_1, \theta) = \ldots = \Psi(\alpha_{k-1}, \theta) = 0.$$

Отсюда следует, что $\Psi(x, \theta)$ делится на $\Phi(x, \theta)$, т. е. $\Psi \equiv \Phi$, и значит, Φ неприводима в теле $\mathbf{P}(\theta)$. Итак:

Теорема. *Если уравнение $F(x) = 0$ в теле $\mathbf{P}$ импримитивно, то, присоединяя к $\mathbf{P}$ непервообразное количество θ из $\mathbf{P}(\alpha)$, мы сделаем $F(x)$ в теле $\mathbf{P}(\theta)$ приводимым: от $F(x)$ отделится множитель $\Phi(x, \theta)$ в теле $\mathbf{P}(\theta)$ степени выше первой, с корнем α.*

Если же уравнение $F(x) = 0$ (или тело $\mathbf{P}(\alpha)$) примитивно, то этого снижения степени уравнения для α мы не сможем достигнуть: тут все количества θ из $\mathbf{P}(\alpha)$ кроме рациональных первообразны; присоединив к $\mathbf{P}$ такое количество θ, мы сразу сделаем α рациональным, или отделим от $F(x)$ линейную функцию $x - \alpha$ в теле $\mathbf{P}(\theta) = \mathbf{P}(\alpha)$. В этом случае и уравнение для θ той же n-й степени, что и $F(x) = 0$.

Присоединив к $\mathbf{P}$, вместо θ, величину θ' или θ'', ..., или $\theta^{(m-1)}$, мы аналогично отделим от $F(x)$ неприводимые множители: $\Phi(x, \theta')$ в теле $\mathbf{P}(\theta')$, $\Phi(x, \theta'')$ в теле $\mathbf{P}(\theta'')$ и т. д., наконец, $\Phi(x, \theta^{(m-1)}$ в теле $\mathbf{P}(\theta^{(m-1)}$.

Легко видеть, что функция $\Phi(x, y)$ здесь одна и та же, — общий наибольший делитель функций $F(x)$ и $\varphi(x) - y$ при $y = \theta, \theta', \theta'', \ldots, \theta^{(m-1)}$. Таким образом в теле $\mathbf{P}(\theta, \theta', \theta'', \ldots, \theta^{(m-1)})$ функция $F(x)$ распадается на m множителей:

$$F(x) = \Phi(x, \theta)\Phi(x, \theta')\Phi(x, \theta'') \cdots \Phi(x, \theta^{(m-1)}).$$

Рассмотрим теперь группу Галуа $\mathfrak{G}$ уравнения $F(x) = 0$; она транзитивна, так как уравнение это неприводимо (§ 227). Пусть $\mathfrak{G}$ — ее подгруппа, подстановки которой оставляют α без изменения. Если существует тело $\mathbf{P}(\theta) \subset \mathbf{P}(\alpha)$, но $\supset \mathbf{P}$, то ведь ему (по теореме 2 § 220) соответствует определенная подгруппа $\mathfrak{H}$ группы $\mathfrak{G}$; а так как $\mathbf{P}(\theta) \subset \mathbf{P}(\alpha)$, то (по теореме 3 § 220) должно быть $\mathfrak{A} \subset \mathfrak{H} \subset \mathfrak{G}$, и обратно. А отсюда следует (§ 209).

Теорема. *Группа Галуа импримитивного уравнения импримитивна, а примитивного уравнения — примитивна.*

Заметим, что системы $\alpha, \alpha_1, \ldots, \alpha_{k-1}$; $\alpha', \alpha'_1, \ldots, \alpha'_{k-1}$; ...; $\alpha^{(m-1)}, \alpha_1^{(m-1)}, \ldots, \alpha_{k-1}^{(m-1)}$ являются системами импримитивности группы $\mathfrak{G}$.

§ 229. Уравнения третьей и четвертой степени. Мы еще раз возвращаемся к этим уравнениям, чтобы вкратце рассмотреть их решения с точки зрения теории Галуа.

Кубическое уравнение: $a_0x^3 + a_1x^2 + a_2x + a_3 = 0$; пусть x_1, x_2, x_3 его корни. Для уравнения в общем виде в абсолютной области рациональности $\mathbf{P}$ группа Галуа есть вся симметрическая группа третьей степени, 6-го порядка:

$$E, \quad A_1 = (2,3), \quad A_2 = (1,3), \quad A_3 = (1,2), \quad B == (1,2,3), \quad C = (1,3,2).$$

Она имеет инвариантную подгруппу индекса 2, — полусимметрическую группу третьей степени и 3-го порядка: E, B, C. Функция от корней, принадлежащая к

этой группе, есть произведение разностей:

$$(x_1 - x_2)(x_2 - x_3)(x_3 - x_1),$$

равное (с точностью до рационального множителя) $\sqrt{D}$, где D — дискриминант уравнения. Итак, присоединив к абсолютной области рациональности $\mathbf{P}$ количество $\sqrt{D}$, мы получим (по теореме 5 § 220) в теле $\mathbf{P}(\sqrt{D})$ группу нашего уравнения E, B, C; эта группа — простейшая, т. е. и уравнение наше в $\mathbf{P}(\sqrt{D})$ — простейшее; оно нормальное и является своей собственной резольвентой Галуа (см. теорему в § 221). Желая свести решение нашего уравнения к решению двучленного уравнения, т. е. к извлечению кубического корня, мы должны найти такую функцию от корней x_1, x_2, x_3, куб которой допускал бы циклическую подстановку $B = (1, 2, 3)$ [а, значит, и $C = B^2$, т. е. был бы в теле $\mathbf{P}(\sqrt{D})$]. Отсюда следует, что сама эта функция от подстановки B может только получить множителем корень кубический из единицы $\omega = \dfrac{-1 + i\sqrt{3}}{2}$ или ω^2. Для этого присоединим заранее ω, или, что то же самое, $\sqrt{-3}$, к нашему телу $\mathbf{P}(\sqrt{D})$; от этого уменьшения группы уменьшения группы не последует, но нам это понадобится.

Теперь строим резольвенты Лагранжа (§ 224):

$$u = x_1 + \omega x_2 + \omega^2 x_3,$$
$$v = x_1 + \omega^2 x_2 + \omega x_3.$$

Легко видеть, что от подстановки B u переходит в $\omega^2 u$, а v — в ωv, и следовательно, u^3, v^3, uv не меняются; значит, u и v — кубические корни из рациональных функций от коэфициентов и выражаются рационально один через другой, ибо uv тоже рационально. Взяв еще уравнение $x_1 + x_2 + x_3 = -\dfrac{a_1}{a_0}$, найдем:

$$3x_1 = -\frac{a_1}{a_0} + u + v,$$
$$3x_2 = -\frac{a_1}{a_0} + \omega^2 u + \omega v$$
$$3x_3 = -\frac{a_1}{a_0} + \omega u + \omega^2 v.$$

Предлагается читателю проверить вычислением, что это — те же самые формулы, что и в § 124.

Уравнение четвертой степени: $a_0 x^4 + a_1 x^3 + a_2 x^2 + a_3 x + a_4 = 0$. И здесь мы присоединяем к абсолютной области рациональности $\mathbf{P}$ корень квадратный из дискриминанта, или, иными словами, произведение:

$$(x_1 - x_2)(x_1 - x_3)(x_1 - x_4)(x_2 - x_3)(x_2 - x_4)(x_3 - x_4),$$

где x_1, x_2, x_3, x_4 — корни нашего уравнения. Этим мы сводим группу Галуа нашего уравнения, которая есть в общем случае симметрическая группа четвертой степени, 24-го порядка, к полусимметрической группе четвертой степени и 12-го порядка, именно:

$$\begin{aligned} E,\ A &= (1,2)(3,4),\quad B = (1,3)(2,4),\quad C = (1,4)(2,3),\\ A_1 &= (1,2,3),\quad A_2 = (1,3,2),\quad A_3 = (1,2,4),\quad A_4 = (1,4,2),\\ A_5 &= (1,3,4),\quad A_6 = (1,4,3),\quad A_7 = (2,3,4),\quad A_8 = (2,4,3). \end{aligned}$$

Мы знаем (§ 207), что композиционный ряд для этой полусимметрической группы 12-го порядка $\mathfrak{G}$ есть:

$$\mathfrak{R}, \quad \mathfrak{Q}, \quad \mathfrak{Q}_1,$$

где $\mathfrak{Q}$ — четверная группа E, A, B, C; $\mathfrak{Q}_1$ — группа 2-го порядка E, A; ряд индексов: $3, 2, 2$. Следовательно, согласно общей теории (§ 222) решение уравнения четвертой степени сводится к решению одного кубического уравнения с группой $\frac{\mathfrak{R}}{\mathfrak{Q}}$ и двух квадратных с группами $\frac{\mathfrak{Q}}{\mathfrak{Q}_1}$ и $\mathfrak{Q}_1$. Мы видим, таким образом, что кубическое уравнение необходимо должно входить в эту цепь уравнений; только в том случае, если эта кубическая резольвента имеет рациональный корень, она как будто бы избегается; такие случаи мы имеем у так называемого «биквадратного», уравнения и у возвратного уравнения четвертой степени, рассматриваемых в элементарной алгебре.

Итак, первым делом мы должны составить функцию от корней, принадлежащую к группе $\mathfrak{Q} = E+A+B+C$, т. е. при всех подстановках группы $\mathfrak{R}$, принимающей только три значения. Такую функцию можно составить различным образом; выражения $x_1x_2 + x_3x_4$, $(x_1 - x_2)(x_3 - x_4)$, $(x_1 + x_2 - x_3 - x_4)^2$ служат примерами таких функций; самое удобное из них последнее, ибо оно позволяет последующим извлечением квадратного корня найти линейные функции от корней. Итак, берем:

$$v_1 = (x_1 + x_2 - x_3 - x_4)^2;$$

перестановками корней найдем еще два значения этой функции:

$$v_2 = (x_1 - x_2 + x_3 - x_4)^2,$$
$$v_3 = (x_1 - x_2 - x_3 + x_4)^2.$$

Можно легко убедиться, что при всех 24 подстановках корней эти функции только переходят одна в другую; следовательно, симметрические функции от них являются симметрическими функциями от корней x_1, x_2, x_3, x_4, т. е. выражаются рационально через коэфициенты данного уравнения; таким образом мы способами § 138–141 можем выразить через коэфициенты данного уравнения коэфициенты того уравнения, корнями которого являются v_1, v_2, v_3, т. е. уравнения:

$$(v - v_1)(v - v_2)(v - v_3) = 0.$$

(Это и есть кубическая резольвента). Решив его и найдя затем v_1, v_2, v_3, получим:

$$x_1 + x_2 - x_3 - x_4 = \sqrt{v_1},$$
$$x_1 - x_2 + x_3 - x_4 = \sqrt{v_2},$$
$$x_1 - x_2 - x_3 + x_4 = \sqrt{v_3},$$
$$x_1 + x_2 + x_3 + x_4 = \frac{a_1}{a_0}.$$

Можно легко проверить, что произведение $\sqrt{v_1}\sqrt{v_2}\sqrt{v_3}$ — тоже симметрическая функция от корней, т. е. рационально выражается через коэфициенты нашего уравнения; это показывает, что между этими тремя корнями $\sqrt{v_1}$, $\sqrt{v_2}$, $\sqrt{v_3}$ есть

зависимость: два из них вполне определяют третий, что ограничивает число комбинаций их знаков четырьмя. Таким образом найдем:

$$4x_1 = -\frac{a_1}{a_0} + \sqrt{v_1} + \sqrt{v_2} + \sqrt{v_3},$$
$$4x_2 = -\frac{a_1}{a_0} + \sqrt{v_1} - \sqrt{v_2} - \sqrt{v_3},$$
$$4x_3 = -\frac{a_1}{a_0} - \sqrt{v_1} + \sqrt{v_2} - \sqrt{v_3},$$
$$4x_4 = -\frac{a_1}{a_0} - \sqrt{v_1} - \sqrt{v_2} + \sqrt{v_3}.$$

Легко видеть, что это — те же формулы, что и в § 128.

§ 230. Уравнения деления угла. Задача деления угла на равные части аналитически выражается так: по данным $\cos m\varphi$ и $\sin m\varphi$ найти $\cos\varphi$ и $\sin\varphi$ (m — целое число, большее нуля). Таким образом $\cos m\varphi$ и $\sin m\varphi$ даны нам как определенные числа, по абсолютной величине меньшие единице, причем сумма их квадратов равна единице.

К абсолютной области рациональности мы присоединяем $\cos m\varphi$, $\sin m\varphi$, $\cos\dfrac{2\pi}{m}$ и $\sin\dfrac{2\pi}{m}$ и полученное после этого присоединения тело обозначаем через $\mathbf{P}$.

Обозначим $x = 2\cos\varphi$; тогда x определится из уравнения:

$$2\cos m\varphi = m\sum_{\lambda=0}^{\left[\frac{m}{2}\right]} \frac{(-1)^\lambda (m-\lambda-1)!}{\lambda!(m-2\lambda)!}\, x^{m-2\lambda} \tag{1}$$

(§ 137). Это уравнение m-й степени. Найдя $\cos\varphi$, мы определим $\sin\varphi$ по формуле (тоже § 137):

$$\frac{\sin m\varphi}{\sin\varphi} = \sum_{\lambda=0}^{\left[\frac{m}{2}\right]} (-1)^\lambda \binom{m-\lambda-1}{\lambda} x^{m-2\lambda-1}, \tag{2}$$

из которой видно, что $\sin\varphi$ выражается рационально через x; m корней уравнения (1) имеют следующие тригонометрические значения:

$$x_0 = 2\cos\varphi, \quad x_1 = 2\cos\left(\varphi + \frac{2\pi}{m}\right), \ \ldots, \ x_{n-1} = 2\cos\left(\varphi + \frac{2(m-1)\pi}{m}\right).$$

Применяя элементарную формулу для косинуса суммы, легко убедиться, что каждый из этих корней есть одна и та же рациональная функция в $\mathbf{P}$ от предыдущего:

$$x_1 = f(x_0), \quad x_2 = f(x_1), \ \ldots, \ x_{m-1} = f(x_{m-2)}, \quad x_0 = f(x_{m-1}). \tag{3}$$

Сверх того уравнение (1) неприводимо в $\mathbf{P}$, ибо если какому-нибудь алгебраическому уравнению в $\mathbf{P}$ удовлетворяет корень x_0:

$$\Phi(x_0, \cos m\varphi, \sin m\varphi) = 0,$$

то, заменив φ на $\varphi + \dfrac{2k\pi}{m}$, мы этого уравнения не нарушим (ибо $\cos m\varphi$ и $\sin m\varphi$ от этого не изменяются), но она перейдет в такое:

$$\Phi(x_k, \cos m\varphi, \sin m\varphi) = 0,$$

т. е. ему удовлетворяют все корни x_k, и следовательно, функция Φ делится на функцию $m \sum_{\lambda=0}^{\left[\frac{m}{2}\right]} \dfrac{(-1)^\lambda (m-\lambda-1)!}{\lambda!(m-2\lambda)!}\, x^{m-2\lambda} - 2\cos m\varphi$, откуда следует, что (1) — неприводимое уравнение.

Отсюда же и из (3) следует, что (1) — нормальное уравнение, т. е. своя собственная резольвента Галуа, и при этом циклическое уравнение; следовательно, оно решается в радикалах (§ 224).

Например, при $m = 3$ имеем уравнение деления угла на три равные части:

$$x^3 - 3x = 2\cos 3\varphi.$$

При произвольном угле 3φ это уравнение неприводимо; оно циклическое; при его решении обязательно приходится извлекать кубический корень. Отсюда следует невозможность деления угла на три равные части при помощи циркуля и линейки, ибо, как известно, при помощи циркуля и линейки можно извлекать точно только квадратные корни.

§ 231. Уравнения деления окружности. Мы уже имели эти уравнения в главе VII, § 120—122; это — уравнение:

$$\Phi_n(x) = 0 \tag{4}$$

степени $\varphi(n)$ [где $\varphi(n)$ означает число натуральных чисел, меньших, чем n, и взаимно простых с n, имеющее корнями все первообразные корни (§ 118) n-й степени из единицы. Мы видели (в § 120–121), что все коэфициенты этого уравнения — целые числа, и для случая, когда n — степень простого числа, доказали, что это уравнение неприводимо (§ 122) в абсолютной области рациональности.

Легко дать решения уравнения (4) в тригонометрической форме: еще в главе I, § 9 мы имели корни n-й степени из единицы в виде:

$$r_k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n} \qquad (k = 0, 1, 2, \ldots, n-1), \tag{5}$$

или сокращенно:

$$r_k = e^{\frac{2k\pi i}{n}}{}^{102}. \tag{5}$$

Первообразные корни будут, очевидно, те, где дробь $\dfrac{k}{n}$ несократима, т. е. где k — взаимно простое с n; число их и есть как раз $\varphi(n)$. При $k = 1$ получаем из (5) всегда первообразный корень; но получаемая при этом дуга $\dfrac{2\pi}{n}$ есть $\dfrac{1}{n}$—я часть 2π, т. е. целой окружности; таким образом алгебраическая задача решения уравнения (4)

[102]Мы применяем тут известную формулу Эйлера: $e^{\alpha i} = \cos\alpha + i\sin\alpha$ (ср. сноску в § 137).

выражается геометрически как деление окружности на n равных частей, откуда происходит и самое название уравнения (4).

Мы рассмотрим теперь алгебраическое решение уравнения (4), причем ограничимся случаем, когда $n = p$ — простое число. Мы имели (§ 120) для этого случая:

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + x + 1 = 0. \tag{4}$$

В § 223, 224 мы доказали, что это уравнение (4a) нормальное и при этом циклическое: именно, если r — один из его корней и через g мы обозначим один из первообразных корней простого числа p, то все корни уравнения (4a) выразятся так:

$$r, \quad r^g, \quad r^{g^2} = (r^g)^g, \quad r^{g^3} = (r^{g^2})^g, \ \ldots, \ r^{g^{p-2}}, \tag{6}$$

тогда как $(r^{g^{p-2}})^p = r^{g^{p-1}} = r$. Числа (6) — те же самые, что

$$r, \quad r^2, \quad r^3, \ \ldots, \ r^{p-1}, \tag{7}$$

только в ином порядке.

В § 224 мы указали общий способ решения циклических уравнений в радикалах, который можно применить и к данному случаю. Но мы укажем здесь иной способ, именно — способ Гаусса сведения нашего уравнения (4a) к цепи простейших уравнений [103]. За исключением тривиального случая $p = 3$ уравнение (4a) не простейшее, ибо $p-1$ четное, т. е. не простое число. Группа Галуа этого уравнения есть циклическая группа, состоящая из степеней цикла $A = (r, r^g, r^{g^2}, \ldots, r^{g^{p-2}} = (0, 1, 2, \ldots, p-2)$, значит, эта группа регулярная (§ 208), т. е. кроме E в ней нет подстановки, которая хотя бы один символ оставляла без изменения. Отсюда же следует, что эта группа $\{A\}$ импримитивная (§ 209), ибо она имеет подгруппу, и каждая подгруппа, конечно, содержит E. А следовательно, по последней теореме § 228 и уравнение (4a) импримитивно, и мы можем, расширив подходящим образом нашу область $\mathbf{P}$ (которая вначале — абсолютная область рациональности), сделать уравнение (4a) приводимым (по первой теореме § 228).

