Дмитрий Граве

Ординарный Профессор Императорскаго Университета Св. Владимира

ЭЛЕМЕНТЫ
ВЫСШЕЙ АЛГЕБРЫ

КИЕВ

Типография Императорского Университета св. Владимира
Акц. О-ва печати, и изд. дела Н. Т. Корчак-Новицкаго, Меринговская, 6.
1914

Предисловие

Уже давно, преподавая высшую алгебру в Университете Св. Владимира по обычной для русских университетов программе общего курса этого предмета, я ощущал известную неловкость, состоявшую как бы в сознании того, что я действовал не согласно с моими внутренними убеждениями. В самом деле, если отнести к курсу введения в анализ многие отделы, часто излагаемые в учебниках высшей алгебры, какъ то: определители, разложение рациональных дробей на простейшие, числа комплексные и т. д., то остается обычный конгломерат теорем и свойств, относящихся к целым функциям большею частью от одного переменного независимого, теорем быть может интересных и даже иногда важных, но не связанных никакою объединяющею мыслью, а главное, не имеющих никакого определенного raison d'être и приложений. Говорится, например, о пределах корней, о задаче отделения корней, как будто главною целью курса является приближенное решение уравнений, однако всем известно в настоящее время, что лучшим в практическом отношении способом приближенного решения уравнений является способ Gräffe, не требующий абсолютно предварительнаго отделения корней. Среди этих излагаемых по известной рутине теорем сиротливо высится колосс — теорема Sturm'a. Но и тут изложение часто придается такой характер, как будто главное значение теоремы Sturm'a состоит в ее приложении к отделению корней.

Меня уже давно мучила мысль, что обычная программа курса высшей алгебры есть не то, что нужно излагать, а что главное дело состоит как раз в том, что не излагается, т. е. в теории групп, теории подстановок, теории Galois и т. п.

Что, в самом деле, должен говорить профессор, выходящий из аудитории и слышащий вопрос студента: «Вы говорили, что буквенный уравнения выше 4-ой степени не решаются в радикалах, а как это доказать?».

Я пробовал различным образом уклоняться от ответа на этот вопрос. Сначала я говорил, что радикал есть знак неудачный, а потому и теория решений уравнений при помощи этого знака есть теория, не имеющая практического значения. Я чувствовал при этом, конечно, что обычный способ разговора двух математиков, когда один критикует предмет, которым занимается другой, совершенно недопустим между профессором и учениками. Да кроме того, профессору трудно будет защитить свою точку зрения, ибо студент ни за что не поверит, что теория, которой занимались Lagrange, Gauss, Abel и Galois, теория, незаслуживающая внимания.

Затем наступил период, когда, я стал давать обычные, так называемые краткие, доказательства теоремы Abel'a о невозможности алгебраическаго решения уравнений выше 4-ой степени. Сознавая неубедительность этих доказательств, я готов был презирать себя за недобросовестность. Наконец, я поставил себе ребром вопрос, почему я не желаю излагать как следует теорию Galois? Я не видел другого объяснения, кроме дурной привычки и рутины. Все говорило за введение

теории Galois в элементарный курс высшей алгебры: и абсолютная необходимость основ теории групп для приличного преподавания чистой математики, и достаточная разработанность теории Galois, позволяющая простое и ясное изложение, и важность этой теории для высших частей алгебры, где этот предмет сливается с теорией чисел в гармоническое целое. Таким образом я излагаю последние несколько лет теорию Galois в общем курсе высшей алгебры.

Издание этой книги, уже давно задуманное, было отложено на несколько лет в ожидании появления малого издания алгебры H. Weber'a. Судя по доходившим до меня сведениям о программе и характере этого издания, я думал в нем найти как раз то, что по моему мнению необходимо для русских университетов. Я думал, что можно будет взять это сокращенное издание, как нормальный учебник, стоящий на высоте современного положения предмета.

Появившаяся книга H. Weber'a разочаровала меня в сильной степени.

Оказалось, что в теории алгебраическаго решения уравнений Weber ограничивается только уравнениями простой степени. Остались недосказанными буквально лишь несколько слов, между тем, как ряд важных результатов остался за бортом. Так, например, я считаю совершенно классическою теорему Abel'a – Galois об импримитивности разрешимого уравнения, в степень которого входят два различных простых числа. Эта теорема в книге не рассматривается.

Затем разочаровали меня самые сокращения по сравнению с большим изданием. Можно судить, на сколько эти сокращения удачны, хотя бы по тому факту, что в одном месте желание сократить доказательство привело к грубой ошибке (стр. 215, три верхние строки).

Благоговея перед памятью знаменитого автора, которого я всегда себе ставил образцом для подражания, я отношу ответственность за эту ошибку на трех молодых ученых, которые, судя по предисловие, принимали деятельное участие в чтении корректур.

Итак, я вернулся опять к мысли издать собственный курс алгебры. План книги и все детали ее выполнения были у меня давно уже готовы, поэтому приведете моей мысли в исполнени не встретило затруднения и не потребовало много времени.

Считаю необходимым более подробно познакомить читателя с наиболее характерными особенностями моего изложения.

Первые четыре главы книги заключают, так сказать, азбуку алгебры.

Первый серьезный вопрос трактуется в пятой главе, посвященной теории подстановок. Будучи убежденным сторонником возможно раннего введения в университетское преподавание основ общей теории групп, я начинаю главу с подробно разобранного определения понятия о группе.

Чтобы еще более подчеркнуть мою мысль, я сделал первые три параграфа главы, заключающее определение понятия группы, точным воспроизведением такого же изложения из моей книги «Элементарный курс теории чиселъ».

Переходя далее к рассмотрению конкретных групп подстановок, я отсылаю читателя, желающаго познакомиться с теорией абстрактных групп, к книге моего многоуважаемого ученика О. Ю. Шмидта, под заглавием «Абстрактная теория группъ», удостоенной физико-математическим факультетом Университета Св. Владимира премии Рахманинова.

Я прошу читателя обратить особенное внимание в этой главе на теоремы о

том, что при $n > 4$ знакопеременная группа простая и что симметрическая группа не имеет других инвариантных подгрупп, кроме знакопеременной.

Из конца книги читатель увидит, что в этих теоремах заключается полное доказательство теоремы о невозможности алгебраическаго решения буквенных уравнений выше 4-ой степени.

Глава шестая заключает изложение элементарных свойств инвариантов. Между прочим я обращаю внимание на очень важный вопрос нахождения конечных групп ортогональных линейных преобразований многомерного пространства. Этот вопрос служил предметом занятий моего семинара по алгебре в осеннем семестре 1913 года. В этом семинаре принимали участие наиболее сильные из моих учеников и мы догадались, что, начиная с пяти измерений, дело исчерпывается группами, которыя я в тексте обозначаю символами Y и Y'. Нам не удалось однако доказать справедливости найденного но интуиции решения.

Далее я прошу читателя обратить внимание на главу восьмую, в которой излагаются свойства целых функций, от миогих переменных независимых. Центром тяжести этой главы является доказательство теоремы о единственности разложения целых функций на неприводимые множители в связи с приложешем Эвклидова алгоритма нахождения общего паибольшего делителя при помощи последовательного деления. Как известно, эта теорема служит основанием всей Kronecker'овской арифметической теории алгебраических величин.

Одиннадцатая глава содержит изложение теоремы Sturm'a.

Доказав теорему Sturm'a и пояснив её на примерах, я обращаюсь к связи теоремы Sturm'a с непрерывными дробями. Я начинаю с замечательных исследований академика А. Маркова. Из формул Маркова я получаю формулы Sylvester'a, а уже отсюда прихожу к исследованиям Hermite'a, указавшим связь с квадратичными формами. Переходя далее к отделению мнимых корней, я излагаю замечательную теорию индексов Cauchy, которая в свою очередь переходить в более широкую теорию характеристик Kronecker'a. Я заканчиваю главу приложением характеристик к доказательствам теоремы Hurwitz'a об уравнениях, все корни которых имеют отрицательные вещественные части. Здесь я должен упомянуть кстати, что в первом томе второго издания алгебры Weber'a находится § 99 под заглавием «Formulierung der Aufgabe durch Hurwitz»; в той части этого параграфа, где дело идет о связи с квадратичными формами, я ничего не вижу выходящаго из круга идей и результатов Hermite'a, теоремы же 3 и 4 вытекают из теории Маркова, как частные случаи.

Двенадцатая глава трактует о приближенном вычислении корней. Отсылая к кииге проф. А. Н. Крылова «Лекции о приближенном вычислении» лиц, желающих научиться вычислять с удобством по семизначным логарифмам как вещественные, так и мнимые корни уравнений по способу Gräffe, я излагаю классические приемы приближенного вычисления главным образом вещественных корней. Излагая способ Gauss'a вычисления корней трехчленных уравнений, я показываю мой способ вычисления вещественных корней подобных уравнений при помощи алгоритма, представляющего некоторое обобщение алгоритма непрерывных дробей.

Тринадцатая глава посвящена двухчленным уравнениям.

Изложив подробно свойства первообразных корней, я даю большое число разнообразных приемов доказательства неприводимости уравнения, которым удовле-

творяют только первообразные корни. Попутно я подчеркиваю очень важное понятие о взаимной приводимости уравнений.

Начиная с четырнадцатой главы весь конец книги заключает мое изложение теории Galois.

Глава четырнадцатая посвящена общей теории полей (Körper). Эта глава представляет почти полную копию с подобной же главы моей книги «Элементарный курс теории чисел». В ней я делаю существенное добавление, принадлежащее Steinitz'у и которого не было в упомянутой моей книге, а именно, что в полях с отличной от нуля характеристикой неприводимый функции могут иметь кратные корни. Однако это добавление в настоящей книге не получает приложения, ибо я в ней рассматриваю исключительно поля с характеристикой нуль.

Переходя к следующим главам, я должен обратить внимание читателя на то, почему я видоизменил изложение теории Galois, встречающееся у моих предшественников.

Я оставлю в стороне критику изложения теории Galois, данного авторами, у которых изложение имеет такой характер, что можно с большой вероятностью предполагать, что сам автор не достаточно понимает излагаемого предмета.

Но даже правильные изложения предмета, из которых одним из лучших является изложение Weber'a, грешат по моему мнению в смысле строгости, простоты и ясности.

Не строгим является такой способ изложения. Рассматриваются сначала численные уравнения, коэффициенты которых суть определенный числа, принадлежащая к некоторому заданному числовому полю; а далее без особенных обоснований предполагается, что теория, получаемая для численных уравнений, годится также для буквенных уравнений, когда все корни, а, значить, и все коэффициенты переменные независимый величины. Предполагается также, что теория сохраняет свою силу для случая промежуточного, случая алгебраических функций от одного или нескольких, переменных независимых.

Если изложение Weber'a и возможно защитит от упрека в нестрогости, то придется сделать такое большое число подстрочных примечаний и оговорок, для защиты читателя от неправильного понимания излагаемого, что во всяком случае остается признать изложение не достаточно ясным.

Что касается отсутствия простоты у моих предшественников, то достаточно сослаться хотя бы на второй том Weber'a, где при изучении уравнений сложной степени в полном ходу теорема Jordan'a о ряде индексов данной группы, между тем как для тех же самых целей, с которыми Weber употребляете теорему Jordan'a, никакой надобности в этой теореме нет.

Читатель увидит в моей книге, что достаточно доказать такую простую теорему: *всякая разрешимая группа имеет отличного от единицы коммутативного нормального делителя.* Из этой теоремы сразу получается все, что нужно для элементарного изложения.

Я уже не упоминаю о том, что существует целый ряд более мелких пунктов, где рассуждения моих предшественников не достаточно просты. Например, когда при переходе к линейным группам доказывают, что подстановки можно представить аналитически системами сравнений по простому модулю, то прибегают к методу индукции, тогда как для произвольной подстановки можно написать сравнения сразу в явном виде.

Основные принципы моего изложения теории Galois приведены мною в статье «Об основных положениях теории Galois». Матем. Сборн. Москва 1914 года.

Лучше всего я резюмирую их, если скажу несколько слов о каждой из следующих глав моей настоящей книги.

Глава пятнадцатая озаглавлена «теория Lagrange'a». Этим я хотел подчеркнуть то обстоятельство, что я считаю Lagrange'a родоначальником и творцом приложения теории групп к исследованию алгебраических уравнений. Lagrange'у принадлежитъ весьма важное разделение уравнений на буквенные и численные. Уравнения будут буквенными если их корни независимые переменные, между которыми не может существовать никаких соотношений, кроме тождественных. Численные уравнения я характеризую как такие, у которых существуют не тождественные соотношения

$$H(x_1, x_2, \ldots, x_n) = 0$$

между корнями. Глава пятнадцатая посвящена исключительно уравнениямъ буквениым.

Следующая шестнадцатая глава посвящена изложению теории Galois. Эта теория оказывается самой общей, в которой, как буквенные, так и численные уравнения входят как частные случаи.

Вместо *буквенной неизменяемости вида* рациональных функций от корней, при подстановках этих корней, которые рассматривались в теории Lagrange'a, приходится рассматривать *численную неизменность* функций, хотя бы вид функций и менялся.

Все теоремы Lagrange'a, приведенные в пятнадцатой главе, восстановляются для численных уравнений, если рассматривать только такие подстановки корней, которые входят в некоторую определенную группу, называемую *группой Galois* данного уравнения.

Я даю такое определение группы Galois: «группа *всех* подстановок, из которых *каждая* не нарушает *всякого рационального* соотношения $H(x_1, x_2, \ldots, x_n) = 0$ между корнями».

Так как между корнями буквеннаго уравнения могут существовать только тождественные соотношения, которые не нарушаются от любой подстановки, то группа Galois для этих уравнений будет всей симметрической.

При помощи одного приема, заимствованного мною у Kronecker'a, я свожу численные уравнения к теории Lagrange'a.

В семнадцатой главе я даю изложению более частный характер, а именно, предполагаю крайний случай численной определенности уравнения, а именно, случай определенных численных коэффициентов. Через это не происходит ограничения общности рассуждения, ибо в предыдущем изложении показана независимость законов теории от характера уравнения, причем играют роль лишь свойства его группы.

Тут я подчеркиваю наиболее важные по приложениям пункты: зависимость неприводимости уравнения от транзитивности группы, понятие об импримитивности и т. д.

Глава восемнадцатая трактует о наиболее важных видах уравнений, решаемых в радикалах, главным образом об уравнениях абелевых. Здесь уделено много места теории двучленных уравнений и ее приложениям. Я руководился при этом

особенно важным для науки значением теории полей, связанной с делением круга. Я приведу здесь слова Hilbert'a «Es ist diese Theorie ofaenbar auf der Höhe des heutigen arithmetischen Wissens die aüsserste erreichte Spitze, und man übersieht von ihr aus in weitem Rundblick das ganze durchforschte Gebiet, da fast jeder wesentliche Gedanke und Begriff aus der Körpertheorie, zum wenigsten in spezieller Fassung bei dem Beweise der höheren Reciprocitätsgesetze seine Anwendung findet».

Глава девятнадцатая посвящена моему изложению вопроса о решении уравнений в радикалах.

В двадцатой главе я разсматриваю уравнения пятой степени, показываю связь их теории с группой икосаэдра и рассматриваю резольвенту 6-ой степени. Тут представляется особенно важной резольвента, вычисленная в первый раз Cayley, отличие которой от Lagrange'овской состоит в том, что взята натуральная иррациональность вместо побочной.

Резольвента Cayley замечательна тем, что на ней удалось Cayley проделать все выкладки до конца, благодаря замечательному по остроумно приему вычисления.

Вот в кратких словах содержание моей книги. Насколько я достиг тех целей, которые мною руководили, судить конечно не мне.

Среди замеченных мною самим недостатков изложения один должен быть указан, а именно, на странице 439 строки 13, 14, 15 сверху должны быть уничтожены, как заключающая неправильную мысль. Фраза эта вкралась по недосмотру из прежнего литографированнаго издания.

Мне пришлось отступить при печатании книги от публикованного проспекта в нескольких пунктах. Между прочим я не излагаю связи решения уравнений пятой степени с эллиптическими функциями и гипергеометрическим рядом, ибо книга и без того достигла большого объема.

Если я буду жить и сохраню трудоспособность, то об этом я скажу в пятом томе проектируемого оочинения под заглавием «Арифметическая теория алгебраическихъ величин», первый том которого выпущен в литографированном виде, второй же том, под заглавиемъ «Теория идеалов», находится в печати.

Печатание настоящей книги проходило при крайне доброжелательном к ней отношении моих учеников, которые чем могли старались мне помочь, за что я и выражаю здесь всем им мою признательность. Особенно должен поблагодарить студента Царевского за составление Index'a nominum et rerum.

Профессор *Дмитрий Граве*

Харьков. Университет. 5 мая 1914.

Оглавление

ПОПРАВКИ

Я не указываю замеченных опечаток, которые по своей очевидности не влияют на понимание изложения, которые читатель сам заметит и поправит.

Обращу внимание лишь на две опечатки, которые, как мне кажется, могут затруднить читателя.

На страниц 114, 10 строка сверху, напечатана буква δ вместо буквы σ.

На странице 264 верхняя формула должна иметь вид

$$\frac{a_1xy+b_1x+c_1y+d_1}{a_2xy+b_2x+c_2y+d_2}=\frac{a_3xy+b_3x+c_3y+d_3}{a_4xy+b_4x+c_4y+d_4}$$

Глава I

О целых функциях

Понятие о целой функции и ее степени

§ 1

Определение. *Целой функцией* от нескольких независимых переменных называется всякий полином вида

$$\sum Ax^{\lambda}y^{\mu}z^{\nu}\dots t^{\tau},$$

показатели λ, μ, ν, $\dots$, τ суть некоторые целые положительные числа или нули, сумма $\sum$ распространяется на конечное число членов, а коэффициенты произвольные числа. Сумма

$$\lambda+\mu+\nu+\dots+\tau$$

называется *степенью* члена. Наибольшая из степеней отдельных членов представляет *степень функции.*

Однородные целые функции

§ 2

Возьмем целую функцию степени n от m переменных независимых $x_1, x_2, x_3, \dots$, x_m. Пусть эта функция будет

$$f(x_1, x_2, x_3, \dots, x_m).$$

Введем еще одну переменную независимую x_{m+1} и составим следующее выражение

$$x_{m+1}^n f\left(\frac{x_1}{x_{m+1}}, \frac{x_2}{x_{m+1}}, \dots, \frac{x_m}{x_{m+1}}\right).$$

Выражение (1) представляешь целую функцию от $m+1$ букв $x_1, x_2, x_3, \dots, x_m$, x_{m+1}. Эта функция обладает таким свойством, что все ее члены имеют одну и ту же степень n. Если мы для сокращения обозначим функцию (1) через $\varphi(x_1, x_2, \dots$, $x_m, x_{m+1})$, то этот знак будет выражать, так называемую, *однородную* целую функцию степени n от $m+1$ букв. Такие однородные функции мы будем для краткости называть *формами*, так что функцию φ можно будет назвать формою степени n от $m+1$ букв.

§ 3

Формы 2-ой и 3-ей степени называются соответственно *квадратичными* и *кубичными* формами; формы от двух и от трех независимых переменных называют соответственно *бинарными* и *тройничными*. Так, например,

$$ax^2 + 2bxy + cy^2$$

есть бинарная квадратичная форма, а

$$x^3 + y^3 + z^3 + 3xyz$$

есть тройничная кубичная форма.

Число членов целой функции

§ 4

Рассмотрим целую функцию

$$f(x_1, x_2, \ldots, x_m) \tag{1}$$

степени n от m букв. Предположим, что эта функция задана в самом общем виде, т. е. в состав ее входят всевозможного вида члены, степени которых не превосходят числа n; коэффициенты же при этих членах мы будем предполагать буквенными, т. е. каждый из этих коэффициентов будем предполагать обозначенным некоторой буквой, которой не придаем никакого определенного численного значения. Поставим себе задачей найти число членов функции (1), если предположить, что в функции нет подобных членов по отношению к независимым переменным.

Если мы перейдем от функции (1) к соответствующей ей форме той же степени n от $m + 1$ букв, как это было сделано в параграфе 2, то нетрудно видеть, что получим самого общего вида форму степени n с $m+1$ переменными независимыми, а потому обратимся к счету числа членов в общего вида форме

$$\varphi(x_1, x_2, \ldots, x_m, x_{m+1}) \tag{2}$$

от $m + 1$ букв. Каждый член такой формы имеет вид

$$Ax_1^{\alpha_1} x_2^{\alpha_2} \ldots x_{m+1}^{\alpha_{m+1}},$$

причем

$$\alpha_1 + \alpha_2 + \ldots + \alpha_{m+1} = n. \tag{3}$$

Итак, мы приходим к следующей задаче: найти сколькими способами можно представить заданное целое число в виде суммы $+1$ целых слагаемых. Сколько будет таких представлений, столько и будет различных членов в форме φ. Последняя задача есть частный случай ряда задач, рассматривавшихся в XVIII столетии под названием partitio numerorum. У нас имеется тот случай этих задач, когда среди слагаемых мы допускаем равные между собою, а также равные нулю. В

этом случае задача решается совершенно элементарно. В самом деле, мы можем формулировать задачу иначе, а именно можно сказать, что число членов в форме (2) равняется числу сочетаний из $m+1$ переменных независимых по n, причем допускаются повторяющиеся элементы.

Для нахождения числа таких сочетаний поступим так: выпишем все эти сочетания и обозначим их совокупность через B. При выписывании каждого из этих сочетаний будем держаться правила, чтобы значок всякого элемента был не меньше значка непосредственно предшествующего ему элемента слева, так что всякое сочетание будет иметь такой вид,

$$x_1 \underbrace{x_1 \dots x_1}_{\alpha_1} x_2 \underbrace{x_2 \dots x_2}_{\alpha_2} \dots x_{m+1} \underbrace{x_{m+1} \dots x_{m+1}}_{\alpha_{m+1}}. \tag{4}$$

Параллельно с выписанными нами сочетаниями B выпишем все сочетания по n элементов из $m+n$ букв

$$x_1, x_2, \dots, x_{m+1}, x_{m+2}, \dots, x_{m+n},$$

но уже без повторения элементов. Назовем совокупность всех таких сочетаний через C. Предположим, что эти новые сочетания так выписаны, что значок каждого элемента больше значка каждого предыдущего слева. Мы убеждаемся сразу, что число сочетаний совокупности B равно числу сочетаний C. В самом деле, если мы прибавим соответственно к каждому из ряда значков

$$\underbrace{1, 1, \dots, 1}_{\alpha_1}, \underbrace{2, 2, \dots, 2}_{\alpha_2}, \dots, \underbrace{m+1, m+1, \dots, m+1}_{\alpha_{m+1}}$$

числа ряда

$$0, 1, 2, \dots, n-1, \tag{5}$$

то получим некоторое сочетание из совокупности C, и обратно, если мы вычтем тот же самый ряд чисел (5) из значков какого-нибудь сочетания совокупности C, то получим непременно одно из сочетаний совокупности B, а так как от прибавления чисел ряда (5) или от вычитания этих чисел не может из одного члена одной из групп B, C получиться два различных члена другой группы, то мы приходим к убеждению, что число членов группы B равно числу членов группы C, и мы получаем для числа членов формы φ выражение

$$C^n_{m+n} = \frac{(m+n)(m+n-1)\dots(m+1)}{1 \cdot 2 \cdot 3 \cdots n} = \frac{\Pi(m+n)}{\Pi(m)\Pi(n)},$$

где $\Pi(n) = 1 \cdot 2 \cdot 3 \cdots n$.

Отсюда получаем, что число членов целой функции степени n от m букв равно C^n_{m+n}.

§ 5

Дадим еще другой вывод числа членов целой функции. Обозначим через N^n_m число членов функции f степени n от m переменных независимых.

Группируя члены функции f по степеням, мы представим ее в виде суммы форм различных степеней

$$f = \varphi_n + \varphi_{n-1} + \varphi_{n-2} + \ldots + \varphi_1 + \varphi_0,$$

где φ_k будет форма самого общего вида степени k от наших m переменных независимых.

Так, например,

$$f = ax^2 + bxy + cy^2 + dx + ey + f,$$
$$\varphi_2 = ax^2 + bxy + cy^2, \quad \varphi_1 = dx + ey, \quad \varphi_0 = f.$$

На основании соображений предыдущего параграфа заключаем, что число членов формы φ_k есть N^k_{m-1}.

Имеем

$$N^n_m = N^n_{m-1} + N^{n-1}_{m-1} + N^{n-2}_{m-1} + \ldots + N^0_{m-1}. \tag{1}$$

Требуется доказать, что

$$N^n_k = C^n_{k+n}. \tag{2}$$

Формула, очевидно, справедлива при $k = 1$, ибо общий вид целой функции степени n от одной независимой переменной есть

$$a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \ldots + a_{n-1}x + a_n$$

и мы имеем

$$N^n_1 = n + 1 = C^1_{n+1} = C^n_{n+1}.$$

Допустим справедливость формулы при $k = m-1$ и выведем ее справедливость для $k = m$. Мы имеем

$$N^n_{m-1} + N^{n-1}_{m-1} + N^{n-2}_{m-1} + \ldots + N^0_{m-1} = C^{m-1}_{m+n-1} + C^{m-1}_{m+n-2} + \ldots + C^{m-1}_{m-1},$$

но на основания известной теоремы элементарной алгебры имеем

$$C^{m-1}_{m+n-1} + C^{m-1}_{m+n-2} + \ldots + C^{m-1}_{m-1} = C^m_{m+n}$$

и получаем, сравнивая с формулой (1), окончательно

$$N^n_m = C^m_{m+n},$$

но формула (2) была доказана в случае $k = 1$, следовательно, она будет справедлива при $k = 2, 3, 4, \ldots$.

Возвышение в степень полинома

§ 6

Будем рассматривать выражение

$$(x_1 + x_2 + \ldots + x_m)^n. \tag{1}$$

Это выражение есть, очевидно, форма степени n от m букв. В частном случае, если число букв равняется двум, получаем

$$(x_1 + x_2)^n = x_1^n + C_n^1 x_1^{n-1} x_2 + C_n^2 x_1^{n-2} x_2^2 + \ldots + x_2^n = \sum C_n^{\alpha_2} x_1^{\alpha_1} x_2^{\alpha_2}, \tag{2}$$

где $\alpha_1 + \alpha_2 = n$. Перепишем формулу (2) еще так

$$(x_1 + x_2)^n = \sum \frac{\Pi(n)}{\Pi(\alpha_1)\Pi(\alpha_2)} x_1^{\alpha_1} x_2^{\alpha_2}. \tag{3}$$

Покажем, что последняя формула (3) может быть обобщена на случай какого-угодно числа m слагаемых, т. е. докажем справедливость следующей формулы

$$(x_1 + x_2 + \ldots + x_m)^n = \sum \frac{\Pi(n)}{\Pi(\alpha_1)\Pi(\alpha_2)\ldots\Pi(\alpha_m)} x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_m^{\alpha_m}. \tag{4}$$

Сумма во второй части формулы (4) распространяется на всевозможные значения показателей $\alpha_1, \alpha_2, \ldots, \alpha_m$, удовлетворяющие равенству

$$\alpha_1 + \alpha_2 + \ldots + \alpha_m = n. \tag{5}$$

Формулу (4) надо понимать так, что, если какой-нибудь из показателей, например, α_1, равен нулю, то надо считать соответствуюший в знаменателе множитель $\Pi(\alpha_1)$? равным 1, т. е. $\Pi(0) = 1$. Из Теории Чисел известно, что выражение

$$\frac{\Pi(n)}{\Pi(\alpha_1)\Pi(\alpha_2)\ldots\Pi(\alpha_m)}$$

при всяком n и при всяких α, удовлетворяющих равенству (5), есть число целое.

Для доказательства справедливости формулы (4) покажем, что, если она справедлива для некоторого показателя n, то она будет справедлива и для показателя $n+1$. Итак, умножим обе части равенства (4) на $x_1 + x_2 + \ldots + x_m$; тогда в первой части получим $(x_1 + x_2 + \ldots + x_m)^{n+1}$, а во второй части получим

$$\sum A x_1^{\beta_1} x_2^{\beta_2} \ldots x_m^{\beta_m}, \tag{6}$$

где показатели β удовлетворяют равенству

$$\beta_1 + \beta_2 + \ldots + \beta_m = n + 1.$$

Посмотрим, чему равен коэффициент A в новой формуле. Этот коэффициент составляется от сложения коэффициентов формулы (4), соответствующих членам с такими буквенными выражениями

$$\begin{gathered} x_1^{\beta_1 - 1} x_2^{\beta_2} \cdots x_m^{\beta_m}, \\ x_1^{\beta_1} x_2^{\beta_2 - 1} \cdots x_m^{\beta_m}, \\ \ldots\ldots\ldots\ldots\ldots, \\ x_1^{\beta_1} x_2^{\beta_2} \cdots x_m^{\beta_m - 1}, \end{gathered} \tag{7}$$

ибо от умножения буквенных выражений (1) последовательно на буквы $x_1, x_2, \ldots, x_m$ получится одно и то же буквенное выражение, стоящее в формуле (6) под знаком суммы, значит выходит

$$A = \frac{\Pi(n)}{\Pi(\beta_1 - 1)\Pi(\beta_2)\ldots\Pi(\beta_m)} + \\ + \frac{\Pi(n)}{\Pi(\beta_1)\Pi(\beta_2 - 1)\ldots\Pi(\beta_m)} + \ldots + \frac{\Pi(n)}{\Pi(\beta_1)\Pi(\beta_2)\ldots\Pi(\beta_m - 1)},$$

или, так как

$$\Pi(\beta) = \beta\Pi(\beta - 1),$$

то получаем

$$A = \frac{(\beta_1 + \beta_2 + \ldots + \beta_m)\Pi(n)}{\Pi(\beta_1)\Pi(\beta_2)\ldots\Pi(\beta_m)} = \frac{\Pi(n+1)}{\Pi(\beta_1)\Pi(\beta_2)\ldots\Pi(\beta_m)},$$

и, следовательно,

$$(x_1 + x_2 + \ldots + x_m)^{n+1} = \sum \frac{\Pi(n+1)}{\Pi(\beta_1)\Pi(\beta_2)\ldots\Pi(\beta_m)} x_1^{\beta_1} x_2^{\beta_2} \ldots x_m^{\beta_m},$$

т. е. формула (4) остается справедливой и для показателя $n + 1$.

Нужно теперь убедиться только, что формула (4) справедлива для $n = 1$. В самом деле, если $n = 1$, то из показателей α один должен равняться единице, а все остальные нули.

Выражение

$$\frac{\Pi(n)}{\Pi(\alpha_1)\Pi(\alpha_2)\ldots\Pi(\alpha_m)}$$

обращается в единицу, и формула (4) удовлетворяется. Итак, формула (4) есть действительно формула, дающая целую степень многочлена.

Пусть, например, требуется написать коэффициент в выражении $(x_1 + x_2 + \ldots + x_m)^{17}$ при члене, буквенное выражение которого есть $x_1^5 x_2^5 x_3^4 x_4^3$. По формуле (4) получим

$$A = \frac{\Pi(17)}{\Pi(5)\Pi(5)\Pi(4)\Pi(3)} = 2 \cdot 3 \cdot 7 \cdot 11 \cdot 13 \cdots 17.$$

§ 7

Дадим еще другое доказательство формулы возвышения полинома в степень.

В самом деле, обозначая $x_2 + x_3 + \ldots + x_m = X_1$, получим

$$(x_1 + X_1)^n = \sum \frac{\Pi(n)}{\Pi(\alpha_1)\Pi(n - \alpha_1)} x_1^{\alpha_1} x_2^{n - \alpha_1},$$

но

$$X_1^{n-\alpha_1} = (x_2 + X_2)^{n-\alpha_1} = \sum \frac{\Pi(n - \alpha_1)}{\Pi(\alpha_2)\Pi(n - \alpha_1 - \alpha_2)} x_2^{\alpha_2} X_2^{n-\alpha_1-\alpha_2},$$

где $X_2 = x_3 + x_4 + \ldots + x_m$. Подставляя второе выражение в первое, получим

$$(x_1 + x_2 + X_2)^n = \sum \frac{\Pi(n)}{\Pi(\alpha_1)\Pi(\alpha_2)\Pi(n - \alpha_1 - \alpha_2)} x_1^{\alpha_1} x_2^{\alpha_2} X_2^{n-\alpha_1-\alpha_2}.$$

Продолжая рассуждение далее придем к требуемой формуле.

Формула Taylor'a для целых функций

§ 8

Рассмотрим целую функций $f(x_1, x_2, \ldots, x_m)$ от m переменных независимых. Поставим себе задачею рассмотреть приращенное значение функции

$$f(x_1 + \xi_1, x_2 + \xi_2, \ldots, x_m + \xi_m) \tag{1}$$

где $\xi_1, \xi_2, \ldots, \xi_m$ произвольно взятые приращения.

Приращенное значение (1) будет, очевидно, некоторою целою функциею от приращений $\xi_1, \xi_2, \ldots, \xi_m$, коэффициенты которой будут, очевидно, целыми функциями от переменных независимых $x_1, x_2, \ldots, x_m$, другими словами, будет иметь место следующая формула

$$f(x_1 + \xi_1, x_2 + \xi_2, \ldots, x_m + \xi_m) = \sum D_{\alpha_1,\alpha_2,\ldots,\alpha_m} f, \tag{2}$$

где знаком $D_{\alpha_1,\alpha_2,\ldots,\alpha_m} f$ обозначена некоторая целая функция от независимых переменных $x_1, x_2, \ldots, x_m$. Покажем теперь, как вычислить функцию

$$D_{\alpha_1,\alpha_2,\ldots,\alpha_m} f. \tag{3}$$

Знак $D_{\alpha_1,\alpha_2,\ldots,\alpha_m}$, поставленный перед знаком функции f, обозначает некоторую операцию, которую надо произвести над заданной функцией f, чтобы получить функцию (3). Будем называть *характеристикой* операции (3) ряд чисел $\alpha_1, \alpha_2, \ldots, \alpha_m$. Если нас не интересует характеристика в операции, то мы будем обозначать операцию просто знаком D. Тождество (2) определяет, очевидно, все свойства операции D. Прежде всего нужно заметить, что операция D обладает следующими двумя замечательными свойствами

$$\begin{gathered} D(f + \varphi) = Df + D\varphi, \\ Dcf = cDf. \end{gathered} \tag{4}$$

Отсюда мы видим, что достаточно уметь производить операцию D только над буквенным выражением каждого члена функции. Рассмотрим поэтому выражение

$$Dx_1^{\lambda_1} x_2^{\lambda_2} \cdots x_m^{\lambda_m}.$$

На основании бинома Newton'a мы имеем

$$(x_i + \xi_i)^{\lambda_i} = \sum \frac{\Pi(\lambda_i)}{\Pi(\alpha_i)\Pi(\lambda_i - \alpha_i)} \xi_i^{\alpha_i} x_i^{\lambda_i - \alpha_i};$$

отсюда приращенное значение выражения

$$x_1^{\lambda_1} x_2^{\lambda_2} \cdots x_m^{\lambda_m}$$

выразится по формуле

$$(5)\quad \begin{aligned}(x_1+\xi_1)^{\lambda_1}(x_2+\xi_2)^{\lambda_2}\cdots(x_m+\xi_m)^{\lambda_m} &= \sum \frac{\Pi(\lambda_1)}{\Pi(\alpha_1)\Pi(\lambda_1-\alpha_1)}\cdot\\ \cdot\frac{\Pi(\lambda_2)}{\Pi(\alpha_2)\Pi(\lambda_2-\alpha_2)}\cdots\frac{\Pi(\lambda_m)}{\Pi(\alpha_m)\Pi(\lambda_m-\alpha_m)}&\xi_1^{\alpha_1}\xi_2^{\alpha_2}\ldots\xi_m^{\alpha_m}x_1^{\lambda_1-\alpha_1}x_2^{\lambda_2-\alpha_2}\cdots x_m^{\lambda_m-\alpha_m}.\end{aligned}$$

На основании формулы (2) мы замечаем, что будем иметь равенство

$$(6)\quad \begin{aligned}&D_{\alpha_1,\alpha_2,\ldots,\alpha_m}x_1^{\lambda_1}x_2^{\lambda_2}\cdots x_m^{\lambda_m} =\\ &= \frac{\Pi(\lambda_1)\Pi(\lambda_2)\ldots\Pi(\lambda_m)}{\Pi(\lambda_1-\alpha_1)\Pi(\lambda_2-\alpha_2)\ldots\Pi(\lambda_m-\alpha_m)}x_1^{\lambda_1-\alpha_1}x_2^{\lambda_2-\alpha_2}\cdots x_m^{\lambda_m-\alpha_m}.\end{aligned}$$

Нетрудно убедиться, что на основании формулы (6) операция D есть не что иное как производная, взятая от функции $f(x_1, x_2, \ldots, x_m)$ α_1 раз по букве x_1, α_2 раз по букве x_2, ... , α_m раз по букве x_m. Для того, чтобы убедиться в сказанном достаточно показать справедливость следующей формулы

$$(7)\quad D_{\beta_1,\beta_2,\ldots,\beta_m}D_{\alpha_1,\alpha_2,\ldots,\alpha_m\alpha} = D_{\alpha_1+\beta_1,\alpha_2+\beta_2\beta,\ldots,\alpha_m+\beta_m}.$$

Перепишем символически это равенство так

$$D_\beta D_\alpha = D_{\beta+\alpha} = D_{\alpha+\beta}.$$

В самом деле, взяв операцию $D_{\beta_1,\beta_2,\ldots,\beta_m}$ от обеих частей формулы (6), получим

$$D_\beta D_\alpha = \frac{\Pi(\lambda_1)\Pi(\lambda_2)\ldots\Pi(\lambda_m)}{\Pi(\lambda_1-\alpha_1)\Pi(\lambda_2-\alpha_2)\ldots\Pi(\lambda_m-\alpha_m)}D_{\beta_1,\beta_2,\ldots,\beta_m}x_1^{\lambda_1-\alpha_1}x_2^{\lambda_2-\alpha_2}\cdots x_m^{\lambda_m-\alpha_m}$$

или

$$\begin{aligned}D_\beta D_\alpha = \frac{\Pi(\lambda_1)\Pi(\lambda_2)\ldots\Pi(\lambda_m)}{\Pi(\lambda_1-\alpha_1-\beta 1)\Pi(\lambda_2-\alpha_2-\beta_2)\ldots\Pi(\lambda_m-\alpha_m-\beta_m)}&\cdot\\ \cdot x_1^{\lambda_1-\alpha_1-\beta_1}x_2^{\lambda_2-\alpha_2-\beta_2}\cdots x_m^{\lambda_m-\alpha_m-\beta_m} &= D_{\alpha+\beta},\end{aligned}$$

т. е. формула (7) оказывается справедливой.

Формула (7) убеждает нас в том, что операции D с произвольными характеристиками перестановочны, т. е.

$$(8)\quad D_{\beta_1,\beta_2,\ldots,\beta_m}D_{\alpha_1,\alpha_2,\ldots,\alpha_m} = D_{\alpha_1,\alpha_2,\ldots,\alpha_m}D_{\beta_1,\beta_2,\ldots,\beta_m}.$$

Кроме того формулы (5) и (6) убеждают нас, что будет иметь место равенство

$$(9)\quad D_{\alpha_1,\alpha_2,\ldots,\alpha_m}x_1^{\lambda_1}x_2^{\lambda_2}\cdots x_m^{\lambda_m} = 0$$

всякий раз, когда элемент α_i характеристики сделается больше соответственного показателя λ_i.

Свойства (8) и (9) операции D показывают, что всякую операцию с произвольной характеристикой $\alpha_1, \alpha_2, \ldots, \alpha_m$, можно получить, если произвести следующий ряд простейших операций: α_1 раз операцию с характеристикой $1, 0, 0, \ldots, 0$; α_2 раз

операцию с характеристикой $0, 1, 0, \ldots, 0$ и т. д., и наконец α_m раз операцию с характеристикой $0, 0, 0, \ldots, 1$. Что же касается этих простейших операции, то они представляют не что иное как простое дифференцирование по одной из переменных. В самом деле, например,

$$D_{1,0,0,\ldots,0} x_1^{\lambda_1} x_2^{\lambda_2} \cdots x_m^{\lambda_m} = \frac{\Pi(\lambda_1)}{\Pi(\lambda_1 - 1)} x_1^{\lambda_1 - 1} x_2^{\lambda_2} \cdots x_m^{\lambda_m} = \\ = \lambda_1 x_1^{\lambda_1 - 1} x_2^{\lambda_2} \cdots x_m^{\lambda_m},$$

т. е., другими словами, операция с характеристикой $1, 0, 0, \ldots, 0$ есть дифференцирование по букве x_1.

§ 9

На основании изложенного можно для операции D употреблять обычные знаки Дифференциального Исчисления, а именно можно писать

$$D_{\alpha_1,\alpha_2,\ldots,\alpha_m} f = \frac{\partial^{\alpha_1+\alpha_2+\ldots+\alpha_m}}{\partial x_1^{\alpha_1} \partial x_2^{\alpha_2} \ldots \partial x_m^{\alpha_m}} = f^{(\alpha_1+\alpha_2+\ldots+\alpha_m)}_{x_1^{\lambda_1} x_2^{\lambda_2} \cdots x_m^{\lambda_m}}(x_1, x_2, \ldots, x_m).$$

§ 10

Формула (2) § 6, которую можно будет переписать следующим образом

$$(1) \qquad f(x_1 + \xi_1, x_2 + \xi_2, \ldots, x_m + \xi_m) = \sum \frac{\xi_1^{\alpha_1} \xi_2^{\alpha_2} \cdots \xi_m^{\alpha_m}}{\Pi(\alpha_1)\Pi(\alpha_2) \ldots \Pi(\alpha_m)} \, f^{(\alpha_1+\alpha_2+\ldots+\alpha_m)}_{x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_m^{\alpha_m}}$$

выражает теорему Taylor'a в приложены к целой функций.

Формула Maclaurin'a

§ 11

Если мы в формул (1) § 10 положим

$$x_1 = 0, \quad x_2 = 0, \ \ldots, \quad x_m = 0, \\ \xi_1 = x_1, \quad \xi_2 = x_2, \ \ldots, \quad \xi_m = x_m,$$

то получим формулу Maclaurin'a для целой функции

$$(1) \qquad f(x_1, x_2, \ldots, x_m) = \sum \frac{x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_m^{\alpha_m}}{\Pi(\alpha_1)\Pi(\alpha_2) \ldots \Pi(\alpha_m)} \, f^{(\alpha_1+\alpha_2+\ldots+\alpha_m)}_{x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_m^{\alpha_m}}(0, 0, \ldots, 0).$$

Формула Maclaurin'a дает возможность составить выражение любого коэффициента целой функции через значения частных производных. В самом деле, если заданная целая функция имеет вид

$$f(x_1, x_2, \ldots, x_m) = \sum A_{\alpha_1,\alpha_2,\ldots,\alpha_m} x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_m^{\alpha_m},$$

то коэффициенты ее выражаются по формуле

$$A_{\alpha_1,\alpha_2,\ldots,\alpha_m} = \frac{1}{\Pi(\alpha_1)\Pi(\alpha_2)\ldots\Pi(\alpha_m)} \quad f^{(\alpha_1+\alpha_2+\ldots+\alpha_m)}_{x_1^{\alpha_1}x_2^{\alpha_2}\ldots x_m^{\alpha_m}}(0,0,\ldots,0).$$

§ 12

Особенно важное значение имеют теоремы Taylor'a и Maclaurin'a в случай одной переменной независимой. В этом случай, если обозначим через n степень целой функции $f(x)$, то получим следующую формулу Taylor'a

$$(1) \qquad f(x+h) = f(x) + \xi f'(x) + \frac{\xi^2}{\Pi(2)}f''(x) + \frac{\xi^3}{\Pi(3)}f'''(x) + \ldots + \frac{\xi^n}{\Pi(n)}f^{(n)}(x)$$

и следующую формулу Maclaurin'a

$$(2) \qquad f(x) = f(0) + xf'(0) + \frac{x^2}{\Pi(2)}f''(0) + \frac{x^3}{\Pi(3)}f'''(0) + \ldots + \frac{x^n}{\Pi(n)}f^{(n)}(0).$$

Теорема Euler'a

§ 13

Применим теорему Taylor'a к некоторой форме $\Phi(x_1, x_2, \ldots, x_m)$ степени n. На основании однородности формы Φ будет существовать тождество

$$\Phi(tx_1, tx_2, \ldots, tx_m) = t^n\Phi(x_1, x_2, \ldots, x_m).$$

Прилагая формулу Taylor'a, будем рассматривать выражение

$$(1) \qquad \Phi(x_1+\xi_1, x_2+\xi_2, \ldots, x_m+\xi_m).$$

Дадим приращениям значения

$$\xi_1 = tx_1, \quad \xi_2 = tx_2, \ \ldots, \quad \xi_m = tx_m;$$

тогда выражение (1) принимает вид

$$\Phi((1+t)x_1, (1+t)x_2, \ldots, (1+t)tx_m) = (1+t)^n\Phi(x_1, x_2, \ldots, x_m).$$

Теорема Taylor'a дает, следовательно,

$$(1+t)^n\Phi(x_1, x_2, \ldots, x_m) = \sum \frac{(tx_1)^{\alpha_1}(tx_2)^{\alpha_2}\ldots(tx_m)^{\alpha_m}}{\Pi(\alpha_1)\Pi(\alpha_2)\ldots\Pi(\alpha_m)} \cdot \frac{\partial^{\alpha_1+\alpha_2+\ldots+\alpha_m}\Phi}{\partial x_1^{\alpha_1}\partial x_2^{\alpha_2}\ldots\partial x_m^{\alpha_m}}.$$

Раскладывая первую часть по степеням t по формуле бинома, приравняем в обеих частях коэффициенты при некоторой определенной степени t^λ. Получим

$$(2) \quad \frac{\Pi(n)}{\Pi(\lambda)\Pi(n-\lambda)}\,\Phi(x_1, x_2, \ldots, x_m) = \sum \frac{x_1^{\alpha_1}x_2^{\alpha_2}\ldots x_m^{\alpha_m}}{\Pi(\alpha_1)\Pi(\alpha_2)\ldots\Pi(\alpha_m)} \cdot \frac{\partial^{\alpha_1+\alpha_2+\ldots+\alpha_m}\Phi}{\partial x_1^{\alpha_1}\partial x_2^{\alpha_2}\ldots\partial x_m^{\alpha_m}}.$$

Сумма в последней формул распространяется на все целые значения показателей $\alpha_1, \alpha_2, \ldots, \alpha_m$ положительный или равные нулю, дающие в сумме λ.

Перепишем формулу (2) в более удобном для запоминания виде умножением обеих частей ее на $\Pi(\lambda)$. Получим

(3)
$$n(n-1)\ldots(n-\lambda+1)\Phi(x_1, x_2, \ldots, x_m) = \sum \frac{\Pi(\lambda)\, x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_m^{\alpha_m}}{\Pi(\alpha_1)\Pi(\alpha_2)\ldots\Pi(\alpha_m)} \cdot \frac{\partial^\lambda \Phi}{\partial x_1^{\alpha_1} \partial x_2^{\alpha_2} \ldots \partial x_m^{\alpha_m}}.$$

Последнее тождество представляет весьма важную теорему, указанную в первый раз Euler'ом и часто прилагаемую в Алгебре.

Особенно важен случай $\lambda = 1$. В этом случае будет

$$n\Phi(x_1, x_2, \ldots, x_m) = x_1\frac{\partial\Phi}{\partial x_1} + x_2\frac{\partial\Phi}{\partial x_2} + \ldots + x_n\frac{\partial\Phi}{\partial x_m}; \tag{4}$$

этот случай имеет постоянное применение.

Обращение целой функции в бесконечность

§ 14

Рассмотрим функцию вида

$$f(z) = p_0 z^n + p_1 z^{n-1} + \ldots + p_{n-1} z + p_n, \tag{1}$$

причем будем предполагать самый общий случай, что коэффициенты $p_0, p_1, \ldots, p_n$, а также и независимая переменная z могут принимать какие угодно комплексные значения. Будем во всем дальнейшем модуль комплексного числа $z = x + iy$ обозначать знакомь $|z|$, причем $|z| = \sqrt{x^2 + y^2}$. Нетрудно видеть, что целая функция (1) для всякого конечного значения z имеет конечное численное значение.

Покажем теперь, что эта функция обращается в бесконечность при бесконечно большом значении z. Более точно можно формулировать указанное свойство целой функции так. *Сколь бы большим ни было задано положительное число C, всегда можно будет указать другое положительное число R такое, что будут иметь место одновременно следующие неравенства*

$$|z| > R, \qquad |f(z)| > C. \tag{2}$$

Обозначим для сокращения модули коэффициентов $p_0, p_1, \ldots, p_n$ через $a_0, a_1, \ldots, a_n$, а через ρ модуль переменной независимой z. Тогда будем иметь

$$f(z) = z^n\left\{p_0 + \frac{p_1}{z} + \frac{p_2}{z^2} + \ldots + \frac{p_n}{z^n}\right\}$$

откуда

$$|f(z)| = |\rho|^n\left|p_0 + \frac{p_1}{z} + \frac{p_2}{z^2} + \ldots + \frac{p_n}{z^n}\right|.$$

Применяя теорему о том, что модуль суммы не больше суммы и не меньше разности модулей слагаемых, можем написать следующий ряд неравенств

$$\left|p_0 + \frac{p_1}{z} + \frac{p_2}{z^2} + \ldots + \frac{p_n}{z^n}\right| \geq a_0 - \left|\frac{p_1}{z} + \frac{p_2}{z^2} + \ldots + \frac{p_n}{z^n}\right| \geq$$
$$\geq a_0 - \left(\frac{a_1}{\rho} + \frac{a_2}{\rho^2} + \ldots + \frac{a_n}{\rho^n}\right).$$

Нетрудно видеть, что при достаточно большом значении ρ сумма

$$\frac{a_1}{\rho} + \frac{a_2}{\rho^2} + \ldots + \frac{a_n}{\rho^n} \tag{3}$$

может быть сделана сколь угодно малою, так что, например, при некотором достаточно большом числе ρ, удовлетворяющем неравенству

$$\rho > \rho_0 \tag{4}$$

где ρ_0 некоторое соответственным образом подобранное достаточно большое число, сумма (3) будет меньше $\frac{a_0}{2}$; тогда получается неравенство

$$\left| p_0 + \frac{p_1}{z} + \frac{p_2}{z^2} + \ldots + \frac{p_n}{z^n} \right| > a_0 - \frac{a_0}{2} > \frac{a_0}{2}.$$

Остается еще подобрать ρ таким образом, чтобы было

$$\rho^n \frac{a_0}{2} > C$$

или

$$\rho > \sqrt[n]{\frac{2C}{a_0}}. \tag{5}$$

Итак, если мы через R_1 обозначим наибольшее из чисел ρ_0 и $\sqrt[n]{\frac{2C}{a_0}}$, то мы замечаем, что неравенство $\rho = |z| > R$ повлечет, как следствие, неравенство

$$|f(z)| > C,$$

что и требовалось доказать.

Так как при возрастании числа C будет возрастать беспредельно также число R_1, то доказанное свойство целой функции можно кратко выразить так: *целая функция обращается в бесконечность только при бесконечно большом значении переменной независимой.*

§ 15

Существуют функции трансцендентные, которые обладают свойством обращаться в бесконечность только при бесконечно большом значении независимого переменного. К числу таких функций принадлежать, например,

$$\sin z, \quad \cos z, \quad e^z, \quad \ldots.$$

Такого рода функциям дают название *целых трансцендентных* или *голоморфных.*

Непрерывность целой функции

§ 16

Покажем, что целая функция есть функция *непрерывная* при всяком значении z независимого переменного.

Дадим переменному независимому приращение h, модуль которого обозначим через δ. Покажем, что модулю δ можно дать столь малое значение, чтобы имело место неравенство

$$|f(z+h)-f(z)|<\varepsilon, \tag{1}$$

где ε произвольно взятое положительное число. По формуле Taylor'a имеем

$$f(z+h)-f(z)=h\left\{f'(z)+\frac{h}{1\cdot 2}f''(z)+\dots\right\}.$$

Выражение, стоящее в скобках, есть некоторый многочлен от двух переменных h и z. Если мы будем предполагать модуль h меньше 1, то модуль этого многочлена будет, очевидно, меньше некоторого положительного числа α, которое можно указать так: все знаки — в многочлене заменим знакомь $+$, h заменим единицей, а переменную h заменим ее модулем δ. Отсюда получаем

$$|f(z+h)-f(z)|<\delta\alpha.$$

Стоить только удовлетворить неравенству $\delta\alpha<\varepsilon$, как и получится искомое неравенство (1).

Непрерывность модуля целой функции

§ 17

Не только сама целая функция, но и ее модуль *непрерывно изменяется при непрерывном изменении* z.

В самом деле, написав формулу Taylor'a в виде

$$f(z+h)-f(z)=A,$$

мы замечаем по предыдущему параграфу, что модуль числа A при достаточно малом модуле числа h может быть сколь угодно мал. Получаем

$$f(z+h)=f(z)+A$$

и два следующих неравенства

$$|f(z)|-|A|\le|f(z+h)|\le|f(z)|+|A|,$$

$$-|A|\le|f(z+h)|-|f(z)|\le+|A|,$$

т. е. при бесконечно малом h разность $|f(z+h)|-|f(z)|$ бесконечно мала, и, следовательно, $|f(z)|$ изменяется непрерывно с изменением z, т. е., другими словами, этот модуль есть непрерывная функция от двух вещественных переменных x и y, входящих в составь переменной z.

Глава II

Корни целой функции от одной независимой переменной

Теорема Cauchy

§ 1

Пусть дана целая функция

$$f(z) = p_0 z^n + p_1 z^{n-1} + \ldots + p_n, \tag{1}$$

коэффициенты которой $p_0, p_1, \ldots, p_n$ суть произвольная действительные или мнимые числа, а первый из них p_0 отличен от нуля. Всякое число α, которое, будучи подставлено вместо z в (1) обращает функцию $f(z)$ в нуль, называется *корнем* уравнения $f(z) = 0$; это число, следовательно, удовлетворяет условию

$$f(\alpha) = 0.$$

Для краткости будем говорить, что α есть *корень функции* $f(z)$. Рассмотрим модуль целой функции $f(z)$. Этот модуль будет функция от двух переменных независимых, вещественной и мнимой части числа z, функция сохраняющая знав плюс при всевозможных вещественных значениях этих переменных. Очевидно, что эта функция имеет нижнюю границу, которая не может быть отрицательным числом. Так как эта функция непрерывная, то по известной теореме Weierstrass'a эта функция должна достигать своей низшей границы, т. е., другими словами, эта низшая граница должна быть minimum'ом рассматриваемого модуля, или еще иначе некоторым частным значением этого модуля, соответствующим некоторому определенному частному значение переменной z.

Для доказательства существовать корня целой функций $f(z)$ достаточно показать, что minimum модуля этой функций должен быть равен нулю. Это мы докажем, доказав теорему Cauchy о том, что minimum модуля не может быть больше нуля.

Теорему Cauchy мы формулируем так.

Если модуль численного значения $f(a)$ заданной функций, соответствующего численному значению a переменного независимого z, больше нуля, то этот модуль можно уменьшить прибавкой к числу a некоторого числа h.

Рассмотрим самый общий случай, когда при значении a сама функция $f(z)$ не обращается в нуль согласно формулировка теоремы, а ряд производных

$$f'(z),\ f''(z),\ \ldots,\ f^{(m-1)}(z)$$

обращается в нуль при $z = a$. По формул Taylor'a имеем

$$f(a+h) = f(a) + \frac{h^m}{\Pi(m)} f^{(m)}(a)\ \{1+Q\}, \tag{1}$$

где

$$Q = \frac{h}{m+1} \cdot \frac{f^{(m+1)}(a)}{f^{(m)}(a)} + \frac{h^2}{(m+1)(m+2)} \cdot \frac{f^{(m+2)}(a)}{f^{(m)}(a)} + \dots.$$

Подберем h удовлетворяющим равенству

$$\frac{h^m}{\Pi(m)}\ f^{(m)}(a) = -\delta a, \tag{2}$$

где δ некоторая положительная правильная дробь, величину которой можно взять сколь угодно малою. Равенство (1) можно переписать так

$$f(a+h) = f(a) - \delta f(a) + \frac{h^m}{\Pi(m)}\ Q = (1-\delta) f(a) + \frac{h^m}{\Pi(m)} f^{(m)}(a)\ Q;$$

отсюда

$$|f(a+h)| \leq (1-\delta)|f(a)| + \left| \frac{h^m}{\Pi(m)} f^{(m)}(a) \right|\ |Q|. \tag{1}$$

Так как Q можно сделать сколь угодно малым при достаточно малом h, то можно будет удовлетворить достаточно малым значением h неравенству

$$|Q| < 1,$$

а тогда на основании равенства (2) будет

$$\left| \frac{h^m}{\Pi(m)}\ f^{(m)}(a) \right| = \delta \cdot |f(a)|,$$

или

$$\left| \frac{h^m}{\Pi(m)} \right| \cdot |Q| < \delta |f(a)|.$$

Неравенство (3) обращается в следующее

$$|f(a+h)| < (1-\delta) \cdot |f(a)| + \delta \cdot |f(a)|,$$

или

$$|f(a+h)| < |f(a)|,$$

что и требовалось доказать.

Итак, мы видим, что наименьшее значение модуля должно равняться нулю, т. е. *целая функция должна иметъ, по крайней мере,один корень.*

§ 2

Доказанная теорема Cauchy о существовали корня целой функции влечет за собою, как следствие, возможность разложения целой функций степени n на n линейных множителей.

В самом деле, если α будет корнем целой функции

$$f(z) = p_0 z^n + p_1 z^{n-1} + \ldots + p_{n-1} z + p_n,$$

то, как известно из Элементарной Алгебры, целая функция $f(z)$ будет делиться на разность $z - \alpha$, так что

$$f(z) = (z - \alpha) f_1(z),$$

где $f_1(z)$ будет целая функция $n-1$ степени. Эта функция в свою очередь должна иметь некоторый корень (3), так что

$$f_1(z) = (z - \beta) f_2(z),$$

где $f_2(z)$ будет опять иметь корень γ и т. д.

Таким образом, мы замечаем, что функцию $f(z)$ можно представить в таком виде

$$f(z) = A(z - \alpha)(z - \beta)(z - \gamma) \cdots (z - \xi), \tag{1}$$

где A некоторое постоянное число, а вторая часть заключает n линейных множителей. Что касается постоянного числа A, то нетрудно видеть, что оно равно старшему коэффициенту p_0 рассматриваемой функции, так что мы получаем окончательно следующее разложение

$$f(z) = p_0(z - \alpha)(z - \beta)(z - \gamma) \cdots (z - \xi). \tag{2}$$

Последняя формула показывает, что теорема о существовали одного корня целой функции влечет, как следствие, существование ряда корней

$$\alpha,\ \beta,\ \gamma,\ \ldots,\ \xi \tag{3}$$

этой функции, причем число корней (3) должно равняться степени n функции.

Нетрудно убедиться, что *более n различных корней функция n-ой степени иметь не может.* Предположим обратное; допустим, что функция $f(z)$ кроме n корней (3) имеет еще корень π отличный от предыдущих; тогда, подставляя его в (2), получим

$$f(\pi) = p_0(\pi - \alpha)(\pi - \beta)(\pi - \gamma) \cdots (\pi - \xi).$$

Но все множители

$$\pi - \alpha,\ \pi - \beta,\ \pi - \gamma,\ \ldots,\ \pi - \xi$$

отличны от нуля, следовательно, должен равняться нулю коэффициент p_0; но если $p_0 = 0$, то также и p_1, ибо в противном случай мы имели бы функцию $n-1$ степени,

обращающуюся в нуль при n различных значениях z; точно также и $p_2 = 0$, одним словом, все коэффициенты $p_0, p_1, p_2, \ldots, p_n$ равны нулю.

Отсюда получается теорема.

Если целая функция $f(z)$ степени n обращается в нуль при большем чем n числе значений независимой переменной z, то все ее коэффициенты равны нулю, т. е., другими словами, функция тождественно равна нулю.

Понятие о кратных корнях

§ 3

Среди чисел ряда (3) предыдущего параграфа могут существовать одинаковые, так что разложение функции на линейные множители может иметь вид

$$f(z) = p_0(z-a)^\lambda (z-b)^\mu (z-c)^\nu \cdots ,$$

где $\lambda, \mu, \nu, \ldots$ целые числа, удовлетворяющая равенству

$$\lambda + \mu + \nu + \ldots = n,$$

а числа $a, b, c, \ldots$ суть различные между собою корни. Если $\lambda = 1$, то корень a называется *простым* корнем функции $f(z)$; если же $\lambda > 1$, то a есть, так называемый, *кратный* корень, причем число λ носить название *порядка* или *кратности* этого корня.

Выражение коэффициентов функции через корни

§ 4

Предполагая старший коэффициент целой функции равным единице, можем написать

$$f(z) = z^n + p_1 z^{n-1} + \ldots + p_n = (z-\alpha_1)(z-\alpha_2)\cdots(z-\alpha_n). \tag{1}$$

Корни $\alpha_1, \alpha_2, \ldots, \alpha_n$ мы будем предполагать какими угодно, или различными, или некоторые из этих корней могут быть равными между собою. Раскрывая в правой части уравнения (1) скобки и сравнивая с первою частью, получим следующий ряд равенств

$$\begin{aligned}
p_1 &= -\sum \alpha_i, \\
p_2 &= \sum \alpha_i \alpha_k, \\
p_3 &= -\sum \alpha_i \alpha_k \alpha_l, \\
&\cdots\cdots\cdots\cdots\cdots \\
p_n &= (-1)^n \sum \alpha_1 \alpha_2 \alpha_3 \cdots \alpha_n,
\end{aligned}$$

где в правой части написаны знаки сумм всевозможных сочетаний корней по одному, по два, по три, и т. д.

Итак, мы видим, что коэффициенты функции выражаются простыми целыми рациональными функциями от корней. Очевидно, что эти же равенства (2) определяют обратно корни $\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_n$ через коэффициенты $p_1, p_2, p_3, \ldots, p_n$, но эта новая задача представляет больше трудности и составляет главный предмет Алгебраического Анализа. Вследствие отсутствия простого алгоритма для получения корней по заданным коэффициентам приходится ставить себе более простые задачи, например,

1-ая задача: вычислить с данной степенью точности корни по заданным численным значениям коэффициентов;

2-ая задача: искать свойства корней, когда указан характер коэффициентов.

Особенно важным представляется следующий частный случай 2-ой задачи. Если коэффициенты будут функциями одной или нескольких переменных независимых, то корни, очевидно, будут также функциями этих переменных независимых. Является важным изучить свойства этих функций, когда коэффициенты суть заданные определенным образом функции от переменных независимых.

Непрерывность корней

§ 5

Какие бы вопросы в Алгебраическом Анализе ни затрагивались всюду встречается необходимость в доказательстве следующего основного свойства корней уравнения.

Корни уравнения суть непрерывные функции его коэффициентов.

Будем рассматривать уравнение вида

$$f(z) = z^n + p_1 z^{n-1} + \ldots + p_{n-1} z + p_n = 0 \tag{1}$$

с коэффициентом единица при старшей степени. Коэффициенты $p_1, p_2, \ldots, p_n$ некоторые переменные числа комплексные или вещественные. На данную минуту для нас безразлично, будут ли эти коэффициенты функции от каких нибудь переменных независимых, или же числа меняются каким нибудь другим образом. Разложим функций $f(z)$ на линейные множители

$$f(z) = (z-a)^\lambda (z-b)^\mu (z-c)^\nu \cdots .$$

Будем изменять коэффициенты уравнения (1) непрерывно, так что приращенное значение $f_1(z)$ функций можно представить так

$$f_1(z) = \varphi(z) + f(z),$$

где

$$\varphi(z) = \varepsilon_1 z^{n-1} + \varepsilon_2 z^{n-2} + \ldots,$$

и где $\varepsilon_1, \varepsilon_2, \ldots$ суть бесконечно малые приращения коэффициентов.

Проведем из начала координат плоскости комплексного переменного круг настолько большого радиуса R, чтобы все корни уравнения $a, b, c, \ldots$ лежали внутри этого круга (см. стр. 20). Около каждого из корней опишем круг некоторого радиуса; пусть радиус круга описанного около a будет ρ, около b будет ρ', около c будет

ρ'' и т. д. Радиусы кругов $\rho, \rho', \rho'', \ldots$ возьмем настолько малыми, чтобы круги не пересекались между собою и не пересекались с кругом R. Достаточно, конечно, взять эти радиусы меньшими половины наименьшего из расстояний между корнями. Обозначим буквою g ту часть плоскости, которая находится внутри круга R, но вне кругов описанных около корней; знаками же

$$(\rho),\ (\rho'),\ (\rho''),\ \ldots$$

обозначим области внутри кругов описанных около корней. Будем теперь уменьшать до нуля все радиусы $\rho, \rho', \rho'', \ldots$.

Теорема, которая будет выражать непрерывность корней, может быть формулирована так.

Теорема. *Сколь бы малыми ни были заданы радиусы $\rho, \rho', \rho'', \ldots$, всегда можно подобрать настолько малые приращения $\varepsilon_1, \varepsilon_2, \ldots$ коэффициентов функций $f(z)$, чтобы корни приращенной функции $f_1(z)$ удовлетворяли следующим двум условиям:* 1° *— все корни функции $f_1(z)$ лежат внутри областей $(\rho), (\rho'), (\rho''), \ldots$ и* 2° *— внутри области (ρ) лежит λ корней приращенной функции, внутри области (ρ') лежит μ корней приращенной функции, внутри области (ρ'') лежит ν корней, и т. д.*

Для всякой точки z области g будем иметь

$$|z-a| > \rho, \quad |z-b| > \rho', \quad |z-c| > \rho'', \quad \ldots,$$

значит,

$$|f(z)| > \rho^\lambda \rho'^\mu \rho''^\nu \cdots . \tag{2}$$

Покажем теперь, что это неравенство (2) для достаточно малых значений $\varepsilon_1, \varepsilon_2, \ldots$ не может иметь места, если под z будем разуметь корень приращенного уравнения. В самом деле, пусть a_1 будет корень функции $f_1(z)$, так что

$$f_1(a_1) = 0;$$

но

$$f_1(z) = f(z) + \varphi(z),$$

следовательно,

$$f(a_1) + \varphi(a_1) = 0,$$

то есть

$$f(a_1) = -\varphi(a_1).$$

Но величина $\varphi(a_1)$ при достаточно малых ε может иметь сколь угодно малый модуль, следовательно, при достаточно малых величинах $\varepsilon_1, \varepsilon_2, \ldots$ будет иметь место

$$|f(a_1)| < \rho^\lambda \rho'^\mu \rho''^\nu \cdots ,$$

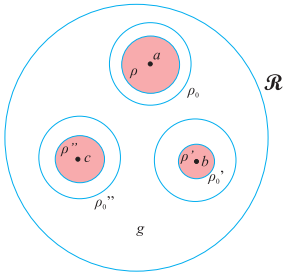
и неравенство (2) характеризующее область g не удовлетворяется, так что при достаточно малых приращениях коэффициентов корни приращенной функций не выходят из областей $(\rho), (\rho'), (\rho''), \ldots$. Первая часть теоремы таким образом доказана.