Пусть $p - 1 = ef$ некоторое разложение $p - 1$ на два натуральных множителя; докажем, что в теле $\mathbf{P}(r)$ существует количество, удовлетворяющее неприводимому в $\mathbf{P}$ уравнению e-й степени; присоединив это количество η_0 к $\mathbf{P}$, получим, что в теле $\mathbf{P}(\eta_0)$ корень r удовлетворит неприводимому уравнению f-й степени. А так как, чтобы решить циклическое уравнение (4a), достаточно найти один его корень r, то мы видим, что это решение одного уравнения (4a) степени $p - 1$ сведется к решению уравнения e-й степени и уравнения f-й степени; оба эти уравнения, как мы увидим, тоже циклические, и если они не простейшие, то их можно свести таким же образом дальше, — пока не сведем уравнение (4a) на цепь простейших уравнений. Возьмем:

$$\eta_0 = r + r^{g^e} + r^{g^{2e}} + \ldots + r^{g^{(f-1)e}};$$

легко проверить, что η_0 не изменится от подстановки A^e, т. е. и от ее степеней, значит, от всех подстановок циклической группы $\{A^e\}$ f-го порядка [ибо $(A^e)^f =$

[103] C. F. Gauss, Disquisitiones arithmeticae (1801), отд. VI

$A^{ef} = A^{p-1} = E$], тогда как от применения к η_0 подстановки A или A^{e+1}, или вообще A^{ke+1} (k — целое) получим:

$$\eta_1 = r^g + r^{g^{e+1}} + r^{g^{2e+1}} + \ldots + r^{g^{(f-1)e+1}};$$

от применения к η_0 подстановок $A^2, A^{e+2}, \ldots, A^{ke+2}$ получим:

$$\eta_2 = r^{g^2} + r^{g^{e+2}} + r^{g^{2e+2}} + \ldots + r^{g^{(f-1)e+2}}$$

и т. д.; наконец, от применения к η_0 подстановок $A^{e-1}, A^{2e-1}, \ldots, A^{fe-1} = A^{p-2}$ получим:

$$\eta_{e-1} = r^{g^{e-1}} + r^{g^{2e-1}} + r^{g^{3e-1}} + \ldots + r^{g^{p-2}}.$$

Эти выражения $\eta_0, \eta_1, \ldots \eta_{e-1}$, Гаусс назвал *$f$-членными периодами*; число их $= e = \dfrac{p-1}{f}$. Мы докажем, что все они различны, откуда будет следовать, что η_0 — функция от корней, принадлежащая к группе $\{A^e\}$. Докажем, именно, более общую теорему:

Теорема 1. *Количества $\eta_0, \eta_1, \eta_2, \ldots, \eta_{e-1}$ линейно независимы (в абсолютной области рациональности $\mathbf{P}$).*

Доказательство. Пусть имеет место равенство:

$$k_0\eta_0 + k_1\eta_1 + \ldots + k_{e-1}\eta_{e-1} = 0$$

с целыми рациональными $k_0, k_1, \ldots, k_{e-1}$. Подставив значения для $\eta_0, \eta_1, \ldots, \eta_{e-1}$, получим:

$$k_0(r^g + r^{g^{e+1}} + r^{g^{2e+1}} + \ldots + r^{g^{(f-1)e+1}}) + k_1(r^g + r^{g^{e+1}} + r^{g^{2e+1}} + \ldots + r^{g^{(f-1)e+1}}) + \ldots + \\ + k_{e-1}(r^{g^{e-1}} + r^{g^{2e-1}} + r^{g^{3e-1}} + \ldots + r^{g^{p-2}}) = 0.$$

Но во все η_λ входят все корни r^λ ($\lambda = 1, 2, \ldots, p-1$), и каждый по одному разу; следовательно, если в предыдущем равенстве раскроем скобки, заменим каждый из показателей его наименьшим положительным вычетом по модулю p, расположим по возрастающим степеням r и сократим на общий множитель r, который не равен нулю, то получим:

$$l_0 + l_1 r + l_2 r^2 + \ldots + l_{p-2} r^{p-2} = 0,$$

где $l_0, l_1, l_2, \ldots, l_{p-2}$ — те же количества $k_0, k_1, \ldots, k_{e-1}$, только в ином порядке, и каждое k_λ повторяется f раз. Последнее равенство показывает, что r удовлетворяет уравнению $(p-2)$-й степени в $\mathbf{P}$, тогда как r удовлетворяет в $\mathbf{P}$ неприводимому уравнению (4a) $(p-1)$-й степени, и значит, уравнению низшей степени в $\mathbf{P}$ удовлетворять не может. Следовательно, все $l_\lambda = 0$ или, что то же самое, все $k_\lambda = 0$, т. е. $\eta_0, \eta_1, \ldots, \eta_{e-1}$ действительно линейно независимы.

Следствие. Количества $\eta_0, \eta_1, \ldots, \eta_{e-1}$ все различны между собою, ибо равенство $\eta_\lambda = \eta_\mu$ или $\eta_\lambda - \eta_\mu = 0$ есть частный случай линейной зависимости.

Теорема 2. *Периоды $\eta_0, \eta_1, \ldots, \eta_{e-1}$ в своей совокупности не зависят от выбора первообразного корня g простого числа p.*

Доказательство. Пусть γ отличный от g первообразный корень простого числа p; из теории чисел известно, что тогда

$$\gamma \equiv g^h \pmod p,$$

где h — число взаимно простое с $p-1$, а следовательно, и с e и с f. Имеем:

$$\varepsilon_0 = r + r^{\gamma^e} + r^{\gamma^{2e}} + \ldots + r^{\gamma^{(f-1)e}} = r + r^{g^{he}} + r^{g^{2he}} + \ldots r^{g^{(f-1)he}};$$

но так как $D(h,f)=1$, то числа $0, h, 2h, \ldots, (f-1)h$ по модулю f сравнимы с числами $0, 1, 2, \ldots, f-1$, только в ином порядке, а следовательно:

$$\varepsilon_0 = \eta_0.$$

Подобным же образом докажем: $\varepsilon_1 = \eta_h$, $\varepsilon_2 = \eta_{2h}$, $\ldots$, $\varepsilon_{e-1} = \eta_{(e-1)h}$; но числа $0, h, 2h, \ldots, (e-1)h$ сравнимы по модулю e с числами $0, 1, 2, \ldots, e-1$, только стоят в другом порядке; отсюда следует, что периоды $\varepsilon_0, \varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{e-1}$ отличаются от периодов $\eta_0, \eta_1, \eta_2, \ldots, \eta_{e-1}$ только порядком, в котором они стоят, и теорема доказана.

Теорема 3. *Сумма всех f-членных периодов равна -1.*

Доказательство. Это следует из того, что во всех ?-членных периодах встречаются все корни уравнения (4a), и каждый по одному разу; следовательно, сумма f-членных периодов равна сумме всех корней уравнения (4a), т. е. равна -1:

$$\eta_0 + \eta_1 + \ldots + \eta_{e-1} = -1.$$

Теорема 4. *Всякая целая рациональная функция периодов $\eta_0, \eta_2, \ldots, \eta_{e-1}$ представляется как линейная функция от тех же периодов, причем если, в данной целой рациональной функции все коэфициенты целые, то и в получаемой линейной функции все коэфициенты остаются целыми.*

Доказательство. Принимая во внимание, что сумма линейных функций есть тоже линейная функция, мы должны только доказать предложенную теорему для произведения двух (различных или равных) f-членных периодов. Итак, имеем:

$$\begin{aligned}
\eta_\lambda \eta_\mu &= (r^{g^\lambda} + r^{g^{e+\lambda}} + \ldots + r^{g^{(f-1)e+\lambda}})(r^{g^\mu} + r^{g^{e+\mu}} + \ldots + r^{g^{(f-1)e+\mu}}) = \\
&= r^{g^\lambda + g^\mu} + r^{g^\lambda + g^{e+\mu}} + \ldots + r^{g^\lambda + g^{(f-1)e+\mu}} + \\
&+ r^{g^{e+\lambda} + g^\mu} + r^{g^{e+\lambda} + g^{e+\mu}} + \ldots + r^{g^{e+\lambda} + g^{(f-1)e+\mu}} + \\
&+ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots + \\
&+ r^{g^{(f-1)e+\lambda} + g^\mu} + r^{g^{(f-1)e+\lambda} + g^{e+\mu}} + \ldots + r^{g^{(f-1)e+\lambda} + g^{(f-1)e+\mu}}.
\end{aligned}$$

Будем суммировать по диагоналям:

$$\begin{aligned}
r^{g^\lambda + g^\mu} &+ r^{g^{e+\lambda} + g^{e+\mu}} + \ldots + r^{g^{(f-1)e+\lambda} + g^{(f-1)e+\mu}} = \\
&= r^{g^\lambda + g^\mu} + r^{(g^\lambda + g^\mu)g^e} + \ldots + r^{(g^\lambda + g^\mu)g^{(f-1)e}};
\end{aligned}$$

если тут $g^\lambda + g^\mu$ не делится на p, то $g^\lambda + g^\mu \equiv g^\nu \pmod p$, и мы получаем просто η_ν (где ν — какое-то из чисел $0, 1, 2, \ldots, p-2$) или η_{ν_1}, если $\nu_1 \equiv \nu \pmod e$; если

$g^\lambda = g^\mu$ делится на p, то каждое слагаемое равно единице, а вся сумма равна f, вместо чего (по теореме 4) можно написать $-f(\eta_0 + \eta_1 + \ldots + \eta_{e-1})$.

Подобным же образом суммируем:

$$\begin{aligned} r^{g^\lambda + g^{e+\mu}} &+ r^{g^{e+\lambda} + g^{2e+\mu}} + \ldots + r^{g^{(f-1)e+\lambda} + g^\mu} = \\ &= r^{g^\lambda + g^{e+\mu}} + r^{(g^\lambda + g^{e+\mu})g^e} + \ldots + r^{(g^\lambda + g^{e+\mu})g^{(f-1)e}}, \end{aligned}$$

ибо $g^{e+\mu} g^{(f-1)e} \equiv g^{fe+\mu} \equiv g^\mu$, так как $g^{fe} \equiv g^{p-1} \equiv 1 \pmod p$. Теперь опять различаем два случая: 1) если $g^\lambda + g^{e+\mu}$ не делится на p, то, следовательно, $g^\lambda + g^{e+\mu} \equiv g^\rho \pmod p$, и взятая сумма дает η_ρ; 2) если $g^\lambda + g^{e+\mu}$ делится на p, то взятая сумма дает $-f(\eta_0 + \eta_1 + \ldots + \eta_{e-1}$ и т. д.

Этим наша теорема доказана; что коэфициенты остаются целыми, следует из того, что при всей этой операции мы нигде не вводим дробей.

Теорема 5. *Всякая целая симметрическая функция от $\eta_0, \eta_1, \ldots, \eta_{e-1}$ с целыми коэфициентами есть целое число.*

Доказательство. Это следует из общей теории (§ 215), ибо $\eta_0, \eta_1, \ldots, \eta_{e-1}$ — сопряженные алгебраические количества относительно абсолютной области $\mathbf{P}$, и следовательно, их симметрические функции имеют рациональные значения. Но так как, по теореме 4, всякая целая рациональная функция от η_λ сводится к линейной функции от них же, а единственная симметрическая линейная функция есть сумма $\eta_0 + \eta_1 + \ldots + \eta_{e-1}$, равная -1, то в случае, когда коэфициенты данной функции целые, дробям неоткуда будет взяться и теорема 6 доказана.

В таком же духе можно продолжать далее: пусть $f = e'f'$, т. е. $p - 1 = (ee')f'$; можно построить (ee') периодов с f' членами:

$$\begin{aligned} \eta'_0 &= r + r^{g^{ee'}} + r^{g^{2ee'}} + \ldots + r^{g^{(f'-1)ee'}}, \\ \eta'_1 &= r^g + r^{g^{ee'+1}} + r^{g^{2ee'+1}} + \ldots + r^{g^{(f'-1)ee'+1}}, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \eta'_e &= r^{g^e} + r^{g^{ee'+e}} + r^{g^{2ee'+e}} + \ldots + r^{g^{(f'-1)ee'+e}}, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \eta'_{ee'-1} &= r^{g^{ee'-1}} + r^{g^{2ee'-1}} + r^{g^{3ee'-1}} + \ldots + r^{g^{f'ee'-1}}. \end{aligned}$$

Легко видеть, что

$$\eta_0 = \eta'_0 + \eta'_e + \eta'_{2e} + \ldots + \eta_{(e'-1)e};$$

относительно этих периодов $\eta'_0, \eta'_e, \eta'_{2e}, \ldots, \eta'_{(e'-1)e}$ правильны те же теоремы, что и относительно $\eta_0, \eta_1, \ldots, \eta_{e-1}$, конечно, с соответствующими модификациями: все они различные корни одного и того же неприводимого уравнения в теле $\mathbf{P}(\eta_0)$; коэфициенты этого уравнения — линейные функции от $\eta_0, \eta_1, \ldots, \eta_{e-1}$, (по теореме 4); группа Галуа этого уравнения — циклическая, именно: $\dfrac{\{A^e\}}{\{A^{ee'}\}}$ (§ 220, теорема 7); сама же функция η'_0 от корней уравнения (4a) принадлежит к группе $\{A^{ee'}\}$.

Продолжая это построение, мы придем к следующему правилу сведения уравнения (4a) к цепи простейших уравнений: раскладываем $p - 1$ на простые множители:

$$p - 1 = abc \cdots k$$

и сначала строим a $\dfrac{p-1}{a}$-членных периодов η; они удовлетворяют неприводимому простейшему уравнению a-й степени с целыми коэфициентами; решив его, т. е. найдя периоды η и присоединив один из них (а следовательно, и все) к $\mathbf{P}$, мы увидим, что левая часть уравнения (4) распадается на a сомножителей степени $\dfrac{p-1}{a}$. Далее, распределяем корни, из которых состоит период η на b меньших периодов η' с $\dfrac{p-1}{ab}$ членами; те периоды η', которые составляют один период η, удовлетворяют простейшему уравнению b-й степени в теле $\mathbf{P}(\eta)$. Найдя η', присоединяем одно из них к $\mathbf{P}(\eta)$; распределяем корни, из которых состоит период η' на c более мелких периодов η'' с $\dfrac{p-1}{abc}$ членами и т. д. В конце концов придем к одночленным периодам, т. е. к самим корням r, и найдем их, решив последние из наших простейших уравнений.

§ 232. Из предыдущего параграфа следует, что для того, чтобы можно было разделить окружность на p равных частей при помощи циркуля и линейки, необходимо и достаточно, чтобы все простейшие уравнения, на которые сводится наше уравнение (4а), были квадратными, ибо тогда решение уравнения (4а) сведется к извлечению цепи квадратных корней, которое можно осуществить при помощи циркуля и линейки; а для этого $p-1$ должно иметь простыми множителями только двойки, т. е. должно быть $p-1=2^k$, откуда

$$p=2^k+1.$$

Мы докажем, что 2^k+1 может быть простым только, если k степень двух. Пусть $k=uv$, где u — нечетное; имеем:

$$\frac{x^u+1}{x+1}=1-x+x^2-\ldots+x^{u-1};$$

положив $x=2v$, получим:

$$2^{uv}+1=(2^v+1)(1-2^v+2^{2v}-\ldots+2^{(u-1)v}),$$

т. е. $2^{uv}+1$ делится на 2^v+1 и значит, непростое.

Итак, должно быть: $p=2^{2^n}+1$ — простое число.

Рассмотрим таблицу:

n	$2^{2^n}+1$
0	3
1	5
2	17
3	257
4	65537

Здесь в правой части таблицы все числа простые. Ферма предположил, что $2^{2^n}+1$ при всяком n есть простое число; но Эйлер показал, что уже при $n=5$ число $2^{2^5}+1$ не простое: оно делится на 641. При $n=6$ число $2^{2^6}+1$ тоже не простое: оно делится на 274177. Доказано, что при $n=12,23,36$ соответствующие числа $2^{2^n}+1$ не простые.

Еще древние греки умели делить окружность при помощи циркуля и линейки на 2^λ, на 3, на 5 частей и на число частей, равное произведению этих чисел. Но в общем виде решил задачу о делении окружности при помощи циркуля и линейки только Гаусс, отметив точно и дату этого своего важного открытия: 30 марта 1796 года, когда ему еще не было полных 19 лет. Он первый показал, что при помощи циркуля и линейки окружность можно разделить и на 17 частей.

Заметим, что, умея делить окружность на k и на l равных частей, мы сумеем разделить ее и на kl равных частей, если k и ? — взаимно простые; это следует просто из того, что неопределенное уравнение $kx + ky = 1$ всегда имеет целые решения при $\mathbf{D}(k, l) = 1$; из этого уравнения следует:

$$\frac{x}{l} + \frac{y}{k} = \frac{1}{kl},$$

т. е., зная $\frac{1}{k}$-ю и $\frac{1}{l}$-ю части окружности, мы по полученной формуле построим и $\frac{1}{kl}$-ю часть окружности.

Таким образом, умея делить окружность на $p, q, r, \ldots$ равных частей (где p, q, r, $\ldots$— различные простые числа вида $2^{2^k} + 1$), мы сумеем разделить ее и на $2^\lambda pqr \ldots$ равных частей.

Возникает вопрос: можно ли делить окружность циркулем и линейкой на p^λ частей, где p — простое, а $\lambda > 1$? Но уравнение $\Phi_{p^\lambda}(x) = 0$ степени $\varphi(p^\lambda) = p^{\lambda-1}(p-1)$; это число при нечетном p не есть степень двух, ибо оно делится на p. Поэтому, рассуждая, как и раньше, найдем, что ни при каком нечетном простом p нельзя разделить окружность циркулем и линейкой на p^λ частей при $\lambda > 1$; следовательно, и подавно нельзя разделить окружносгь на m частей, где m делится по крайней мере на один квадрат простого нечетного числа. Итак:

Теорема. *При помощи циркуля и линейки можно разделить окружность на* 2^λ, *на* p *и на*

$$m = 2^\lambda pp'p'' \ldots$$

равных частей, где $\lambda \geq 0$, *а* p, p', p'', $\ldots$ — *различные простые числа вида* $2^{2^n} + 1$; *больше ни на какое число равных частей нельзя разделить окружность при помощи циркуля и линейки.*

Пример 1. $p = 5$; уравнение: $x^4 + x^3 + x^2 + x + 1 = 0$, $p - 1 = 4 = 2 \cdot 2$. Один из первообразных корней числа 5 есть $g = 2$.

Составляем:

$$\eta_0 = r + r^4 = r + r^{-1},$$

ибо $r^5 = 1$,

$$\eta_1 = r^2 + r^3 = r^2 + r^{-2};$$

$\eta_0 + \eta_1 = -1$, $\eta_0\eta_1 = -1$. Следовательно, уравнение для η_0, η_1 имеет вид:

$$\eta^2 + \eta - 1, \quad \text{откуда} \quad \eta = \frac{-1 \pm \sqrt{5}}{2}.$$

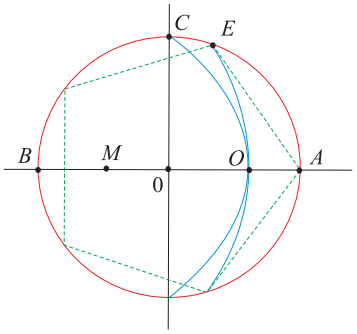
Можно выразить η и в трансцендентной форме: ведь $r = \cos\frac{2\pi}{5} + i\sin\frac{2\pi}{5}$, $r^4 = r^{-1} = \cos\frac{2\pi}{5} - i\sin\frac{2\pi}{5}$; отсюда $\eta_0 = 2\cos\frac{2\pi}{5}$. Таким же образом находим $\eta_1 =$

$2\cos\frac{4\pi}{5}$. Отсюда видно, что $\eta_0 > 0$, следовательно: $\eta_0 = \frac{-1+\sqrt{5}}{2}$, $\eta_1 = \frac{-1-\sqrt{5}}{2}$ и, наконец:

$$\cos\frac{\pi}{5} = \cos\left(\pi - \frac{4\pi}{5}\right) = \frac{1+\sqrt{5}}{4},$$

r удовлетворяет уравнению $x^2 - \eta_0 x + 1 = 0$.

Отсюда вытекает способ геометрического построения $\frac{1}{5}$-й части окружности: делим (черт. 28) OB пополам в точке M; радиусом MC описываем дугу пересекающую AB в точке D радиусом BD описываем дугу с центром в B, пересекающую данную окружность в точке E; дуга AE и есть искомая $\frac{1}{5}$-я часть окружности.



Черт. 28

Действительно, пусть радиус окружности $OA = OB = 1$; тогда

$$MO = \frac{1}{2}, \quad MC = \frac{1}{2}\sqrt{5}, \quad MD = \frac{1}{2}\sqrt{5}, \quad BD = BE = \frac{1}{2}(1+\sqrt{5});$$

из треугольника BEA находим: $\frac{BE}{BA} = \frac{1+\sqrt{5}}{4} = \cos(\angle ABE)$, следовательно, $ABE = \frac{\pi}{5}$, а отсюда $\angle AOE = \frac{2\pi}{5}$, что и требовалось доказать.

Пример 2. $p = 11$; уравнение $\frac{x^{11}-1}{x-1} = 0$ можно свести к уравнению степени $\frac{p-1}{2} = 5$; это последнее уравнение — циклическое; оно является первым по времени уравнением пятой степени, решенным в радикалах. Его решил Вандермонд (Vandermonde) в 1770 г., в сочинении «Mèmoire sur la résolution des équations».

Один из первообразных корней числа 11 есть $g = 2$; строим таблицу:

η_0	=	0	1	2	3	4	5	6	7	8	9	10
2^λ	$\equiv$	1	2	4	8	5	10	9	7	3	6	1

Находим пятичленные периоды:

$$\eta_0 = r + r^4 + r^5 + r^9 + r^3,$$
$$\eta_1 = r^2 + r^3 + r^{10} + r^7 + r^6;$$

вычисляя, найдем $\eta_0 + \eta_1 = -1$, $\eta_0\eta_1 = 3$; следовательно, уравнение для η_0, η_1 будет: $\eta^2 + \eta + 3 = 0$, уравнение для r:

$$x^5 - \eta_0 x^4 - x^3 + x^2 - \eta_0 x - 1 = 0;$$

его корни: r, r^4, r^5, r^9, r^3; коэфициенты его вычисляются как элементарные симметрические функции от этих корней.

Мы можем решись уравнение $\frac{x^{11}-1}{x-1} = 0$ иначе; составим сначала 5 двучленных периодов:

$$z_1 = r + r^{-1}, \quad z_2 = r^2 + r^{-2}, \quad z_3 = r^3 + r^{-3}, \quad z_4 = r^4 + r^{-4}, \quad r_5 = r^5 + r^{-5},$$

и найдем уравнение для z_1, z_2, z_3, z_4, z_5;

$$z^5 + z^4 - 4z^3 - 3z^2 + 3z + 1 = 0.$$

Это уравнение — циклическое; мы его можем решить в радикалах (§ 224); найдя z_1, получим уравнение для r и r:

$$x^2 - z_1 x + 1 = 0.$$

Пример 3. $p = 17$; уравнение $\dfrac{x^{17} - 1}{x - 1} = 0$.