Остается показать, что, если a будет иметь кратность λ, то в области (ρ) окажется как раз λ корней приращенного уравнения. Пусть приращенные корни располагаются так: в области (ρ) находятся корни a_1 кратности λ_1, a_2 кратности λ_2, a_3 кратности λ_3, и т. д.; в области (ρ') корни b_1 кратности μ_1, b_2 кратности μ_2, b_3 кратности μ_3 и т. д.; в области (ρ'') корни c_1 кратности ν_1, c_2 кратности ν_2, и т. д. Так как степень приращенного уравнения остается та же самая, то должно быть

$$\lambda_1 + \lambda_2 + \ldots + \mu_1 + \mu_2 + \ldots + \nu_1 + \nu_2 + \ldots = n. \tag{3}$$

Необходимо показать, что

$$\begin{aligned} \lambda &= \lambda_1 + \lambda_2 + \lambda_3 + \ldots \\ \mu &= \mu_1 + \mu_2 + \mu_3 + \ldots \\ \nu &= \nu_1 + \nu_2 + \nu_3 + \ldots \\ &\ldots\ldots\ldots\ldots\ldots\ldots \end{aligned}$$



Черт. 1

Рассмотрим одну из областей около корней, например, область (ρ). Тогда, обозначая,

$$\begin{aligned} f(z) &= (z-a)^{\lambda}\psi(z), \\ f_1(z) &= (z-a_1)^{\lambda_1}(z-a_2)^{\lambda_2}(z-a_3)^{\lambda_3}\cdots\ \psi_1(z), \end{aligned}$$

где функции $\psi(z)$ и $\psi_1(z)$ имеют корни в других областях, мы замечаем, что можно указать четыре положительных числа A, B, A_1, A_2, независимых от переменных радиусов $\rho, \rho', \rho'', \ldots$; при которых будут иметь место неравенства

$$\begin{aligned} A < |\psi(z)| < B, \\ A_1 < |\psi_1(z)| < B_1 \end{aligned} \tag{4}$$

для всех точек области (ρ). В самом деле, при уменьшении до нуля радиусов $\rho, \rho', \rho'', \ldots$ мы можем предполагать, что все эти радиусы становятся и остаются меньше некоторого достаточно малого радиуса ρ_0; тогда, если мы около всех корней a, b, c первоначальной функции опишем круги радиуса ρ_0, то из следующих соображений получим меньшие пределы A и A_1 для модулей $|\psi(z)|$ и $|\psi_1(z)|$. Так как

$$\begin{aligned} \psi(z) &= (z-b)^{\mu}(z-c)^{\nu}\ldots \\ \psi_1(z) &= (z-b_1)^{\mu_1}(z-b_2)^{\mu_2}\cdots(z-c_1)^{\nu_1}(z-c_2)^{\nu_2}\cdots, \end{aligned}$$

то мы замечаем, что в состав модулей

$$|\psi(z)| \quad \text{и} \quad |\psi_1(z)|$$

входят выражения $|z-\alpha|$, где z соответствует точке в области (ρ), а α есть одно из чисел

$$b,\ c,\ \ldots,\ b_1,\ b_2,\ \ldots,\ c_1, c_2,\ \ldots$$

Так как α принадлежит к одной из других областей $(\rho'), (\rho''), \ldots$, то мы получим низшие границы модулей A и A_1, если вместо всякого множителя $|z-\alpha|$

напишем наименьшее расстояние между точками двух кругов радиуса ρ_0 соответствующих z и α. Подобным же образом, заменяя каждое из выражений $|z-\alpha|$ расстоянием двух наиболее удаленных точек этих кругов, получим в произведении два числа B и B_1 большие модулей $|\psi(z)|$ и $|\psi_1(z)|$, так что выясняется возможность выбора четырех чисел A, A_1, B, B_1 независимых от переменных радиусов $\rho, \rho', \rho'', \ldots$, при которых неравенства (4) имеют место для всех точек области (ρ).

Если мы будем рассматривать значения переменной z на самом круге ρ, то будем иметь

$$|z-\alpha| = \rho.$$

Из равенства

$$f(z_1) = f_1(z) - \varphi(z)$$

получаем неравенство

$$|f(z)| \leq |f_1(z)| + |\varphi(z)|,$$

или иначе

$$|z-a|^{\lambda} \cdot |\psi(z)| \leq |\psi_1(z)| \cdot |z-a_1|^{\lambda_1} \cdot |z-a_2|^{\lambda_2} \cdots + |\varphi(z)|.$$

При изменении z по кругу ρ модули $|z-a_1|, |z-a_2|, \ldots$ не превосходят диаметра 2ρ. Поэтому, принимая во внимание неравенства (4), приходим к следующему неравенству

$$\rho^{\lambda} A < 2^{\lambda_1+\lambda_2+\lambda_3+\cdots} \rho^{\lambda_1+\lambda_2+\lambda_3+\cdots} \cdot B + |\varphi(z)|.$$

Так как величина $\varphi(z)$ есть бесконечно малая, то, значит, можно подобрать приращения $\varepsilon_1, \varepsilon_2, \ldots$ коэффициентов столь малыми, чтобы было

$$|\varphi(z)| < A'\rho^{\lambda},$$

где A' некоторое положительное число произвольно взятое меньшее числа A. Получаем по сокращении неравенства на ρ^{λ}

$$A - A' < 2^{\lambda_1+\lambda_2+\cdots} B_1 \rho^{-\lambda+\lambda_1+\lambda_2+\cdots}. \tag{5}$$

Так как такое неравенство должно иметь место при сколь угодно малом ρ, то, очевидно, что показатель

$$-\lambda + \lambda_1 + \lambda_2 + \ldots$$

над буквою ρ во второй части (5) не может быть числом положительным, потому что тогда вторая часть, будучи величиной бесконечно малой не могла бы оставаться больше некоторого определенного положительного числа $A - A'$. Итак, показатель должен быть или нуль, или отрицательное число, и мы получим

$$\lambda \geq \lambda_1 + \lambda_2 + \lambda_3 + \ldots \tag{6}$$

Рассуждая совершенно подобным образом, мы придем к аналогичным неравенствам для остальных корней $b, c, \ldots$

$$\begin{gathered} \mu \geq \mu_1 + \mu_2 + \mu_3 + \ldots, \\ \nu \geq \nu_1 + \nu_2 + \nu_3 + \ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots \end{gathered} \tag{7}$$

Но так как обе функции $f(z)$ и $f_1(z)$, будучи степени n, должны иметь каждая по n корней, то в неравенствах (6) и (7) должна равняться n сумма как первых частей λ, μ, ν так и сумма вторых частей. Отсюда вытекает невозможность существования знаков неравенств в формулах (6) и (7); так что мы получаем окончательно

$$\lambda = \lambda_1 + \lambda_2 + \lambda_3 + \dots$$
$$\mu = \mu_1 + \mu_2 + \mu_3 + \dots$$
$$\nu = \nu_1 + \nu_2 + \nu_3 + \dots$$
$$\dots\dots\dots\dots\dots\dots,$$

что и доказывается вторая часть теоремы.

Приближение к нулю нескольких старших коэффициентов

§ 6

Как следствие доказанной теоремы о непрерывности корней можно будет доказать следующее свойство корней целой функции.

Пусть в функции

$$f(z) = p_0 z^n + p_1 z^{n-1} + \dots + p_{n-1} z + p_n,$$

k последних коэффициентов

$$p_{n-k+1},\ p_{n-k+2},\ \dots,\ p_n,$$

непрерывно изменяясь, приближаются к нулю. Тогда функция наша приближается в новой функции

$$f_1(z) = z^k f_2(z),$$

где

$$f_2(z) = p_0 z^{n-k} + p_1 z^{n-k-1} + \dots + p_{n-k}.$$

Новая функция $f_1(z)$ имеет число нуль k-кратным корнем, остальные корни суть корни функции $f_2(z)$. Отсюда получаем теорему.

Теорема. *При приближении к нулю k последних коэффициентов функции $f(z)$ приближаются к нулю k корней этой функции.*

Заменой z на $\dfrac{1}{z}$ мы переводим уравнение $f(z) = 0$ в уравнение

$$F(z) = 0,$$

у которого кооэффициенты идут в обратном порядке. Нулевым корням первого будут соответствовать бесконечно большие корни другого. Мы получим теорему.

Теорема. *Если в целой функции $f(z)$ приближаются к нулю первые k коэффициентов $p_0, p_1, p_2, \dots, p_{k-1}$, то k корней функции беспредельно возрастают по абсолютной величине.*

Так, например, для квадратной функций

$$ax^2 + bx + c$$

при уменьшении коэффициента a до нуля один корень обращается в бесконечность, а другой приближается к корню функции

$$bx + c.$$

Условия, при которых корень a имеет кратность k.

§ 7

Теорема Taylor'a дает возможность написать общий вид остатка от деления функции $f(z)$ на $(z-a)^k$.

В самом деле, напишем формулу Taylor'a в таком виде

$$f(z) = f(a) + (z-a)f'(a) = \frac{(z-a)^2}{2!}f''(a) + \ldots + \frac{(z-a)^{k-1}}{(k-1)!}f^{(k-1)}(a) + (z-a)^k Q,$$

где

$$Q = \frac{1}{k!}f^{(k)}(a) + \frac{z-a}{(k+1)!}f^{(k+1)}(a) + \frac{(z-a)^2}{(k+2)!}f^{(k+1)}(a) + \ldots$$

Тогда мы видим, что от деления на $(z-a)^k$ получается частное Q и остаток

$$f(a) + (z-a)f'(a) = \frac{(z-a)^2}{2!}f''(a) + \ldots + \frac{(z-a)^{k-1}}{(k-1)!}f^{(k-1)}(a).$$

Чтобы этот остаток был тождественно равен нулю, необходимо и достаточно удовлетворить следующим равенствам

$$f(a) = 0, \quad f'(a) = 0, \quad f''(a) = 0, \ \ldots, \ f^{(k-1)}(a) = 0. \tag{1}$$

Равенства (1) представляюсь необходимые условия для того, чтобы корень имел кратность k. Для получения достаточных условий, необходимо потребовать, чтобы частное Q не делилось больше на разность $z-a$, т. е., другими словами, должно быть

$$f^{(k)}(a) \neq 0. \tag{2}$$

Итак, мы видим, что условия необходимые и достаточные для того, чтобы корень a имел кратность k, состоят из равенств (1) и неравенства (2).

Из полученных условий легко заметить, что, если a есть корень функции $f(z)$ кратности k, то он будет корнем первой производной кратности $k-1$, корнем второй производной кратности $k-2$, и т. д.; в самом деле, эти условия

$$f'(a) = f''(a) = \ldots = f^{(k-1)}(a) = 0, \quad f^{(k)}(a) \neq 0,$$

если обозначить

$$f'(z) = \varphi(z),$$

дают

$$\varphi(a) = 0, \quad \varphi'(a) = 0, \ \ldots, \ \varphi^{(k-2)}(a) = 0$$

$$\varphi^{(k-1)}(a) \neq 0.$$

Аналогичные условия получим для второй производной и т. д.

Освобождение уравнений от кратных корней

§ 8

Обозначим корни уравнения $f(z) = 0$ через

$$a_1,\ a_2,\ \ldots,\ a_{k-1},\ a_k, \tag{1}$$

а соответственные их кратности через

$$m_1,\ m_2,\ \ldots,\ m_{k-1},\ m_k,$$

тогда функция $f(x)$ будет иметь вид

$$f(x) = p_0(x - a_1)^{m_1}(x - a_2)^{m_2} \cdots (x - a_k)^{m_k},$$

где

$$m_1 + m_2 + \ldots + m_k = n, \tag{2}$$

степени функции.

На основании предыдущего §-а мы можем сказать, что производная $f'(x)$ будет иметь вид

$$f'(x) = (x - a_1)^{m_1 - 1}(x - a_2)^{m_2 - 1} \cdots (x - a_k)^{m_k - 1} \cdot \varphi(x),$$

где $\varphi(x)$ целая функция, не имеющая ни одного из корней (1). Обозначив через l степень функций $\varphi(x)$, получим

$$n - 1 = m_1 - 1 + m_2 - 1 + \ldots + m_k - 1 + l,$$

откуда, принимая во внимание (2), получим

$$l = k - 1.$$

Общим наибольшим делителем функций $f(x)$ и ее производной $f'(x)$ будет, очевидно, многочлен

$$(x - a_1)^{m_1 - 1}(x - a_2)^{m_2 - 1} \cdots (x - a_k)^{m_k - 1}. \tag{3}$$

Если все числа

$$m_1,\ m_2,\ \ldots,\ m_k$$

равны единице, то общий наибольший делитель приводится к единице. Отсюда получаем такую теорему.

Теорема. *Если есть корни функций $f(x)$ простые, то эта функция не имеет общих делителей с производной.*

Итак, мы видим, что все кратные корни целой функции $f(x)$ суть в то же время корни общего наибольшего делителя (3) функции $f(x)$ и ее производной $f'(x)$.

Если общий наибольший делитель (3) найден, то, разделяя на него $f(x)$, получим новую функцию

$$f_1(x) = p_0(x - a_1)(x - a_2)\cdots(x - a_k)$$

и новое уравнение

$$f_1(x) = 0 \tag{4}$$

такое, что его корни будут совпадать с корнями (1) заданного уравнения, но все эти корни для нового уравнения (4) будут уже простыми.

Итак, для нахождения искомых корней заданного уравнения $f(x) = 0$ достаточно решить уравнение (4), которое уже не имеет кратных корней. Из курса Элементарной Алгебры известно, что общий наибольший делитель двух многочленов находится при помощи последовательных делений, то, следовательно, мы видим, что освобождение уравнения от кратных корней совершается при помощи рациональных действий и значит представляет задачу характера элементарного.

§ 9

Обозначишь через X_1 произведение множителей вида

$$x - a,$$

соответствующих простым корням a некоторой целой функции; через X_2 произведение множителей вида

$$x - b$$

соответствующих двукратным корням, взятым по одному только разу; и т. д. Тогда получим

$$f(x) = X_1 X_2^2 X_3^3 X_4^4 \cdots X_k^k,$$

если примем коэффициент при наивысшей степени x равным единице и обозначим через k наибольшую кратность корней данного уравнения.

Обозначим через $P_1, P_2, \ldots, P_k$ общие наибольшие делители

P_1	для функции	$f(x)$	и ее производной	$f'(x)$,
P_2	”	P_1	”	P_1',
P_1	”	$f(x)$	”	$f'(x)$,
$\ldots$	$\ldots\ldots\ldots\ldots$	$\ldots$	$\ldots\ldots\ldots\ldots\ldots$	$\ldots$
P_k	”	P_{k-1}	”	P_{k-1}'.

Выражения каждой из функций P по § 8 будут

$$\begin{aligned} f(x) &= X_1 X_2^2 X_3^3 X_4^4 \cdots X_k^k, \\ P_1 &= X_2 X_3^2 \cdots X_k^{k-1}, \\ P_2 &= X_3 X_4^2 \cdots X_k^{k-2}, \\ \cdots &\quad \cdots \quad \cdots\cdots, \\ P_{k-1} &= X_k, \\ P_k &= 1. \end{aligned}$$

Разделяя последовательно функцию $f(x)$ на P_1, функцию P_1 на P_2, ... функцию P_{k-1} на P_k, и обозначая соответственные частные через $\Theta_1, \Theta_2, \ldots, \Theta_k$, получим

$$\Theta_1 = X_1 X_2 \cdots X_k,$$

$$\Theta_2 = X_2 X_3 \cdots X_k,$$

$$\cdots\cdots\cdots\cdots..,$$

$$\Theta_k = X_k$$

Отсюда мы видишь, что функция Θ_1 делится на Θ_2, функция Θ_2 на Θ_3 и т. д.; производя это деление, получим

$$\frac{\Theta_1}{\Theta_2} = X_1, \quad \frac{\Theta_2}{\Theta_3} = X_2, \ \ldots, \ \frac{\Theta_{k-1}}{\Theta_k} = X_{k-1}, \ \ \Theta_k = X_k.$$

Все функции

$$X_1, \ X_2, \ \ldots, \ X_k$$

определяются таким образом посредством *алгебраического деления.*

Мы видим, что решение уравнения $f(x) = 0$ сводится к уравнений

$$X_1 = 0, \ X_2 = 0, \ \ldots, \ X_k = 0,$$

из которых каждое имеет уже только простые корни.

§ 10

Поясним теорию примером. Пусть требуется освободить от кратных корней уравнение

$$f(x) = x^6 + 3x^5 - 6x^3 - 3x^2 + 3x + 2 = 0.$$

Имеем

$$f'(x) = 6x^5 + 15x^4 - 18x^2 - 6x + 3.$$

Будем делить на многочлен

$$\frac{1}{3} f'(x) = 2x^5 + 5x^4 - 6x^2 - 2x + 1 \tag{1}$$

функцию $f(x)$, умножив ее предварительно на 2.

Напомним, что при нахождении общего наибольшего делителя можно во избежание дробных коэффициентов умножить на 2 каждый из промежуточных остатков, т. е. можно повести действие деления так:

$$\begin{array}{r|l}
2x^6+6x^5-12x^3-6x^2+6x+4 & 2x^5+5x^4-6x^2-2x+1 \\
\cline{2-2}
2x^6+5x^5-6x^3-2x^2+x & x+1 \\
\cline{1-1}
x^5-6x^3-4x^2+5x+4 & \\
2x^5-12x^3-8x^2+10x+8 & \\
\cline{1-1}
2x^5+5x^3-6x^2-25x+1 & \\
\cline{1-1}
-5x^4+12x^3-2x^2+12x+7 &
\end{array}$$

Делим на полученный остаток функцию (1), умножив предварительно последнюю на 5 и умножая на 5 промежуточный остаток

$$\begin{array}{r|l}
10x^5+25x^4-30x^2-10x+5 & 5x^4+12x^3-2x^2-12x-7 \\
\cline{2-2}
10x^5+24x^4+4x^3-24x^2-14x & 2x+1 \\
\cline{1-1}
5x^4-20x^3-30x^2+20x+25 & \\
5x^4+12x^3+2x^2-12x-7 & \\
\cline{1-1}
-32x^3-32x^2+32x+32 &
\end{array}$$

Продолжая деление, получим

$$\begin{array}{r|l}
5x^4+12x^3-2x^2-12x-7 & x^3+x^2-x-1 \\
\cline{2-2}
5x^4+5x^3-5x^2-5x & 5x+7 \\
\cline{1-1}
7x^3+7x^2-7x-7 & \\
7x^3+7x^2-7x-7 & \\
\cline{1-1}
0 &
\end{array}$$

Итак,

$$P_1 = x^3+x^2-x-1;$$

производная от P_1 есть

$$P_1' = 3x^2+2x-1.$$

Производя деление

$$\begin{array}{r|l}
3x^3+3x^2-3x-3 & 3x^2+2x-1 \\
\cline{2-2}
3x^3+2x^2-x & x+1 \\
\cline{1-1}
x^2-2x-3 & \\
3x^2-6x-9 & \\
\cline{1-1}
3x^2+2x-1 & \\
\cline{1-1}
-8x-8 &
\end{array}$$

$$\begin{array}{r|l}
3x^2+2x-1 & x+1 \\
\cline{2-2}
3x^2+3x & 3x-1 \\
\cline{1-1}
-x-1 & \\
-x-1 & \\
\cline{1-1}
0 &
\end{array}$$

получим

$$P_2 = x+1.$$

Далее, производя деление

$$\begin{array}{rrrrrr|l}
x^6 & +3x^5 & & -6x^3 & -3x^2 & +3x+2 & x^3+x^2-x-1 \\
\cline{7-7}
x^6 & +x^5 & -x^4 & -x^3 & & & x^3+2x^2-x-2 \\
\cline{1-4}
 & 2x^5 & +x^4 & -5x^3 & -3x^2 & & \\
 & 2x^5 & +2x^4 & -2x^3 & -2x^2 & & \\
\cline{2-5}
 & & -x^4 & -3x^3 & -x^2 & +3x & \\
 & & -x^4 & -x^3 & +x^2 & +x & \\
\cline{3-6}
 & & & -2x^3 & -2x^2 & +2x+2 & \\
 & & & -2x^3 & -2x^2 & +2x+2 & \\
\cline{4-6}
 & & & & & 0 &
\end{array}$$

получим

$$\Theta_1 = x^3 + 2x^2 - x - 2;$$

деля

$$\begin{array}{rrrrr|l}
x^3 & +x^2 & -x & -1 & & x+1 \\
\cline{6-6}
x^3 & +x^2 & -x & -1 & & x^2-1 \\
\cline{1-4}
 & & & 0 & &
\end{array}$$

получим

$$\Theta_2 = x^2 - 1.$$

Отсюда, производя деление

$$\begin{array}{rrrrr|l}
x^3 & +2x^2 & -x & -2 & & x^2-1 \\
\cline{6-6}
x^3 & +2x^2 & -x & -2 & & x+2 \\
\cline{1-4}
 & & & 0 & &
\end{array}$$

получим

$$X_1 = x + 2, \quad X_2 = \frac{\Theta_2}{P_2} = x - 1, \quad X_3 = P_2 = x + 1.$$

Получаем, следовательно,

$$f(x) = (x+2)(x-1)^2(x+1)^3,$$

и заданное уравнение приводится к трем следующим

$$x + 2 = 0, \quad x - 1 = 0, \quad x + 1 = 0.$$

Корни заданного уравнения суть, следовательно, -2, $+1$, -1.

Знак целой функции при бесконечно большом значении независимого переменного

§ 11

Обратимся к рассмотрению целых функций с вещественными коэффициентами.

Докажем следующую теорему.

Теорема. *При достаточно больших по абсолютной величине вещественных значениях переменной независимой x знак целой функции*

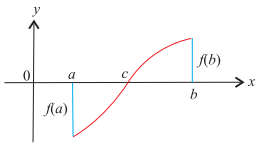
$$f(x) = p_0 z^n + p_1 z^{n-1} + \ldots + p_n$$

совпадает со знаком первого ее члена.

В самом деле, переписав функций $f(x)$ в виде

$$f(x) = p_0 x^n \left\{ 1 + \frac{p_1}{p_0} \cdot \frac{1}{x} + \ldots + \frac{p_n}{p_0} \cdot \frac{1}{x^n} \right\},$$

мы замечаем, что сумма всех чденов, кроме первого, в выражении, стоящем в скобках, может быть сделана сколь угодно малою при достаточно больших значениях x. Значить, знак всей суммы будет совпадать со знаком $p_0 x^n$ при достаточно больших значениях x, теорема таким образом доказана.



Черт. 2

Из этой теоремы в связи с доказанною раньше непрерывностью функции $f(x)$ можно вывести несколько важных общих замечаний. Из анализа бесконечно малых известно, что всякая непрерывная функция $f(x)$ проходит все промежуточные значения между каждыми двумя значениями $f(a)$ и $f(b)$. Отсюда следует, что, если два значения $f(a)$ и $f(b)$ разных знаков, то между значениями a и b независимого переменного должно существовать значение c, при котором функция $f(x)$ обращается в нуль, т. е., другими словами, между числами a и b должен существовать корень уравнения $f(x) = 0$. На основании сказанного приходим к следующим двум теоремам.

Теорема I. *Всякое уравнение $f(x) = 0$ нечетной степени с вещественными коэффициентами должно иметь по крайней мере один вещественный корень.*

В самом деле, предполагая показатель n старшего члена нечетным, мы замечаем, что при достаточно больших положительных значениях x знак функции $f(x)$ совпадает с знаком коэффициента p_0, а при достаточно больших отрицательных значениях знак $f(x)$ обратный знаку коэффициента p_0. Будем обозначать через $f(+\infty)$ значение функции $f(x)$ при бесконечно больших положительных значениях, а через $f(-\infty)$ значение функции $f(x)$ при бесконечно больших по абсолютной величине отрицательных значениях независимого переменного. Тогда $f(+\infty)$ и $f(-\infty)$ будут разных знаков, и, значить, должен существовать по крайней мере один вещественный корень функции $f(x)$. Знак его обратный знаку p_n.

Теорема II. *Если крайние коэффициенты p_0 и p_n целой функции четной степени имеют разные знаки, то эта функция имеет по крайней мере один положительный и один отрицательный корень.*

Рассматривая три значения

$$f(-\infty), \quad f(0), \quad f(+\infty),$$

мы замечаем, что в данном случае $f(-\infty)$ и $f(+\infty)$ совпадают по знаку с коэффициентом p_0, а $f(0) = p_n$; следовательно уравнение $f(x) = 0$ должно иметь по крайней мере по одному корню в каждом из промежутков $(-\infty, 0)$ и $(0, +\infty)$.

Попарная сопряженность мнимых корней

§ 12

Теорема. *Если целая функция $f(x)$ с вещественными коэффициентами имеет корень $x = \alpha + \beta i$, то она должна также иметь и корень $x = \alpha - \beta i$.*

В самом деле, пусть

$$f(\alpha + \beta i) = 0;$$

разделяя функцию $f(x)$ на $(x-\alpha)^2 + \beta^2$, получим

$$f(x) = \{(x-\alpha)^2 + \beta^2\}Q(x) + mx + n.$$

Подставляя сюда $x = \alpha + \beta i$, получим

$$m(\alpha + \beta i) + n = 0,$$

откуда

$$m\alpha + n = 0, \qquad m\beta = 0.$$

Так как β не $= 0$, то $m = n = 0$, и функция $f(x)$ делится на

$$(x - \alpha - \beta i)(x - \alpha + \beta i);$$

отсюда мы замечаем, что число $\alpha - \beta i$ есть корень функции $f(x)$.

Легко видеть, что кратность корня $\alpha - \beta i$ будет та же, что и корня $\alpha + \beta i$, ибо равенства

$$f(\alpha + \beta i) = 0, \quad f'(\alpha + \beta i) = 0, \quad f''(\alpha + \beta i) = 0, \ \ldots$$

влекут за собою равенства

$$f(\alpha - \beta i) = 0, \quad f'(\alpha - \beta i) = 0, \quad f''(\alpha - \beta i) = 0, \ \ldots$$

Итак, мнимые корни входят в уравнение попарно; из этого следует, что уравнение нечетной степени должно иметь хоть один вещественный корень, что мы уже видели из других соображений.

Глава III

Об алгебраических функциях

Основные понятия

§ 1

Алгебраическим уравнением называется всякое уравнение вида

$$U = 0,$$

где U есть целая функция от ряда переменных $x, y, z, \ldots, u, v, \ldots$.

§ 2

Если выражение функции задано прямо через независимые переменные, то такая функция называется *явною*. Если же для получения выражения функции через независимые переменные нужно решить одно или несколько уравнений, то в таком случай функция называется *неявной*. Так, например, если функция v от двух переменных x и y задана уравнением

$$v^2 - 2xv - y^2 = 0,$$

то v будет, очевидно, неявной функцией. Эту неявную функцию мы обратим в явную, если решим уравнение относительно v. Получаем

$$v = x \pm \sqrt{x^2 + y^2}.$$

§ 3

Если функция может удовлетворять алгебраическому уравнению, связывающему ее с переменными независимыми, то она называется *алгебраической функцией*. В обратном случае она называется *трансцендентной*, т. е., другими словами, функция называется трансцендентною, если нельзя подобрать никакого алгебраического уравнения, которому эта функция удовлетворяет. Так, функция

$$v = x + \sqrt{x^2 + y^2}$$

есть алгебраическая, ибо она удовлетворяет алгебраическому уравнению

$$v^2 - 2xv - y^2 = 0.$$

Функция $v = \lg x$ есть функция трансцендентная, ибо не трудно показать, что она не может удовлетворять никакому алгебраическому уравнению.

§ 4

Алгебраические функции подразделяются на *рациональные* и *иррациональные*. Рациональной называется такая алгебраическая функция, которая удовлетворяет алгебраическому уравнение первой степени. Если же уравнение самой низкой степени, которому удовлетворяет алгебраическая функция, степени выше первой, то функцию называют иррациональною. Согласно этому определению всякая рациональная функция v должна удовлетворять уравнению вида

$$Qv - P = 0,$$

где Q и P целые функции независимых переменных. Можно всегда предполагать, что P и Q суть многочлены, не имеющие общих делителей, заключающих независимые переменные, ибо, если бы такой делитель существовал, то мы предварительно сократили бы на него все уравнение. Решая последнее уравнение относительно v, получим

$$v = \frac{P}{Q}.$$

Это показывает, что рациональная функция есть частное двух целых функций. В частном случае, если Q не будет содержать независимых переменных, то это Q будет некоторое постоянное число A, тогда

$$v = \frac{1}{A}P,$$

т. е. v представляешь собою целую функцию, и мы видим, что целая функция есть частный случай функции рациональной.

§ 5

Если уравнение, которому удовлетворяет иррациональная функция будет второй, третьей и четвертой степени, то мы можем его решить и найти явное выражение этой функции через переменные независимые. Когда уравнение выше четвертой степени, то задача приведения неявной функций в явную делается в общем случай невозможною и может решаться только в известных частных случаях.

Рассмотрим сначала алгебраическое решение уравнений 3-ей и 4-ой степени.

Решение уравнений 3-ей степени

§ 6

Мы рассмотрим способ Hudde'a. Сделаем два вспомогательных замечания.

Уравнение 3-ей степени можем рассматривать без члена с x^2, ибо во всяком уравнении n-ой степени *можно уничтожить член с* x^{n-1}. Покажем это; пусть дано уравнение

$$x^n + a_1 x^{n-1} + \ldots + a_{n-1}x + a_n = 0; \tag{1}$$

сделаем подстановку

$$x = y + \alpha,$$

где α пока остается неопределенным, тогда получим в левой части уравнения (1)

$$(y+\alpha)^n + a_1(y+\alpha)^{n-1} + \ldots + a_{n-1}(y+\alpha) + a_n = 0,$$

или

$$y^n + (n\alpha + a_1)y^{n-1} + \ldots = 0.$$

Чтобы в преобразованном уравнении пропал член с y^{n-1}, достаточно положить

$$n\alpha + a_1 = 0,$$

или

$$\alpha = -\frac{a_1}{n},$$

что всегда возможно.

Другое замечание состоит в том, что уравнение

$$x^3 - 1 = 0$$

имеет три корня

$$1, \quad \varepsilon = \frac{-1+\sqrt{-3}}{2}, \quad \varepsilon^2 = \frac{-1-\sqrt{-3}}{2},$$

что легко проверить.

§ 7

Возьмем кубическое уравнение в виде

(1) $$x^3 + px + q = 0.$$

Сделаем подстановку

$$x = u + v,$$

тогда уравнение (1) примет вид

$$u^3 + 3u^2v + 3uv^2 + v^3 + p(u+v) + q = 0,$$

или, вынося $u+v$ за скобку,

$$u^3 + v^3 + (u+v)(3uv+p) + q = 0.$$

Так как неизвестные величины u и v подчинены только одному условию, чтобы их сумма была x, то мы можем связать их еще вторым произвольным условием, например,

(2) $$3uv + p = 0.$$

Тогда уравнение примет вид

(3) $$u^3 + v^3 + q = 0.$$

Уравнения (2) и (3) решить легко, потому что они дают сумму и произведение количеств u^3 и v^3, именно

$$u^3 + v^3 = -q, \qquad u^3 v^3 = -\frac{p^3}{27}.$$

Итак, u^3 и v^3 суть корни квадратного уравнения

$$\xi^2 + q\xi - \frac{p^3}{27} = 0,$$

откуда

$$u^3 = -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}},$$

$$v^3 = -\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}},$$

следовательно

$$x = u + v = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}},$$

и мы получили формулу, носящую название *формулы Cardano*, итальянского математика 16-го столетия, претендовавшего на приоритет относительно решения уравнения 3-ей степени.

§ 8

Полученная формула Cardano дает все корни кубического уравнения. В самом деле, всякое число R имеет три значения кубического из этого числа корня, причем из одного из них получаются два других через умножение на ε и ε^2. Уравнение (2) показывает, что произведение uv радикалов $u = \sqrt[3]{R}$ и $v = \sqrt[3]{R_1}$ равно вещественному числу $-\frac{p}{3}$. Пусть два таких значения будут $\sqrt[3]{R}$ и $\sqrt[3]{R_1}$; тогда получим один из корней x_1 в виде

$$\alpha = \sqrt[3]{R} + \sqrt[3]{R_1}.$$

Остальные значения радикалов u и v будут $\varepsilon\sqrt[3]{R}$, $\varepsilon^2\sqrt[3]{R}$, $\varepsilon\sqrt[3]{R_1}$, $\varepsilon^2\sqrt[3]{R_1}$. Чтобы их произведения были вещественны, необходимо выбрать две следующие комбинации, дающие два остальных корня кубического уравнения

$$\alpha_1 = \varepsilon^2\sqrt[3]{R} + \varepsilon\sqrt[3]{R_1},$$

$$\alpha_2 = \varepsilon\sqrt[3]{R} + \varepsilon^2\sqrt[3]{R_1}.$$

§ 9

Исследуем, когда корни кубического уравнения будут вещественны.

Если

$$\frac{q^2}{4} + \frac{p^3}{27} > 0,$$

то оба числа R и R_1 будут вещественны и различны, следовательно, каждое из них имеет по одному вещественному кубическому корню. Обозначим эти корни через $\sqrt[3]{R}$ и $\sqrt[3]{R_1}$; следовательно, корень

$$\alpha = \sqrt[3]{R} + \sqrt[3]{R_1}$$

будет вещественный, а два других, очевидно, мнимые, ибо

$$(1)\qquad \begin{aligned} \alpha_1 &= \varepsilon^2\sqrt[3]{R} + \varepsilon\sqrt[3]{R_1} = -\frac{\sqrt[3]{R}+\sqrt[3]{R_1}}{2} - \frac{\sqrt[3]{R}-\sqrt[3]{R_1}}{2}\, i\sqrt{3}, \\ \alpha_2 &= \varepsilon\sqrt[3]{R} + \varepsilon^2\sqrt[3]{R_1} = -\frac{\sqrt[3]{R}+\sqrt[3]{R_1}}{2} - \frac{\sqrt[3]{R}-\sqrt[3]{R_1}}{2}\, i\sqrt{3}, \end{aligned}$$

где $i = \sqrt{-1}$; так как $\sqrt[3]{R}$ не $= \sqrt[3]{R_1}$, то мнимые члены не могут пропасть. Эти два корня, очевидно, сопряженные.

Если

$$\frac{q^2}{4} + \frac{p^3}{27} = 0,$$

то $\sqrt[3]{R} = \sqrt[3]{R_1} = \sqrt[3]{-\frac{q}{2}}$; два корня будут одинаковые, притом все три вещественные

$$\alpha = -2\sqrt[3]{\frac{q}{2}},$$
$$\alpha_1 = \alpha_2 = \sqrt[3]{\frac{q}{2}}.$$

Наконец, если

$$\frac{q^2}{4} + \frac{p^3}{27} < 0,$$

что возможно, очевидно, при $p < 0$, получаем все три корня вещественные, хотя радикал

$$\sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$$

мнимый. В этом случае два радикала $\sqrt[3]{R}$ и $\sqrt[3]{R_1}$ суть мнимые и сопряженные. Полагая

$$\sqrt[3]{R} = \lambda + i\mu,$$
$$\sqrt[3]{R_1} = \lambda - i\mu,$$

получим

$$\alpha = 2\lambda,$$

$$\alpha_1 = \varepsilon^2(\lambda + i\mu) + \varepsilon(\lambda - i\mu) = \frac{-1 - i\sqrt{3}}{2}(\lambda + i\mu) + \frac{-1 + i\sqrt{4}}{2}(\lambda - i\mu) = -\lambda + \mu\sqrt{3},$$

$$\alpha_2 = -\lambda - \mu\sqrt{3}.$$

Случай трех вещественных корней представляет одну замечательную особенность в формулах Cardano. А именно, хотя все три корня вещественны, но формулы Cardano представляют их в таком виде, что там фигурируют мнимости, ибо

корень квадратный, стоящий под кубическим корнем, мнимый. Если бы мы пожелали каждый из кубических корней $\sqrt[3]{R}$ и $\sqrt[3]{R_1}$ представить под видом $\lambda + i\mu$, то для определения чисел λ и μ мы получили бы кубичесие уравнения подобные заданному. Так, например, для определения λ получим уравнение, имеющее три вещественных корня, и, следовательно, выражение для λ будет опять заключать мнимость. Этот случай мы называем *неприводимым случаем* (casus irreductibilis).

§ 10

Введением тригонометрических величин возможно привести формулы Cardano к виду, удобному для логарифмирования, а также и в непрнводимом случае можно получить окончательную формулу для трех вещественных корней.

Действительно, при

$$\frac{q^2}{4} + \frac{p^3}{27} < 0,$$

если мы предположим

$$-\frac{q}{2} = \rho\cos\varphi, \qquad \frac{q^2}{4} + \frac{p^3}{27} = -\rho^2 sin^2\varphi,$$

то формулы Cardano примут вид

$$x = \sqrt[3]{\rho\cos\varphi + i\rho\sin\varphi} + \sqrt[3]{\rho\cos\varphi - i\rho\sin\varphi}.$$

По формуле Moivre'a имеем

$$x = \sqrt[3]{\rho}\left\{\cos\frac{\varphi+2k\pi}{3} + \sin\frac{\varphi+2k\pi}{3}\right\} + \sqrt[3]{\rho}\left\{\cos\frac{\varphi+2k\pi}{3} - i\sin\frac{\varphi+2k\pi}{3}\right\},$$

где числу k надо давать значения 0, 1, 2.

Получаем следующее выражения для трех корней уравнения

$$\alpha = 2\sqrt[3]{\rho}\cos\frac{\varphi}{3}$$
$$\alpha_1 = 2\sqrt[3]{\rho}\cos\left(\frac{\varphi}{3} + 120^\circ\right),$$
$$\alpha_2 = 2\sqrt[3]{\rho}\cos\left(\frac{\varphi}{3} + 240^\circ\right).$$

Для определения же ρ и φ (ρ величина существенно положительная) имеем выражения

$$\rho = \sqrt{-\frac{p^3}{27}}, \qquad \cos\varphi = -\frac{q}{2\rho}.$$

Дадим теперь для случая одного вещественного корня формулы, удобные для логарифмирования.

I случай.

$$\frac{q^2}{4} + \frac{p^3}{27} > 0, \qquad p < 0.$$

Положим

$$\sqrt{-\frac{p^3}{27}} = \frac{q}{2}\sin\omega,$$

тогда

$$\sqrt[3]{R} = \sqrt[3]{-\frac{q}{2} + \frac{q}{2}\cos\omega} = \sqrt[3]{-q\sin^2\frac{\omega}{2}}$$
$$\sqrt[3]{R_1} = \sqrt[3]{-\frac{q}{2} - \frac{q}{2}\cos\omega} = \sqrt[3]{-q\cos^2\frac{\omega}{2}}.$$

Подставляя вместо q его выражение через p, а именно

$$q = \frac{2}{\sin\omega}\sqrt{-\frac{p^3}{27}},$$

получим

$$\sqrt[3]{R} = -\sqrt{\frac{-p}{3}}\cdot\sqrt[3]{\operatorname{tg}\frac{\omega}{2}}$$
$$\sqrt[3]{R_1} = -\sqrt{\frac{-p}{3}}\cdot\sqrt[3]{\operatorname{ctg}\frac{\omega}{2}}.$$

Введем новый угол ψ так, что

$$\operatorname{tg}\psi = \sqrt[3]{\operatorname{tg}\frac{\omega}{2}},$$

и подставляя, получим

$$\sqrt[3]{R} = -\sqrt{-\frac{p}{3}}\cdot\operatorname{tg}\psi, \qquad \sqrt[3]{R_1} = -\sqrt{\frac{-p}{3}}\cdot\operatorname{ctg}\psi,$$

откуда

$$\alpha = -\sqrt{\frac{-p}{3}}\,\{\operatorname{tg}\psi + \operatorname{ctg}\psi\} = -2\sqrt{\frac{-p}{3}}\,\operatorname{cosec}2\psi.$$

II случай

$$\frac{q^2}{4} + \frac{p^3}{27} > 0, \qquad p > 0.$$

Тогда, полагая

$$\sqrt{\frac{p^3}{27}} = \frac{q}{2}\operatorname{tg}\theta,$$

получим

$$\sqrt[3]{R} = \sqrt[3]{\frac{q\sin^2\dfrac{\theta}{2}}{\cos\theta}}, \qquad \sqrt[3]{R_1} = \sqrt[3]{\frac{-q\cos^2\dfrac{\theta}{2}}{\cos\theta}},$$

или, вставив вместо q его значение

$$q = 2\operatorname{ctg}\theta\sqrt{\frac{p^3}{27}},$$

будем иметь

$$\sqrt[3]{R} = \sqrt{\frac{p}{3}}\cdot\sqrt[3]{\operatorname{tg}\frac{\theta}{2}}, \qquad \sqrt[3]{R_1} = \sqrt{\frac{p}{3}}\cdot\sqrt[3]{\operatorname{ctg}\frac{\theta}{2}}.$$

Вводя новый угол φ по уравнению

$$\operatorname{tg}\varphi = \sqrt[3]{\operatorname{tg}\frac{\theta}{2}},$$

получим выражения

$$\sqrt[3]{R} = \sqrt{\frac{p}{3}}\cdot\operatorname{tg}\varphi, \qquad \sqrt[3]{R_1} = -\sqrt{\frac{p}{3}}\cdot\operatorname{ctg}\varphi,$$

и, следовательно,

$$\alpha = -2\sqrt{\frac{p}{3}}\ \operatorname{ctg} 2\varphi.$$

Формулы для вычисления мнимых корней также получаются в удобном для логарифмирования виде; в самом деле, по формулам (1) § 9 получаем в I случае

$$\alpha_1, \alpha_2 = \sqrt{\frac{-p}{3}}\ \operatorname{cosec} 2\psi \pm i\sqrt{-p}\ \operatorname{ctg} 2\psi,$$

а во II случае

$$\alpha_1, \alpha_2 = \sqrt{\frac{p}{3}}\ \operatorname{ctg} 2\varphi \pm i\sqrt{p}\ \operatorname{cosec} 2\varphi.$$

Решение уравнений 4-ой степени

§ 11

Мы видели, что решение кубического уравнения приводится к решению квадратного; подобным же образом мы покажем, что решение уравнения 4-ой степени приводится к решению уравнения 3-ей степени.

Придадим нашему изложению геометрический характер. Возьмем самое общее уравнение 4-ой степени с вещественными коэффициентами

$$x^4 + ax^3 + bx^2 + cx + d = 0. \tag{1}$$

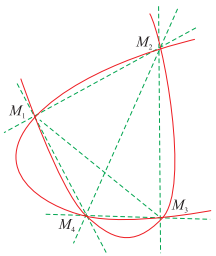
Полагая

$$y = x^2 \tag{2}$$

мы можем переписать уравнение (1) в таком виде

$$y^2 + axy + by + cx + d = 0. \tag{3}$$

Мы видим, что найти x, удовлетворяющий уравнение (1), все равно, что найти абсциссу точки встречи параболы $y = x^2$ с линией второго порядка, определяемой уравнением (3).



Черт. 3

Четыре корня уравнения 4-й степени (1) суть абсциссы четырех точек M_1, M_2, M_3, M_4 встречи двух линий (2) и (3). Рассмотрим пучок линий 2-го порядка, проходящих через точки встречи M_1, M_2, M_3, M_4 двух заданных линий (2) и (3).

Уравнение такого пучка будет

$$y^2 + axy + by + cx + d + \lambda(y - x^2) = 0. \tag{4}$$

Среди линий пучка (4) существует три системы прямых

$$(M_1M_2,\ M_3, M_4), \quad (M_1M_4,\ M_2, M_3) \ \text{ и } \ (M_1M_3, M_2, M_4).$$

Эти три системы мы получим, приравнивая нулю дискриминант второй степени (4). Это уравнение можно написать так

$$y^2 = \lambda x^2 + axy + cx + (b + \lambda)y + d = 0.$$

Условием приводимости линии (4) к системе двух прямых будет

$$\begin{vmatrix} -\lambda, & \frac{a}{2}, & \frac{c}{2} \\ \frac{a}{2}, & 1, & \frac{b+\lambda}{2} \\ \frac{c}{2}, & \frac{b+\lambda}{2}, & d \end{vmatrix} = 0;$$

раскрывая этот определитель, получим уравнение 3-ей степени

$$\lambda^3 + 2b\lambda^2 - \lambda(4d - ac - b^2) - a(da - cb) - c^2 = 0, \tag{5}$$

относительно λ. Мы уже видели, что уравнение 3-ей степени всегда имеет по крайней мере один вещественный корень; назовем его λ_0; подставляя его в уравнение пучка (4) и решая относительно y, получим два линейных выражения относительно x

$$\begin{gathered} y = \alpha x + \beta, \\ y = \alpha_1 x + \beta_1. \end{gathered} \tag{6}$$

Четыре корня уравнения (1) получаются, находя пересечение параболы $y = x^2$ с прямыми (6), т. е. решая два квадратных уравнения

$$x^2 - \alpha x - \beta = 0, \tag{7}$$

$$x^2 = \alpha_1 x - \beta_1 = 0. \tag{8}$$

Здесь мы получаем четыре корня, из которых два даются уравнением (7), а два уравнением (8).

Рассмотрим следующие случаи.

I случай:

$$\alpha^2 + 4\beta > 0, \qquad \alpha_1^2 + 4\beta_1 > 0.$$

Все четыре корня действительны, хотя корни уравнения (7) могут быть равны корням уравнения (8), и тогда получим число различных корней меньшее четырех.

II случай:

$$\alpha^2 + 4\beta < 0, \qquad \alpha_1^2 + 4\beta_1 > 0.$$

Два корня уравнения (7) мнимые сопряженные; два же других из уравнения (8) вещественны.

III случай:

$$\alpha^2 + 4\beta < 0, \qquad \alpha_1^2 + 4\beta_1 < 0.$$

Все четыре корня мнимые и попарно сопряженные.

§ 12

Поясним теорию примером. Пусть задано уравнение

$$x^4 - x^3 - 7x^2 + x + 6 = 0.$$

Уравнение (3) § 11 будет

$$y^2 - xy - 7y + x + 6 = 0;$$

уравнение пучка

$$\lambda(y - x^2) + y^2 - xy - 7y + x + 6 = 0.$$

Подбираем λ так, чтобы последнее уравнение давало две прямые; раскрывая дискриминант этого уравнения, получим уравнение

$$\lambda(\lambda^2 - 14\lambda + 24) = 0.$$

Достаточно взять один корень, например,

$$\lambda = 0.$$

Тогда уравнение пучка будет

$$y^2 - xy - 7y + x + 6 = 0;$$

решая его относительно y, получаем

$$y = \frac{x+7}{2} \pm \frac{\sqrt{x^2 + 10x + 25}}{2} = \frac{x+7}{2} \pm \frac{x+5}{2}.$$

Два уравнения прямых будут

$$y = x + 6, \qquad y = 1.$$

Два квадратных уравнения (7) и (8) § 16 будут в данном случае:

$$x^2 = 1, \qquad x^2 = x + 6.$$

Отсюда четыре искомых корня заданного уравнения (1) будут

$$x_1 = +1, \quad x_2 = -1, \quad x_3 = -2, \quad x_4 = 3.$$

§ 13

Покажем, еще один простой способ решения 4-ой степени. Пусть дано общее уравнение

$$x^4 + ax^3 + bx^2 + cx + d = 0. \tag{1}$$

Введем в рассмотрение

$$\left(x^2 + \frac{a}{2}x + y\right)^2 = x^4 + ax^3 + x^2\left(2y + \frac{a^2}{4}\right) + ayx + y^2, \tag{2}$$

где y пока некоторое неопределенное число. Прибавляя к обеим частям уравнения (1) соответственно обе части тождества (2), получим

$$\left(x^2 + \frac{a}{2}x + y\right)^2 = x^2A + xB + C,$$

где

$$A = 2y + \frac{a^2}{4} - b,$$
$$B = ay - c,$$
$$C = y^2 - d.$$

Определим A, B и C так, чтобы трехчлен, стоящий в правой части (3), был полным квадратом; для этого необходимо удовлетворить равенству

$$B^2 - 4AC = 0,$$

или, другими словами,

$$(a - yc)^2 - 4(y^2 - d)\left(2y + \frac{a^2}{4} - b\right) = 0.$$

Получилось уравнение 3-ей степени для определения y, которое есть, следовательно, резольвента заданного уравнении. Это уравнение имеет по крайней мере один действительный корень; обозначим его через y_0; определяя соответствующие y_0 значения A_0, B_0, C_0, получим

$$\left(x^2 + \frac{a}{2}x + y_0\right)^2 = (x\sqrt{A_0} + \sqrt{C_0})^2,$$

откуда получаем два уравнения

$$x^2 + \frac{a}{2}x + y_0 = x\sqrt{A_0} + \sqrt{C_0},$$
$$x^2 + \frac{a}{2}x + y_0 = -x\sqrt{A_0} - \sqrt{C_0}$$

для определения x; эти два уравнения и дадут четыре корня заданного уравнения (1).

Один пример уравнения, решаемого в радикалах

§ 14

Хотя уравнения выше четвертой степени не допускают общего решения в радикалах, тем не менее существуют многие случаи уравнений частного вида алгебраически разрешимых. Один из таких случаев мы здесь рассмотрим.

Возьмем целую функцию

$$f(x) = \cos n \arccos x, \tag{1}$$

где n целое число.

Для ее вычисления применим формулу Moivre'a

$$(\cos\omega + i\sin\omega)^n = \cos n\omega + i\sin n\omega.$$

Раскрывая по биному Newton'a, получим

$$\cos n\omega = \cos^n\omega - \frac{n(n-1)}{1\cdot 2}\cos^{n-2}\omega\sin^2\omega + \ldots =$$
$$= \cos n\omega - \frac{n(n-1)}{1\cdot 2}\cos^{n-2}\omega(1-\cos^2\omega) + \ldots$$

Полагая $\cos\omega = x$, получим

$$\cos n \arccos x = x^n - \frac{n(n-1)}{1\cdot 2}x^{n-2}(1-x^2) + \ldots$$

Так, например,

$$\cos 2 \arccos x = 2x^2 - 1.$$

Рассмотрим уравнение

$$\cos n \arccos x = a, \tag{1}$$

где a произвольная величина.

Решить уравнение (1), это все равно, что найти $x = \cos\omega$, если известен косинус кратного угла $a = \cos n\omega$.

Имеем

$$\cos n\omega + i\sin n\omega = a + i\sqrt{1-a^2},$$
$$(\cos\omega + i\sin\omega)^n = a + i\sqrt{1-a^2},$$
$$\cos\omega + i\sin\omega = \sqrt[n]{a + i\sqrt{1-a^2}};$$

изменяя знак при i, получим

$$\cos\omega - i\sin\omega = \sqrt[n]{a - i\sqrt{1-a^2}},$$

откуда окончательно

$$x = \cos\omega = \frac{1}{2}\left\{\sqrt[n]{a + i\sqrt{1-a^2}} + \sqrt[n]{a - i\sqrt{1-a^2}}\right\}.$$

§ 15

Невозможность обращения в явную алгебраических функций, определяемых уравнениями высших степеней, не помешала однако прогрессу теории алгебраических функций, пришлось только судить о свойствах алгебраических функций по тому алгебраическому уравнению, которому она удовлетворяет, совершенно независимо от того, умеем ли мы решить это уравнение или нет.

Первоначальным своим развитием теория алгебраических функций обязана геометрии, ибо алгебраическое уравнение вида $f(x, y) = 0$, где $f(x, y)$ есть целая функция от плоских декартовых координат x, y, определяет так называемую *алгебраическую линию* на плоскости, а уравнение $f(x, y, z) = 0$, где $f(x, y, z)$ — целая функция пространственных координат, определяет *алгебраическую поверхность* в пространстве.

Всякая наука при начальном своем состоянии интересуется обыкновенно задачами более конкретными, причем чаще всего задачами просто формулируемыми.

Когда простые задачи оказываются уже решенными и когда многие просто формулируемые задачи, но своевременно не решенные, оказываются в высший степени трудными, тогда начинается процесс, состоящий в углублении в теорию для изучения царствующих там законов. Это изучение сопровождается надеждой при более ясном представлении себе этих законов получить возможность решать задачи, казавшиеся ранее трудными.

Конечно, можно приветствовать направление науки, ставящее себе целью решать новые конкретные задачи и вопросы. Увеличение числа конкретных результатов обогащает в идейном отношении науку и делает ее более способной к решению новых задач.

Так именно было с теорией алгебраических функций. В начале она была теорией алгебраических линий и поверхностей. Геометрические образы ставили определенные аналитические задачи. Можно сказать, что и вообще при n переменных независимых алгебраическая функция соответствует некоторому геометрическому образу в пространстве $n+1$ измерений; конечно, непосредственная геометрическая интуиция прекращается уже после трех измерений.

Теорию алгебраических функций в ее чистом виде можно считать восходящей еще к Newton'у. Newton'у принадлежит способ изучать алгебраическую функцию при помощи ее разложения в бесконечные ряды. Можно сказать, что этот способ проходит красною нитью через всю дальнейшую историю науки до последнего времени. Известен особенный прием, помогающий разложению в ряды и носящий название *параллелограмма Newton'a*.

Дальнейшая история науки дала только один серьезный толчок в этом направлении, а именно, введение в рассмотрение комплексных значений независимым переменным, тогда как прежде под влиянием геометрических задач рассматривались лишь вещественные числа.

Введение чисел комплексных помогло приведению в порядок теории функций алгебраических.

Задачи вычислительного характера, а также задачи доказательства различных свойств вещественных алгебраических линий и поверхностей заменяются за-

дачами изучения свойств алгебраических функций. В 19-м столетии были два обстоятельства давшие громадный толчок в деле развитая теории алгебраических функций, эти два обстоятельства суть: теорема Abel'a и прогресс теории чисел.

Abel'ю принадлежит замечательная теорема интегрального исчисления, в которой участвуют алгебраические функции. Теорема Abel'a дала путь к большим новым догадкам. Была создана теория новых трансцендентных функций, которым было присвоено название *абелевых*. Алгебраические функции оказались так тесно связанными с абелевыми, что считалось почти обязательным параллельное их изучение. Главное значение абелевых функций состоит в обобщении теории *эллиптических* функций, представляющей славу математики 19-го столетия.

Новый идейный толчок в теории алгебраических функций относится к самому последнему времени и исходить из теории чисел.

§ 16

Остановимся несколько подробнее на влиянии теории чисел. Естественным явилось введение в науку понятия о числах алгебраических.

Алгебраической *функцией* называется корень уравнения

$$a_0x^n + a_1x^{n-1} + a_2x^{n-2} + \ldots + a_{n-1}x + a_n = 0, \tag{1}$$

в котором коэффициенты $a_0, a_1, a_2, \ldots, a_n$ суть целые *функции* от независимых переменных.

Алгебраическим числом называется корень уравнения (1), если коэффициенты $a_0, a_1, a_2, \ldots, a_n$ суть *целые числа* (взятые со знакомь + или − натуральный числа).

Если число не удовлетворяет никакому уравнению (1) с целыми коэффициентами, то оно называется *трансцендентными*.

Доказать, что постоянное число есть трансцендентное, гораздо труднее, чем доказать трансцендентность функций. Лишь во второй половине 19-го столетия удалось доказать трансцендентность чисел e (основание Neper'овых логарифмов) и π (отношение окружности к диаметру).

Трансцендентность числа π показала с очевидностью невозможность квадратуры круга.

Изучение алгебраических чисел дает путь к выяснению вопроса о возможности построения циркулем и линейкой той или другой задачи, в чем может видеть пользу их любитель конкретных задач.

Я же лично вижу пользу изучения алгебраических чисел главным образом в тех грандиозных обобщениях, которые достижимы в теории чисел, и которые были начаты в книге Gauss'a «Disqiiisitiones arithmeticae».

Развитие теории алгебраических чисел в 19-м столетии привело к открытию первостепенной важности, к открытие новых чисел, названных *идеальными*, или *идеалами*.

Явилось стремление перенести блестящие результаты, достигнутые в теории алгебраических чисел на теории функций алгебраических. Это течение только что началось благодаря исследованиям Dedekind'a и Weber'a, двух первоклассных знатоков теории идеалов.

§ 17

Из всего сказанного читатель поймет, что теория алгебраических функций есть обширная часть современной математики, имеющая богатую литературу. Можно порекомендовать, как хороший очерк этой литературы, статью A. Brill'a и M. Noeter'a под заглавием «Die Entwicklung der Theorie der algebraischen Funktttionen in älterer und neuerer Zeit», помещенную в 111 томе Jahresbericht der deutschen Mathematiker Vereinigund. 1894. В этом очерке не затронуто новое направление Dedekind'a и Weber'a. Чтобы скорее познакомиться с ним можно порекомендовать конец третьего тома «Lehrbuch der Algebra» Weber'a и большое сочинение «Theorie der algebraischen Funktionen einer Variablen» von K. Hensel und G. Landsberg.

От сближения теории алгебраических чисел и функций выиграла также теория чисел, ибо разложено функций в ряды навело Hensel'a на открытие так называемых *p-адических* чисел.

Несмотря на то, что эти числа встречены несколько холодно математиками, я продолжаю придавать им значение, особенно после последней книги Hensel'a «Zahlentheorie» 1913.

Теория алгебраических чисел не может входить, конечно, в программу моей книги, тем не менее я не считаю возможным умолчать о некоторых результатах, относящихся к алгебраическим функциям.

Рациональные функции

§ 18

Ограничимся рассмотрением рациональных функций от одной независимой переменной

$$\frac{f(x)}{F(x)},$$

где $f(x)$ и $F(x)$ целые функции.

Мы ограничимся рассмотрением следующих двух основных свойств рациональных функций:

1° разложение рациональных функций на простейшие дроби,

2° разложение рациональных функций в, так называемые, *возвратные* ряды.

Разложение рациональных функций на простейшие дроби

§ 19

Относительно разложения рациональных функций на простейшие достаточно обратить внимание на следующую общую теорему.

Если знаменатель $F(x)$ рациональной функции может быть представлен в виде

$$F(x) = \{\Phi(x)\}^m\{\Psi(x)\}^n \cdots \{\Omega(x)\}^p,$$

где

$$\Phi(x), \quad \Psi(x), \ \ldots, \ \Omega(x)$$

целые функции, то будет всегда существовать следующее тождество

$$\frac{f(x)}{F(x)} = \Pi(x) \quad + \frac{\varphi_1(x)}{\{\Phi(x)\}^m} + \frac{\varphi_2(x)}{\{\Phi(x)\}^{m-1}} + \ldots + \frac{\varphi_m(x)}{\Phi(x)} +$$
$$+ \frac{\psi_1(x)}{\{\Psi(x)\}^n} + \frac{\psi_2(x)}{\{\Psi(x)\}^{n-1}} + \ldots + \frac{\psi_m(x)}{\Psi(x)} +$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$+ \frac{\omega_1(x)}{\{\Omega(x)\}^p} + \frac{\omega_2(x)}{\{\Omega(x)\}^{p-1}} + \ldots + \frac{\omega_p(x)}{\Omega(x)},$$

где $\Pi(x)$ *есть некоторая целая функция, и все числители* φ, ψ, ω, *суть также целые функции, причем степени функций* $\varphi_1(x), \varphi_2(x), \ldots, \varphi_m(x)$ *ниже степени* $\Phi(x)$, *степени функций* $\psi_1(x), \psi_2(x), \ldots, \psi_n(x)$ *ниже степени функций* $\Psi(x)$ *и т. д., наконец, степени функций* $\omega_1(x), \omega_2(x), \ldots, \omega_p(x)$ *ниже степени* $\Omega(x)$.

Разложение это совершается одним только способом и представляет из себя то, что называют обыкновенно разложением рациональной функции на простейшие дроби.

Мы не будем рассматривать теорему в высказанном общем виде, а ограничимся наиболее важными в приложениях случаями, когда все функции

$$\Phi(x), \quad \Psi(x), \ \ldots, \ \Omega(x)$$

не выше второй степени, т. е. или 1-ой, или 2-ой. Рассуждения об этих более простых случаях теоремы мы поведем таким образом, чтобы из этих рассуждений непосредственно вытекала справедливость теоремы в общем случае.

§ 20

Предположим, что знаменатель $F(x)$ рациональной дроби имеет такой вид

$$F(x) = (x-a)^m F_1(x),$$

причем функция $F_1(x)$ не делится уже на $x-a$. Покажем, что в этом случае существует тождество

$$\frac{f(x)}{F(x)} = \frac{A}{(x-a)^m} + \frac{f_1(x)}{(x-a)^{m-1}F_1(x)}, \tag{1}$$

где A постоянное число, а $f_1(x)$ некоторая целая функция.

В самом деле, рассмотрим разность

$$\frac{f(x)}{F(x)} - \frac{A}{(x-a)^m} = \frac{f(x) - AF_1(x)}{(x-a)^m F_1(x)}.$$

Покажем. что коэффициент A можно будет подобрать таким образом, чтобы числитель $f(x) - AF_1(x)$ делился на $x-a$. Для этого заметим, что, если некоторая целая функция делится на $x-a$, то она должна обращаться в нуль при подстановка $x=a$, и мы получаем

$$f(a) - AF_1(a) = 0. \tag{2}$$

Нетрудно убедиться, что не равны нулю $f(a)$ и $F(a)$. В самом деле, не может равняться нулю $F_1(a)$, ибо мы предположили, что функция $F_1(x)$ не делится на $x-a$; совершенно подобным образом мы должны считать отличным от нуля $f(a)$, ибо предположение, что $f(x)$ делится на $x-a$ имело бы следствием, что заданная рациональная дробь сокращается на $x-a$, а, понятно, мы имеем право предполагать заданную дробь несократимой.

Итак, уравнение (2) дает для коэффициента A следующее отличное от нуля и бесконечности значение

$$A=\frac{f(a)}{F_1(a)}, \tag{3}$$

при котором целая функция

$$f(x)-AF_1(x) \tag{4}$$

будет целиться нацело на $x-a$ тогда можно будет написать

$$f(x)-AF_1(x)=(x-a)f_1(x),$$

где знаком $f_1(x)$ обозначено частное от деления функций (4) на ее $x-a$. Отсюда разделяя на $F(x)$ и получим тождество (1).

Например, из дроби

$$\frac{x^2+3}{(x+1)^3(x^2-2x-2)}$$

можно будет выделить часть вида

$$\frac{A}{(x+1)^3},$$

причем останется выражение вида

$$\frac{f_1(x)}{(x+1)^2(x^2-2x-2)}.$$

Мы замечам, что в данном случай

$$f(x)=x^2+3, \qquad F_1(x)=x^2-2x-2.$$

Требуется подобрать A таким образом, чтобы выражение

$$x^2+3-A(x^2-2x-2) \tag{5}$$

делилось на $x+1$. Подставляя в (5) $x=-1$, получим $A=4$.

После подстановки $A=4$ в выражение (5) получим функцию

$$-3x^2+8x+11,$$

делящуюся нацело на $x+1$

$$\begin{array}{r|l} -3x^2+8x+11 & x+1 \\ \cline{2-2} -3x^2-3x & -3x+11 \\ \cline{1-1} \quad 11x+11 & \\ \quad 11x+11 & \\ \cline{1-1} \quad 0 & \end{array}$$

так что

$$f_1(x) = -3x + 11.$$

Итак, получаем тождество

$$\frac{x^2+3}{(x+1)^3(x^2-2x-2)} = \frac{4}{(x+1)^3} + \frac{-3x+11}{(x+1)^2(x^2-2x-2)}.$$

§ 21

На основании соображений предыдущего параграфа мы замечаем, что получается следующее разложение рациональной функции предыдущего параграфа

$$\frac{f(x)}{F(x)} = \frac{A}{(x-a)^m} + \frac{A_1}{(x-a)^{m-1}} + \ldots + \frac{A_{m-1}}{(x-a)} + \frac{\varphi(x)}{F_1(x)}. \tag{1}$$

Разлагая функцию $F_1(x)$ на линейные множители, получим

$$F_1(x) = (x-b)^n \cdots (x-l)^p,$$

откуда, применяя те же рассуждения, получим следующее окончательное разложение функции

$$\begin{aligned} \frac{f(x)}{F(x)} &= \frac{A}{(x-a)^m} + \frac{A_1}{(x-a)^{m-1}} + \ldots + \frac{A_{m-1}}{(x-a)} + \\ &= \frac{B}{(x-b)^n} + \frac{B_1}{(x-b)^{n-1}} + \ldots + \frac{B_{n-1}}{(x-b)} + \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ &= \frac{L}{(x-l)^p} + \frac{L_1}{(x-l)^{p-1}} + \ldots + \frac{L_{m-1}}{(x-l)} + \quad \Pi(x), \end{aligned} \tag{2}$$

представляющее из себя частный случай общей теоремы § 19, а именно тот случай, когда

$$\Phi(x) = x - a, \quad \Psi(x) = x - b, \quad \ldots, \quad \Omega(x) = x - l.$$

§ 22

Хотя соображения § 20 достаточны для вычисления всех коэффициентов

$$A,\ A_1,\ \ldots,\quad B,\ B_1,\ \ldots,\quad \ldots,\quad L,\ L_1,\ \ldots,$$

но мы укажем еще один способ вычисления этих коэффициентов, очень удобный на практике. Мы назовем этот способ *способом деления*.

Подставим в формулу (1) § 4 новую переменную z, определяемую равенством

$$x = a + z$$

тогда получаем

$$\frac{f(a+z)}{F(a+z)} = \frac{A}{z^m} + \frac{A_1}{z^{m-1}} + \ldots + \frac{A_{m-1}}{z} + \frac{\varphi(a+z)}{F_1(a+z)}.$$

Но на основании равенства

$$F(x) = (x-a)^m F_1(z)$$

получаем

$$F(a+z) = z^m F_1(a+z),$$

следовательно,

$$(1) \qquad f(a+z) = (A + A_1 z + A_2 z^2 + \ldots + A_{m-1} z^{m-1}) F_1(a+z) + z^m \varphi(a+z).$$

Последнее тождество показывает, что полином

$$(2) \qquad A + A_1 z + A_2 z^2 + \ldots + A_{m-1} z^{m-1}$$

может быть найден алгебраическим делением полинома $f(a+z)$ на полином $F_1(a+z)$, причем остатком от такого деления должно быть выражение

$$z^m \varphi(a+z).$$

Способ получения полинома (2) при помощи алгебраического деления настолько прост, что его достаточно пояснить на одном примере.

Пусть дана рациональная дробь

$$\frac{x^2+3}{(x+1)^3(x^2-2x-2)}.$$

Полагая $x+1=z$ или $x=-1+z$, получим

$$f(x) = x^2+3 = (-1+z)^2+3 = 4-2z+z^2$$
$$F_1(x) = x^2-2x-2 = (-1+z^2)^2 - 2(-1+z) - 2 = 1-4z+z^2.$$

Будем делить теперь выражение $4-2z+z^2$ на выражение $1-4z+z^2$, причем оба выражения будем предполагать расположенными по возрастающим степеням буквы z; тогда наибольшие степени остатков будут возрастать. В самом деле,

$$\begin{array}{l|l}
4 \;\; -2z \;\; +z^2 & 1-4z+z^2 \\
\cline{2-2}
4 \;\; -16z \;\; +4z^2 & 4+14z+53z^2 \\
\cline{1-1}
\quad 14z \;\; -3z^2 & \\
\quad 14z \;\; -56z^2 \;\; -14z^3 & \\
\cline{1-1}
\qquad\qquad 53z^2 \;\; -14z^3 & \\
\qquad\qquad 53z^2 \;\; -212z^3 \;\; +53z^4 & \\
\cline{1-1}
\qquad\qquad\qquad\quad 198z^3 \;\; -53z^4 &
\end{array}$$

Итак, мы видим, что в нашем случай полином $A + A_1 z + A_2 z^2 + \ldots$ есть не что иное как

$$4 + 14z + 53z^2,$$

а остаток $z^m \varphi(a+z)$ есть

$$z^3(198 - 53z),$$

и, значит, $\varphi(a+z) = 198 - 53z$ и

$$\varphi(x) = 198 - 53(x+1) = 145 - 53x.$$

Итак, получаем разложение

$$\frac{x^2+3}{(x+1)^3(x^2-2x-2)} = \frac{4}{(x+1)^3} + \frac{14}{(x+1)^2} + \frac{53}{x+1} + \frac{245-53x}{x^2-2x-2}.$$

§ 23

Особого внимания заслуживает случай, когда все корни знаменателя $F(x)$ простые, т. е., когда $m = 1$, $n = 1$, ... , $p = 1$, и мы имеем

$$F(x) = (x-a)(x-b)\cdots(x-l). \tag{1}$$

Формула разложения принимает вид

$$\frac{f(x)}{F(x)} = \Pi(x) + \frac{A}{x-a} + \frac{B}{x-b} + \ldots + \frac{L}{x-l} \tag{2}$$

Пусть степень знаменателя $F(x)$ будет n. Введем в рассмотрение целые функции $n-1$ степени

$$\frac{F(x)}{x-a} = F_1(x), \quad \frac{F(x)}{x-b} = F_2(x), \quad \ldots, \quad \frac{F(x)}{x-l} = F_n(x).$$

Тогда умножая на $F(x)$ равенство (2), получим

$$f(x) = \Pi(x)\cdot F(x) + \Omega(x), \tag{3}$$

где $\Omega(x)$ есть целая функция не выше $n-1$, потому что ее выражение есть

$$AF_1(x) + BF_2(x) + \ldots + LF_n(x).$$

Равенство (3) показывает, что целая функция $\Pi(x)$ есть частное от деления $f(x)$ на $F(x)$, а $\Omega(x)$ есть остаток от этого деления и мы получаем

$$\frac{\Omega(x)}{F(x)} = \frac{A}{x-a} + \frac{B}{x-b} + \ldots + \frac{L}{x-l}. \tag{4}$$

Обратим внимание на формулу (4). Это есть формула, предложенная Lagrange'ем для теории интерполирования и потому называется *интерполяцгонной формулой Lagrange'a.*

Lagrange показал хороший способ вычисления коэффиц1ентов $A, B, \ldots, L$. В самом деле, умножая обе части равенства (4) на $x-a$, мы получим

$$\frac{\Omega(x)}{(x-b)(x-c)\cdots(x-l)} = A + (x-a)\left\{\frac{B}{x-b} + \ldots + \frac{L}{x-l}\right\};$$

подставляя $x = a$, получаем

$$\frac{\Omega(a)}{(a-b)(a-c)\cdots(a-l)} = A.$$

Подобным же образом

$$\frac{\Omega(b)}{(b-a)(b-c)\cdots(b-l)} = B, \ \ldots, \ \frac{\Omega(l)}{(l-a)(l-c)\cdots} = L.$$

Покажем еще другой способ вычисления коэффициентов, разлагая знаменатель функции по формуле Tailor'a. Получаем

$$F(x) = F(a) + (x-a)F'(a) + \frac{(x-a)^2}{1\cdot 2}F''(a) + \ldots$$

Так как a есть один из корней знаменателя, то будет иметь место равенство

$$F(a) = 0,$$

и мы получаем

$$\frac{F(x)}{x-a} = F'(a) + \frac{x-a}{1\cdot 2}F''(a) + \ldots,$$

или иначе

$$F_1(x) = F'(a) + \frac{x-a}{1\cdot 2}F''(a) + \ldots$$

Подставляя в последнее тождество $a = a$, получим

$$F_1(a) = F'(a).$$

Подобным образом получим

$$F_2(b) = F'(b), \quad \ldots, \quad F_n(l) = F''(l),$$

и мы получаем

$$A = \frac{\Omega(a)}{F_1(a)} = \frac{\Omega(a)}{F'(a)}, \quad B = \frac{\Omega(b)}{F'(b)}, \quad \ldots, \quad L = \frac{\Omega(l)}{F'(l)}.$$

Таким образом формулу Lagrange'a можно переписать так

$$\frac{\Omega(x)}{F(x)} = \sum \frac{\Omega(\alpha)}{F'(\alpha)} \cdot \frac{1}{x-\alpha}.$$

где $\sum$ распространяется на все корни α знаменателя $F(x)$.

§ 24

Выведенное в § 21 разложение рациональной дроби на простейшие представляет на практике неудобство, состоящее в том что некоторые из корней знаменателя могут оказаться мнимыми. Чтобы избежать введения мнимости, покажем другой способ разложения дробей на простейшие. Мы видели уже, что мнимые корни целых функций с вещественными коэффициентами входят попарно, причем всякому

корню $\alpha+\beta i$ соответствует корень $\alpha-\beta i$, и сама функция делится на квадратное выражение вида

$$(x-\alpha)^2+\beta^2.$$

Поэтому, если мы желаем ограничиться рассмотрением чисел вещественных, то можно знаменателя $F(x)$ разложить на линейных и квадратных множителей следующим образом

$$F(x)=(x-a)^{m_1}(x-b)^{n_1}\cdots(x-l)^{p_1}(x^2+px+q)^m\ldots(x^2+tx+u)^p,$$

где все числа

$$a,\ b,\ \ldots,\ p,\ q,\ r,\ \ldots,\ s,\ t,\ u$$

вещественные, а трехчлены

$$x^2+px+q, x^2+rx+s,\ \ldots,\ x^2+tx+u$$

не имеют вещественных корней.

Пусть

$$F(x)=(x^2+px+q)^mF_1(x).$$

Докажем следующее предложение.

Предполагая, что функция $F_1(x)$ не имеет общих корней с трехчленом

$$x^2+px+q$$

можно всегда подобрать два числа P и Q и целую функцию $\varphi(x)$, чтобы было

$$\frac{f(x)}{F(x)}=\frac{Px+Q}{(x^2+px+q)^m}+\frac{\varphi(x)}{(x^2+px+q)^{m-1}F_1(x)}.$$

Для доказательства высказанной теоремы воспользуемся следующим тождеством

$$\frac{f(x)}{F(x)}-\frac{Px+Q}{(x^2+px+q)^m}=\frac{f(x)-(Px+Q)F_1(x)}{(x^2+px+q)^mF_1(x)}=\frac{\dfrac{f(x)-(Px+Q)F_1(x)}{x^2+px+q}}{(x^2+px+q)^{m-1}F_1(x)},$$

из которого мы получаем для искомой функции $\varphi(x)$ выражение

$$\varphi(x)=\frac{f(x)-(Px+Q)F_1(x)}{x^2+px+q}. \tag{1}$$

Последнее выражение будет дробным при всевозможных численных значениях P и Q за исключением одной системы численных значений, которую мы сейчас получим. Итак, поставим себе задачею подобрать числа P и Q таким образом, чтобы выражение (1) было функцией целой. Для облегчения задачи разделим предварительно функции $f(x)$ и $F_1(x)$ на квадратное выражение

$$x^2+px+q;$$

пусть частные, полученные от деления будут $\psi(x)$ и $\omega(x)$, а остатки

$$\alpha x+\beta \quad \text{и} \quad \gamma x+\delta,$$

так что

$$f(x) = \psi(x)(x^2 + px + q) + \alpha x + \beta,$$
$$F_1(x) = \omega(x)(x^2 + px + q) + \gamma x + \delta. \tag{2}$$

На основании последних равенств выражение (1) можно представить так:

$$\varphi(x) = \psi(x) - (Px + Q)\omega(x) + \frac{\alpha x + \beta - (Px + Q)(\gamma x + \delta)}{x^2 + px + q}.$$

Производя деление, получим

$$\begin{array}{l|l} -P\gamma x^2 + (\alpha - P\delta - Q\gamma)x + \beta - Q\delta & x^2 + px + q \\ \underline{-P\gamma x^2 - Pp\gamma x - P\gamma q} & \underline{-P\gamma} \\ (\alpha - P\delta - Q\gamma + Pp\gamma)x + \beta - Q\delta + P\gamma q & \end{array}$$

чтобы деление совершилось нацело, т. е., чтобы функция ?, как мы желаем, была целой, необходимо и достаточно, чтобы остаток от последнего деления тождественно равнялся нулю, и мы получаем следующих два уравнения

$$\begin{array}{rcrcl} & P(\delta - \gamma p) & + & Q\gamma & = & \alpha, \\ - & P\gamma q & + & Q\delta & = & \beta \end{array} \tag{3}$$

для определения P и Q. Покажем, что систему (3) всегда можно решить относительно P и Q; для этой цели достаточно показать, что определитель

$$\begin{vmatrix} \delta - \gamma p, & \gamma \\ -\gamma q, & \delta \end{vmatrix} = \delta^2 - \gamma\delta p + \gamma^2 q$$

отличен от нуля. В самом деде, так как целая функция $F_1(x)$, по предположение, не делится на $x^2 + px + q$, то, значить, остаток $\gamma x + \delta$ не может тождественно равняться нулю, т. е. не могут обращаться в нуль два числа γ и δ.

1°. $\gamma = 0$

Тогда δ не должно равняться нулю, а тем самым окажется отличным от нуля и выражение

$$\delta^2 - \gamma\delta p + \gamma^2 q.$$

2°. γ не $= 0$.

Если мы допустим что будет

$$\delta^2 - \gamma\delta p + \gamma^2 q = 0, \tag{4}$$

то придем к противоречию с поставленными в теорем условиями; в самом деле, равенство (4) может быть переписано так

$$\left(-\frac{\delta}{\gamma}\right)^2 + p\left(-\frac{\delta}{\gamma}\right) + q = 0,$$

и, следовательно, число $-\dfrac{\delta}{\gamma}$ оказывается корнем трехчлена $x^2 + px + q$, а тогда, подставляя во второе из уравнение (2) $x = -\dfrac{\delta}{\gamma}$, получим

$$F_1\left(-\frac{\delta}{\gamma}\right) = \omega\left(-\frac{\delta}{\gamma}\right)\left\{\left(-\frac{\delta}{\gamma}\right)^2 + p\left(-\frac{\delta}{\gamma}\right) + q\right\} + \gamma\left(-\frac{\delta}{\gamma}\right) + \delta;$$

в правой части получается тождественно нуль, и, значит, $F_1(x)$ имеет общий корень $-\dfrac{\delta}{\gamma}$ с трехчленом x^2+px+q, что противоречит предположению.

Итак, система (3) допускает определенное решение относительно неизвестных P и Q; так что устанавливается возможность одним только способом выделить из дроби

$$\frac{f(x)}{(x^2+px+q)^m F_1(x)}$$

простейшую дробь

$$\frac{Px+Q}{(x^2+px+q)^m},$$

причем остается дробь

$$\frac{\varphi(x)}{(x^2+px+q)^{m-1}F_1(x)},$$

где $\varphi(x)$ целая функция.

Рассмотрим численный пример:

$$\frac{3x^3+1}{(x^2+10^2)(x-1)} = \frac{Px+Q}{(x^2+1)^2} + \frac{\varphi(x)}{(x^2+1)(x-1)}.$$

Согласно теории надо подобрать P и Q таким образом, чтобы

$$3x^3+1-(Px+Q)(x-1)$$

делилось нацело на x^2+1. Произведем на самом деле деление

$$\begin{array}{l|l}
3x^3 - Px^2 + (P-Q)x + Q + 1 & x^2+ \\
\cline{2-2}
3x^2 \qquad\qquad + 3x & 3x - P \\
\cline{1-1}
\quad - Px^2 \quad + (P-Q-3)x \quad + Q + 1 & \\
\quad - Px^2 \qquad\qquad\quad - P & \\
\cline{1-1}
\qquad\qquad (P-Q-3)x \quad + Q + P + 1 &
\end{array}$$

Приравнивая нулю коэффициенты остатка, получим два уравнения

$$P-Q-3=0$$

$$P+Q+1=0,$$

откуда

$$P=1, \qquad Q=-2.$$

Отсюда

$$\varphi(x) = 3x - P = 3x-1,$$

и мы получаем окончательно следующее разложение

$$\frac{3x^3+1}{(x^2+1)^2(x-1)} = \frac{x-2}{(x^2+1)^2} + \frac{3x-1}{(x^2+1)(x-1)}$$

на простейшие дроби.

§ 25

Указанное в предыдущем параграфе приведение дробей к простейшей дроби приводит к следующему окончательному виду разложения дроби на простейшие.

Теорема. *Если*

$$F(x) = (x^2+px+q)^m(x^2+rx+s)^n\cdots(x^2+tx+u)^p\cdot(x-a)^{m_1}(x-b)^{n_1}\cdots(x-l)^{p_1},$$

то

$$\begin{aligned}\frac{f(x)}{F(x)} = \Pi(x) &+ \frac{Px+Q}{(x^2+px+q)^m} + \frac{P_1x+Q_1}{(x^2+px+q)^{m-1}} + \ldots + \frac{P_{m-1}x+Q_{m-1}}{x^2+px+q} +\\ &+ \frac{Rx+S}{(x^2+rx+s)^n} + \frac{R_1x+S_1}{(x^2+rx+s)^{n-1}} + \ldots + \frac{R_{n-1}x+S_{n-1}}{x^2+rx+s} +\\ &+ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots +\\ &+ \frac{Tx+Y}{(x^2+tx+u)^p} + \frac{T_1x+Y_1}{(x^2+tx+s)^{p-1}} + \ldots + \frac{T_{p-1}x+S_{p-1}}{x^2+tx+u} +\\ &+ \frac{A}{(x-a)^{m_1}} + \frac{A_1}{(x-a)^{m_1-1}} + \ldots + \frac{A_{m_1-1}}{x-a} +\\ &+ \frac{B}{(x-b)^{n_1}} + \frac{B_1}{(x-b)^{n_1-1}} + \ldots + \frac{B_{n_1-1}}{x-a} +\\ &+ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots +\\ &+ \frac{L}{(x-l)^{p_1}} + \frac{L_1}{(x-l)^{p_1-1}} + \ldots + \frac{L_{p_1-1}}{x-a},\end{aligned}$$

где $\Pi(x)$ *есть целая часть, заключающаяся в рациональной дроби.*

Связь рациональных функций с возвратными рядами

§ 26

Скажем несколько слов о разложении функций в ряды по степеням x. Предположим, что имеется следующее разложение рациональной функции

$$\frac{f(x)}{F(x)} = a_0 + a_1x + a_2x^2 + \ldots + a_nx^n + \ldots \tag{1}$$

Для возможности этого разложения необходимо во первых, чтобы рациональная дробь не обращалась в ∞ при $x=0$, а чтобы было

$$\frac{f(0)}{F(0)} = a_0,$$

где a_0 некоторое определенное число; во вторых разложение (1) будет иметь всегда место для таких значений x, модули которых не превосходят некоторого определенного числа.

Умножая тождество (1) на знаменателя

$$F(x) = p_0x^n + p_1x^{n-1} + \ldots + p_{n-1}x + p_n,$$

получим

$$f(x) = A_0 + A_1 x + A_2 x^2 + \ldots + A_m x^m + \ldots \tag{2}$$

Нетрудно убедиться, что при $m \geq n$ коэффициент A_m будет определяться по формуле

$$A_m = a_m p_n + a_{m-1} p_{n-1} + \ldots + a_{m-n} p_0.$$

Так как в тождестве (2) в первой части находится целая функция $f(x)$, а во второй части бесконечный ряд, то, значит, все коэффициенты бесконечного ряда, начиная с известного места, должны тождественно равняться нулю. Итак, начиная с некоторого числа m и для всех больших n

$$a_m p_n + a_{m-1} p_{n-1} + \ldots + a_{m-n} p_0. \tag{3}$$

Такие ряды, между коэффициентами которых, начиная с известного места, имеет место соотношение вида (3), называются возвратными или рекуррентными, и мы приходим к теореме.

Теорема. *Рациональные функции раскладываются в возвратные ряды, и обратно, всякий возвратный ряд имеет своей суммой рациональную функцию.*

§ 27

Поясним сказанное примером. Рассмотрим ряд

$$1 + x\cos\alpha + x^2\cos 2\alpha + \ldots + x^n \cos n\alpha + \ldots$$

Нетрудно убедиться, что этот ряд возвратный, потому что

$$\cos n\alpha + \cos(n-2)\alpha = 2\cos(n-1)\alpha\cos\alpha.$$

Итак, если обозначим

$$a_n = \cos n\alpha,$$

то между коэффициентами заданного ряда получаем следующее возвратное соотношение

$$a_n + a_{n-2} = 2a_{n-1}\cos\alpha,$$

или иначе

$$a_n - 2a_{n-1}\cos\alpha + a_{n-2} = 0.$$

Чтобы найти сумму заданного ряда, мы будем, следуя изложенной теории, умножать наш ряд на полином

$$x^2 - 2x\cos\alpha + 1.$$

Получаем

$$\begin{array}{l} 1 + x\cos\alpha + x^2\cos 2\alpha + \ldots \\ \underline{1 - 2x\cos\alpha + x^2} \\ 1 - x\cos\alpha + 0x^2 + 0x^3 + \ldots \end{array}$$

Итак, получаем окончательно

$$\frac{1 - x\cos\alpha}{1 - 2x\cos\alpha + x^2} = 1 + x\cos\alpha + x^2\cos 2\alpha + x^3\cos 3\alpha + \ldots$$

Параллелограм Newton'a

§ 28

Желая указать приемы разложения алгебраических функций в ряды, Newton пришел к решению одной особенной задачи о наибольших и наименьших величинах.

Пусть алгебраическое уравнение, определяющее y, как функцию от x, будет такого вида

$$A_1x^{m_1}y^{n_1} + A_2x^{m_2}y^{n_2} + A_3x^{m_3}y^{n_3} + \ldots = 0, \tag{1}$$

где первая часть представляет собою сумму конечного числа слагаемых.

Построим в плоскости прямоугольных координат точки, координатами которых являются показатели при x и y в одночленах, т. е., точки $(m_1, n_1), (m_1, n_1), (m_1, n_1), \ldots$. Показатели m_i и n_i мы предполагаем, очевидно, целыми положительными числами или нулями.

Пусть y разложен в ряд по возрастающим степеням x

$$y = \mathfrak{A}x^{\alpha} + \mathfrak{B}x^{\beta} + \ldots \tag{2}$$

Перепишем равенство (2) в таком виде

$$y = \mathfrak{A}'x^{\alpha}, \tag{3}$$

где

$$\mathfrak{A}' = \mathfrak{A} + \mathfrak{B}x^{\beta-\alpha} + \ldots$$

Очевидно, что

$$\lim_{x=0} \mathfrak{A}' = \mathfrak{A}.$$

Подставляя выражение (3) в уравнение (1), получаем

$$A_1\mathfrak{A}'^{n_1}x^{m_1+\alpha n_1} + A_2\mathfrak{A}'^{n_2} + x^{m_2+\alpha n_2} + \ldots = 0. \tag{4}$$

Если число α указано таким образом, что в ряде линейных выражений

$$m_1 + \alpha n_1,\ m_2 + \alpha n_2,\ m_3 + \alpha n_3,\ \ldots, \tag{5}$$

стоящих в показателях, *одно* из этих выражений, например, $m_i + \alpha n_i$, оказывается меньше всех остальных, то по сокращении уравнения (4) на $x^{m_i+\alpha n_i}$ мы получим

$$A_i\mathfrak{A}^{n_i} + K_1x^{\lambda_1} + K_2x^{\lambda_2} + \ldots = 0, \tag{6}$$

где $\lambda_1, \lambda_2, \ldots$ суть положительные показатели. Тогда, подводя x к нулю, получаем

$$A_i\mathfrak{A}^{n_i} = 0,$$

т. е.

$$\mathfrak{A} = 0$$

и разложение (2) невозможно, ибо коэффициент при первом члене равен нулю. Для того, чтобы разложение (2) стало возможным, необходимо, чтобы по крайней мере два из линейных выражений (5) сделались одинаковыми и меньшими всех остальных. Так, например, если будут одинаковы и меньше всех остальных два первых из числа выражений (5), то, сокращая на $x^{m_1+\alpha n_1} = x^{m_2+n_2}$ получим

$$A_1\mathfrak{A}'^{n_1} + A_2\mathfrak{A}'^{n_2} + K_1x^{\lambda_1} + K_2x^{\lambda_2} + \ldots = 0.$$

Подводя x к нулю, получаем

$$A_1\mathfrak{A}^{n_1} + A_2\mathfrak{A}^{n_2} = 0$$

и тогда, если $n_2 >_1$, то

$$\mathfrak{A} = \sqrt[n_2-n_1]{-\frac{A_1}{A_2}}.$$

§ 29

Итак, мы пришли к задаче нахождения такого значения α, при котором два из выражения

$$m_1 + \alpha n_1,\ m_2 + \alpha n_2,\ m_3 + \alpha n_3,\ \ldots, \tag{1}$$

делаются равными между собой и не большими остальных.

Так как выражения (1) конечное число, то задачу можно решить, очевидно, пробами. Можно взять из (1) два выражения

$$m_i + \alpha n_i \quad \text{и} \quad m_k + \alpha n_k. \tag{2}$$

приравнять их, т. е. положить

$$m_i + \alpha n_i = m_k + \alpha n_k,$$

откуда получится

$$\alpha = \frac{m_i - m_k}{n_k - m_k} \tag{3}$$

и подставить такое значение во все выражения (1). Если при этом действительно выражения (2) окажутся не большими всех остальных, то значение (3) для α будет одним из искомых.

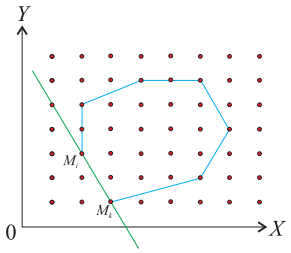
Newton дал простое геометрическое правило, позволяющее избежать излишнего числа проб и прямо находить искомые значения α. Lagrange представил правило Newton'a в аналитической форме. Сообщим здесь правило Newton'a.

Рассмотрим картину всех точек $M_i(m_i, n_i)$, соответствующих показателям различных членов заданного алгебраического уравнения. Легко убедиться, что если

пара выражений (2) дает выражение (3) для α, решающее задачу, то тогда прямая, соединяющая точки M_i и M_k, так расположена, что остальные точки лежат выше ее. Рассмотрим прямую линию

$$x + \alpha y = \beta. \tag{4}$$

Очевидно, что α будет тангенсом угла, который прямая образует с осью y-ов, а β будет абсцисса точки, в которой прямая пересекает ось x-ов. Тогда очевидно, что $m_i + \alpha n_i$ даст выражение β для прямой, имеющей вид (4) с данным угловым коэффициентом α и проходящей через точку M_i. Следовательно, задача решается при помощи такого направления α, при котором два выражения для β, соответствующие двум точкам M_i и M_k, одинаковы и не больше остальных; а отсюда вытекает следующее геометрическое построение.



Черт. 4

Проводим (черт. 4) такой многоугольный контур, вершинами которого были бы некоторый из точек M_i, чтобы все остальные точки M_i заключались внутри этого контура или лежали на нем самом. Тогда те из сторон контура, отсекающих на обеих осях положительные отрезки, относительно которых контур и начало координат расположены по разные стороны, дают решения выставленной задачи.

§ 30

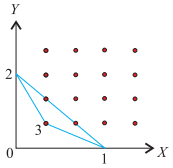
Поясним эту теорию на примере. Требуется разложить по возрастающим степеням x функцию y, определяемую уравнением

$$x^3 + y^3 - 3xy = 0. \tag{1}$$

Получаем три точки (черт. 5). Точка 1 соответствуешь члену x^3, точка 2 члену y^3, точка 3 члену $-3xy$. Для определения показателя α, с которого начнется разложение

$$y = \mathfrak{A}' x^{\alpha} \tag{2}$$

могут служить две стороны $(1, 3)$ и $(2, 3)$.



Черт. 5

Линейные выражения (1) предыдущего §-а для данного случая будут

$$3,\ 3\alpha,\ \alpha + 1. \tag{3}$$

Сторона $(1, 3)$ дает $3 = \alpha + 1$, т. е. $\alpha = 2$, и действительно, в этом случае выражения (3) принимают численные значения $3, 6, 3$, так что выражения для точек (1) и (3) оказываются равными между собою и меньшими, чем число 6 для точки (2). Подставляя выражение (2) в уравнение (1), получим

$$x^3 + \mathfrak{A}'^3 x^6 - 3x^3 \mathfrak{A}' = 0,$$

откуда, сокращая на x^3,

$$1 + \mathfrak{A}'^3 x^3 - 3\mathfrak{A}' = 0.$$

Подводя x к пределу 0, найдем

$$3\mathfrak{A} = 1, \qquad \mathfrak{A} = \frac{1}{3}.$$

Значить, разложение y будет иметь вид

$$y = \frac{1}{3}\, x^2 + \mathfrak{B} x^\beta + \ldots \tag{4}$$

Показатели β и коэффициенты $\mathfrak{B}, \ldots$ определяются при помощи подстановки ряда (4) в уравнение (1) и подбора этих показателей и коэффициентов для уничтожения всех членов, чтобы уравнение (1) действительно удовлетворялось.

Вторая сторона $(3, 2)$ дает равенство

$$3\alpha = \alpha + 1,$$

откуда

$$\alpha = \frac{1}{2},$$

и тогда придется откинуть первый член и решить уравнение

$$y^3 - 3xy = 0,$$

откуда

$$y^2 = 3x, \qquad y = \sqrt{3} \cdot x^{\frac{1}{2}};$$

значит, разложение будет

$$y = \sqrt{3}\, x^{\frac{1}{2}} + \mathfrak{B} x^\beta + \ldots$$

Кривая линия, определяемая уравнением (1), имеет в начале координат узловую точку, в которой пересекаются две ветви. Вблизи начала координат численные значения ординаты y при бесконечно малых значениях x на одной из этих ветвей вычисляются при помощи ряда (4), а на другой при помощи ряда (5).

Теорема Eisenstein'a

§ 31

Предположим, что ряд

$$y = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \ldots \tag{1}$$

с *рациональными* коэффициентами $\alpha_0, \alpha_1, \alpha_2, \ldots$, удовлетворяет алгебраическому уравнению

$$F(x, y) = 0 \tag{2}$$

с *целыми* коэффициентами.

Eisenstein'y принадлежите интересное замечание, что можно подобрать такое целое число k, что от замены x на kx все коэффициенты ряда (1) делаются числами целыми.

Мы дадим доказательство, принадлежащее Hermite'y,[1] ограничиваясь случаем, когда ряд (1) рассматривается вблизи неособенной точки линии (2).

Изменим y на α_0+y, чтобы получить новое уравнение, которое удовлетворяется значениями $x=0$, $y=0$. Раскладывая это новое уравнение по степеням y, получим $P+P_1y+P_2y^2+\ldots=0$, где $P, P_1, P_2, \ldots$ полиномы от x, из которых первый обращается в нуль при $x=0$

$$P = gx + hx^2 + \ldots$$

$$P_1 = g_1 + h_1x + \ldots$$

$$P_2 = g_2 + h_2x + \ldots$$

$$\ldots\ldots\ldots\ldots\ldots$$

Если точка $x=0$, $y=0$ не особенная, то g_1 отлично от нуля. Число g_1 целое, ибо мы предполагаем целыми все коэффициенты уравнения (2). Положим теперь $x=g_1^2t$, $y=g_1u$. Можно будет сократить множитель g_1^2 в уравнении между новыми переменными t и u. Это уравнение имеет следующий вид

$$\begin{aligned} Gt + Ht^2 + \ldots + [1 + G_1t + H_1t^2 + \ldots]u + \\ + [G_2 + H_2t + \ldots]u^2 + \\ + \ldots = 0, \end{aligned}$$

$G, G_1, \ldots, H, H_1, \ldots$ числа целые.

Напишем это соотношение так

$$u = -\frac{Gt + Ht^2 + \ldots}{1 + G_1t + H_1t^2 + \ldots} - \frac{G_2 + H_2t + \ldots}{1 + G_1t + H_1t^2 + \ldots}u^2 - \ldots$$

или, выполняя деление, т. е. заменяя рациональные дроби рядами

$$u = At + A't^2 + \ldots + (B + B't + \ldots)u^2 + \ldots!$$

Делая в последнем уравнении подстановку

$$u = mt + m't^2 + m''t^3 + \ldots,$$

получаем

$$m = A$$

$$m' = A' + Bm^2$$

$$m'' = A'' + 2Bmm' + B'm^2 + \ldots$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

[1] Cours de M. Hermite. Professé pendant le 2-e Semestre 1881–82 Rédigé Par M. Andoyer.

Последние равенства показывают, что теорема Eisenstein'a справедлива, ибо все числа $A, A', A'', \ldots, B, B', \ldots$ суть числа целые.

Так, например, уравнение $y^n = (1-x)^{-m}$, где n и m числа натуральные, удовлетворяется, как известно, биномиальным рядом

$$y = \sum \frac{m(m+n)\cdots[m+(i-1)n]}{1\cdot 2\cdots in}\, x^i. \tag{3}$$

Изменяя y на $1+y$, получим

$$ny + \frac{n(n-1)}{1\cdot 2}y^2 + \ldots = mx + \frac{m(m+1)}{1\cdot 2}x^2 + \ldots$$

Мы видим, что число g_1 в данном случае есть n, а потому коэффициенты ряда (3) должны сделаться числами целыми, если подставить вместо x величину n^2t и далее положить $y = nu$. Мы приходим к заключению, что будет целым число

$$\frac{m(m+n)\ldots[m+n(i-1)]}{1\cdot 2\cdot 3\cdots i}n^{i-1}.$$

Как следствие теоремы Eisenstein'a получается замечание, что функции e^x и $\lg(1+x)$ не могут удовлетворять алгебраическому уравнению с рациональными коэффициентами. В самом деле, ряды

$$\lg(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \ldots \pm \frac{x^n}{n} \mp \ldots$$

$$e^x = 1 + \frac{x}{1} + \frac{x^2}{1\cdot 2} + \ldots + \frac{x^n}{1\cdot 2\cdots n} + \ldots$$

имеют в знаменателях коэффициентов бесчисленное множество различных простых чисел и потому не могут быть приведены к рядам с целыми коэффициентами.

Глава IV

Об определителях

§ 1

Пусть заданы 2 уравнения 1-ой степени с 2-мя неизвестными

$$\begin{aligned} a_1x + b_1y &= c_1 \\ a_2x + b_2y &= c_2. \end{aligned}$$

Через решение этих уравнений относительно x и y получаем

$$\begin{aligned} x &= \frac{c_1b_2 - c_2b_1}{a_1b_2 - a_2b_1} \\ y &= \frac{a_1c_2 - a_2c_1}{a_1b_2 - a_2b_1}. \end{aligned} \tag{1}$$

Если мы возьмем уравнения 1-ой степени с 3-мя неизвестными

$$\begin{aligned} a_1x + b_1y + c_1z &= d_1 \\ a_2x + b_2y + c_2z &= d_2 \\ a_3x + b_3y + c_3z &= d_3, \end{aligned}$$

то, решая эти уравнения относительно 3 неизвестных x, y, z, получим выражения

$$\begin{aligned} x &= \frac{d_1b_2c_3 - d_1b_3c_2 + d_2b_3c_1 - d_2b_1c_3 + d_3b_1c_2 - d_3b_2c_1}{a_1b_2c_3 - a_1b_3c_2 + a_2b_3c_1 - a_2b_1c_3 + a_3b_1c_2 - a_3b_2c_1} \\ y &= \frac{a_1d_2c_3 - a_1d_3c_2 + a_2d_3c_1 - a_2d_1c_3 + a_3d_1c_2 - a_3d_2c_1}{a_1b_2c_3 - a_1b_3c_2 + a_2b_3c_1 - a_2b_1c_3 + a_3b_1c_2 - a_3b_2c_1} \\ z &= \frac{a_1b_2d_3 - a_1b_3d_2 + a_2b_3d_1 - a_2b_1d_3 + a_3b_1d_2 - a_3b_2d_1}{a_1b_2c_3 - a_1b_3c_2 + a_2b_3c_1 - a_2b_1c_3 + a_3b_1c_2 - a_3b_2c_1}. \end{aligned} \tag{2}$$

Если мы введем следующие обозначения

$$a_1b_2 - a_2b_1 = \begin{vmatrix} a_1, & b_1 \\ a_2, & b_2 \end{vmatrix} \tag{3}$$

и

$$a_1b_2c_3 - a_1b_3c_2 + a_2b_3c_1 - a_2b_1c_3 + a_3b_1c_2 - a_3b_2c_1 = \begin{vmatrix} a_1, & b_1, & c_1 \\ a_2, & b_2, & c_2 \\ a_3, & b_3, & c_3 \end{vmatrix}, \tag{4}$$

то получим выражения, который носят название *определителей* или *детерминантов*.

Употребляя обозначение определителей, можно будет переписать формулы (1) в таком виде

$$x = \frac{\begin{vmatrix} c_1 & b_1 \\ c_2 & b_2 \end{vmatrix}}{\begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix}}, \qquad y = \frac{\begin{vmatrix} a_1 & c_1 \\ a_2 & c_2 \end{vmatrix}}{\begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix}}.$$

Подобным же образом формулы (2) примут вид

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

При помощи определителей упрощаются выкладки решения уравнений 1-й степени с несколькими неизвестными.

Эти упрощения основаны на важных свойствах определителей, к перечислению которых мы и перейдем.

Разделение перемещений на два класса

§ 2

Будем рассматривать перемещения n предметов, которые обозначим числами $1, 2, 3, \ldots, n$.

Известно, что число различных перемещений n предметов равно

$$1 \cdot 2 \cdot 3 \cdots n = n! = \Pi(n).$$

Так, например, получается $24 = 1 \cdot 2 \cdot 3 \cdot 4$ различных перемещений 4 предметов $(1, 2, 3, 4)$

1234	2134	3124	4123
1243	2143	3142	4132
1324	2314	3214	4213
1342	23441	3241	4231
1423	2413	3412	4312
1432	2431	3421	4321.

Перемещение

$$1 \ . \ 2 \ . \ 3 \ \ldots \ n,$$

в котором числа, указывающая предметы, расположены в натуральном порядке возрастания, называется *главным*.

Переход от главного перемещения к какому либо произвольному совершается при помощи операции, состоящей в перестановки элементов. Такая перестановка

элементов перемещения, обыкновенно, называется *подстановкой* этих элементов (substitution).

§ 3

Простейшей подстановкой является перестановка 2 элементов, так, например, подстановка, переводящая перемещение 12345 в 32145 есть не что иное, как перестановка 2 элементов. Перестановку 2 элементов будем называть *транспозицией*.

Покажем, что всякую подстановку можно рассматривать, как совокупность нескольких транспозиций. В самом деле, например, подстановка, переводящая главное перемещение 12345 в 43521 может быть получена, как совокупность следующих транспозиций: производим транспозицию, которая ставит на место 1-ого элемента 1 элемент 4; значить, надо переставить элементы 14: получаем

42315.

Далее, надо на 2-ое место поставить элемент 3; значит, надо переставить элементы 23. Получаем

43215.

Надо поставить на 3-е место элемент 5, следовательно, придется переставить элементы 25; получаем

43512.

Остается произвести последнюю транспозицию элементов 12. Получаем окончательно

43521.

Рассуждая подобно тому, как это мы делали на только что приведенном примере, мы можем осуществить всякую подстановку при помощи ряда транспозиций.

Разобьем все $\Pi(n)$ перемещений на 2 *класса*, причем к *первому* классу мы отнесем все те перемещения, которые получаются из главного при помощи четного числа транспозиций, и ко *второму* классу отнесем те перемещения, которые получаются после нечетного числа транспозиций.

Само главное перемещение мы отнесем к 1-ому классу, потому что можно считать, что оно происходить из самого себя при помощи 0 числа транспозиций. Число же 0 можно отнести к числу четных.

§ 4

Покажем простой способ узнавать, к какому классу принадлежит перемещение. Для этой цели введем новое понятие «*беспорядок*». Мы будем говорить, что 2 элемента перемещения образуют *порядок*, если больший элемент стоить направо от меньшого, и *беспорядок*, если больший элемент стоить налево от меньшого.

Главное перемещение

$$12\cdots n$$

не имеет беспорядков, тогда как в перемещении

45312

существуют следующие беспорядки

$$(3,1)\ \ (4,1)\ \ (5,1)$$
$$(3,2)\ \ (4,2)\ \ (5,2)$$
$$(4,3)\ \ (5,3).$$

Итак, перемещение

$$45312$$

заключает 8 беспорядков.

Теорема. *Перемещение принадлежит к первому классу, если оно заключает четное число (или 0) беспорядков, и ко второму, если заключает нечетное число беспорядков.*

Так, например, перемещение

$$45312$$

принадлежать к первому классу, потому что оно заключает 8 беспорядков.

Для доказательства этой теоремы достаточно убедиться, что всякая транспозиция изменяет число беспорядков на нечетное число.

Отсюда будет следовать, что от произведения над главным перемещением нечетного числа транспозиций произойдет в результате нечетное число беспорядков; после же четного числа транспозиций, число беспорядков окажется четным.

Пусть рассматривается перемещение вида

$$AaBbC. \tag{1}$$

В этом перемещении у нас указаны 2 элемента a и b; остальные же не указаны в отдельности, а лишь обозначена буквой A совокупность элементов, стоящих слева от элемента a; буквой B обозначены элементы, столице между a и b, и, наконец, буквой C обозначены элементы, столице направо от b.

Посмотрим, как изменится число беспорядков перемещений (1), если мы переставим a и b, т. е. напишем

$$AbBaC. \tag{2}$$

Беспорядки, которые заключаются в группах A, B и C, останутся без перемены; следовательно, надо рассматривать беспорядки, заключающиеся в следующих парах элементов: в паре (a, b) и в парах, происходящих от сопоставления каждого из элементов a, b с другими элементами.

Что касается пары (a, b), то может быть 2 случая: если в перемещении (1) эта пара (a, b) представляла порядок, то она будет представлять беспорядок в перемещений (2), и, обратно, беспорядок этой пары, если он имел место в перемещении (1), пропадет в перемещении (2), а потому, получается при рассмотрении пары (a, b) или появление одного беспоряцка, или исчезновение одного беспорядка. В обоих случаях получается изменение числа беспорядков на нечетное число.

Для окончательного доказательства теоремы остается доказать, что в парах, сопоставляющих один из элементов a, b с элементами групп A, B, C, происходит четное число изменений беспорядков.

Пусть α один из элементов системы A, β — один из элементов системы B и γ — один из элементов системы C.

В двух парах (α, a) и (α, b) не происходит изменения числа беспорядков, потому что при транспозиции оба элемента a и b остаются направо от элемента α, так что порядок остается после транспозиции также порядком, а беспорядок — беспорядком.

Совершенно подобным образом не происходит изменения беспорядков в парах (a, γ) и (b, γ), ибо элементы a и b остаются при транспозиции налево от элемента γ.

Посмотрим, как изменится число беспорядков в системе 3 элементов $(a\beta b)$ при транспозиции элементов ab.

Рассмотрим 4 возможных случая:

	$a\beta b$		$b\beta a$	
I	поряд.	поряд.	беспор.	беспор.
II	поряд.	беспор.	поряд.	беспор.
III	беспор.	поряд.	беспор.	поряд.
IV	беспор.	беспор.	поряд.	поряд.

потому что транспозиция элементов a и b обращает в группе $(a\beta b)$ порядок в беспорядок и обратно.

Итак, мы замечаем, что в случаях II и III в системе $a\beta b$ не происходит изменения числа беспорядков, в случай же I число беспорядков увеличивается на 2, и, наконец, в случае IV число беспорядков уменьшается на 2. В общем можно сказать, что число беспорядков в групп $(a\beta b)$ от транспозиции изменяется на четное число

Следовательно, можно считать доказанным, что всякая транспозиция изменяет число беспорядков на число нечетное, и, значить, подлежащая доказательству теорема оказывается справедливой.

§ 5

Теорема. *В каждом классе заключается по одинаковому числу перемещений.*

Пусть рассматриваются перемещения n элементов, и пусть $\mathfrak{A}$ представляет из себя совокупность перемещений 1-ого класса а $\mathfrak{B}$ — совокупность перемещений 2-ого класса. Сделаем во всех написанных перемещениях обоих классов транспозицию 2 определенно выбранных элементов. Тогда можно утверждать, что, после такой транспозиции, воспроизведутся все перемещения, только они будут написаны в другом порядке. В самом деле, транспозиция не может обратить 2 различных перемещения в одно и то же, ибо тогда обратная транспозиция из одного перемещения давала бы 2 разных, что невозможно; значить все $\Pi(n)$ различных перемещений обращаются после транспозиции 2 элементов в те же самые различные перемещения. Но, с другой стороны, если мы обратим внимание на то обстоятельство, что транспозиция переводить перемещения одного класса в перемещения другого класса, то значит, совокупность всех перемещений $(\mathfrak{A}, \mathfrak{B})$ перейдет после транспозиции в ту же самую полную совокупность перемещений только в том случае, если в обоих классах $\mathfrak{A}$ и $\mathfrak{B}$ будет по одинаковому числу перемещений; тогда после транспозиции класс $\mathfrak{A}$ переходить полностью в класс $\mathfrak{B}$, и обратно.

§ 6

Пусть заданы на плоскости n^2 чисел, написанных следующим образом:

$$(1)\qquad \begin{array}{ccccc} a_1{}^{(1)} & a_2{}^{(1)} & a_3{}^{(1)} & \dots & a_n{}^{(1)} \\ a_1{}^{(2)} & a_2{}^{(2)} & a_3{}^{(2)} & \dots & a_n{}^{(2)} \\ a_1{}^{(3)} & a_2{}^{(3)} & a_3{}^{(3)} & \dots & a_n{}^{(3)} \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ a_1{}^{(n)} & a_2{}^{(n)} & a_3{}^{(n)} & \dots & a_n{}^{(n)} \end{array}$$

Заданные числа расположены на плоскости в n горизонтальных и n вертикальных рядах, причем в каждом числе

$$a_k{}^{(i)}$$

верхний значок i (иидекс) показывает, что число находится в i-ой горизонтали (считая сверху), а нижний значок k указывает, что число находится в k-ой колонне (считая слева).

Картина, образованная написанными указанным образом n^2 числами, называется *числовою квадратной матрицею порядка n*.

Мы будем рассматривать такую целую функцию от элементов матрицы (1)

$$(2)\qquad \sum (-1)^W a_{i_1}^{(1)} a_{i_2}^{(2)} a_{i_3}^{(3)} \dots a_{i_n}^{(n)},$$

где знак суммы $\sum$ распространяется на всевозможные перемещения

$$i_1 \;\; i_2 \;\; \dots \;\; i_n$$

нижних значков, W же представляет число беспорядков в перемещении $i_1\ i_2\ \dots\ i_n$.

Очевидно, что в целой функций (2) число членов будет $\Pi(n)$, причем эти члены будут со знаком $+$, если перемещение будет принадлежать к 1-ому классу, и со знаком $-$, если перемещение будет принадлежать ко 2-ому классу.

Сумма (2) называется *определителем матрицы* (1) и обозначается обыкновенно знаком

$$\begin{vmatrix} a_1{}^{(1)} & a_2{}^{(1)} & \dots & a_n{}^{(1)} \\ a_1{}^{(2)} & a_2{}^{(2)} & \dots & a_n{}^{(2)} \\ \dots\dots\dots\dots\dots\dots\dots\dots \\ a_1{}^{(n)} & a_2{}^{(n)} & \dots & a_n{}^{(n)} \end{vmatrix}.$$

§ 7

Рассмотрим для примера случай $n = 3$, тогда матрица имеет вид

$$\begin{array}{ccc} a_1{}^{(1)} & a_2{}^{(1)} & a_3{}^{(1)} \\ a_1{}^{(2)} & a_2{}^{(2)} & a_3{}^{(2)} \\ a_1{}^{(3)} & a_2{}^{(3)} & a_3{}^{(3)}. \end{array}$$

До данному в предыдущем параграфе определению, получим

$$\begin{vmatrix} a_1{}^{(1)} & a_2{}^{(1)} & a_3{}^{(1)} \\ a_1{}^{(2)} & a_2{}^{(2)} & a_3{}^{(2)} \\ a_1{}^{(3)} & a_2{}^{(3)} & a_3{}^{(3)} \end{vmatrix} = \sum (-1)^W a_{i_1}{}^{(1)} a_{i_2}{}^{(2)} a_{i_3}{}^{(3)}.$$

Давая нижним значкам всевозможные перемещения 3 элементов (123), которых может быть $1 \cdot 2 \cdot 3 = 6$), получим члены

$$\begin{array}{lll} a_1{}^{(1)} a_2{}^{(2)} a_3{}^{(3)}; & a_1{}^{(1)} a_3{}^{(2)} a_2{}^{(3)}; & a_2{}^{(1)} a_1{}^{(2)} a_3{}^{(3)}; \\ a_2{}^{(1)} a_3{}^{(2)} a_1{}^{(3)}; & a_3{}^{(1)} a_1{}^{(2)} a_2{}^{(3)}; & a_3{}^{(1)} a_2{}^{(2)} a_1{}^{(3)}. \end{array} \tag{3}$$

Так как число беспорядков в нижних значках членов (3) выражается последовательно числами

$$0; \quad 1; \quad 1; \quad 2; \quad 2; \quad 3,$$

следовательно, искомый определитель нашей матрицы третьего порядка будет написан так:

$$a_1{}^{(1)} a_2{}^{(2)} a_3{}^{(3)} - a_1{}^{(1)} a_3{}^{(2)} a_2{}^{(3)} - a_2{}^{(1)} a_1{}^{(2)} a_3{}^{(3)} + a_2{}^{(1)} a_3{}^{(2)} a_1{}^{(3)} + \\ + a_3{}^{(1)} a_1{}^{(2)} a_2{}^{(3)} - a_3{}^{(1)} a_2{}^{(2)} a_1{}^{(3)}.$$

Сравнивая с формулой (4) § 1, мы замечаем полное совпадение, если только нижние значки отмечать различными буквами, а верхние значки перенести вниз. Например

$$\begin{array}{lll} a_1 = a; & a_2 = b; & a_3 = c \\ a_1{}^{(2)} = a_2; & a_2{}^{(3)} = b_3; & a_3{}^{(1)} = c_1. \end{array}$$

Другими словами, если для элементов 1-ой колонны писать букву a, для элементов 2-ой колонны писать букву b и для элементов 3-ей колонны — c. Горизонтали же отличать нижними значками.

§ 8

Очевидно, что в каждом члене определителя

$$\sum (-1)^W a_{i_1}^{(1)} a_{i_2}^{(2)} \dots a_{i_n}^{(n)} \tag{1}$$

множителей можно переставить таким образом, чтобы нижние значки

$$i_1 \quad i_2 \quad \dots \quad i_n$$

оказались расположенными в натуральном порядке возрастания; тогда произойдут беспорядки в верхних индексах; при этом можно убедиться, что тот же самый определитель можно написать и в такой форме

$$\sum (-1)^{W'} a_1{}^{(k_1)} a_2{}^{(k_2)} a_3{}^{(k_3)} \dots a_n{}^{(k_n)}, \tag{2}$$

сумма $\sum$ распространяется на все различные перемещения верхних значков

$$k_1 \quad k_2 \quad \dots \quad k_n,$$

W' есть число беспорядков в верхних значках.

Для того, чтобы убедиться, что выражения (1) и (2) тождественны, достаточно показать, что, если мы из члена

$$a_{i_1}^{(1)} a_{i_2}^{(2)} \dots a_{i_n}^{(n)}$$

суммы (1) получаем перемещением множителей соответствующий член

$$a_1{}^{(k_1)} a_2{}^{(k_2)} \dots a_n{}^{(k_n)}$$

суммы (2), то оба перемещения

$$i_1 \quad i_2 \quad \dots \quad i_n$$

и

$$k_1 \quad k_2 \quad \dots \quad k_n$$

принадлежать к одному и тому же классу. Для того, чтобы убедиться в сказанном, достаточно принять в соображение, что приведение в порядок нижних индексов может быть достигнуто при помощи некоторого числа транспозиций множителей, причем, это число транспозиций будет четное, если перемещение

(3) $$i_1 \quad i_2 \quad \dots \quad i_n$$

было 1-ого класса, и нечетное, если 2-ого класса; но, так как при перестановке множителей каждый множитель влечет за собою оба значка (и верхний, и нижний), то транспозициям множителей будут соответствовать транснозиции верхних значков. Первоначальное перемещение в сумме (1) верхних значков беспорядков не имело; очевидно, что окончательное размещение

(4) $$k_1 \quad k_2 \quad \dots \quad k_n$$

верхних значков будет 1-го класса, если число транспозиций множителей было четное, и 2-ого класса, если это число транспозиций было нечетное.

Итак, мы видим, что перемещения (3) и (4) принадлежать к одному классу.

§ 9

Нетрудно видеть, что может быть написана более общая формула, выражающая состав определителя, а именно

(1) $$\sum (-1)^{I+K} a_{i_1}{}^{(k_1)} a_{i_2}{}^{(k_2)} \dots a_{i_n}{}^{(k_n)},$$

в которой множители не расположены в порядок ни по нижним, ни по верхним значкам. В этой формуле I обозначает число беспорядков в ряде нижних значков, а K — число беспорядков в ряде верхних значков. Доказательство этой последней формулы остается одинаковым с приведенным в предыдущем параграфе.

§ 10

Теорема. *Величина определителя не меняется, если горизонтали заменить колоннами, и обратно.*

В самом деле, замена горизонталей колоннами сводится к замене верхних значков нижними и обратно. Между тем, формула (1) предыдущего параграфа показывает, что от такой замены верхних значков нижними числа I и K меняются ролями, и, следовательно, рассматриваемый член войдет в общую сумму с тем же знаком. Значит, новое значение суммы остается тождественно равным первоначальному.

§ 11

Теорема. *От перестановки двух горизонталей (колонн) величина определителя меняет свой знак.*

Справедливость теоремы вытекает из того соображения, что перестановка 2 горизонталей соответствует перестановке 2 нижних значков. В § 4 мы видели, что перестановка 2 элементов перемещения изменяет класс этого перемещения, а тогда каждый член определителя изменит свой знак, и, следовательно, изменить знак и весь определитель.

§ 12

Определитель тождественно равен 0*, если, он имеет две одинаковые горизонтали (колонны).*

Пусть Δ есть величина определителя, имеющего две одинаковые горизонтали. При перестановке этих горизонталей должно происходить, с одной стороны, изменение знака определителя (см. предыд. парагр.), с другой стороны, определитель, очевидно, остается тем же, ибо обе горизонтали одинаковы; и мы получаем

$$\Delta = -\Delta.$$

Откуда $2\Delta = 0$ или $\Delta = 0$, что и требовалось доказать.

§ 13

Разложение определителя по элементам горизонтали (колонны).

На основании сказанного о составлении определителя, мы замечаем, что каждый элемент определителя может входить в различных его членах только в 1-ой степени, ибо иначе значки этого элемента повторились бы несколько раз в одном члене определителя, что невозможно, потому что, как верхние, так и нижние значки должны представлять перемещения без повторений.

Посмотрим, с каким коэффициентом входит в определитель некоторый элемент

$$a_i{}^{(k)}.$$

Начнем с рассмотрения левого верхнего элемента

$$a_1{}^{(1)}.$$

Нетрудно видеть, что, если мы этот элемент $a_1{}^{(1)}$ возьмем за скобку и предположим, что в членах определителя нижние значки приведены в порядок, то замечаем, что в скобках окажется выражение

$$\sum (-1)^{W'} a_2{}^{(l_2)} a_3{}^{(l_3)} \dots a_n{}^{(l_n)},$$

где

$$l_2 \ \ l_3 \ \dots \ l_n$$

представляют из себя различные перемещения $n-1$ значков

$$2 \ \ 3 \ \dots \ n,$$

а W' будет представлять число беспорядков в перемещении

$$l_2 \ \ l_3 \ \dots \ l_n.$$

Итак, мы видим, что коэффициентом у ${a_1}^{(1)}$ оказывается определитель

$$\begin{vmatrix} {a_2}^{(2)} & {a_3}^{(2)} & \dots & {n_2}^{(2)} \\ {a_2}^{(3)} & {a_3}^{(3)} & \dots & {n_2}^{(3)} \\ \multicolumn{4}{c}{\dotfill} \\ {a_2}^{(n)} & {a_3}^{(n)} & \dots & {n_2}^{(n)} \end{vmatrix}$$

получающийся из рассматриваемого основного определителя через вычеркивание 1-ой горизонтали и 1-ой колонны.

Обращаемся теперь к рассмотрений коэффициента, на который умножается общий элемент ${a_i}^{(k)}$ определителя

$$(1) \qquad \begin{vmatrix} & & & {a_i}^{(1)} & & \\ & & & {a_i}^{(2)} & & \\ & & & \vdots & & \\ {a_1}^{(k)} & {a_2}^{(k)} & \dots & {a_i}^{(k)} & \dots & {a_n}^{(k)} \\ & & & \vdots & & \\ & & & {a_i}^{(n)} & & \end{vmatrix}$$

Перенесем k-ую горизонталь на место 1-ой горизонтали без изменения взаимного расположения остальных горизонталей. Этого можно будет достигнуть так: сначала перемещаем горизонтали $k-1$ и k; затем k-ую перемещаем далее с места $k-1$ на место $k-2$ и продолжаем такое перемещение k-ой горизонтали со следующими верхними до тех пор, пока k-ая горизонталь не займет верхнее место в определителе. Тогда определитель будет иметь такой вид

$$(2) \qquad \begin{vmatrix} {a_1}^{(k)} & {a_2}^{(k)} & \dots & {a_i}^{(k)} & \dots & {a_n}^{(k)} \\ {a_1}^{(1)} & {a_2}^{(1)} & \dots & {a_i}^{(1)} & \dots & {a_n}^{(1)} \\ {a_1}^{(2)} & {a_2}^{(2)} & \dots & {a_i}^{(2)} & \dots & {a_n}^{(2)} \\ \multicolumn{6}{c}{\dotfill} \\ {a_1}^{(k-1)} & {a_2}^{(k-1)} & \dots & {a_i}^{(k-1)} & \dots & {a_n}^{(k-1)} \\ {a_1}^{(k+1)} & {a_2}^{(k+1)} & \dots & {a_i}^{(k+1)} & \dots & {a_n}^{(k+1)} \end{vmatrix}.$$

Если теперь подобным же образом, не нарушая порядка остальных колонн, мы перенесем i-ую колонну на 1-ое место, то получаем

$$(3) \qquad \begin{vmatrix} {a_i}^{(k)} & {a_1}^{(k)} & {a_2}^{(k)} & \dots & {a_{i-1}}^{(k)} & {a_{i+1}}^{(k)} & \dots \\ {a_i}^{(1)} & {a_1}^{(1)} & {a_2}^{(1)} & \dots & {a_{i-1}}^{(1)} & {a_{i+1}}^{(1)} & \dots \\ {a_i}^{(2)} & {a_1}^{(2)} & {a_2}^{(2)} & \dots & {a_{i-1}}^{(2)} & {a_{i+1}}^{(2)} & \dots \\ \multicolumn{7}{c}{\dotfill} \\ {a_i}^{(k-1)} & {a_1}^{(k-1)} & {a_2}^{(k-1)} & \dots & {a_{i-1}}^{(k-1)} & {a_{i+1}}^{(k-1)} & \dots \\ {a_i}^{(k+1)} & {a_1}^{(k+1)} & {a_2}^{(k+1)} & \dots & {a_{i-1}}^{(k+1)} & {a_{i+1}}^{(k+1)} & \dots \\ \multicolumn{7}{c}{\dotfill} \end{vmatrix}.$$

Так как переход от определителя (1) к определителю (2) совершается при помощи $(k-1)$ перестановок 2 горизонталей, следовательно определитель (2) отличается от определителя (1) множителем $(-1)^{k-1}$. Подобным же образом, при переходе от определителя (2) к определителю (3), мы получаем множитель $(-1)^{i-1}$; значить, окончательный переход от определителя (1) к определителю (3) совершается при помощи умножения на $(-1)^{k+i}$.

Итак, мы замечаем по виду определителя (3), что коэффициент при ${a_i}^{(k)}$ в этом определителе будет определителем, который получается из определителя (3) вычеркиванием 1-ой горизонтали и 1-ой колонны.

Следовательно, окончательно мы замечаем, что коэффициент при ${a_i}^{(k)}$ в первоначальном определителе (1) будет выражаться

$$(4)\qquad (-1)^{k+i}\begin{vmatrix} {a_1}^{(1)} & {a_2}^{(1)} & \dots & {a_{i-1}}^{(1)} & {a_{i+1}}^{(1)} & \dots & {a_n}^{(1)} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ {a_1}^{(k-1)} & {a_2}^{(k-1)} & \dots & {a_{i-1}}^{(k-1)} & {a_{i+1}}^{(k-1)} & \dots & {a_n}^{(k-1)} \\ {a_1}^{(k+1)} & {a_2}^{(k+1)} & \dots & {a_{i-1}}^{(k+1)} & {a_{i+1}}^{(k+1)} & \dots & {a_n}^{(1)} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \end{vmatrix}.$$

Это выражение (4) мы будем называть *алгебраическим дополнением* элемента ${a_i}^{(k)}$ и будем обозначать ${A_i}^{(k)}$.

Определитель в выражении (4) происходит от вычеркивания из первоначального определителя (1) i-ой колонны и k-ой горизонтали, оставляя взаимное расположение элементов других горизонталей и колонн тем же самым.

Такого рода определители, которые получаются из первоначального вычеркиванием колонн и горизонталей, носят название *миноров* первоначального определителя. Итак, алгебраическое дополнение всякого элемента определителя есть взятый с тем или другим знакомь минор получающийся от вычеркивания той горизонтали и той колонны, на пересечении которых рассматриваемый элемент находится.

§ 14

Напишем первоначальный определитель в виде

$$\Delta = \sum (-1)^W {a_{i_1}}^{(1)} {a_{i_2}}^{(2)} \dots {a_{i_n}}^{(n)}$$

и будем в нем брать за скобки в различных его членах элемент

$${a_1}^{(l)} \quad {a_2}^{(l)} \quad \dots$$

некоторой l-ой горизонтали; тогда, очевидно, что, на оснований сказанного об алгебраическом дополнении элементов, мы получим формулу

$$(1)\qquad \Delta = {a_1}^{(l)} {A_1}^{(l)} + {a_2}^{(l)} {A_2}^{(l)} + \dots + {a_n}^{(l)} {A_n}^{(n)}.$$

Эта формула представляет весьма важное разложение определителя по элементам l-ой горизонтали.

Если мы подставим вместо l-ой горизонтали какую-нибудь другую k-ую горизонталь, то получаем определитель, у которого две k-ых горизонтали; и, следовательно, определитель обратится в 0, т. е. другими словами, мы получаем новую, весьма важную, формулу

$$0 = a_1{}^{(k)}A_1{}^{(l)} + a_2{}^{(k)}A_2{}^{(l)} + \ldots + a_n{}^{(k)}A_n{}^{(n)}. \tag{2}$$

Очевидно, что можно получить аналогичные разложения но элементам колонны, т. е.

$$\Delta = a_i{}^{(1)}A_i{}^{(1)} + a_i{}^{(2)}A_i{}^{(2)} + \ldots + a_i{}^{(n)}A_i{}^{(n)}, \tag{3}$$

$$0 = a_k{}^{(1)}A_i{}^{(1)} + a_k{}^{(2)}A_i{}^{(2)} + \ldots + a_k{}^{(n)}A_i{}^{(n)}. \tag{4}$$

Решение системы n уравнений 1-ой степени с n неизвестными

§ 15

Пусть задана система

$$\begin{array}{c} a_1{}^{(1)}x_1 + a_2{}^{(1)}x_2 + \ldots + a_i{}^{(1)}x_i + \ldots + a_n{}^{(1)}x_n = b^{(1)} \\ a_1{}^{(2)}x_1 + a_2{}^{(2)}x_2 + \ldots + a_i{}^{(2)}x_i + \ldots + a_n{}^{(2)}x_n = b^{(2)} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_1{}^{(n)}x_1 + a_2{}^{(n)}x_2 + \ldots + a_i{}^{(n)}x_i + \ldots + a_n{}^{(n)}x_n = b^{(n)} \end{array} \tag{1}$$

где все числа $a_i{}^{(k)}$ и $b^{(i)}$ заданы. Требуется решит эту систему n уравнений относительно m неизвестных

$$x_1 \quad x_2 \quad \ldots \quad x_n.$$

Покажем, как найти неизвестное x_i. Для этой цели мы умножим уравнение (1) по порядку на числа

$$A_i{}^{(1)} \quad A_i{}^{(2)} \quad \ldots \quad A_i{}^{(n)}$$

и сложим. Тогда получим

$$\begin{array}{c} x_1[a_1{}^{(1)}A_i{}^{(1)} + a_1{}^{(2)}A_i{}^{(2)} + \ldots + a_1{}^{(n)}A_i{}^{(n)}] + \\ + x_2[a_2{}^{(1)}A_i{}^{(1)} + a_2{}^{(2)}A_i{}^{(2)} + \ldots + a_2{}^{(n)}A_i{}^{(n)}] + \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ + x_i[a_i{}^{(1)}A_i{}^{(1)} + a_i{}^{(2)}A_i{}^{(2)} + \ldots + a_i{}^{(n)}A_i{}^{(n)}] + \\ + x_n[a_n{}^{(1)}A_i{}^{(1)} + a_n{}^{(2)}A_i{}^{(2)} + \ldots + a_n{}^{(n)}A_i{}^{(n)}] = \\ = b^{(1)}A_i{}^{(1)} + b^{(2)}A_i{}^{(2)} + \ldots + b^{(n)}A_i{}^{(n)}. \end{array}$$

На основали тождеств (3) и (4) предыдущего параграфа мы замечаем, что обращаются в 0 все скобки левой части уравнения, кроме одной, которая умножается на x_i, и которая равна Δ, т. е. определителю, составленному из коэффициентов $a_i{}^{(k)}$; и мы получаем

$$\Delta x_i = b^{(1)}A_i{}^{(1)} + b^{(2)}A_i{}^{(2)} + \ldots + b^{(n)}A_i{}^{(n)}. \tag{2}$$

Правая часть представляет из себя определитель, который получается из определителя Δ заменой i-ой колонны

$$\begin{matrix} a_i{}^{(1)} \\ a_i{}^{(2)} \\ \vdots \end{matrix}$$

колонной правых частей

$$\begin{matrix} b^{(1)} \\ b^{(2)} \\ \vdots \end{matrix}$$

в уравнениях (1).

Если определитель Δ не равен 0, то из уравнения (2) получается вполне определенное численное значение для x_i и так как значок i мы взяли произвольно, то, следовательно, у нас получаются определенные численные значения для всех неизвестных

$$x_1 \quad x_2 \quad \ldots \quad x_n.$$

Рассмотрим теперь случай

$$\Delta = 0,$$

тогда, если выражение, стоящее в правой части уравнения (2) не равно 0, то уравнение (2) нельзя решить относительно x_i, или, как иногда, говорят, получается для x_i бесконечное значение, что иногда обозначаюсь $x_i = \infty$.

Собственно говоря, в этом случай система заключает противоречие, потому что по уравнению (2) получается

$$0 = b^{(1)} A_i{}^{(1)} + b^{(2)} A_i{}^{(2)} + \ldots,$$

что невозможно.

Если правая часть уравнения (2) также равняется 0, то получается неопределенное решение: уравнение (2) удовлетворяется при всяких численных значениях x_i.

Итак, можно высказать следующую теорему:

Условием, необходимым и достаточным для существования определенного решения уравнений вида (1), является *неравенство* нулю определителя Δ, составленного из коэффициентов при неизвестных.

Если определитель Δ равен 0, то в этом случай система может представлять или неопределенность, или же она может вести к противоречию (бесконечные решения).

Случай противоречия встретится тогда, если получается бесконечное значение по крайней мере для одной неизвестной.

§ 16

Рассмотрим теперь случай, когда правые части уравнений (1) § 15 равны 0; получаются так называемые *однородные* уравнения

$$\begin{matrix} a_1{}^{(1)} x_1 + \ldots + a_n{}^{(1)} x_n = 0 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_1{}^{(n)} x_1 + \ldots + a_n{}^{(n)} x_n = 0. \end{matrix} \tag{1}$$

Произведя выкладки предыдущего параграфа, мы придем к уравнению

$$\Delta x_i = 0, \tag{2}$$

ибо все $b^{(i)} = 0$.