Для числа 17 первообразный корень есть $g = 3$. Имеем таблицу:

λ	$=$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
3^λ	$\equiv$	1	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1

Составляем два восьмичленных периода:

$$y_0 = r + r^9 + r^{13} + r^{15} + r^{16} + r^3 + r^4 + r^2$$
$$y_1 = r^3 + r^{10} + r^5 + r^{11} + r^{14} + r^7 + r^{12} + r^6;$$

$y_0 + y_1 = -1$, $y_0 y_1 = -4$; уравнение для y_0 и y_1:

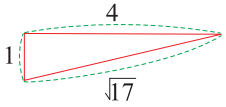
$$y^2 + y - 4 = 0.$$

Составляем четыре четырехчленных периода:

$$z_0 + r + r^{13} + r^{16} + r^4, \quad z_1 = r^3 + r^5 + r^{14} + r^{12},$$
$$z_3 = r^9 + r^{15} + r^8 + r^2, \quad z_3 = r^{10} + r^{11} + r^7 + r^6;$$

z_0 и z_2 удовлетворяют в теле $\mathbf{P}(y_0)$ уравнению:

$$z^2 - y_0 z - 1 = 0.$$



Черт. 29

Аналогично для z_1 и $z3$ имеем уравнение:

$$z^2 - y_1 z - 1 = 0.$$

Перемножив почленно два последних уравнения, найдем одно уравнение четвертой степени для z_0, z_1, z_3, $z - 4$ в теле $\mathbf{P}$:

$$z^4 + z^3 - 6z^2 - z + 1 = 0.$$

Составим теперь 8 двучленных периодов:

$$u_0 = r + r^{16} = r + r^{-1}, \quad u_1 = r^3 + r^{14} = r^3 + r^{-3}, \quad u_2 = r_2 + r^8 = r^8 + r^{-8},$$
$$u_3 = r^{10} + r^7 = r^7 + r^{-7}, \quad u_4 = r^{13} + r^4 = r^4 + r^{-4}, \quad u_5 = r^5 + r^{12} = r^5 + r^{-5},$$
$$u_6 = r^{15} + r^2 = r^2 + r^{-2}, \quad u_7 = r^{11} + r^6 = r^6 + r^{-6}.$$

Для u_0, u_4 имеем квадратное уравнение в теле $\mathbf{P}(z_0)$:

$$u^2 - z_0 u + z_1 = 0.$$

Найдя u_0, получим квадратное уравнение уже для r и r^{-1} в теле $\mathbf{P}(u_0)$:

$$x^2 - u_0 x + 1 = 0.$$

Итак, решение уравнения $\dfrac{x^{17}-1}{x-1} = 0$ свелось к решению цепи четырех квадратных уравнений:

$$y^2 + y - 4 = 0, \quad z^2 - y_0 z - 1 = 0, \quad u^2 - z_0 u + z_1 = 0, \quad x^2 - u_0 x + 1 = 0.$$

Тут $u_0 = 2\cos\dfrac{2\pi}{17}$, так что для геометрического построения достаточно уже вычислить u_0 (или какое-нибудь одно из u_λ).

Имеем:

$$\left.\begin{aligned} y_0 &= \frac{-1+\sqrt{17}}{2}, \\ y_1 &= \frac{-1-\sqrt{17}}{2}, \end{aligned}\right\} \qquad \left.\begin{aligned} z_0 &= \frac{y_0+\sqrt{y_0^2+4}}{2}, \\ z_1 &= \frac{y_1+\sqrt{y_1^2+4}}{2}, \end{aligned}\right\}$$

$$u = \frac{z_0+\sqrt{z_0^2-4z_1}}{2}, \qquad r = \frac{u+\sqrt{u^2-4}}{2}.$$

Итак; деление окружности на 17 равных частей совершается так: строим $\sqrt{17}$ (черт. 29), находим y_0 и $-y_1$; строим $\sqrt{y_0^2+4}$ и $\sqrt{y_1^2+4}$, находи z_0 и z_1; затем находим $u = 2\cos\dfrac{2k\pi}{17}$ и $\cos\dfrac{2k\pi}{17} = \dfrac{u}{2}$; число k неизвестно, но для построения оно и не требуется; из самого построения выявится, какое (целое) значение имеет k.

§ 233. Метациклическое уравнение. Рассмотрим неприводимое равнение $F(x) = 0$ в данном теле $\mathbf{P}$, имеющее степенью простое число $p > 2$. По § 227 группа Галуа этого уравнения транзитивна, а следовательно, ее порядок делится на ее степень p; с другой стороны, этот порядок есть делитель числа $p!$, которое имеет множителя p только и первой степени. Итак, порядок группы Галуа $\mathfrak{G}$ уравнения $F(x) = 0$ имеет вид: kp, где k не делится на p.

Пусть наше уравнение разрешимо в радикалах, т. е. и группа его $\mathfrak{G}$ разрешима; следовательно, в композиционном ряду для $\mathfrak{G}$

$$\mathfrak{G}, \quad \mathfrak{G}_1, \quad \mathfrak{G}_2, \ \ldots, \ \mathfrak{G}_{m-1}, \quad E$$

ряд индексов состоит из простых чисел, и все дополнительные группы $\dfrac{\mathfrak{G}_{\lambda-1}}{\mathfrak{G}_\lambda}$ (включая и $\dfrac{\mathfrak{G}_{m-1}}{E} = \mathfrak{G}_{m-1}$) — простейшие. Таким образом решение данного уравнения $F(x) = 0$ сводится к решению цепи простейших уравнений с группами $\dfrac{\mathfrak{G}_{\lambda-1}}{\mathfrak{G}_\lambda}$, причем группа данного уравнения сводится последовательно к $\mathfrak{G}_1, \mathfrak{G}_2, \ldots, \mathfrak{G}_{m-1}$, и,

наконец, к E; в этом последнем случае функция $F(x)$ после присоединения к телу $\mathbf{P}$ корней всех решенных уравнений распадется на линейные множители, и наше уравнение будет решено. Но до этого последнего присоединения функция $F(x)$ все время будет неприводимой, ибо (§ 228) она, сделавшись приводимой, должна распасться на ряд неприводимых сомножителей одинаковой степени, а степень $F(x)$ есть простое число p, т. е. $F(x)$ может распасться только на p сомножителей первой степени. Следовательно, когда мы расширим наше тело $\mathbf{P}$ так, что группа уравнения $F(x) = 0$ приведется к $\mathfrak{G}_{m-1}$, то в этом расширенном теле $\mathbf{P}'$ наше уравнение будет еще неприводимо. Но группа $\mathfrak{G}_{m-1}$ простейшая, порядок ее простое число и делится на степень p, ибо $\mathfrak{G}_{m-1}$ как группа неприводимого уравнения транзитивна (§ 227). Следовательно, порядок группы $\mathfrak{G}_{m-1}$ есть p, и она состоит из степеней одной и той же циклической подстановки $\mathbf{P}$ p-го порядка. Обозначив через $x0$, x_1, x_2, …, x_{p-1} корни нашего уравнения и, выбрав их нумерацию подходящим образом, мы будем иметь:

$$P = (0, 1, 2, \ldots, p-1).$$

Обозначим еще $\mathfrak{G}_{m-1} = \mathfrak{P} = \{P\}$. Докажем теперь две следующие леммы:

Лемма 1. *Если $\mathfrak{P}$ — инвариантная подгруппа группы $\mathfrak{A}$ a-го порядка и $\mathbf{D}\left(p, \frac{a}{p}\right) = 1$, то $\mathfrak{P}$ — единственная подгруппа p-го порядка для $\mathfrak{A}$.*

Доказательство. Пусть $\mathfrak{P}_1$ — другая подгруппа p-го порядка для $\mathfrak{A}$, тогда $\mathfrak{P}$ и $\mathfrak{P}_1$ — взаимно простые и переместимы друг с другом (ибо $\mathfrak{P}$ как инвариантная подгруппа переместима с каждым элементом из $\mathfrak{A}$, т. е. и из $\mathfrak{P}_1$); следовательно (по второй теореме § 195), $\mathfrak{B} = \mathfrak{P}\mathfrak{P}_1 = \mathfrak{P}_1\mathfrak{P}$ — тоже группа. Докажем, что при P и P' из $\mathfrak{P}$ и P_1 и P_1' из $\mathfrak{P}_1$ тогда и только тогда будет

$$PP_1 = P'P_1', \tag{8}$$

если $P = P'$ и $P_1 = P_1'$. Действительно, из (8) выводим:

$$P^{-1}PP_1P_1'^{-1} = P^{-1}P'P_1'P_1'^{-1},$$

или

$$P_1P_1'^{-1} = P^{-1}P'; \tag{9}$$

но левая часть в (9) есть элементы из $\mathfrak{P}_1$, а правая — из $\mathfrak{P}$, а так как единственный общий этим двум группам элемент есть E, то

$$P^{-1}P' = E, \qquad P_1P_1'^{-1} = T, \qquad \text{т. е.} \qquad P = P', \quad P_1 = P_1'.$$

Отсюда следует, что группа $\mathfrak{P}$ имеет p^2 различных элементов, т. е. порядок ее p^2; но $\mathfrak{B} \subset \mathfrak{A}$, значит, a делится на p^2 (§ 194), т. е. $\frac{a}{p}$ делится на p, что противоречит условию: $\mathbf{D}\left(p, \frac{a}{p}\right) = 1$. Отсюда следует, что иной подгруппы p-го порядка кроме $\mathfrak{P}$ группа $\mathfrak{A}$ не имеет.

Лемма 2. *Если $\mathfrak{P}$ инвариантная подгруппа для $\mathfrak{B}$, а $\mathfrak{B}$ инвариантная подгруппа для $\mathfrak{A}$ и p, b, a соответственно их порядки, причем p — простое и числа p и $\frac{b}{p}$ взаимно простые, то $\mathfrak{P}$ инвариантная подгруппа для $\mathfrak{A}$.*

Доказательство. По лемме 1 $\mathfrak{P}$ единственная подгруппа p-го порядка группы $\mathfrak{B}$. Пусть A — некоторый элемент из $\mathfrak{A}$; так как $\mathfrak{B} \supset \mathfrak{P}$, то, следовательно:

$$A^{-1}\mathfrak{B}A \supset A^{-1}\mathfrak{P}A,$$

но $A^{-1}\mathfrak{B}A = \mathfrak{B}$, а $A^{-1}\mathfrak{P}A$ — подгруппа p-го порядка для $\mathfrak{B}$; так как единственная подгруппа p-го порядка у $\mathfrak{B}$ есть $\mathfrak{P}$, то, следовательно:

$$A^{-1}\mathfrak{P}A = \mathfrak{P}$$

для всякого элемента A из $\mathfrak{A}$; этим лемма 2 доказана.

Возвращаемся к композиционному ряду для $\mathfrak{G}$; $\mathfrak{G}_{m-1} = \mathfrak{P}$ есть инвариантная подгруппа группы $\mathfrak{G}_{m-2}$; но $\mathfrak{G}_{m-2}$ инвариантная подгруппа группы $\mathfrak{G}_{m-3}$ и порядок $\mathfrak{G}_{m-2}$ имеет вид pq, где q — взаимно простое с p; отсюда по лемме 2 заключаем, что $\mathfrak{P}$ инвариантная подгруппа группы $\mathfrak{G}_{m-3}$. Но теперь мы совершенно так же докажем, что $\mathfrak{P}$ инвариантная подгруппа группы $\mathfrak{G}_{m-4}$ и т. д., наконец, что $\mathfrak{P}$ -— инвариантная подгруппа для $\mathfrak{G}$. Итак, транзитивная группа $\mathfrak{G}$ p-й степени имеет инвариантную подгруппу $\mathfrak{P}$ p-го порядка.

Обратно, пусть нам теперь дано, что транзитивная группа $\mathfrak{G}$ p-й степени имеет инвариантную подгруппу $\mathfrak{P}$ p-го порядка. Легко видеть, что все (кроме E) подстановки $\mathfrak{P}$ циклические, вида

$$P = (0, 1, 2, \ldots, p-1),$$

и группа $\mathfrak{P}$ состоит из степеней такой подстановки: $\mathfrak{P} = \{P\}$. Здесь символы $0, 1, 2, \ldots, p-1$ являются номерами корней нашего уравнения $F(x) = 0$; будем эти номера считать по модулю p; тогда подстановка P представится в виде: $P = \big(\lambda\lambda + 1\big)$; но тогда $P^2 = \begin{pmatrix} \lambda \\ \lambda + 2 \end{pmatrix}$, $P^3 = \begin{pmatrix} \lambda \\ \lambda + 3 \end{pmatrix}$, и вообще $P^\beta = \begin{pmatrix} \lambda \\ \lambda + \beta \end{pmatrix}$. Пусть Q — подстановка из $\mathfrak{G}$: так как $\mathfrak{P}$ инвариантная подгруппа группы $\mathfrak{G}$, то

$$Q^{-1}PQ = P^\alpha,$$
$$Q^{-1}P^\lambda Q = P^{\alpha\lambda};$$

следовательно:

$$Q = P^{-\lambda}QP^{\alpha\lambda} = . \tag{10}$$

Пусть Q — такая подстановка из $\mathfrak{G}$, которая не изменяет нуля; $P^{-\lambda}$ заменяет λ через нуль; $P^{\alpha\lambda}$ заменяет нуль через $\alpha\lambda$; следовательно, по (10), Q заменяет λ через $\alpha\lambda$, т. е. $Q = \begin{pmatrix} \lambda \\ \alpha\lambda \end{pmatrix}$; при этом $\alpha \neq 0$, так как иначе, все символы в Q заменялись бы нулем; итак: $\alpha = 1, 2, 3, \ldots, p-1$; при $\alpha = 1$ имеем $Q = E$.

Пусть теперь R — подстановка из $\mathfrak{G}$, заменяющая нуль на β; подстановка $Q = RP^{-\beta}$ оставляет нуль без изменения, т. е.

$$Q = RP^{-\beta} = \begin{pmatrix} \lambda \\ \alpha\lambda \end{pmatrix},$$

$$R = QP^\beta = \begin{pmatrix} \lambda \\ \alpha\lambda \end{pmatrix}\begin{pmatrix} \lambda \\ \lambda + \beta \end{pmatrix} = \begin{pmatrix} \lambda \\ \alpha\lambda \end{pmatrix}\begin{pmatrix} \alpha\lambda \\ \alpha\lambda + \beta \end{pmatrix} = \begin{pmatrix} \lambda \\ \alpha\lambda + \beta \end{pmatrix} \tag{11}$$
$$(\alpha = 1, 2, \ldots, p-1, \quad \beta = 0, 1, 2, \ldots, p-1).$$

Давая все эти значения для α и для β, мы получаем всего $p(p-1)$ таких подстановок; все подстановки из $\mathfrak{G}$ такого вида, т. е. порядок $\mathfrak{G} \leq p(p-1)$ [ибо в $\mathfrak{G}$ могут входить и не все подстановки вида (11)]. Но все подстановки (11) составляют группу $\mathfrak{M}$ $p(p-1)$-го порядка. Именно, легко видеть, что

$$\begin{pmatrix} \lambda \\ \alpha\lambda+\beta \end{pmatrix} \begin{pmatrix} \lambda \\ \alpha_1\lambda+\beta_1 \end{pmatrix} = \begin{pmatrix} \lambda \\ \alpha_1\alpha\lambda+\alpha_1\beta+\beta_1 \end{pmatrix},$$

т. е. произведение двух подстановок (11) есть подстановка того же типа; далее, среди подстановок (11) имеется E (при $\alpha = 1$, $\beta = 0$), и для каждой данной подстановки $\begin{pmatrix} \lambda \\ \alpha\lambda+\beta \end{pmatrix}$ есть обратная: $\begin{pmatrix} \lambda \\ \alpha_1(\lambda-\beta) \end{pmatrix}$, где $\alpha\alpha_1 \equiv 1 \pmod p$. Итак, $\mathfrak{M} \supseteq \mathfrak{G}$.

Эта группа $\mathfrak{M}$ называется *полной линейной* или *метациклической* (по Кронекеру).

Название «линейная группа» происходит от того, что символ $\begin{pmatrix} \lambda \\ \alpha\lambda+\beta \end{pmatrix}$ представляет собой линейную подстановку по модулю p.

Обозначим $Q = \begin{pmatrix} \lambda \\ \alpha\lambda \end{pmatrix}$ $(\alpha = 1, 2, \ldots, p-1)$; всякая подстановка $R \subset \mathfrak{M}$ (или $\mathfrak{G}$) имеет вид: $R = Q_\alpha P^\beta$. Имеем:

$$Q_\alpha + Q_\alpha P + Q_\alpha P^2 + \ldots + Q_\alpha P^{p-1} = Q_\alpha \mathfrak{P} = \mathfrak{P} Q_\alpha;$$

отсюда

$$\mathfrak{M} = \mathfrak{P} Q_1 + \mathfrak{P} Q_2 + \ldots + \mathfrak{P} Q_{p-1} \qquad (Q_0 = E).$$

Подстановки $Q_1, Q_2, \ldots, Q_{p-1}$ суть все подстановки из $\mathfrak{M}$, не меняющие нуля; они составляют группу $\mathfrak{Q}$ (-1)-го порядка. Имеем:

$$\mathfrak{M} = \mathfrak{P}\cdot; \qquad \frac{\mathfrak{M}}{\mathfrak{P}} \quad \text{изоморфно с} \quad \mathfrak{Q}.$$

Докажем, что $\mathfrak{Q}$ циклическая группа; пусть γ — первообразный корень простого числа p; числа $\gamma, \gamma^2, \ldots, \gamma^{p-1}$ по модулю p сравнимы с числами $1, 2, 3, \ldots, p-1$, только в ином порядке; следовательно, вместо $Q_1, Q_2, \ldots, Q_{p-1}$ можно взять $Q_\gamma, Q_{\gamma^2}, Q_{\gamma^3}, \ldots, Q_{\gamma^{p-1}}$; но $Q_{\gamma^2} = Q_\gamma^2$, $Q_{\gamma^3} = Q_\gamma^3$ и т. д. Этим доказана цикличность группы $\mathfrak{Q}$. Но произведение двух циклических групп, очевидно, разрешимо; следовательно, группа $\mathfrak{M} = \mathfrak{P} \cdot \mathfrak{Q}$ разрешимая.

Мы видели, что $\mathfrak{G} \supset \mathfrak{M}$ и, следовательно, $\dfrac{\mathfrak{G}}{\mathfrak{P}} \subset \dfrac{\mathfrak{M}}{\mathfrak{P}}$; а так как $\dfrac{\mathfrak{M}}{\mathfrak{P}}$, будучи изоморфной с $\mathfrak{Q}$, циклическая, то и $\dfrac{\mathfrak{G}}{\mathfrak{P}}$ тоже циклическая, как подгруппа циклической группы. Следовательно, и группа $\mathfrak{G}$ разрешима, ибо она имеет инвариантную простейшую группу $\mathfrak{P}$, и дополнительная группа $\dfrac{\mathfrak{G}}{\mathfrak{P}}$ разрешима, как циклическая. Итак:

Теорема. *Необходимое и достаточное условие разрешимости в радикалах неприводимого уравнения простой степени p состоит в том, что его группа Галуа должна иметь инвариантную подгруппу p-го порядка.*

При доказательстве этой теоремы мы попутно вывели:

Следствие. Линейная (или метациклическая) группа всегда разрешима.

Уравнение с линейной группой Галуа называется *метациклическим*.

Пусть x_ρ и x_σ два различных корня метациклического уравнения; присоединим их к области $\mathbf{P}$; тогда группа Галуа данного уравнения сведется к той подгруппе линейной группы, которая не изменяет ни x_ρ, ни x_σ; но подстановки линейной группы имеют вид $\begin{pmatrix} \lambda \\ \alpha\lambda+\beta \end{pmatrix}$; следовательно, мы получаем:

$$\rho \equiv \alpha\rho + \beta \pmod p,$$
$$\sigma = \alpha\sigma + \beta \pmod p,$$

отсюда

$$\rho - \sigma \equiv \alpha(\rho - \sigma) \pmod p.$$

Так как $\rho \not\equiv \sigma \pmod p$, то, следовательно: $\alpha \equiv 1 \pmod p$. Но тогда $\rho = \rho + \beta \pmod p$, т. е. $\beta \equiv 0 \pmod p$, и, значит, подстановка, не меняющая ни ρ, ни σ, должна быть $\begin{pmatrix} \lambda \\ \lambda \end{pmatrix} = E$. Таким образом в теле $\mathbf{P}(x_\rho, x_\sigma)$ группа уравнения есть E, т. е. в этом теле лежат и все остальные корни нашего уравнения, которые, таким образом, выражаются рационально через x_ρ и x_σ.