Итак, мы приходим к следующей системе уравнений

$$\Delta x_1 = 0, \quad \Delta x_2 = 0, \ \ldots, \ \Delta x_n = 0. \tag{3}$$

Если определитель Δ it не равен нулю, то из уравнений (3) получаем

$$x_1 = 0, \quad x_2 = 0, \ \ldots, \ x_n = 0.$$

т. е. равны нулю все неизвестные. Если же $\Delta = 0$, то значения неизвестных произвольны.

Отсюда получаем теорему: *Если однородные уравнения* 1*-ой степени* (1) *допускают отличных от нуля значения неизвестных, то должен, обязательно, равняться нулю определитель, составленный из коэффициентов.*

§ 17

Из того обстоятельства, что можно определитель разложением по элементам горизонтали (колонны) представить в виде линейной функции от элементов этой горизонтали, следуют такие свойства определителей.

1. От умножения на некоторое число k всех элементов некоторой горизонтали (колонны) определитель получает этого множителя, например

$$\begin{vmatrix} a_1 & ka_2 & a_3 \\ b_1 & kb_2 & b_3 \\ c_1 & kc_2 & c_3 \end{vmatrix} = k \begin{vmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{vmatrix}.$$

2. Если все члены какой либо горизонтали (колонны) представляют суммы m слагаемых, то весь определитель можно рассматривать, как сумму m определителей.

В самом деле, если

$$\Delta = \sum_k a_k{}^{(i)} A_k{}^{(i)},$$

а

$$a_k{}^{(i)} = \alpha_k{}^{(i)} + \beta_k{}^{(i)} + \ldots + \sigma_k{}^{(i)},$$

то

$$\Delta = \sum_k (\alpha_k{}^{(i)} + \beta_k{}^{(i)} + \ldots + \sigma_k{}^{(i)}) A_k{}^{(i)} = \sum_k \alpha_k{}^{(i)} A_k{}^{(i)} + \sum_k \beta_k{}^{(i)} A_k{}^{(i)} + \ldots + \sum_k \sigma_k{}^{(i)} A_k{}^{(i)}.$$

Другими словами, заданный определитель представился суммой определителей

$$\sum_k \alpha_k{}^{(i)} A_k{}^{(i)}, \quad \sum_k \beta_k{}^{(i)} A_k{}^{(i)}, \ \ldots \ \sum_k \sigma_k{}^{(i)} A_k{}^{(i)},$$

которые получаются от замены элементов $a_k{}^{(i)}$ k-ой колонны числами $\alpha_k{}^{(i)}, \beta_k{}^{(i)}, \ldots, \sigma_k{}^{(i)}$.

Например[2]

$$\begin{vmatrix} \alpha_1{}^{(1)} + \alpha_1{}^{(2)} + \alpha_1{}^{(3)} & a_1{}^{(2)} & a_1{}^{(3)} \\ \alpha_2{}^{(1)} + \alpha_2{}^{(2)} + \alpha_2{}^{(3)} & a_2{}^{(2)} & a_2{}^{(3)} \\ \alpha_3{}^{(1)} + \alpha_3{}^{(2)} + \alpha_3{}^{(3)} & a_3{}^{(2)} & a_3{}^{(3)} \end{vmatrix} =$$

$$\begin{vmatrix} \alpha_1{}^{(1)} & a_1{}^{(2)} & a_1{}^{(3)} \\ \alpha_2{}^{(1)} & a_2{}^{(2)} & a_2{}^{(3)} \\ \alpha_3{}^{(1)} & a_3{}^{(2)} & a_3{}^{(3)} \end{vmatrix} + \begin{vmatrix} \alpha_1{}^{(2)} & a_1{}^{(2)} & a_1{}^{(3)} \\ \alpha_2{}^{(2)} & a_2{}^{(2)} & a_2{}^{(3)} \\ \alpha_3{}^{(2)} & a_3{}^{(2)} & a_3{}^{(3)} \end{vmatrix} + \begin{vmatrix} \alpha_1{}^{(3)} & a_1{}^{(2)} & a_1{}^{(3)} \\ \alpha_2{}^{(3)} & a_2{}^{(2)} & a_2{}^{(3)} \\ \alpha_3{}^{(3)} & a_3{}^{(2)} & a_3{}^{(3)} \end{vmatrix}.$$

§ 18

При вычислении определителей имеет важное значение следующее *свойство* определителя: можно без изменения величины определителя прибавить к элементам некоторой горизонтали (колонны) соответственные элементы другой горизонтали (колонны), умноженные на произвольного множителя k. В самом деле, определитель

$$\begin{vmatrix} a_1 & a_2 + ka_1 & a_3 \\ b_1 & b_2 + kb_1 & b_3 \\ c_1 & c_2 + kc_1 & c_3 \end{vmatrix}$$

может быть представлен в виде суммы определителей

$$\begin{vmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{vmatrix} + \begin{vmatrix} a_1 & ka_1 & a_3 \\ b_1 & kb_1 & b_3 \\ c_1 & kc_1 & c_3 \end{vmatrix}.$$

В последней сумме 2-ой определитель равен нулю, ибо он равен

$$k \begin{vmatrix} a_1 & a_1 & a_3 \\ b_1 & b_1 & b_3 \\ c_1 & c_1 & c_3 \end{vmatrix}.$$

Итак, мы получаем равенство

$$\begin{vmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{vmatrix} = \begin{vmatrix} a_1 & a_2 + ka_1 & a_3 \\ b_1 & b_2 + kb_1 & b_3 \\ c_1 & c_2 + kc_1 & c_3 \end{vmatrix},$$

выражающее справедливость высказанной теоремы.

§ 19

Решить уравнение относительно x

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

[2]В этом примере верхними значками обозначены колонны, что, конечно, также возможно сделать

В самом деле,

$$\begin{vmatrix} a_1 & a_2 & a_3+0 \\ b_1 & b_2 & b_3+0 \\ c_1 & c_2 & c_3+x \end{vmatrix} = \begin{vmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{vmatrix} + \begin{vmatrix} a_1 & a_2 & 0 \\ b_1 & b_2 & 0 \\ c_1 & c_2 & x \end{vmatrix} = 0$$

или

$$\begin{vmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{vmatrix} + x(-1)^{3+3} \begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix} = 0.$$

Откуда окончательно

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

Умножение определителей

§ 20

Будем рассматривать следующее линейное преобразование

$$\begin{aligned} x_1 &= a_1{}^{(1)}x'_1 + a_2{}^{(1)}x'_2 + \ldots + a_n{}^{(1)}x'_n \\ x_2 &= a_1{}^{(2)}x'_1 + a_2{}^{(2)}x'_2 + \ldots + a_n{}^{(2)}x'_n \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ x_n &= a_1{}^{(n)}x'_1 + a_2{}^{(n)}x'_2 + \ldots + a_n{}^{(n)}x'_n \end{aligned} \tag{1}$$

заменяющее переменные независимые

$$x_1 \;\; x_2 \;\; \ldots \;\; x_n$$

новыми

$$x'_1 \;\; x'_2 \;\; \ldots \;\; x'_n.$$

Если мы обозначим через A матрицу, образованную из коэффициентов преобразования (1), то для сокращения письма можно обозначить преобразование (1) такою символическою формулою:

$$x = A(x'). \tag{2}$$

Перейдем от переменных

$$x'_1 \;\; x'_2 \;\; \ldots \;\; x'_n$$

к новым третьим

$$x''_1 \;\; x''_2 \;\; \ldots \;\; x''_n$$

при помощи нового линейного преобразования

$$\begin{aligned} x'_1 &= b_1{}^{(1)}x''_1 + b_2{}^{(1)}x''_2 + \ldots + b_n{}^{(1)}x''_n \\ x'_2 &= b_1{}^{(2)}x''_1 + b_2{}^{(2)}x''_2 + \ldots + b_n{}^{(2)}x''_n \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ x'_n &= b_1{}^{(n)}x''_1 + b_2{}^{(n)}x''_2 + \ldots + b_n{}^{(n)}x''_n \end{aligned} \tag{3}$$

которое можно символически написать

$$x' = B(x'') \tag{4}$$

Если мы в правых частях равенств (1) подставим вместо $x'_1 \;\; x'_2 \;\; \ldots \;\; x'_n$ их выражения (3), то у нас получится новое линейное преобразование, переводящее первоначальный переменные $x_1 \;\; x_2 \;\; \ldots \;\; x_n$ в $x''_1 \;\; x''_2 \;\; \ldots \;\; x''_n$.

Пусть это прообразование будет

$$\begin{aligned} x_1 &= c_1{}^{(1)}x''_1 + c_2{}^{(1)}x''_2 + \ldots + c_n{}^{(1)}x''_n \\ x_2 &= c_1{}^{(2)}x''_1 + c_2{}^{(2)}x''_2 + \ldots + c_n{}^{(2)}x''_n \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ x_n &= c_1{}^{(n)}x''_1 + c_2{}^{(n)}x''_2 + \ldots + c_n{}^{(n)}x''_n \end{aligned} \tag{5}$$

которое обозначили, символически

$$x = C(x''). \tag{6}$$

Очевидно, что преобразование (5) есть результат двух преобразований (1) и (3), причем сначала произведено преобразование (1), а потом преобразование (3). Можем написать, следовательно, на основании (2) и (4)

$$x = AB(x''). \tag{7}$$

Формула (7) написана таким образом, чтобы подчеркнуть то обстоятельство, что преобразование (6) с матрицей C получается от последовательного производства двух преобразований: сначала преобразование с матрицей A, а потом преобразование с матрицей B.

Мы будем писать символическое равенство

$$C = A \cdot B \tag{8}$$

и говорить, что матрица C происходит от умножения матрицы A на матрицу B.

Посмотрим, как составляются элементы матрицы C по элементам матриц A и B. Нетрудно убедиться, что мы приходим к формул

$$c_i{}^{(k)} = a_1{}^{(k)}b_i{}^{(1)} + a_2{}^{(k)}b_i{}^{(2)} + a_3{}^{(k)}b_i{}^{(3)} + \ldots + a_n{}^{(k)}b_i{}^{(n)}. \tag{9}$$

Итак, мы замечаем, что каждый элемент $c_i{}^{(k)}$ матрицы C, представляющий из себя произведение матриц A и B, образуется по формуле (9) из элементов k-ой горизонтали 1-ого множителя A и элементов i-ой колонны 2-ого множителя B.

Нетрудно на простых примерах заметить, что, если мы будем 2 матрицы считать равными только в случай их полной тождественности, то умножение матриц есть операция не перестановочная, т. е. вообще говоря $A \cdot B$ не равно $B \cdot A$.

§ 21

Теорема. *Определитель матрицы $C = A \cdot B$ равен произведению определителей матриц A и B.*

Если мы условимся обозначать знаком $|A|$ определитель матрицы A, то теорема выразится равенством

$$|C| = |A| \cdot |B|.$$

В самом деле, мы имеем

$$|C| = \begin{vmatrix} a_1{}^{(1)}b_1{}^{(1)} + a_2{}^{(1)}b_1{}^{(2)} + a_3{}^{(1)}b_1{}^{(3)} + \dots & a_1{}^{(1)}b_2{}^{(1)} + a_2{}^{(1)}b_2{}^{(2)} + \dots \\ a_1{}^{(2)}b_1{}^{(1)} + a_2{}^{(2)}b_1{}^{(2)} + a_3{}^{(2)}b_1{}^{(3)} + \dots & a_1{}^{(2)}b_2{}^{(2)} + a_2{}^{(2)}b_2{}^{(2)} + \dots \\ a_1{}^{(3)}b_1{}^{(1)} + a_2{}^{(3)}b_1{}^{(2)} + a_3{}^{(3)}b_1{}^{(3)} + \dots & a_1{}^{(3)}b_2{}^{(1)} + a_2{}^{(3)}b_2{}^{(2)} + \dots \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots & \end{vmatrix}. \tag{1}$$

Очевидно, что определитель правой части равенства (1) распадается, на сумму всевозможных таких определителей

$$\begin{vmatrix} a_{i_1}^{(1)}b_1^{(i_1)} & a_{i_2}^{(1)}b_2^{(i_2)} & \dots & a_{i_n}^{(1)}b_n^{(i_n)} \\ a_{i_1}^{(2)}b_1^{(i_1)} & a_{i_2}^{(2)}b_2^{(i_2)} & \dots & a_{i_n}^{(2)}b_n^{(i_n)} \\ \dots & \dots & \dots & \dots \\ a_{i_1}^{(n)}b_1^{(i_1)} & a_{i_2}^{(n)}b_2^{(i_2)} & \dots & a_{i_n}^{(i_n)}b_n^{(i_n)} \end{vmatrix} = b_1^{(i_1)}b_2^{(i_2)}\cdots b_n^{(i_n)} \begin{vmatrix} a_{i_1}^{(1)} & a_{i_2}^{(1)} & \dots & a_{i_n}^{(1)} \\ a_{i_1}^{(2)} & a_{i_2}^{(2)} & \dots & a_{i_n}^{(2)} \\ \dots & \dots & \dots & \dots \\ a_{i_1}^{(n)} & a_{i_2}^{(n)} & \dots & a_{i_n}^{(i_n)} \end{vmatrix}. \tag{2}$$

Это же выражение (2) будет равно 0, если среди чисел $i_1 \;\; i_2 \; \dots \; i_n$ будут одинаковые.

Итак, определитель (1), который мы вычисляем, будет суммой выражений (2), распространенных на такие целые значения

$$i_1 \;\; i_2 \; \dots \; i_n$$

которые представляют собою различные перемещения без повторений целых чисел $1\ 2\ 3\ \dots\ n$, следовательно, получаем формулу

$$|C| = \sum b_1^{(i_1)}b_2^{(i_2)}\cdots b_n^{(i_n)} \begin{vmatrix} a_{i_1}^{(1)} & a_{i_2}^{(1)} & \dots & a_{i_n}^{(1)} \\ a_{i_1}^{(2)} & a_{i_2}^{(2)} & \dots & a_{i_n}^{(2)} \\ \dots & \dots & \dots & \dots \\ a_{i_1}^{(n)} & a_{i_2}^{(n)} & \dots & a_{i_n}^{(i_n)} \end{vmatrix}.$$

Нетрудно видеть, что если мы в последнем уравнении в правой его части приведем в порядок нижние значки под знаком определителя, то получим окончательно

$$|C| = |A| \; \sum (-1)^I b_1^{(i_1)}b_2^{(i_2)}\cdots b_n^{(i_n)},$$

где показатель I обозначает число беспорядков в перемещении

$$i_1 \;\; i_2 \; \dots \; i_n.$$

Мы получаем, следовательно, формулу

$$|C| = |A| \cdot |B|,$$

что и требовалось доказать.

§ 22

Доказанная в предыдущем параграфе теорема дает возможность представить произведение двух определителей одного и того же порядка в виде нового определителя того же порядка. Матрица произведения находится выше указанным правилом умножения матриц.

§ 23

Хотя правило умножения матриц не обладает перестановочным законом, но правило умножения определителей уже таким законом обладает, и мы получаем для двух матриц AB и BA один и тот же определитель

$$|A| \cdot |B|.$$

§ 24

Так как определитель не меняется от замены горизонталей колоннами, то вместо того, чтобы умножать горизонтали 1-го множителя на колонны 2-го, можно было бы поступить обратно, умножать колонны 1-го множителя на горизонтали 2-го или же, наконец, перемножать горизонтали обоих множителей или же колонны обоих множителей. Так, например,

$$\begin{vmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{vmatrix} \cdot \begin{vmatrix} \alpha_1 & \alpha_2 & \alpha_3 \\ \beta_1 & \beta_2 & \beta_3 \\ \gamma_1 & \gamma_2 & \gamma_3 \end{vmatrix} =$$

$$= \begin{vmatrix} a_1\alpha_1 + a_2\alpha_2 + a_3\alpha_3 & a_1\beta_1 + a_2\beta_2 + a_3\beta_3 & a_1\gamma_1 + a_2\gamma_2 + a_3\gamma_3 \\ b_1\alpha_1 + b_2\alpha_2 + b_3\alpha_3 & b_1\beta_1 + b_2\beta_2 + b_3\beta_3 & b_1\gamma_1 + b_2\gamma_2 + b_3\gamma_3 \\ c_1\alpha_1 + c_2\alpha_2 + c_3\alpha_3 & c_1\beta_1 + c_2\beta_2 + c_3\beta_3 & c_1\gamma_1 + c_2\gamma_2 + c_3\gamma_3 \end{vmatrix} =$$

$$= \begin{vmatrix} a_1\alpha_2 + b_1\alpha_2 + c_1\alpha_3 & a_1\beta_1 + b_1\beta_2 + c_1\beta_3 & a_1\gamma_1 + b_1\gamma_2 + c_1\gamma_3 \\ a_2\alpha_1 + b_2\alpha_2 + c_2\alpha_3 & a_2\beta_1 + b_2\beta_2 + c_2\beta_3 & a_2\gamma_1 + b_2\gamma_2 + c_2\gamma_3 \\ a_3\alpha_1 + b_3\alpha_2 + c_3\alpha_3 & a_3\beta_1 + b_3\beta_2 + c_3\beta_3 & a_3\gamma_1 + b_3\gamma_2 + c_3\gamma_3 \end{vmatrix}$$

и т. д.

§ 25

Распространим теперь правило перемножения квадратных матриц на случай матриц не квадратных, предполагая эти матрицы *подобными* в том смысл что у них одинаковое число как горизонталей, так и колонн.

Отступим от установленного нами в § 20 для квадратных ыатриц правила умножения, состоящего в умножений элементе в горизонтали первого (левого) множителя на элементы колонны второго.

Будем производить перемножения матриц при помоции перемножетя горизонталей.

Рассмотрим сначала случай перемножения по горизонталям матриц, число колонн которых меньше числа горизонталей.

Возьмем, например,

$$\left\|\begin{matrix} a & a_1 \\ b & b_1 \\ c & c_1 \end{matrix}\right\| \quad \text{и} \quad \left\|\begin{matrix} \alpha & \alpha_1 \\ \beta & \beta_1 \\ \gamma & \gamma 1 \end{matrix}\right\|$$

Перемножая по горизонталям, получим матрицу

$$\left\|\begin{matrix} a\alpha + a_1\alpha_1 & a\beta + a_1\beta_1 & a\gamma + a_1\gamma_1 \\ b\alpha + b_1\alpha_1 & b\beta + b_1\beta_1 & b\gamma + b_1\gamma_1 \\ c\alpha + c_1\alpha_1 & c\beta + c_1\beta_1 & c\gamma + c_1\gamma_1 \end{matrix}\right\|.$$

Нетрудно видеть, что определитель последней матрицы равен нулю ибо этот определитель может быть переписан так

$$\begin{vmatrix} a\alpha + a_1\alpha_1 + 0\cdot 0 & a\beta + a_1\beta_1 + 0\cdot 0 & a\gamma + a_1\gamma_1 + 0\cdot 0 \\ b\alpha + b_1\alpha_1 + 0\cdot 0 & b\beta + b_1\beta_1 + 0\cdot 0 & b\gamma + b_1\gamma_1 + 0\cdot 0 \\ c\alpha + c_1\alpha_1 + 0\cdot 0 & c\beta + c_1\beta_1 + 0\cdot 0 & c\gamma + c_1\gamma_1 + 0\cdot 0 \end{vmatrix}$$

откуда мы видим, что он равен произведений таких 2-х определителей

$$\begin{vmatrix} a & a_1 & 0 \\ b & b_1 & 0 \\ c & c_1 & 0 \end{vmatrix}, \qquad \begin{vmatrix} \alpha & \alpha_1 & 0 \\ \beta & \beta_1 & 0 \\ \gamma & \gamma_1 & 0 \end{vmatrix},$$

из которых каждый равен нулю.

При помощи аналогичных рассуждений можно будет доказать такую общую теорему:

От перемножения по горизонталями двух подобных матриц, число колонн которых меньше числа горизонталей, получается квадратная матрица, определитель которой равен нулю.

§ 26

Рассмотрим теперь случай перемножения по горизонталям 2-х матриц, у которых число колонн больше числа горизонталей

$$\left\|\begin{matrix} a & b & c \\ a_1 & b_1 & c_1 \end{matrix}\right\|, \qquad \left\|\begin{matrix} \alpha & \beta & \gamma \\ \alpha_1 & \beta_1 & \gamma_1 \end{matrix}\right\|$$

После умножения получаем матрицу

$$\left\|\begin{matrix} a\alpha + b\beta + c\gamma & a_1\alpha + b_1\beta + c_1\gamma \\ a\alpha_1 + b\beta_1 + c\gamma_1 & a_1\alpha_1 + b_1\beta_1 + c_1\gamma_1 \end{matrix}\right\|$$

Эта матрица имеет определитель, который на основании соображений, подобных приведенным в § 21, представится в виде суммы произведений таких определителей

$$\begin{vmatrix} a & b \\ a_1 & b_1 \end{vmatrix} \cdot \begin{vmatrix} \alpha & \beta \\ \alpha_1 & \beta_1 \end{vmatrix} + \begin{vmatrix} a & c \\ a_1 & c_1 \end{vmatrix} \cdot \begin{vmatrix} \alpha & \gamma \\ \alpha_1 & \gamma_1 \end{vmatrix} + \begin{vmatrix} b & c \\ b_1 & c_1 \end{vmatrix} \cdot \begin{vmatrix} \beta & \gamma \\ \beta_1 & \gamma_1 \end{vmatrix}$$

и мы приходим к такой общей теореме:

От перемножения по горизонталям двух подобных матриц, число колонн которых больше числа горизонталей, получается квадратная матрица, определитель которой равен сумме произведений всевозможных определителей одной матрицы на соответственные определители другой.

В этой теореме определители имеют порядок, равный числу горизонталей перемножаемых матриц.

§ 27

Покажем приложение последней теоремы к выводу замечательного тождества, указанного Euler'ом.

Возвысим по горизонталям в квадрат матрицу

$$\left\| \begin{matrix} a & b & c & d \\ a_1 & b_1 & c_1 & d_1 \end{matrix} \right\|$$

т. е., другими словами, перемножим две тождественные матрицы. Получим по теореме предыдущего §-а формулу

$$\begin{vmatrix} a^2+b^2+c^2+d^2 & a_1+b_1b+c_1c+d_1d \\ aa_1+bb_1+cc_1+dd_1 & a_1^2+b_1^2+c_1^2+d_1^2 \end{vmatrix} \tag{1}$$
$$(ab_1)^2+(ac_1)^2+(ad_1)^2+(bc_1)^2+(bd_1)^2+(cd_1)^2,$$

где $(ab+1)=\begin{vmatrix} a & b \\ a_1 & b_1 \end{vmatrix} = ab_1 - a_1b$, $(ac_1) = ac_1 - a_1c$) и т. д.

Нетрудно видеть (см. § 18), что существует тождество

$$\begin{vmatrix} ab_1-ba_1 & b_1 & b \\ ac_1-ca_1 & c_1 & c \\ ad_1-da_1 & d_1 & d \end{vmatrix} = 0. \tag{2}$$

Раскладывая тождество (2) по элементам первой колонны, получим

$$(ab_1-ba_1)(c_1d-d_1c)+(ac_1-ca_1)(bd_1-db_1)+(ad_1-da_1)(b_1c-cb_1)=0.$$

Перепишем это тождество так:

$$(ab_1)(c_1d)+(ac_1)(bd_1)+(ad_1)(b_1c)=0. \tag{3}$$

Перепишем равенство (1) следующим образом

$$(a^2+b^2+c^2+d^2)(a_1^2+b_1^2+c_1^2+d_1)^2-(aa_1+bb_1+cc_1+dd_1)^2 = \\ = (ab_1)^2+(ac_1)^2+(ad_1)^2+(bc_1)^2+(bd_1)^2+(cd_1)^2,$$

прикладывая к правой части последнего равенства удвоенное тождество (3), получим

$$(a^2+b^2+c^2+d^2)(a_1^2+b_1^2+c_1^2+d_1)^2-(aa_1+bb_1+cc_1+dd_1)^2 = \\ = [(ab_1)+(c_2)]^2+[(ac_1)+(bd_1)]^2+[(ad_1)+(b_1c)]^2.$$

Это тождество можно окончательно переписать так

$$(a^2+b^2+c^2+d^2)(a_1^2+b_1^2+c_1^2+d_1)^2 =$$
$$= (aa_1+bb_1+cc_1+dd_1)^2+(ab_1-ba_1+c_1d-cd+_1)^2+$$
$$+(ac_1-ca_1+bd_1-b_1d)^2+(ad_1-a_1d=b_1c-bc_1)^2.$$

Это тождество Euler'а выражает такую теорему.

Если перемножаются два выражения, из которых каждое есть сумма четырех квадратов, то и произведение есть сумма четырех квадратов.

Эта теорема применяется между прочим при доказательстве теоремы теории чисел, что всякое целое число есть сумма четырех квадратов, напр. $31 = 3^2+3^2+3^2+2^2$.

§ 28

Рассмотрим два уравнения с тремя неизвестными

(1)
$$\begin{aligned} ax+by+cz&=0\\ a_1x+b_1y+c_1z&=0 \end{aligned}$$

Непосредственное вычисление показывает. что можно преобразовать заданную систему (1) в такую пропорцию

$$\frac{x}{\begin{vmatrix} b & c\\ b_1 & c_1\end{vmatrix}} = \frac{y}{\begin{vmatrix} c & a\\ c_1 & a_1\end{vmatrix}} = \frac{z}{\begin{vmatrix} a & b\\ a_1 & b_1\end{vmatrix}}.$$

Итак, уравнения (1) удовлетворяются значениями

$$bc_1-cb_1,\quad ca_1-asc_1,\quad ab_1-ba_1$$

неизвестных x, y, z.

Указанное свойство системы (1) обобщается на случай $n-1$ однородных уравнений с n неизвестными

(2)
$$\begin{array}{lllll} a_1x_1 & +b_1x_2 & +c_1x_3 & +\dots & +g_1x_n=0\\ a_2x_1 & +b_2x_2 & +c_2x_3 & +\dots & +g_2x_n=0\\ \multicolumn{5}{c}{\dotfill}\\ a_{n-1}x_1 & +b_{n-1}x_2 & +c_{n-1}x_3 & +\dots & +g_{n-1}x_n=0 \end{array}$$

Нетрудно убедиться, что эти уравнения равносильны такой пропорции

(3)
$$\frac{x_1}{\begin{vmatrix} b_1 & c_1 & \dots & g_1\\ \multicolumn{4}{c}{\dotfill}\\ b_{n-1} & c_{n-1} & \dots & g_{n-1}\end{vmatrix}} = \frac{x_1}{\begin{vmatrix} c_1 & \dots & g_1 & a_1\\ \multicolumn{4}{c}{\dotfill}\\ c_{n-1} & \dots & g_{n-1} & a_{n-1}\end{vmatrix}} = \dots,$$

т. е., другими словами, система (2) удовлетворяется, если мы положим вместо $x_1, x_2, \dots, x_n$ соответственные определители, столице в знаменателях (3). После

подстановки уравнения (2) обращаются, очевидно, в тождества, ибо левые их части становятся определителями с двумя одинаковыми горизонталями.

Линейные формы

§ 29

Будем рассматривать m функций первой степени от n неизвестных

$$x_1,\ \ x_2,\ \ x_3,\ \ldots,\ x_n, \tag{1}$$

а именно функций вида

$$\begin{aligned} X_1 &= a_1{}^{(1)}x_1 + a_1{}^{(2)}x_2 + \ldots + a_1{}^{(n)}x_n - b_1, \\ X_2 &= a_2{}^{(1)}x_1 + a_2{}^{(2)}x_2 + \ldots + a_2{}^{(n)}x_n - b_2, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ X_m &= a_m{}^{(1)}x_1 + a_m{}^{(2)}x_2 + \ldots + a_m{}^{(n)}x_n - b_m, \end{aligned} \tag{2}$$

Мы будем называть линейные функции (2) *независимыми* между собою, если можно подобрать такие численные значения независимых переменных (1), чтобы функции $X_1,\ \ X_2,,\ \ldots,\ X_m$ получили ряд произвольно назначенных численных значений, т. е. чтобы было

$$X_1 = \alpha_1, \quad X_2 = \alpha_2,, \quad \ldots, \quad X_m = \alpha_m, \tag{3}$$

где числа $\alpha_1,\ \ \alpha_2, \ldots, \alpha_m$ совершенно произвольные.

Если же равенства (3) перестанут удовлетворяться при некотором выборе чисел $\alpha_1,\ \ \alpha_2, \ldots, \alpha_m$, то мы будем говорить, что функций $X_1,\ \ X_2,,\ \ldots,\ X_m$ *зависимы* между собою.

§ 30

Рассмотрим случай $m = n$. Тогда вопрос о независимости функций $X_1,\ \ X_2,,\ \ldots,\ X_m$ приводится в вопросу решения следующей системы уравнений

$$\begin{aligned} X_1 &= a_1{}^{(1)}x_1 + a_1{}^{(2)}x_2 + \ldots + a_1{}^{(n)}x_n - b_1, \\ X_2 &= a_2{}^{(1)}x_1 + a_2{}^{(2)}x_2 + \ldots + a_2{}^{(n)}x_n - b_2, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ X_n &= a_n{}^{(1)}x_1 + a_n{}^{(2)}x_2 + \ldots + a_n{}^{(n)}x_n - b_n, \end{aligned} \tag{1}$$

с n неизвестными $x_1,\ \ x_2,\ \ldots,\ x_n$.

Рассмотрим определитель

$$\Delta = \begin{vmatrix} a_1{}^{(1)} & a_1{}^{(2)} & \ldots & a_1{}^{(n)} \\ a_2{}^{(1)} & a_2{}^{(2)} & \ldots & a_2{}^{(n)} \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots \\ a_n{}^{(1)} & a_n{}^{(2)} & \ldots & a_n{}^{(n)} \end{vmatrix}, \tag{2}$$

а также *взаимный* определитель

$$\Delta^{n-1} = \begin{vmatrix} A_1{}^{(1)} & A_1{}^{(2)} & \dots & A_1{}^{(n)} \\ A_2{}^{(1)} & A_2{}^{(2)} & \dots & A_2{}^{(n)} \\ \dots\dots\dots\dots\dots\dots\dots\dots \\ A_n{}^{(1)} & A_n{}^{(2)} & \dots & A_n{}^{(n)} \end{vmatrix}. \tag{3}$$

Обозначим

$$\Delta_h = b_1 A_1{}^{(h)} + b_2 A_2{}^{(h)} + \dots + b_n A_n{}^{(h)}.$$

Очевидно, что Δ_h есть ничто иное, как определитель, который получается от замены h-ой колонны определителя Δ колонной коэффициентов $b_1,\ b_2,\ \dots,\ b_n$.

Умножая уравнения (1) последовательно на миноры 1-ой колонны взаимного определителя и складывая, получим

$$\Delta x_1 - b_1 = X_1 A_1{}^{(1)} + X_2 A_2{}^{(1)} + \dots + X_n A_n{}^{(1)}; \tag{4}$$

совершенно подобным образом, умножая на другие колонны определителя, получим ряд равенств

$$\begin{aligned} \Delta x_2 - b_2 &= X_1 A_1{}^{(2)} + X_2 A_2{}^{(2)} + \dots + X_n A_n{}^{(2)}, \\ &\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots, \\ \Delta x_n - b_n &= X_1 A_1{}^{(n)} + X_2 A_2{}^{(n)} + \dots + X_n A_n{}^{(n)}. \end{aligned} \tag{5}$$

Равенства (4) и (5) показывают, что для независимости рассматриваемых n функций необходимо и достаточно, чтобы определитель Δ был отличен от нуля, потому что только в этом случае мы получим определенные значения неизвестных $x_1,\ x_2,\ \dots,\ x_n$, если произвольно заданы численные значения функций $X_1,\ X_2,,\ \dots,\ X_n$.

В частном случае, когда положим

$$X_1 = 0,\ \ X_2 = 0,\ \dots,\ X_n = 0, \tag{6}$$

то получаем, очевидно, основную задачу о решении n уравнений 1-ой степени с n неизвестными, и получается, следовательно, теорема:

Система уравнений (6) *имеет определенное решение только в том случае, когда определитель* Δ *не равен нулю, и тогда по уравнениям* (4) *и* (5) *получается решение этой системы в таком виде*

$$x_1 = \frac{\Delta_1}{\Delta},\ \ x_2 = \frac{\Delta_2}{\Delta},\ \dots,\ x_n = \frac{\Delta_n}{\Delta}.$$

§ 31

Чтобы дополнить анализ, надо было бы рассмотреть случай $\Delta = 0$, но будет короче, если мы этот случай будем рассматривать, как частный случай более общих соображений, к которым мы теперь перейдем.

Ранг системы линейных функций

§ 32

Вернемся теперь к самому общему случаю, разобранному в § 29, когда число функций m не равно числу переменных n.

Составим теперь прямоугольную фигуру

$$\begin{array}{cccc} a_1{}^{(1)}, & a_1{}^{(2)}, & \ldots, & a_1{}^{(2)} \\ a_2{}^{(1)}, & a_2{}^{(2)}, & \ldots, & a_2{}^{(2)} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_m{}^{(1)}, & a_m{}^{(2)}, & \ldots, & a_m{}^{(2)} \end{array}$$

из коэффициентов этих функций при неизвестных таким образом, чтобы по горизонталям находились коэффициенты одной и той же функции, а по колоннам коэффициенты при одном и том же неизвестном.

Будем называть полученную таким образом фигуру *матрицей* коэффициентов заданной системы функций. Если мы укажем α некоторых горизонталей матрицы, а также α вертикалей ее, то из α^2 элементов находящихся на пересечении выбранных горизонталей с выбранными вертикалями, можно будет составить определитель; если мы этот определитель так составим, что элементы какой нибудь горизонтали матрицы образуют горизонталь в определителе, и также элементы вертикали матрицы образуют вертикаль в определителе, то будем говорить что полученный таким образом определитель *взят* из матрицы. Очевидно что, если $\alpha = 1$, то определитель, взятый из матрицы, будет ничем иным, как одним из ее элементов. Конечно, самое большое значение порядка α определителя, взятого из матрицы, не может превосходить наименьшего из чисел m и n.

Назовем *рангом* матрицы наибольший порядок отличного от нуля определителя, взятого из матрицы.

Поясним наше определение примерами:

1-ый пример. Все элементы матрицы равны нулю. Очевидно, что в этом случае будут равняться нулю все определители, взятые из матрицы. Можно сказать, что в этом случае ранг матрицы равен нулю. Обыкновенно матрицы ранга, равного нулю не рассматриваются.

2-ой пример. Покажем пример матрицы ранга, равного единице. Возьмем матрицу

$$\begin{array}{cccc} \alpha_1\beta_1, & \alpha_1\beta_2, & \ldots, & \alpha_1\beta_n \\ \alpha_2\beta_1, & \alpha_2\beta_2, & \ldots, & \alpha_2\beta_n \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \alpha_n\beta_1, & \alpha_n\beta_2, & \ldots, & \alpha_n\beta_n \end{array} \tag{1}$$

каждый элемент которой состоять из двух множителей, причем первые множители одинаковы по горизонталям, а вторые множители одинаковы по вертикалям. Если ни один из входящих в рассмотрение множителей не равен нулю, то не будет равняться нулю ни один из элементов матрицы, т. е., другими словами, все определители первого порядка данной матрицы отличны от нуля. Нетрудно убедиться,

что все определители, взятые из данной матрицы, начиная со второго порядка, будут равны нулю. Например, определители

$$\begin{vmatrix} \alpha_1\beta_1 & \alpha_1\beta_2 & \alpha_1\beta_3 \\ \alpha_2\beta_1 & \alpha_2\beta_2 & \alpha_2\beta_3 \\ \alpha_3\beta_1 & \alpha_3\beta_2 & \alpha_3\beta_3 \end{vmatrix} = \alpha_1\alpha_2\alpha_3 \begin{vmatrix} \beta_1 & \beta_2 & \beta_3 \\ \beta_1 & \beta_2 & \beta_3 \\ \beta_1 & \beta_2 & \beta_3 \end{vmatrix} = 0,$$

$$\begin{vmatrix} \alpha_1\beta_1 & \alpha_1\beta_2 \\ \alpha_2\beta_1 & \alpha_2\beta_2 \end{vmatrix} = \alpha_1\alpha_2 \begin{vmatrix} \beta_1 & \beta_2 \\ \beta_1 & \beta_2 \end{vmatrix} = 0.$$

Итак, мы видим, что ранг заданной матрицы есть 1-ый.

Нетрудно показать, что самый обший вид матрицы 1-го ранга есть вышенаписанный (1).

3-ий пример. Рассмотренный в § 30 случай неравенства нулю определителя Δ, составленного из всей квадратной матрицы с n колоннами и с n горизонталями, убеждает нас, что матрица этого определителя имеет ранг n.

§ 33

Покажем теперь условия, необходимые и достаточный для совместимости m уравнений с n неизвестными. Рассмотрим опять систему (2) линейных функций § 29.

Составим матрицу коэффициентов при неизвестных для этих функций. Пусть ранг этой матрицы будет p. Будем число p называть *рангом системы.* Тогда очевидно, что существует по крайней мере один определитель порядка p, взятый из матрицы, который не будет равняться нулю; все же определители высших порядков будут равны нулю. Если будет несколько неравных нулю определителей порядка p, тогда мы возьмем один из них. Будем называть *главным* этот неравный нулю определитель порядка p матрицы ранга p. Не нарушая общности вопроса, мы можем считать, что главный определитель будет

$$\delta = \begin{vmatrix} a_1{}^{(1)}, & a_1{}^{(2)}, & \dots, & a_1{}^{(p)} \\ a_2{}^{(1)}, & a_2{}^{(2)}, & \dots, & a_2{}^{(p)} \\ \dots\dots\dots\dots\dots\dots\dots\dots \\ a_p{}^{(1)}, & a_p{}^{(2)}, & \dots, & a_p{}^{(p)} \end{vmatrix},$$

потому что всегда можем переставить, как функции, так и переменные.

Составим теперь следующий определитель $p+1$ порядка

$$\delta_{p+\alpha} = \begin{vmatrix} a_1{}^{(1)}, & a_1{}^{(2)}, & \dots, & a_1{}^{(2)} & b_1 \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ a_p{}^{(1)}, & a_p{}^{(2)}, & \dots, & a_p{}^{(p)}, & b_p \\ a_{p+\alpha}{}^{(1)}, & a_{p+\alpha}{}^{(2)}, & \dots, & a_{p+\alpha}{}^{(p)}, & b_{p+\alpha} \end{vmatrix}.$$

Очевидно, что таких определителей можно будет составить $m-p$, давая числу α значения $1, 2, 3, \dots, m-p$. Будем называть такие определители *характеристическими.* Если бы случилось, что $p = m$, то мы скажем, что характеристический определитель равен нулю.

Основная теорема. *Необходимым и достаточным условием совместимости m уравнений первой степени с n неизвестными является равенство нулю всех*

характеристических определителей. Если ранг системы равен числу неизвестных, то получается одна система решений; во всех других случаях получается бесчисленное множество решений.

В самом деле, рассмотрим определитель

$$(2)\qquad \begin{vmatrix} a_1{}^{(1)}, & a_1{}^{(2)}, & \dots, & a_1{}^{(p)} & X_1 \\ a_2{}^{(1)}, & a_2{}^{(2)}, & \dots, & a_2{}^{(p)} & X_2 \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ a_p{}^{(1)}, & a_p{}^{(2)}, & \dots, & a_p{}^{(p)}, & X_p \\ a_{p+\alpha}{}^{(1)}, & a_{p+\alpha}{}^{(2)}, & \dots, & a_{p+\alpha}{}^{(p)}, & X_{p+\alpha} \end{vmatrix};$$

так как каждый элемент последней колонны есть сумма нескольких членов, то разложим этот определитель на сумму определителей; получаются определители следующих двух видов:

$$(3)\qquad \begin{vmatrix} a_1{}^{(1)}, & a_1{}^{(2)}, & \dots, & a_1{}^{(p)} & a_1{}^{(r)}x_r \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ a_p{}^{(1)}, & a_p{}^{(2)}, & \dots, & a_p{}^{(p)}, & a_p{}^{(r)}x_r \\ a_{p+\alpha}{}^{(1)}, & a_{p+\alpha}{}^{(2)}, & \dots, & a_{p+\alpha}{}^{(p)}, & a_{p+\alpha}{}^{(r)}x_r \end{vmatrix}$$

и

$$(4)\qquad \begin{vmatrix} a_1{}^{(1)}, & \dots, & a_1{}^{(p)}, & -b_1 \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ a_{p+\alpha}{}^{(1)}, & \dots, & a_{p+\alpha}{}^{(p)}, & -b_{p+\alpha} \end{vmatrix}$$

Что касается определителей (3), то все они равны нулю, ибо в них можно вынести из под знака определителя x_r и тогда у нас выйдет при $r \leq p$ определитель с двумя одинаковыми колоннами, а при $r > p$ получается определитель порядка $p1$, взятый из матрицы, а такие определители все равны нулю, потому что ранг матрицы есть p; значить, получаем равенство

$$(5)\qquad \begin{vmatrix} a_1{}^{(1)}, & a_1{}^{(2)}, & \dots, & a_1{}^{(p)}, & X_1 \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ a_p{}^{(1)}, & a_p{}^{(2)}, & \dots, & a_p{}^{(p)}, & X_p \\ a_{p+\alpha}{}^{(1)}, & a_{p+\alpha}{}^{(2)}, & \dots, & a_{p+\alpha}{}^{(p)}, & X_{p+\alpha} \end{vmatrix} = -\delta_{p+\alpha}.$$

Так как главный определитель δ отличен от нуля, то по теореме § 30 можно решить систему

$$(6)\qquad X_1 = 0, \quad X_2 = 0, \ \dots, \ X_p = 0$$

относительно p неизвестных

$$(7)\qquad x_1, \quad x_2, \dots, x_p$$

и выразить эти неизвестные при помощи линейных выражений через остальные переменные

$$(8)\qquad x_{p+1}, \ \dots, \ x_n,$$

которые остаются совершенно произвольными. Дадим этим последним какие нибудь произвольные частные значения, например,

$$x'_{p+1},\quad x'_{p+2},\ \ldots,\ x'_n; \tag{9}$$

тогда через решение уравнений (6) относительно неизвестных (7) получим соответствующая значения

$$x'_1,\quad x'_2,\ldots,\ x'_p. \tag{10}$$

Итак, совокупность значений (9) и (10) обращает уравнения (6) в тождества. Подставим значения (9) и (10) в функцию

$$X_{p+\alpha};$$

пусть эта функция получит значение $X'_{p+\alpha}$. Если мы подставим те же самые численные значения (9) и (10) в уравнение (5), то это уравнение может быть переписано так

$$\delta X'_{p+\alpha} = -\delta_{p+\alpha}. \tag{11}$$

Так как определитель δ не 0, то, если мы хотим. чтобы уравнения

$$X_1 = 0,\quad X_2 = 0,\ \ldots,\ X_p = 0,\ \ldots,\ X_m = 0$$

были совместны, то должно иметь место равенство

$$X'_{p+\alpha} = 0$$

при всяком значении α, потому что значения переменных, удовлетворяюшие первым p уравнениям, должны также и другим удовлетворять. Мы видим, что необходимым и достаточным условием равенства нулю всех $X'_{p+\alpha}$ является равенство нулю всех характеристических определителей:

$$\delta_{p+\alpha}.$$

Вторая часть теоремы следует из того, что, если $p = n$, то тогда все переменные заключаются в системе (7) и не существует уже произвольных переменных (8), так что решение получается вполне определенное.

§ 34

Поясним теорию предыдущего параграфа на простейших примерах.

1-ый пример. Дана система

$$\begin{aligned} ax + by &= c,\\ a_1x + b_1y &= c_1. \end{aligned} \tag{1}$$

1°. Ранг матрицы, составленной из коэффициентов при неизвестных, есть 2, значит, не равен нулю определитель

$$\begin{vmatrix} a & b\\ a_1 & b_1 \end{vmatrix};$$

мы получаем определенное решение системы (1)

$$x = \frac{-bc_1 + b_1c}{ab_1 - a_1b},$$
$$y = \frac{-ca_1 + ac_1}{ab_1 - a_1b}.$$

2°. Ранг матрицы равен 1; пусть главный определитель будет a, так что

$$a \text{ не } = 0$$

Тогда характеристический определитель будет

$$\delta = \begin{vmatrix} a & c \\ a_1 & c_1 \end{vmatrix}.$$

α) если δ не 0, то уравнения (1) несовместны,
β) если $\delta = 0$, то второе уравнение есть следствие первого, и мы получаем

$$x = -\frac{b}{a}y_1 + \frac{c}{a}$$
$$y = y_1,$$

где y_1 число совершенно произвольное.

2-ой пример. Пусть дана система:

$$\begin{aligned} ax + by + cz &= d, \\ a_1x + b_1y + c_1z &= d_1, \\ a_2x + b_2y + c_2z &= d_2. \end{aligned} \tag{2}$$

1°. Ранг матрицы коэффициентов первой части есть 3 , т. е. неравен нулю определитель

$$\begin{vmatrix} a & b & c \\ a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \end{vmatrix} = D.$$

Если введем взаимный определитель

$$\begin{vmatrix} A & B & C \\ A_1 & B_1 & C_1 \\ A_2 & B_2 & C_2 \end{vmatrix} = D^2,$$

то получается определенное решение системы

$$x = \frac{dA + d_1A_1 + d_2A_2}{D},$$
$$y = \frac{dB + d_1B_1 + d_2B_2}{D},$$
$$z = \frac{dC + d_1C_1 + d_2C_2}{D}.$$

2°. Ранг матрицы есть 2. Пусть главный определитель будет

$$C_2 = \begin{vmatrix} a & b \\ a_1 & b_1 \end{vmatrix};$$

тогда для совместности системы необходимо рассмотреть характеристический определитель

$$\delta = \begin{vmatrix} a & b & d \\ a_1 & b_1 & d_1 \\ a_2 & b_2 & d_3 \end{vmatrix} = dC + d_1C_1 + d_2C_2.$$

α) δ не $= 0$; в системе противоречие.

β) $\delta = 0$; тогда система совместна, но третье уравнение есть следствие первых двух; решая эти первые два уравнения относительно x и y, получим

$$\begin{aligned} x &= \frac{bc_1 - cb_1}{ab_1 - a_1b}z_1 + \frac{db_1 - bd_1}{ab_1 - a_1b}, \\ y &= \frac{ca_1 - ac_1}{ab_1 - a_1b}z_1 + \frac{ad_1 - da_1}{ab_1 - a_1b}, \\ z &= z_1, \end{aligned}$$

где z_1 совершенно произвольное число.

3°. Ранг матрицы есть 1. Главный определитель a не $= 0$. Тогда надо рассмотреть два характеристических определителя

$$\delta_1 = \begin{vmatrix} a & d \\ a_1 & d_1 \end{vmatrix}, \qquad \delta_2 = \begin{vmatrix} a & d \\ a_2 & d_2 \end{vmatrix}.$$

α) если по крайней мере одbн из двух характеристических определителей δ_1 и δ_2 не равен нулю, то в системе противоречие.

β) если $\delta_1 = 0$, $\delta_2 = 0$, то система совместна, но второе и третье уравнения равносильны первому, так что мы получаем следующее решение системы

$$\begin{aligned} x &= -\frac{b}{a}y_1 - \frac{c}{a}z_1, + \frac{d}{a}, \\ y &= y_1, \\ z &= z_1, \end{aligned}$$

где y_1 и z_1 совершенно произвольные числа.

§ 35

Обращаемся теперь к вопросу о независимости линейных функций в том случае, когда число функций не равняется числу переменных независимых. Будем называть *рангом* системы заданных линейных функций ранг матрицы, составленной из коэффициентов при неизвестных в этой системе. Докажем теорему.

Если ранг системы, функций

$$X_1, \quad X_2, \ldots, \; X_m$$

равен числу p, то независимыми из этих функций будут только p.

Рассмотрим сначала случай, когда ранг p равен числу m функций.

Так как рассуждения будут те же, что и в общем случае, то мы рассмотрим случай трех функций с пятью переменными независимыми

$$\begin{aligned} X &= ax + by + cz + du + et + f, \\ X_1 &= a_1x + b_1y + c_1z + d_1u + e_1t + f_1, \\ X_2 &= a_2x + b_2y + c_2z + d_2u + e_2t + f_2. \end{aligned} \tag{1}$$

Если ранг этой системы есть 3, то есть равен числу функций, то можно считать, что не равен нулю главный определитель

$$\begin{vmatrix} a & b & c \\ a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \end{vmatrix},$$

значит, можно будет систему (1) решить относительно трех переменных независимых x, y и z, причем выражения для этих переменных будут заключать, кроме коэффициентов, еще переменные независимые

$$\begin{matrix} u, & t, \\ X, & X_1, & X_2. \end{matrix} \tag{2}$$

Так как решение системы (1) зависело только от неравенства нулю главного определителя, а не от частных значений букв (2), то, значит, переменным X, X_1, X_2 можно дать численный значения по произволу, и, значит, наши функции все независимы между собою. Теорема подтверждается, ибо, действительно, оказывается, что число независимых функций равно рангу системы.

Рассмотрим теперь случай, когда ранг системы на единицу меньше числа функций. Пусть задана система четырех функций 3-го ранга

$$\begin{aligned} X &= ax + by + cz + du + et + f, \\ X_1 &= a_1x + b_1y + c_1z + d_1u + e_1t + f_1, \\ X_2 &= a_2x + b_2y + c_2z + d_2u + e_2t + f_2, \\ X_3 &= a_3x + b_3y + c_3z + d_3u + e_3t + f_3. \end{aligned} \tag{3}$$

Пусть главный определитель будет

$$\begin{vmatrix} a & b & c \\ a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \end{vmatrix}.$$

Рассмотрим еще характеристический определитель

$$\delta = \begin{vmatrix} a & b & c & f \\ a_1 & b_1 & c_1 & f_1 \\ a_2 & b_2 & c_2 & f_2 \\ a_3 & b_3 & c_3 & f_3 \end{vmatrix} = fF + f_1F_1 + f_2F_2 + f_3F_3, \tag{4}$$

где F_3 есть ничто иное, как главный определитель.

Умножить уравнения системы (3) последовательно на числа F, F_1, F_2, F_3, тогда получим после сложения

$$XF + X_1F_1 + X_2F_2 + X_3F_3 = \delta, \tag{5}$$

потому что от замены в определителе (4) последней колонны f, f_1, f_2, f_3 различными колоннами коэффициентов при неизвестных будут получаться нули, так как матрица есть 3-го ранга.

Решая равенство (5) относительно функций X_3, получим

$$X_3 == \frac{\delta}{F_3} - \frac{F}{F_3}X - \frac{F_1}{F_3}X_1 - \frac{F_2}{F_3}X_2,$$

т. е. имеем

$$X_3 = \alpha X + \beta X_1 + \gamma X_2 + \varepsilon, \tag{6}$$

где α, β, γ, ε суть определенные числа. Равенство (6) показывает, что заданные функций не независимы между собою, ибо, если зададим по произволу значения X, X_1, X_2, то значение четвертой функций X_3 не будет уже произвольным, а будет определяться по уравнению (6). Что касается трех функций X, X_1, X_2, то они независимы, потому что их ранг 3 равен числу функций. Итак, можно считать высказанную теорему вполне доказанною.

Рассмотрим численный пример:

$$\begin{aligned} X &= -x + y + z + 2t - 3, \\ X_1 &= x - y + z - 3u + 5, \\ X_2 &= x + y - z + 3u - 2t - 1, \\ X_3 &= x + y + z. \end{aligned}$$

Очевидно, что эти функций не независимы, потому что легко убедиться, что

$$X_3 = X + X_1 + X_2 - 1.$$

§ 36

Докажем еще теорему:

Если заданные линейные формы

$$X_1, \quad X_2, \ \ldots, \ X_m$$

от m независимых переменных не независимы, то существуешь тождество

$$\lambda_1X_1 + \lambda_2X_2 + \ldots + \lambda_mX_m = 0. \tag{1}$$

В самом деле, раскрывая тождество (1) и приравнивая нулю коэффициенты при всех неизвестных, получаем совместную систему уравнений первой степени относительно λ_1, λ_2, $\ldots$, λ_m, из которой получатся отличные от нуля значения этих неизвестных.

Из всего выше изложенного следует, что, если задана система зависимых линейных функций, то всегда можно выразить эти линейные функций линейным образом через независимые.

Теорема Laplace'a

§ 37

Пусть целое число σ меньше n. Рассмотрим все члены определителя $A = |a_i{}^{(k)}|$, в которых входит множитель

$$a_1{}^{(1)} a_2{}^{(2)} \cdots a_\sigma{}^{(\sigma)}. \tag{1}$$

представляющей произведение σ верхних элементов главной диагонали. Эти члены получатся из главного члена

$$a_1{}^{(1)} a_2{}^{(2)} \cdots a_\sigma{}^{(\sigma)} a_{\sigma+1}{}^{(\sigma+1)} \cdots a_n{}^{(n)},$$

если, оставляя без изменения верхние индексы, мы будем так менять нижние, что первые σ индексы $1, 2, \ldots, \sigma$ останутся без перемены, а меняются лишь остальные $\sigma+1, \sigma+2, \ldots, n$; при этом, конечно, члену всякий раз приписывается соответственный знак.

На оснований определения понятая об определителе рассматриваемая совокупность членов может быть представлена в таком виде

$$a_1{}^{(1)} a_2{}^{(2)} \cdots a_\sigma{}^{(\sigma)} \begin{vmatrix} a_{\sigma+1}{}^{(\sigma+1)} & a_{\sigma+2}{}^{(\sigma+1)} & \ldots & a_n{}^{(\sigma+1)} \\ & \ldots & & \\ a_{\sigma+1}{}^{(n)} & a_{\sigma+2}{}^{(n)} & \ldots & a_n{}^{(n)} \end{vmatrix}. \tag{2}$$

В последней формуле определитель получается из определителя A вычеркиванием первых (верхних) σ горизонталей и первых (левых) σ колонн.

Будем называть таким образом полученный определитель *минором порядка* σ и будем обозначать

$$A^{(1,2,\ldots,\sigma)}_{1,2,\ldots,\sigma}.$$

В последнем знаке нижние индексы показывают нумера выкинутых колонн, а верхние — нумера выкинутых горизонталей.

Вообще говоря, мы обозначим символом

$$A^{(k_1,k_2,\ldots,k_\sigma)}_{i_1,i_2,\ldots,i_\sigma}$$

минор порядка σ, получаемый из определителя A от вычеркивания колонн, имеющих нумера $i_1, i_2, \ldots, i_\sigma$, и горизонталей с нумерами $k_1, k_2, \ldots, k_\sigma$, и умноженный на $(-1)^{K+I}$, где $K = k_1 + k_2 + \ldots k_\sigma$, $I = i_1 + i_2 + \ldots i_\sigma$.

Покажем, что коэффициентом при

$$a_{i_1}{}^{(k_1)} a_{i_2}{}^{(k_2)} \cdots a_{i_\sigma}{}^{(k_\sigma)}$$

будет как раз выражение $A^{(k_1,k_2,\ldots,k_\sigma)}_{i_1,i_2,\ldots,i_\sigma}$.

Пусть $i_1 < i_2 < \dots i_\sigma$, $k_1 < k_2 < \dots < k_\sigma$. Перенесем k_1-ую горизонталь на верх, оставляя остальные горизонтали в их первоначальном порядке, т. е., если одна из остальных горизонталей была выше какой нибудь другой до перенесения, то она должна остаться лежащей выше и после перенесения. Такое перенесение будет совершаться при помощи ряда транспозиций горизонталей: мы переносим k_1-ую горизонталь сначала на $k_1 - 1$-ое место, затем на $k_1 - 2$-ое и так далее, наконец на первое (верхнее) место. От такого перенесения весь определитель умножается на $(-1)^{k_1-1}$. Будем теперь переносить на верх k_2-ую горизонталь, причем сделаем ее окончательно второю сверху. Определитель получит множитель $(-1)^{k_2-2}$, ибо придется произвести k_2-2 транспозиций горизонталей, так как k_1-ой горизонтали (перенесенной наверх) нет на прежнем месте.

Итак, перенесение горизонталей с нумерами $k_1,\ \ k_2, \dots,\ k_\sigma$ наверх без нарушения взаимного расположения других горизонталей, причем эти верхние горизонтали будут следовать одна под другою в порядке возрастания значков $k_1,\ \ k_2, \dots,\ k_\sigma$, будет сопровождаться умножением всего определителя на множитель

$$(-1)^{k_1-1+k_2-2+\dots+k_\sigma-\sigma} = (-1)^{K-\frac{\sigma(\sigma+1)}{2}}.$$

Совершенно подобным же образом сдвинем налево колонны с нумерами $i_1, i_2, \dots, i_\sigma$, не нарушая их взаимного расположения, а также, не нарушая взаимного расположения остальных колонн; тогда определитель умножится на $(-1)^{I-\frac{\sigma(\sigma+1)}{2}}$.

После одновременного сдвига горизонталей наверх и колонн налево определитель умножится на

$$(-1)^{K+I-\sigma(\sigma+1)} = (-1)^{K+I},$$

ибо одно из двух чисел σ и $\sigma+1$ четное, а элементы ${a_{i_1}}^{(k_1)}{a_{i_2}}^{(k_2)}\cdots{a_{i_\sigma}}^{(k_\sigma)}$ сделаются верхними в главной диагонали. Тогда, принимая во внимание формулу (1), получим выражение

$$(2) \qquad {a_{i_1}}^{(k_1)}{a_{i_2}}^{(k_2)}\cdots{a_{i_\sigma}}^{(k_\sigma)}\ A^{(k_1,k_2,\dots,k_\sigma)}_{i_1,i_2,\dots,i_\sigma}$$

для совокупности всех членов определителя A, имеющих множителя ${a_{i_1}}^{(k_1)}{a_{i_2}}^{(k_2)}\cdots {a_{i_\sigma}}^{(k_\sigma)}$.

Обозначим через $B^{(k_1,k_2,\dots,k_\sigma)}_{i_1,i_2,\dots,i_\sigma}$ минор, образованный из элементов, стоящих на пересечений горизонталей, имеющих нумера $k_1,\ \ k_2, \dots,\ k_\sigma$, и колонн, имеющих нумера $i_1,\ \ i_2, \dots,\ i_\sigma$.

Получаем формулу

$$B^{(k_1,k_2,\dots,k_\sigma)}_{i_1,i_2,\dots,i_\sigma} = \sum \pm {a_{i_1}}^{(k_1)}{a_{i_2}}^{(k_2)}\cdots{a_{i_\sigma}}^{(k_\sigma)},$$

причем сумма распространяется или на все перемещения верхних индексов, если нижние находятся в естественном порядке возрастания или наоборот на все перемещения нижних индексов без изменения верхних.

На оснований формулы (3) мы видим, что в состав определителя ? войдет полностью такое произведение

$$B^{(k_1,k_2,\dots,k_\sigma)}_{i_1,i_2,\dots,i_\sigma}\ A^{(k_1,k_2,\dots,k_\sigma)}_{i_1,i_2,\dots,i_\sigma}.$$

Величина $A^{(k_1,k_2,\dots,k_\sigma)}_{i_1,i_2,\dots,i_\sigma}$, равная некоторому минору, умноженному, на $(-1)^{I+K}$ носит название *алгебраического дополнения* минора $B^{(k_1,k_2,\dots,k_\sigma)}_{i_1,i_2,\dots,i_\sigma}$.

Миноры $B_{i_1,i_2,\ldots,i_\sigma}^{(k_1,k_2,\ldots,k_\sigma)}$ и $A_{i_1,i_2,\ldots,i_\sigma}^{(k_1,k_2,\ldots,k_\sigma)}$ носят название *дополнительных.*

§ 38

Докажем теперь формулу

$$A = \sum B_{i_1,i_2,\ldots,i_\sigma}^{(k_1,k_2,\ldots,k_\sigma)} A_{i_1,i_2,\ldots,i_\sigma}^{(k_1,k_2,\ldots,k_\sigma)}, \tag{1}$$

выражающую теорему Laplace'a. В этой формуле суммирование производится так: или числа $k_1,\ k_2,\ldots,\ k_\sigma$ оставляются *определенными* и сумма распространяется на *всевозможные сочетания* $i_1,\ i_2,\ldots,\ i_\sigma$ индексов $1,2,\ldots,n$ по σ индексов в каждом, или же числа $i_1,\ i_2,\ldots,\ i_\sigma$ остаются без перемены, а меняются индексы $k_1,\ k_2,\ldots,\ k_\sigma$.

Прежде всего мы замечаем, что в миноре $B_{i_1,i_2,\ldots,i_\sigma}^{(k_1,k_2,\ldots,k_\sigma)}$ заключается $1\cdot 2\cdots\sigma$ членов, а в миноре $A_{i_1,i_2,\ldots,i_\sigma}^{(k_1,k_2,\ldots,k_\sigma)}$ будет $1\cdot 2\cdots(n-\sigma)=(n-\sigma)!$ членов. Отсюда следует, что в каждом члене суммы (1), представляющем произведение двух миноров, будет всего $\sigma!(n-\sigma)!$ членов. Сумма (1) не имеет подобных членов, следовательно, во всей правой части (1) общее число членов будет $\sigma!(n-\sigma)!C_n^\sigma$, где C_n^σ есть число сочетаний из n элементов по σ.

Принимая же во внимание, что

$$\sigma!(n-\sigma)!C_n^\sigma = n!$$

получим все элементы определителя A, так что формула (1) оказывается справедливой.

В случае $\sigma = 1$ получаем выведенную нами раньше формулу разложения определителя A по элементам горизонтали или колонны

$$A = \sum B_i{}^{(k)} A_i{}^{(k)} = \sum a_i{}^{(k)} A_i{}^{(k)},$$

ибо $B_i{}^{(k)} = a_i{}^{(k)}$.

О взаимном определителе

§ 39

Составим для определителя

$$A = \begin{vmatrix} a_1{}^{(1)} & \ldots & a_n{}^{(1)} \\ \ldots\ldots\ldots\ldots\ldots \\ a_1{}^{(n)} & \ldots & a_n{}^{(n)} \end{vmatrix}$$

новый определитель

$$\mathfrak{A} = \begin{vmatrix} A_1{}^{(1)} & \ldots & A_n{}^{(1)} \\ \ldots\ldots\ldots\ldots\ldots \\ A_1{}^{(n)} & \ldots & A_n{}^{(n)} \end{vmatrix},$$

элементы которого $A_i{}^{(k)}$ суть алгебраические дополнения соответственных элементов $a_i{}^{(k)}$ первоначального определителя. Определитель $\mathfrak{A}$ называется взаимным относительно определителя A.

Умножим заданный определитель A на его взаимный $\mathfrak{A}$, тогда на оснований формул (1), (2), (3) и (4) § 14 получим

$$A\mathfrak{A} = \begin{vmatrix} A & 0 & \dots & 0 \\ 0 & A & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & A \end{vmatrix} = A^n,$$

откуда

$$\mathfrak{A} = A^{n-1}.$$

Взаимный определитель равен $(n-1)$-ой степени заданного определителя.

§ 40

Докажем теперь такое свойство взаимного определителя:

Во взаимном определителе $\mathfrak{A}$ всякий минор порядка $n-\sigma$ равен алгебраическому дополнению соответствующего ему минора в первоначальном определителе, умноженному на $A^{\sigma-1}$.

Рассмотрим минор

$$\mathfrak{A} = \begin{vmatrix} {A_1}^{(1)} & \dots & {A_\sigma}^{(1)} \\ \dots & \dots & \dots \\ {A_1}^{(\sigma)} & \dots & {A_\sigma}^{(\sigma)} \end{vmatrix}$$

составленный из σ верхних горизонталей и σ левых колонн взаимного определителя $\mathfrak{A}$.

Добавлением равных единице диагональных элементов, мы получим

$$A_\sigma = \begin{vmatrix} {A_1}^{(1)} & \dots & {A_\sigma}^{(1)} & {A_{\sigma+1}}^{(1)} & \dots & {A_n}^{(1)} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ {A_1}^{(\sigma)} & \dots & {A_\sigma}^{(\sigma)} & {A_{\sigma+1}}^{(\sigma)} & \dots & {A_n}^{(\sigma)} \\ 0 & \dots & 0 & 1 & \dots & 0 \\ 0 & \dots & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & 0 & \dots & 1 \end{vmatrix}.$$

Умножая определитель A на $\mathfrak{A}_\sigma$, получим

$$A\mathfrak{A}_\sigma = \begin{vmatrix} A & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & A & \dots & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & A & 0 & \dots & 0 \\ {a_{\sigma+1}}^{(1)} & \dots & {a_{\sigma+1}}^{(\sigma)} & {a_{\sigma+1}}^{(\sigma+1)} & \dots & {a_{\sigma+1}}^{(n)} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ {a_n}^{(1)} & \dots & {a_n}^{(\sigma)} & {a_n}^{(\sigma+1)} & \dots & {a_n}^{(n)} \end{vmatrix};$$

откуда окончательно

$$\mathfrak{A}_\sigma = A^{\sigma-1} \begin{vmatrix} {a_{\sigma+1}}^{(\sigma+1)} & {a_{\sigma+1}}^{(\sigma+2)} & \dots & {a_{\sigma+1}}^{(n)} \\ \dots & \dots & \dots & \dots \\ {a_n}^{(\sigma+1)} & {a_n}^{(\sigma+2)} & \dots & {a_n}^{(n)} \end{vmatrix}$$

и теорема доказана для случая *главного* минора A_σ (составленного из верхних и левых рядов).

Чтобы доказать теорему в общем случае, достаточно передвинуть горизонтали и колонны вверх и влево, как это было сделано в § 37.

§ 41

Как частный случай теоремы предыдущего §-а, может быть написана формула

$$A_{i_1}{}^{(k_1)}A_{i_2}{}^{(k_2)} - A_{i_1}{}^{(k_2)}A_{i_2}{}^{(k_1)} = AA_{i_1i_2}{}^{(k_1k_2)}.$$

Если $A = 0$, то имеется пропорция $\dfrac{A_{i_1}{}^{(k_1)}}{A_{i_1}{}^{(k_2)}} = \dfrac{A_{i_2}{}^{(k_1)}}{A_{i_2}{}^{(k_2)}}$, то есть элементы одной горизонтали (колонны) пропорциональны соответственным элементам другой.