Обратно, пусть все корни нашего неприводимого уравнения $F(x) = 0$ p-й степени выражаются рационально через два определенные из них, например, через x_0 и x_1. Группа $\mathfrak{G}$ уравнения по присоединении к области $\mathbf{P}$ только корня x_0 перейдет в группу $\mathfrak{G}_0$ порядка $\frac{g}{p} = g_0$, где g — порядок $\mathfrak{G}$. Но тогда вместо уравнения $F(x) = 0$ мы получим уравнение $(p-1)$-й степени для остальных корней. Присоединив еще x_1 к области $\mathbf{P}(x_0)$, мы сведем группу $\mathfrak{G}_0$ к E; но от этого присоединения порядок группы станет равным $\frac{g_0}{m}$, где $m \leq p-1$; следовательно:

$$\frac{g_0}{m} = 1, \quad \text{т. е.} \quad g_0 = m, \qquad g = pm < p^2.$$

По теореме Силова (§ 203) группа $\mathfrak{G}$ имеет подгруппу $\mathfrak{P}$ p-го порядка; эта подгруппа $\mathfrak{P}$ — циклическая; докажем, что она единственная. Пусть $\mathfrak{P}'$ другая подгруппа p-го порядка группы $\mathfrak{G}$. Следовательно, $\mathfrak{G}$ содержит и комплекс $\mathfrak{P}\mathfrak{P}'$; состоящий из p^2 различных элементов, ибо $\mathfrak{P}$ и $\mathfrak{P}'$ взаимно простые; но тогда порядок $\mathfrak{G}$: $g \geq p^2$, а мы видели, что $g < p^2$. Итак, $\mathfrak{P}$ единственная подгруппа группы $\mathfrak{G}$ p-го порядка, т. е. она инвариантна. А отсюда по предыдущей теореме следует, что группа $\mathfrak{G}$ разрешима, т. е. уравнение $F(x) = 0$ разрешимо в радикалах. Итак:

Теорема Галуа. *Необходимое и достаточное условие разрешимости в радикалах приводимого уравнения простой степени заключается в том, что все корни этого уравнения должны выражаться рационально (в данной области* $\mathbf{P}$*) через два определенные из них.*

ГЛАВА ЧЕТЫРНАДЦАТАЯ

ВВЕДЕНИЕ В НОВУЮ АЛГЕБРУ

§ 234. Абстрактная теория тел. Еще в главе 1 § 13 мы встретились с понятием области, рациональности, или тела, или поля; в дальнейшем мы постоянно возвращались к этому понятию: мы вновь столкнулись с ним и в конце главы IV, и в конце главы VI, и в конце главы VIII; наконец, в главах XII и XIII это понятие играло основную роль: мы видели, что сама проблема решения уравнения сводится к проблеме расширения первоначально данного тела до такого, в котором данная целая рациональная функция распадается на линейные множители. Но подобно тому как теория групп отвлеклась от специальных свойств тех элементов (подстановок, матриц), над которыми производится действие, постулировала основные свойства действия и превратилась, таким образом, в абстрактную теорию групп, — так же точно возникает вопрос о построении абстрактной теории тел, где бы вместо чисел мы просто брали «элементы», над которыми специальною системою постулатов определялось бы не одно действие, как в теории групп, — а два основных действия — «сложение» и «умножение» (что касается «вычитания» и «деления», то эти действия естественно определять просто как «обратные» к сложению и умножению). Такая абстрактная теория тел и была построена, хотя и несколько позже абстрактной теории групп. Первый ввел абстрактные тела, определив их системою постулатов, Г. Вебер (H. Weber) [104] в 1893 г. В 1905 г. Л. Е. Диксон (L. E. Dickson) [105] и Э. В. Хентингтон (E. V. Huntington) [106] дали иные системы постулатов для определения тела (поля) и доказали независимость постулатов своих систем. Наконец, в 1910 г. Э. Штейниц (E. Steinitz) [107] разработал полную абстрактную теорию тел.

Абстрактная теория тел оказалась шире теории конкретных, числовых и функциональных тел, известных до ее построения; кроме тех конкретных случаев числовых и функциональных тел, которые встречались и в нашем курсе, абстрактная теория тел дает и другие типы тел, не встречающиеся среди числовых и функциональных тел, например, конечные тела, стоящие в тесной связи с так называемыми

[104] Die aligemeinen Grundlagen der Galois'schen Qleichungstheorie, «Math. Annalen», Bd. 43 (1893), стр. 521–549.

[105] Definitions of a group and a field by independent postulates, «Transact. of the Amer. Math. Soc.», vol. 6 (1905), стр. 198-—204.

[106] Note on the definitions of abstract groups and fields by sets of independent postulates, «Transact, of the Amer. Math. Soc.», vol. 6 (1905), стр. 181–197.

[107] Algebraische Theorie der Körper, «Journ. für die reine und angew. Mathem,», Bd, 337 (1910), гтр, 147–309.

мнимыми числами Галуа. В настоящей главе мы имеем в виду дать введение в абстрактную теорию тел, разобрав основные их типы и их возможные расширения; далее, имеем в виду указать на более общие системы с двумя действиями, — кольца (в частном случае — области целости) и системы гиперкомплексных чисел (так называемые «линейные алгебры»).

§ 235. Система постулатов, определяющих тело. Мы даем эту систему в том виде, как ее дает Штейниц; следует заметить, что не все постулаты его системы независимы, друг от друга.

Итак, *областью рациональности*, или *телом*, или *полем* называется система элементов, содержащая не меньше двух различных элементов [108], с двумя действиями над этими элементами, — «сложением» (обозначаемым знаком + и «умножением» (обозначаемым или точкой, или просто тем, что «перемножаемые» элементы ставятся рядом), причем эти действия подчинены следующим постулатам:

1. *Ассоциативный закон сложения:* $(a+b)+c=a+(b+c)$ [109].
2. *Коммутативный закон сложения:* $a+b=b+a$.
3. *Ассоциативный закон умножения:* $(ab)c=a(bc)$.
4. *Коммутативный закон умножения:* $ab=ba$ [110].
5. *Дистрибутивный закон:* $a(b+c)=ab+ac$.
6. *Закон неограниченного и однозначного вычитания:* при данных a и b уравнение $a+x=b$ имеет всегда и только одно решение $x=b-a$ — разность элементов b и a.
7. *Закон, неограниченного и однозначного деления:* при данных a и b, если только $a\neq 0$, где 0 — особый элемент, — так называемый *единичный элемент для сложения* (см. ниже) — уравнение $ax=b$ имеет всегда и только одно решение: $x=\frac{b}{a}=b:a$.

Следствия из основных постулатов.

Из постулатов 1, 2 и 6 следует, что *тело представляет собою абелеву группу относительно сложения.* Обозначим через 0 единичный элемент этой абелевой группы и назовем его «нулем» данного тела; «обратный» элемент к данному элементу a обозначим через $-a$; имеем, таким образом:

$$a+0=0+a=a, \qquad -0=0, \qquad a+(-a)=a-a=(-a)+a=0. \tag{1}$$

«Степени» элемента a относительно сложения естественно обозначить как целочисленные «кратные» элемента a; но чтобы их не спутать с произведениями элементов тела, мы будем это «скалярное умножение» элемента a на целое число (играющее в сложении ту же роль, что и показатель в умножении) временно обозначать знаком $\times$, ставя при этом численный сомножитель слева; таким образом:

$$a+a=2\times a, \qquad (2\times a)+a=3\times a,$$

вообще

$$\underbrace{a+a+\ldots+a}_{n\text{ раз}}=n\times a=[(n-1)\times a]+a, \tag{2}$$

[108] Этим условием мы исключаем неинтересный для нас тривиальный случай тела, состоящего только из одного элемента «нуль».

[109] В дальнейшем мы будем обозначать отдельные элементы малыми латинскими буквами.

[110] Имеется обобщение понятия тела, где отбрасывается коммутативный закон умножения, именно, так называемое «некоммутативное тело», в дальнейшем мы им не будем заниматься.

где n — натуральное число; далее: $-a = (-1) \times a$ (как «минус-первая степень»);

$$(-n) \times a = n \times (-a) = \underbrace{-a - a - \ldots - a}_{n \text{ раз}}. \tag{2}$$

Легко проверить на основании ассоциативного закона, что

$$(n \times a) + (-n \times a) = 0,$$

т. е.

$$(-n) \times a = -(n \times a). \tag{3}$$

Обозначим еще: $1 \times a = a$.

Обращаемся теперь к умножению. Имеем по 5: $ab = (a + 0)b = ab + 0b$; следовательно:

$$ab - ab = 0 \cdot b = b \cdot 0$$

(по 4); но $ab - ba = 0$ [по (1)], а по 6 разность однозначно определена; следовательно:

$$b \cdot 0 = 0 \cdot b = 0 \tag{4}$$

для всякого элемента b.

Из 7, как и для групп (гл. XI), следует существование единичного элемента ε для умножения и «обратного» элемента относительно умножения a^{-1} для всякого данного элемента $a \neq 0$ 0; именно:

$$a\varepsilon = \varepsilon a = a, \qquad aa^{-1} = a^{-1}a = \varepsilon,$$

(последнее при $a \neq 0$). В частности и $0 \cdot \varepsilon = \varepsilon \cdot 0 = 0$.

Итак, если $a \neq 0$ (а такой элемент в теле имеется, ибо до условию в теле не меньше двух различных элементов), то $a\varepsilon = a \neq 0$, тогда как $a \cdot 0 = 0$, откуда следует:

$$\varepsilon \neq 0. \tag{5}$$

Пусть теперь $a \neq 0$, но $ab = 0$; умножая обе части этого равенства на a^{-1}, получим;

$$a^{-1}ab = a^{-1}0,$$

или

$$\varepsilon b = b = 0.$$

Точно так же при $b \neq 0$ и $ab = 0$ мы нашли бы и $a = 0$. Отсюда непосредственно следует закон отсутствия нулевых делителей (глава I, § 5):

Произведение равно нулю только, если по крайней мере один из сомножителей равен нулю.

Из предыдущего следует (по постулатам 3, 4 и 7): *все элементы тела кроме нуля образуют абелеву группу относительно умножения.*

Из постулата 5 следует, далее:

$$0 = a \cdot 0 = a[b + (-b)] = ab + a(-b);$$

отсюда [см. (1)]:

$$a(-b) = -(ab).$$

По постулату 4 легко убедимся, что и

$$(-a)b = -(ab).$$

Заменив теперь b на $-b$, получим:

$$(-a)(-b) = -[a(-b)] = -[-(ab)] = ab,$$

т. е. для умножения верно обычное «правило знаков».

Из того же постулата 5 непосредственно следует правильность обычного правила умножения многочлена на многочлен; отсюда в частности получим:

$$\underbrace{(a + a + \ldots + a)}_{n \text{ раз}}\underbrace{(b + b + \ldots + b)}_{n \text{ раз}} = \underbrace{ab + ab + \ldots + ab)}_{nm \text{ раз}},$$

или

$$(n \times a)(m \times b) = nm \times ab; \tag{6}$$

отсюда при $m = 1$ получаем:

$$(n \times a)b = n \times ab = a(n \times b), \tag{6}$$

т. е. для произведений элементов и чисел верны ассоциативный и коммутативный законы. Далее, заметим:

$$a = \varepsilon a; \quad \text{следовательно:} \quad n \times a = (n \times \varepsilon)a,$$

т. е. скалярное произведение сводится к произведению элементов, если только скалярный множитель n заменить элементом $n \times \varepsilon$. Поэтому в дальнейшем мы можем просто писать na вместо $n \times a$ недоразумений не будет, если при этом под na подразумевать $(n\varepsilon)a$.

Из предыдущего видно, что оба действия — сложение и умножение — играют в теле не одну и ту же роль: тут есть известная асимметрия, обусловленная дистрибутивным законом (постулат 5), не симметричным относительно сложения и умножения; этот же закон придает особую роль единичному элементу сложения, обращая его в «нулевой элемент».

§ 236. Область целости. Если для системы элементов с двумя действиями выполнены постулаты 1–6 § 235, а постулат 7 вообще не верен, то такая система называется *кольцом*. О кольце вообще в дальнейшем еще будет речь; теперь же мы рассмотрим частный случай кольца, — именно, кольцо, для которого верен закон отсутствия нулевых делителей, т. е. в котором произведение равно нулю, только при равенстве нулю по крайней мере одного из сомножителей; такое кольцо называется *областью целости* (ср. главу I, § 13).

Докажем, что в области целости для умножения верен закон однозначной обратимости, т. е. из $ab = ac$ при $a \neq 0$ следует $b = c$. Действительно, из $ab = ac$ следует:

$$ab - ac = 0,$$

а отсюда по постулату 5:

$$a(b - c) = 0.$$

А так как $a \neq 0$ и нулевых делителей область целости не имеет, то

$$b - c = 0, \quad \text{т. е.} \quad b = c.$$

Из определения области целости следует что тело есть частный случай области целости. Если ε — единичный элемент умножения в теле, то все целочисленные кратные элемента $n\varepsilon$ составляют, очевидно, область целости: действительно, сумма, разность и произведение таких кратных n тоже подобные же кратные, а нулевых делителей нет во всем теле; следовательно, нет и в каждой части его. Эта область целости всех кратных элемента ε замечательна тем, что имеет единичный элемент ε. (Некоторые авторы, в том числе и сам Штейниц, ставят существование единичного элемента как особый постулат для определения области целости.) Возьмем теперь систему всех четных кратных элемента $n\varepsilon$, т. е. систему элементов вида $n\varepsilon$, где n — четное число; такая система, как легко убедиться, — тоже область целости, но без единичного элемента.

Таким образом область целости является не чем иным, как «неполным телом»; область целости, содержащаяся в данном теле, есть такая часть этого тела, которая, содержа элементы a и b, всегда содержит их сумму, разность и произведение, но не всегда их частное; в случае если и частное $\dfrac{a}{b} = ab^{-1} = c$ содержится в области целости, т. е. $a = bc$, говорят, что *a делится на b*, *b — делитель a*, *a — кратное b*. Таким образом в области целости может быть построена *теория делимости*, — подобно теории делимости целых чисел. Заметим, что понятие о делимости — относительное, — оно зависит от взятой области целости в данном теле.

Но возникает вопрос: если нам дана только область целости — совершенно абстрактно, без всякого тела, — то можно ли ее так «расширить», создав подходящим образом новые элементы, чтобы она превратилась в тело? Это та же задача, что и задача, приводящая к созданию дробей и расширяющая область целых чисел до области всех рациональных чисел, в которой деление всегда возможно (кроме деления на нуль). Задача эта разрешима для всякой данной области целости; именно, имеется теорема:

Теорема об образовании частных. *Всякую область целости можно расширить до тела, введя подходящим образом новые элементы.*

Доказательство. Если элемент a не делится на b в данной области целости, то при расширении ее до тела приходится вводить новый элемент: «дробь» $\dfrac{a}{b}$. Мы должны определить, во-первых, равенство таких дробей, во-вторых, их сумму и, в-третьих, их произведение; эти определения, формально произвольные, по существу выбираются так, чтобы полученная более широкая система была действительно телом, содержащим данную область целости (ср. главу I, § 3), Чтобы не запутаться в обозначениях, вводя эти частные $\dfrac{a}{b}$, будем их обозначать пока как «пары элементов» (a, b) (при $b \neq 0$), определив формально, тремя постулатами, их равенство, сумму и произведение. Именно:

I. $(a, b) = (c, d)$ тогда и только тогда, если $ad = bc$.

II. $(a, b) + (c, d) = (ad + bc, bd)$.

III. $(a, b)(c, d) = (ac, bd)$.

Докажем, что равенство, определенное по I, удовлетворяет законам симметрии, рефлективности и транзитивности (см. главу I, § 2); для первых двух законов

это очевидно; рассмотрим третий: пусть $(a, b) = (c, d)$, $(, d) = (e, f)$; тогда, следовательно: $ad = b$, $cf = de$. Перемножив почленно эти равенства, найдем: $adcf = bcde$. Имеем $d \neq 0$; если и $c \neq 0$, то сократим на cd получим: $af = be$, т. е. по постулату I $(a, b) = (e, f)$; это и доказывает закон транзитивности. Если же $c = 0$, то легко видеть, что и $a = 0$, и $e = 0$, и опять очевидно: $(0, b) = (0, f)$.

Таким образом для каждого из созданных элементов (т. е. пар) имеется бесчисленное множество «представителей»; по постулату I очевидно, что для всякого $c \neq 0$

$$(a, b) = (ac, bc)$$

хотя в общем случае нельзя утверждать, что все «представители» данного элемента должны иметь вид (ac, bc) при каких-то определенных элементах a, b.

Нам требуется еще доказать, что сложение и умножение, определенные по постулатам II и III, однозначны, т. е. их результаты не зависят от выбора «представителей» данных элементов. Итак, пусть

$$(a, b) = (a_1, b_1), \quad (c, d) = (c_1, d_1), \qquad \text{т. е.} \qquad ab_1 = a_1 b, \quad cd_1 = c_1 d;$$

тогда

$$ab_1 dd_1 = a_1 bdd_1, \qquad cd_1 bb_1 = c_1 dbb_1;$$

складывая, найдем:

$$ab_1 dd_1 + cd_1 bb_1 = a_1 bdd_1 + c_1 dbb_1;$$

отсюда

$$(ad + bc)b_1 d_1 = (a_1 d_1 + b_1 c_1)bd,$$

а это по постулату I дает

$$(ad + bc, bd) = (a_1 d_1 + b_1 c_1 m b_1 d_1),$$

т. е. по постулату II

$$(a, b) + (c, d) = (a_1, b_1) + (c_1, d_1).$$

Далее, имеем:

$$ab_1 cd_1 = a_1 bc_1 d \qquad \text{или} \qquad (ac)(b_1 d_1) = (a_1 c_1)(bd);$$

отсюда

$$(ac, bd) = (a_1 c_1, b_1 d_1),$$

т. е. по постулату III

$$(a, b)(c, d) = (a_1, b_1)(c_1, d_1).$$

Итак, мы теперь имеем систему наших новых элементов (пар) с двумя однозначными действиями над ними. Докажем, что эта система есть тело, т. е. проверим для нее все постулаты 1–7 § 235. Постулаты 1–5 проверяются непосредственно вычислением, и мы на них не будем останавливаться. Для постулата 6 заметим, что нулем в системе наших пар являются пары вида: $(0, a)$ для любого $a \neq 0$; далее: $-(a, b) = (-a, b) = (a, -b)$. Действительно:

$$(a, b) + (-a, b) = (ab - ab, b^2) = (0, b^2) = 0.$$

Теперь ясно, что (обозначая наши пары греческими буквами):

$$\alpha - \beta = \alpha + (-\beta),$$

и это значение единственное. Переходя к постулату 7, заметим, что в нашей системе пар пара $\varepsilon = (a, a)$ для любого $a \neq 0$ есть единичный элемент умножения, что легко проверить. Далее:

$$(a, b) \cdot (b, a) = (ab, ab) = \varepsilon \qquad \text{при} \qquad a \neq 0, \quad b \neq 0,$$

т. е. всякий неравный нулю элемент (a, b) имеет обратный элемент относительно умножения:

$$(a, b)^{-1} = (b, a).$$

Теперь ясно, что уравнение $\alpha\xi = \beta$ имеет решение $\xi = \alpha^{-1}\beta$, и это решение единственное, ибо из $\alpha\xi = \alpha\xi_1$ следует:

$$\alpha^{-1}\alpha\xi = \alpha^{-1}\alpha\xi_1, \qquad \text{или} \qquad \varepsilon\xi = \varepsilon\xi_1, \qquad \text{т. е.} \qquad \xi = \xi_1.$$

Итак, система наших пар есть действительно тело. Доказать, что данная область целости входит в это тело как часть, мы, конечно, прямо не можем, ибо элементы $a, b, \ldots$ области целости ведь не являются парами, из которых и состоит полученное тело. Но мы докажем, что и полученном теле содержится область целости, изоморфная данной.

Два тела $\mathfrak{K}$ и $\mathfrak{K}_1$ или две области целости $\mathfrak{F}$ и $\mathfrak{F}_1$ называются *изоморфными*, если между их элементами существует взаимно однозначное соотношение, причем

если	a	из	$\mathfrak{K}$	(или	из	$\mathfrak{F}$)	соответствует	a_1	из	$\mathfrak{K}_1$	(или	из	$\mathfrak{F}_1$),
	b	〃	〃	〃	〃	〃	〃	b_1	〃	〃	〃	〃	〃	
то	$a+b$	〃	〃	〃	〃	〃	〃	a_1+b_1	〃	〃	〃	〃	〃	
	ab	〃	〃	〃	〃	〃	〃	a_1b_1	〃	〃	〃	〃	〃	

Отвлеченно два изоморфных друг другу тела (или области целости) отличаются друг от друга только обозначениями своих элементов.

Так вот, пусть элементу a из данной области целости соответствуют (равные друг другу) пары (ab, b) для всякого $b \neq 0$; тогда

элементу	a	соответствует	пара	$(ax, x), \quad x \neq 0,$
〃	b	〃	〃	$(by, y), \quad y \neq 0,$
〃	$a+b$	〃	〃	$((a+b)z, z), \quad z \neq 0,$
〃	ab	〃	〃	$(abz, z), \quad z \neq 0.$

Но, взяв $z = xy \neq 0$, мы получим:

$$((a+b)z, z) = (ax, x) + (by, y),$$
$$(abz, z) = (ax, x) \cdot (by, y).$$

Этим и доказано, что пары вида (ax, x) образуют область целости, изоморфную данной. Остается теперь отождествить (ax, x) и a, и наша теорема будет доказана.