Симметрические определители

§ 42

Назовем *сопряженным* с элементом $a_i{}^{(k)}$ элемент $a_k{}^{(i)}$, индексы которого переставлены. Подобным образом минор

$$B_{i_1i_2\ldots i_\sigma}{}^{(k_1k_2\ldots k_\sigma)}$$

мы будем называть *сопряженным* с минором

$$B_{k_1k_2\ldots k_\sigma}{}^{(i_1i_2\ldots i_\sigma)}.$$

Определитель, в котором каждый элемент равеу своему сопряженному $a_i{}^{(k)} = a_k{}^{(i)}$, называется *симметрическим*. Определитель называется *косым симметрическим*, если каждые два сопряженных элемента равны между собой по абсолютной величине, но противоположны по знаку, $a_i{}^{(k)} = -a_k{}^{(i)}$; а, следовательно, в частности все элементы главной диагонали равны нулю: $a_i{}^{(i)} = 0$.

Сопряженные миноры симметрического определителя равны между собой; отсюда следует, что взаимный определитель симметрического есть также симметрический.

§ 43

Покажем теперь, что *косые симметрические определители нечетного порядка тождественно равны нулю.*

Если мы в одном из таких косых определителей A заменим горизонтали вертикалями и обратно, то такая замена будет равносильна умножений на -1 всех элементов определителя; другими словами, с одной стороны определитель не изменится, с другой стороны он умножится на $(-1)^n$, и мы получим $A = (-1)^n$, но n есть число нечетное, значить $A = 0$.

Покажем, что *косой симметрический определитель четного порядка будет полным квадратом.*

Например,

$$\begin{vmatrix} 0 & -a & -b & -d \\ a & 0 & -c & -e \\ b & c & 0 & -f \\ d & e & f & 0 \end{vmatrix} = (af - be + dc)^2.$$

Для $n = 2$ справедливость теоремы очевидна

$$\begin{vmatrix} 0 & -a \\ a & 0 \end{vmatrix} = a^2.$$

Докажем справедливость теоремы для n, если предположить ее справедливость для $n - 2$.

Имеем, очевидно,

$$A = a_r{}^{(r)} A_r{}^{(r)} - \sum \mathfrak{a}_{ij} a_r{}^{(i)} a_j{}^{(r)},$$

где $\mathfrak{a}_{ij}$ есть алгебраическое дополнение элемента $a_j{}^{(i)}$ в определителе $A_r{}^{(r)}$. На основании свойства элементов косого определителя имеем

$$A = \sum \mathfrak{a}_{ij} a_i{}^{(r)} a_j{}^{(r)}. \tag{1}$$

Но минор $A_r{}^{(r)}$ есть также косой симметрический нечетного порядка $n-1$. На оснований формулы § 41 получаем

$$\mathfrak{a}_{ii}\mathfrak{a}_{jj} - \mathfrak{a}_{ij}\mathfrak{a}_{ji} = 0. \tag{2}$$

Но, очевидно, что алгебраическая дополнения сопряженных элементов косого симметрического определителя нечетного порядка равны между собой, т. е. $\mathfrak{a}_{ij} = \mathfrak{a}_{ji}$. Формула (2) дает

$$\mathfrak{a}_{ij}{}^2 = \mathfrak{a}_{ii}\mathfrak{a}_{jj} \quad \text{или} \quad \mathfrak{a}_{ij} = \sqrt{\mathfrak{a}_{ii}}\ \sqrt{\mathfrak{a}_{jj}}.$$

Значить, по формуле (1) получаем

$$A = \sum_{ij} (a_i{}^{(r)} \sqrt{\mathfrak{a}_{ii}}\, a_j{}^{(r)} \sqrt{\mathfrak{a}_{jj}}) = \left(\sum_i a_i{}^{(r)} \sqrt{\mathfrak{a}_{ii}} \right)^2. \tag{3}$$

Миноры $\mathfrak{a}_{ii}$ суть косые определители порядка $n-2$, следовательно, согласно предположение справедливости теоремы для $n-2$ величины $\mathfrak{a}_{ii}$ суть полные квадраты, а, следовательно, радикалы $\sqrt{\mathfrak{a}_{ii}}$ являются выражениями рациональными; таким образом мы видим, что по формуле (3) оказывается полным квадратом также и определитель A порядка n, и теорема доказана.

Приемы вычисления определителей

§ 45

Покажем на ряде примеров способы вычисления определителей.

I. Определитель Vandermonde'a

$$\begin{vmatrix} {\alpha_1}^{n-1} & {\alpha_1}^{n-2} & \dots & \alpha_1 & 1 \\ {\alpha_2}^{n-1} & {\alpha_2}^{n-2} & \dots & \alpha_2 & 1 \\ \dots\dots\dots\dots\dots\dots\dots\dots & & & & \\ {\alpha_n}^{n-1} & {\alpha_n}^{n-2} & \dots & \alpha_n & 1 \end{vmatrix} = D$$

Располагая определитель D по элементам первой строки, получим

$$D = \mathfrak{A}_0{\alpha_1}^{n-1} + \mathfrak{A}_1{\alpha_1}^{n-2} + \dots + \mathfrak{A}_{n-2}\alpha_1 + \mathfrak{A}_{n-1}, \tag{1}$$

где

$$\mathfrak{A}_0,\ \ \mathfrak{A}_1,\ \dots,\ \mathfrak{A}_{n-2},\ \ \mathfrak{A}_{n-1}$$

суть функции от $\alpha_2,\quad \alpha_3,\ \dots,\ \alpha_n$, причем

$$\mathfrak{A}_0 = \begin{vmatrix} {\alpha_2}^{n-2} & {\alpha_2}^{n-3} & \dots & \alpha_2 & 1 \\ {\alpha_3}^{n-2} & {\alpha_3}^{n-3} & \dots & \alpha_3 & 1 \\ \dots\dots\dots\dots\dots\dots\dots\dots & & & & \\ {\alpha_n}^{n-1} & {\alpha_n}^{n-2} & \dots & \alpha_n & 1 \end{vmatrix}.$$

Предполагая в D величину α_1 как переменную независимую, а величины $\alpha_2,\ \alpha_3,\ \dots,\ \alpha_n$, как заданные числа, заметим, что функция (1) будет иметь $n-1$ корней $\alpha_2,\quad \alpha_3,\ \dots,\ \alpha_n$, ибо, подставляя эти числа вместо α_1, получаем две одинаковые строки, следовательно, $D = 0$. Итак

$$D = \mathfrak{A}_0(\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)\cdots(\alpha_1 - \alpha_n).$$

Подобным же образом, располагая определитель $\mathfrak{A}_0$ по элементам первой строки, находим, что

$$\mathfrak{A}_0 = \mathfrak{B}_0(\alpha_2 - \alpha_3)(\alpha_2 - \alpha_4)\cdots(\alpha_2 - \alpha_n)$$

и т. д. Отсюда получаем окончательно следующее выражение для определителя D

$$\begin{aligned} D = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)\cdots(\alpha_1 - \alpha_n) \\ (\alpha_2 - \alpha_3)(\alpha_2 - \alpha_4)\cdots(\alpha_2 - \alpha_n) \\ \dots\dots\dots\dots\dots\dots \\ (\alpha_{n-1} - \alpha_n) \end{aligned}.$$

II. Называются *циркулянтами* определители, различные горизонтали которых получаются при помощи круговой подстановки, произведенной над элементами первой горизонтали.

Чтобы вычислить значение циркулянта

$$D = \begin{vmatrix} a_1 & a_2 & a_3 & \dots & a_n \\ a_n & a_1 & a_2 & \dots & a_{n-1} \\ \dots\dots\dots\dots\dots\dots & & & & \\ a_2 & a_3 & a_4 & \dots & a_1 \end{vmatrix},$$

умножим его на определитель

$$\Delta = \begin{vmatrix} 1 & \alpha_1 & {\alpha_1}^2 & \dots & {\alpha_1}^{n-1} \\ 1 & \alpha_2 & {\alpha_2}^2 & \dots & {\alpha_2}^{n-1} \\ & & & & \\ 1 & \alpha_n & {\alpha_n}^2 & \dots & {\alpha_n}^{n-1} \end{vmatrix},$$

где $\alpha_1,\ \alpha_2,\ \dots,\ \alpha_n$ суть все корни двучленного уравнения $x^n - 1 = 0$.

Полагая для сокращения

$$f(x) = a_1 + a_2 x + a_3 x^2 + \dots + a_n x^{n-1},$$

получим

$$D\Delta = \begin{vmatrix} f(\alpha_1) & \alpha_1 f(\alpha_1) & {\alpha_1}^2 f(\alpha_1) & \dots & {\alpha_1}^{n-1} f(\alpha_1) \\ f(\alpha_2) & \alpha_2 f(\alpha_2) & {\alpha_2}^2 f(\alpha_2) & \dots & {\alpha_2}^{n-1} f(\alpha_2) \\ \dots & \dots & \dots & \dots & \dots \end{vmatrix}$$

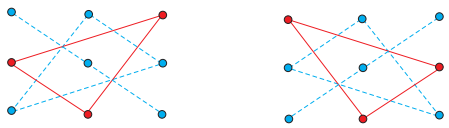
по выделении множителей $f(\alpha_1), f(\alpha_2), \dots, f(\alpha_n)$ остается определитель Δ, и мы получаем

$$D = f(\alpha_1)\ f(\alpha_2)\ \cdots\ f(\alpha_n).$$

Например, случай $n = 4$ дает $f(x) = a + bx_c x^2 + dx^3$; корни уравнения $x^4 - 1 = 0$ суть $1,\ -1,\ i,\ -i,\ (i = \sqrt{-1}),\ f(1) = a + b + c + d,\ f(-1) = a - b + c - d,\ f(i) = a - c + (b - d)i,\ f(-i) = a - c - (b - d)i$, следовательно,

$$\begin{vmatrix} a & b & c & d \\ d & a & b & c \\ c & d & a & b \\ b & c & d & a \end{vmatrix} = (a + b + c + d)(a - b + c - d)[(a - c)^2 + (b - d)^2].$$

III. При вычислений определителей третьего порядка полезно иметь в виду правило Sarrus'a



Черт. 6

Надо перемножить между собою элементы, стоящие на вершинах двух треугольников левой фигуры, а также надо перемножить элементы главной диагонали; таким образом получатся три члена определителя, перед которыми придется поставить знак +; аналогичным образом получим члены с − из правой фигуры

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

IV. При вычислений определителей с заданными элементами самым практическим способом является сделать элементы одной из горизонталей (колонн) за исключением одного равными нулю, тогда порядок определителя понижается.

Например, требуется вычислить определитель

$$\begin{vmatrix} 4 & 5 & 1 & 3 \\ 2 & 4 & -3 & 7 \\ 5 & 6 & 0 & 1 \\ 3 & 4 & 1 & 7 \end{vmatrix}.$$

Прибавляем в элементам второй горизонтали утроенные элементы первой, а из элементов четвертой горизонтали вычитаем элементы первой, тогда мы получаем

$$\begin{vmatrix} 4 & 5 & 1 & 3 \\ 14 & 19 & 0 & 16 \\ 5 & 6 & 0 & 1 \\ -1 & -1 & 0 & 4 \end{vmatrix}.$$

Раскладывая этот определитель по элементам третьей колонны, получим

$$1 \cdot (-1)^{1+3} \begin{vmatrix} 14 & 19 & 16 \\ 5 & 6 & 1 \\ -1 & -1 & 4 \end{vmatrix} + 0,$$

то есть порядок определителя, подлежащего вычислению, понижен на единицу.

V. К наиболее трудным вопросам, относящимся к определителям, принадлежит вопрос об условиях, когда определители сохраняют свой знак. Я приведу здесь один прпмер[3] такого рода исследования.

Пусть $m_0 = 1$, $m_i = \dfrac{1^2 3^2 \cdots (2i-1)^2}{2^2 4^2 \cdots (2i)^2}$.

Требуется доказать, что будут положительными определители

$$V_i^{(k)} = \begin{vmatrix} 1 & 0 & 0 & 0 & \dots & 0 & m_{k-i} \\ m_1 & 1 & 0 & 0 & \dots & 0 & m_{k-i+1} \\ m_2 & m_1 & 1 & 0 & \dots & 0 & m_{k-i+2} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ m_i & m_{i-1} & m_{i-2} & m_{i-3} & \dots & m_1 & m_k \end{vmatrix}, \qquad V_i^{(k)} = m_k$$

при $i < k$.

Раскладывая по первой горизонтали, получим

$$V_i^{(k)} = {V_{i-1}}^{(k)} + (-1)^i m_{k-i} \mu_i, \tag{2}$$

где

$$\mu_i = \begin{vmatrix} m_1 & 1 & 0 & \dots & 0 \\ m_2 & m_1 & 1 & \dots & 0 \\ & & & & \\ m_{i-1} & m_{i-2} & \dots & \dots & 1 \\ m_i & m_{i-1} & \dots & \dots & m_1 \end{vmatrix}, \qquad \mu_1 = m_1.$$

Подставляя в формулы (2) вместо i значения $1, 2, \dots, l$, где $l < k$, получим

$$\begin{aligned} V_l^{(k)} &= {V_{l-1}}^{(k)} + (-1)^l m_{k-l} \mu_l, \\ &\dots\dots\dots\dots\dots\dots \\ V_2^{(k)} &= V_1^{(k)} + m_{k-2} \mu_2, \\ V_1^{(k)} &= V_0^{(k)} - m_{k-1} \mu_1. \end{aligned} \tag{3}$$

[3] D. Grawe. Zur Theorie der elliptischen Funcktionen. Унив. Изв. Киев, 1909.

Раскрывая μ_i, мы получим

$$\mu_i = \mu_{i-1}m_1 - \mu_{i-2}m_2 + \ldots + (-1)^{l-1}\mu_2 m_{l-2} + (-1)^l \mu_1 m_{l-1} + (-1)^{l+1} m_l$$

или

$$-m_l = -\mu_1 m_{l-1} + \mu_2 m_{l-2} - \ldots (-1)^{l-1}\mu_{l-1}m_1 + (-1)^l \mu_l.$$

Умножая равенства (3) на

$$\frac{1}{m_{k-l}},\ \ \frac{m_1}{m_{k-l+1}},\ \ \frac{m_3}{m_{k-l+2}},\ \ldots,\ \frac{m_{l-1}}{m_{k-1}}$$

и складывая, получим

$$\frac{1}{m_{k-l}} V_l^{(k)} = \sum_{i=0}^{i=l-1} V_i^{(k)} \left[\frac{m_{l-i-1}}{m_{k-i-1}} - \frac{m_{l-1}}{m_{k-1}} \right].$$

Разности в скобках правой части положительны, ибо величина

$$\frac{m_{l-i}}{m_{k-i}}$$

возрастает с возрастанием i. Отсюда будет положителен определитель $V_i^{(k)}$ при $i = l$, если он положителен при $i < l$; но положительность $V_1{}^{(k)}$, $V_2{}^{(k)}$ проверяется непосредственно; следовательно, теорема доказана

Исчисление матриц

§ 46

Совокупность n^2 чисел, расположенных в следующей квадратной схеме:

$$\left\| \begin{matrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{matrix} \right\| = \|a_{ik}\|$$

образуют так называемую *квадратную матрицу* порядка n. Cayley[4] первый обратил внимание на то обстоятельство, что матрицу можно рассматривать как одно *комплексное* число. Можно установить правила сложения и умножения матриц, откуда появится новая алгебра действий над матрицами.

Будем рассматривать всю совокупность W комплексных чисел обыкновенной алгебры, кроме этих чисел будем рассматривать *всевозможные* матрицы порядка ?, элементами которых являются числа W. Эти матрицы вместе с числами W образуют новую совокупность предметов M, в составь которой входит совокупность W как часть. Для сокращения речи будем называть числа W *величинами скалярными*, а матрицы *величинами комплексными*.

Будем обозначать матрицы большими готическими буквами

$$\mathfrak{A},\ \ \mathfrak{B},\ \ \mathfrak{C},\ \ldots$$

[4]Cayley. Coll. math. papers 2, 475.

Определение равенства двух матриц. Две матрицы

$$\mathfrak{A} = \|a_{ik}\| \quad и \quad \mathfrak{B} = \|b_{ik}\|$$

называются равными, если каждый из n^2 *элементов матрицы* $\mathfrak{A}$ *равен соответственному элементу матрицы* $\mathfrak{B}$*, то есть* $\mathfrak{A} = \mathfrak{B}$*, если*

$$a_{ik} = b_{ik} \qquad (i, k = 1, 2, \ldots, n).$$

Определение нуля. Матрица $\mathfrak{A}$ *называется нулем тогда и только тогда, когда все ее элементы равны нулю, т. е.* $\mathfrak{A} = 0$*, если*

$$a_{ik} = 0 \qquad (i, k = 1, 2, \ldots, n).$$

Определение сложения матриц. По соответственным элементам a_{ik} и b_{ik} двух произвольно взятых матриц $\mathfrak{A}$ и $\mathfrak{B}$ составляем элемент

$$s_{ik} = a_{ik} + b_{ik}$$

новой матрицы $\mathfrak{S}$. Эту матрицу $\mathfrak{S}$ называют суммой $\mathfrak{A}$ и $\mathfrak{B}$ и пишут

$$\mathfrak{S} = \mathfrak{A} + \mathfrak{B}.$$

Таким образом мы приходим к следующему определению сложения матриц:

Под суммой двух матриц разумеется такая новая, элементы которой суть суммы соответственных элементов слагаемых матриц.

Правило вычитания матриц получается как следствие из определения сложения.

Разностью двух матриц будет такая новая, элементы которой суть разности соответственных элементов обеих заданных.

Итак, мы видим, что матрицы представляют относительно сложения абелеву группу, ибо из определения сложения вытекает существование как перестановочного

$$\mathfrak{A} + \mathfrak{B} = \mathfrak{B} + \mathfrak{A},$$

так и сочетательного

$$(\mathfrak{A} + \mathfrak{B}) + \mathfrak{C} = \mathfrak{A} + (\mathfrak{B} + \mathfrak{C})$$

законов.

Единицей группы является матрица, равная нулю.

Обратным элементом группы для каждой матрицы является матрица, элементы которой получаются от умножения на -1 элементов матрицы .

Приступая к умножений матриц, рассмотрим сначала умножение матрицы на скалярную величину и поставим такое определение:

Определение. Под произведением k*,* $\mathfrak{A}$ *или* $\mathfrak{A}$*,* k *матрицы* $\mathfrak{A}$ *на скалярную величину* k *разумеется матрица, каждый элемент которой происходит от умножения на* k *соответствующего элемента матрицы* $\mathfrak{A}$*.*

Умножение на скалярную величину удовлетворяет законам перестановочному и распределительному

$$k\mathfrak{A} = \mathfrak{A}k$$
$$k\mathfrak{A} + k\mathfrak{B} = k(\mathfrak{A} + \mathfrak{B})$$
$$k\mathfrak{A} + l\mathfrak{A} = (k + l)\mathfrak{A},$$

где k и l скалярные величины.

Мы будем употреблять обозначение

$$-\mathfrak{A} = (-1)\mathfrak{A}.$$

§ 48

Переходим теперь к определению умножения двух матриц, причем возьмем правило умножения из теории определителей.

Определение умножения. Под произведением $\mathfrak{AB}$ *двух матриц* $\mathfrak{A}$ *и* $\mathfrak{B}$ *разумеется такая новая матрица, у которой элемент* (i, j)*, стоящий на пересечении* i*-ой горизонтали с* j*-ой колонной, получается через умножение каждого элемента* i*-ой горизонтали* $\mathfrak{A}$ *на соответственный элемент* j*-ой колонны* $\mathfrak{B}$ *и сложения полученных отдельных произведений.*

Так, например, элемент (i, j) в произведении $\mathfrak{A}$, $\mathfrak{B}$ будет

$$a_{i1}b_{1j} + a_{i2}b_{2j} + \ldots + a_{in}b_{nj}. \tag{1}$$

Подобным же образом тот же элемент (i, j) произведения $\mathfrak{BA}$ будет

$$b_{i1}a_{1j} + b_{i2}a_{2j} + \ldots + b_{in}a_{nj}. \tag{2}$$

Так как в общем случай числа (1) и (2) неодинаковы, то мы получаем теорему:

Умножение матриц есть действие, вообще говоря, неперестановочное, т. е.

$$\mathfrak{AB} \neq \mathfrak{BA}.$$

Хотя умножение матриц обладает законами сочетаниельным и распределительным

$$(\mathfrak{AB})\mathfrak{C} = \mathfrak{A}(\mathfrak{BC})$$
$$\mathfrak{A}(\mathfrak{B} + \mathfrak{C}) = \mathfrak{AB} + \mathfrak{AC},$$

но совокупность M скалярных величин и матриц не будет *полем*. Отличным от свойств поля является неперестановочность умножения. Еще более важное отличие от поля представляет то обстоятельство, что произведение нескольких матриц может равняться нулю, тогда как ни один из множителей не равен нулю. В этом мы можем убедиться на следующем простом примере.

$$\begin{Vmatrix} a_{11} & a_{12} & 0 \\ a_{21} & a_{22} & 0 \\ a_{31} & a_{32} & 0 \end{Vmatrix} \cdot \begin{Vmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ b_{31} & b_{32} & b_{33} \end{Vmatrix} = \begin{Vmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{Vmatrix} = 0.$$

Получаем теорему:

Произведение двух матриц может равняться нулю, когда оба множителя отличны от нуля.

Мы будем матрицу $= \|a_{ik}\|$ называаать *особенною*, если *равен нулю* определитель $|a_{ik}|$, составленный из ее элементов.

Для *неособенных* матриц получаем теорему:

Определитель произведения двух матриц равен произведению определителей множителей.

Матрицу $\mathfrak{A}$ мы будем называть *делителем нуля*, если можно подобрать такую отличную от нуля матрицу $\mathfrak{B}$, что будет или $\mathfrak{AB} = 0$ или $\mathfrak{BA} = 0$.

Нетрудно доказать теорему:

Делителем нуля может быть только особенная матрица.

§ 49

В теории определителей горизонтали и колонны могли быть заменяемы одни другими. При матрицах происходить другое. Две матрицы

$$\mathfrak{A} = \left\|\begin{matrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{matrix}\right\|, \qquad \mathfrak{A}' = \left\|\begin{matrix} a_{11} & a_{21} & \dots & a_{n1} \\ a_{12} & a_{22} & \dots & a_{n2} \\ \dots & \dots & \dots & \dots \\ a_{1n} & a_{2n} & \dots & a_{nn} \end{matrix}\right\|$$

обладающие свойством, что горизонтали одной совпадают с колоннами другой называются *сопряженными*. Сопряженные матрицы имеют одинаковые определители, но сами, вообще говоря, *неравны* между собой.

Если $\mathfrak{A} = \mathfrak{A}'$, то есть, если матрица $\mathfrak{a}$ равна своей сопряженной $\mathfrak{A}'$, то она должна быть *симметричною*, т. е.

$$a_{ik} = a_{ki}.$$

Заменяя колонны горизонталями и обратно, мы получим равенство

$$(\mathfrak{AB})' = \mathfrak{B}'\mathfrak{A}',$$

выражающее теорему.

Сопряженная величина произведения матриц равна произведению сопряженных величин множителей, причем их надо перемножать в обратном порядке.

Элементарные делители

§ 50

Мы дадим теперь понятие о теории, основанной Sylvestr'ом, H. Smith'ом и особенно Weierstrass'ом. Эта теория имеет значение в Алгебре и была предметом изучения ряда выдающихся математиков: Kronecker'a, Frobenius'a и других.

Мы будем рассматривать λ-матрицы, у которых все элементы суть целые функции от переменной независимой λ.

Введем понятие о так называемых *элементарных преобразованиях* матрицы.

Определение. Под элементарным преобразованием λ-матрицы мы будем разуметь одну из следующих операций:

a) Перестановку двух горизонталей или колонн.

b) Умножение всех элементов горизонтали или колонны на один и тот же отличный от нуля постоянный множитель.

c) Прибавка, умноженных на один и тот же полином от λ, элементов горизонтали или колонны к соответственным элементам другой горизонтали или колонны.

§ 51

Две λ-матрицы мы будем называть *эквивалентными*, если от одной из них можно перейти к другой при помощи конечного числа элементарных преобразований.

Нетрудно видеть, что две эквивалентные матрицы имеют один и тот же ранг. В самом деле, преобразования a) и b) не изменяют ранга матрицы, ибо ими не нарушается обращение или необращение в нуль определителя, взятого из матрицы. Остается рассмотреть только влияние на ранг операции c).

Пусть операция c) состоит в прибавлении к p-ой горизонтали матрицы q-ой горизонтали, умноженной на $\psi(\lambda)$. Очевидно, что *определители* матрицы, в которых или нет p-ой горизонтали, или находятся обе горизонтали p-ая и q-ая, *не меняются* от указанной операции.

Определители же порядка r, где находится p-ая горизонталь, но не находится q-ая, обращаются в

$$C = A + \psi(\lambda)B,$$

где A и B определители порядка r первоначальной матрицы. Если $A = 0$ и $B = 0$, то и $C = 0$. Может, конечно, случиться, что при $A \neq 0$, $B \neq 0$ будет $C = 0$. Итак, ранг матрицы от преобразования c) не может *увеличиться*. Очевидно, что преобразование c) не может также уменьшить ранг, ибо тогда обратное преобразование его увеличило бы.

§ 52

Каждый из определителей, взятых из λ-матрицы есть некоторая целая функция от λ. Обозначить через $D_i(\lambda)$ общий наибольший делитель всех определителей порядка i данной λ-матрицы. Покажем, что $D_i(\lambda)$ есть выражение, не меняющееся от элементарных преобразований. Для этой цели докажем такую лемму.

Если все определители порядка i матрицы имеют общий множитель $\varphi(\lambda)$, то такой же множитель имеют все определители порядка i у всякой матрицы эквивалентной с данною.

В самом деле, операции a) и b), очевидно, могут вводить в определители матрицы лишь постоянные множители. Пусть операция c) состоит в прибавлении к элементам p-ой горизонтали умноженных на $\psi(\lambda)$ соответственных элементов q-ой. Определители матрицы или не изменяются, или же принимаюсь вид

$$A + \psi(\lambda)B,$$

где A и B определители прежней матрицы. Во всех случаях остается тот же делитель $\varphi(\lambda)$.

Так как для всех двух эквивалентных λ-матриц общий делитель определителей i-ого порядка одной из них есть общий делитель также для другой, то мы приходим, очевидно, к заключению, что общий наибольший делитель $D_i(\lambda)$ есть выражение, не меняющееся от элементарных преобразований, и, следовательно, общее для всех эквивалентных между собой матриц.

§ 53

Итак, мы видим, что эквивалентные между собой матрицы ранга r имеют общими выражения

$$D_1(\lambda), \quad D_2(\lambda), \ \ldots, \ D_r(\lambda).$$

Покажем, что и обратно, если две матрицы ранга r имеют общими выражения (1), то они эквивалентны.

Для этой цели докажем лемму.

Если первый[5] *элемента $f(\lambda)$ матрицы не уничтожается тождественно и не делит алгебраически всех остальных элементов матрицы, то можно составить эквивалентную матрицу, у которой первый элемент не равен нулю и имеет степень, меньшую чем $f(\lambda)$.*

Допустим сначала, что уже в первой горизонтали находится элемент $f_1(\lambda)$, не делящийся на $f(\lambda)$; пусть этот элемент стоит на пересечении первой горизонтали с i-ой колонной. Делим $f_1(\lambda)$ на $f(\lambda)$ и обозначим неравный нулю остаток этого деления через $r(\lambda)$

$$f_1(\lambda) = f(\lambda)q(\lambda) + r(\lambda).$$

Этот остаток степени *ниже*, чем $f(\lambda)$. Вычтем из i-ой колонны первую умноженную на $q(\lambda)$, тогда наверху i-ой колонны будет стоять $r(\lambda)$. Перемещением первой и i-ой колонн сделаем $r(\lambda)$ первым элементом матрицы, и теорема доказана для рассматриваемого случая.

Подобным же образом рассматривается случай, когда неделящийся на $f(\lambda)$ элемент находится в первой колоний.

Пусть теперь каждый элемент как первой горизонтали так и первой колонны делится на $f(\lambda)$. Элемент же матрицы, не деляшийся на $f(\lambda)$ пусть находится на пересечений i-ой колонны с k-ой горизонталью.

Пусть наверху i-ой колонны стоит элемент $f(\lambda)\omega(\lambda)$, тогда, вычитая из i-ой колонны первую, умноженную на $\omega(\lambda)$, получим *нуль* на верху i-ой колонны, причем в этой последней колонне, на k-ой горизонтали но прежнему будет стоять член, не делящийся на $f(\lambda)$. Прибавим теперь новую i-ую колонну к первой, тогда в этой последней первый элемент не изменится, а на пересечений с k-ой горизонталью окажется член, не делящийя на $f(\lambda)$, и мы приходим к случаю, уже разобранному.

§ 54

Докажем еще такую лемму:

Матрица с неравными нулю элементами может всегда быть превращена в ей эквивалентную, обладающую такими свойствами:

[5] Верхний левый.

a) *первый элемент $f(\lambda)$ не уничтожается тождественно;*

b) *все остальные элементы первой горизонтали и первой колонны тождественно равны нулю;*

c) *все остальные, отличные от нуля, элементы делятся на $f(\lambda)$).*

Перемещением горизонталей и колонн мы можем сделать первым любой из не равных тождественно нулю элементов матрицы. По лемме § 53 можно уменьшить степень первого элемента, если на него не делятся все остальные элементы матрицы. Так как уменьшение степени можно совершать конечное число раз, то мы придем окончательно к такой матрице, у которой все элементы делятся на первый $f(\lambda)$. В частном случай степень функции $f(\lambda)$ может равняться нулю, так что эта функция сводится к постоянному числу. Применением операции c) § 50 мы достигнем того, что требуется в лемме, то есть равенства нулю всех элементов первой горизонтали и первой колонны, кроме первого.

§ 55

Итак λ-матрица n-то порядка и ранга $r > 0$

$$\left\|\begin{matrix} a_{11} & \dots & a_{1n} \\ \dots\dots\dots\dots \\ a_{n1} & \dots & a_{nn} \end{matrix}\right\| \tag{1}$$

элементарными операциями приводится к виду

$$\left\|\begin{matrix} f_1(\lambda) & 0 & \dots & 0 \\ 0 & b_{11} & \dots & b_{1\,n-1} \\ \dots\dots\dots\dots\dots\dots\dots\dots \\ 0 & b_{n-1\,1} & \dots & b_{n-1\,n-1} \end{matrix}\right\|,$$

где матрица

$$\left\|\begin{matrix} b_{11} & \dots & b_{1\,n-1} \\ \dots\dots\dots\dots\dots \\ b_{n-1\,1} & \dots & b_{n-1\,n-1} \end{matrix}\right\| \tag{2}$$

имеет, очевидно, ранг $r-1$ и все ее элементы делятся на функцию $f_1(\lambda)$. Если $r > 1$, то матрица (2) может быть приведена к виду

$$\left\|\begin{matrix} f_2(\lambda) & 0 & \dots & 0 \\ 0 & c_{11} & \dots & c_{1\,n-2} \\ \dots\dots\dots\dots\dots\dots\dots\dots \\ 0 & c_{n-2\,1} & \dots & b_{n-2\,n-2} \end{matrix}\right\|.$$

Продолжая рассуждение далее, мы приведем матрицу (1) окончательно к виду

$$\left\|\begin{matrix} f_1(\lambda) & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & f_2(\lambda) & \dots & 0 & 0 & \dots & 0 \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ 0 & 0 & \dots & f_r(\lambda) & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ 0 & 0 & \dots & 0 & 0 & \dots & 0 \end{matrix}\right\|. \tag{3}$$

Очевидно, что в функциях $f_1(\lambda), f_2(\lambda), \ldots, f_r(\lambda)$ можно предполагать старшие коэффициенты равными единице, ибо среди элементарных преобразований существуют операции b) § 50, состоящие в умножении элементов строки или горизонтали на постоянные числа.

И мы приходим к теореме:

Всякую λ-матрицу n-ого порядка и r-ого ранга можно при помощи элементарных операций привести к виду (3) *причем всякий полином $f_i(\lambda)$ будет иметь равный единице коэффициент при старшей степени и кроме того функция $f_i(\lambda)$ будет делителем $f_{i+1}(\lambda)$ при $i = 1, 2, 3, \ldots, r-1$.*

Вид (3) будем называть *нормальным* видом матрицы.

§ 56

Неизменяющиеся, как было в § 52 доказано, при элементарных преобразованиях величины $D_i(\lambda)$ определяются, очевидно, по формуле

$$D_i(\lambda) = f_1(\lambda) f_2(\lambda) \cdots f_i(\lambda).$$

Теперь мы имеем все данные для доказательства поставленной выше теоремы:

Необходимым и достаточным условием эквивалентности двух λ-матриц является: 1) *одинаковый ранг r и* 2) *общие величины $D_1(\lambda), D_2(\lambda), \ldots, D_r(\lambda)$.*

Необходимость теоремы следует из соображений § 52. В достаточности же теоремы можно убедиться таким образом.

Предполагая у обеих заданных матриц одинаковый ранг r и одинаковые делители миноров

$$D_1(\lambda), \quad D_2(\lambda), \ \ldots, \ D_r(\lambda) \tag{1}$$

приведем обе матрицы к нормальному виду.

Тогда, на основании существования одинаковых выражений (1), будем иметь

$$\begin{aligned} &f_1'(\lambda) = f_1(\lambda), \\ &f_1'(\lambda) f_2'(\lambda) = f_1(\lambda) f_2(\lambda) \\ &\ldots\ldots\ldots\ldots\ldots\ldots \end{aligned}$$

Откуда получаем $f_i'(\lambda) = f_i(\lambda)$, т. е. обе заданные матрицы имеют общую нормальную форму. Каждая из заданных матриц эквивалентна с общей нормальною, следовательно, они эквивалентны между собой, что и требовалось доказать.

§ 57

На основании соображений § 56 функций $f_1(\lambda), f_2(\lambda), \ldots, f_r(\lambda)$ называются *инвариантными множителями* класса эквивалентных между собой матриц.

Пусть $D_r(\lambda)$ есть по прежнему общий наибольший делитель всех определителей порядка r заданной λ-матрицы ранга r. Линейные множители

$$\lambda - a, \quad \lambda - a', \quad \lambda - a'', \ \ldots,$$

где a, a', a'', суть корни $D_r(\lambda) = 0$ называются *линейными множителями* матрицы.

Пусть

$$f_i(\lambda) = (\lambda - a)^{e_i}(\lambda - a')^{e'_i}(\lambda - a'')^{e''_i} \cdots$$

инвариантные множители матрицы $\mathfrak{A}$ ранга r, для которой все различные между собой линейные множители суть

$$\lambda - a, \quad \lambda - a', \quad \lambda - a'', \ \ldots$$

Тогда, следуя Weierstrass'у, мы называем *элементарными делителями* матрицы $\mathfrak{A}$ те из величин

$$\begin{array}{llll} (\lambda-a)^{e_1}, & (\lambda-a)^{e_2}, & \ldots, & (\lambda-a)^{e_r} \\ (\lambda-a)^{e'_1}, & (\lambda-a)^{e'_2}, & \ldots, & (\lambda-a)^{e'_r} \\ (\lambda-a)^{e''_1}, & (\lambda-a)^{e''_2}, & \ldots, & (\lambda-a)^{e''_r} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \end{array}$$

которые не приводятся к единице.

Очевидно, что $e_i \leq e_{i+1}$.

§ 58

Покажем на примере вычисление элементарных делителей.

Возьмем матрицу

$$\left\| \begin{array}{ccccccc} \lambda - a & b_1 & 0 & 0 & \ldots & 0 & 0 \\ 0 & \lambda - a & b_2 & 0 & \ldots & 0 & 0 \\ 0 & 0 & \lambda - a & b_3 & \ldots & 0 & 0 \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots \\ 0 & 0 & 0 & 0 & \ldots & \lambda - a & b_{n-1} \\ 0 & 0 & 0 & 0 & \ldots & 0 & \lambda - a \end{array} \right\|,$$

у которой диагональные элементы суть $\lambda - a$, все же остальные элементы нули, за исключением элементов $b_1, b_2, \ldots, b_{n-1}$, лежащих непосредственно выше диагональных.

В этом случае определитель матрицы будет

$$D_n(\lambda) = (\lambda - a)^n;$$

далее

$$D_{n-1}(\lambda) = 1,$$

ибо, если мы отбросим первую (левую) колонну и последнюю (нижнюю) горизонталь, то получим матрицу имеющую постоянный определитель

$$b_1 b_2 \cdots b_{n-1};$$

значит, у заданной матрицы существует единственный элементарный делитель

$$(\lambda - a)^n.$$

§ 59

Изложенная теория элементарных делителей может быть обобщена и перенесена на матрицы другого рода. Так например, можно рассматривать матрицы, элементы которых суть целые функций от многих независимых переменных.

Для теории чисел особенно важны исследования λ-матриц с целыми коэффициентами, а также когда элементы матрицы не целые функции, а целые числа, взятые из некоторого поля.

Для желающих ближе познакомиться с этой важной теорией можно порекомендовать: *Bôcher*. Einführung in die höhere Algebra 1910. *Muth*, Theorie und Anwendung des Elementarsteiler. *Bachmann*. Die Arithmetik der Quadratischen Formen 1898. (Zweiter Abschnitt. Zweites Kapitel).

Глава V

Теория подстановок

Понятие о группе

§ 1

Мы положим в основу наших дальнейших исследований понятие о так называемой *группе* однородных предметов, понятие, давшее возможность сблизить самые разнородные части математики.

Формулируем понятие о группе в его современном самом общем виде. Рассматривается совокупность $\mathfrak{M}$ некоторых однородных предметов. Эти предметы могут быть самой разнообразной природы: числа, формулы, аналитическая операции, геометрические фигуры, механические движения и т. д. Число предметов совокупности $\mathfrak{M}$ может быть как конечное так и бесконечное.

Установим понятие об операции *сопоставления* или *композиции* предметов совокупности $\mathfrak{M}$. Предположим, что указаны правила, по которым всяким двум предметам A и B совокупности $\mathfrak{M}$ сопоставляем некоторый определенный предмет C той же совокупности. Такое сопоставление будем обозначать символическим равенством

$$A * B = C,$$

где знак $*$ есть знак композиции, которую будем иногда называть *символическим умножением*. Композицию будем предполагать, вообще говоря, действием не перестановочным, то есть будем считать два результата композиции

$$A * B \quad \text{и} \quad B * A,$$

вообще говоря, различными.

Определение группы. Группой называется всякая совокупность G предметов $\mathfrak{M}$, обладающая следующими четыръмя свойствами:

I. *Композиция, всяких двух предметов совокупности G дает предмет той же совокупности.*

II. *Композиция предметов совокупности G обладает сочетательным (ассоциативным) законом*

$$A * (B * C) = (A * B) * C.$$

III. *Существуют в совокупности G предметы I такого вида, что для всякого предмета A из совокупности G имеет место равенство*

$$A * I = A.$$

Предмет I носит название **правой единицы** *группы.*

IV. *Для некоторой определенной из единиц I и для всякого предмета A совокупности G существует в совокупности G другой предмет X, удовлетворяющей равенству*

$$A * X = I;$$

элемент X носит название **правого обратного относительно** A.

§ 2

Предметы, входяшие в состав группы, носят название ее *элементов.*

Если число элементов группы конечное, то группа называется *конечною*, в обратном случае *бесконечною.* Число элементов конечной группы называется ее **порядком.**

Можно доказать, что данные в предыдущем параграфе четыре постулата: I, II, III, и IV, определяющее группу, независимы между собой.

Не имея в виду излагать полную теорию групп, мы остановимся только на самых важных свойствах групп.

Покажем прежде всего, что существует только одна единственная единица в группе.

Допустим существование двух единиц I и I_1, причем единица I есть та, которая требуется в постулате IV.

На основании постулата IV можем единице I_1 сопоставить элемент X такой, чтобы было

$$I_1 * X = I. \tag{1}$$

Умножая в смысле композиции это равенство слева на I_1, получим

$$I_1 * (I_1 * X) = I_1 * I,$$

откуда

$$(I_1 * I_1) * X = I_1 * I, \tag{2}$$

но I и I_1 единицы, следовательно,

$$I_1 * I_1 = I_1, \qquad I_1 * I = I_1,$$

и равенство (2) дает

$$I_1 * X = I_1,$$

откуда, сравнивая с (1), получим

$$I = I_1.$$

Покажем, что единственная правая единица I есть в то же самое время и левая. Положим, что

$$I * A = B. \tag{1}$$

Докажем, что $B = A$.

Возьмем для A правый обратный элемента Y и умножим на него справа равенство (1)

$$I * A * Y = B * Y,$$

где

(2) $$A * Y = I,$$

получаем

$$I * I = B * Y.$$

Сравнивая с (2), получим

$$A * Y = B * Y.$$

Умножая последнее равенство справа на элемента обратный Y, получим

$$A = B,$$

что и требовалось доказать.

Покажем наконец, что правый обратный элемент есть в то же самое время и левый обратный, то есть, что равенство

(1) $$A * X = I$$

влечет за собой как следствие

(2) $$X * A = I.$$

В самом деле, умножая равенство (1) слева на X, получим

$$X * A * X = X,$$

и, наконец, умножая справа на элемент обратный X, получим равенство (2).

§ 3

Резюмируя сказанное, мы замечаем, что в группе существует всегда единственная единица; ее мы будем обозначать через I.

При символическом умножении в смысле композиции элементов группы элементы, равные единице, можно пропускать

$$I * A * I * B * C = A * B * C.$$

Кроме того для всякого элемента A существует в группе элемент обратный, которой мы будем обозначать знаком A^{-1}, причем можно будет писать

$$A * A^{-1} = I, \qquad A^{-1} * A = I.$$

Нетрудно убедиться, что обратный элемент единственный.

Обратный элемент для обратного есть первоначальный, т. е.

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

Нетрудно видеть, что для группы решаются всегда уравнения первой степени

$$A * X = B, \qquad Y * A = B,$$

где A и B заданные элементы, а X, Y элементы искомые. Мы получаем

$$A = A^{-1} * B, \qquad Y = B * A^{-1}.$$

Если для всяких двух элементов группы имеет место *перестановочный* (*коммутативный*) закон композиции т. е.

$$A * B = B * A,$$

то группа носить название *абелевой* или *коммутативной.*

Оставляя в стороне *абстрактную* теорию групп, мы перейдем к группам конкретного вида, которые даются рассмотрением, так называемых, подстановок. Для желающих познакомиться с абстрактной теорией групп, независящей от природы их элементов, можно порекомендовать прекрасное сочинение моего ученика О. Ю. Шмидта. Абстрактная теория групп. Киев 1914 г.

Основные свойства подстановок

§ 4

Рассмотрим различные перемещения (permutations) n букв

$$a, \quad b, \quad c, , \ \ldots , \ k, \quad l.$$

Из элементарной алгебры известно, что число таких перемещений

$$N = 1 \cdot 2 \cdot 3 \cdots n.$$

Обозначим эти перемещения буквами:

$$A_0, \quad A_1, \quad A_2, \ \ldots , \ A_{N-1}.$$

Будем называть *подстановкою* (substitution) операцию, состоящую в переходе от одного какого-нибудь перемещения A_i к другому A_k, причем будем обозначать эту подстановку символом

$$\begin{pmatrix} A_k \\ A_i \end{pmatrix}.$$

Будем называть A_i *знаменателем* подстановки, а A_k ее *числителем.*

§ 5

Нетрудно видеть, что одну и ту же подстановку можно писать различными символами, причем можно писать различные знаменатели. Тогда числители должны также соответственно изменяться, ибо знак подстановки должен указывать, какою буквою заменяется каждая буква знаменателя. Порядок же букв в знаменателе вполне произволен.

Так, например, следующее знаки выражают одну подстановку:

$$\begin{pmatrix} b & c & a & d \\ a & b & c & d \end{pmatrix}, \quad \begin{pmatrix} a & b & c & d \\ c & a & b & d \end{pmatrix}, \quad \begin{pmatrix} d & c & b & a \\ d & b & a & c \end{pmatrix}.$$

Очевидно, что всякую подстановку можно написать так, чтобы знаменателем было данное перемещение, например A_0. Тогда различных подстановок будет только N, и все они могут быть представлены так:

$$\begin{pmatrix} A_0 \\ A_0 \end{pmatrix}, \quad \begin{pmatrix} A_1 \\ A_0 \end{pmatrix}, \quad \begin{pmatrix} A_2 \\ A_0 \end{pmatrix}, \ \ldots, \ \begin{pmatrix} A_{N-1} \\ A_0 \end{pmatrix},$$

где $\begin{pmatrix} A_0 \\ A_0 \end{pmatrix}$ есть так называемая *тождественная* подстановка, состоящая в том, что порядок букв перемещения не меняется.

§ 6

Что касается до символа подстановки, то мы будем рассматривать приведение его к простейшему виду, причем под простейшим видом будем разуметь такой, в котором пропущены все буквы, не изменяющиеся подстановкою, или, другими словами, занимающая одни и те же места в числителе и знаменателе.

Так, например, для подстановки

$$\begin{pmatrix} a & c & e & d & g & f & b \\ a & b & c & d & e & f & g \end{pmatrix}$$

простейшим видом будет:

$$\begin{pmatrix} c & e & g & b \\ b & c & e & g \end{pmatrix}$$

ибо буквы a, d, f не меняются.

§ 7

Введем понятие о *произведении* двух подстановок:

$$S = \begin{pmatrix} A_1 \\ A_0 \end{pmatrix}, \qquad T = \begin{pmatrix} A_2 \\ A_0 \end{pmatrix}.$$

Будем называть *произведением* двух подстановок третью, которая производит такую перемену в расположении букв перемещения, какую производят обе подстановки, одна за другою произведенные.

При рассмотрении произведения двух подстановок приходится указывать, в каком порядке эти две подстановки должны одна за другою следовать, ибо, вообще говоря, произведение двух подстановок зависит от порядка перемножения.

Например. две подстановки:

$$S_1 = \begin{pmatrix} b & c & e & a & d \\ a & b & c & d & e \end{pmatrix}, \qquad S_2 = \begin{pmatrix} c & a & e & b & d \\ a & b & c & d & e \end{pmatrix},$$

перемноженные таким образом, что первою совершается подстановка S_1, дают результаты

$$\begin{pmatrix} a & e & d & c & b \\ a & b & c & d & e \end{pmatrix}.$$

Перемноженные же в другом порядке, они дадут произведение:

$$\begin{pmatrix} e & b & d & c & a \\ a & b & c & d & e \end{pmatrix}.$$

Произведение двух подстановок мы будем обозначать так же, как и алгебраическое произведение, но только с условием, что знак, соответствующий подстановке, совершаемой сначала, будем писать налево от знака другой.

Так, например, произведение:

$$ST = \begin{pmatrix} A_1 \\ A_0 \end{pmatrix} \begin{pmatrix} A_2 \\ A_0 \end{pmatrix}$$

должно быть понимаемо в таком смысле, что первою должна быть произведена подстановка S, а затем уже T.

Если две подстановки S и T таковы, что будет

$$TS = ST,$$

то они называются *обратимыми*, или *коммутативными*.

Так, например, если две подстановки T и S, приведенные к простейшему виду, не имеют общих букв, то они, очевидно, обратимые.

Если мы рассмотрим несколько подстановок:

$$S, \quad T, \quad U, \quad V, , \ \ldots,$$

то, согласно сделанному условию, произведение:

$$STUV \cdots$$

должно пониматься в том смысле, что сначала подстановка S умножается на T, полученный результат умножается на U, новый результата на V, и так далее.

§ 8

Если все перемножаемые подстановки одинаковы, и число их μ, то произведение называется μ-ою степенью подстановки и обозначается знаком

$$S^{\mu}.$$

Если одна из перемножаемых подстановок есть тождественная

$$\begin{pmatrix} A_0 \\ A_0 \end{pmatrix},$$

то знак, соответствующий ей, может быть в произведена пропущен ибо эта подстановка не меняет букв, и мы имеем право считать ее равною единице, то есть

$$\begin{pmatrix} A_0 \\ A_0 \end{pmatrix} = I.$$

Наконец, приходится условиться считать символ S^μ равным единице при $\mu = 0$, какова бы ни была подстановка S.

§ 9

Пусть S будет некоторая подстановка, Напишем ряд ее степеней, начиная с нулевой,

$$I, \quad S, \quad S^2, \quad S^3, \quad \ldots \tag{1}$$

Так как общее число различных между собою подстановок конечное (именно, равное N), то в ряде (1), достаточно далеко продолженном, должна повториться одна из предыдущих подстановок.

Положим, что, получается: $S^{\mu+\nu} = S^\mu$; или, что то же, $S^\mu S^\nu = S^\mu$. Отсюда следует, что подстановка S^ν не меняет переставляемых букв, то есть она есть не что иное, как тождественная, именно:

$$S^\nu = I. \tag{2}$$

Возвышая равенство (2) в некоторую произвольную степень q, получим: $(S^\nu)^q = I$, или $S^{\nu q} = I$. Далее, умножая на S^r, получим, если r целое число,

$$S^{r+\nu q} = S^r. \tag{3}$$

Отсюда мы видим, что ряд подстановок (1) периодический, и что период состоит из подстановок

$$I, \quad S, \quad S^2, \quad \ldots, \quad S^{r-1}. \tag{4}$$

Нетрудно видеть, что подстановки (4) будут все различны между собой, если ν будет наименьшим показателем, при котором имеет место равенство (2). В самом деле, равенство: $S^{\mu_1+\nu_1} = S^{\mu_1}$ в предположении числа $\mu_1 + \nu_1$ меньшого, чем ν, влекло бы за собой $S^{\nu_1} = I$, что невозможно, ибо $\nu_1 < \nu$. Итак, будем называть *порядком* подстановки наименьший показатель ν, при котором $S^\nu = I$.

Другими словами, порядок подстановки показывает число раз, которое нужно перемножить подстановку, чтобы придти к первоначальному перемещению.

§ 10

Условимся распространить равенство $S^{r+\nu q} = S^r$ на отрицательные значения показателя r. Определим отрицательную степень S^{-r} подстановки равенством: $S^{-r} = S^{\nu q - r}$. При $r = 1$ можно взять $q = 1$, и мы получаем: $S^{-1} = S^{\nu-1}$.

Подстановки S и S^{-1} дают в произведении единицу и называются поэтому *обратными* одна относительно другой.

Очевидно, что если

$$S = \begin{pmatrix} A_1 \\ A_0 \end{pmatrix},$$

то будет иметь место формула:

$$S^{-1} = \begin{pmatrix} A_0 \\ A_1 \end{pmatrix}.$$

Теорема. *Если порядок подстановки S есть ν, то порядок подстановки S^μ будет $\dfrac{\nu}{\theta}$, где θ — общий наибольший делитель чисел ν и μ.*

Действительно, для нахождения порядка подстановки S^μ необходимо найти наименьшее число x, при котором $(S^\mu)^x = I$, или $S^{\mu x} = I$. Мы видим, что μx должно быть числом, кратным порядка ν подстановки, то есть $\mu x = \nu q$, где q целое число.

Отсюда

$$x = \frac{\nu}{\theta}\ \frac{q}{\frac{\mu}{\theta}},$$

где θ общий наибольший делитель чисел μ и ν.

Очевидно, что наименьшее значение для x получится при $q = \dfrac{\mu}{\theta}$ и равно $\dfrac{\nu}{\theta}$.

Если числа μ и ν взаимно простые, то $\theta = 1$ и, следовательно, порядок подстановки $T = S^\mu$ равен ν, то есть такой же, как у подстановки S.

Нетрудно убедиться, что в этом случае подстановки

$$I,\ \ T,\ \ T^2,\ \ T^3,\ \ \ldots,\ T^{\nu-1}$$

такие же, как и в ряде (4) § 9, но порядок их будет иной.

Нетрудно указать такое число x, при котором имеет место равенство: $S = T^x$. В самом деле, разложим дробь $\dfrac{\nu}{\mu}$ в непрерывную и обозначим предпоследнюю подходящую через $\dfrac{x}{y}$. Тогда, как известно, будем иметь:

$$\frac{\nu}{\mu} - \frac{x}{y} = \pm\frac{1}{\mu y}.$$

Отсюда получаем:

$$\mu x - \nu y = \mp 1.$$

Если мы соответственным образом подберем знаки чисел x и y, то эти числа будут удовлетворять равенству:

$$\mu x - \nu y = 1. \tag{1}$$

Нетрудно видеть, что и обратно возможность удовлетворить равенству (1) целыми значениями x и y влечет за собою, как следствие, что числа μ и ν взаимно-простые, так как очевидно, что эти числа не могут иметь общего делителя, отличного от единицы, ибо на этого общего делителя должна была бы делиться вторая часть, которая $= 1$.

Если числа μ и ν имеют некоторый общий делитель δ, то очевидно, что всегда можно найти такие числа x и y, что будет

$$\mu x - \nu y = \delta.$$

Итак, возвращаясь к нашей задаче, предположим, что мы подобрали числа x и y удовлетворяющими равенству (1). Тогда имеем:

$$S^{\mu x - \nu y} = S.$$

Но

$$S^\nu = I, \qquad S^\mu = T.$$

Следовательно, имеем:

$$S = T^x.$$

Разложение подстановок на циклы

§ 12

Пусть будет

$$A_0 = a\ b\ c\ \ldots\ k\ l$$

одно из перемещений заданных n букв.

Если вычеркнем букву a, занимающую первое место, и переместим ее, поместив направо от последней буквы l, то получим новое перемещение

$$A_1 = b\ c\ \ldots\ k\ l\ a.$$

Рассмотрим подстановку:

$$\begin{pmatrix} A_1 \\ A_0 \end{pmatrix} = \begin{pmatrix} b & c & d & \ldots & l & a \\ a & b & c & \ldots & k & l \end{pmatrix}.$$

Чтобы выполнить эту подстановку, достаточно разделить окружность округа на n частей, написать в точках деления буквы

$$a,\ b,\ c,\ \ldots,\ k,\ l$$

по порядку и заменять каждую букву следующей за нею в одну сторону вдоль по кругу. Другими словами, расположение A_1 букв получим из расположения A_0 поворотом окружности на $\frac{1}{n}$ часть 2π. Поэтому подстановка, которую мы рассматриваем, называется *круговою*, или *циклом*.

Очевидно, что порядок круговой подстановки равен числу n букв, которые эта подстановка перемещает, ибо после n поворотов круг возвращается в первоначальное свое положение.

Рассматриваемую круговую подстановку мы будем для сокращения обозначать знаком

$$(a, b, c, \ldots, k, l),$$

где в скобках написано то расположен букв, в котором следуют вдоль по кругу. Первая буква последнего обозначения круговой подстановки произвольна, то есть ту же самую подстановку мы будем обозначать знаками:

$$(b, c, \ldots, k, l, a), \qquad (c, \ldots, k, l, a.b), \quad \ldots,$$

причем можем начинать с любой буквы, лишь бы расположило всех букв соответствовало их чередованию на круге в одну и ту же сторону.

Цикл, состояний из двух букв

$$(a, b)$$

будем называть *транспозицией* этих букв.

§ 13

Теорема I. *Каждая подстановка, если она не круговая, есть произведение нескольких круговых не имеющих общих букв.*

Пусть S будет некоторая подстановка. Берем одну из букв, перемещаемых этой подстановкой, например a. Пусть эта буква заменяется некоторою другою b. Пусть затем буква b заменяется буквою c и так далее. Продолжая следить за рядом последовательных букв $a,\ b,\ c,\ \ldots$, необходимо дойдем, наконец, до такой буквы f, которая заменяется первой буквой a.

Получаем таким образом цикл:

$$C_0 = (a, b, c, \ldots, f).$$

Если этим циклом исчерпываются все буквы, перемещаемые подстановкой S, то сама подстановка S есть не что иное, как круговая C_0. Если же подстановка S не круговая, то цикл C_0 не исчерпывает перемещаемых букв. Берем какую-нибудь из остальных букв и, оперируя по прежнему, составляем новую группу букв, образующих новый цикл C_1.

Продолжая далее выделение циклов, исчерпаем, наконец, все буквы подстановки S.

Получим:

$$S = C_0 C_1 C_2 \cdots ,$$

то есть, требуемое разложение подстановки на циклы.

Очевидно, что множители в последней формул могут быть перещены.

Например, подстановка

$$S = \begin{pmatrix} h & k & d & f & b & j & a & g & e & c & i \\ a & b & c & d & e & f & g & h & i & j & k \end{pmatrix}$$

раскладывается на следующие циклы:

$$S = (a, h, g)(k, k, i, e)(c, d, f, j).$$

Если подстановка S не изменяет некоторых букв, то эти буквы не входят в простейшее выражение подстановки и, следовательно, не входят также в разложение по циклам.

Иногда желательно не терять из виду этих неизменяемых подстановкой букв. Тогда является полезным рассматривать циклы из одной буквы, например

$$(a),$$

причем знаком (a) указывать, что буква не меняется.

Тогда, например подстановку

$$S = \begin{pmatrix} d & c & b & a & e & f \\ a & b & c & d & e & f \end{pmatrix}$$

можно переписать так:

$$S = (a, d)(b, c)(e)(f).$$

§ 14

Теорема II. *Порядок подстановки есть наименьшее кратное порядков ее циклов.*

Пусть будет

$$S = C_0 C_1 C_2 \cdots ,$$

где $C_0, C_1, C_2, \ldots$ — циклы.

Тогда, обозначая через ν порядок подстановки S, получим:

$$C_0^\nu C_1^\nu C_1 \nu \cdots = I.$$

Так как циклы не имеют общих букв, то из предыдущего равенства вытекают, как необходимые следствия, следующие:

$$C_0^\nu = I, \quad C_1^\nu = I, \quad C_2^\nu = I, \ \ldots$$

Отсюда следует, что число ν должно быть кратным порядков циклов.

§ 15

Будем называть подстановку *правильною*, если порядки всех ее циклов одинаковы, и *неправильною* в обратном случай.

Например, подстановка

$$\begin{pmatrix} d & f & b & e & a & c \\ a & b & c & d & e & f \end{pmatrix} = (a, d, e)(b, f, c)$$

есть правильная.

Подстановка же

$$\begin{pmatrix} a & c & e & f & b & g & d \\ a & b & c & d & e & f & g \end{pmatrix} = (a)(b, c, e)(d, f, g)$$

неправильная.

§ 16

Теорема III. *Степень μ круговой подстановки порядка ν есть сама круговая подстановка, если μ и ν — числа взаимно-простые. Если же μ и ν имеют общий множитель θ, отличный от единицы, то S^μ будет правильная подстановка из θ циклов по $\dfrac{\nu}{\theta}$ букв в каждом.*

В самом деле, расположим буквы круговой подстановки S вдоль по кругу. Тогда подстановка S^μ будет соответствовать повороту круга на угол $\mu\dfrac{2\pi}{\nu}$. Будем раскладывать эту подстановку на циклы. Начнем с какой-нибудь буквы, находящейся на некоторой точке круга. Эта буква заменяется другою, отстоящей на расстоянии $\mu\dfrac{2\pi}{\nu}$ по дуге круга. Эта последняя заменена будет новою, находящейся от первой буквы на расстоянии $\mu\dfrac{2\pi}{\nu}$ 2. И так далее. Наконец, мы придем к первоначальной букве, когда в выражении $\mu\dfrac{2\pi}{\nu}$ x целое число x будет наименьшее, при

котором число: $\mu\frac{2\pi}{\nu}\,x$ сделается кратностью 2π, то есть, когда будет: $\mu\frac{2\pi}{\nu}\,x = q2\pi$. Отсюда видим, что число x придется искать, как наименьшее, удовлетворяющее равенству: $\mu x = \nu q$. На основании соображений, приведенных в § 11, замечаем, что искомое значение x есть $\frac{\nu}{\theta}$, откуда следует справедливость теоремы. Если μ и ν — числа, взаимно-простые, $\theta = 1$, и подстановка S^μ есть круговая.

Пример:

$$S = (a, b, c, d, e, f)$$
$$S^2 = (a, c, e)(b, d, f)$$
$$S^3 = (a, d)(b, e)(c, f)$$
$$S^4 = (a, e, c)(b, f, d)$$
$$S^5 = (a, f, e, d, c, b)$$
$$S^6 = I.$$

В этой таблице мы получили круговую подстановку только для пятой степени, ибо 5 — единственное число, кроме 1, меньшее ? и взаимно простое с ним.

§ 17

Теорема IV. *Правильная подстановка есть степень некоторой круговой* (теорема, обратная предыдущей).

В самом деле, нетрудно убедиться, что правильная подстановка

$$S = (a_1, b_1, \ldots, g_1)(a_2, b_2, \ldots, g_2)\ \ldots\ (a_\theta, b_\theta, \ldots, g_\theta),$$

составленная из θ циклов по $\frac{\nu}{\theta}$ букв в каждом, есть степень θ такой круговой подстановки ν букв:

$$C = (a_1, a_2, a_3, \ldots, a_\theta, b_1, b_2, b_3, \ldots, b_\theta, \ldots, g_1, g_2, g_3, \ldots, g_\theta),$$

так что

$$S = C^\theta.$$

§ 18

Две подстановки мы будем называть *подобными*, если они состоят из одинакового числа циклов, причем порядки этих циклов в обоих подстановках представляют одну и ту же систему чисел.

Например, подобны подстановки:

$$(a, b, c)(d, e)(f), \qquad (b, e, f)(c, a)(d).$$

§ 19

Теорема V. *Если S и S' суть две подобные подстановки, то существует такая подстановка P, что имеет место равенство:*

$$PS' = SP; \tag{1}$$

и обратно, если существует подстановка P, удовлетворяющая предыдущему равенству, то S и S' подобные подстановки.

Напишем обе подстановки S и S' разложенными на циклы (с указанием циклов из одной буквы) одну под другую таким образом, чтобы под каждым циклом одной подстановки был написан цикл другой, состоящей из того-же числа букв.

Тогда, если мы пропустим скобки в циклах, то получим два перемещения из n букв, написанных одно под другим:

$$a \quad b \quad c \quad \ldots \quad k \quad l, \tag{2}$$

$$a' \; b' \; c' \; \ldots \; k' \; l', \tag{3}$$

где буквы (3) суть те же, что и буквы (2), только написанные в другом порядке.

Так например, для подстановок:

$$(a, b, c)(d, e)(f),$$
$$(b, e, f)(c, a)(d)$$

перемещения (2) и (3) будут такие:

$$\begin{matrix} a & b & c & d & e & f, \\ a' & b' & c' & d' & e' & f', \end{matrix}$$

где

$$a' = b, \quad b' = e, \quad c' = f, \quad d' = c, \quad e' = a, \quad f' = d.$$

Будем рассматривать подстановку P, состоящую в замене каждой буквы ряда (2) соответственною, стоящею в ряде (3).

Принимая обозначение (3), можно сказать, что подстановка P состоит в добавлении к каждой букве значка.

Будем рассматривать ряд перемещений:

$$A, \quad B, \; \ldots$$

Пусть он при помощи подстановки P обращается в ряд следующих перемещений:

$$A', \quad B', \; \ldots$$

Тогда очевидно, что подстановку P можно написать в одном из следующих видов:

$$\begin{pmatrix} A' \\ A \end{pmatrix}, \qquad \begin{pmatrix} B' \\ B \end{pmatrix}.$$

Нетрудно видеть, что если одна из двух подстановок есть:

$$S = \begin{pmatrix} B \\ A \end{pmatrix},$$

то другая подстановка будет:

$$S' = \begin{pmatrix} B' \\ A' \end{pmatrix}.$$

Но очевидно, что

$$S' = \binom{A}{A'}\binom{B}{A}\binom{B'}{B}.$$

Далее имеем:

$$\binom{A'}{A} = \binom{B'}{B} = P,$$

откуда

$$\binom{A}{A'} = P^{-1}.$$

Получаем:

$$S' = P^{-1}SP.$$

Таким образом мы нашли подстановку P, удовлетворяющую равенству (1).

Обратная теорема также справедлива.

В самом деле, обозначая через S произвольную подстановку, а через P одну из равносильных:

$$\binom{A'}{A}, \qquad \binom{B'}{B},$$

состоящую в замене ряда букв (2) рядом букв (8), получаем из равенства:

$$S' = P^{-1}SP$$

такое:

$$S' = \binom{A'}{A}\binom{B}{A}\binom{B'}{B} = \binom{B'}{A'}.$$

Отсюда видим что подстановка S' будет подобна подстановке S, ибо происходит из этой последней через замену букв (2), находящихся в циклах, буквами (3).

Следствие. *Два произведения: ST и TS двух произвольных подстановок суть подстановки подобные.*

В самом деле, обозначая: $ST = P$, $TS = Q$, получим из второго равенства: $S = T^{-1}Q$. Подставляя в первое равенство, получим: $P = T^{-1}QT$, откуда следует, что подстановки Q и P подобные.

Например, рассмотрим две подстановки:

$$S = (a, b, c, d)(e, f)$$
$$T = (a, b, c)(d, e, f).$$

Получим

$$ST = (a, c, e, d, b)(f),$$
$$TS = (a, c, b, d, f)(e).$$

§ 20

Мы видели уже два примера обратимых подстановок, а именно таковы степени одной и той же подстановки, а также подстановки, не имеющие общих букв.

Обратимся теперь к рассмотрению самого общего вида обратимых подстановок. Если две подстановки обратимы, то имеет место равенство: $TS = ST$, или $S = T^{-1}ST$. Но мы видели, что подстановка $T^{-1}ST$ выводится из подстановки S через производство подстановки T в циклах подстановки S.

Последнее равенство показывает, что подобное преобразование подстановки S при помощи подстановки T не должно в этом случай менять этой подстановки. Следовательно, подстановка T должна производить только следующее перемещение букв:

> перемещение циклов одинакового порядка подстановки S одного на место другого и
>
> простое перемещение букв каждого цикла, состоящее из передвижения какой-либо буквы на первое место без изменения последовательности букв.

Например, если задана подстановка:

$$S = (a, b, c)(d, e, f)(g, h)(k)$$

и мы эту же самую подстановку подпишем под нею по правилам, указанным выше, допуская при этом только изменение расположения циклов с одинаковым числом букв, а также изменение первой буквы циклов, то новый вид подстановки, например

$$(d, .e, f)(b, c, a)(h, g)(k),$$

приведет к подстановке:

$$T = \begin{pmatrix} d & e & f & b & c & a & h & g & k \\ a & b & c & d & e & f & g & h & k \end{pmatrix},$$

которая будет обратима с заданною.