В дополнение докажем, что полученное тело — единственное по своей структуре; это будет доказано, если доказать более общее предложение: *полученное тело пар содержится во всяком теле, содержащем данную область целости, или точнее: если тело содержит область целости, изоморфную данной, то оно содержит и тело, изоморфное полученному телу пар.*

Действительно, если данное тело $\mathfrak{A}$ содержит данную область целости $\mathfrak{F}$, то, будучи телом, и содержа элементы a, b ($b \neq 0$) из $\mathfrak{F}$, $\mathfrak{A}$ содержит и все частные $\frac{a}{b}$; над этими частными производятся действия по правилам действий над обыкновенными дробями, и равенство таких дробей подчинено нашему постулату I; следовательно, можно установить взаимно однозначное соответствие между этими дробями и нашими парами:

$$\text{дроби} \qquad \frac{a}{b} \qquad \text{соответствует пара} \qquad (a, b),$$

и очевидно, что тогда сумме и произведению этих дробей будут (по постулатам II и III) соответствовать сумма и произведение соответствующих пар. Этим наше предложение доказано, ибо попутно доказано, что такие дроби $\frac{a}{b}$ составляют тело.

§ 237. Делители тела; простое тело. В предыдущем параграфе мы видели, что данное тело $\mathfrak{K}$ может заключать в себе другое тело $\mathfrak{K}_1$, как часть, или, как говорят, *содержать делитель* (подтело) $\mathfrak{K}_1$; этот факт мы будем обозначать знаком:

$$\mathfrak{K} \supset \mathfrak{K}_1.$$

(Точно так же, если тело или область целости $\mathfrak{K}$ содержит элемент a, то мы будем обозначать: $a \subset \mathfrak{K}$ или $\mathfrak{K} \supset a$.)

Теорема. *Если $\mathfrak{K}_1, \mathfrak{K}_2, \ldots$ конечное, счетное или несчетное множество тел, содержащихся в данном теле, то все элементы, общие всем телам $\mathfrak{K}_1, \mathfrak{K}_2, \ldots$, образуют тело ϑ.*

Это тело ϑ называется *пересечением* (или *общим наибольшим делителем*) тел $\mathfrak{K}_1, \mathfrak{K}_2, \ldots$

Доказательство. Теорема следует из того, что если элементы a и b принадлежат всем телам $\mathfrak{K}_1, \mathfrak{K}_2, \ldots$, то и $a + b$ и ab и $\frac{a}{b}$ (при $b \neq 0$) тоже принадлежат всем этим телам.

Подобная же теорема существует и для областей целости.

Тело, совсем не имеющее делителей (кроме самого себя), называется *простым.* Точно так же определяется *простая область целости.*

Теорема. *Каждое, тело содержит одно и только одно простое тело.*

Доказательство. Пусть $\mathfrak{K}_1, \mathfrak{K}_2, \ldots$ совокупность всех делителей данного тела $\mathfrak{K}$ и $\mathfrak{P}$ их пересечение [111]; тогда $\mathfrak{P} \subset \mathfrak{K}$ и $\mathfrak{P}$ — простое. Действительно, если бы было

$$\mathfrak{P} \supset \mathfrak{P}',$$

то было бы, очевидно, $\mathfrak{K} \supset \mathfrak{P}'$, т. е. тело $\mathfrak{P}'$ принадлежало бы к совокупности делителей тела $\mathfrak{K}$; но тогда было бы

$$\mathfrak{P} \subset \mathfrak{P}', \quad \text{т. е.} \quad \mathfrak{P}\mathfrak{P}',$$

[111] Очевидно, что пересечение тел, содержащихся в одном данном теле, никогда не может быть «пустым»: нулевой и единичный элементы у них во всяком случае общие.

и, значит, $\mathfrak{P}$ действительно простое. Если тело $\mathfrak{K}$ имеет делителем еще иное простое тело $\mathfrak{P}_1$, то опять заключаем: $\mathfrak{P} \subset \mathfrak{P}_1$, т. е. $\mathfrak{P} = \mathfrak{P}_1$— единственное простое тело в $\mathfrak{K}$, и теорема доказана.

Подобная же теорема существует и для областей целости, имеющих единичный элемент.

Следствие. Если $\mathfrak{K} \supset \mathfrak{K}_1$ и тело $\mathfrak{K}$ содержит простое тело $\mathfrak{P}$, то и тело $\mathfrak{K}_1$ содержит то же простое тело $\mathfrak{P}$.

Посмотрим теперь, какие существуют простые тела (и простые области целости с единичным элементом). Во всяком теле имеется нулевой и единичный элементы, а следовательно, и все целые кратные единичного элемента: $\pm n\varepsilon$, где n — любое натуральное число; но все эти кратные составляют область целости с единичным элементом (§ 236) и при этом простую такую область. Но тут следует различать два случая:

1) При различных целых n все элементы $n\varepsilon$ различны, т. е. равенство $n\varepsilon = n'\varepsilon$ влечет за собою $n = n'$. Эта область целости $\mathfrak{F}_0$ бесконечна и изоморфна области всех целых рациональных чисел. По теореме об образовании частных (§ 236) расширяем область $\mathfrak{F}_0$ до тела $\mathfrak{P}_0$. Для этого, первым делом, вводим «обратные элементы» к $n\varepsilon$, обозначая: $(n\varepsilon)^{-1} = \dfrac{1}{n}\varepsilon$; далее, обозначаем:

$$m\left(\frac{1}{n}\varepsilon\right) = \frac{m}{n}\varepsilon.$$

Заметим, что при $\dfrac{m}{n} = \dfrac{m'}{n'}$ и $\dfrac{m}{n}\varepsilon = \dfrac{m'}{n'}\varepsilon$; действительно,

$$\frac{m}{n}\varepsilon \cdot nn'\varepsilon = mn' \cdot n \cdot \frac{1}{n}\varepsilon = mn'\varepsilon,$$
$$\frac{m'}{n'}\varepsilon \cdot nn'\varepsilon = m'n \cdot n' \cdot \frac{1}{n'}\varepsilon = m'n\varepsilon,$$

но так как $mn' = m'n$, то, следовательно:

$$\frac{m'}{n'}\varepsilon \cdot nn'\varepsilon = \frac{m}{n}\varepsilon \cdot nn'\varepsilon,$$

а отсюда по закону однозначной обратимости:

$$\frac{m'}{n'}\varepsilon = \frac{m}{n}\varepsilon,$$

что и требовалось доказать.

Отсюда же легко вытекает, что над элементами $\dfrac{m}{n}\varepsilon$ действия совершаются так же, как над обычными дробями $\dfrac{m}{n}$, и все такие элементы и составляют искомое тело $\mathfrak{P}_0$, изоморфное абсолютной области рациональности, которая, таким образом, является простым телом. Действительно, уравнение

$$\frac{m}{n}\varepsilon \cdot x = \frac{m_1}{n_1}\varepsilon$$

имеет единственное решение $x = \dfrac{m_1 n}{mn_1}\varepsilon$, т. е. для $\mathfrak{P}_0$ выполнен и постулат 7 § 235.

Если данное тело $\mathfrak{K}$ имеет делителем простое тело $\mathfrak{P}_0$, то говорят, что тело $\mathfrak{K}$ имеет *характеристику нуль*. Все числовые тела имеют характеристику нуль (ср. главу I, § 13).

2) Пусть теперь для некоторых целых чисел $m \neq m'$ имеем $m\varepsilon = m'\varepsilon$; тогда $(m - m')\varepsilon = 0$. Следовательно, для некоторого положительного n

$$n\varepsilon = 0^{112} \tag{7}$$

Выберем наименьшее целое положительное n так, чтобы (7) имело место; пусть это n составное: $n = n_1 n_2$, $1 < n_1 < n$, $1 < n_2 < n$; тогда $n\varepsilon = n_1\varepsilon \cdot n_2\varepsilon = 0$, но $n_1\varepsilon \neq 0$, $n_2\varepsilon \neq 0$, т. е. произведение равно нулю, тогда как ни один сомножитель не равен нулю. А так как для области целости верен закон об отсутствии нулевых делителей, то мы пришли к противоречию. Следовательно, $n = p$ — число простое.

Из $p\varepsilon = 0$ следует: $p\varepsilon + \varepsilon = (p + 1)\varepsilon = \varepsilon$; точно так же $(p + 2)\varepsilon = 2\varepsilon$; далее $(np)\varepsilon = 0$ и вообще $(np + m)\varepsilon = m\varepsilon$.

Обратно, пусть $k\varepsilon = l\varepsilon$; тогда $(k - l)\varepsilon = 0$. Если разделим $k - l$ на p, то найдем: $k - l = pq + r$, где $0 \leq r < p$; далее $(pq + r)\varepsilon = (pq)\varepsilon + r\varepsilon = 0$; но $(pq)\varepsilon = 0$, следовательно: $r\varepsilon = 0$. Но $0 \leq r < p$ и p наименьшее положительное число, для которого $p\varepsilon = 0$; следовательно, $r = 0$ и $k - l = pq$, или

$$k \equiv l \pmod{p}.$$

Это — необходимое и достаточное условие того, чтобы было

$$k\varepsilon \equiv l\varepsilon,$$

где k и l — целые числа, не равные нулю.

Итак, в этом случае существует только p различных элементов, кратных ε, именно: $\varepsilon, 2\varepsilon, 3\varepsilon, \ldots, (p-1)\varepsilon$, $p\varepsilon = 0$. Эти p элементов составляют простую область целости с единицей; но мы докажем, что эта область целости является и телом, — простым и, как мы видим, конечным, для этого достаточно показать, что уравнение $k\varepsilon \cdot x = l\varepsilon$ всегда имеет решение того же вида: $x = m\varepsilon$; действительно, это уравнение сводится к сравнению $km \equiv l \pmod{p}$, имеющему всегда при данных k, l, не делящихся на p, единственное (по модулю p) решение m.

Полученное тело обозначим через $\mathfrak{P}_p$. Если тело $\mathfrak{K}$ имеет делителем простое тело $\mathfrak{P}_p$, то говорят, что оно имеет *характеристику* p. Тело $\mathfrak{P}_p$ изоморфно телу вычетов целых чисел по простому модулю p.

Предыдущее позволяет высказать следующую теорему:

Теорема. *Единственные существующие типы простых тел суть: тип* $\mathfrak{P}_0$ *(изоморфный абсолютной области рациональности) и тип* $\mathfrak{P}_p$ *(изоморфный телу вычетов целых чисел по простому модулю* p*).*

§ 238. Рациональные функции в теле. Пусть $\mathfrak{K}$ — данное тело, а x — какой-то новый, не входящий в $\mathfrak{K}$ элемент. Выражение

$$f(x) = a_0 x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n = \sum_{\lambda=0}^{n} a_\lambda x^{n-\lambda}, \tag{8}$$

[112] Это не противоречит закону об отсутствии нулевых делителей, так как n не есть элемент тела.

где $a_0, a_1, \ldots, a_n$ — элементы из тела $\mathfrak{K}$, называется *целой рациональной функцией* от x в теле $\mathfrak{K}$. При этом мы подразумеваем, что над элементом x и элементами из $\mathfrak{K}$ возможны действия сложения, вычитания и умножения, что степени x определяются как произведения сомножителей, равных x, и, наконец, что $x^0 = \varepsilon$. Для действий над x и над элементами из $\mathfrak{K}$ мы считаем выполненными постулаты 1–7 § 235. Этот элемент x иногда называют *переменным*; мы можем вместо него подставить любой элемент c из $\mathfrak{K}$, и тогда $f(x)$ обратится в $f(c)$; это — тоже некоторый элемент из $\mathfrak{K}$. Но в алгебре понятие о «переменном» не имеет того значения, что в анализе: мы здесь не исследуем, как «изменяется» функция в зависимости от «изменения» ее аргумента; в алгебре «переменное» есть просто символ для нового элемента, не связанного никакими соотношениями с элементами данного тела; в этом смысле наше «переменное» x называется *трансцендентным* элементом.

Определим теперь действия сложения, вычитания, умножения над целыми рациональными функциями от x вида (8), как над обычными числовыми многочленами; но для этого мы еще ставим условие, что нулевой и единичный элементы тела $\mathfrak{K}$ являются нулевым и единичным элементами и для x, т. е. что

$$0 \cdot x = x \cdot 0 = 0, \qquad \varepsilon \cdot x = x \cdot \varepsilon = x.$$

Таким образом те члены в (8), у которых соответствующие «коэфициенты» a_λ равны нулю, можно просто не писать; первый (или «высший») коэфициент a_0 берется не равным нулю, и тогда n называется *степенью* функции (8). Ц. р. функция первой степени называется *линейной*. Отдельный элемент $a \neq 0$ из $\mathfrak{K}$ мы будем считать ц. р. функцией *нулевой* степени, принимая во внимание, что $a = a\varepsilon = ax^0$. Нуль играет особую роль; ц. р. функция равна нулю, если все его коэфициенты равны нулю, и только в этом случае. Из главы III, § 46 известно, что степень алгебраической суммы целых рациональных функций не выше наивысшей степени слагаемого, а степень произведения равна сумме степеней сомножителей; все это верно и здесь, ибо мы определяем сложение, вычитание и умножение наших целых рациональных функций формально по тем же правилам, что и в § 46.

Рассматривая теперь совокупность всех целых рациональных функций от x в теле $\mathfrak{K}$, мы можем сказать, что эта совокупность есть *область целости*; обозначим ее через $\mathfrak{K}[x]$. Действительно, постулаты 1–6 § 235 проверяются непосредственно, закон же отсутствия нулевых делителей тоже верен: если ц. р. функции $f(x)$ и $g(x)$ отличны от нуля, то и их произведение $f(x)g(x)$ тоже отлично от нуля, ибо по известной теореме из элементарной алгебры члены этого произведения не могут все сократиться.

Расширим теперь область целости $\mathfrak{K}[x]$ до тела по теореме об образовании частных (§ 236); это сведется к тому, что кроме ц. р. функций мы построим и дробные рациональные функции вида $\dfrac{f(x)}{g(x)}$, где $f(x)$ и $g(x)$ — целые рациональные функции в $\mathfrak{K}$, причем $g(x) \neq 0$. Полученное таким образом тело мы обозначим через $\mathfrak{K}(x)$. Так как сами элементы из $\mathfrak{K}$ рассматриваются как ц. р. функции от x нулевой степени, т. е. принадлежат к $\mathfrak{K}[x]$, то, следовательно: $\mathfrak{K} \subset \mathfrak{K}[x]$ и значит и $\mathfrak{K} \subset \mathfrak{K}(x)$. В этом смысле тело $\mathfrak{K}(x)$ есть расширение тела $\mathfrak{K}$, и при этом — трансцендентное расширение, ибо x — трансцендентный элемент. Мы рассмотрим это расширение подробнее в следующем параграфе.

§ 239. Трансцендентное расширение тела. Пусть, как и раньше, $\mathfrak{K}(x)$ — трансцендентное расширение тела $\mathfrak{K}$. Возьмем два элемента из $\mathfrak{K}(x)$, т. е. две рациональные функции в $\mathfrak{K}$: $\dfrac{f_1(x)}{g_1(x)}$ и $\dfrac{f_2(x)}{g_2(x)}$, и посмотрим, когда они равны друг другу: если $\dfrac{f_1(x)}{g_1(x)} = \dfrac{f_2(x)}{g_2(x)}$, то должно быть:

$$f_1(x)g_2(x) - f_2(x)g_1(x) = 0. \tag{9}$$

Левая часть в (9) есть ц. р. функция: она равна нулю, т. е. все ее коэфициенты равны нулю (ср. § 238); этот факт есть следствие того, что x — трансцендентный элемент: иначе (9) дало бы некоторое соотношение элемента x и элементов из $\mathfrak{K}$. Назовем такое равенство, как (9), когда в левой части все коэфициенты равны нулю, — *тождеством*; все равенства, вытекаемые из тождества, тоже назовем тождествами, а обе части тождества — *тождественными*, или тождественно равными друг другу. Итак, можно сказать, что в теле $\mathfrak{K}(x)$ два элемента равны тогда и только тогда, если они тождественны. Иными словами, все равенства в теле $\mathfrak{K}(x)$ имеют характер тождеств.

Рассмотрим элементы из $\mathfrak{K}[x]$, иными словами, ц. р. функции от x в $\mathfrak{K}$. Если $f(x)$ и $g(x)$ две такие функции, то мы можем формально разделить $f(x)$ на $g(x)$ (§ 47), найдя неполное частное $q(x)$ и остаток $r(x)$ тоже как элементы из $\mathfrak{K}[x]$, причем степень $r(x)$ меньше степени $g(x)$; получим (как и в § 47):

$$f(x) = g(x)q(x) + r(x). \tag{10}$$

А отсюда вытекает вся теория делимости в области $\mathfrak{K}[x]$. Если $r(x) = 0$, то $f(x)$ *делится на* $g(x)$. Все теоремы § 48, теорема Декарта (§ 49), способ Горнера деления на линейную функцию — остаются в силе; верен также алгорифм Эвклида и вытекающие из него следствия; как и в главе III, вводится понятие об общем наибольшем делителе ц. р. функций, причем этот общий наибольший делитель определен с точностью до множителя из $\mathfrak{K}$, далее, вводится понятие о взаимно простых функциях, за общий наибольший делитель которых можно взять единичный элемент ε. Далее, остаются также верными теоремы § 53 о взаимно простых функциях. Наконец, как и в § 111, определяются приводимые и неприводимые в $\mathfrak{K}$ функции и доказывается теорема о разложимости всякой ц. р. функции в $\mathfrak{K}$ на неприводимых в $\mathfrak{K}$ множителей и об однозначности этого разложения.

Упомянем еще о таких свойствах трансцендентного расширения тела:

Все расширения тела $\mathfrak{K}$ посредством одного трансцендентного элемента изоморфны друг другу, причем в этих изоморфизмах тело $\mathfrak{K}$ соответствует само себе (такой изоморфизм называется *эквивалентностью*). Следовательно, тела $\mathfrak{K}(x)$ и $\mathfrak{K}(y)$, где x и y — два различных трансцендентных относительно $\mathfrak{K}$ элемента, — эквивалентны; это — очевидно, ибо такие тела только обозначением отличаются друг от друга.

Если x — трансцендентный относительно $\mathfrak{K}$ элемент, то все элементы тела $\mathfrak{K}(x)$ за исключением элементов из $\mathfrak{K}$ — трансцендентны.

Эта теорема легко доказывается при помощи теоремы о том, что если $f(x)$ и $g(x)$ — рациональные в $\mathfrak{K}$ функции, не равные тождественно нулю, то и $f(g(x))$ тоже не равно тождественно нулю; на этой теореме мы останавливаться не будем.

На основании предыдущих двух свойств мы заключаем, что если $f(x)$ — любая рациональная функция в теле $\mathfrak{K}$ степени выше нулевой, то тела $\mathfrak{K}(x)$ и $\mathfrak{K}(f(x))$ эквивалентны, причем, очевидно, $\mathfrak{K}(x) \supset \mathfrak{K}(f(x))$; $\mathfrak{K}(x) = \mathfrak{K}(f(x))$ тогда и только тогда, если и x есть рациональная функция в $\mathfrak{K}$ от $y = f(x)$; а это в свою очередь имеет месте тогда и только тогда, если $f(x) = \dfrac{ax+b}{cx+d}$, т. е. является *дробной линейной* функцией от x. Элемент y тела $\mathfrak{K}(x)$, отличающийся свойством, что всякий элемент этого тела есть рациональная функция от y в теле $\mathfrak{K}$, называется *первообразным* (*примитивным*). Мы можем сказать:

Первообразными элементами тела $\mathfrak{K}(x)$ являются кроме x все линейные (дробные и целые) функции от x в теле $\mathfrak{K}$, и только они.

§ 240. Алгебраическое расширение тела. Пусть теперь присоединяемый к телу $\mathfrak{K}$ элемент x связан с элементами тела $\mathfrak{K}$ некоторым соотношением; это соотношение мы только и можем представить себе как некоторое равенство двух, не равных друг другу тождественно, рациональных функций от x в теле $\mathfrak{K}$ (ибо никаких иных действий над элементами из $\mathfrak{K}$ и над элементом x, кроме четырех рациональных действий, мы не знаем). Но, помножив обе части такого равенства:

$$\frac{f_1(x)}{g_1(x)} = \frac{f_2(x)}{g_2(x)}, \tag{11}$$

(где f_1, g_1, f_2, g_2 — ц. р. функции в $\mathfrak{K}$ на $g_1(x)g_2(x)$ и перенеся все члены в левую часть, мы получим равенство вида:

$$F(x) = 0, \tag{11}$$

где F — целая рациональная функция в $\mathfrak{K}$. Таким образом (11а) есть *алгебраическое уравнение* в $\mathfrak{K}$, которому удовлетворяет x; в этом смысле x есть *алгебраический элемент* относительно тела $\mathfrak{K}$. Уравнение (11а) имеет вид:

$$a_0x^m + a_1x^{m-1} + \ldots + a_{m-1}x^1 + a_mx^0 = 0, \tag{11}$$

где $a_0, a_1, \ldots, a_{m-1}, a_m$ — элементы из $\mathfrak{K}$, при этом $a_0 \neq 0$. Таким образом (11б) показывает, что степени $x^0, x^1, x^2, \ldots, x^m$ элемента x *линейно зависимы относительно тела* $\mathfrak{K}$ (ср. § 42), или, точнее, x^m *линейно зависит* от $x^0 = \varepsilon, x^1, x^2, \ldots, x^{m-1}$. В этом существенное отличие алгебраических элементов относительно $\mathfrak{K}$ от трансцендентных: для последних любая конечная совокупность их различных степеней линейно независима относительно тела $\mathfrak{K}$.

Если функция $F(x)$ в (11а) приводима в теле $\mathfrak{K}$, то разложим ее на неприводимые множители:

$$F(x) = f(x)f_1(x)f_2(x)\cdots;$$

это — тождество, верное для любого элемента x; если x удовлетворяет уравнению (11а) (или является корнем этого уравнения), то, следовательно:

$$f(x)f_1(x)f_2(x)\cdots = 0, \tag{11}$$

а так как для нашего умножения верен закон об отсутствии нулевых делителей, то по крайней мере один из сомножителей левой части (11в) должен быть равен нулю для рассматриваемого элемента x, например,

$$f(x) = 0. \tag{12}$$

Это — *неприводимое уравнение* для x в теле $\mathfrak{K}$. Неприводимая в теле $\mathfrak{K}$ функция $f(x)$ определена с точностью до множителя из $\mathfrak{K}$. Действительно, если $g(x)$ какая-нибудь иная отличная от $f(x)$ неприводимая в $\mathfrak{K}$ ц. р. функция, то (по следствию VII § 110, которое здесь имеет место) она не может иметь общего корня с функцией $f(x)$, если только она не равна $cf(x)$, где $c \subset \mathfrak{K}$.

Если случайно окажется, что функция $f(x)$ в (12) линейная, то x окажется элементом из $\mathfrak{K}$ (т. е. «рациональным» элементом относительно $\mathfrak{K}$). Таким образом, если x — алгебраический элемент относительно $\mathfrak{K}$, но не рациональный, то функция $f(x)$ в (12) степени выше первой. Итак, всякий алгебраический (но не рациональный) относительно $\mathfrak{K}$ элемент x удовлетворяет одному и только одному неприводимому в $\mathfrak{K}$ уравнению степени выше первой. Эта степень называется степенью элемента x относительно $\mathfrak{K}$, а также степенью алгебраического тела $\mathfrak{K}(x)$ над $\mathfrak{K}$.

Но мы должны еще выяснить, что представляет собой такое тело $\mathfrak{K}(x)$, да и будет ли оно вообще телом. Посмотрим, чем отличается $\mathfrak{K}(x)$ при алгебраическом элементе x от $\mathfrak{K}(x)$ при трансцендентном x; при трансцендентном x целые рациональные функции от x в $\mathfrak{K}$ считаются различными, если они не равны тождественно друг другу; но если x — алгебраический элемент, удовлетворяющий уравнению (12), то две ц. р. функции в $\mathfrak{K}$ $\varphi_1(x)$ и $\varphi_2(x)$ мы считаем равными, если они различаются на кратное функции $f(x)$, т. е. если $\varphi_1(x) = \varphi_2(x) + f(x)g(x)$, ибо ведь $f(x) = 0$. Такие функции $\varphi_1(x)$ и $\varphi_2(x)$ называются *сравнимыми* (*конгруентными*) *по модулю* $f(x)$; обозначают:

$$\varphi_1(x) \equiv \varphi_2(x) \pmod{f(x)}. \tag{13}$$

Таким образом алгебраическое тело отличается от трансцендентного тем, что в первом из них мы равенства заменяем сравнениями вида (13), или, иными словами, — более широко понимаем равенство. Для сравнений вида (13) верны три основных закона равенств (глава I, § 2); далее, легко видеть, что из (13) и из сравнения

$$\psi_1(x) \equiv \psi_2(x) \pmod{f(x)}$$

следует:

$$\left.\begin{aligned} \varphi_1(x) + \psi_1(x) &\equiv \varphi_2(x) + \psi_2(x), \\ \varphi_1(x)\psi_1(x) &\equiv \varphi_2(x)\psi_2(x), \end{aligned}\right\} \pmod{f(x)}. \tag{14}$$

А отсюда легко следует, что все ц. р. функции от x в теле $\mathfrak{K}$ (включая сюда и самые элементы тела $\mathfrak{K}$, или, иными словами, — все элементы области целости $\mathfrak{K}[x]$, — распределяются по классам, причем (14) позволяют определить действия сложения и умножения над классами сложением и умножением соответствующих представителей этих классов. Следовательно, эта система классов есть система с двумя действиями, причем можно непосредственно убедиться, что постулаты 1–6 § 235 для нее выполнены, т. е. эта система есть кольцо. Но мы докажем, что и постулат 7 § 235 верен, т. е. что эта система классов есть тело («тело классов»). Пусть $\varphi(x)$ — ц. р. функция в $\mathfrak{K}$, не делящаяся на $f(x)$, т. е. взаимно простая с $f(x)$ (по следствию I, § 110); тогда (по второй теореме § 52) можно найти такие ц. р. функции в $\mathfrak{K}$ $f_1(x)$ и $\varphi_1(x)$, что

$$\varphi(x)\varphi_1(x) + f(x)f_1(x) = \varepsilon.$$

Написав это как сравнение по модулю $f(x)$, получим:

$$\varphi(x)\varphi_1(x) \equiv \varepsilon \qquad (\mathrm{mod}\, f(x)).$$

Если теперь $\psi(x)$ — любая целая рациональная функция в $\mathfrak{K}$, то

$$\varphi(x)[\varphi_1(x)\psi(x)] \equiv \psi(x)\ (\mathrm{mod}\, f(x)),$$

т. е. сравнение $\varphi(x)\cdot X \equiv \psi(x)\ (\mathrm{mod}\, f(x))$ имеет решение $X = \varphi_1(x)\psi(x)$ при любых данных $\varphi(x)$ и $\psi(x)$, если только

$$\varphi(x) \not\equiv 0\ (\mathrm{mod}\, f(x))$$

[т. е. если $\varphi(x)$ не делится на $f(x)$]. Докажем, что это решение — единственное. Пусть мы имеем два решения X_1 и X_2; тогда

$$\varphi(x)X_1 \equiv \varphi(x)X_2\ (\mathrm{mod}\, f(x)),$$

или

$$\varphi(x)(X_1 - X_2) \equiv 0\ (\mathrm{mod}\, f(x)),$$

т. е. произведение $\varphi(x)(X_1 - X_2)$ делится на $f(x)$, но $\varphi(x)$ и $F(x)$ взаимно простые; следовательно (по теореме 1 § 53), $X_1 - X_2$ делится на $f(x)$, т. е. $X_1 - X_2 \equiv 0\ (\mathrm{mod}\, f(x))$, или

$$X_1 \equiv X_2\ (\mathrm{mod}\, f(x)),$$

т. е. функции X_1 и X_2 принадлежат к одному и тому же классу, и, значит, являются представителями одного и того же решения. Этим доказана верность постулата 7 § 235 для кольца классов элементов из $\mathfrak{K}[x]$; таким образом это кольцо есть тело; это и есть по существу алгебраическое тело $\mathfrak{K}(x)$, где x — алгебраический элемент относительно $\mathfrak{K}$. [Если желательно, то можно считать, что алгебраическое тело $\mathfrak{K}(x)$ изоморфно телу классов, которое мы рассмотрели; это по существу одно и то же.] Таким образом для формирования алгебраического тела $\mathfrak{K}(x)$ нет надобности вводить дробные функции от x: эти дробные функции здесь оказываются равными целым функциям.

Таким образом алгебраическое расширение $\mathfrak{K}(x)$ тела $\mathfrak{K}$ вполне определяется неприводимой функцией $f(x)$ в теле $\mathfrak{K}$, корнем которой является x; но эта функция $f(x)$ определяет только одно тело классов, структура которого совершенно не зависит от взятого корня x. Это показывает, что, какой бы из корней уравнения (12) мы ни присоединили к $\mathfrak{K}$, получаемые алгебраические расширения $\mathfrak{K}(x)$ друг другу эквивалентны (§ 239) [113].

Из предыдущего следует, что алгебраическое расширение возможно не для всякого тела, а только для такого, в котором имеются неприводимые целые рациональные функции степени выше первой. Если же в данном теле $\mathfrak{K}$ неприводимыми являются только функции первой степени, т. е. если в $\mathfrak{K}$ всякая целая

[113] Это вполне ясно по отношению к конкретным, например, числовым телам, где нам из других источников известно существование корней данного уравнения и число этих корней. В абстрактной теории «существование» корня неприводимого уравнения по существу равнозначно с возможностью алгебраического расширения тела; число же корней обусловливается возможностью распадения всякой целой рациональной функции на липейные множители.

рациональная функция раскладывается на линейные множители, то для такого тела $\mathfrak{K}$ алгебраическое расширение невозможно. Такое тело называется *алгебраически замкнутым* (ср. § 76).

§ 241. Кратные корни. Пусть опять $f(x)$ неприводимая функция n-й степени в теле $\mathfrak{K}$. Через x теперь обозначим трансцендентный элемент («переменное»), а корень функции $f(x)$ обозначим через j. Тогда в теле $\mathfrak{K}(j)$ функция $f(x)$ делается приводимой: она разделится на $x-j$ [это следует из § 239 (10) при $g(x)=x-j$ — совершенно так же, как в § 49 вытекало аналогичное следствие из теоремы Декарта]. Обозначая теперь $\dfrac{f(x)}{x-j}=f_1(x)$, присоединяем к телу $\mathfrak{K}_1=\mathfrak{K}(j)$ корень j_1 функции $f_1(x)$ или одного из ее неприводимых множителей, — если эта функция приводима. Расширяя, таким образом, все дальше и дальше тело $\mathfrak{K}$, мы дойдем до такого его расширения, в котором наша функция $f(x)$ n-й степени распадается на n линейных множителей:

$$f(x)=(x-j_1)(x-j_2)\cdots(x-j_n).$$

И здесь, как в § 50, объединяя одинаковые сомножители, получим:

$$f(x)=(x-\rho)^{\alpha}(x-\sigma)^{\beta}(x-\tau)^{\gamma}\cdots,$$

где $\rho,\sigma,\tau,\ldots$ — *различные* элементы. При $\alpha>1$ корень ρ называется *кратным*, и именно *α-кратным*, и то же самое для $\sigma,\tau,\ldots$ При $\alpha=1$ корень ρ простой. Для того чтобы обобщить теоремы § 57 о кратных корнях на нашу абстрактную теорию, мы должны дать определение производной. Как и в § 54, мы определяем производные чисто формально.

Если

$$f(x)=a_0x^n+a_1x^{n-1}+a_2x^{n-2}+\ldots+a_{n-1}x+a_n,$$

то

$$\begin{aligned}
f'(x) &= na_0x^{n-1}+(n-1)a_1x^{n-1}+(n-2)a_2x^{n-3}+\ldots+a_{n-1},\\
f''(x) &= n(n-1)a_0x^{n-2}+(n-1)(n-2)a_1x^{n-3}+\\
&\quad +(n-2)(n-3)a_2x^{n-4}+\ldots+2a_{n-2},\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
f^{(n)}(x) &= n!a_0\\
f^{(n+1)}(x) &= 0.
\end{aligned}$$

Можно проверить вычислением, что

$$[f(x)+g(x)]'=f'(x)+g'(x),$$
$$[f(x)g(x)]'=f(x)g'(x)+f'(x)g(x).$$

Выясним теперь, при каких условиях производная целой рациональной функции тождественно равна нулю. Это будет, конечно, тогда, если $f(x)$ нулевой степени, то-есть является элементом из $\mathfrak{K}$. Если тело $\mathfrak{K}$ характеристики нуль, то этот случай и единственный. Если же тело $\mathfrak{K}$ характеристики p, то есть еще другие случаи, когда производная целой рациональной функции тождественно равна нулю: это, именно, когда данная функция зависит только от x^p, т. е. имеет вид:

$$f(x)=a_0x^{kp}+a_1x^{(k-1)p}+\ldots+a_{k-1}x^p+a_k.$$

В самом деле, тогда

$$f'(x) = kpa_0x^{kp-1} + (k-1)pa_1x^{(k-1)p-1} + \ldots + pa_{k-1}x^{p-1};$$

но (§ 237) $pa_0 = p\varepsilon\cdot a_0 = 0$, $pa_1 = p\varepsilon\cdot a_1 = 0, \ldots, pa_{k-1} = 0$; следовательно: $f'(x) = 0$ тождественно.

Пусть теперь ц. р. функция $f(x)$ в теле $\mathfrak{K}$ имеет r-кратный корень α, т. е.

$$f(x) = (x-\alpha)^r g(x),$$

где $g(x)$ уже не делится на $x-\alpha$. Тогда

$$f'(x) = (x-\alpha)^{r-1}[r\varepsilon\cdot g(x) + (x-\alpha)g'(x)]. \tag{15}$$

Из (15) видно, что $f'(x)$ содержит множителем $x-\alpha$ по крайней мере $r-1$ раз; при этом *точно* $r-1$ раз, если $r\varepsilon \neq 0$, т, е. если $\mathfrak{K}$ характеристики нуль, или если $\mathfrak{K}$ характеристики p, но r не делится на p; если же r делится на p, то $r\varepsilon = 0$ и $f'(x) = (x-\alpha)^r g'(x)$, т. е. в этом случае корень α для функции $f(x)$ по крайней мере кратности r.

Если корень α — простой для функции $f(x)$, то он совсем не является корнем для производной, т. е. $f'(\alpha)$.

Если ц. р. функция $f(x)$ заверит только от x^p:

$$f(x) = F(x^p),$$

то для всякого корня α этой функции и ее производная равна нулю, ибо $f'(x) =$ тождественно. Следовательно, показатель r кратности всякого корня делится на p, т. е. если

$$f(x) = (x-\alpha_1)^{r_1}(x-\alpha_2)^{r_2}\cdots(x-\alpha_\nu)^{r_\nu},$$

то все r_λ делятся на p; но тогда $f(x)$ есть точная p-я степень ц. р. функции. Обратно, если все r_λ делятся на p, т. е. если $f(x)$ точная p-я степень ц. р. функции, то $f'(x)$ содержит $x-\alpha_\lambda$ (при $\lambda = 1, 2, \ldots, \nu$) по крайней мере r_λ раз, и $f'(x)$ делится на $f(x)$, т. е. $f'(x) = 0$ тождественно, откуда следует, что $f(x)$ зависит только от x^p.

Итак, если тело $\mathfrak{K}$ характеристики p, то бывают случаи, когда производная целой рациональной функции в $\mathfrak{K}$ тождественно равна нулю, тогда как сама эта ц. р. функция содержит «переменное» (не является элементом из $\mathfrak{K}$). Отсюда вытекает, что следствие VI § 110 вообще не имеет места, и неприводимое уравнение в теле $\mathfrak{K}$ с характеристикой p в некоторых случаях может иметь и кратные корни. Различают тела *совершенные* и *несовершенные*; совершенные тела таковы, что всякая неприводимая функция в них не имеет кратных корней; в несовершенном же теле существуют неприводимые функции с кратными корнями. Очевидно, что всякое тело с характеристикой нуль совершенно. Для тел с характеристикой p существует такая теорема:

Тело с характеристикой p совершенно тогда и только тогда, если в этом теле неограниченно возможно извлечение корня p-й степени (и это действие здесь однозначно).

Обратим внимание еще на следующую формулу для элементов тела с характеристикой p:

$$(a_1 + a_2 + \ldots + a_m)^{p^f} = a_1^{p^f} + a_2^{p^f} + \ldots + a_m^{p^f}.$$

§ 242. Конечные тела. Эти тела называются еще телами Галуа, открывшего их. Очевидно, что характеристика такого тела не может быть нулем, ибо уже простое тело с характеристикой нуль бесконечно. Пусть наше конечное тело $\mathfrak{K}$ имеет характеристику p. Обозначим через $\mathfrak{P}$ простое тело с характеристикой p, т. е. тело, изоморфное (§ 237) телу классов чисел по простому модулю p. Тело $\mathfrak{K}$ содержит $\mathfrak{P}$, т. е. является телом над $\mathfrak{P}$. Пусть n — наибольшее число элементов из $\mathfrak{K}$, линейно независимых относительно $\mathfrak{P}$, и пусть эти линейно независимые относительно $\mathfrak{P}$ элементы из $\mathfrak{K}$ суть: $\alpha_1, \alpha_2, \ldots, \alpha_n$. Число n конечно, ибо $\mathfrak{K}$ вообще содержит только конечное число элементов. Отсюда, далее, следует, что всякий элемент α из $\mathfrak{K}$ представляется, и при этом однозначно, в виде:

$$\alpha = c_1\alpha_1 + c_2\alpha_2 + \ldots + c_n\alpha_n,$$

где $c_1, c_2, \ldots, c_n$ — элементы из $\mathfrak{P}$. Но каждый элемент c_λ может иметь всего p значений, т. е. существуют всего p^n комбинаций $c_1, c_2, \ldots, c_n$, и различным комбинациям соответствуют различные элементы α. Следовательно, тело $\mathfrak{P}$ имеет всего p^n различных элементов.

Отбросив нулевой элемент, получим, что все остальные элементы тела $\mathfrak{P}$ образуют группу относительно умножения; таким образом эта труппа порядка $p^n - 1$. Отсюда следует, что порядок всякого элемента этой группы — делитель числа $p^n - 1$, т. е. для всякого элемента α этой группы

$$\alpha^{p^n-1} = 1.$$

Отсюда легко найдем

$$\alpha^{p^n} - \alpha = 0. \tag{16}$$

Этому уравнению удовлетворяют уже все элементы тела $\mathfrak{K}$, включая и нулевой элемент; если эти элементы мы обозначим через $\alpha_1, \alpha_2, \ldots, \alpha_{p^n}$, то, следовательно:

$$x^{p^n} - x = \prod_{\lambda=1}^{p^n}(x - \alpha_\lambda). \tag{16}$$

Итак, тело получается из $\mathfrak{K}$ присоединением к $\mathfrak{P}$ всех корней уравнения (16). Этим структура тела $\mathfrak{K}$ вполне определена, т. е. существует только один тип конечного тела с p^n элементами при данных p (простом) и n (натуральном).

Сам Галуа пришел к названным его именем конечным телам, рассматривая задачу решения сравнений с простым модулем в теории чисел [114]. Пусть имеем такое неприводимое сравнение n-й степени:

$$f(x) \equiv 0 \pmod p, \tag{17}$$

где $f(x)$ — функция, не приводимая по модулю p, т. е. $f(x)$ не раскладывается по модулю p на множителей, и сравнение (17) обычных целых корней не имеет. Галуа вводит новое, «мнимое» число j, которое он определяет как корень сравнения (17), т. е.

$$f(j) \equiv \pmod p. \tag{17}$$

[114] См. E. Galois, Sur *l*a théorie des nombres, Oeuvres de Galois, publ. par Picard, Paris 1897, стр. 15–23. Готовится к печати русское издание сочинений Эвариста Галуа.

Далее, Галуа рассматривает выражения:

$$\alpha = a_0 + a_1 j + a_2 j^2 + \ldots + a_{n-1} j^{n-1}. \tag{18}$$

Здесь $a_0, a_1, a_2, \ldots, a_{n-1}$ — целые, определенные по модулю p коэфициенты; каждый из них имеет p значений (например, $0, 1, 2, \ldots, p-1$), т. е. всего имеем p^n различных комбинаций этих значений; различным комбинациям соответствуют различные «числа» α; именно, если двум различным комбинациям соответствовало бы одно и то же число α, то разность этих чисел была бы сравнима с нулем, и мы имели бы сравнение вида:

$$\varphi(j) = c_0 + c_1 j + c_2 j^2 + \ldots + c_{n-1} j^{n-1} \equiv 0 \pmod{p}, \tag{19}$$

где не все $c_0, c_1, c_2, \ldots, c_{n-1}$ сравнимы с нулем; но отсюда следовало бы, что функции $f(x)$ и $\varphi(x)$ были бы не взаимно простые, чего не может быть, ибо $f(x)$ неприводима, а $\varphi(x)$ степени, низшей, чем $f(x)$. Но сумма и произведение чисел вида (18) — тоже числа того же вида, ибо коэфициенты a_λ определены по модулю p, а если в произведениях получаются функции от j степени большей или равной n, то мы делим их на $f(j)$ и берем остатки [иначе: «сводим по модулю $f(j)$], поскольку $f(j) \equiv 0$.

Итак, числа вида (18) представляют замкнутую систему с двумя действиями — сложением и умножением, причем постулаты 1–7 § 235 для нее выполнены, т. е. эта система есть тело, — конечное тело, имеющее p^n элементов.

Проверим постулат 7. Пусть $\alpha = \varphi(j)$ — одно из выражений вида (18); φ — ц. р. функция степени не большей $n-1$ с целыми коэфициентами. Требуется решить сравнение:

$$\varphi(j) X \equiv 1 \pmod{p}.$$

Но так как функции $\varphi(x)$ и $f(x)$ взаимно простые, то можно (по § 52) найти такие функции $\Phi(x)$ и $F(x)$, чтобы было

$$\varphi(x)\Phi(x) + f(x)F(x) = a, \tag{20}$$

где a — некоторое целое число, не делящееся на p, и коэфициенты в функциях Φ и F все целые. Положив теперь $x = j$, получим из (20) по (17):

$$\varphi(j)\Phi(j) = a.$$

Найдем теперь целое число b так, чтобы было $ab \equiv 1 \pmod{p}$; тогда

$$\varphi(j) \cdot b\Phi(j) \equiv 1 \pmod{p};$$

следовательно, $X = b\Phi(j)$; эта функция (или «мнимое» число) X «обратна» к $\varphi(j)$. Если теперь требуется решить сравнение

$$\varphi(j) Y \equiv \psi(j) \pmod{p},$$

то решение (и при этом единственное) будет: $Y = X\psi(j)$ и постулат 7 доказан.