§ 21

Покажем теперь, что *каждую подстановку можно представить, как произведение транспозиций.*

Возьмем произвольную подстановку:

$$S = \begin{pmatrix} a' & b' & c' & \dots & k' & l' \\ a & b & c & \dots & k & l \end{pmatrix},$$

где $a', b', c', \dots, k', l'$ иное перемещение букв: $a, b, c, \dots, k, l$. Умножим подстановку S на транспозицию (l, l'). Тогда в произведении: $S' == S(l, l')$ буква l не перемещается и, следовательно, подстановка S' перемещает $n-1$ остальных букв: $a, b, c, \dots, k$ и может быть написана так

$$S' = \begin{pmatrix} a'' & b'' & c'' & \dots & k'' \\ a & b & c & \dots & k \end{pmatrix}.$$

Но, принимая во внимание, что $(l, l')^2 = I$, получаем:

$$S = S'(l, l'). \tag{1}$$

Умножая далее S' на транспозицию (k, k''), получим подстановку S'', перемещающую только $n-2$ оставшаяся буквы. Следовательно, выходит: $S' = S''(k, k'')$, откуда, на основаны равенства (1), получаем: $S = S''(k, k'')(l, l')$.

Продолжая дальнейшее преобразование подстановки S'', представим окончательно подстановку S в виде произведения транспозиций.

Очевидно, что такое разложение может быть произведено не одним способом.

Докажем. что *если при одном способе разложения мы представим подстановку в виде произведения четного (нечетного) числа транспозиций, то и при другом способе разложены получим четное (нечетное) число множителей.*

Предположим, что данная подстановка S разбита на циклы.

Посмотрим, какое влияние на число циклов будет иметь умножение данной подстановки S на транспозицию

$$T = (a, f)$$

Рассмотрим два случая:

1) Обе буквы a и f принадлежать к одному циклу подстановки S;

2) эти буквы принадлежать к разным циклам.

Рассмотрим сначала первый случай; пусть цикл, заключающей буквы транспозицию T, будет:

$$C = (a, b, \ldots, e, f, g, \ldots, k).$$

Нетрудно видеть, что C, после умножения на T слева, распадается на два цикла:

$$(a, g, \ldots, k)(f, b, \ldots, e).$$

Итак, транспозиция T разбивает цикл C на 2 новых. Остальные же циклы транспозиция T оставляет без перемены.

Обращаемся теперь к рассмотрению случая, когда буквы транспозиции:

$$T = (a, a')$$

принадлежать к двум различным циклам:

$$C = (a, b, \ldots, g), \qquad C' = (a', b', \ldots, k').$$

Тогда имеем:

$$TCC' = (a, b', \ldots, k', a', b, \ldots, g).$$

Другими словами, транспозиция T соединяет два цикла, не изменяя их.

Предположим что подстановка S состоит из ν циклов и может быть представлена в виде произведения μ транспозиций.

Тогда, умножая это произведение на транспозицию в обратном порядке, придем к тождественной подстановке, имеющей n однобуквенных циклов (n число всех букв).

Получается, следовательно, приобретение $n - \nu$ циклов.

Но так как умножению на каждую транспозицию должно соответствовать приобретение или потеря одного цикла, то очевидно, что число μ транспозиций, на которые разлагается подстановка, может отличаться только на четное число от числа $n - \nu$.

Но число $n - \nu$ зависит только от числа циклов заданной подстановки и не зависит от метода разложения ее на транспозиции. Отсюда следует, что высказанное утверждение справедливо.

§ 22

Теорема VI. *Все подстановки из n букв распадаются на два рода, из которых подстановки первого рода могут быть разложены на четное число транспозиций двух букв, подстановки же второго рода на нечетное.*

Нетрудно видеть, что в каждом роде заключается одинаковое число подстановок, а именно $\frac{1}{2} N$, ибо умножением на транспозицию каждая подстановка первого рода переходить в подстановку второго рода, и обратно.

О группах подстановок

§ 23

Очевидно, что образует группу такая совокупность подстановок, что каждые две подстановки этой совокупности дают в произведений подстановку той же совокупности.

Мы будем называть порядком группы подстановок число подстановок, образующих группу. Число n перемещаемых букв мы назовем *степенью* группы подстановок.

§ 24

Все N подстановок степени n образуют группу.

Функции от n букв, не изменяющиеся при всех N подстановках, называются *симметрическими*. Отсюда группу всех N подстановок называют *симметрическою*.

§ 25

Нетрудно видеть, что *подстановки первого рода, эквивалентные четному числу перестановок, образуют группу.*

Рассмотрим такую функцию:

$$\begin{aligned} U = (x_1 - x_2)(x_1 - x_3) \cdots (x_1 - x_n) \\ (x_2 - x_3) \cdots (x_2 - x_n) \\ \cdots\cdots\cdots\cdots \\ (x_{n-1} - x_n) \end{aligned}$$

от n независимых переменных:

$$x_1,\ x_2,\ x_3,\ \ldots,\ x_{n-1},\ x_n.$$

Тут функция U меняет свой знак при транспозиции двух из числа n значков:

$$1,\ 2,\ \ldots,\ n,$$

и мы видим, что функция U принимает два различных значений $+U$ и $-U$, причем, она

$$\begin{aligned} &\text{равна} \quad +U \quad \text{при подстановках первого рода} \\ &\text{и равна} \quad -U \quad \text{при подстановках второго рода.} \end{aligned}$$

Функции, подобные U, изменяющие при подстановке неизвестных только свой знак, называются *знакопеременными*.

Поэтому группа подстановок первого рода, не меняющих функции U, носит название *знакопеременной группы*.

§ 26

Укажем еще примеры групп подстановок.

a) Степени:

$$I,\ S,\ S^2,\ \ldots,\ S^{\nu-1},$$

образующие период подстановки S, составляют, очевидно, группу порядка ν.

Эту группу будем называть *циклическою*.

b) Подстановки, оставляющие без перемены k букв, образуют группу порядка:

$$1 \cdot 2 \cdot 3 \cdots (n-k)$$

(число всех подстановок, меняющих остальные $n-k$ букв).

c) Подстановки, оставляютция без перемены некоторую функцию, образуют всегда группу.

Например, функция:

$$x_1x_2 + x_3x_4$$

от четырех букв:

$$x_1,\quad x_2,\quad x_3,\quad x_4$$

не меняется при следующих подстановках четырех цифр: $1, 2, 3, 4$:

$$1,\ (1,2),\ (3,4),\ (1,2)(3,4),\ (1,3)(2,4),\ (1,4)(2,3),\ (1,3,2,4),\ (1,4,2,3).$$

Эти подстановки образуют группу восьмого порядка.

§ 27

Из определения понятия о группе подстановок следует, что в каждой группе должна, во первых, заключаться тождественная подстановка, а во вторых, каждой подстановке группы должна соответствовать входящая в эту группу обратная подстановка. В самом деле, возьмем какую нибудь подстановку S группы; тогда в группу должны входить, очевидно, все степени подстановки S:

$$S,\ S^2,\ S^3,\ \ldots,\ S^{\nu-1},\ S^{\nu} = I,$$

где ν порядок подстановки S.

Итак, мы видим, что *в группу входят* I *и* $S^{\nu-1} = S^{-1}$.

Если две группы Γ и G таковы, что все подстановки группы G входят в состав группы Γ, то группа G называется *делителем группы* Γ, или *подгруппой*.

Теорема Langrange'a. *Порядок делителя G есть делитель порядка группы* Γ.

Пусть μ порядок группы G, а m порядок группы Γ. Не предполагая делитель G тождественным с Γ, мы должны допустить, что

$$m > \mu.$$

Рассмотрим все μ подстановок группы G:

$$I,\ S_1,\ S_2,\ \ldots,\ S_{\mu-1}. \tag{1}$$

Так как $m > \mu$, то среди подстановок группы Γ будет существовать, по крайней мере, одна T_1, не принадлежащая делителю G. Умножим подстановку (1) справа на T_1; тогда получим систему подстановок:

$$T_1,\ S_1T_1,\ S_2T_1,\ \ldots,\ S_{\mu-1}T_1. \tag{2}$$

Все подстановки системы (2) принадлежат группе Γ и, очевидно, различны между собой, ибо равенство:

$$S_iT_1 = S_jT_1$$

влекло бы за собой:

$$S_i = S_j,$$

что невозможно, ибо в ряде (1) указаны различный между собой подстановки группы G.

Далее, ни одна из подстановок (2) не может входить в состав группы (1), ибо, допустив обратное, т. е., что

$$S_iT_1 = S_j,$$

получили бы:

$$T_1 = S_i^{-1}S_j,$$

т. е. выходило бы, что T_1 принадлежит к группе (1), ибо в состав группы (1) входит, на основании сказанного в § 27, подстановка:

$$S_i^{-1}.$$

Если двумя системами (1) и (2) исчерпана группа Γ, то следовательно,

$$m = 2\mu,$$

и теорема доказана.

Если же $m > 2\mu$, то должна существовать в группе Γ подстановка T_2, не входящая ни в одну из систем (1) и (2). Умножая справа на эту подстановку все подстановки группы (1), получим новую систему:

$$T_2,\ S_1T_2,\ S_2T_2,\ \ldots,\ S_{\mu-1}T_2. \tag{3}$$

Подобно предыдущему убеждаемся, что подстановки системы (3) все различны между собой и отличны от подстановок группы (1). Нетрудно убедиться, что подстановки (3) отличны также от подстановок (2). В самом деле, если бы было:

$$S_i T_2 = S_j T_1,$$

то мы имели бы:

$$T_2 = S_1^{-1} S_j T_1;$$

но $S_i^{-1} S_j$ принадлежит к групп (1) и, следовательно, T_2 принадлежала бы к системе (2), что противоречит сделанному предположению.

Если тремя системами (1), (2), (3) исчерпывается группа Γ, то $m = 3\mu$, и теорема доказана; если $m > 3\mu$, то продолжаем рассуждение далее. Очевидно, что мы к конце концов получим:

$$m = q\mu, \tag{4}$$

где q есть целое число, и группа Γ разбивается на q систем:

$$\begin{array}{llllll} I, & S_1, & S_2, & \ldots, & S_{\mu-1}; \\ T_1, & S_1T_1, & S_2T_1, & \ldots, & S_{\mu-1}T_1; \\ T_2, & S_1T_2, & S_2T_2, & \ldots, & S_{\mu-1}T_2; \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ T_{q-1}, & S_1T_{q-1}, & S_2T_{q-1}, & \ldots, & S_{\mu-1}T_{q-1}. \end{array} \tag{5}$$

Системы (5) будем называть *сопряженными с группой* (1).

Нетрудно показать, что *из сопряженных систем только одна первая (1) есть группа.*

В самом деле, если бы система:

$$T_i,\ S_1T_i,\ S_2T_i,\ \ldots,\ S_{\mu-1}T_i$$

была группой, то было бы:

$$(S_kT_i)(S_lT_i) = S_rT_i,$$

откуда

$$S_kT_iS_l = S_r,$$

или, окончательно,

$$T_i = S_k^{-1} S_r S_l^{-1},$$

т. е. подстановка T_i принадлежала бы к делителю (1), что невозможно.

§ 29

Сопряженный системы (5) предыдущего §-а получились умножением подстановок группы G справа на подстановки:

$$I,\ T_1,\ T_2,\ \ldots,\ T_{q-1}.$$

Подобным же образом можно найти подстановки:

$$I,\ U_1,\ U_2,\ \ldots,\ U_{q-1},$$

умножением на которые слева получим разложение группы T на сопряженные системы следующего вида:

$$\begin{array}{lllll} I, & S_1, & S_2, & \ldots, & S_{\mu-1}; \\ U_1, & U_1S_1, & U_1S_2, & \ldots, & U_1S_{\mu-1}; \\ \multicolumn{5}{l}{\dotfill;} \\ U_{q-1}, & U_{q-1}S_1, & U_{q-1}S_2, & \ldots, & U_{q-1}S_{\mu-1}. \end{array}$$

§ 30

Очевидно, что всякая группа подстановок представляет делитель симметрической группы, и, следовательно, порядок всякой группы должен быть делителем числа:

$$N = 1 \cdot 2 \cdot 3 \cdot 4 \cdots n.$$

Кроме того, порядок группы должен равняться кратному порядков отдельных, входящих в состав ее подстановок, ибо, если ν будет порядок подстановки S группы, то группа:

$$I,\ S,\ S^2,\ \ldots,\ S^{\nu-1}$$

порядка ν будет делителем рассматриваемой группы, и, следовательно, порядок группы должен быть кратным порядка ν входящей в нее подстановки S.

Если число n перемещаемых букв простое, то всякая группа порядка n должна состоять из степеней круговой подстановки этих букв.

В самом деле, порядок каждой из входящих в группу подстановок, будучи делителем простого числа n, должен равняться или n или единице; следовательно, группа должна состоять из степеней одной подстановки. Покажем, что эта подстановка должна быть круговая.

Так как порядок входящего в подстановку цикла должен быть делителем порядка подстановки, то в данном случай у подстановки должны быть циклы одного из двух порядков: 1 или n; следовательно, подстановка должна состоять из одного цикла порядка n.

§ 31

Подстановки, общие двум группам, образуют, очевидно, группу, которая называется *наибольшим общим делителем данных групп.*

Пусть порядок группы будет m, а порядок ее делителя будет μ, причем

$$m = q\mu.$$

Целое число q называется *индексом делителя.*

§ 32

Одной из наиболее важных по приложениям к алгебре задач теории групп подстановок, является задача нахождения всех групп подстановок из данного числа букв, или иначе, задача нахождения всех делителей симметрической группы.

Lagrange и после него ряд выдающихся математиков занимались этой задачей, но, несмотря на их усилия, до сих пор наука владеет лишь небольшим числом общих предложений, относящихся к этой задаче.

Мы изложим результаты, имеющие наиболее важное значение.

§ 33

Индексы всех делителей симметрической группы должны быть, конечно, делителями числа:

$$N = 1 \cdot 2 \cdot 3 \cdots n.$$

Наименьший из таких делителей есть 2. Мы видели уже, что знакопеременная группа имеет индекс, равный 2.

Покажем теперь предложение обратное, а именно, что *группа с индексом* 2 *не может отличаться от знакопеременной.*

Итак, рассмотрим группу индекса 2:

$$I,\ S_1,\ S_2,\ \ldots,\ S_{\frac{N}{2}}. \tag{1}$$

Умножим группу (1) справа и слива на подстановку T симметрической группы, получим две системы:

$$T,\ TS_1,\ TS_2,\ \ldots,\ TS_{\frac{N}{2}}; \tag{2}$$

$$T,\ S_1T,\ S_2T,\ \ldots,\ S_{\frac{N}{2}}T. \tag{3}$$

Обе системы (2) и (3) совпадают, какова бы ни была подстановка T.

В самом деле, если подстановка T принадлежите к группе (1), то обе системы совпадают с группой (1) и, следовательно, совпадают между собой; если же подстановка T не принадлежите к группе (1), то обе системы (2) и (3) также совпадают, ибо в случае индекса 2 должна существовать только одна система, сопряженная с группой.

Итак, всегда, всякому значку i можно будет сопоставить такой значок j, что будет

$$TS_i = S_jT,$$

или

$$S_i = T^{-1}S_jT.$$

Отсюда мы видим, что группа (1) должна заключать все подстановки, подобные с какою нибудь S_j, ибо T произвольная подстановка.

Можно утверждать, что в группе (1) не должно быть ни одной транспозиции, состоящей из двух букв. Допустив обратное, а именно, что к группе (1) принадлежите какая нибудь перестановка двух букв, мы придем к ложному заключению, что в группу входят все перестановки двух букв, т. е. группа симметрическая.

Представим себе теперь, что T есть транспозиция двух букв; тогда очевидно, что все транспозиции двух букв должны входить в составь сопряженной системы (2), ибо они не входят в группу (1). Если мы, далее, умножим обе системы (1) и (2) на транспозицию U двух букв, то системы (1) и (2) перейдут одна в другую следовательно, группа (1) заключает все произведения по две транспозиции двух букв и потому совпадает с знакопеременной, что и требовалось показать.

§ 34

Теорема. *Все подстановки знакопеременной группы могут быть представлены в виде произведений тройных циклов.*

Справедливость теоремы доказывается тем, что всякая пара перестановок двух букв дает в произведении один или два тройных цикла. В самом деле

$$(a, b)(a, c) = (a, b, c),$$

а

$$(a, b)(c, d) = (a, c, d)(a, c, b).$$

§ 35

Теорема. *Группа, заключающая все транспозиции по две буквы*

$$a,\ b,\ c,\ \ldots,\ k,\ l,$$

с общей буквой, так, например, транспозиции

$$(a, b),\ (a, c),\ \ldots,\ (a, k),\ (a, l), \tag{1}$$

есть симметрическая.

Доказательство основывается на том, что всякая транспозиция двух букв равносильна одной или нескольких из ряда (1). В самом деле,

$$(b, c) = (a, b)(a, c)(a, b).$$

§ 36

Теорема. *Если группа заключаешь все тройные циклы с двумя одинаковыми буквами, то она должна заключать знакопеременную группу, как делитель.*

Пусть перемещаемые буквы будут

$$a_1,\ a_2,\ \ldots,\ a_n$$

и пусть в состав группы входят циклы

$$(a_1, a_2, a_3),\ (a_1, a_2, a_4),\ \ldots,\ (a_1, a_2, a_4).$$

Нетрудно убедиться. что в группу должны входить все тройные циклы и, следовательно, вся знакопеременная группа. В справедливости сказанного убеждаемся из формул

$$(a_2, a_1, a_4) = (a_1, a_2, a_3)^2,$$
$$(a_1, a_3, a_4) = (a_1, a_2, a_3)(a_2, a_1, a_4)(a_2, a_1, a_3),$$
$$(a_2, a_3, a_4) = (a_2, a_1, a_3)(a_1, a_2, a_4)(a1, a_2, a_3),$$
$$(a_3, a_4, a_5) = (a_2, a_1, a_3)(a_2, a_4, a_5)(a_1, a_2, a_3).$$

§ 37

Будем называть по примеру Cauchy группу *транзитивною*, если среди ее подстановок может быть указана такая, которая переводит одну из букв в произвольно выбранную другую.

В обратном случае группа называется *интранзитивною*. Так, например, группа подстановок, не меняющая некоторую букву a, интранзитивная, ибо в группе не существует подстановок, заменяющих букву a на некоторую другую.

Высказанное понятие о транзитивности группы может быть обобщено следующим образом: группа называется *m раз транзитивною*, если подстановки группы допускают замену некоторых определенных m букв на m произвольно выбранных других.

Если группа m раз транзнтивна, то она способна заменять m произвольно выбранных букв

$$a_1,\ a_2,\ \ldots,\ a_m \tag{1}$$

на другие, также произвольно выбранные

$$b_1,\ b_2,\ \ldots,\ b_m, \tag{2}$$

ибо по определению существует m букв, которые заменяются, как буквами (1), так и буквами (2).

Нетрудно видеть, что *симметрическая группа есть $n-1$ раз транзитивная.*

Покажем, что *зкакопеременная группа может быть рассматриваема, как $n-2$ раз транзитивная.* В этом можно убедиться так: составим подстановку, заменяющую одни определенный $n-2$ буквы

$$a_1,\ a_2,\ \ldots,\ a_{n-2}$$

на другие, произвольно указанная

$$b_1,\ b_2,\ \ldots,\ b_{n-2}.$$

Вид такой подстановки будет

$$\begin{pmatrix} b_1 & b_2 & b_3 & \ldots & b_{n-2} & b_{n-1} & b_n \\ a_1 & a_2 & a_3 & \ldots & a_{n-2} & a_{n-1} & a_n \end{pmatrix},$$

где

$$a_{n-1},\ a_n,\ b_{n-1}, b_n$$

остальные перемещаемые буквы. Пишем в нашей подстановке эти остальные буквы в произвольном порядке. Если подстановка оказывается не принадлежащей знакопеременной группе. то достаточно переставить буквы b_{n-1} и b_n, чтобы получить подстановку знакопеременной группы.

Если в группу входит круговая подстановка всех букв, то группа, очевидно, транзитивная.

§ 38

Если все n переставляемых букв распадаются на несколько рядов

$$\begin{array}{llll} a_1, & a_2, & \dots & a_k; \\ a_{k+1}, & a_{k+2}, & \dots & a_{2k}; \\ \dots\dots\dots\dots\dots\dots\dots\dots & & & \\ a_{n-k+1}, & a_{n-k+2}, & \dots & a_n; \end{array} \tag{1}$$

по k букв в каждом ряде, причем все подстановки группы перемещают буквы только так, что буквы рядов (1) не разделяются, другими словами, две буквы одного ряда не могут замениться буквами разных, то группа называется *импримитивною.* Ряды (1) называются *системами импримитивности.*

Если нельзя разбить переставляемые буквы на системы, обладающие вышеуказанным свойством, то группа называется *примитивною.*

Так например, группа степеней круговой подстановки из букв

$$\begin{aligned} &I \\ &S_1 = (a, b, c, d, e, f) \\ &S_2 = (a, c, e)(b, d, f) \\ &S_3 = (a, d)(b, e)(c, f) \\ &S_4 = (a, e, c)(b, f, d) \\ &S_5 = (a, f, e, d, c, b) \end{aligned}$$

двойным образом импримитивна, причем за системы импримитивности можно выбрать

$$\begin{array}{c} a,\ c,\ e \\ b,\ d,\ f \end{array} \quad \text{или} \quad \begin{array}{c} a,\ d \\ b,\ e \\ c,\ f. \end{array}$$

§ 39

Теорема. *Если транзитивная группа подстановок содержит отдельную транспозицию двух букв, то она или, симметрическая, или примитивная.*

Итак, пусть транзитивная группа содержит транснозицию

$$(a_1, a_2).$$

Пусть, кроме того, в группе содержатся транспозиция

$$(a_1, a_3),\ (a_1, a_4),\ \ldots,\ (a_1, a_m),$$

переводящая букву a_1 в другие

$$a_3,\ \ldots,\ a_m.$$

Число m может быть равно 2; тогда в группу входить только одна транспозиция

$$(a_1, a_2).$$

Если $m = n$, где n число всех букв, то по теореме § 34 группа должна быть симметрическою.

Если $m < n$, то покажем, что группа импримитивная.

Возьмем какую нибудь букву b, не принадлежащую к системе

$$a_1,\ a_2,\ \ldots,\ a_m. \tag{1}$$

В группе не может заключаться транспозиция, перемещающая букву b с какою нибудь из букв

$$a_2,\ \ldots,\ a_m.$$

В самом деле, допустим обратное, т. е. что в группе находится транспозиция (a_i, b); тогда замечаем, что должна находиться в этой группе также транспозиция

$$(a_1, b) = (a_1, a_i)(a_i, b)((a_1, a_i).$$

что противоречить предположение.

Так как группа транзитивна, то будет существовать некоторая подстановка T_1 переводящая букву a_1 в b_1, где b_1 не входит в систему (1).

Покажем, что подстановка T_1 должна переводить все другие буквы

$$a_2,\ a_3,\ \ldots,\ a_m$$

в буквы

$$b_2,\ b_3,\ \ldots,\ b_m,$$

не входящие в систему (1).

Допустим обратное, а именно, что какая нибудь буква a_i подстановкою T_1 превращается в букву a_k той же системы (1); тогда, преобразовывая при помощи подстановки T_1 транспозицию (a_1, a_i), должны получить

$$T_1^{-1}(a_1, a_i)T_1 = (b_1, a_k).$$

Итак, в группе должна заключаться транспозиция (b_1, a_k), что как мы видели, невозможно.

Если системами (1) и

$$b_1,\ b_2,\ \ldots,\ b_m \tag{2}$$

не исчерпывается совокупность переставляемых букв, то должна существовать подстановка T_2, переводящая букву a_1 в букву c_1, не заключающуюся в системах

(1) и (2). Нетрудно видеть, что вся система букв (1) переходить через подстановку T_2 в новую систему

$$c_1,\ c_2,\ \ldots,\ c_m. \tag{3}$$

Мы видим, что система (3) не может иметь букв, общих с системой (1).

Покажем теперь, что система (3) не заключаешь также элементов системы (2). Допустим, что подстановка T_2 переводить некоторую букву, например a_2 системы (1) в некоторую букву b_i; системы (2); тогда в группе должна заключаться транспозиция

$$T_2^{-1}(a_1, a_2)T_2 = (c_1, b_i).$$

Преобразуем теперь полученную транспозицию при помощи подстановки T_1^{-1}; получаем

$$T_1T_2^{-1}(a_1, a_2)T_2T_1^{-1} = T_1(c_1, b_i)T_1^{-1}.$$

Подстановка T_1^{-1}, обратная подстановке T_1, переводить буквы системы (2) в буквы системы (1); следовательно, буква b_i заменяется некоторою a_k. Пусть подстановка T_1^{-1} переводит букву c_1 в некоторую α, которая наверно не принадлежишь системе (1); тогда в нашей группе должна существовать транспозиция

$$T_1(c_1, b_i)T_1^{-1} = (\alpha, a_k),$$

что невозможно.

Итак, мы видим, что группа импримитивна, если только не обращается в симметрическую.

Если число n букв простое, то группа не можешь быть импримитивною, и, следовательно, в этом случае транзитивная группа, заключающая одну перестановку двух букв, должна быть симметрическою.

Я должен предупредить на этом месте русских читателей, что в книге H. Weber, Lehrbuch der Algebra. Kleine Ausgabe in einem Bande 1912. S. 215 доказательство последней теоремы совершенно ошибочно. Там говорится, что, если в группу входят транспозиции $(a_1, a_2), (a_1, a_3), \ldots, (a_1, a_m)$, то в нее должна входить вся симметрическая группа Σ_m, элементов $a_1, a_2, \ldots, a_m$. Это, конечно, верно, но дальнейшее заявление, что группа Σ_m, есть нормальный делитель заданной, представляет грубый просмотр, ибо заданная группа транзитивна, а, значить, заключает подстановку S, переводящую a_1 в a_{m+1}. Преобразуя при помощи S подстановки группы Σ_m, введем новую букву a_{m+1}, которой в этих подстановках раньше не было и, следовательно, Σ_m после преобразования переходит в другую группу.

§ 40

Теорема. *Если транзитивная группа заключает тройной цикл, то она или делится на знакопеременную группу, или импримитивна.*

Пусть группа заключаешь цикл (a_1, a_2, a_3).

Рассмотрим случай более общий, когда в группу входишь ряд циклов

$$(a_1, a_2, a_3),\ (a_1, a_2, a_4),\ \ldots,\ (a_1, a_2, a_m), \quad \text{где} \quad m \geq 3.!$$

Если $m = n$, то по теореме § 36 мы замечаем. что группа должна делиться на знакопеременную.

Предположим, что $m < n$. По указанной теореме рассматриваемая группа должна заключать знакопеременную группу из элементов

$$a_1,\ a_2,\ \ldots,\ a_m. \tag{1}$$

Покажем теперь, что в группе не должно заключаться ни одного цикла, связывающего одну из букв ряда (1) с новыми буквами

$$a_{m+1},\ a_{m+2},\ \ldots$$

В самом деле, предположим обратное, а именно, что существует в группе тройной цикл

$$(a_1, a_{m+1}, a_{m+2}). \tag{2}$$

Так как группа заключает все подстановки знакопеременной группы из букв (1), то, следовательно, в группе заключается тройной цикл, переводящую букву a_1 в любую букву a_k ряда (1). Преобразуя цикл (2) при помощи этого последнего цикла, мы замечаем, что в группе должен заключаться цикл

$$(a_k, a_{m+1}, a_{m+2}),$$

т. е. другими словами, все циклы

$$(a_{m+1}, a_{m+2}, a_1),\ (a_{m+1}, a_{m+2}, a_2),\ \ldots,\ (a_{m+1}, a_{m+2}, a_m),$$

т. е. в группе заключается знакопеременная группа букв

$$a_1,\ \ldots,\ a_{m+2},$$

а, следовательно, и циклы (a_1, a_2, a_{m+1}), (a_1, a_2, a_{m+2}), что противоречит предположению, что m наибольший значок, с которым цикл (a_1, a_2, a_m) входит в группу. Подобным же образом мы придем к противоречию, если допустим, что в группу входит цикл (a_i, a_k, a_{m+1}), где a_i и a_k суть два элемента из ряда (1).

В самом деле, преобразуя последний цикл при помощи (a_i, a_k, a_1), получим цикл

$$(a_k, a_1, a_{m+1}).$$

Преобразовывая далее при помощи цикла

$$(a_k, a_1, a_2),$$

приходим к циклу

$$(a_1, a_2, a_{m+1}),$$

существование которого в группе противоречит предположению.

Итак, группа, если она не делится на знакопеременную, должна быть импримитивною, ибо все ее подстановки должны или заменять буквы системы (1) новыми буквами, или же заменять другим расположением букв той же системы.

Допустив обратное, а именно предположив, что существует подстановка, заменяющая некоторые буквы системы (1) буквами той же системы, а другие буквы

этой системы новыми, мы придем к противоречию, ибо, взяв тройной цикл, элементы которого принадлежать к буквам системы (1), взятым из обеих указанных категорий, мы получили бы, преобразовывал этот цикл при помощи рассматриваемой подстановки, тройной цикл, связывающий буквы системы (1) с новыми, что невозможно. Следовательно, группа импримитивна.

§ 41

В теории алгебраического решения уравнений представляет большую важность рассмотрение групп подстановок возможно высоких порядков, другими словами, групп с возможно малыми индексами.

Мы видели уже в § 2, что знакопеременная группа есть единственная с наименьшим после симметрической группы индексом 2.

Далее очевидно, что подстановки, не меняющие одной из n букв, образуют интранзитивную группу, порядок которой есть

$$1 \cdot 2 \cdots (n-1),$$

а индекс n.

Ruffini, рассматривая главным образом уравнения пятой степени, пришел к заключению, что в случае пяти букв индекс группы, если он больше двух, то не меньше пяти.

Cauchy обобщил этот результат и показал, что *индекс группы подстановок не может быть в одно и то же время большие* 2 *и меньше наибольшего из простых чисел, не превосходящих* n.

Таким образом, в случае n *простого* получается теорема, что *индекс группы не может заключаться между числами* 2 *и* n.

Обращаясь к случаю n составного, Cauchy показал, что для случая $n = 6$ индекс не может заключаться между числами 2 и 6.

Наконец, Bertrand'у удалось доказать окончательно следующую теорему.

Теорема Bertrand'a: *При* $n > 4$ *индекс группы не может заключаться между числами* 2 *и* n.

Теорема Bertrand'a получила известность, кроме своего значения в алгебре, еще по тем серьезным затруднениям, которые она встретила при своем доказательстве. Так например, автор ее принужден был ввести для ее доказательства в рассмотрение, как постулат, такое предложение теории чисел:

Если $n > 7$, *то существует по крайней мере одно простое число между* $\frac{n}{2}$ *и* $n - 2$.

Постулат этот был лишь впоследствии вполне строго доказан Чебышевым.

Кроме приведенной теоремы, укажем еще одну теорему, замеченную Bertrand'ом.

Теорема: *При* $n > 9$ *индекс группы, если он больше числа* n, *то не меньшие* $2n$.

В 1849 году Serret представил Парижской Академш Наук мемуар, в котором освободил доказательство теоремы Bertrand'a от вышеуказанного постулата и привел ряд представляющих интерес новых предложений. Укажем здесь некоторые.

I. *Если индекс группы равен числу* n *переставляемых буква, то группа состоит из подстановок* $n - 1$ *букв. Единственное исключение представляет случай* $n = 6$.

II. *Если индекс группы n букв больше $2n$, то он не меньше $\frac{n(n-1)}{2}$, если $n > 12$.*

С усовершенствованием теории групп доказательство теоремы Bertrand'a было упрощено. Мы приведем здесь доказательство, помещенное в сочинении Weber'a: «Lehrbuch der Algebra» (Grenzen des Index eines Theilers der symmetrischen Permutations Gruppe. Band II, § 86, Seite 143. Zweite Auflage), исправив лишь несущественный промах[6], допущенный знаменитым автором.

Разобьем доказательство теоремы на три части.

Теорема I. *Если $n > 4$, то индекс импримитивного делителя симметрической группы больше n.*

Пусть Q будет импримитивный делитель симметрической группы P с индексом j, и пусть все буквы распадаются на r систем импримитивности по s букв в каждой, так что $n = rs$.

Легко получить число, не меньшее порядка группы Q, если пересчитать всевозможный подстановки, образованные перемещением букв в каждой из r систем, а также перемещением самих систем. Число таких подстановок, очевидно, равно

$$[\Pi(s)]^r \Pi(r). \tag{1}$$

Мы видим, следовательно, что если мы разделим порядок симметрической группы на число (1), то получим число, не большее индекса j, т. е.

$$j \geq \frac{\Pi(n)}{[\Pi(s)]^r \Pi(r)}.$$

Покажем, что при $n > 4$ это число больше n. Оба числа s и r мы предполагаем, конечно, большими единицы, причем одно из этих чисел должно быть больше 2. Предполагая $s > 2$, получим

$$\frac{\Pi(n)}{[\Pi(s)]^r \Pi(r)} = \frac{(r+1)(r+2)\cdots n}{(2\cdot 3\cdots s)^r} = \tag{2}$$

$$= \frac{n}{2}\left(\frac{r+1}{2}\frac{r+2}{2}\cdots\frac{2r-1}{2}\right)\left(\frac{2r}{3}\frac{2r+1}{3}\cdots\frac{3r-1}{3}\right)\cdots\left(\frac{(s-1)r}{s}\frac{(s-1)r+1}{s}\cdots\frac{n-1}{s}\right).$$

Отсюда

$$j > \frac{n}{2}\left(\frac{r+1}{2}\right)^{r-1}\left(\frac{2r}{3}\right)^r\cdots\left(\frac{(s-1)r}{s}\right)^r.$$

Все множители

$$\frac{r+1}{2},\ \frac{2r}{3},\ \cdots,\ \frac{(s-1)r}{s}$$

больше единицы.

В самом деле

$$\frac{r+1}{2} > 1$$

[6]См. статью Д. Граве: О теореме Bertrand'a (Университетские Известия (Киев, 1901 г.), или отдельный оттиск оттуда; также: Протоколы Физико-Математического Общества при Императорском Университете Св. Владимира за тот же год).

ибо $r > 1$, а вычитая единицу из каждого следующего числа $\dfrac{(h-1)r}{h}$, получим число

$$\frac{(h-1)r}{h} - 1 = \frac{(h-1)r - h + 1 - 1}{h} = \frac{(h-1)(r-1) - 1}{h}$$

положительное, так как

$$r > 1, \qquad h > 2.$$

При $r > 2$ имеем:

$$\left(\frac{r+1}{2}\right)^{r-1} > 2$$

и, следовательно,

$$j > \frac{n}{2}\left(\frac{r+1}{2}\right)^{r-1} > \frac{n}{2} \cdot 2,$$

т. е. $j > n$.

Если $r = 2$, то

$$\left(\frac{r+1}{2}\right)^{r-1}\left(\frac{2r}{3}\right)^{r} = \frac{3}{2}\left(\frac{4}{3}\right)^{2} = \frac{8}{3} > 2.$$

Следовательно, также выходить, что $j > n$.

Если $s = 2$, а $r > 2$, то тогда

$$j \geq \frac{n}{2}\left(\frac{r+1}{2}\frac{r+2}{2}\cdots\frac{2r-1}{2}\right).$$

Следовательно, можно взять два первых множителя: таким образом получаем

$$j > \frac{n(r+1)}{4},$$

т. е. $j > n$.

Случай $n = 4$, $r = 2$, $s = 2$ дает исключение, именно,

$$\frac{\Pi(n)}{[\Pi(s)]^r \Pi(r)} = \frac{1 \cdot 2 \cdot 3 \cdot 4}{(1 \cdot 2)^2 \cdot 1 \cdot 2} = 3.$$

В самом деле, группа, указанная в пункте c) § 26, есть как раз импримитивная группа четырех букв восьмого порядка, имеющая, следовательно, индекс 3. Эта группа, очевидно, импримитивная, с системами импримитивности

$$\begin{matrix} 1, & 2 \\ 3, & 4. \end{matrix}$$

Теорема II. *Индекс интранзитивного делителя симметрической группы равен или больше n, причем он равен n, когда делитель не перемещает одной буквы и состоит из всех подстановок, остальных $n-1$ букв.*

Если группа Q интранзитивна, то можно разбить все буквы на две системы, одну из a букв, другую из b букв, так что

$$a + b = n,$$

притом таких, что буквы одной системы не могут быть подстановками группы Q заменены буквами другой. Ясно, что все подстановки группы Q должны заключаться между подстановками, перемещающими отдельно буквы этих систем. Следовательно, порядок Q не может превосходить числа

$$\Pi(a)\Pi(b).$$

Значит,

$$j \geq \frac{\Pi(n)}{\Pi(a)\Pi(b)} = \frac{n}{1} \cdot \frac{n-1}{2} \cdots \frac{b+1}{a}.$$

Индекс j может равняться n только в случае $a = 1$, что очевидно.

Если оба числа a и b отличны от единицы, то, предполагая $b \geq a$, заметим, что все числа

$$\frac{n-1}{2},\ \frac{n-2}{3},\ \ldots,\ \frac{b+1}{a}$$

больше единицы, и, следовательно. получаем:

$$j > n.$$

Теорема III. *Если $a = 1$, так что группа Q не перемещает одну букву, то ее порядок есть делитель числа $\Pi(n-1)$. Если же $a > 1$, то порядок Q равен или меньше $\Pi(n-2)\Pi(n)$.*

Первая часть теоремы очевидна из того соображения, что всякая группа, перемещающая $n-1$ букв, должна быть делителем симметрической группы этих букв.

Вторая же часть теоремы следует из того, что биномиальные коэффициенты возрастают по мере приближении к среднему члену разложения и, следовательно,

$$\frac{\Pi(n)}{\Pi(a)\Pi(b)} \geq \frac{\Pi(n)}{\Pi(n-2)\Pi(2)},$$

что дает неравенство

$$j \geq \frac{\Pi(n)}{\Pi(n-2)\Pi(2)},$$

или, окончательно,

$$\frac{\Pi(n)}{j} \geq \Pi(n-2)\Pi(n),$$

что и требовалось доказать.

Теорема IV. *Кроме знакопеременной группы, не существует транзитивного и примитивного делителя Q симметрической группы, индекс которого не больше n. Единственное исключите представляет случай $n = 6$.*

Пусть будет Q примитивный и транзитивный делитель индекса j симметрической группы цифр

$$0,\ 1,\ 2,\ \ldots,\ n-1,$$

предполагая $j > 2$.

На оснований сказанного в § 28, можно симметрическую группу разбить на j сопряженных систем

$$Q,\ QT_1,\ QT_2,\ \ldots,\ QT_{j-1}, \tag{3}$$

причем знаком QT_i мы обозначаем совокупность подстановок, получающихся от умножения подстановок группы Q справа на T_i.

Если группа Q примитивная и транзитивная, то она не може заключать ни одной транспозиции (см. § 39)

$$(0,1),\ (0,2),\ \ldots,\ (0,n-1). \tag{4}$$

Если $j < n$, то по крайней мере две транспозиции, например $(0,1)$ и $(0,2)$, должны входить в одну из систем (3), например в систему QT_1. Значить, в группе Q должны быть две подстановки S_1, S_2, дающие $S_1T_1 = (0,1)$ и $S_2T_1 = (0,2)$.

Отсюда получаем

$$S_1T_1T_1^{-1}S_2^{-1} = (0,1)(0,2),$$

или, иначе,

$$S_1S_2^{-1} = (0,1,2).$$

Итак, группа Q должна заключать тройной цикл, что невозможно, если она не заключает знакопеременной группы (см. § 40).

Рассмотрим теперь случай $j = n$ и покажем, что он невозможен для всякого n, кроме $n = 6$.

При $j = n$ порядок группы Q, если она существует, должен быть

$$\Pi(n-1).$$

Тогда $n-1$ транспозиции (4) должны входить по одной в различные системы

$$QT_1,\ QT_2,\ QT_3,\ \ldots,\ QT_{n-1}$$

и симметрическую группу можно представить, как совокупность систем

$$Q,\ Q(0,1),\ Q(0,2),\ \ldots,\ Q(0,n-1),$$

ибо за подстановки

$$T_1,\ T_2,\ldots,\ T_{n-1}$$

можно будет принять транспозиции (4).

Рассмотрим теперь какую нибудь новую транспозицию, например $(2,3)$. Эта транспозиция, очевидно, не может входить в системы

$$Q(0,2),\quad Q(0,3),$$

ибо в обратном случай группа Q заключала бы тройные циклы

$$(0,2)(2,3),\quad (0,3)(2,3).$$

Не нарушая общности, можно предположить, что транспозиция $(2,3)$ входить в систему $Q(0,1)$, а значить в группу Q входит подстановка

$$(0,1)(2,3).$$

Рассмотрим делитель Q_0 группы Q, образованного подстановками, не перемещающими цифры 0.

Так как группа Q транзитивна, то в ней заключаются подстановки

$$S_1,\ S_2,\ \ldots,\ S_{n-1},$$

заменяющие цифру 0 последовательно цифрами

$$1,\ 2,3,\ \ldots,\ n-1.$$

Нетрудно видеть, что группа Q должна состоять из следующей системы

$$Q_0,\ Q_0S_1,\ Q_0S_2,\ \ldots,\ Q_0S_{n-1}.$$

Итак, порядок g группы Q_0 получается от деления на n порядка Q , т. е.

$$g = \frac{\Pi(n-1)}{n}.$$

Так как порядок всякой группы есть целое число, то должно делиться на n произведение $\Pi(n-1)$, а потому мы придем к противоречию в случае, когда n число простое или равно 4.

Итак, мы должны предполагать n не меньше 6. Покажем, что группа Q_0 должна быть транзитивною относительно цифр

$$1,\ 2,\ \ldots,\ n-1.$$

В самом деле, допустим обратное, т. е., что группа Q_0 интранзитивная, мы получим одно из двух (см. теорему III): или $\Pi(n-2)$ делится на g, или

$$\Pi(n-3)\Pi(2) \geq g.$$

Отсюда получаем, что или должно равняться целому числу число

$$\frac{\Pi(n-2)}{\frac{\Pi(n-1)}{n}} = \frac{n}{n-1},$$

или же

$$n^2 - 5n + 2 \leq 0.$$

При $n > 5$ оба предположения невозможны.

Итак, группа Q_0 должна быть транзитивною относительно сказанных букв.

Рассмотрим делитель $Q_{0,1}$ группы Q, не перемещающего двух цифр

$$0,\quad 1.$$

Так как Q_0, рассматриваемая, как группа от $n-1$ цифр, есть транзитивный делитель Q, то, применяя рассуждения, подобные приведенным выше, получаем. что порядок g_1 делителя $Q_{0,1}$ равен $\dfrac{g}{n-1}$, т. е.

$$g_1 = \frac{\Pi(n-2)}{n}.$$

Покажем, что группа $Q_{0,1}$ транзитивная относительно букв

$$2,\ 3,\ \ldots,\ n-1.$$

Если бы это было не так, то имело бы место одно из двух: или $\Pi(n-3)$ делится на g_1, или же

$$g_1 \leq \Pi(n-4)\Pi(2).$$

Первое предположение невозможно при $n > 4$; второе же неравенство дает

$$n^2 - 7n + 6 \leq 0,$$

что невозможно при $n > 6$.

В случае $n = 6$ противоречие отсутствует.

Рассмотрим теперь делитель $Q_{0,1,2}$ группы Q, который не перемещает трех элементов

$$0,\ 1,\ 2.$$

Его порядок есть

$$g_2 = \frac{\Pi(n-3)}{n}.$$

При $n = 6$

$$g_2 = \frac{1 \cdot 2 \cdot 3}{6} = 1$$

и группа $Q_{0,1,2}$ сводится к тождественной подстановке.

Оставляя пока в стороне случай $n = 6$ и предполагая, следовательно, $n > 6$, заметим, что $Q_{0,1,2}$ не может не перемещать какой нибудь четвертый элемент, например 3; если бы это было так, то его порядок должен был бы делить число

$$\Pi(n-4),$$

т. е. должно было бы быть целым число

$$\frac{n\Pi(n-4)}{\Pi(n-3)}.$$

Другими словами,

$$\frac{n}{n-3} \geq 2, \qquad n \leq 6,$$

что противоречить предположению.

Итак, мы видим, что при $n > 6$ в группу Q должна входить подстановка S, переводящая элементы $0, 1, 2, 3$ в элементы $0, 1, 2, 4$, где 4 есть отличный от 3 элемент. Группа Q, как мы видели, имеет подстановку $(0,1)(2,3)$; следовательно, она должна будет также заключать подстановку

$$S^{-1}(0,1)(2,3)S = (0,1)(2,4),$$

а потому в группе Q должна заключаться следующая подстановка

$$(0,1)(2,3)(0,1)(2,4) = (2,3,4),$$

что невозможно.

Итак, теорема наша доказана для всех случаев, кроме $n = 6$.

Нетрудно убедиться, что при $n = 6$ теорема несправедлива, и что *существует примитивный и транзитивный делитель симметрической группы шести элементов, имеющий индекс* 6 *и порядок* 120.

В самом деле, этот делитель может быть образован следующим образом. Берем три основные подстановки

$$U = (0, 1, 2, 3)$$
$$V = (0, 4, 2, 3, 1)$$
$$W = (0, 4, 1, 2, 3, 5);$$

тогда подстановки вида

$$U^i V^j W^k,$$

где i, j, k всевозможный целые числа. образуют требуемую группу.

О нормальных делителях групп

§ 42

В § 19 мы видели, что подстановка

$$S_1 = T^{-1} S T$$

подобна подстановке S и получается через производство в циклах подстановки S изменения букв, указанного подстановкою T. Будем говорить, что подстановка S_1 есть *преобразование подстановки* S *при помощи* T.

§ 43

Рассмотрим группу H, состоящую из подстановок

$$I,\ S_1,\ S_2, \ldots,\ S_{\mu-1} \tag{1}$$

и пусть группа H есть делитель другой группы G порядка m, причем, очевидно,

$$m = \mu\nu,$$

где ν некоторое целое число.

Возьмем какую нибудь подстановку T группы G, не входящую в состав делителя H. Преобразуем при помощи T все подстановки (1); получаем тогда подстановки

$$I,\ T^{-1}S_1T,\ T^{-1}S_2T, \ldots,\ T^{-1}S_{\mu-1}T. \tag{2}$$

Нетрудно видеть, что *подстановки* (2) *образуют также группу*, ибо имеем равенство

$$(T^{-1}S_iT)(T^{-1}S_jT) = T^{-1}(S_iS_j)T.$$

Группу (2) мы будем называть *преобразованием группы* H *при помощи подстановки* T и обозначать для сокращения знаком

$$T^{-1}HT.$$

§ 44

Две группы одного порядка

$$I,\ S_1,\ S_2, \ldots,\ S_{m-1}$$

и

$$I,\ \Sigma_1,\ \Sigma_2, \ldots,\ \Sigma_{m-1}$$

мы будем называть *изоморфными*, если возможно таким образом сопоставить элементы одной группы элементам другой, что всякому соотношению

$$S_i S_k = S_l \tag{1}$$

подстановок одной группы соответствует подобное же соотношение

$$\Sigma_i \Sigma_k = \Sigma_l \tag{2}$$

для другой с теми же индексами

$$i,\quad k,\quad l.$$

Очевидно, что *группы* H *и* $T^{-1}HT$ предыдущего §-а *изоморфны.*

В самом деле, обозначая

$$\Sigma_i = T^{-1} S_i T,$$

мы заметим, что равенству (1) будет соответствовать равенство (2).

§ 45

Будем называть группу $T^{-1}HT$, которая есть, очевидно, также делитель группы G, *сопряженным с* H *делителем.* Выбирая за T всевозможные подстановки группы G, получим всевозможные сопряженные с H делители.

Если все сопряженные с H делители группы G совпадают с самим делителем H, то группа H называется *нормальным делителем.*[7]

§ 46

Приведем примеры нормальных делителей:

a) Нетрудно видеть, что *знакопеременная группа есть нормальный делитель симметрической.*

В самом деле, будем преобразовывать знакопеременную группу при помощи произвольной подстановки T. Так как, при преобразовании каждой подстановки S знакопеременной группы, число циклов и их порядки не меняются, то после преобразования подстановка S превращается в другую подстановку S_1, принадлежащую той же знакопеременной группе (см. § 33).

b) Рассмотрим теперь делитель H группы G, не совпадающий с сопряженными делителями

$$H_1,\quad H_2,\ \ldots \tag{1}$$

[7]Некоторые авторы называюсь нормальные делители *инвариантными подгруппами.*

Нетрудно убедиться, что *подстановки, общие всем сопряженным делителям*

$$H, \quad H_1, \quad H_2, \ \ldots$$

образуют группу R, которая будешь нормальним делителем группы G.

Возьмем произвольную подстановку T группы G; тогда в ряде групп

$$T^{-1}HT, \ T^{-1}H_1T, \ T^{-1}H_2T, \ldots \tag{2}$$

входят только группы (1).

Общие подстановки ряда групп (2), очевидно, будут образовывать группу

$$T^{-1}RT.$$

Но так как ряд (2) образован теми же самими группами (1), то должно быть

$$R = T^{-1}RT,$$

т. е. группа R есть нормальный делитель, ибо T есть произвольная подстановка группы G.

Конечно, общий делитель R, сопряженных групп (1) может приводиться к единице, которая, очевидно, является нормальным делителем всякой группы.

§ 47

Будем называть группу *простою* если она не имеет нормальных делителей, отличных от единицы и самой себя, и *составною*, если она имеет нормальные делители.

Группа простого порядка, очевидно, *простая.*

Симметрическая группа при всяком числе перемещаемых букв *составная*, ибо у нее всегда имеется в качеств нормального делителя знакопеременная группа.

§ 48

Рассмотришь симметрическую группу трех элементов

$$0, \ 1, \ 2.$$

Эта группа состоит, очевидно, из подстановок

$$I, \ (0,1), \ (0,2), \ (1,2), \ (0,1,2), \ (0,2,1)$$

и имеет нормальным делителем знакопеременную

$$I, \ (0,1,2), \ (0,2,1),$$

которая, будучи простого порядка, есть простая.

§ 49

Рассмотрим теперь симметрическую группу четырех элементов $0, 1, 2, 3$:

$$I,\ (0,1),\ (0,2),\ (0,3),\ (1,2),\ (1,3),\ (2,3)$$
$$(0,1)(2,3),\ (0,2)(1,3),\ (0,3)(1,2),$$
$$(0,1,2),\ (0,2,1),\ (0,1,3),\ (0,3,1),\ (0,2,3),\ (0,3,2),\ (1,2,3),\ (1,3,2)$$
$$(0,1,2,3),\ (0,3,2,1),\ (0,1,3,2),\ (0,2,3,1),\ (0,2,1,3),\ (0,3,1,2).$$

Знакопеременная группа состоит из двенадцати подстановок

$$I,\ (0,1)(2,3),\ (0,2)(1,3),\ (0,3)(1,2)$$
$$(0,1,2),\ (0,2,1),\ (0,1,3),\ (0,3,1),\ (0,2,3),\ (0,3,2),\ (1,2,3),\ (1,3,2).$$

Нетрудно видеть, что эта группа имеет нормальный делитель индекса 3

$$I,\ (0,1)(2,3),\ (0,2)(1,3),\ (0,3)(1,2).$$

Эта группа в свою очередь имеет нормальным делителем индекса 2 группу

$$I,\ (0,1)(2,3),$$

которая, будучи второго порядка, будет простою.

§ 50

Покажем теперь, что *при числе элементов большем четырех знакопеременная группа есть группа простая.*

Пусть Q будет нормальный делитель знакопеременной группы элементов $1, 2, 3, \ldots, n$.

Покажем прежде всего, что при $n > 4$ группа Q *не может включать* подстановки, состоящей из одиночного тройного цикла. Допустим обратное, а именно, что в группе Q есть подстановка $(1, 2, 3)$, тогда в ней будет заключаться всякий тройной цикл (abc), ибо на основании § 37 знакопеременная группа $n - 2$ раз транзитивная и, следовательно, при $n > 4$ *три* элемента 1 23 могут обратиться в *три* произвольно выбранные. Значит в знакопеременной группе существует подстановка, переводящая 1 2 3 в a b c. Пусть эта подстановка, будет

$$s = \begin{pmatrix} a & b & c & \ldots \\ 1 & 2 & 3 & \ldots \end{pmatrix}.$$

В нормальном делителе Q должна входить подстановка $s^{-1}(1, 2, 3)s = (a, b, c)$, другими словами, в Q входит произвольный тройной цикл значит, Q совпадает с самой знакопеременною группой, что противоречит предположению.

Дальнейшее доказательство несуществования при $n > 4$ нормального делителя Q знакопеременной группы может быть произведено так. Допустим обратное, а именно, что существует нормальный делитель знакопеременной группы, отличный от нее самой и единицы.

Пусть S будет одна из входящих в него подстановок, а T произвольно взятая подстановка знакопеременной группы. В группу должны будут входить обе подстановки S и $T^{-1}ST$, а, следовательно, и подстановка

$$U = S^{-1}T^{-1}ST.$$

Мы докажем невозможность существования нормально делителя Q, показав, что можно подобрать подстановки S и T таким образом, чтобы U обращалась в тройной цикл, ибо по выше доказанному группа Q не должна заключать тройных циклов.

Для сказанного подбора подстановок S и T предположим. что они разложены на циклы. Мы имеем право обращать наше внимание только на те циклы, буквы которых изменяются подстановкой T, ибо остальные циклы уничтожаются в произведение подстановок SS^{-1}.

Рассмотрим все возможные различные случаи:

1) S содержать цикл более, чем из трех элементов.

Например, $S = (1, 2, 3, 4, \ldots, m)(\ldots)(\ldots)\ldots$.

Возьмем $T = (1, 2, 3)$, тогда $S^{-1}T^{-1}ST = S^{-1}(1, 2, 3)S = (2, 4, 3)$. Значить, $U = (2, 4, 3)(1, 2, 3) = (1, 2, 4)$. Итак, приходим к противоречию, а именно, что делитель Q должен заключать тройной цикл $(1, 2, 4)$.

2) В S входят два тройных цикла, $S = (1, 2, 3)(4, 5, 6)\ldots$. Возьмем $T = (1, 3, 4)$. В этом случае $S^{-1}T^{-1}ST = S^{-1}(1, 4, 3)S = (2, 5, 1)$ и, значить, $U = (2, 5, 1)(1, 3, 4) = (1, 2, 5, 3, 4)$.

Итак, в группе Q оказывается подстановка, заключающая цикл более, чем из трех букв. Эту подстановку можно принять за S, причем тогда подучим предыдущий случай.

3) Подстановка S заключает только один тройной цикл, остальные же циклы двойные и одиночные.

Очевидно, что квадрат такой подстановки сводится к тройному циклу.

4) Циклы подстановки S только двойные и одиночные; число двойных циклов не может равняться единице, ибо в этом случае подстановка S есть нечто иное, как транспозиция двух только букв, которая не может входить в состав знакопеременной группы.

Остается рассмотреть при $n > 4$ два случая.

α) В S входят только двойные циклы, число которых, следовательно, больше двух

$$S = (1, 2)(3, 4)(5, 6)\ldots$$

Возьмем $T = (1, 3, 5)$. Получаем $S^{-1}T^{-1}ST = S^{-1}(1, 5, 3)S = (2, 6, 4),$, откуда $U = (2, 6, 4)(1, 3, 5)$ и, следовательно, приходим к случаю 2).

β) В S входит по крайней мере один одиночный цикл

$$(1, 2)(3, 4)(5)\ldots$$

Возьмем $T = (1, 2, 5)$. Получаем $S^{-1}T^{-1}ST = S^{-1}(1, 5, 2)S = (2, 5, 1)$. Откуда $U = (2, 5, 1)(1, 2, 5) = (1, 2, 5)^2 = (1, 5, 2)$, что невозможно.

Итак, при $n > 4$ мы исчерпали все случаи, и все они приводят к противоречию; следовательно, высказанная теорема справедлива.

Случай $n = 4$ представляет исключение, ибо тогда возможна комбинация для подстановки S, состоящая из двух транспозиций. В этом случае существует нормальный делитель

$$I,\ (1,2)(3,4),\ (1,3)(2,4),\ (1,4)(2,3).$$

§ 51

Покажем теперь, что *при $n > 4$ симметрическая группа не имеет отличного от знакопеременной нормального делителя.*

Пусть P будет симметрическая группа, а Q знакопеременная группа. Допустим, что симметрическая группа имеет нормальиый делитель R, отличный от Q. Нетрудно убедиться, что общий наибольшей делитель групп R и Q не может быть отличен от единицы.

Допустим, что этот общий делитель W (образующий, очевидно, группу) отличен от единицы, тогда он должен быть нормальным делителем знакопеременной группы Q, что невозможно при $n > 4$. В самом деле, любая подстановка S группы W от преобразования любой подстановкой группы P обращается в подстановку, с одной стороны, принадлежащую к группе Q, ибо Q нормальный делитель P, с другой стороны, обращается в подстановку группы R, ибо R также нормальный делитель. Другими словами, подстановка S переходить в подстановку из того же общего делителя. Итак W будет нормальным делителем как для P, так и для Q.

Итак, нормальный делитель R симметрической группы, отличный от знакопеременной, может иметь с нею общею подстановкой только единицу; следовательно, все другие его подстановки принадлежать ко второму роду (см. § 22).

Возьмем две какие нибудь подстановки S_1 и S_2 группы R, отличные от единицы. Тогда две подстановки S_1^2 и S_1S_2, с одной стороны, должны входить в группу R, с другой стороны, будучи подстановками первого рода, обе они должны обращаться в единицу и, следовательно, получается равенство $S_1^2 = S_1S_2$ или $S_1 = S_2$.

Другими словами, все остальные подстановки группы R должны быть равны между собой; следовательно, группа R должна быть второго порядка и, кроме единицы, должна заключать только одну подстановку S. Так как по предположений группа R нормальный делитель симметрической группы, то от преобразования всякой подстановкой T подстановка S не должна меняться, что невозможно.

В самом деле, подстановка S, будучи второго порядка, должна разлагаться на циклы второго порядка, из которых один пусть будет $(1, 2)$. Если число букв больше двух, то существует подстановка, преобразующая цикл $(1, 2)$ в новый $(1, 3)$ и, следовательно, преобразованная подстановка не может равняться первоначальной.

Связь подстановок с общей теорией групп

§ 52

Обратимся к рассмотрений некоторой абстрактной группы ? порядка ?, образованной элементами

$$I,\ A_0,\ A_1,\ A_2, \ldots,\ A_n. \tag{1}$$

Рассмотрим совокупность PA_i. Эта совокупность, как известно, тождественна с самой группой и может отличаться от нее только порядком расположения элементов. Рассмотрим подстановку n букв A с различными индексами

$$\begin{pmatrix} A_i & A_1A_i & A_2A_i & \dots & A_{n-1}A_i \\ A_0 & A_1 & A_2 & \dots & A_{n-1} \end{pmatrix},$$

дающую новое перемещение элементов (1). Будем эту подстановку обозначать для кратности знаком

$$\begin{pmatrix} PA_i \\ P \end{pmatrix}.$$

Подстановки

$$I,\ \begin{pmatrix} PA_1 \\ P \end{pmatrix},\ \begin{pmatrix} PA_2 \\ P \end{pmatrix},\ \dots,\ \begin{pmatrix} PA_{n-1} \\ P \end{pmatrix} \tag{2}$$

образуют, очевидно, группу, ибо

$$\begin{pmatrix} PA_i \\ P \end{pmatrix}\begin{pmatrix} PA_k \\ P \end{pmatrix} = \begin{pmatrix} PA_i \\ P \end{pmatrix}\begin{pmatrix} PA_iPA_k \\ PA_i \end{pmatrix} = \begin{pmatrix} PA_iA_k \\ P \end{pmatrix}.$$

Из сопоставления крайних частей последнего равенства следует, что группа подстановок (2) однозначно изоморфна с группой элементов (1). Получаем таким образом теорему.

Всякая абстрактная группа порядка n однозначно изоморфна с некоторой транзитивной группой подстановок n.

Транзитивность группы (2) следует из того соображения, что всегда можно указать такой элемента A_i, при котором произведение A_kA_i обратится в новый элемент A_i.

Весьма важным является вопрос о нахождении для группы данного порядка изоморфной транзитивной группы подстановок возможно меньшего числа букв.

§ 53

Очевидно, что всякую группу подстановок можно рассматривать, как некоторое линейное преобразование. Например подстановку

$$(x_1, x_3, x_2)(x_4, x_5)$$

можно рассматривать как линейное преобразование букв x_1, x_2, x_3, x_4, x_5 в такая новые $x'_1, x'_2, x'_3, x'_4, x'_5$, причем существует преобразование

$$\begin{aligned} x'_1 &= \dots x_3 \dots \\ x'_2 &= x_1 \dots\dots \\ x'_3 &= \dots x_2 \dots \\ x'_4 &= \dots\dots x_5 \\ x'_5 &= \dots x_4 \dots \end{aligned}$$

с матрицей

$$\left\|\begin{matrix}0&0&1&0&0\\1&0&0&0&0\\0&1&0&0&0\\0&0&0&0&1\\0&0&0&1&0\end{matrix}\right\|.$$

Определитель матрицы подобного преобразования всегда равен ± 1.

§ 54

Уравнение

$$\begin{vmatrix} a_1{}^{(1)}-x & a_2{}^{(1)} & \dots & a_n{}^{(1)} \\ a_1{}^{(2)} & a_2{}^{(2)}-x & \dots & a_n{}^{(2)} \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ a_1{}^{(n)} & a_2{}^{(n)} & \dots & a_n{}^{(n)}-x \end{vmatrix} = 0$$

получающееся от вычисления неизвестного x из всех элементов главной диагонали определителя матрицы $\|a_i{}^{(k)}$ носить название *характеристического* уравнения[8] матрицы $\|a_i{}^{(k)}$.

Нетрудно убедиться, что, если мы представим подстановку S в циклах

$$S = C_1{}^{(k_1)} C_2{}^{(k_2)} \cdots C_e{}^{(k_e)},$$

где верхний значок k указывает порядок цикла $C_i{}^{(k_i)}$?, то характеристическое уравнение соответствующей матрицы будет иметь вид

$$(x^{k_1}-1)(x^{k_2}-1)\cdots(x^{k_e}-1)=0.$$

Например, для матрицы § 53 получаем

$$\begin{vmatrix} -x & 0 & 1 & 0 & 0 \\ 1 & -x & 0 & 0 & 0 \\ 0 & 1 & -x & 0 & 0 \\ 0 & 0 & 0 & -x & 1 \\ 0 & 0 & 0 & 1 & -x \end{vmatrix} =$$

$$= \begin{vmatrix} -x & 0 & 1 \\ 1 & -x & 0 \\ 0 & 1 & -x \end{vmatrix} \cdot \begin{vmatrix} -x & 1 \\ 1 & x \end{vmatrix} = -(x^3-1)(x^2-1).$$

[8] См. Д. Граве. Элементарный курс теории чисел. Киев. 1913. Глава XIII, § 2

Глава VI

Основы исчисления инвариантов

Геометрические инварианты

§ 1

Теория инвариантов есть та часть алгебры, которая развилась под непосредственным влиянием геометрии, а потому мы придадим нашему изложению также геометрический характер.

§ 2

Рассмотрим в трехмерном пространстве движение некоторой неизменяемой фигуры. Как известно из аналитической геометрии, это движение можно указать, как преобразование прямоугольных координат

$$\begin{aligned} x' &= a + \alpha x + \beta y + \gamma z \\ y' &= b + \alpha_1 x + \beta_1 y + \gamma_1 z \\ z' &= c + \alpha_2 x + \beta_2 y + \gamma_2 z, \end{aligned} \tag{1}$$

где a, b, c суть координаты нового начала, а девять косинусов α, β, γ, α_1, β_1, γ_1, α_2, β_2, γ_2 связаны шестью соотношениями

$$\begin{aligned} &\alpha^2 + \alpha_1^2 + \alpha_2^2 = 1, \quad \alpha\beta + \alpha_1\beta_1 + \alpha_2\beta_2 = 0, \\ &\beta^2 + \beta_1^2 + \beta_2^2 = 1, \quad \alpha\gamma + \alpha_1\gamma_1 + \alpha_2\gamma_2 = 0, \\ &\gamma^2 + \gamma_1^2 + \gamma_2^2 = 1, \quad \beta\gamma + \beta_1\gamma_1 + \beta_2\gamma_2 = 0, \end{aligned} \qquad \begin{vmatrix} \alpha & \beta & \gamma \\ \alpha_1 & \beta_1 & \gamma_1 \\ \alpha_2 & \beta_2 & \gamma_2 \end{vmatrix} = 1. \tag{2}$$

Движения в пространстве, очевидно, образуют бесконечную группу, если под композицией движений мы будем понимать выполнение этих движений одного за другим в известном порядке. Единицей этой группы будет покой, т. е. отсутствие движения. Обратным элементом явится обратное движение, переводящее фигуру из ее конечного положения в первоначальное.

§ 3

Существует ряд свойств фигур, не изменяющихся при движении; эти свойства можно назвать *инвариантами* группы движений.

К числу инвариантов движения принадлежать, так например, два основных: расстояние каждых двух точек движущейся фигуры и угол между двумя прямыми.

Если свойство неизменности указанных *геометрических инвариантов* перевести на язык алгебры, то мы получим *алгебраические инварианты*, т. е. формулы, не меняющиеся при преобразованиях вида (1) § 2.

Формулы (1) § (2) преобразуют координаты (x, y, z) в (x', y', z'). Если мы рассмотрим другую точку (x_0, y_0, z_0), переходящую от движения в точку (x_0', y_0', z_0'), то на основании (1) § 2 получим

$$\begin{aligned} x' - x_0' &= \alpha(x - x_0) + \beta(y - y_0) + \gamma(z - z_0) \\ y' - y_0' &= \alpha_1(x - x_0) + \beta_1(y - y_0) + \gamma_1(z - z_0) \\ z' - z_0' &= \alpha_2(x - x_0) + \beta_2(y - y_0) + \gamma_2(z - z_0); \end{aligned}$$

возвышая в квадрат и складывая, будем иметь

$$(x' - x_0')^2 + (y' - y_0')^2 + (z' - z_0')^2 = (x - x_0)^2 + (y - y_0)^2 + (z - z_0)^2,$$

что показывает, что формула

$$+\sqrt{(x - x_0)^2 + (y - y_0)^2 + (z - z_0)^2},$$

выражающая расстояние двух точек, есть инвариант.