Заметим, что функция $x^{p^n} - x$ делится по модулю p на всякую неприводимую по модулю p функцию, степень которой есть n или делитель числа n; корни всех этих функций представляются в виде (18).

Заметим также, что вся эта теория конечных тел есть по существу теория сравнения с двойным модулем p и $f(x)$. Именно, пусть нашими элементами будут целые рациональные функции от x с целыми, определенными по простому модулю p коэфициентами, причем две такие функции мы будем считать равными, если их разность делится на неприводимую по модулю p функцию $f(x)$.

Такое «равенство» функций $\varphi(x)$ и $\psi(x)$ мы будем обозначать, как сравнение по двойному модулю:

$$\varphi(x) \equiv \psi(x) \ (\mathrm{mod}\, p, f(x)).$$

Легко видеть, что всякая функция сравнима с одной и только с одной «приведенной» функцией вида:

$$a_0 + a_1 x + a_2 x^2 + \ldots + a_{n-1} x^{n-1} \tag{21}$$

степени $\leq n-1$?, где все коэфициенты $a_0, a_1, a_2, \ldots, a_{n-1}$ — целые числа ≥ 0 и $\leq p-1$. Таким образом в теории сравнений с двойным модулем мы оперируем с функциями вида (21); но эти функции — те же элементы (18), только вместо буквы j взята буква x.

§ 243. Кольца. Идеалы. В § 236 уже встречалось понятие кольца; кольцо есть система элементов с двумя действиями, для которых выполнены постулаты 1—6 § 235 [115]. Тела и области целости являются, таким образом, частными случаями колец. В кольцах общего вида могут встречаться так называемые «нулевые делители», т. е. такие, не равные нулю элементы, которые в произведении дают нуль:

$$ab = 0, \quad \text{тогда как} \quad a \neq 0,\ b \neq 0.$$

Если a — нулевой делитель, а x — любой элемент кольца, то ax — тоже нулевой делитель, ибо из $ab = 0$ следует $abx = (ax)b = 0$. С другой стороны, произведение чисел, не являющихся нулевыми делителями, не может быть нулевым делителем, ибо если $(xy)z = 0$, то ведь и $x(yz) = 0$, т. е. если xy — нулевой делитель, то и x — тоже нулевой делитель.

Итак, произведение нулевых делителей дает также нулевой делитель; но отсюда не следует, что нулевые делители составляют группу относительно умножения: ведь для этого умножения неверен закон неограниченной обратимости (т. е. постулат 7 § 235). Произведение не нулевых делителей — тоже не нулевой делитель; все не нулевые делители кольца образуют полугруппу (§ 211); именно, для их умножения верен закон однозначной обратимости; в самом деле, пусть a не нулевой делитель и $ab = ac$, тогда $a(b-c) = 0$, и так как a не нулевой делитель, то, следовательно, $b - c = 0$, $b = c$. В частном случае эта полугруппа не нулевых делителей кольца может быть группою (например, всегда, если кольцо конечно).

Как пример кольца, не являющегося ни телом, ни областью целости, можно взять совокупность всех m классов целых чисел по составному модулю m; действия здесь обычные — сложение и умножение. Нулевым элементом является здесь класс чисел, делящихся на m, нулевыми делителями — классы чисел, не

[115] Точнее, такое кольцо называется коммутативным; рассматриваются кольца и более общего вида, для которых неверен коммутативный закон умножения (постулат 4 § 235); на таких, более общих, кольцах мы останавливаться не будем.

взаимно простых с m. Если $\mathbf{D}(a, m) = d$, $\dfrac{m}{d} = b$, то

$$ab = \frac{a}{d}\, d\, \frac{m}{d} = \frac{a}{d}\, m \equiv 0 \pmod{m}.$$

Не нулевые делители это классы чисел, взаимно простых с m; они, как известно, образуют группу порядка $\varphi(m)$ относительно умножения.

Из постулатов 1, 2 и 6 следует, что кольцо, как и тело, представляет собою абелеву группу относительно сложения.

Если данное кольцо содержит в себе как часть другое кольцо, то это последнее называется *делителем*, или *подкольцом* первого. Для того чтобы проверить, составляет ли данная часть элементов данного кольца тоже кольцо, мы должны выяснить, является ли эта часть замкнутой системой относительно сложения и умножения и верны ли для этой части постулаты 1–6 § 235; но постулаты 1—-5, будучи верными для всего данного кольца, верны и для всякой его части; постулат же 6 (совместно с постулатом 1) говорит, что рассматриваемая часть есть группа относительно сложения; этот постулат 6 может быть заменен требованием наличия в рассматриваемой части нулевого элемента («единицы» для сложения») и «противоположного» элемента $-a$ ко всякому элементу a в этой части. А это последнее будет само собой иметь место, если мы замкнутость относительно сложения заменим замкнутостью относительно вычитания, т. е. выскажем следующее предложение:

Часть кольца является подкольцом тогда и только тогда, если для всяких элементов a и b из этой части к этой же части принадлежат и элементы: 1) $a - b$, 2) ab.

Действительно, из 1) при $a = b$ имеем: $a - a = 0$, т. е. элемент 0 принадлежит ко взятой части; положив в 1) $a = 0$, найдем $0 - b = -b$, т. е. вместе с элементом b ко взятой части принадлежит и $-b$; заменив теперь в 1) b через $-b$, найдем $a - (-b) = a + b$, т. е вместе с a и b ко взятой части принадлежит и $a + b$. Это все говорит, что взятая часть есть группа относительно сложения; 2) говорит, что взятая часть замкнута относительно умножения, т. е. эта взятая часть действительно есть подкольцо.

Заметим, что группа относительно сложения часто называется *модулем*.

Рассмотрим теперь специальный вид подкольца: условие 1) оставим в силе, условие же 2) заменим таким: 2а) *если элемент a — из взятой части, а r — какой-нибудь элемент из данного кольца, то ar тоже принадлежит ко взятой части*. Такая часть кольца (которая является частным видом подкольца) называется *идеалом*.

Таким образом, если a, b, c, ... — элементы из идеала, а r — какой-нибудь элемент данного кольца, то ar, br, cr, ... — тоже элементы того же идеала, т. е. буква r здесь есть как бы символ некоторого действия, в результате которого мы элемент a переводим в ar, точно так же b — в br и т. д. Такой символ действия называется *оператором*; следовательно, для идеала каждый элемент кольца является оператором. Идеал, таким образом, является модулем с операторами.

Идеалы обозначаются строчными готическими буквами: $\mathfrak{a}$, $\mathfrak{b}$, $\mathfrak{c}$, ...

Примеры идеалов.

1. *Нулевой идеал*, состоящий из одного элемента 0.

2. *Единичный идеал* $\mathfrak{r}$, совпадающий со всем данным кольцом т. е. содержащий все элементы кольца).

3. *Идеал* (a)*, порожденный элементом* a, состоящий из элементов вида $ra+na$, где r — любой элемент кольца, а n — любое целое число. Легко видеть, что для системы таких элементов кольца выполнены условия 1) и 2a), т. е. эта система есть действительно идеал. Этот идеал (a) — наименьший, содержащий элемент a.

Если данное кольцо имеет единичный элемент ε, то

$$ra + na = ra + n\varepsilon \cdot a = (r + n\varepsilon)a = r'a,$$

где r' — такой же любой элемент кольца, как и r. В этом случае идеал (a) состоит из всех кратных элемента a.

Идеал (a), т. е. порожденный одним элементом, называется *главным идеалом*. Нулевой идеал (0) всегда главный. Единичный идеал $\mathfrak{r}$ — главный, если кольцо имеет единичный элемент ε; именно, тогда $\mathfrak{r} = (\varepsilon)$.

4. *Идеал, порожденный несколькими, элементами* $a_1, a_2, \ldots, a_n$; он состоит из элементов вида:

$$\sum_{i=1}^{n} r_i a_i + \sum_{i=1}^{n} n_i a_i,$$

или (если данное кольцо имеет единичный элемент) из элементов вида $\sum_{i=1}^{n} r_i a_i$. Этот идеал обозначается через $(a_1, \ldots, a_n)$. Элементы $a_1, \ldots, a_n$ составляют *базис* идеала.

5. *Идеал может порождаться и бесчисленным множеством элементов* $\mathfrak{M}$; он состоит из конечных сумм вида:

$$\sum r_i a_i + \sum n_i a_i,$$

($a_i \subset \mathfrak{M}$; r_i — элементы кольца, n_i — целые числа). Обозначается такой идеал через $(\mathfrak{M})$.

Если элемент a принадлежит к идеалу $\mathfrak{a}$, то говорят, что a делится на идеал $\mathfrak{a}$, и обозначают:

$$a \equiv 0 \pmod{\mathfrak{a}}$$

(словами: элемент a сравним с нулем по идеальному модулю $\mathfrak{a}$. Если все элементы идеала $\mathfrak{b}$ находятся и в идеале $\mathfrak{a}$, то говорят, что $\mathfrak{b}$ *делится на* $\mathfrak{a}$, и обозначают:

$$\mathfrak{b} \equiv 0 \pmod{\mathfrak{a}}. \tag{22}$$

Если $\mathfrak{a} = (a)$, $\mathfrak{b} = (b)$ — главные идеалы, и данное кольцо имеет единичный элемент, то (22) равносильно тому, что b делится на a: $b = ar$. Поэтому делимость идеалов определяется именно так, как указано выше, а не наоборот, хотя это казалось бы естественнее с первого взгляда.

Вообще, элементы a и b из кольца называются *сравнимыми* друг с другом по идеальному модулю $\mathfrak{m}$, если $a - b$ принадлежит к идеалу $\mathfrak{m}$; обозначают:

$$a \equiv b \pmod{\mathfrak{m}}.$$

Легко проверить, что для сравнения выполнены три основных закона равенств (§ 2). Это дает возможность распределить все элементы кольца по *классам сравнимых друг с другом по модулю* $\mathfrak{m}$ *элементов*.

Если $a \equiv a_1$, $b \equiv b_1 \pmod{\mathfrak{m}}$, то легко видеть, что

$$a + b \equiv a_1 + b_1,\ ab \equiv a_1 b_1 \pmod{\mathfrak{m}}^{116}$$

Это дает возможность определить действия сложения и умножения над классами. Легко видеть, что постулаты 1–5 § 235 выполнены для этих, действий над классами. Сам идеал $\mathfrak{m}$ является одним из классов, причем этот класс играет роль нуля в действиях над классами; кроме того, для каждого класса имеется «противоположный» класс: именно если a, b, c, ... элементы данного класса, то «противоположный» класс образуется элементами $-a$, $-b$, $-c$, ... Это показывает, что совокупность этих классов составляет группу относительно сложения (или «модуль»); а отсюда уже легко следует, что и постулат 6 § 235 здесь выполнен. Таким образом рассматриваемая совокупность классов есть кольцо — так называемое «кольцо классов».

Если через $\mathfrak{N}$ обозначим данное кольцо, то рассмотренное «кольцо классов» по модулю $\mathfrak{m}$ обозначается знаком $\mathfrak{N}/\mathfrak{m}$.

Теория идеалов была разработана Дедекиндом (R. Dedekind) во второй половине XIX века как известное завершение теории делимости алгебраических чисел. Дело в том, что, желая обобщить теорию делимости обычных целых чисел на область целых алгебраических чисел в данном теле, столкнулись с непредвиденными трудностями: основная теорема об однозначности разложения целого числа на неразложимые («простые») множители оказалась неверною для целых алгебраических чисел. Дедекинд превозмог эту трудность, введя определенные системы чисел, — «идеалы», и оперируя с этими идеалами вместо чисел. Это введение идеалов увеличивает множество объектов нашего исчисления, ибо сами числа заменяются соответствующими им главными идеалами, да, кроме того, мы получаем еще бесчисленное множество «не главных» идеалов. В области идеалов алгебраических чисел верна теорема об однозначности разложения всякого идеала на «простые» идеалы.

Итак, идеалы появились в математике вначале в «конкретном» виде — как системы чисел. С созданием теории колец было обобщено и понятие идеала — как системы элементов в кольце, удовлетворяющей выше приведенным условиям 1) и 2а). В теории колец эти идеалы играют весьма важную роль.

Мы не имеем возможности подробнее останавливаться на этой теории. Желающих детально ознакомиться с ней отсылаем к книге ван-дер-Вардена, «Современная алгебра» (имеется в русском переводе том I, ГТТИ, 1934, том II, ОНТИ, 1937).

§ 244. Гиперкомплекскые числа. Пусть **P** — данная числовая область

[116] Если $a \equiv a_1$, то $a - a_1 \subset \mathfrak{m}$; но тогда (по 2а) и $(a - a_1)b = ab - a_1 b \subset \mathfrak{m}$, следовательно, $ab \equiv a_1 b$; но аналогично докажем, что $a_1 b \equiv ab$, следовательно,

$$ab \equiv a_1 b_1 \pmod{\mathfrak{m}}.$$

рациональности [117], $e_1, e_2, \ldots, e_n$ n новых символов; мы рассматриваем такие символические суммы:

$$x = x_1e_1 + x_2e_2 + \ldots + x_ne_n, \tag{23}$$

где $x_1, x_2, \ldots, x_n$ — числа из области $\mathbf{P}$. Эти выражения (23) и называются *гиперкомплексными числами* с n основными единицами $e_1, e_2, \ldots, e_n$. Конечно, мы должны еще указать, как оперировать с этими числами (23); для этого же (ср. главу I, § 3) мы должны выставить три основных постулата, определяющих равенство, сумму и произведение чисел (23). Мы даем их в следующем виде:

I. Два гиперкомплексных числа $x = x_1e_1 + x_2e_2 + \ldots + x_ne_n$ и $x' = x'_1e_1 + x'_2e_2 + \ldots + x'_ne_n$ считаются равными тогда и только тогда, если равны их соответствующие компоненты [118]:

$$x_1 = x'_1, \quad x_2 = x'_2, \ \ldots, \ x_n = x'_n.$$

II. Сумму гиперкомплексных чисел находим, складывая их соответствующие компоненты:

$$(x_1e_1 + x_2e_2 + \ldots + x_ne_n) + (y_1e_1 + y_2e_2 + \ldots + y_ne_n) =$$
$$= (x_1 + y_1)e_1 + (x_2 + y_2)e_2 + \ldots + (x_n + y_n)e_n.$$

III. Произведение гиперкомплексных чисел находим как произведение обычных сумм (согласно дистрибутивному закону), причем произведение «единиц» определяется формулами:

$$e_ie_j = \sum_{k=1}^{n} \gamma_{ijk}e_k, \qquad , i, j = 1, 2, \ldots, n, \quad \gamma_{ijk} \subset \mathbf{P}. \tag{24}$$

Кроме этого определяется еще «скалярное» произведение гиперкомплексного числа (23) на число ρ из $\mathbf{P}$ следующим образом:

$$\rho x = x\rho = \rho x_1e_1 + \rho x_2e_2 + \ldots + \rho x_ne_n. \tag{25}$$

Постулат I говорит, что «единицы» $e_1, e_2, \ldots, e_n$ линейно независимы относительно $\mathbf{P}$. Число $0 \cdot e_1 + 0 \cdot e_2 + \ldots + 0 \cdot e_n$ мы обозначим просто через 0; в операциях с гиперкомплексными числами оно играет роль нуля. Из постулата I следует, что $a_1e_1 + a_2e_2 + \ldots + a_ne_n = 0$, только если все $a_\lambda = 0$.

Из постулата II следует, что система гиперкомплексных чисел составляет (абелеву) группу относительно сложения. Из постулатов II и III легко получаем, что для сложения и умножения верен дистрибутивный закон; из постулата II и (25) следует, что дистрибутивный закон верен и для скалярного умножения со сложением.

Если мы условимся обозначать:

$$0 \cdot e_1 + \ldots + 0 \cdot e_{\lambda-1} + a_\lambda e_\lambda + 0 \cdot e_{\lambda+1} + \ldots + 0 \cdot e_n = a_\lambda e_\lambda,$$

то символическую сумму (23) можно рассматривать (согласно постулату II) как действительную сумму гиперкомплексных чисел $x_1e_1, x_2e_2, \ldots, x_ne_n$.

[117] В новое время имеются и обобщения, когда за $\mathbf{P}$ берется абстрактное тело или даже кольцо; но мы этих обобщений касаться не будем.

[118] Можно пользоваться геометрическим языком, представляя гиперкомплексное число (23) как вектор в n-мерном пространстве с компонентами $x_1, x_2, \ldots, x_n$ (если тело $\mathbf{P}$ действительное).

В зависимости от значений коэфициентов γ_{ijk} в (24) для умножения гиперкомплексных чисел могут быть верны те или иные законы.

Система всех чисел вида (23) (где $x_1, x_2, \ldots, x_n$ пробегают независимо друг от друга значения всех чисел из $\mathbf{P}$) при выполнении постулатов I–III и (25) и при данных коэфициентах γ_{ijk} в (24) называется *системою гиперкомплексных чисел* или *линейною алгеброй*.

Особенно важен случай, когда в линейной алгебре умножение ассоциативно; легко видеть, что для этого необходимо и достаточно, чтобы ассоциативный закон был верен для произведений единиц. Мы имеем [по (24)]:

$$(e_i e_j)e_k = \sum_{r,s=1}^{n} \gamma_{ijr}\gamma_{rks}e_s,$$

$$e_i(e_j e_k) = \sum_{r,s=1}^{n} \gamma_{jkr}\gamma_{irs}e_s,$$

если $(e_i e_j)e_k = e_i(e_j e_k)$, то (по постулату I) должно быть:

$$\sum_{r=1}^{n} \gamma_{ijr}\gamma_{rks} = \sum_{r=1}^{n} \gamma_{jkr}\gamma_{irs} \qquad (i, j, k, s = 1, 2, \ldots). \tag{26}$$

Коммутативный закон для умножения будет верен тоже тогда и только тогда, если он окажется верным для «единиц»; (24) дает для этого условие:

$$\gamma_{ijk} = \gamma_{jik} \qquad (i, j, k = 1, 2, \ldots, n). \tag{27}$$

Может возникнуть вопрос: какое понятие следует считать более общим: линейной алгебры или кольца? Но дело в том, что не всякая линейная алгебра есть кольцо и не всякое кольцо — линейная алгебра, так что эти два понятия являются обобщениями понятия тела, ведущими в разные стороны. Можно сказать только, что всякая ассоциативная алгебра есть частный случай кольца (вообще — некоммутативного).

Рассмотрим теперь вопрос о возможности деления, т. е. действий, обратных умножению, в нашей линейной алгебре. Пусть

$$a = \sum_{\varkappa=1}^{n} a_\varkappa e_\varkappa, \qquad b = \sum_{\mu=1}^{n} b_\mu e_\mu$$

два данных гиперкомплексных числа; посмотрим, разрешимы ли уравнения:

$$ax = b, \qquad ya = b. \tag{28}$$

Разрешимость первого из уравнений (28) есть возможность *левого деления на* a, разрешимость второго уравнения (28) — возможность *правого деления на* a. Пусть

$$x = \sum_{\lambda=1}^{n} x_\lambda e_\lambda, \qquad y = \sum_{\lambda=1}^{n} y_\lambda e_\lambda;$$

подставляя это в (28), найдем по постулату III и (24):

$$\sum_{\mu=1}^{n} e_\mu \left(\sum_{\lambda=1}^{n} x_\lambda \sum_{\varkappa=1}^{n} a_\varkappa \gamma_{\varkappa\lambda\mu} \right) = \sum_{\mu=1}^{n} b_\mu e_\mu,$$

$$\sum_{\mu=1}^{n} e_\mu \left(\sum_{\lambda=1}^{n} y_\lambda \sum_{\varkappa=1}^{n} a_\varkappa \gamma_{\lambda\varkappa\mu} \right) = \sum_{\mu=1}^{n} b_\mu e_\mu.$$

Отсюда же по постулату I:

$$\sum_{\lambda=1}^{n} x_\lambda \sum_{\varkappa=1}^{n} a_\varkappa \gamma_{\varkappa\lambda\mu} = b_\mu \qquad (\mu = 1, 2, \ldots, n), \tag{29}$$

$$\sum_{\lambda=1}^{n} y_\lambda \sum_{\varkappa=1}^{n} a_\varkappa \gamma_{\lambda\varkappa\mu} = b_\mu \qquad (\mu = 1, 2, \ldots, n). \tag{29}$$

Формула (29) выражает систему n линейных уравнений (в $\mathbf{P}$) с n неизвестными $x_1, x_2, \ldots, x_n$; (29a) подобная же система с неизвестными $y_1, y_2, \ldots, y_n$. При $b \neq 0$ система (29) имеет одну и только одну систему решений $x_1, x_2, \ldots, x_n$, если только детерминант

$$\Delta(x) = \left| \sum_{\varkappa=1}^{n} a_\varkappa \gamma_{\varkappa\lambda\mu} \right| \qquad (\lambda, \mu = 1, 2, \ldots, n) \tag{30}$$

не равен нулю; точно так же система (29a) имеет одну и только одну систему решений, если детерминант

$$\Delta'(x) = \left| \sum_{\varkappa=1}^{n} a_\varkappa \gamma_{\lambda\varkappa\mu} \right| \qquad (\lambda, \mu = 1, 2, \ldots, n) \tag{30}$$

отличен от нуля.

Если же $\Delta(x) = 0$, то (§ 41) уравнение $ax = 0$ имеет решение $x \neq 0$; если при этом $a \neq 0$, то a — *левый нулевой делитель*.