Возьмем две прямых линии в пространстве

$$(1) \qquad \frac{x - \xi}{l} = \frac{y - \eta}{m} = \frac{z - \zeta}{n}; \qquad \frac{x - \xi_1}{l_1} = \frac{y - \eta_1}{m_1} = \frac{z - \zeta_1}{n_1};$$

косинус угла между ними выражается по формуле

$$(2) \qquad \frac{ll_1 + mm_1 + nn_1}{\sqrt{l^2 + m^2 + n^2}\ \sqrt{l_1^2 + m_1^2 + n_1^2}};$$

легко проверить, что эта формула есть действительно инвариант преобразования (1) § 2.

От преобразования прямые (1) переходят в такие

$$\frac{x' - \xi'}{l'} = \frac{y' - \eta'}{m'} = \frac{z' - \zeta'}{n'}; \qquad \frac{x' - \xi_1'}{l_1'} = \frac{y' - \eta_1'}{m_1'} = \frac{z' - \zeta_1'}{n_1'},$$

где новые угловые коэффициенты связаны с первоначальными при помощи равенств

$$\begin{aligned} \rho l' &= \alpha l + \beta m + \gamma n, \quad \rho_1 l_1' = \alpha l_1 + \beta m_1 + \gamma n_1 \\ \rho m' &= \alpha_1 l + \beta_1 m + \gamma_1 n, \quad \rho_1 m_1' = \alpha_1 l_1 + \beta_1 m_1 + \gamma_1 n_1 \\ \rho n' &= \alpha_2 l + \beta_2 m + \gamma_2 n, \quad \rho_1 n_1' = \alpha_2 l_1 + \beta_2 m_1 + \gamma_2 n_1 \end{aligned}$$

где ρ и ρ_1 произвольные множители.

После простых преобразований, принимая во внимание формулы (2) § 2, получим

$$\begin{aligned} \rho\rho_1(l'l_1' + m'm_1' + nn_1') &= ll_1 + mm_1 + nn_1 \\ \rho\sqrt{l'^2 + m'^2 + n'^2} &= \sqrt{l^2 + m^2 + n^2} \\ \rho_1\sqrt{l_1'^2 + m_1'^2 + n_1'^2} &= \sqrt{l'^2 + m'^2 + n'^2}, \end{aligned}$$

откуда окончательно

$$\frac{l'l'_1+m'm'_1+n'n'_1}{\sqrt{l'^2+m'^2+n'^2}\,\sqrt{l'^2_1+m'^2_1+n'^2_1}}=\frac{ll_1+mm_1+nn_1}{\sqrt{l^2+m^2+n^2}\,\sqrt{l^2_1+m^2_1+n^2_1}}.$$

Итак, мы видим, что формула (2) есть инвариант.

§ 4

Рассмотрим теперь общее проективное преобразование однородных координат трехмерного пространства[9]

$$(1)\qquad \begin{aligned} x' &= ax+by+cz+du\\ y' &= a_1x+b_1y+c_1z+d_1u\\ y' &= a_2x+b_2y+c_2z+d_2u\\ u' &= a_3x+b_3y+c_3z+d_3u \end{aligned}$$

с неравным нулю определителем

$$\varepsilon=\begin{vmatrix} a & b & c & d\\ a_1 & b_1 & c & d_1\\ a_2 & b_2 & c_2 & d_2\\ a_3 & b_3 & c_3 & d_3 \end{vmatrix},$$

который мы будем называть *модулем* преобразования.

Линейное преобразовало (1) мы будем называть *особенным*, если определитель ε равен нулю и *неособенным* в обратном случае.

Очевидно, что неособенные проективные преобразования образуют группу, ибо последовательное применение двух преобразований равносильно одному также проективному преобразований, как это мы видели в § 20 Главы IV. Единицей группы является тождественное преобразование

$$x'=x,\quad y'=y,\quad z'=z,\quad u'=u,$$

имеющее матрицу

$$\begin{vmatrix} 1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1 \end{vmatrix}.$$

Обратным элементом группы является преобразование новых переменных x', y', z', u' в первоначальные x, y, z, u. Это преобразование получается через решение четырех уравнений (1) относительно четырех неизвестных x, y, z, u.

Назовем проективным такое свойство фигур, которое не нарушается при проективном преобразовании.

К числу таких проективных свойств принадлежат например: нахождение трех точек на одной прямой, прохождение четырех плоскостей через одну точку, касание двух кривых, или кривой с поверхностью, или двух поверхностей и т. д.

[9]См. Д. Граве. Основы аналитической геометрии. Часть II, геометрия в пространстве. 1913 (литография).

Из курса аналитической геометрии известен один весьма важный алгебраический инвариант проективного преобразования, а именно, так называемое *ангармоническое* отношение.

§ 5

Сказанное в двух предыдущих параграфах можно заключить в следующем общем определении.

Рассматривается группа G преобразований геометрических образов в пространстве n измерений, причем под композицией двух преобразований разумеется последовательное осуществление их одного за другими.

Всякая величина, связанная с рассматриваемыми геометрическими образами, не изменяющаяся от преобразований группы G, носит название инварианта группы G.

Относительные инварианты

§ 6

Данное нами выше понятие об инварианте группы преобразований может быть значительно расширено, если допустить некоторое измененение инварианта в зависимости от данного линейного преобразования.

Мы будем называть величину $\mathfrak{A}$ *относительным инвариантом* группы линейных преобразований, если от преобразования получаем новую величину $\mathfrak{A}'$ этого инварианта, связанную с первоначальною величиною при помощи равенства

$$\mathfrak{A}' = \varepsilon^k \mathfrak{A},$$

где ε модуль преобразования, а k — число, называемое *весом* инварианта.

Если $k = 0$, то мы приходим к первоначальному данному определению инварианта. Будем называть инвариант в случае $k = 0$ *абсолютиым*.

На следующем простом примере можно пояснить понятие об относительном инварианте.

Возьмем бинарную квадратичную форму

$$Ax^2 + 2Bxy + Cy^2 \tag{1}$$

и подвергнем переменные независимые следующему преобразованию

$$\begin{matrix} x = \alpha x' + \beta y' \\ y = \gamma x' + \delta y' \end{matrix} , \qquad \varepsilon = \begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix} = \alpha\delta - \beta\gamma \neq 0 \ ;$$

тогда форма (1) преобразуется в такую

$$A'x'^2 + 2B'x'y' + C'y'^2,$$

где

$$\begin{aligned} A' &= A\alpha^2 + 2B\alpha\gamma + C\gamma^2, \\ B' &= A\alpha\beta + B(\alpha\delta + \beta\gamma) + C\gamma\delta, \\ C' &= A\beta^2 + 2B\beta\delta + C\delta^2. \end{aligned}$$

Простые выкладки убеждают в справедливости формулы

$$B'^2 - A'C' = (B^2 - AC)(\alpha\delta - \beta\gamma)^2 = \varepsilon^2(B^2 - AC);$$

итак, величина $B^2 - AC$ есть относительный инвариант, вес которого равен 2.

Эквивалентность

§ 7

Пусть A и B будут: или два геометрических образа, или два алгебраических выражения, или две системы подобных предметов.

Определение. Если A и B так связаны с некоторой группой преобразований, что существует в этой группе преобразование, переводящее A в B ; то A и B называются эквивалентными по отношение к группе.

Можно установить понятие об эквивалентности по отношение к системе преобразований, не образующей группы. Придется только требовать существование обратного преобразовала, переводящего B в A.

§ 8

Поясним понятие об эквивалентности на примере.

Рассмотрим две системы n линейных форм от n переменных независимых

$$(1)\quad \begin{cases} a_{11}x_1 + \ldots + a_{1n}x_n \\ a_{21}x_1 + \ldots + a_{2n}x_n \\ \ldots\ldots\ldots\ldots\ldots \\ a_{n1}x_1 + \ldots + a_{nn}x_n \end{cases} \qquad (2)\quad \begin{cases} b_{11}x_1 + \ldots + b_{1n}x_n \\ b_{21}x_1 + \ldots + b_{2n}x_n \\ \ldots\ldots\ldots\ldots\ldots \\ b_{n1}x_1 + \ldots + b_{nn}x_n \end{cases}$$

Можно доказать теорему:

Системы (1) *и* (2) *эквивалентны по отношению к группе неособенных линейных преобразовать, когда оба определителя $|a_{ik}|$ и $|b_{ik}|$ не равны нулю.*

Рассмотрим, в самом деле, преобразования

$$(\mathfrak{a})\quad \begin{cases} x'_1 = a_{11}x_1 + \ldots + a_{1n}x_n \\ x'_2 = a_{21}x_1 + \ldots + a_{2n}x_n \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ x'_n = a_{n1}x_1 + \ldots + a_{nn}x_n \end{cases} \qquad (\mathfrak{b})\quad \begin{cases} x'_1 = b_{11}x_1 + \ldots + b_{1n}x_n \\ x'_2 = b_{21}x_1 + \ldots + b_{2n}x_n \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ x'_n = b_{n1}x_1 + \ldots + b_{nn}x_n \end{cases}$$

которые приводят системы (1) и (2) к одному и тому же нормальному виду

$$\begin{cases} x'_1 \ldots\ldots\ldots \\ \ldots x'_2 \ldots\ldots \\ \ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots x'_n \end{cases}$$

Но преобразования $\mathfrak{a}$ и $\mathfrak{b}$ допускают обратные, а потому преобразование $\mathfrak{b}^{-1}\mathfrak{a}$ преобразует (2) в (1), и теорема доказана,

§ 9

В связи с понятием об эквивалентности устанавливается понятие о так называемой *полной системе* независимых инвариантов.

Самый простой пример пояснит дело. Если мы рассмотрим группу пространственных движений, то понятие об *эквивалентности* двух треугольников совпадет с данным в начале элементарной геометрии понятием о *равенстве*. Инвариантами движения, как было сказано выше, являются длины и углы; значить, стороны и углы треугольника. Известно, что для эквивалентности (равенства) треугольников достаточно существования только трех независимых между собой инвариантов: или двух сторон и угла между ними, или двух углов, прилежащих к одной сторон, или, наконец, трех сторон.

Мы устанавливаем такое определение полной системы инвариантов.

Полной называется такая система I абсолютных инвариантов, которые одинаковы для каждых двух эквивалентных предметов, причем эквивалентность нарушается, если хоть один из инвариантов системы I перестает быть одинаковым для этих двух предметов.

Алгебраическая теория инвариантов

§ 10

В 19 столетии разрабатывалась теория инвариантов, которой можно дать название *алгебраической*, причем главным образом рассматривались относительные инварианты. Эта теория, вызванная к жизни теорией алгебраических линий и поверхностей, ставила себе более широкие цели улучшения приемов вычислений, относящихся к целым функциям, в том случае, когда трудности происходят от большого числа переменных независимых и высоких степеней этих функций. В последнее время замечается значительное охлаждение интереса к этой теории, вызванное в значительной степени тем обстоятельством, что полученные результаты не оправдали надежд, первоначально возлагавшихся на теорию. Изучение форм бинарных разрослось в целую науку, тогда как при большем числе переменных независимых теория инвариантов представляла на каждом шагу непреодолимые трудности. Теория линейных форм какого угодно числа переменных независимых, давшая теорию определителей, осталась единственным примером символики, упрощавшей действия и вычисления при большом числе входящих букв. Ничего подобного при формах высших степеней не найдено. Квадратичные формы представляли единственное исключение, ибо они, как мы увидим далее, сводились при помощи билинеарных форм к теории определителей.

Современное состояние теории поверхностей третьего порядка — лучший пример, иллюстрирующий несовершенство теории кубических форм с четырьмя переменными.

Под влиянием новых задач, между прочим под влиянием теории Galois, о которой будет сказано в конце книги, теория инвариантов линейных преобразований видоизменяет свой внешний вид и переходит в теории групповых инвариантов.

Не имея цели по характеру книги входить в подробное изучение алгебраической теории инвариантов, отошлем читателя к классическому учебнику *Salmon,*

G. «Vorlesungen über die Algebra der linearen Transformationen». Deutsch von W. Fiedler. 2 Aullage 1877. Для первоначального же знакомства с групповыми инвариантами можно посоветовать «Siebenter Abschnitt. Gruppeninvarianten» второго тома «Lehrbuch der Algebra» von H. Weber. 1899.

Мы ограничимся изложением лишь определений и теорем, сделавшихся классическими.

Инварианты и коварианты

§ 11

Определение I. Рациональная функция коэффициентов одной формы или системы форм, которая получает множителем k-ую степень (k число целое) модуля неособенного преобразования, приложенного к этим формам, называется относительным инвариантом или просто инвариантом рассматриваемых форм.

Определение II. Целое число k носит название веса инварианта.

Абсолютные инварианты можно рассматривать как относительные, вес которых есть нуль.

Относительный инвариант обращается в абсолютный для преобразования с модулем $+1$.

§ 12

Если мы рассмотрим систему n линейных форм

$$(1)\qquad \begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ a_{n1}x_1 + a_{n2}x_2 + \ldots + a_{nn}x_n \end{cases}$$

то определитель $|a_{ik}|$ будет, очевидно, инвариантом системы (1).

Подвергнем в самом деле, систему (1) линейному преобразованию

$$(2)\qquad \begin{gathered} x_1 = c_{11}x'_1 + \ldots + c_{1n}x'_n \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ x_n = c_{n1}x'_1 + \ldots + c_{nn}x'_n \end{gathered}$$

с модулем $\varepsilon = |c_{ik}|$, отличным от нуля.

Преобразование (2) переводит систему (1) в новую

$$(3)\qquad \begin{cases} a'_{11}x'_1 + \ldots + a'_{1n}x'_n \\ \ldots\ldots\ldots\ldots\ldots \\ a'_{n1}x'_1 + \ldots + a'_{nn}x'_n, \end{cases}$$

где

$$a'_{ik} = a_{i1}c_{1k} + a_{i2}c_{2k} + \ldots + a_{in}c_{nk}.$$

так что дело сводится к умножений матриц.

$$\|a'_{ik}\| = \|a_{ik}\| \cdot \|c_{ik}\|.$$

Переходя к определителям, получим $|a'_{ik}| = \varepsilon |a_{ik}|$, т. е. $|a_{ik}|$ есть инвариант, вес которого есть 1.

§ 13

Определение. Рассматривается ряд систем независимых переменных

$$(x, y, z, \ldots), \quad (x_1, y_1, z_1, \ldots), \quad (x_2, y_2, z_2, \ldots)$$

Если все эти системы подвергнуты одному и тому же линейному преобразованию, то говорят, что эти системы преобразуются когредиентно. Когредиентное изменение можно геометрически характеризовать так. Если задано проективное преобразовало многомерного пространства, то очевидно, что координаты всех точек пространства изменяются когредиентно.

§ 14

Придадим изложению геометрический характер в смысле языка, оставаясь по существу в области чистой алгебры.

Определение 1. Рациональная функция от коэффициентов одной формы или системы форм от n переменных независимых $x_1, x_2, \ldots, x_n$, заключающая кроме этих коэффициентов еще координаты некоторого конечного числа точек $(y_1, y_2, \ldots, y_n)$, $z_1, z_2, \ldots, z_n)$, ... называется относительным ковариантом формы или системы форм, если она приобретает целую степень ε^k модуля неособенного преобразования, когда этому преобразованию когредиентно подвергнуты как переменные $x_1, x_2, \ldots, x_n$ основных форм, так и координаты $(y_1, y_2, \ldots, y_n)$, $(z_1, z_2, \ldots, z_n)$, ... точек.

Ковариант может не заключать совершенно коэффициентов основных форм, а только координаты точек.

Определение II. Показатель k носит название веса коварианта.

§ 15

Определитель

$$|x_i(k) = \begin{vmatrix} x_1{}^{(1)} & \ldots & x_n{}^{(1)} \\ \ldots & \ldots & \ldots \\ x_1{}^{(n)} & \ldots & x_n{}^{(n)} \end{vmatrix}$$

есть относительный ковариант веса -1 системы точек

$$(x_1{}^{(1)}, \ldots, x_n{}^{(1)}), \quad x_1{}^{(2)}, \ldots, x_n{}^{(2)}, \ldots, \; x_1{}^{(n)}, \ldots, x_n{}^{(n)},$$

ибо, выполняя преобразование

$$x_1 = c_{11}X_1 + \ldots + c_{1n}X_n$$
$$\ldots\ldots\ldots\ldots\ldots\ldots$$
$$x_n = c_{n1}X_1 + \ldots + c_{nn}X_n$$

получаем

$$\begin{vmatrix} x_1^{(1)} & \dots & x_n^{(1)} \\ \dots\dots\dots & & \\ x_1^{(n)} & \dots & x_n^{(n)} \end{vmatrix} = |c_{ik}| \cdot \begin{vmatrix} X_1^{(1)} & \dots & X_n^{(1)} \\ \dots\dots\dots & & \\ X_1^{(n)} & \dots & X_n^{(n)} \end{vmatrix};$$

откуда, обозначая модуль преобразовагпя через ε, получим

$$|X_i^{(k)}| = \varepsilon^{-1} \cdot |x_i^{(k)},$$

что доказывает поставленную теорему,

§ 16

Система, состоящая из формы $f(x_1, \dots, x_n)$ и точки $(y_1, \dots, y_n)$, имеет относительно линейного преобразования абсолютный ковариант

$$f(y_1, y_2, \dots, y_n),$$

где $f(y_1, y_2, \dots, y_n)$ результат подстановки координат в форму на место независимых переменных.

Для доказательства рассмотрим уравнение

$$f(x_1, \dots, x_n) = K,$$

где K произвольная постоянная величина, уравнение (1) определяет некоторый образ в многомерном пространстве, которой мы можем назвать *сверхповерхностью*.

Если точка $(y_1, \dots, y_n)$ лежит на сверхповерхности (1), то имеет место тождество

$$f(y_1, \dots, y_n) = K.$$

Это равенство можно написать подробнее, если указать коэффициенты $a_1, a_2, \dots$ формы f,

$$f(a_1, a_2, \dots; y_1, \dots, y_n) = K. \tag{2}$$

Очевидно, что свойство точки находиться на известной сверхповерхности не может нарушиться от преобразования координаты; то мы имеем после преобразования

$$f(a_1', a_2', \dots; y_1', \dots, y_n') = K. \tag{3}$$

Сопоставляя (2) и (3), получим

$$f(a_1', a_2', \dots; y_1', \dots, y_n') = f(a_1, a_2, \dots; y_1, \dots, y_n)$$

и рассматриваемое выражение есть, действительно, ковариант.

§ 17

Понятие о контрагредиентных преобразованиях взято из геометрии. Рассмотрим трехмерное пространство, точки которого определяются четырьмя однородными координатами

$$x_1, \quad x_2, \quad x_3, \quad x_4.$$

Коэффициенты

$$u_1, \quad u_2, \quad u_3, \quad u_4$$

уравнений плоскости

$$u_1x_1 + u_2x_2 + u_3x_3 + u_4x_4 = 0 \tag{1}$$

можно считать *координатами* плоскости (1), т. е. величинами, определяющими положение плоскости (1) в пространстве. Это так называемые *однородные плоскостные координаты.*

§ 18

Посмотрим, каким преобразованиям подвергаются плоскостные координаты, когда точечные координаты x_i подвергаются проективному преобразованию $\mathfrak{c}$

$$x_i' = c_{i1}x_1 + c_{i2}x_2 + c_{i3}x_3 + c_{i4}x_4 \qquad (i = 1, 2, 3, 4) \tag{$\mathfrak{c}$}$$

с отличным от нуля определителем

$$\varepsilon = |c_{ik}|.$$

Обозначая через C_{ik} алгебраическая добавления элементов определителя ?, получим обратное преобразование

$$x_i = \frac{C_{1i}}{\varepsilon}x_1' + \frac{C_{2i}}{\varepsilon}x_2' + \frac{C_{3i}}{\varepsilon}x_3' + \frac{C_{4i}}{\varepsilon}x_4' \qquad (i = 1, 2, 3, 4). \tag{$\mathfrak{c}^{-1}$}$$

Подставляя эти выражения x_i через x_i' в основное уравнение (1), дающее соотношение между u_i и x_i, получим

$$u_1'x_1' + u_2'x_2' + u_3'x_3' + u_4'x_4' = 0,$$

где

$$u_i' = \frac{C_{i1}}{\varepsilon}u_1 + \frac{C_{i2}}{\varepsilon}u_2 + \frac{C_{i3}}{\varepsilon}u_3 + \frac{C_{i4}}{\varepsilon}u_4 \qquad (i = 1, 2, 3, 4). \tag{$\mathfrak{d}$}$$

Итак мы видим, что плоскостные координаты преобразовываются при помощи преобразования

$$\mathfrak{d} = (\mathfrak{c}^{-1})',$$

сопряженного с обратным от $\mathfrak{c}$.

§ 19

Две системы n переменных независимых называются контрагредиентными, если при неособенном линейиом преобразование одной другая преобразуется при помощи сопряженного с обратным от первого.

Получим теорему.

Если две системы контрагредиентных переменных

$$x_1,\ \ldots,\ x_n \quad u \quad u_1,\ \ldots,\ u_n$$

преобразовываются в новые

$$x'_1,\ \ldots,\ x'_n \quad u \quad u'_1,\ \ldots,\ u'_n,$$

то выражение

$$u_1x_1 + u_2x_2 + \ldots + u_nx_n = 0$$

переходит в

$$u'_1x'_1 + u'_2x'_2 + \ldots + u'_nx'_n = 0.$$

В связи с контрагредиентными переменными вводится понятая о так называемом *контравариантe.*

Контравариантом называется всякая рациональная функция от коэффициентов заданных форм и от контрагредиентных переменных

$$(u_1, \ldots, u_n), \quad (u'_1, \ldots, u'_n),$$

которая приобретает некоторую целую степень модуля преобразования.

Очевидно, что понятие о контравариантe является излишним, если контрагредиентные переменные рассматривать как коэффициенты линейных форм. Тогда контравариант обращается в инвариант.

Тоже самое относится к более общему понятии *смешанного комитанта* (Zwischenform), в который кроме коэффициентов форм и контрагредиентных переменных входят еще и когредиентные.

Вообще является недостатком излагаемой теории введение большого числа названий,[10] причем составляются из этих названии теоремы, часто являющаяся совершенно тривиальными. как, например, следующая.

Комитант ковариантa есть комитант первоначальной формы.

Ортогональные преобразования

§ 20

Рассмотрим задачу: найти тождественные контрагредиентные преобразования.

Употребляя символы § 17, можем формулировать задачу, как нахождение матрицы $\mathfrak{c}$, для которой

$$(\mathfrak{c}^{-1})' = \mathfrak{c}.$$

[10]Так, например, кроме указанных выше имеются названия: эвектант, эманант, ... и т. д.

Рассмотрим случай трех переменных независимых

$$\mathfrak{c} = \left\| \begin{matrix} a & b & c \\ a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \end{matrix} \right\|, \qquad \varepsilon = \begin{vmatrix} a & b & c \\ a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \end{vmatrix}.$$

Обозначая большими буквами A, A_1, A_2, B, B_1, B_2, C, C_1, C_2 алгебраическая дополнения элементов a, b, c, a_1, b_1, b_2, c, c_1, c_2, приведем задачу к ряду равенств

$$A = a\varepsilon, \quad B = b\varepsilon, \quad C = c\varepsilon, \tag{1}$$

$$A_1 = a_1\varepsilon, \quad B_1 = b_1\varepsilon, \quad C_1 = c_2, \varepsilon \tag{2}$$

$$A_2 = a_2\varepsilon, \quad B_2 = b_2\varepsilon, \quad C_2 = c_2.\varepsilon \tag{3}$$

Умножая равенство (1) на a, b, c и складывая, получим

$$\varepsilon = \varepsilon(a^2 + b^2 + c^2),$$

но $\varepsilon \neq 0$, следовательно, будет

$$a^2 + b^2 + c^2 = 1;$$

подобным же образом получаем

$$a_1^2 + b_1^2 + c_1^2 = 1,$$
$$a_2^2 + b_2^2 + c_2^2 = 1.$$

Кроме того

$$aa_1 + bb_1 + cc_1 = 0,$$
$$aa_2 + bb_2 + cc_2 = 0,$$
$$a_1a_2 + b_1b_2 + c_1c_2 = 0.$$

Далее

$$\varepsilon^2 = \begin{vmatrix} a_1^2 + b_1^2 + c_1^2 & aa_1 + bb_1 + cc_1 & \dots \\ \dots\dots\dots\dots\dots\dots\dots\dots & & \\ \dots\dots\dots\dots\dots\dots\dots\dots & & \end{vmatrix} = \begin{vmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{vmatrix} = 1,$$

откуда $\varepsilon = \pm 1$.

§ 21

Мы пришли к так называемому *ортогональному* преобразованию, определяемому равенствами:

$$\begin{gathered} c_{1i}^2 + c_{2i}^2 + \ldots + c_{ni}^2 = 1 \qquad (i = 1, 2, \ldots, n), \\ c_{1i}c_{1k} + c_{2i}c_{2k} + \ldots + c_{ni}c_{nk} = 0 \qquad \left(\begin{matrix} i = 1, 2, \ldots, n \\ k = 1, 2, \ldots, n \end{matrix}, \quad i \neq k \right). \end{gathered} \tag{1}$$

В случае $n = 3$, как известно, получается вращение прямоугольной системы координата около начала, откуда происходит и само название ортогонального преобразования.

Из равенств (1) вытекает:

I. $\varepsilon = |c_{ik}| = \pm 1$, ибо

$$\varepsilon^2 = \begin{vmatrix} c_{11}^2 + c_{21}^2 + \ldots + c_{n1}^2 & \ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \end{vmatrix} = \begin{vmatrix} 1 & 0 & \ldots & 0 \\ \ldots\ldots\ldots\ldots \\ 0 & 0 & \ldots & 1 \end{vmatrix} = 1.$$

II. Обозначая алгебраическое дополнение элемента c_{ik} через C_{ik}, получим

$$C_{ik} = \varepsilon c_{ik}, \tag{2}$$

ибо можно будет написать ряд тождеств

$$\begin{gathered} (C_{1k} - \varepsilon c_{1k})c_{11} + (C_{2k} - \varepsilon c_{2k})c_{21} + \ldots + (C_{nk} - \varepsilon c_{nk})c_{n1} = 0 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ (C_{1k} - \varepsilon c_{1k})c_{1n} + (C_{2k} - \varepsilon c_{2k})c_{2n} + \ldots + (C_{nk} - \varepsilon c_{nk})c_{nn} = 0 \end{gathered}$$

из которых получаются соотношения (2), ибо отличен от нуля определитель ?.

III. Получаются равенства

$$\begin{gathered} c_{i1}^2 + c_{i2}^2 + \ldots + c_{in}^2 = 1 \qquad (i = 1, 2, \ldots, n), \\ c_{i1}c_{j1} + c_{i2}c_{j2} + \ldots + c_{in}c_{jn} = 0 \qquad \left(\begin{array}{c} i = 1, 2, \ldots, n \\ j = 1, 2, \ldots, n \end{array} , \quad i \neq j \right). \end{gathered}$$

Последние равенства получаются, если умножить на c_{jk} равенства (2) и просуммировать по k.

Преобразования с определителем $+1$ мы будем называть *собственными*, а с определителем -1 — *несобственными.*

§ 22

Ортогональные преобразования были предметом разнообразных исследований и имеют довольно богатую литературу.

Укажем здесь на главнейшие вопросы, интересовавшие математиков.

Так как ортогональное преобразовало соответствует тому случаю, когда контрагредиентное преобразование совпадает с начальным, то в этом случай можно заменить перемгенные u_i на x_i, и мы заметим, что ортогональное преобразование переводить выражение

$$x_1x_1 + x_2x_2 + \ldots + x_nx_n$$

в новое

$$x'_1x'_1 + x'_2x'_2 + \ldots + x'_nx'_n.$$

Это можно выразить так: *ортогональное преобразование переводит квадратичную форму*

$$x_1^2 + x_2^2 + \ldots + x_n^2$$

в самое себя.

Hermite[11] поставил более общий вопрос изучения преобразований, переводящие общего вида квадратичную форму $\sum a_{ik}x_ix_k$ в самое себя. Задача Hermite'а имеет особенное значение для теории чисел, когда формы рассматриваются с целыми коэффициентами, ибо, как нам известно из элементарного курса теории чисел, подстановки с целыми коэффициентами, переводящая бинарную квадратичную форму в самое себя, связаны с уравнением Pell'а. Так что задача Hermite'а для форм с целыми коэффициентами связана с труднейшими и глубочайшими исследованиями теории чисел.

Оставаясь в области алгебры, то есть, не предполагая коэффициентов подстановки числами целыми, ограничимся относительно преобразований Hermite'а указанием на то, что определитель такого преобразования равен ± 1. Это будет ясно из следующей главы, посвященной алгебраической теории квадратичных форм.

Особенное внимание было обращено на рассмотрение характеристического уравнения ортогональной матрицы. Brioschi[12] заметил, что это уравнение возвратное, а именно, что, если λ есть один его корень, то будет существовать другой $\frac{1}{\lambda}$. Frobenius[13] при помощи теории элементарных делителей подверг это уравнение подробному исследованию.

§ 23

Так как между n^2 коэффициентами ортогонального преобразования существует $n + \frac{n(n-1)}{2}$ соотношений, то независимыми из числа этих коэффициентов остаются только $\frac{n(n-1)}{2}$. Можно выразить все коэффициенты в виде функций от $\frac{n(n-1)}{2}$ независимых переменных.

Euler[14] показал, как составить элементы ортогональной матрицы определителя ± 1 при помощи $\frac{n(n-1)}{2}$ произвольных вспомогательных углов. Для трехмерного пространства ($n = 3$) получаются знаменитые Euler'овы углы, постоянно употребляющееся в механике.

Euler представляет ортогональную матрицу как произведение $\frac{n(n-1)}{2}$ матриц вида

$$\left\|\begin{matrix} \cos\varphi & -\sin\varphi & 0 & 0 & & & \\ \sin\varphi & \cos\varphi & 0 & 0 & & & \\ 0 & 0 & 1 & 0 & & & \\ 0 & 0 & 0 & 1 & & & \\ & & & & 1 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{matrix}\right\|$$

у которых все элементы главной диагонали, кроме двух, равны 1; эти два суть $\cos\varphi$

[11]Hermite. Euvres I, 195 (1854).
[12]Brioschi. Journal de Liouville. 19, 253 (1854).
[13]Frobenius. Journ. j. r. u. a. Math. 84, 48 (1878).
[14]Leonhardi Euleri. Commentationes arithmeticae. T. 1, 427.

и $\cos\varphi$; этим двум элементам диагонали соответствуют два элемента $-\sin\varphi$ и $\sin\varphi$, расположенные на тех же горизонталях и колоннах, остальные элементы нули. Взяв всевозможные сочетания n элементов диагонали по два, получим формулы Euler'a.

Так например, в случай трех измерений надо ввести три угла φ, ψ, θ:

$$\begin{Vmatrix}\cos\varphi & \sin\varphi & 0\\ \sin\varphi & -\cos\varphi & 0\\ 0 & 0 & 1\end{Vmatrix}\cdot\begin{Vmatrix}\cos\psi & 0 & \sin\psi\\ 0 & 1 & 0\\ \sin\psi & 0 & -\cos\psi\end{Vmatrix}\cdot\begin{Vmatrix}0 & 0 & 0\\ 0 & \cos\theta & \sin\theta\\ 0 & \sin\theta & -\cos\theta\end{Vmatrix}.$$

Перемножая матрицы, получаем окончательно матрицу Euler'a[15]

$$\begin{Vmatrix}\cos\varphi\cos\psi & \sin\varphi\cos\theta+\cos\varphi\sin\theta\sin\psi & \sin\varphi\sin\theta-\cos\varphi\cos\theta\sin\psi\\ \sin\varphi\cos\psi & -\cos\varphi\cos\theta+\sin\varphi\sin\theta\sin\psi & -\cos\varphi\sin\theta-\sin\varphi\cos\theta\sin\psi\\ \sin\psi & -\cos\psi\sin\theta & \cos\psi\cos\theta\end{Vmatrix}.$$

Для случая пространства четырех измерений надо перемножить шесть матриц

$$\begin{Vmatrix}\cos\varphi_1 & \sin\varphi_1 & 0 & 0\\ \sin\varphi_1 & -\cos\varphi_1 & 0 & 0\\ 0 & 0 & 1 & 0\\ 0 & 0 & 0 & 1\end{Vmatrix}\cdot\begin{Vmatrix}\cos\varphi_2 & 0 & \sin\varphi_2 & 0\\ 0 & 1 & 0 & 0\\ \sin\varphi_2 & 0 & -\cos\varphi_2 & 0\\ 0 & 0 & 0 & 1\end{Vmatrix}\cdot\begin{Vmatrix}\cos\varphi_3 & 0 & 0 & \sin\varphi_3\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\\ \sin\varphi_3 & 0 & 0 & -\cos\varphi_3\end{Vmatrix}\cdot$$

$$\cdot\begin{Vmatrix}1 & 0 & 0 & 0\\ 0 & \cos\varphi_4 & \sin\varphi_4 & 0\\ 0 & \sin\varphi_4 & -\cos\varphi_4 & 0\\ 0 & 0 & 0 & 1\end{Vmatrix}\cdot\begin{Vmatrix}1 & 0 & 0 & 0\\ 0 & \cos\varphi_5 & 0 & \sin\varphi_5\\ 0 & 0 & 1 & 0\\ 0 & \sin\varphi_5 & 0 & -\cos\varphi_5\end{Vmatrix}\cdot\begin{Vmatrix}1 & 0 & 0 & 0\\ 0 & 1 & 0 & 0\\ 0 & 0 & \cos\varphi_6 & \sin\varphi_6\\ 0 & 0 & \sin\varphi_6 & -\cos\varphi_6\end{Vmatrix}.$$

Подобные же соображения относятся к какому угодно числу измерений.

§ 24

Если ввести функции $\tau_i = \mathrm{tg}$
$frac\varphi_i 2$, где φ_i Euler'овские углы, как новые независимые переменные, то коэффициенты ортогонального преобразования выразятся рационально через τ_i. Итак, может быть поставлен вопрос о наиболее общем представлении коэффициентов ортогонального преобразования в виде рациональных функций от переменных независимых.

Euler'у принадлежат наиболее замечательные представления такого рода, относящаяся к случаям $n = 3$ и $n = 4$. Для $n = 3$

$$c_{11} = \frac{p^2+q^2-r^2-s^2}{u},\quad c_{12} = \frac{2qr+2ps}{u},\quad c_{13} = \frac{2qs-2pr}{u},$$
$$c_{21} = \frac{2qr-2ps}{u},\quad c_{22} = \frac{p^2-q^2+r^2-s^2}{u},\quad c_{23} = \frac{2pq+2rs}{u},$$
$$c_{31} = \frac{2qs+2pr}{u},\quad c_{32} = \frac{2rs-2pq}{u},\quad c_{33} = \frac{p^2-q^2+s^2-r^2}{u},$$

где

$$u = p^2+q^2+r^2+s^2.$$

[15]Здесь я показываю, как получить несобственную матрицу.

Для $n = 4$ Euler дает такую матрицу

$$\left\|\begin{matrix} ap+bq+cr-ds & ar-bs-cp+dq & -as-br+cq+dp & aq-bp+cs-dr \\ -aq+bp+cs-dr & as+br-cq+dp & ar-bs+cp-dq & ap+bq-cr-ds \\ ar+bs-cp-dq & -ap+bq-cr+ds & aq+bp+cs+dr & as-br-cq+dp \\ -as+br-cq+dp & -aq-bp+cs+dr & -ap+bq+cr-ds & ar+bs+cp+dq \end{matrix}\right\|.$$

В этой матрице суммы квадратов каждой горизонтали и каждой колонны дают одно и тоже число

$$(a^2+b^2+c^2+d^2)(p^2+q^2+r^2+s^2),$$

а суммы произведений элементов двух различных горизонталей или колонн равны нулю.

Euler заявляет, что все его попытки дать подобные формулы для пространства более четырех измерений были неудачны.

Чебыниев[16] и Cayley[17] дали подобные формулы для произвольного числа n, которые нельзя однако считать общими.

§ 25

Особенно важное значение имеет рассмотрение конечных групп ортогональных преобразований. Нетрудно видеть, что будет ортогональным преобразованием, которое мы рассматривали в § 53 Главы V и которое соответствует подстановки переменных независимых. В этих преобразованиях матрица состоит из нулей и единиц, причем в каждой горизонтали и в каждой колоний находится по одному элементу, равному единице, тогда как остальные суть нули. Группы подстановок букв находиться, следовательно, среди ортогональных групп.

Будем называть матрицы, соответствующие подстановкам, Y-матрицами. Матрица, соответствующая транспозиции (i, k), имеет вид

(1)

				i-ая колонна			k-ая колонна	
1	0	0		0	. . . . .		0	. . . 0
0	1	0	$\ddots$	0	. . . . .		0	. . . 0
. . . . .				. . .	. . . . .		. . .	. . . . .
0	0	0	. . .	0	. . . . .		1	. . . 0
0	0	0	. . .	0	1	$\ddots$	0	. . . 0
. . . . .				. . .	. . . . .		. . .	. . . . .
0	0	0	. . .	0	0 . . .	1	0	. . . . .
0	0	0	. . .	1	0 . . .	0	0	. . . . .
0	0	0	. . .	0	0 . . .	0	0	. . . 1

и получается из единичной матрицы через перестановку двух горизонталей или колонн i-ой и k-ой.

[16] Чебышев. Полное собрание сочинений. Т. I. Стр. 226.

[17] Cayley. Journ. t. u. Math. 22, 120 (1846).

Матрица (1), соответствующая транспозия (i, k), имеет определитель $\varepsilon = -1$.

Матрица $Y \cdot (i, k)$ происходить из Y через перестановку двух колонн i-ой и k-ой, а матрица $(i, k)Y$ происходит из Y через перестановку двух горизонталей.

Из сказанного следует, что подстановкам знакопеременной группы соответствуют собственные преобразования, подстановкам же, равносильным нечетному числу транспозиций, соответствуют несобственные преобразования.

§ 26

Вся группа ортогональных преобразований, как собственных, так и несобственных, коэффициенты которых произвольный вещественные или комплексные числа, имеет подгруппой группу собственных преобразований.

Принимая во внимание сказанное, мы замечаем, что среди конечных групп ортогональных преобразований, заключаются прежде всего группы подстановок, то есть, группы собственных и несобственных преобразований вида Y.

Далее можно указать на группы преобразований Y', получающихся из Y заменой единиц на ± 1.

Группы преобразований Y и Y' сводятся к изменению названий осей координат, причем группы собственных преобразований Y можно характеризовать как группы вращений системы координат около начала, когда одна ось приходят в совпадение с другими по положение и по направлению. Порядок группы всех преобразований Y есть $n!$, а порядок всех преобразований Y' есть $2^n n!$.

§ 27

Обращаясь далее к рассмотрению конечных групп ортогональных вещественных преобразований, отличных от Y и Y', мы заметим, что для трехмерного пространства задача решена вполне.

Скажем в немногих словах, в чем состоит это решение.

Обращаемся сначала к конечным группам собственных преобразований, отличных от Y, Y'.

Пусть задана конечная группа вращений порядка n, тогда этой группе соответствует n положений некоторого тела, неизменно связанного с вращающеюся средой. Эти n положений тела образуют правильную фигуру, которая совпадать с самой собою при указанной группе вращений.

Если перемещающимся телом будет плоскость, то мы естественно приходим к правильным многогранникам.

Перебирая все возможные случаи конечных групп вращений, мы должны будем рассмотреть следующие тела: правильную пирамиду, двойную пирамиду, тетраэдр, октаэдр, куб, додекаэдр и икосаэдр.

Правильная пирамида с g боковыми гранями совпадет с самой собой при g-кратном повторении поворота около оси на угол $\dfrac{2\pi}{g}$.

Двойная пирамида, т. е. такая, ребра которой продолжены за вершину, если она имеет четное число боковых граней, может быть совмещена с самой собою, кроме вращений около оси, еще при помощи опрокидывания на 180 градусов около вершины.

Обращаясь к правильным многогранникам в собственном смысле слова, мы заметим, как по виду многогранника найти порядок соответствующей ему группы. В самом деле, многогранник может быть приведен в совпадение с самим собой наложением одной его грани на все остальные, при этом наложение можно произвести на столько способов сколько вершин заключаешь эта грань.

Приходим к такому способу. Порядок группы вращений правильного тела равен:

1) произведению числа граней на число углов в каждой грани,

2) произведение числа вершин на число граней, встречающихся в каждой вершине,

3) двойному числу ребер.

По этому счислению порядок группы будет:

для тетраэдра	12,
для куба и октаэдра	24,
для додекаэдра и икосаэдра	60.

Надо заметить, что, если мы около октаэдра опишем шар и продолжим до пересечения с шаром перпендикуляры, опущенные из центра на 8 граней, то получим куб, вписанный в тот же шар. Этот куб мы назовем сопряженным с октаэдром. Группа вращений куба совпадаешь с группой вращения сопряженного октаэдра. Подобным же образом додекаэдр и икосаэдр суть сопряженные между собой тела и имеют общую группу.

Итак, мы приходим к пяти группам вращений:

1) группа пирамиды,

2) группа двойной пирамиды.

3) группа тетраэдра,

4) группа октаэдра,

5) группа икосаэдра.

§ 28

Перейдем теперь к конечным группам ортогональных преобразований общего вида как собственных, так и несобственных. Нетрудно видеть, что несобственные преобразования можно считать получающимися из собственных через умножение на одну несобственную матрицу

$$\begin{Vmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{Vmatrix}$$

Эта матрица соответствует преобразование

$$x_1 = x, \quad y_1 = y, \quad z_1 = -z,$$

изменяющему лишь знак координаты z.

Это преобразование можно рассматривать как зеркальное изображение фигуры, если зеркальною поверхностью является плоскость xy.

Допустив кроме вращений еще операцию зеркального опрокидывания фигуры, мы приходим к конечным группам, носящим название *групп кристаллографических*.

Русский известный минералог Федоров исчерпывающим образом изучил симметрии пространственных фигур, а потому задача нахождения кристаллографнческих групп сводится к его исследованиям и допускает полное решение.

Было бы важно решить задачу нахождения конечных групп ортогональных преобразований для произвольного числа измерений, ибо изучение симметрии многомерных пространств приводит к решению важных задач теории чисел. Эта задача была предметом занятий на моем семинаре по алгебре в 1913 г. в Уннверситете св. Владимира. Полное ее решение для четырех измерений дал Goursat.[18]

Я утверждаю, что, начиная с пяти измерений, дело исчерпывается группами Y и Y'. Вопрос имеет связь с вопросом о представлении групп при помощи групп подстановок наименьшого числа предметов.

Полная система инвариантов

§ 29

В § 9 этой главы мы дали понятие о полной системе независимых инвариантов. В излагаемой нами алгебраической теории иивариантов название *полная система* употребляется в несколько более узком смысле слова. Здесь мы рассмотрим целые, рациональные, относительные инварианты. Под полной системой таких инвартантов понимаемся совокупность известного числа так выбранных инвариантов, что всякий инвариант выражается через выбранные в виде целой рациональной функции. Поясним сказанное на простом примере.

Мы видели уже в § 12, что определитель a системы линейных форм

$$\begin{array}{c} a_{11}x_1 + \ldots + a_{1n}x_n \\ \ldots\ldots\ldots\ldots\ldots \\ a_{n1}x_1 + \ldots + a_{nn}x_n \end{array} \tag{1}$$

есть инвариант этой системы.

Покажем теперь, что в нашем случае определитель a есть единственный независимый инвариант, при чем всякий другой инвариант будет степенью этого инварианта с натуральным показателем, взятою с постоянным множителем.

Сделаем линейное преобразование, имеющее матрицу $\|c_{ik}\|$ с определителем $c = |c_{ik}|$. Пусть новая система линейных форм будет

$$\begin{array}{c} a'_{11}x'_1 + \ldots + a'_{1n}x'_n \\ \ldots\ldots\ldots\ldots\ldots \\ a'_{n1}x'_1 + \ldots + a'_{nn}x'_n \end{array}$$

Обозначая определитель новой системы через a', получим, очевидно,

$$a'ac.$$

[18]Goursat. Annales sc. de l'Ecole Normale Supérieure. Serie III. T. VI. 1889.

Пусть

$$I(a_{11}, \ldots, a_{nn})$$

произвольный инвариант системы (1) и, обозначая для краткости $I' = I(a'_{11}, \ldots, a'_{nn})$, получим по определению понятая об инварианте

$$I' = c^k I,$$

где k вес инварианта I. Применим такое преобразование, которое переводить систему линейных форм в нормальный вид

$$\begin{matrix} x'_1 & \ldots & \ldots \\ \ldots & x'_2 & \ldots \\ \ldots & \ldots & \ldots \\ \ldots & \ldots & x'_n \end{matrix} \tag{2}$$

В этом случае $a' = 1$, т. е. $ac = 1$, $c = a^{-1}$.

Обозначим через I_0 постоянное число, в которое обращается инвариант I для системы (2), тогда мы получим

$$I_0 = c^l I = a^{-k} I,$$

откуда

$$I = I_0 a^k,$$

что и требовалось показать.

Нетрудно видеть, что если система m линейных форм от n переменных независимых состоит из меньшого числа форм, чем число переменных независимых ($m < n$), то система не имеет совсем целых рациональных инвариантов.

В самом деле, добавляя $n - m$ форм с произвольными коэффициентами, получим как единственный инвариант степень определителя. Этот инвариант не может быть инвариантом заданных форм, ибо он заключает произвольные элементы.

§ 30

Задача о нахождении полной системы рациональных инвариантов обобщается таким образом, что к инвариантам присоединяются еще и коварианты.

Как было сказано в § 10, теория инвариантов под влиянием приложений постепенно переходит в теории групповых инвариантов, т. е. теории форм $f(x_1, x_2, \ldots, x_n)$, не меняющихся или приобретающих постоянный множитель при линейном преобразований переменных независимых, принадлежащем к некоторой группе таких преобразовали. Hilbert'y[19] принадлежите такая важная теорема.

Число независимых абсолютных иивариантов всякой конечной группы однородных линейных преобразований конечно.

[19]D. Hilbert. Math. Ann. 36, 473 (1890) H. Weber. Algebra. 2 B. 218.

Арифметические инварианты

§ 31

Кроме геометрических и алгебраических инвариантов приходится иногда рассматривать так называемые, числовые или арифметические инварианты.

Пример такого рода инвариантов представляет ранг матрицы коэффициентов системы n линейных форм от n переменных независимых. Нетрудно видеть,[20] что этот ранг не изменяется от умножения матрицы на матрицу неособенного линейного преобразования.

Второй пример подобного инварианта представляет матрица однородных координат m точек $n-1$ мерного пространства

$$\begin{gathered} {x_1}^{(1)},\ {x_1}^{(1)},\ \ldots,\ {x_n}^{(1)} \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ {x_1}^{(m)},\ {x_1}^{(m)},\ \ldots,\ {x_n}^{(m)} \end{gathered}$$

В самом деле, если ранг матрицы есть 1, то точки совпадают, что очевидно не нарушается при проективном преобразовании пространства. Подобным же образом, если ранг есть 2, точки лежат на одной прямой, обстоятельство также сохраняющееся при проективном преобразовании. Подобным же образом докажем, что каков бы ранг матрицы ни был, он сохраняется при линейном преобразовании.

Как пример полной системы инвариантов можно привести соображения § 57 главы IV: *ранг и элементарные делители составляют полную систему инвариантов для группы элементарных преобразований матрицы.*

Билинеарные формы

§ 32

Билинеарными называются такие квадратичные формы относительно ? переменных

$$(x_1, x_2, \ldots, x_n) \quad (y_1, y_2, \ldots, y_n),$$

когда каждый их член будет первой степени как относительно x, так и относительно y.

Общего вида билинеарная форма при $n = 3$ будет

$$\begin{gathered} a_{11}x_1y_1 + a_{12}x_1y_2 + a_{13}x_1y_3 + \\ + a_{21}x_2y_1 + a_{22}x_2y_2 + a_{23}x_2y_3 + \\ + a_{31}x_3y_1 + a_{32}x_3y_2 + a_{33}x_3y_3. \end{gathered}$$

Ее можно обозначить кратко так:

$$\sum_1^3 a_{ij}x_iy_j.$$

[20] Д. Граве. Элементарный курс теории чисел. Издание второе. 1913 стр. 287.

Матрица

$$\mathfrak{a} = \|a_{ij}\|$$

носит название матрицы билинеарной формы.

Определитель матрицы билинеарной формы называется *определителем формы*. Если определитель равен нулю, то форма называется *особенной*.

Билинеарную форму можно предполагать происходящею из линейных форм двояким образом. Или рассматривается система линейных форм относительно $y_1, y_2, \ldots, y_n$ с матрицей $\mathfrak{a}$, которые умножаются по порядку на $x_1, x_2, \ldots, x_n$ и складываются, или берутся формы относительно $x_1, x_2, \ldots, x_n$ с сопряженной матрицей $\mathfrak{a}'$, умножаются по порядку на $y_1, y_2, \ldots, y_n$ и складываются.

Если возьмем первый способ образования, то явится очевидным, что, если мы подвергнем буквы y преобразованию с матрицей $\mathfrak{b}$, то новая матрица формы будет $\mathfrak{ab}$.

Если же возьмем второй способ образования и подвергнем буквы x преобразованию с матрицей $\mathfrak{c}$, то сопряженная матрица обратится $\mathfrak{c}$, откуда настоящие матрица билинеарной формы обратится в $(\mathfrak{a}'\mathfrak{c})' = \mathfrak{c}'\mathfrak{a}$.

Итак, если в билинеарной форме подвергнуть одновременно буквы y преобразованию с матрицей $\mathfrak{b}$, а буквы x преобразованию с матрицей $\mathfrak{c}$, то матрица $\mathfrak{a}$ формы обратится в такую

$$\mathfrak{c}'\mathfrak{ab}.$$

Переходя к определителям и замечая что $|\mathfrak{c}'| = |\mathfrak{c}|$, ибо определитель не меняет величины от замены горизонталей колоннами и обратно, мы можем высказать предложение:

Определитель формы получает множителем произведение определителей преобразований букв x и букв y.

Ранг билинеарной формы будет очевидно инвариантом неособенного преобразования переменных x и y.

Билинеарная форма называется *симметрической*, если ее матрица симмметрическая, т. е.

$$\mathfrak{a}' = \mathfrak{a}.$$

§ 33

Приведем в заключение несколько просто доказываемых свойств билинеарных форм.

Если в симметрической форме буквы x и y преобразованы когредиентно, то получается снова симметрическая форма, ибо

$$(\mathfrak{c}'\mathfrak{ac})' = \mathfrak{c}'\mathfrak{a}'\mathfrak{c} = \mathfrak{c}'\mathfrak{ac}.$$

Билинеарная форма

$$x_1y_1 + x_2y_2 + \ldots + x_ny_n$$

тогда и только тогда не изменяет своего вида, если x и y изменяются контрагредиентно, ибо

$$\mathfrak{c}' \cdot \mathbf{1} \cdot \mathfrak{b} = \mathbf{1}, \qquad \mathfrak{c}'\mathfrak{b} = \mathbf{1}.$$

Две билинеарные формы эквивалентны,[21] когда обе имеют один и тот же ранг.

Так как всякая матрица ранга r сводится к ее эквивалентной, у которой r диагональных элементов единицы, все же остальные элементы нули, то всякая билинеарная форма ранга r приводится неособеными линейными преобразованиями x и y к нормальному виду

$$x_1y_1 + x_2y_2 + \ldots + x_ry_r.$$

[21]Переводятся одна в другую при помощи неособенных линейных преобразований.

Глава VII

Квадратичные Формы

§ 1

Мы будем представлять самую общую, квадратичную форму от n переменных независимых в таком виде:

$$\begin{aligned}\sum_1^n a_{ij}x_ix_j \quad &= a_{11}x_1^2 + a_{12}x_1x_2 + \ldots + a_{1n}x_1x_n + \\ &+ a_{21}x_2x_1 + a_{22}x_1x_2 + \ldots + a_{2n}x_2x_n + \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ &+ a_{n1}x_nx_12 + a_{n2}x_nx_2 + \ldots + a_{nn}x_n^2.\end{aligned} \tag{1}$$

Матрицу коэффициентов

$$\mathfrak{a} = \left\|\begin{matrix} a_{11} & \ldots & a_{1n} \\ \ldots & \ldots & \ldots \\ a_{n1} & \ldots & a_{nn}\end{matrix}\right\|$$

мы будем называть *матрицей квадратичной формы*, ее определитель $a = |\mathfrak{a}|$ мы будем называть *дискриминантом* квадратичной формы, а ранг матрицы $\mathfrak{a}$ будем называть рангом самой формы.

На основании того, что квадратичную форму можно считать происшедшею из билинеарной, в которой обе системы переменных независимых совпадают, мы можем утверждать, что, если применить к квадратичной форме линейное преобразование

$$\begin{aligned} x_1 &= c_{11}x_1' + \ldots + c_{1n}x_n' \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ x_n &= c_{n1}x_1' + \ldots + c_{nn}x_n'\end{aligned} \tag{2}$$

с матрицей $\mathfrak{c} = \|c_{ik}\|$, то квадратичная форма обратится в новую, матрица которой будет

$$\mathfrak{a}_1 = \mathfrak{c}'\mathfrak{a}\mathfrak{c}, \tag{3}$$

где $\mathfrak{c}'$ обозначает матрицу, сопряженную с $\mathfrak{a}$.

На оснований теоремы[22] о неизменности ранга матрицы при умножений ее на другую неособенную, мы заключаем, что *ранг квадратичной формы не меняется от неособенного линейного преобразования.*

[22] Д. Граве. Элементарный курс теории чисел. Вт. изд. 1913. § 24. Глава XIII.

Переходя от матриц формулы (3) к их определителям и замечая, что определитель $|\mathfrak{c}'|$ сопряженной матрицы не отличается от определителя $\mathfrak{c}$, получаем

$$|\mathfrak{a}_1| = |\mathfrak{a}| \cdot |\mathfrak{c}|^2,$$

откуда следует теорема: *Дискриминант квадратичной формы есть ее относительный инвариант веса* 2.

Полярная форма

§ 2

Не нарушая общности теории квадратичных форм, когда коэффициенты остаются произвольными, можно предполагать матрицу формы симметричною, т. е.

$$a_{ij} = a_{ji}.$$

Мы будем называть билинеарную форму

$$\sum_1^n a_{ij} x_i z_j$$

полярною формой по отношений квадратичной $\sum_1^n a_{ij} x_i x_j$.

Пусть переменный y и z подвергнуты когредиентно преобразованию (2) § 1 с матрицей $\mathfrak{c}$, тогда полярная форма (1) преобразуется в новую

$$\sum_1^n {a_{ij}}^0 y'_i z'_j.$$

Если при таком преобразовании $\mathfrak{c}$ сама квадратичная форма (1) § 1 переходит в такую

$$\sum_1^n {a_{ij}}' x'_i x'_j,$$

то можно показать, что

$${a_{ij}}^0 = {a_{ij}}'.$$

В самом деле, если мы напишем два равенства

$$\sum a_{ij} x_i x_j = \sum {a_{ij}}' x'_i x'_j, \tag{2}$$

$$\sum a_{ij} y_i z_j = \sum {a_{ij}}^0 y'_i z'_j, \tag{3}$$

то их можно считать за тождества, если под x_i, y_i, z_i в левых частях разуметь линейные выражения через x'_i, y'_i, z'_i. Тождества не нарушаются, какие бы выражения ни подставлять вместо входящих в них букв. Полагая например в тождестве (3)

$$y'_i = x'_i, \quad z'_i = x'_i \qquad (i = 1, 2, \ldots, n),$$

получим

$$\sum a_{ij}x_ix_j = \sum a_{ij}{}^0x'_ix'_j.$$

Отсюда, сравнивая с (2), получим *тождество*

$$\sum a_{ij}{}'x_ix'_j = \sum a_{ij}{}^0x'_ix'_j. \tag{4}$$

Сравнивая в тождестве (4) коэффициенты при одинаковых буквенных выражениях, получим

$$a^0_{ii} = a_{ii}{}', \qquad a_{ij}{}^0 + a_{ji}{}^0 = a_{ij}{}' + a_{ji}{}'.$$

Но мы знаем, что при когредиентном преобразовании симметрическая билинеарная форма обращается также в симметрическую; тоже самое будет иметь, очевидно, место и для квадратичной формы; следовательно,

$$a_{ij}{}^0 = a_{ji}{}^0, \qquad a_{ij}{}' = a_{ji}{}'.$$

Итак окончательно,

$$a_{ij}{}^0 = a_{ij}{}'.$$

Мы пришли таким образом к теореме:

Полярная форма есть абсолютный ковариант квадратичной формы и двух точек $(y_1, y_2, \ldots, y_n)$ *и* $(z_1, z_2, \ldots, z_n)$.

Двойная точка квадратичной формулы

§ 3

Под названием *двойной точки* или *вершины* квадратичной формы $\sum a_{ij}x_ix_j$ разумеется точка $(c_1, c_2, \ldots, c_n)$, для которой не все c обращаются в нуль, но для которой имеет *тождество*

$$\sum a_{ij}x_ic_j = 0. \tag{1}$$

Если равенство (1) есть тождество относительно x_i, то полагая x_ic_i, получим новое тождество

$$\sum a_{ij}c_ic_j = 0,$$

выражающее такое свойство.

Квадратичная форма обращается в нуль во всех ее двойных точках.

Приравнивая нулю в тождеств (1) коэффициенты при всех x_i, получим ряд тождеств

$$a_{11}c_1 + \ldots + a_{1n}c_n = 0$$

$$\ldots\ldots\ldots\ldots\ldots\ldots$$

$$a_{n1}c_1 + \ldots + a_{nn}c_n = 0.$$

Так как определитель последней системы есть дискриминант квадратичной формы, то мы приходим к теореме.

Квадратичная форма может иметь тогда и только тогда двойные точки, если ее дискриминант равен нулю. Пусть r *будет ранг квадратичной формы, то*

она имеет $n - r$ линейно независимых двойных точек. Линейно зависимые от последних точки будут также двойные.

Если дискриминант квадратной формы равен нулю, то точка $A_{i1}, A_{i2}, \ldots, A_{in}$ будет двойная, если не все ее координаты обращаются в нуль. Здесь под A_{ik} мы разумеем алгебраическое дополнение элемента a_{ik} матрицы формы (см. § 41 глава IV).

Разложение на сумму квадратов

§ 4

Всякую квадратичную форму можно представить в виде алгебраической суммы квадратов независимых между собой линейных функций.

Для доказательства этой теоремы мы применим методу Gauss'a, дающую непосредственно искомое разложение. Предположим, что заданная квадратичная форма заключает квадрат какой нибудь переменной, например x_1, так что она имеет вид

$$f = \alpha_1 x_1^2 + \ldots$$

Если x_1 не входить в остальные члены, то мы можем сказать, что первая из искомых линейных функций есть ничто иное как x_1, и таким образом выделен квадрат этой первой функций. Если же первая степень x_1 входить в нескольких членах, то, взяв ее за скобку, получим

$$f = \alpha_1 x_1^2 + 2P_1 x_1 + Q_1, \tag{1}$$

где P_1 линейная форма, а Q_1 квадратичная форма от остальных букв $x_2, x_3, \ldots, x_n$. Тогда форму (1) можно переписать так

$$f = \alpha_1 \left(x + \frac{P_1}{\alpha_1} \right)^2 + Q_1 - \frac{1}{\alpha_1} P_1^2.$$

Обозначая

$$Q_1 - \frac{1}{\alpha_1} P_1^2 = f',$$

получим

$$f = \alpha_1 X_1^2 + f',$$

где

$$X_1 = x + \frac{1}{\alpha_1} P_1$$

есть линейная форма, а f' есть квадратичная форма от $n - 1$ остальных букв $x_2, x_2, \ldots, x_n$.

Совершенно подобным же образом, если в форму f' входит квадрат какой нибудь буквы. например x_2, то будем иметь

$$f' = \alpha_2 X_2^2 + \ldots$$

В этой функции можно выделить квадрат новой линейной функции

$$X_2 = x_2 + \frac{1}{\alpha_2} P_2,$$

где P_2 будет некоторая линейная форма от $n-2$ букв $x_3, x_4, \ldots, x_n$.

Предположим, что, продолжая таким образом далее, мы исчерпали после k выделений квадратов все члены нашей квадратичной формы, тогда мы получаем следующее представление нашей формы в виде алгебраической суммы квадратов линейных функций

$$f = \alpha_1 X_1^2 + \alpha_2 X_2^2 + \ldots + \alpha_k X_k^2.$$

Остается показать, что полученные таким образом линейные функции $X_1, X_2, = ldots, X_k$ суть независимый между собою функции.

В самом деле, по способу последовательного вычисления этих функции мы замечаем, что они имеют такой вид:

$$\begin{aligned}
X_1 = &\quad x_1 + g_1{}^{(2)} + g_1{}^{(3)} + \ldots \\
X_2 = &\qquad\quad x_2 + g_2{}^{(3)} + \ldots \\
X_3 = &\qquad\qquad\quad x_3 + \ldots \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
X_k = &\qquad\qquad\qquad\quad x_k + g_k{}^{(k+1)} x_{k+1} + \ldots
\end{aligned}$$

Независимость этих функций следует из того обстоятельства, что определитель, соответствующий переменным независимыми отличен от нуля, ибо он имеет вид.

$$\begin{vmatrix}
1 & g_1{}^{(2)} & g_1{}^{(3)} & \ldots & \\
0 & 1 & g_2{}^{(2)} & \ldots & \\
\ldots & \ldots & \ldots & \ldots & \ldots \\
0 & 0 & 0 & \ldots & 1
\end{vmatrix}$$

§ 5

Соображения § 4 требуют некоторого добавления, ибо может случиться, что после выделения нескольких квадратов остается такая квадратичная форма, в которой нет ни одного квадрата переменной.

Тогда дальнейшее выделение квадратов будет совершаться несколько иначе. Возьмем квадратичную форму φ, которая не заключает ни одного квадрата, а, значить, каждая буква входит в эту форму в первой степени. Рассмотрим какие нибудь две из независимых переменных формы φ и обозначим их для сокращения x и y; тогда

$$\varphi = axy + Px + Qy + R, \tag{1}$$

где P и Q линейные формы от остальных букв, а R квадратичная форма от тех же букв. Можем написать

$$\varphi = \frac{1}{a}(ax + q)(ay + P) + R - \frac{1}{a}PQ.$$

Нетрудно видеть, что

$$ax + P, \qquad ay + P$$

суть частные производные от функции φ по x и по y, т. е.

$$\varphi'_x = ay + P, \qquad \varphi'_y + ax + Q,$$

значит

$$\varphi = \frac{1}{a}\varphi'_x\varphi'_y + T,$$

где

$$T = R - \frac{1}{a}PQ,$$

или иначе

$$\varphi = \frac{1}{a}\left(\frac{\varphi'_x + \varphi'_y}{2}\right)^2 - \frac{1}{a}\left(\frac{\varphi'_x - \varphi'_y}{2}\right) + T.$$

Итак, в этом случае сразу выделяются два квадрата от линейных функций

$$\frac{\varphi'_x + \varphi'_y}{2}, \qquad \frac{\varphi'_x - \varphi'_y}{2}.$$

Дальнейшее выделение квадратов в квадратичной форме T будет продолжаться уже по указанным приемам. Необходимо только убедиться, что указанное в настоящем параграфе видоизменение способа выделения квадратов оставляет отличным от нуля главный определитель, составленный из коэффициентов первых k переменных. В самом деле, в этом случае получаем две таких горизонтали этого определителя

$$\begin{matrix} 0,\ 0,\ \ldots,\ 0, & \frac{a}{2},\ \frac{a}{2},\ \ldots \\ 0,\ 0,\ \ldots,\ 0, & -\frac{a}{2},\ \frac{a}{2},\ \ldots \end{matrix} \tag{2}$$

Если мы ко второй строке (2) прибавим первую, то получим две таких строки

$$\begin{matrix} 0,\ 0,\ \ldots,\ 0, & \frac{a}{2},\ \frac{a}{2},\ \ldots \\ 0,\ 0,\ \ldots,\ 0,\ 0, & a,\ \ldots \end{matrix}$$

так что и при последнем способе выделения квадратов главный определитель будет отличен от нуля, потому что его можно преобразовать таким образом, что все элементы ниже главной д1огоиали будут равны нулю, а в элементах главной диагонали будут появляться пары отличных от нуля элементов вида $\frac{a}{2}$, a,

Итак, можно считать доказанным утверждение о возможности представить квадратичную форму в виде алгебраической суммы квадратов линейных форм.

Такое представление квадратичной формы является простейшим ее видом и дает возможность доказать некоторые важные предложения, относящиеся к квадратичным формам. Мы остановимся на нескольких самых важных теоремах такого рода.

§ 6

Если квадратичная форма раскладывается на k квадратов независимых между собою функций, то ранг дискриминанта должен равняться числу k.

В самом деле, пусть

$$f = \alpha_1 X_1^2 + \alpha_2 X_2^2 + \ldots + \alpha_k X_k^2, \tag{1}$$

где

$$\begin{aligned} X_1 &= b_1{}^{(1)} x_1 + b_1{}^{(2)} x_2 + \ldots + b_1{}^{(k)} x_k + \ldots \\ X_2 &= b_2{}^{(1)} x_1 + b_2{}^{(2)} x_2 + \ldots + b_2{}^{(k)} x_k + \ldots \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ X_k &= b_k{}^{(1)} x_1 + b_k{}^{(2)} x_2 + \ldots + b_k{}^{(k)} x_k + \ldots \end{aligned} \tag{2}$$

Если функции (2) независимы, то главный определитель этих функций должен быть порядка k. Пусть переменный независимые так обозначены, что этот главный определитель будет определитель, составленный из коэффициентов при k первых буквах, т. е.

$$D = \begin{vmatrix} b_1{}^{(1)} & b_1{}^{(2)} & \ldots & b_1{}^{(k)} \\ \ldots & \ldots & \ldots & \ldots \\ b_k{}^{(1)} & b_k{}^{(2)} & \ldots & b_k{}^{(k)} \end{vmatrix}$$

Подставляем выражения форм (2) в функцию (1) и составляем выражения для частных производных от формы f:

$$\begin{aligned} f_1 = &\quad \alpha_1 b_1{}^{(1)} X_1 + \alpha_2 b_2{}^{(1)} X_2 + \ldots + \alpha_k b_k{}^{(1)} X_k, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ f_k = &\quad \alpha_1 b_1{}^{(k)} X_1 + \alpha_2 b_2{}^{(k)} X_2 + \ldots + \alpha_k b_k{}^{(k)} X_k, \\ f_{k+1} = &\quad \alpha_1 b_1{}^{(k+1)} X_1 + \alpha_2 b_2{}^{(k=1)} X_2 + \ldots + \alpha_k b_k{}^{(k+1)} X_k, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ f_n = &\quad \alpha_1 b_1{}^{(n)} X_1 + \alpha_2 b_2{}^{(n)} X_2 + \ldots + \alpha_k b_k{}^{(n)} X_k, \end{aligned}$$

Последние формулы показывают, что среди n частных производных $f_1, f_2, \ldots,$ f_n будет не больше k независимых между собой, ибо все эти частные производные выражаются линейно через k переменных

$$X_1,\ X_2,\ \ldots,\ X_k;$$

число же независимых функций, как мы видели раньше, не может превосходить числа переменных независимых.