Точно так же при $\Delta'(x) = 0$, a есть *правый нулевой делитель*.

Может случиться, что данная линейная алгебра имеет *главную единицу*, т. е. такое число $\varepsilon = \varepsilon_1 e_1 + \varepsilon_2 e_2 + \ldots + \varepsilon_n e_n$, что для всякого числа x из этой алгебры

$$x\varepsilon = \varepsilon x = x. \tag{31}$$

Заметим, что, главная единица, если она существует, — единственная в данной алгебре: если ε и ε' две главных единицы, то непосредственно получаем $\varepsilon\varepsilon' = \varepsilon$и $\varepsilon\varepsilon' = \varepsilon'$; т. е. $\varepsilon = \varepsilon'$.

Формула (31) дает при $x = e_i$:

$$e_i\varepsilon = \varepsilon e_i = e_i,$$

а это дает:

$$\sum_{\nu=1}^{n} \varepsilon_\varkappa \gamma_{\varkappa\lambda\mu} = \sum_{\varkappa=1}^{n} \varepsilon_\varkappa \gamma_{\lambda\varkappa\mu} = e_{\lambda\mu}, \quad \text{где} \quad e_{\lambda\mu} = \begin{cases} 1 & \text{при} \quad \lambda = \mu, \\ 0 & \text{при} \quad \lambda \neq \mu. \end{cases}$$

Отсюда

$$\Delta(\varepsilon) = \Delta'(\varepsilon) = 1,$$

т. е. ни $\Delta(x)$, ни $\Delta'(x)$ не равны нулю тождественно (относительно $x_1, x_2, \ldots, x_n$).

Докажем, что в линейной *ассоциативной* алгебре (т. е. в такой, где для умножения верен ассоциативный закон) условие, что $\Delta(x)$ и $\Delta'(x)$ не равны тождественно нулю, достаточно для наличия в этой алгебре главной единицы.

Действительно, ведь $\Delta(x)$ и $\Delta'(x)$ — ц. р. функции от $x_1, x_2, \ldots, x_n$ в $\mathbf{P}$; по лемме § 214 можно дать для $x_1, x_2, \ldots, x_n$ такие ц. р. (а, следовательно, принадлежащие к области $\mathbf{P}$) значения $u_1, u_2, \ldots, u_n$, при которых оба детерминанта $\Delta(u)$ и $\Delta'(u)$, где $u = u_1e_1 + u_2e_2 + \ldots + u_ne_n$, будут отличны от нуля. В таком случае уравнения $u\varepsilon = u$ и $zu = x$, где x — любое гиперкомплексное число из нашей алгебры, — всегда имеют решения ε и z. Теперь имеем (применяя ассоциативный закон):

$$x\varepsilon = (zu)\varepsilon = z(u\varepsilon) = zu = x, \qquad u(\varepsilon x) = (u\varepsilon)x = ux;$$

но если $ux = v$, то x — единственное решение этого уравнения; следовательно, из $u(\varepsilon x) = ux$ заключаем: $\varepsilon x = x$, т. е.

$$x\varepsilon = \varepsilon x = x$$

для всякого числа x нашей алгебры, т. е. ε — главная единица.

В такой алгебре для всякого числа x при $\Delta(x) \neq 0$ существует единственное обратное число x^{-1} — такое, что

$$xx^{-1} = \varepsilon,$$

но тогда

$$x(x^{-1}x - \varepsilon) = \varepsilon x - x\varepsilon = 0,$$

и, следовательно, так как $\Delta(x) \neq 0$, т. е. x не является левым нулевым делителем, то

$$x^{-1}x - \varepsilon = 0, \qquad x^{-1}x = \varepsilon.$$

Обратно, если $x'x = \varepsilon$, то, умножая обе части этого равенства справа на x^{-1}, найдем:

$$(x'x)x^{-1} = \varepsilon x^{-1} \quad \text{или} \quad x'(xx^{-1}) = \varepsilon x^{-1}, \qquad x' = x^{-1}.$$

Таким образом это обратное число x^{-1} одновременно и правое, и левое, и притом — единственное; а это влечет за собою, что $\Delta'(x) \neq 0$.

Итак, *в линейной ассоциативной алгебре для данного числа x оба детерминанта $\Delta(x)$ и $\Delta'(x)$ или одновременно равны нулю, или одновременно отличны от нуля.*

Для данной алгебры основные единицы $e_1, e_2, \ldots, e_n$ определены не однозначно; возьмем n чисел:

$$E_i = \sum_{j=1}^{n} c_{ij}e_j \qquad (i = 1, 2, \ldots, n), \tag{32}$$

где c_{ij} — числа из области $\mathbf{P}$, причем детерминант $|c_{ij}| \neq 0$. Тогда уравнения (32) однозначно разрешимы относительно $e_1, e_2, \ldots, e_n$:

$$e_i = \sum_{j=1}^{n} d_{ij} E_j \qquad (i = 1, 2, \ldots, n), \tag{32}$$

и детерминант $|d_{ij}| \neq 0$.

Из (32) и (32а) видно, что всякая линейная в теле $\mathbf{P}$ функция от $e_1, e_2, \ldots, e_n$ выражается линейно (в теле $\mathbf{P}$) через $E_1, E_2, \ldots, E_n$, и обратно, т. е. вместо $e_1, e_2, \ldots, e_n$ можно взять за основные единицы $E_1, E_2, \ldots, E_n$. В частности найдем

$$E_i E_j = \sum_{k=1}^{n} \Gamma_{ijk} E_k, \quad \text{где} \quad \Gamma_{ijk} = \sum_{\varkappa,\lambda,\mu=1}^{n} c_{i\varkappa} c_{j\lambda} \gamma_{\varkappa\lambda\mu} d_{\mu k}.$$

Получаемая, таким образом, линейная алгебра с основными единицами $E_1, E_2, \ldots, E_n$ называется *эквивалентной* предыдущей.

§ 245. Матричные алгебры. Теория матриц является источником линейных ассоциативных алгебр. Пусть, например,

$$E_1, E_2, \ldots, E_n$$

матрицы m-го порядка с элементами из данного тела $\mathbf{P}$, подобранные так, что все произведения $E_\alpha E_\beta$ выражаются линейно через

$$E_1, E_2, \ldots, E_n$$

в теле $\mathbf{P}$:

$$E_\alpha E_\beta = \sum_{\lambda=1}^{n} \gamma_{\alpha\beta\lambda} E_\lambda,$$

где $\gamma_{\alpha\beta\lambda}$ — числа из тела $\mathbf{P}$; тогда все матрицы вида $\sum_{\lambda=1}^{n} a_\lambda E_\lambda$„ где a_λ — числа из $\mathbf{P}$, составляют линейную ассоциативную алгебру.

Пример. Возьмем две такие матрицы 2-го порядка: $E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ и $I = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Имеем: $I^2 = -E$, $E^2 = E$, $EI = IE = I$. Следовательно, матрицы вида

$$A = aE + bI = \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

при любых действительных числах a, b составляют линейную ассоциативную алгебру. В данном случае $\gamma_{111} = \gamma_{122} = \gamma_{212} = 1$, $\gamma_{112} = \gamma_{121} = \gamma_{211} = \gamma_{222} = 0$; отсюда легко найдем:

$$\Delta(A) = \Delta'(A) = |A| = \begin{vmatrix} a & -b \\ b & a \end{vmatrix} = a^2 + b^2.$$

Это обращается в нуль только при $a = b = 0$. Таким образом рассматриваемая алгебра совсем не имеет нулевых делителей. Далее, как легко проверить:

$$(aE + bI)(cE + dI) = (ac - bd)E + (bc + ad)I.$$

Эта формула показывает, что для произведения рассматриваемых матриц верен и коммутативный закон. Легко видеть, что рассматриваемая алгебра изоморфна алгебре обычных комплексных чисел.

Возвращаясь к общим исследованиям, заметим, что совокупность всех матриц данного m-то порядка в любом данном теле $\mathbf{P}$ составляет линейную (конечно, ассоциативную) алгебру с m^2 основными единицами. Действительно, обозначим через $E_{\alpha\beta}$ матрицу m-го порядка, у которой элемент, стоящий на пересечении α-й строки и β-го столбца, равен единице, а остальные элементы все равны нулю. Тогда для любой матрицы m-го порядка (с элементами из $\mathbf{P}$) имеем:

$$\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1m} \\ a_{21} & a_{22} & \dots & a_{2m} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mm} \end{pmatrix} = \sum_{\alpha,\beta=1}^{n} a_{\alpha\beta} E_{\alpha\beta}.$$

Это можно рассматривать как гиперкомплексное число с основными единицами $E_{\alpha\beta}$.

Существует такая теорема: *всякая линейная ассоциативная алгебра в теле* $\mathbf{P}$ *может быть представлена как алгебра матриц в том же теле* $\mathbf{P}$ [119].

§ 246. Кватернионы. Система действительных кватернионов, введенная Гамильтоном (W. R. Hamilton) в 1843 г., является первой по времени системой гиперкомплексных чисел. Кватернионы — гиперкомплексные числа с четырьмя основными единицами, обозначаемыми обычно через 1, i, j, k, со следующей таблицей умножения:

	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

Таким образом общий вид кватерниона: $p = d + ai + bj + ck$, где вещественны a, b, c, d. Можно вычислить, что здесь

$$\Delta(p) = \Delta'(p) = (a^2 + b^2 + c^2 + d^2)^2,$$

откуда видно, что $\Delta(p) = \Delta'(p) = 0$ только при $a = b = c = d = 0$, т. е. при $p = 0$. Таким образом и в системе действительных кватернионов нет нулевых делителей. Имеем, далее:

$$\begin{aligned}(d + ai + bj + ck)(w + xi + yj + zk) &= (dw - ax - by - cz) + \\ &+ (aw + dx + bz - cy)i + (bw + dy + cx - az)j + \\ &+ (cw + dz + ay - bx)k.\end{aligned}$$

Отсюда видно, что для умножения кватернионов неверен коммутативный закон; но ассоциативный закон верен, как легко проверить на произведениях единиц.

[119] Доказательство этой теоремы читатель может найти в книге Dickson'a: «Algebren und ihre Zahlentheorie» (Zürich u. Leipzig 1927), стр. 33.

Величина $T = \sqrt{a^2+b^2+c^2+d^2}$ (где берется положительное значение корня) играет большую роль в теории кватернионов; она называется «абсолютной величиной» или «тензором» кватерниона.

Кватернион $\overline{p} = d - ai - bj - ck$ называется *сопряженным* с p; можно легко проверить, что $p\overline{p} = \overline{p}p = T^2 = a^2+b^2+c^2+d^2$. Отсюда

$$p^{-1} = \frac{1}{p} = \frac{\overline{p}}{T^2}, \qquad pp^{-1} = p^{-1}p = 1.$$

Теперь мы имеем возможность решить уравнения:

$$px = q \quad \text{и} \quad yp = q$$

при данных кватернионах p и q (причем $p \neq 0$) и искомом x. Найдем:

$$x = p^{-1}q = \frac{\overline{p}q}{T^2}, \qquad y = qp^{-1} = \frac{q\overline{p}}{T^2}.$$

В кватернионе $p = d + ai + bj + ck$ часть d называется *скалярной* частью, а $ai + bj + ck$ — *векторной* частью; именно, мы можем рассматривать a, b, c как составляющие вектора в трехмерном пространстве. Возьмем произведение двух кватернионов со скалярными частями, равными нулю:

$$\begin{aligned}(ai+bj+ck)(xi+yi+zk) &= -(ax+by+cz) + (bz-cy)i + \\ &\quad +(cx-az)j + (ay-bx)k.\end{aligned}$$

Взятая с обратным знаком скалярная часть произведения $ax+by+cz$ есть не что иное, как так называемое «скалярное произведение» векторов (a,b,c) и (x,y,z); коэфициенты же $bz-cy$, $cx-az$, $ay-bx$ суть составляющие так называемого «векторного произведения» тех же векторов.

Есть еще одна геометрическая интерпретация кватернионов, как векторов в четырехмерном пространстве.

Как всякая ассоциативная линейная алгебра, и алгебра действительных кватернионов может быть интерпретирована, как алгебра матриц. Эту интерпретацию мы получим, положив:

$$E = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad I = \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \quad J = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix},$$

$$K = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

Алгебра матриц вида $dE + aI + bJ + cK$ изоморфна алгебре кватернионов $d + ai + bj + ck$.

Можно представить алгебру кватернионов и как алгебру матриц 2-го порядка, но только с комплексными элементами; для этого следует взять:

$$E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad I = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad J = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}, \quad K = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix},$$

где $i = \sqrt{-1}$.

Предлагается читателю построить.таблицу умножения матриц E, I, J, K (в обоих случаях) и выяснить, что эта таблица — та же самая, что и приведенная выше таблица умножения для «единиц» 1, i, j, k.

ЛИТЕРАТУРА ПО ВЫСШЕЙ АЛГЕБРЕ

Б. Я. Букреев, Элементы алгебраического анализа, Киев 1912.

М. Е. Ващенко-Захарченко, Алгебраический анализ или высшая алгебра, Киев 1887.

М. Е. Ващенко-Захарченко, Теория определителей и теория форм, Киев 1877. [К главам II, IX.]

М. Е. Ващенко-Захарченко, Высшая алгебра. Теория подстановленпй и приложение ее к алгебраическим уравнениям, Киев 1890. [К главам XI, XII.]

Д. А. Граве, Элементы высшей алгебры, Киев 1914.

Д. А. Граве, Теория конечных групп, Киев 1908, [К главе XI.]

А. М. Журавский, Сборник задач по высшей алгебре, ОНТИ, Москва 1933.

В. Ф. Каган, Основания теории определителей, Госиздат Украины, 1922. [К главам II, IX.]

Н. И. Лобачевский, Алгебра (1846 г.).

Б. К. Млодзеевский, Основы высшей алгебры, ГИЗ, 1923.

Б. К. Млодзеевский, Решение численных уравнений, ГИЗ, 1924. [К главе V.]

М. В. Остроградский, Лекции алгебраического и трансцендентного анализа, Спб. 1837. [К главе V.]

Ю. В. Сохоцкий, Высшая алгебра, часть первая, Спб. 1882.

Ю. В. Сохоцкий, Высшая алгебра, изд. III, Спб. 1911 (литогр. курс).

А. К. Сушкевич, Лекции по теории конечных групп, сост. доц. Брянским под ред. автора (стеклограф.), Днепропетровск 1931. [К главе XI.]

М. Тихомандрицкий, Краткий курс высшей алгебры, Харьков 1887.

Тодгентер, Начальная теория уравнений, изд. Войтинского, Спб. 1890.

Н. Г. Чеботарев, Основы теории Галуа, ч. 1, ГТТИ 1934. [К главам XI, XII, XIII.]

Г. М. Шапиро, Высшая алгебра, Москва 1935.

С. О. Шатуновский, Алгебра как учение о сравнениях по функциональным модулям, Одесса. [К главе XIV.]

О. Ю. Шмидт, Абстрактная теория групп, Киев 1916; 2-е издание ГТТИ, 1923. [К главе XI.]

А. Шульце, Графічна алгебра, за ред. В. Б. Фурсенка, ОНТВУ, 1933 [К главе V.]

P. Bachmann, Die Lehre von der Kreisteilung, Lpz. 1872. [К главе XIII.]

P. Baltzer, Theorie und Anwendimg der Determinanten, 4-е изд., Lpz. 1875. [К главе II.]

L. Baumgartner, Grupperitheorie, Berl. u. Lpz. 1921; есть русский перевод под ред. Чунихина: Теория групп, ГТТИ, 1934. [К главе XI.]

L. Bianchi, Lezioni sulla teoria dei gruppi di sostituzioni e delle equazioni algebriche secondo Galois, Pisa 1900. [К главам XI, XII.]
Bieberbach-Bauer, Vorlesungen über Algebra, 1928.
M. Bôcher, Einführung in die höhere Algebra, 2-е изд. 1925; есть русский перевод под ред. А. Г. Куроша: Введение в высшую алгебру, ГТТИ, 1933. [К главам II, VIII, IX, X.]
Borel et Drach, Introduction à *l*'etude de *l*a théorie des nombres et de *l*'aigebre supérieure, Paris 1895.
Burnside, Theory of groups of finite order, 2-е изд., Cambridge 1911. [К главе XI.]
Burnside and Panton, The theory of equations, Vol. I and II, 1899, 1901.
F. Cajori, An introduction to the modern theory of equations, New York 1904.
J. Carnoy, Cours d'algèbre supérieure, Louvin – Paris 1892.
L. E. Dickson, Linear Algebras, Cambridge 1914; есть русский перевод: Л. Е. Диксон, Линейные алгебры, Харьков ОНТВУ, 1935. [К главе XIV.]
L. E. Dickson, Algebren und ihre Zahlentheorie, Zurich u. Lpz. 1927. [К главе XIV.]
L. E. Dickson, Höhere Algebra, Hrsg. v. Bodewig, 1929. [К главам IX, X, XI, XII.]
R. Fricke, Lehrbuch der Algebra, Bd. I (1924), II (1926), III (1928).
P. Gordan, Vorlesungen über Invariantentheorie, Hrsg. v. Kerschensteiner, Bd. I, u. II, Lpz. 1885, 1887. [К главе X.]
J. H. Grace and A. Young, The Algebra of Invariants, Cambridge 1903 [К главе X.]
Hasse, Höhere Algebra, Bd. I u. II, 1927 (Samml. Göschen).
Haupt. Einführung in die Algebra, Bd. I u. II, Lpz. 1929. [К главам XI, XII, XIV.]
A. Hilton, An introduction to the theory of groups of finite order, Oxford 1908. [К главе XI.]
H. Hilton, Homogeneous *l*inear substitutions, Oxford 1914. [К главам IX, X.]
G. Jordan, Traité des substitutions et des équations algébriques, Paris 1870. [К главам XI, XII, XIII.]
G. Kowalewski, Einführung in die Determinantentheorie, Lpz. 1909. [К главе II.]
L. Kronecker, Vorlesungen über die Theorie der Determinanten, bearb. v. K. Hensel, Bd. I, Lpz. 1903. [К главам II, IX.]
A. Loewy, Lehrbuch der Algebra, I Teil, Lpz. 1915.
G. B. Mathews, Algebraic equations, 2-е изд., 1915. [К главам XII, XIII.]
L. Matthiessen, Grundzüge der antiken und modernen Algebra der *l*itteralen Gleichungen, 2-е изд., Lpz. 1896. [К главе VII.]
W. Fr. Meyer, Allgemeine Formen und Invariantentheorie, Bd. I, Lpz. 1909. [К гл. X.]
G. A. Miller, H. F. Blichfeldt, L. E. Dickson, Theorie and applications of finite groups, New York 1916. [К главе XI.]
E. Netto, Vorlesungen über Algebra, Bd. I u. II, Lpz. 1896, 1900.
E. Netto, Substitutionentheorie und ihre Anwendung auf die Algebra, Lpz. 1882. [К главам XI, XII, XIII.]
E. Netto, Gruppen und Substitutionentheorie, Lpz. 1908. [К гл. XI.]
E. Netto, Elementare Algebra. Lpz. u. Berlin 1913.
F. Pascal, Die Determinanten, Lpz. 1900. [К главе II.]
O. Perron, Algebra, Bd. I u. II, 1927.
S. Pincherle, Lezioni di algebra compiementare, Parte I, II, Boiogna.

K. Runge. Praxis der Gleichungen, 2-е изд., 1921. [К главе V.]
G. Salmon, Vorlesungen über die Algebra der *l*inearen Transformation. Deutsch v. Fiedler, 2-е изд., 1877. [К главе X.]
de Léguier, Elements de *l*a thèorie des groupes abstraits, Paris 1904. [К главе XI.]
de Léguier, Elements de *l*a théorie des groupes de substitutions, Paris 1912. [К главе XI.]
O. Schreier und E. Sperner, Einführung in die analitische Geometrie und Algebra, Bd. I, Lpz. 1931; есть русский перевод под заглавием: «Введение в линейную алгебру в геометрическом изложении», ОНТИ, 1934 [К главам II, IV, XII.]
J. A. Serret, Cours d'algèbre supérieure, T. I et II, Paris 1866.
A. Speiser, Theorie der Gruppen von endlicher Ordnung, Berlin 1923. [К главе XI.]
H. Voght, Leçons sur *l*a résolution algébrique des équations, Paris 1895 [К гл. XII, XIII.]
B. L. van der Waerden, Moderne Algebra, T. I u. II, 1930–931; есть русский перевод I части: «Современная алгебра», ГТТИ, 1934. [К гл. XIV.]
H. Weber, Lehrbuch der Algebra, Bd. I, II, III, 2-е изд., 1898, 1899, 1908.

Редакция И. Я. Акушского. Оформление Н. Я. Костиной
Корректура З. Л. Соколиной и Р. Ф. Шаровой.

Сдано в производство 28/I 1937 г. Подписано в печать 26/V 1937 г.
Печ. л. 29 3/4. Бум. л. 14 5/8. Уч. а. л. 38,75. Формат 62 × 94 1/16. Кол. тип. знак, в 1 бум. л. 51.000.
Уч. № 4506. Гл. ред. техн.-теорет. лит. № 2. Тираж 7.000. Уполном. Главл. № Б 13837. Зак. № 1593.

2-я тип. ОНТИ им. Евг. Соколовой. Ленинград, пр. Кр. Командиров, 29.