Нетрудно видеть, что за независимые между собою частные производные можно будет принять функций

$$f_1,\ f_2,\ \ldots,\ f_k, \tag{3}$$

ибо будет отличен от нуля определитель, составленный из коэффициентов этих функций при независимых переменных $X_1, X_2, \ldots, X_k$. Этот определитель, очевидно, равен

$$\alpha_1 \alpha_2 \cdots \alpha_k D \neq 0,$$

значить, можно будет выразить буквы $X_1, X_2, \ldots, X_k$ линейным образом через $f_1, X_2, \ldots, f_k$. Подставлял полученные выражения в следующие функции

$$f_{k+1},\ f_{k+2}, \ldots,\ f_n,$$

мы выразим окончательно все частные производные через k независимых между собою функций (3).

Итак, очевидно, что система частных производных имеет ранг k, что и требовалось доказать.

§ 7

Из теоремы предыдущего параграфа следует такое предложение:

Если дискриминант формы отличен от нуля, то форма раскладывается на n квадратов независимых между собою линейных функций, если n есть число всех независимых переменных.

Кроме того:

Если дискриминант равен пулю, то число независимых квадратов должно быть меньше числа независимых переменных, и квадратов будет столько, каков ранг квадратичной формы.

Как частный случай этой теоремы является теорема о дискриминанте тройничной квадратичной формы, играющая важную роль в Аналитической Геометрии при рассмотрений лиши 2-го порядка.

Там доказывается теорема, что равенство нулю дискриминанта есть необходимое и достаточное условие, чтобы линия 2-го порядка обращалась в систему двух прямых.

В самом деле, если мы перейдем к однородным координатам, то уравнение линии 2-го порядка будет

$$f(x, y, z) = 0,$$

где первая часть есть тройничная квадратичная форма от однородных координат x, y. z. Если дискриминант не равен нулю, то первая часть раскладывается на 3 квадрата; если же дискриминант равен нулю, то число квадратов будет меньше: или один, или два, так что наше уравнение может быть переписано в одном из следующих видов:

$$X_1^2 = 0,$$
$$\alpha_1 X_1^2 + \alpha_2 X_2^2 = 0,$$

но второе уравнение можно переписать так

$$(\sqrt{\alpha_1} X_1 + i\sqrt{\alpha_2} X_2)(\sqrt{\alpha_1} X_1 - i\sqrt{\alpha_2} X_2) = 0,$$

следовательно, в обоих случаях форма раскладывается на два линейных множителя, т. е., другими словами, получается система двух прямых.

§ 8

Если квадратичная форма с вещественными коэффициентами от n переменных независимых раскладывается на n квадратов независимых линейных функций

$$f = \alpha_1 X_1^2 + \alpha_2 X_2^2 + \ldots + \alpha_n X_n^2,$$

и эти квадраты имеют коэффициенты $\alpha_1, \alpha_2, \ldots, \alpha_n$ одного знака, то эта форма сохраняет общий знак при всех вещественных значениях независимых переменных и может обращаться в нуль, когда обращаются сразу в нуль все эти квадраты, т. е.

$$X_1 = 0, \quad X_2 = 0, \ \ldots, \ X_n = 0. \tag{1}$$

Нетрудно видеть, что равенства (1) имеют место, когда все переменные обращаются в нуль

$$x_1 = 0, \quad x_2 = 0, \ \ldots, \ x_n = 0,$$

ибо определитель, составленный из коэффициентов не нуль.

Будем этот очевидный случай обращения в нуль формы при равных нулю значениях всех переменных независимых отбрасывать, так что, если мы будем говорить, что некоторая форма обращается в нуль, то под этим будем разуметь тот случай, когда форма делается равной нулю при отличных от нуля значениях x независимых переменных. При такой оговорке мы введем следующие названия: будем форму называть *определенною*, если она сохраняет свой знак, не обращаясь в нуль; будем форму называть *полуопределенною*, если она сохраняет свой знак, но может обращаться в нуль; и, наконец, назовем форму *неопределенною*, если она может менять свой знак.

Определенные формы мы разобьем в свою очередь на формы *положительные* и *отрицательные* в зависимости от того, какой знак эта форма сохраняет. Очевидно, что форма будет определенною, если все коэффициенты α_i одного знака и число квадратов есть n; форма будет полуопределенною, если все коэффициенты одного знака, но число квадратов меньше n, потому что в этом случай все эти квадраты можно будет обратить в нуль, оставляя некоторые переменные независимые совершенно произвольными; и, наконец, форма будет неопределенною, если коэффициенты α_i будут разных знаков, потому что в этом случай мы получим положительное значение для формы, если приравняем нулю все квадраты с отрицательными коэффициентами, и получим отрицательное значение, если приравняем нулю все квадраты с положительными коэффициентами.

§ 9

Относительно вещественных форм имеет место замечательный закон, названный Sylvester-ом законом инерции.

Если мы назовем через r число квадратов с положительными коэффициентами неопределенной формы, а через s число квадратов с отрицательными коэффициентами той же формы, то эти числа остаются неизменными, каким бы образом ни раскладывать форму на сумму k квадратов.

Допустим обратное, а именно, что форма разлагается двумя способами на k квадратов

$$(1)\qquad \begin{aligned} &\alpha_1 X_1^2 + \ldots + \alpha_r X_r^2 - \alpha'_1 X_1'^2 - \alpha'_2 X_2'^2 - \ldots - \alpha'_s X_s'^2 = \\ &= \beta_1 Y_1^2 + \ldots + \beta_\rho Y_\rho^2 - \beta'_1 Y_1'^2 - \beta'_2 Y_2'^2 - \ldots - \beta'_\sigma Y_\sigma'^2 \quad , \end{aligned}$$

причем все коэффициенты α, α', β, β' положительные числа, а

$$r < \rho, \quad r + s = k, \quad \rho + \sigma = k, \quad k \leq n.$$

Рассмотрим уравнения

$$(2)\qquad \begin{aligned} &X_1 = 0, \quad X_2 = 0, \ \ldots, \ X_r = 0 \\ &Y'_1 = 0, \quad Y'_2 = 0, \ \ldots, \ Y'_\sigma = 0. \end{aligned}$$

Если мы обозначим через n общее число первоначальных независимых x_i, линейными формами которых являются все X, X', Y, Y', то из неравенств

$$r + \sigma < \rho + \sigma \leq n$$

замечаем, что линейные уравнения (2) оставляют произвольными по крайней мере $n - r - \sigma$ переменных независимых x_i. Подставляя в тождество (1) значения x_i, удовлетворяющие уравнениям (2), получаем

$$\beta_1 Y_1^2 + \ldots + \beta_\rho Y_\rho^2 = -\alpha'_1 X_1'^2 - \alpha'_2 X_2'^2 - \ldots - \alpha'_s X_s'^2,$$

которое не иначе возможно, если все Y и X' равны нулю,

Итак, уравнения

$$(3)\qquad Y_1 = 0, \ \ldots, \ Y_\rho = 0$$

должны удовлетворяться при всех значениях x_i, удовлетворяющих уравнениям (2). Обозначим через q число остающихся независимыми из x_i. Все линейные функции Y, Y' суть независимы между собой, значит, система уравнений

$$Y'_1 = 0, \ \ldots, \ Y'_\sigma = 0; \ Y_1 = 0, \ \ldots, \ Y_\rho = 0$$

имеем ранг, точно равный $\rho + \sigma$, значит

$$q \leq n - \rho - \sigma.$$

С другой стороны самое общее решение системы (2) будет иметь не менее $n - r - \sigma$ независимых величин, откуда

$$n - r - \sigma \leq n - \rho - \sigma,$$

и мы приходим к неравенству $\rho \leq r$, находящемуся в противоречии с допущенным $r < \rho$.

§ 10

Если обозначить через P число положительных квадратов, а через N число отрицательных квадратов, то очевидно, что эти два числа суть арифметические инварианты относительно линейных преобразований с вещественными коэффициентами.

Сумма этих чисел равна общему числу квадратов, то есть рангу r формы

$$P + N = r.$$

Введем по примеру Frobenius'a в рассмотрение еще их разность

$$P - N = s,$$

которую будем называть *сигнатурой* формы.

Ранг r есть арифметический инвариант формы по отношению к всевозможным как вещественным, так и мнимым неособенным преобразованиям; сигнатура есть инвариант по отношению к вещественным неособенным преобразованиям.

§ 11

Будем рассматривать квадратичные формы в общем виде, не ограничиваясь вещественными числами. Если, ранг формы есть r, то можно, как мы видели, привести ее к виду

$$\alpha_1 X_1^2 + \alpha_2 X_2^2 + \ldots + \alpha_r X_r^2. \tag{1}$$

Эти функций $X_1, X_2, \ldots, X_r$ независимы между собой, т. е. уравнения

$$X_1 = 0, \quad X_2 = 0, \ \ldots, \ X_r = 0 \tag{2}$$

можно решить относительно r величин x_i, выбирая приличным образом обозначения, мы можем сказать, что уравнения (2) решаются относительно

$$x_1, \quad x_2, \ \ldots, \ x_r.$$

Пусть функций X имеют вид

$$\begin{aligned} X_1 &= a_1{}^{(1)}x_1 + \ldots + a_r{}^{(1)}x_r + a_{r+1}^{(1)}x_{r+1} + \ldots + a_n{}^{(1)}x_n \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ X_r &= a_1{}^{(r)}x_1 + \ldots + a_r{}^{(r)}x_r + a_{r+1}^{(r)}x_{r+1} + \ldots + a_n{}^{(r)}x_n \end{aligned}$$

Их главный определитель

$$A = \begin{vmatrix} a_1{}^{(1)} & \ldots & a_r{}^{(1)} \\ \ldots & \ldots & \ldots \\ a_1{}^{(r)} & \ldots & a_r{}^{(r)} \end{vmatrix}$$

не равен нулю.

Можно сказать, что заданная форма приводится к виду (1), представляющему сумму квадратов, при помощи такого *неособенного* преобразования

$$\begin{aligned}
X_1 &= a_1{}^{(1)}x_1 + \ldots + a_r{}^{(1)}x_r + \ldots \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
X_r &= a_1{}^{(r)}x_1 + \ldots + a_r{}^{(r)}x_r + \ldots \\
X_{r+1} &= x_{r+1} \\
&\ldots\ldots\ldots\ldots \\
X_n &= x_n,
\end{aligned}$$

где $X_i = x_i$ при $i > r$.

Очевидно, что от вида (1) можно перейти к виду

$$k_1 X_1'^2 + k_2 X_2'^2 + \ldots + k_r X_r'^2,$$

где $k_1, \ldots, k_r$ произвольно выбранные числа, при помощи преобразования

$$X_1 = \sqrt{\frac{k_1}{\alpha_1}}X_1',\ \ldots,\ X_r = \sqrt{\frac{k_r}{\alpha_r}}X_r' + \quad X_{r+1} = X_{r+1}',\ \ldots,\ X_n = X_n'.$$

Приходим окончательно к теореме.

Всякая квадратичная форма ранга r приводится при помощи неособенного преобразования к нормальному виду

$$x_1^2 + x_2^2 + \ldots + x_r^2;$$

ибо можно положить $k_1 = k_2 = \ldots = k_r = 1$.

Приспособляясь к терминологии главы VI, можно будет высказать теорему.

Две квадратичный формы тогда и только тогда эквивалентны по отношение к группе неособенных линейиых преобразований, когда они имеют один и тот же ранг.

Ибо они сводятся к одному и тому же нормальному виду.

§ 12

Рассмотрим квадратичную форму *буквенного* вида, т. е. такую, в которой все коэффициенты суть переменные независимые между собой. В этом случай соображения § 5 но имеют места и, следовательно, следуя § 4, мы получим

$$f = \alpha_1 X_1^2 + \alpha_2 X_2^2 + \ldots + \alpha_n X_n^2, \tag{1}$$

где

$$\begin{aligned}
x_1 &= c_{11}x_1' + \ldots + c_{1n}x_n' \\
&\ldots\ldots\ldots\ldots\ldots\ldots \\
x_n &= c_{n1}x_1' + \ldots + c_{nn}x_n'
\end{aligned} \tag{2}$$

Главный определитель системы (2) равен 1.

Дискриминант Δ_n формы f будет равен, очевидно, произведению $\alpha_1\alpha_2\cdots\alpha_n$; ибо дискриминант относительно переменных $X_1, X_2, \ldots, X_n$ есть как раз произведение $\alpha_1\alpha_2\cdots\alpha_n$, этот же дискриминант надо будет помножить на квадрат определителя преобразования (2).

Итак

$$\Delta_n = \alpha_1\alpha_2\cdots\alpha_n.$$

Если мы оставим отличными от нуля только переменные $x_1, x_2, \ldots, x_{n-i}$, остальные же приравняем нулю

$$x_{n-i+1} = 0, \quad x_{n-i+2} = 0, \ \ldots, \ x_n = 0, \tag{3}$$

то форма приводится к виду

$$f^0 = \alpha_1 X_1^{0\,2} + \ldots + \alpha_{n-i} X_{n-i}^{0\,2}, \tag{4}$$

где X^0 выражает результат подстановки величин (3) в функций X. Обозначим дискриминант формы (4) через Δ_{n-i}. Нетрудно видеть, что этот дискриминант есть минор порядка i от Δ_n, в котором сохранены $n-i$ верхних горизонталей и $n-i$ левых колонн. На основании (4) мы имеем

$$\Delta_{n-i} = \alpha_1\alpha_2\cdots\alpha_{n-i}. \tag{5}$$

Применяя формулу (5) к различным значениям i от $n-1$ до 0, получим

$$\Delta_1 = \alpha_1, \quad \Delta_2 = \alpha_1\alpha_2, \quad \Delta_3 = \alpha_1\alpha_2\alpha_3, \ \ldots, \ \Delta_n = \alpha_1\alpha_2\cdots\alpha_n,$$

откуда

$$\alpha_1 = \Delta_1, \quad \alpha_2 = \frac{\Delta_2}{\Delta_1}, \quad \alpha_3 = \frac{\Delta_3}{\Delta_2}. \ \ldots, \ \alpha_n = \frac{\Delta_n}{\Delta_{n-1}}.$$

Мы получаем следующую, заслуживающую внимания формулу

$$f = \Delta_1 X_1^2 + \frac{\Delta_2}{\Delta_1} X_2^2 + \frac{\Delta_3}{\Delta_2} X_3^2 + \ldots + \frac{\Delta_n}{\Delta_{n-1}} X_n^2. \tag{6}$$

Мы предполагали коэффициенты формы f неопределенными; очевидно, что формула (6) будет оставаться справедливой и в том случай, если коэффициентам первоначального вида формы приданы некоторые численные значения, лишь бы не обращался в нуль ни один определитель

$$\Delta_1, \quad \Delta_2, \quad \Delta_3, \ \ldots, \ \Delta_n.$$

§ 13

Приведем теперь весьма важное замечание относительно преобразования квадратичных форм, принадлежащее Kronecker'y. Обозначим через $f_1, f_2, \ldots, f_n$ частные производные от заданной квадратичной формы f по независимым переменным $x_1, x_2, \ldots, x_n$.

Очевидно, что если ранг квадратичной формы есть r, то независимых между собой частных производных будет равно r; пусть это будут $f_1, f_2, \ldots, f_r$.

Если мы предположим, что система

$$f_1 = 0, \quad f_2 = 0, \ \ldots, \ f_r = 0 \tag{1}$$

решается относительно переменных $x_1, x_2, \ldots, x_r$, то для них получаются выражения через остальные $x_{r+1}, x_{r+2}, \ldots, x_n$, которые остаются совершенно произвольными. Дадим этим последним величинам произвольно выбранные значения

$$x_{r+1} = \xi_{r+1}, \quad x_{r+2} = \xi_{r+2}, \ \ldots, \ x_n = \xi_n.$$

Из уравнения (1) получаются значения

$$\xi_1, \quad \xi_2, \ \ldots, \ \xi_r$$

для букв $x_1, x_2, \ldots, x_r$, эти значения суть линейные функций от $\xi_{r+1}, \xi_{r+2}, \ldots, \xi_n$.

Kronecker рассматривает преобразование

$$x_1 = X_1 + \xi_1, \quad x_2 = X_2 + \xi_2, \ \ldots, \ x_r = X_r + \xi_r,$$
$$x_{r+1} = \xi_{r+1}, \quad x_{r+2} = \xi_{r+2}, \ \ldots, \ x_n = \xi_n.$$

Таким образом

$$f(x_1, x_2, \ldots, x_n) = f(X_1 + \xi_1, X_2 + \xi_2, \ldots, X_r + \xi_r, 0 + \xi_{r+1}, 0 + \xi_{r+2}, \ldots, 0 + \xi_n).$$

Применяя формулу Taylor'a, получим

$$f(x_1, x_2, \ldots, x_n) == f(X_1, X_2, \ldots, X_r, 0, 0, \ldots, 0). \tag{2}$$

В самом деле, величины ξ_i обращают в нуль все частные производные $f_1, f_2, \ldots, f_n$, ибо эти величины обращают в нуль частные производные $f_1, f_2, \ldots, f_r$ (уравнения (1)), остальные же частные производные $f_{r+1}, \ldots, f_n$ также обращаются в нуль, ибо они выражаются линейно через $f_1, f_2, \ldots, f_r$. Значит, обращаются независимо от значений $X_1, X_2, \ldots, X_n$ в нуль оба выражения

$$X_1 f_1 + X_2 f_2 + \ldots + X_r f_r,$$
$$f = \frac{1}{2} \ (x_1 f_1 + x_2 f_2 + \ldots + x_n f_n).$$

Итак, формула Kronecker'a (2) оказывается справедливою.

§ 14

В связи с разложением квадратичной формы на сумму квадратов, можно показать, что дискриминант есть единственный независимый инвариант квадратичной формы. Мы докажем теорему.

Всякий целый рациональный инвариант квадратичной формы отличается постоянным множителем от степени дискриминанта.

Мы ограничимся рассмотрением случая, когда дискриминант не равен нулю.

Обозначим через c определитель преобразования заданной формы $\sum a_{ij} x_i x_j$ в сумму квадратов $x_1'^2 + x_2'^2 + \ldots + x_n'^2$.

Пусть рассматривается целый рациональный инвариант

$$I(a_{11}, \ldots, a_{nn}) \tag{1}$$

формы $\sum a_{ij}x_ix_j$, имеющий вес k. Обозначим через I_0 значение того-же инварианта для преобразованной формы. I_0 получается из выражения (1), если подставить $a_{ii} = 1$, $a_{ij} = 0$. По свойству инварианта получаем

$$I_0 = c^k I(a_{11}, \ldots, a_{nn}). \tag{2}$$

Но мы знаем, что дискриминант $A = |a_{ij}|$ формы есть инвариант веса 2, и кроме того, что A обращается в 1 для преобразованной формы $x_1'^2 + x_2'^2 + \ldots + x_n'^2$; то получаем

$$1 = c^2 A. \tag{3}$$

Возвышая (2) в квадрат и (3) в степень k, и исключая c, получим

$$[I(a_{11}, \ldots, a_{nn})]^2 = I_0^2 A^k. \tag{4}$$

Последнее равенство есть тождество, как следствие двух тождеств. Тождество (4) имеет степень k относительно a_{11}. Очевидно, что эта степень должна быть четная, то есть $k = 2l$. Извлекая корень квадратный, мы получаем одно из двух

$$I(a_{11}, \ldots, a_{nn}) = I_0 A^l, \qquad I(a_{11}, \ldots, a_{nn}) = -I_0 A^l,$$

и теорема доказана.

Эта теорема показывает, что полной системой инвариантов в смысле § 28 главы VI является для квадратичной формы один только дискриминант.

§ 15

Квадратичная форма будет *приводимою*, если она раскладывается на два линейных множителя

$$\sum a_{ij}x_ix_j = (b_1x_1 + b_2x_2 + \ldots + b_nx_n)(c_1x_1 + c_2x_2 + \ldots + c_nx_n).$$

Эти множители могут быть одинаковы, тогда форма будет равна квадрату линейной формы

$$\sum a_{ij}x_ix_j = (b_1x_1 + b_2x_2 + \ldots + b_nx_n)^2.$$

Так как в первом случай форма раскладывается на два квадрата

$$\left\{\frac{b_1 + c_1}{2}x_1 + \ldots\right\}^2 - \left\{\frac{b_1 - c_1}{2}x_1 + \ldots\right\}^2,$$

а во втором на один, то мы получаем теорему.

Необходимыми и достаточным условием приводимости формы является требование, чтобы ранг не превосходил числа 2.

§ 16

Придадим изложение геометричсский характер.[23] Будем рассматривать *сверхповерхность второго порядка*, определяемую уравнением

$$\sum a_{ij}x_ix_j = 0 \tag{1}$$

в пространстве $n-1$ измерения, в котором каждая точка определяется n однородными координатами

$$(x_1, x_2, \ldots, x_n). \tag{2}$$

Возьмем еще одну точку

$$(y_1, y_2, \ldots, y_n) \tag{3}$$

пространства.

Координаты точки, делящей в отношении λ расстояние между точками (2) и (3), будут

$$(y_1 + \lambda x_1, y_2 + \lambda x_2, \ldots, y_n + \lambda x_n). \tag{4}$$

Если $\lambda > 0$, то точка (4) лежит на прямой, соединяющей точки (2) и (3) внутри отрезка между этими точками.

Так например, при $\lambda = 1$ получается середина отрезка.

Чтобы найти точки, в которых пересекается сверхповерхность (1) с прямою, соединяющею точки x_i и y_i, надо будет найти λ из квадратного уравнения

$$\sum a_{ij}(y_i + \lambda x_i)(y_j + \lambda x_j) = 0,$$

которое можно переписать еще так

$$\sum a_{ij}y_iy_j + 2\lambda \sum a_{ij}y_ix_j + \lambda^2 \sum a_{ij}x_ix_j = 0. \tag{5}$$

Если точка y лежит на сверхповерхности (1), то $\sum a_{ij}y_iy_j = 0$, и уравнение (5) имеет один корень $\lambda = 0$. Если кроме того еще имеет место равенство

$$\sum a_{ij}y_ix_j = 0, \tag{6}$$

то уравнение (5) имеет двухкратный корень $\lambda = 0$. В этом случае прямая, соединяющая точки x_i и y_i, касается в точке y_i с (1). Уравнение (6), когда заданы координаты y_i точки, лежащей на сверхповерхности (1), будет уравнением так называемой *касательной гиперплоскости*; точка y_i будет называться ее *точкой касания*. Первую часть уравнения касательной сверхплоскости составляет, как мы видим, полярная форма.

[23]Можно сравнить Д. Граве. Основы Аналитической Геоыетрии.Часть I глава XII.

Введем подобно тому, как это делается для трехмерного пространства, *плоскостные координаты* $u_1 u_2, \ldots, u_n$.

Пусть рассматривается уравнение

$$u_1 x_1 + u_2 x_2 + \ldots + u_n x_n = 0 \tag{1}$$

некоторой переменной сверхплоскости. Меняя параметры $u_1, u_2, \ldots, u_n$, заставим сверхплоскость менять свое положение в пространстве.

Если мы желаем рассматривать сверхповерхность $\S \sum a_{ij} x_i x_j = 0$, как огибающую плоскость (1), то мы должны выразить условие того, что уравнение (1) есть уравнение касательной сверхплоскости; сравнивая с уравнением (6) § 16, мы получаем следующдй ряд уравнений

$$\begin{aligned} a_{11} y_1 + a_{21} y_2 + \ldots + a_{n1} y_n &= \lambda u_1 \\ a_{12} y_1 + a_{22} y_2 + \ldots + a_{n2} y_n &= \lambda u_2 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & \\ a_{1n} y_1 + a_{2n} y_2 + \ldots + a_{nn} y_n &= \lambda u_n, \end{aligned} \tag{2}$$

где λ произвольный множитель пропорциональности. Если к уравнениям (2) мы присоединим еще уравнение

$$u_1 y_1 + u_2 y_2 + \ldots + u_n y_n = 0, \tag{3}$$

выражающее, что точка касания $(y_1, y_2, \ldots, y_n)$ лежит на касательной сверхплоскости; то, исключая из $n+1$ уравнений (2) и (3) и $n+1$ однородно входящих величин $y_1, y_2, \ldots, y_n, \lambda$, получим уравнение сверхповерхности второго порядка

$$\begin{vmatrix} a_{11} & a_{21} & \ldots & a_{n1} & u_1 \\ a_{12} & a_{22} & \ldots & a_{n2} & u_2 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ a_{1n} & a_{2n} & \ldots & a_{nn} & u_n \\ u_1 & u_2 & \ldots & u_n & 0 \end{vmatrix} = 0 \tag{4}$$

в плоскостных координатах.

Мы видим, что в левой части уравнения (4) находится квадратичная форма

$$-\sum A_{ij} u_i u_j \tag{5}$$

относительно плоскостных координат u_i, коэффициентами которой являются алгебраические дополнения A_{ij} соответственных коэффициентов a_{ij} первоначальной формы.

Форма (5) называется *союзною* относительно первоначальной формы

$$\sum a_{ij} x_i x_j.$$

Матрица союзной формы будет взаимною (см. § 39 главы IV) относительно первоначальной.

§ 18

Рассмотрим линейное преобразование

$$\xi = \mathfrak{a}(\xi'),$$

тогда обратное преобразование

$$\xi' = \mathfrak{a}^{-1}(\xi)$$

приводит к обратной матрице

$$\mathfrak{a}^{-1} = \left\| \begin{matrix} \dfrac{A_{11}}{a} & \dots & \dfrac{A_{n1}}{a} \\ \dots & \dots & \dots \\ \dfrac{A_{1n}}{a} & \dots & \dfrac{A_{nn}}{a} \end{matrix} \right\|, \quad \text{где} \quad a = |\mathfrak{a}|.$$

Квадратичная форма с обратной матрицей носить название *обратной* квадратичной формы. Принимая во внимание предположение о симметричности матрицы формы, мы приходим к заключению, что обратная матрица отличается лишь множителем $\dfrac{1}{a}$ от союзной.

Квадратичная форма с неособенной матрицей может быть преобразована в обратную при помощи неособенного преобразования:

$$x_i' = a_{i1}x_1 + \ldots + a_{in}x_n \qquad (i = 1, 2, \ldots, n). \tag{1}$$

В самом деле, мы имеем тождество

$$\sum a_{ij}x_ix_j = \sum x_ix_i'. \tag{2}$$

Обращая преобразование (1), получаем

$$x_i = \frac{1}{a}\,[A_{i1}x_1' + \ldots + A_{in}x_n'];$$

откуда, подставляя в (2), находим

$$\sum a_{ij}x_ix_j = \frac{1}{a}\,\sum A_{ij}x_i'x_j'.$$

Если заданная квадратная форма вещественна, то вещественно также и преобразование (1) и, следовательно, *сигнатура обратной формы одинакова с сигнатурой заданной.*

§ 19

Теорема. *Союзная форма* $\sum A_{ij}u_iu_j$ *есть инвариант веса* 2 *системы двух форм*

$$\sum a_{ij}x_ix_j, \qquad \sum u_ix_i.$$

Рассмотрим квадратичную форму

$$\sum a_{ij}x_ix_j + 2t(u_1x_1 + u_2x_2 + \ldots + u_nx_n)$$

от переменных независимых $x_1, x_2, \ldots, x_n, t$.

Ее дискриминант равен как раз союзной форме

$$\begin{vmatrix} a_{i1} & \ldots & a_{1n} & u_1 \\ \ldots & \ldots & \ldots & \ldots \\ a_{n1} & \ldots & a_{nn} & u_n \\ u_1 & \ldots & u_n & 0 \end{vmatrix}. \tag{1}$$

Пусть преобразование координат x_i будет

$$\begin{aligned} x_1 &= c_{11}x'_1 + \ldots + c_{1n}x'_n, \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ x_n &= c_{n1}x'_1 + \ldots + c_{nn}x'_n. \end{aligned} \tag{2}$$

Если мы добавим еще новое равенство

$$t = t', \tag{3}$$

то преобразовало $n+1$ букв $x_1, \ldots, x_n, t$, выражаемое формулами (2) и (3), имеет тот же определитель c, что и преобразование (2), рассматриваемое отдельно.

Дискриминант же (1) приобретает множитель c^2 при преобразованиях (2), (3) н теорема доказана.

Можно составить инвариант веса 2 для квадратичной формы $\sum a_{ij}x_ix_j$ и ряда линейных форм

$$\sum u_ix_i, \quad \sum v_ix_i, \ \ldots, \ \sum w_ix_i.$$

Этот инвариант будет иметь вид

$$\begin{vmatrix} a_{11} & \ldots & a_{1n} & u_1 & v_1 & \ldots & w_1 \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots \\ a_{n1} & \ldots & a_{nn} & u_n & v_n & \ldots & w_n \\ u_1 & \ldots & u_n & 0 & 0 & \ldots & 0 \\ v_1 & \ldots & v_n & 0 & 0 & \ldots & 0 \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots \\ w_1 & \ldots & w_n & 0 & 0 & \ldots & 0 \end{vmatrix}$$

§ 20

Пусть r будет ранг заданной формы $\sum_1^n a_{ij}x_ix_j$, а R ранг союзной $\sum_1^n A_{ij}u_iu_j$.

Если $r = n$, то дискриминант a формы заданной не равен нулю, а следовательно, не равен нулю также и дискриминант союзной формы, ибо он как взаимный определитель, равен a^{n-1}; значит $R = n$.

Если $r = n - 1$, то взаимная матрица $\|A_{ij}\|$ не равна нулю. Она имеет ранг $R = 1$, ибо пропадают на основании § 41 главы IV все миноры, составленные из двух горизонталей и колонн.

Наконец, если $r < n-1$, то $R = 0$.

Если $r = n-1$, то союзная форма, будучи первого ранга, должна при разложении на сумму квадратов давать один только квадрат; и мы приходим к теореме.

Если квадратная форма от n переменных имеет ранг $n-1$, то союзная форма есть квадрат линейной.

Полагая

$$\sum A_{ij}u_iu_j = \left(\sum \alpha_i u_i\right)^2 = \sum \alpha_i\alpha_j u_iu_j,$$

получаем

$$A_{ij} = \alpha_i\alpha_j.$$

Все α_i не могут равняться нулю. Пусть $\alpha_h \neq 0$, тогда $A_{hh} = \alpha_h^2 \neq 0$ и следовательно, не уничтожаются все величины $(A_{h1}, A_{h2}, \ldots, A_{hn})$. На основании § 3 точка $(A_{h1}, A_{h2}, \ldots, A_{hn})$ или, что одно и тоже точка $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ будет двойною для первоначальной квадратичной формы.

Эквивалентность форм

§ 21

В предыдущей главе было установлено понятие о предметах эквивалентных по отношению к некоторой группе преобразований. Между прочим мы можем заметить, что все квадратичные формы, имеющие один и тот же ранг, эквивалентны по отношению к группе неособенных линейных преобразований. Подобным же образом эквивалентны по отношению к вещественным линейным преобразованиям формы, имеюшие одинаковые ранг и сигнатуру.

Эквивалентные между собой предметы образуют так называемый класс, таким образом мы приходим к понятию о классе квадратичных форм.

Во многих задачах полезно установить для каждого класса предметов его представителя. Стоит припомнить, как в элементарной теории чисел[24] берется за представителя класса чисел по модулю вычетов этого класса.

Понятие о классе квадратичных форм зависит всецело от той группы линейных преобразований, которая кладется в основу исследования; чем эта группа шире, тем проще решается вопрос о выборе представителя класса. Так например, задача делается совершенно тривиальной, если рассматривать неособенные линейные преобразования самого общего вида, причем допустим комплексные числа. Тогда класс квадратичных форм завесит только от ранга r, так что за представительницу класса можно принять форму

$$x_1^2 + x_2^2 + \ldots + x_r^2, \tag{1}$$

все формы класса приводятся к виду (1) при помощи некоторого линейного преобразования.

Форма (1) носить название *канонической* или *приведенной* формы класса.

[24]См. Д. Граве. Элементарный курс теории чисел. 1913. § 6. Глава III.

§ 22

Особенно важное научное значение имеет так называемая *арифметическая теория* квадратичных форм. В этой теории обыкновенно рассматриваются формы $\sum a_{ij}x_ix_j$, коэффициенты которых a_{ij} суть целые числа; переменным независимым даются также целые значения. Линейные преобразования рассматривают также только такие, которые имеют целые коэффициенты.

Началом арифметической теории форм явились вопросы теории чисел о представлении целых чисел квадратичными формами. В этих вопросах было важным рассматривать преобразования с целыми коэффициентами, определитель которых равен ± 1, ибо, очевидно, что эквивалентные относительно таких преобразований квадратичные формы представляют при целых значениях переменных x_i одинаковые числа. В этом легко убедиться, если заметить, что для таких преобразований обратное преобразование имеет также целые коэффициенты. Формы называются proprie-эквивалентными, если определитель всякого преобразования, переводящего одну в другую, есть $+1$ и improprie-эквивалентными при определителе -1.

Понятие об эквивалентности форм в арифметическом смысле слова установлено Lagrange'ем, при чем ему принадлежит весьма важное понятие о приведенной форме,[25] как представительнице класса. Ввиду важности этого понятия а также ввиду замечательных следствий и обобщений я должен сказать два слова о теории Lagrange'a.

§ 23

Ограничимся случаем бинарных квадратичных форм, как это сделано у Lagrange'a.

Назовем *приведенною* форму

$$ax^2 + 2bxy + cy^2, \tag{1}$$

в которой целые коэффициенты a, b, c удовлетворяюсь неравенствам

$$|2b| \leq |a|, \qquad |2b| \leq |c|. \tag{2}$$

Возможность привести форму (1), не удовлетворяющую неравенствам (2), к виду, коэффициенты которого уже удовлетворяют неравенствам (2), основывается на следующих соображениях.

Если форма (1) не приведенная, то сделаем преобразование переменных

$$\begin{aligned} x &= x' - my', \\ y &= y', \end{aligned} \tag{3}$$

определитель которого есть

$$\begin{vmatrix} 1 & -m \\ 0 & 1 \end{vmatrix} = 1.$$

Новая форма будет

$$a'x'^2 + 2b'x'y' + c'y'^2,$$

где

$$a' = a, \quad b' = b - am, \quad c' = c - 2bm + am^2.$$

[25] Lagrange. Recherches d'arithmétigue. Nouv. Mém. de Berlin 1773, 1775.

Названия переменных x и y могут быть выбраны так, что абсолютная величина a меньше абсолютной величины $2b$. Если мы возьмем за b' абсолютно малый вычет числа b по модулю a, то будем иметь

$$|2b'| < |a|.$$

Форма (1) предполагается неприведенною, значит, наверно $|2b| > |a|$, значит

$$|2b'| < |2b|;$$

итак, если форма (1) неприведенная, то при помощи преобразования (3) мы уменьшили коэффициент при xy по абсолютной его величине.

Если в полученной нами форме этот коэффициент превосходит один из коэффициентов крайних членов, мы со снова также преобразовываем, как преобразовали $ax^2 + 2bxy + cy^2$ и будем повторять это преобразование до тех пор, пока не получим форму, где такое преобразование невозможно и, следовательно, средний коэффициент не превосходит ни одного из крайних.

При рассмотрении вычисляемых таким образом приведенных форм получается большая разница в изучении двух случаев, когда дискриминант $b^2 - ac$ *отрицательный* и когда он *положительный*.

Отсылая читателя к моему курсу теории чисел, где в главе XI вопрос о приведенных формах изложен подробно, я должен обратить внимание на то обстоятельство, что C. Fr. Gauss в бессмертной книге *Disguisitiones arithmeticae* видоизменил определение приведенной формы в случае положительного дискриминанта $b^2 - ac$. В моей книге я придерживался идей Gauss'a. В добавлении к там сказанному я хочу обратить внимание на замечательное геометрическое толкование приведенных форм метода Gauss'a.

Пусть вещественные коэффициенты a, b, c квадратичной формы

$$ax^2 + 2bxy + cy^2 \tag{1}$$

рассматриваются как прямоугольные координаты трехмерного пространства; тогда каждой форме (1) соответствует точка пространства и обратно.

Все формы (1) данного дискриминанта D соответствуют точкам *гиперболоида*, определяемого уравнением

$$y^2 - xz = D, \tag{2}$$

если перейдем от обозначения a, b, c координат трехмерного пространства, к обыкновенному обозначению x, y, z.

При $D < 0$ гиперболоид будет двуполый, а при $D > 0$ однополый.

Строим восемь прямолинейных образующих однополого гиперболоида (при $D > 0$), проходящих через четыре вершины эллипса перехвата (горла). Эти образующие замыкают на поверхности эллипсоида четыре куска поверхности конечных размеров. Каждый из этих кусков ограничен косым четыреугольником, сторонами которого являются части построенных прямолинейных образующих.

Приведенный в смысле Gauss'a квадратичных формы соответствуют точкам, лежащим внутри этих четырех кусков.

Мысли Lagrange'a получили в книге Gauss'a развитие, поражающее по богатству и глубине новых идей. Книга Gauss'a была откровением, из которого в продолжении столетия наука черпает материал для новых обобщений. Появилась арифметическая теория алгебраических форм произвольной степени и с произвольным числом переменных, первой главой которой является теория Gauss'a бинарных квадратичных форм.

Обобщение во что бы то ни стало, обобщение, не оправдываемое какими либо более серьезными мотивами, не есть цель науки. Целью науки являются такие обобщения, которые вызваны действительно научною потребностью. Эта потребность может быть двух категорий: или потребность вызывается желанием решать те или другие конкретные задали, или же потребность завершить ясное представление о существующих закономерностях изучением предмета еще не ясно представляемого, представляющего таким образом пробел в общей картине знания. Таким образом под влиянием действительных научных потребностей в арифметической теории форм обобщение идей Gauss'a пошло главным образом в двух направлениях: 1) в направлении изучения так называемых *разложимых форм* и 2) в направлены изучения *квадратичных* форм *произвольного* числа переменных.

Под разложимыми формами я разумею здесь форму n-ой степени, которая представляет из себя произведение n линейных форм с иррациональными коэффициентами.

Теория разложимых форм вылилась в замечательную теорию новых чисел, названных *идеальными*.

Как в теории идеальных чисел, так и в арифметической теории квадратичных форм большого числа переменных независимых играет большую роль понятие о *приведенном* предмете некоторого класса эквивалентных предметов.

Установлением этого понятая для квадратичных форм наука обязана после Lagrange'a и Gauss'a немецкому математику Seeber'y.[26] Последний показал, что в каждом классе положительных тройничных квадратичных форм существует форма, целые коэффициенты которой удовлетворяют некоторым им установленным неравенствам.

Для изучения арифметической теории квадратичных форм можно рекомендовать книгу: P. Bachmann. Die Arithmetik der quadratischen Formen. Leipzig 1898.

[26]Seeber. Untersuchungen über die Eigenschaften der positiven ternären quadratischen Formen, Freiburg i. Br. 1831.

Глава VIII

Дальнейшие свойства целых функций

Тождественное обращение в нуль целой функции

§ 1

В основу нашего исследования мы поставим следующее определение.

Две целые функции от любою числа переменных независимых называются тождественно равными, если численных значения их совпадают при всяких значениях независимых переменных.

Как частный случай этого определения, можно установить:

Целая функция уничтожается тождественно, если она равна нулю при всяких значениях переменных независимых.

§ 2

Теорема. *Целая функция произвольного числа переменных независимых уничтожается тождественно, тогда и только тогда, когда все ее коэффициенты равны нулю.*

Достаточность этой теоремы очевидна. Докажем ее необходимость по индукции. В самом деле, ее справедливость в случай одной переменной независимой вытекает непосредственно из заключительного замечания § 2 главы II. Покажем теперь, что теорема справедлива для случая m переменных независимых, если она верна при $m-1$ переменных независимых.

Пусть целая функция

$$f(x_1, x_2, \ldots, x_m) = a_0(x_2, \ldots, x_m)x_1^n + a_1(x_2, \ldots, x_m)x_1^{n-1} + \ldots + a_n(x_2, \ldots, x_m)$$

уничтожается тождественно. Дадим переменным независимым $x_2, \ldots, x_m$ некоторые определенные численные значения $x_2^0, \ldots, x_m^0$; тогда функция f обращается в функцию от одной переменной независимой x_1. По предцоложению эта функция обращается в нуль при всех значениях x_1, значить, равны нулю все коэффициенты

$$a_i(x_2^0, x_3^0, \ldots, x_m^0).$$

Другими словами, все целые функций $a_0, a_1, \ldots, a_n$ обращаются в нуль при всех значениях переменных независимых, ибо значения $x_2^0, x_3^0, \ldots, x_m^0$ выбраны совершенно произвольно.

Итак, по предположение справедливости теоремы при $m-1$ независимых переменных мы заключаем о равенстве нулю всех коэффициентов полиномов $a_0, a_1, \ldots, a_n$, и наша теорема доказана.

Следствие. *Две целые функции тогда и только тогда тождественно равны между собою, когда одинаковы коэффициенты соответственных членов.*

Тождественное равенство двух функций есть не что иное, как тождественное равенство нулю их разности.

§ 3

Теорема. *Произведение $f_1 f_2$ целой функций f_1 степени n_1 на целую функцию f_2 степени n_2 имеет степень $n_1 + n_2$.*

Теорема очевидна для случая одной переменной независимой.

Рассмотрим сначала теорему для случая однородных функций, или форм. Очевидно, что каждое отдельное произведение члена формы f_1 на член формы f_2 будет иметь произведение степени $n_1 + n_2$. Нужно, следовательно, убедиться только в том, что не обращаются в нуль все коэффициенты произведения $f_1 f_2$.

Расположим переменные независимые $x_1, x_2, \ldots, x_m$ в порядке возрастания значков. Начнем с x_1 и соберем все члены функций f_1, в которые входить x_1 с наибольшим показателем μ_1. Из этих членов выберем те, у которых x_2 имеет наибольшей показатель μ_2. Из последних членов выбираем те, у которых x_3 имеет наибольший показатель μ_3, и так продолжаем до последней переменней x_m. Получаем ряд показателей $\mu_1, \mu_2, \ldots, \mu_m$, среди которых могут быть, конечно, равные нулю. Полученный таким образом член

$$ax_1^{\mu_1} x_2^{\mu_2} \cdots x_m^{\mu_m} \tag{1}$$

можно' назвать *старшим*. Данное нами понятие о старшем члене соответствует, конечно, выбранному расположенно переменныхъ независимых,[27] при другом расположены старшим может быть другой член.

Пусть при том же расположении перем4нных независимых будет старшим в функций f_2 член

$$bx_1^{\nu_1} x_2^{\nu_2} \cdots x_m^{\nu_m}. \tag{2}$$

Произведение членов (1) н (2) дает

$$abx_1^{\mu_1+\nu_1} x_2^{\mu_2+\nu_2} \cdots x_m^{\mu_m+\nu_m}. \tag{3}$$

Нетрудно убедиться, что член (3) окажется старшим в произведении $f_1 f_2$ относительно данного расположения переменных независимых и не будет иметь себе подобных. Значит, коэффициент ab члена (3) не может обратиться в нуль, ибо отличны от нуля оба множителя a и b.

Итак; теорема доказана для случая однородных функций.

Обращаясь теперь к общему случаю, мы можем разложить неоднородные функции на однородный составные части

$$f_1 = \varphi_1^{(n_1)}(x_1, \ldots, x_m) + \varphi_1^{(n_1-1)}(x_1, \ldots, x_m) + \ldots,$$
$$f_2 = \varphi_2^{(n_2)}(x_1, \ldots, x_m) + \varphi_2^{(n_2-1)}(x_1, \ldots, x_m) + \ldots,$$

[27] Так, напрнмер, в целой функции

$$x^4y^3z + x^5yz^7 + x^5y^3z + 2 + x^4z^2 + z^3y$$

будет старшим x^5y^3z для расположения букв (x, y, z), а для расположения (x, z, y) будет старшим член x^5yz^7.

где $\varphi_1^{(i)}$, $\varphi_2^{(j)}$ формы i-ой, j-ой степени, некоторые из которых могут *тождественно равняться нулю.*

Так как функций f_1 и f_2 имеют степени, *точно* равные числам n_1 и n_2, следовательно, не равны тождественно нулю функции $\varphi_1^{(n_1)}$ и $\varphi_2^{(n_2)}$. Итак, старшие степени в произведений $f_1 f_2$ получаются из произведения $\varphi_1^{(n_1)}\varphi_2^{(n_2)}$; это последнее не может равняться нулю на основании уже доказанной справедливости теоремы для форм.

Итак, степень произведения $f_1 f_2$ есть $n_1 + n_2$, что и требовалось показать.

§ 4

Теорема. *Если произведение двух или большего числа целых функций тождественно равно нулю, то один из множителей должен равняться тождественно нулю.*

В, самом деле, если бы ни один множитель произведения не равнялся тождественно нулю, то каждый из них имел бы некоторую определенную степень: сумма этих степеней давала бы степень произведения, следовательно, это произведение не могло бы тождественно равняться нулю.

Весьма важное практическое следствие из доказанной теоремы состоит в том, что можно всякое алгебраическое тождество сокращать на множители нетождественно равные нулю; от такого сокращения тождество остается тождеством.

§ 5

Теорема. *Если целая функция $f(x_1, x_2, \ldots, x_m)$ не равна тождественно нулю, то уничтожается тождественно целая функция $\varphi(x_1, x_2, \ldots, x_m)$, если только она обращается в нуль при значениях $x_1, x_2, \ldots, x_m$, не обращающих f в нуль.*

Эта теорема есть следствие предыдущей, если принять в соображение, что произведение $f\varphi$ тождественно равно нулю.

§ 6

Будем рассматривать теперь целые функции в *окрестности* некоторой *аналитической точки.*

Пусть независимым переменные $x_1, x_2, \ldots, x_m$ рассматриваются как *координаты* пространства m измерений.

Если переменным независимым заданы некоторые численные значения $(x_1^0, x_2^0, \ldots, x_m^0)$, то мы будем говорить, что задана аналитическая точка. Будем переменным независимым давать как вещественные так и мнимые значения.

Пусть для каждой переменной независимой x_i рассматривается особая плоскость комплексных чисел. Дадим частному значение x_i^0 этой переменной независимое приращение h_i.

Мы будем говорить, что новая точка

$$(x_1^0 + h_1, x_2^0 + h_2, \ldots, x_m^0 + h_m)$$

находится в *окрестности* точки $(x_1^0, x_2^0, \ldots, x_m^0)$, если модули приращений h_i удо-

влетворяют неравенствам

$$|h_1| < \alpha_1, \quad |h_2| < \alpha_2, \ \ldots, \ |h_m| < \alpha_m,$$

где $\alpha_1, \alpha_2, \ldots, \alpha_m$ *произвольно* заданные положительные числа.

§ 7

Теорема. *Для тождественного уничтожения целой функции*

$$f(x_1, x_2, \ldots, x_m)$$

необходимо и достаточно, чтобы она равнялась нулю для всех точек в окрестности некоторой определенной точки.

Доказательство этой теоремы тоже самое, что и для теоремы § 2, ибо при доказательстве той теоремы играло роль лишь то обстоятельство, что каждая из координат могла принимать бесчисленное множество значений; это же обстоятельство имеет место и в данном случае.

Следствие. *Для тождественного равенства двух целых функций необходимо и достаточно равенство этих функций лишь для точек окрестности какой либо определенной точки.*

§ 8

Данное нами в § 16 главы I доказательство непрерывности целой функции от одной переменной независимой, может быть обобщено и на случай нескольких переменных независимых.

Мы назовем функцию $f(x_1, x_2, \ldots, x_m)$ *непрерывною в точке* $(x_1^0, x_2^0, \ldots, x_m^0)$, *если всякому положительному числу* ε *можно сопоставить такую окрестность точки* $(x_1^0, x_2^0, \ldots, x_m^0)$, *что для всякой точки* $(x_1', x_2', \ldots, x_m')$ *этой окрестности будет*

$$|f(x_1', x_2', \ldots, x_m') - f(x_1^0, x_2^0, \ldots, x_m^0)| < \varepsilon.$$

Покажем, что *для всякой аналитической точки целая функция есть функция непрерывная.*

Докажем предварительно две леммы.

Лемма I. *Сумма конечного числа функций непрерывных в точке есть функция непрерывная в той же точке.*

Достаточно доказать эту лемму для двух функций f_1 и f_2. Обозначим через f_1^0 и f_2^0 значения функций в рассматриваемой точке. Если обе функции непрерывные в точке, то[28]

$$|f_1 - f_1^0| < \frac{\varepsilon}{2} \quad \text{при} \quad |x_i - x_i^0| < \delta_1,$$
$$|f_2 - f_2^0| < \frac{\varepsilon}{2} \quad \text{при} \quad |x_i - x_i^0| < \delta_2.$$

Тогда, обозначая через δ меньшее из чисел δ_1 и δ_2, получим

$$|f_1 - f_1^0| + |f_2 - f_2^0| < \varepsilon \quad \text{при} \quad |x_i - x_i^0| < \delta.$$

[28]Здесь через δ обозначено наименьшее из чисел $\alpha_1, \alpha_2, \ldots, \alpha_m$.

Но по формуле

$$|a| + |b| \geq |a + b|$$

получаем

$$|(f_1 + f_2) - (f_1^0 + f_2^0)| < \varepsilon \quad \text{при} \quad |x_i - x_i^0| < \delta,$$

и, значить, сумма $f_1 + f_2$ есть функция непрерывная.

Лемма II. *Произведение конечного числа непрерывных в точке множителей есть функция непрерывная в той же точке.*

Достаточно доказать эту теорему для случая двух множителей.

Взяв произвольно малое положительное число η, подберем положительные числа δ_1 и δ_2 таким образом, чтобы было

$$|f_1 - f_1^0| < \eta \quad \text{при} \quad |x_i - x_i^0| < \delta_1,$$

$$|f_2 - f_2^0| < \eta \quad \text{при} \quad |x_i - x_i^0| < \delta_2.$$

Тогда, обозначая по прежнему через δ наименьшее из чисел δ_1 и δ_2,

$$|(f_1 - f_1^0)(f_2 - f_2 - f_2^0) + f_1^0(f_2 - f_2^0) + f_2(f_1 - f_1^0)| = |f_1 f_2 - f_1^0 f_2^0|,$$

следовательно,

$$|f_1 f_2 - f_1^0 f_2^0| < \{|f_1^0| + |f_2^0|\}\eta + \eta^2.$$

Остается подобрать η так, чтобы было

$$\{|f_1^0| + |f_2^0|\}\eta + \eta^2 < \varepsilon,$$

и теорема доказана, ибо

$$|f_1 f_2 - f_1^0 f_2^0| < \varepsilon \quad \text{при} \quad |x_i - x_i^0| < \delta.$$

На оснований приведенных лемм убеждаемся в непрерывности функции вида $ax_1^{\alpha_1} \cdots x_m^{\alpha_m}$, где α_i целые числа или нули. Суммируя отдельные члены, мы докажем непрерывность целой функции.

§ 9

Теорема. *Если целая функция $f(x_1, \ldots, x_m)$ не обращается в нуль в точке $(x_1^0, x_2^0, \ldots, x_m^0)$, то около этой точки можно указать такую окрестность, что во всех ее точках функция f отлична от нуля.*

Положим $f(x_1^0, \ldots, x_m^0) = f^0$. Возьмем δ настолько малым, чтобы при $|x_i - x_i^0| < \delta$ было

$$|f - f^0| < \frac{1}{2}|f^0|.$$

Если $f = 0$ для какой нибудь из точек указанной окрестности, то мы приходим к противоречию

$$|f^0| < \frac{1}{2}|f^0|.$$

§ 10

Если между тремя целыми функциями f, φ, ψ существует соотношение

$$f = \varphi\psi,$$

которое является тождеством, т. е. которое справедливо при всех значениях независимых переменных $x_1, x_2, \ldots, x_m$, то каждая из функций φ и ψ называется *делителем* функции f.

Всякая постоянная величина, отличная от нуля, есть делитель всякой целой функции.

Всякая целая функция может быть рассматриваема как делитель, тождественно равный нулю целой функции.

Целая функция нулевой степени, которая есть нечто иное, как постоянная величина, *не может* иметь целых делителей *не нулевой* степени.

Целая функция $x_1, x_2, \ldots, x_m$, не равная тождественно нулю, не может иметь делителей, заключающих еще другие переменные независимые.

§ 11

Теперь мы установим еще одно весьма важное понятие, а именно, понятие о так называемой *приводимости* целых функции.

Целую функцию мы назовем приводимою, если она тождественно равна произведению двух целых функций, из которых каждая не сводится к постоянному числу.

В обратном случай функция называется неприводимою.

Как пример приводимой функции можно указать

$$x^3 + y^3 + z^3 + 3xyz = (x + y + z)(x + \alpha y + \alpha^2 z)(x + \alpha^2 y + \alpha z),$$

где α есть корень уравнения $\alpha^2 + \alpha + 1 = 0$.

В виде примера неприводимой функций можно указать

$$f(x) + y,$$

где $f(x)$ произвольная целая функция от одной независимой переменной x.

§ 12

В дальнейшем изложений понятие о приводимости целых функций будет подвергнуто некоторому изменению.

В предыдущих параграфах коэффициенты целых функций считаются произвольными как вещественными, так и мнимыми числами. Понимаемые в этом смысле приводимость или неприводимость мы будем называть *абсолютными*. В дальнейшем мы установим понятие об *условной* приводимости в зависимости от характера коэффициентов. Так например, функция $x^2 + 1$ приводима в абсолютном смысле, ибо она равна $(x + \sqrt{-1})(x - \sqrt{-1})$, но она становится *неприводимою*,

если мы допускаем только вещественные коэффициенты. В настоящей главе мы будем исключительно заниматься абсолютною приводимостью.

§ 13

Теорема. *Определитель порядка n есть неприводимая функция его n^2 элементов, если эти элементы рассматривать как независимых переменные.*

Допустим, что определитель $D = |a_{ik}|$ будет функцией приводимой, так что

$$D = f_1(a_{11}, \ldots, a_{nn}) f_2(a_{11}, \ldots, a_{nn}).$$

Так как всякий элемент определителя входит в него в первой степени, значить, он должен входить в этой первой степени в одну из функций, а в другую не должен входить. Рассмотрим элемент a_{ii} главной диагонали. Пусть он входит в функцию f_1, тогда в функцию f_2 не могут входить элементы i горизонтали и i-ой колонны, ибо иначе в членах определителя входило бы одно из произведений $a_{ii}a_{ij}$ или $a_{ii}a_{ji}$, что противоречить закону составления определителя. Рассмотрим теперь другой элемент a_{jj} главной горизонтали. Можно показать, что он не может входить в f_2. В самом деле, допустим это, тогда в функций f_1 не входит ни один член j-ой горизонтали и j-ой колонны. Сопоставляя с предыдущим, мы придем к ложному заключению, что элементы a_{ij}, a_{ji} не входят ни в один из множителей f_1, f_2. Итак, если a_{ii} входит в функцию f_1, то в эту же функцию входит и всякий другой член a_{jj} главной горизонтали, а вместе с ним и все элементы определителя. Функция f_2 сведется к постоянному числу, что и требовалось доказать.

§ 14

Если в выражений целой функций

$$ax_1^{\alpha_1} \cdots x_m^{\alpha_m} + bx_1^{\beta_1} \cdots x_m^{\beta_m} + \ldots$$

нет подобных членов и все коэффициенты $a, b, \ldots$ суть независимые переменные, то функция неприводима, если предположить, что показатели

$$\alpha_i,\ \beta_i,\ \ldots$$

над всякой буквой x_i не во всех членах суть числа положительные.

§ 15

Часто полезно сопоставлять однородные и неоднородные целые функции.

Если мы составим из неоднородной целой функций степени n от переменных независимых $x_1, x_2, \ldots, x_m$ новую целую функцию через умножение членов степени ниже n на соответственные степени новой переменной независимой x_{m+1}, таким образом, чтобы получалась однородная функция от $m+1$ переменных независимых, то эта однородная функция носит название соответствующей.

Очевидно, что для целой функции $f(x_1, x_2, \ldots, x_m)$ будет соответствующею функция

$$x_{m+1}^n f\left(\frac{x_1}{x_{m+1}}, \frac{x_2}{x_{m+1}}, \ldots, \frac{x_m}{x_{m+1}}\right). \tag{1}$$

Из однородной соответствующей функции получим первоначальную, полагая $x_{m+1} = 1$.

Нетрудно видеть, что у всякой неоднородной функции существует одна соответствующая. Однородная же функция может иметь несколько соответствующих функции, судя по тому, которую из переменных мы приравняем единице. Однородная функция не будет иметь соответствующей, если все переменный независимый входят в каждый член ее, например, $x_1^2x_2x_3 + x_1x_2^2x_3 + x_1x_2x_3^2$.

Теорема. *Если одна из друг другу соответствущих функций приводимая, то такова же будет и другая; при этом множители одной соответствуют множителям другой.*

Пусть неоднородная функция f приводимая

$$f(x_1, x_2, \ldots, x_m) = \varphi(x_1, x_2, \ldots, x_m)\psi(x_1, x_2, \ldots, x_m). \tag{1}$$

Предполагая $x_{m+1} \neq 0$, подставим в тождество (1) вместо $x_1, x_2, \ldots, x_m$ их отношения в x_{m+1}

$$f\left(\frac{x_1}{x_{m+1}}, \frac{x_2}{x_{m+1}}, \ldots, \frac{x_m}{x_{m+1}}\right) = \varphi\left(\frac{x_1}{x_{m+1}}, \ldots, \frac{x_m}{x_{m+1}}\right)\psi\left(\frac{x_1}{x_{m+1}}, \ldots, \frac{x_m}{x_{m+1}}\right); \tag{2}$$

обозначая степени φ и ϕ через p и q и умножая тождество (2) на x_m^{p+q}, получим равенство

$$f_1(x_1, \ldots, x_m, x_{m+1}) = \varphi_1(x_1, \ldots, x_m, x_{m+1})\psi_1(x_1, \ldots, x_m, x_{m+1}) \tag{3}$$

для соответствующих форм. Равенство (3) имеет место при всех отличных от нуля значениях x_{m+1}, следовательно, на основании теоремы § 5 заключаем. что (3) есть тождество, и соответствующий полином $f1$, приводимый. Обратно из тождества (3) получим (1), если положим x_{m+1}.

§ 16

Основная теорема алгебры о существовали у всякого полинома по крайней мере одного корня показывает, что целая функция от одной независимой переменной степени выше первой есть всегда абсолютно приводимая.

Целая функция от одной переменной степени n раскладывается на n множителей первой степени

$$f(x) = p_0(x - a_1)(x - a_2)\cdots(x - a_n),$$

где $a_1, a_2, \ldots, a_n$ суть корни функций $f(x)$.

Если полиномы, отличающиеся постоянными множителями, не считать за различные, то получается теорема.

Полином степени n от одной независимой переменной раскладывается только одним способом на неразложимые (простые) множители первой степени.

Вводя новую переменную независимую y и переходя к функции соответствующей, мы получим формулу

$$f_1(x, y) = p_0(x - a_1y)(x - a_2y)\cdots(x - a_ny),$$

выражающую свойство абсолютной приводимости бинарной формы.

Алгоритм Эвклида для целых функций

§ 17

Перейдем теперь к нахождение общего наибольшего делителя двух целых функций при помощи последовательного деления. Другими словами, мы переходим к изучение знаменитого алгоритма Эвклида, который можно назвать алгоритмом непрерывных дробей; причем будем этот алгоритм рассматривать в применении к целым функциям. Эвклид изучает этот алгоритм по двум поводам: 1) для нахождения общего наибольшего делителя двух целых чисел, 2) для нахождения общей меры двух отрезков в теории, трактующей об измерении протяженных величин.

В применении к нахождению общей меры двух отрезков алгоритм приводит к разложению отношения отрезков в непрерывную дробь. Если дробь эта окажется бесконечною, то отношение двух отрезков есть число несоизмеримое. Этот случай не имеет места, когда мы применяем алгоритм Эвклида к нахождению наибольшего делителя двух целых чисел. Здесь алгоритм всегда оказывается конечным.

В теории чисел[29] показывается, что из конечности алгоритма Эвклида следуют все основные теоремы о делимости чисел; между прочим, фундаментальная теорема о единственной разложимости целого числа на простые множители.

К аналогичным выводам можно придти, рассматривая алгоритм Эвклида в применении к полиномам. Конечность этого действия влечет те же следствия, что и в арифметике. Располагая два полинома по степеням одной и той же буквы x, мы можем последовательным делением с уменьшающимися степенями, остатков получить общий наибольший делитель заданных двух полиномов или же убедиться, что эти полиномы не имеют общего делителя, заключающего букву x. Проделав тоже самое относительно всех входящих в полиномы букв, найдем все общие делители этих полиномов.

§ 18

Рассмотрение применения алгоритма Эвклида к полиномам представляет некоторую разницу случая одной переменной независимой от случая полиномов от многих букв. Хотя эта разница не существенная и не нарушает полной общности выводов, остающихся одними и теми же во всех случаях, тем не менее полезно при изложений рассмотреть сначала случай одной переменной независимой.

Начнем с известного из арифметики способа нахождения общего наибольшего делителя двух чисел a и b при помощи последовательного деления.

Пусть $a > b$.

Получаем ряд равенств

$$a = qb + r_1, \quad b = q_1 r_1 + r_2, \quad r_1 = q_2 r_2 + r_3, \ \ldots$$
$$r_{k-2} = q_{k-1} r_{k-1} + r_k, \quad r_{k-1} = q_k r_k,$$

[29] Д. Граве. Элементарный курс теории чисел. 2-ое издание. Киев. 1913 г. Глава I.

где $q, q_1, \ldots, q_{k-1}$ последовательные частные деления, а r_i убывающие остатки

$$b > r_1 > r_2 > \ldots > r_{k-1} > r_k.$$

Как известно r_k есть общий наибольший делитель чисел a и b.

Первое из уравнений (1) дает

$$r_1 = a - qb. \tag{2}$$

Подставляя во второе мы получим

$$r_2 = -q_1 q + (qq_1 + 1)b. \tag{3}$$

Далее из третьего

$$r_3 = (q_1 q_2 + 1)a - (qq_1 q_2 + q_2 + q)b. \tag{4}$$

Можно ввести новый символ, часто употребляющейся математиками. Этот символ определяется вполне следующими формулами

$$\begin{aligned}
[\,] &= 1 \\
[\xi_1] &= \xi_1 \\
[\xi_1, \xi_2] &= \xi_1\xi_2 + 1 \\
[\xi_1, \xi_2, \xi_3] &= \xi_1\xi_2\xi_3 + \xi_1 + \xi_3 \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
[\xi_1, \ldots, \xi_n] &= [\xi_1, \ldots, \xi_{n-1}]\xi_n + [\xi_1, \ldots, \xi_{n-2}].
\end{aligned}$$

Этот символ обладает между прочим свойством

$$[\xi_1, \xi_2, \ldots, \xi_{n-1}, \xi_n] = [\xi_n, \xi_{n-1}, \ldots, \xi_2, \xi_1].$$

При помощи нового символа получаем, принимая во внимание (2), (3), (4), выражение всякого остатка r_l линейно через a и b

$$r_l = ax_l + by_l,$$

где

$$x_l = (-1)^{l-1}[q_1, q_2, \ldots, q_{l-1}], \qquad y_l = (-1)^l[q, q_1, q_2, \ldots, q_{l-1}]. \tag{5}$$

Применяя к случаю $l = k$, получаем формулу для общего наибольшего делителя r_k

$$r_k = ax_k + by_k.$$

Если $r_k = 1$, то два числа a и b взаимно простыл, и мы получаем формулу

$$ax + by = 1,$$

где x и y целые числа, из которых, конечно, одно положительное, а другое отрицательное.

И мы приходим к заключению.

Два числа a и b тогда и только тогда взаимно простые, если можно подобрать два целых числа x и y таких, чтобы было

$$ax + by = 1.$$

§ 19

Обращаемся теперь к нахождение общего наибольшего делителя двух многочленов $f(x)$ и $\varphi(x)$, причем предположим, что ни один из них не сводится к постоянной величине и что степень f не менее степени φ.

Последовательное деление приводить к ряду тождеств:

$$\begin{aligned} f(x) &= Q(x)\varphi(x) + R_1(x) \\ \varphi(x) &= Q_1(x)R_1(x) + R_2(x) \\ R_1(x)(x) &= Q_2(x)R_2(x) + R_3(x) \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ R_{k-1}(x) &= Q_k(x)R_k(x) + R_{k+1}(x). \end{aligned}$$

Здесь последовательные остатки R_i имеют степени, убывающие с возрастанием значка i. Деление продолжается до тех пор пока мы не дойдем до достатка R_{k+1}, равного постоянному числу (нулевой степени).

Если постоянный остаток R_{k+1} отличен от нуля, то целые функции $f(x)$ и $\varphi(x)$ не имеют общего делителя, заключающего букву x, ибо на основании соображений аналогичных приведенным в § 17 мы замечаем, что общий наибольший делитель $f(x)$ и $\varphi(x)$ должен быть делителем всякого остатка R_l, а следовательно, и остатка R_{k+1}; это же невозможно, ибо постоянное число не может делиться на целую функцию. Итак, функции $f(x)$ и $\varphi(x)$ будут *взаимно простыми*,[30] если R_{k+1} отлично от нуля.

Если же $R_{k+1} = 0$, тогда предпоследний остаток $R_k(x)$ будет общим наибольшим делителем всех предыдущих остатков, а также и функций $f(x)$ и $\varphi(x)$, то есть

$$f(x) = R_k(x)f_1(x), \qquad \varphi(x) = R_k(x)\varphi_1(x),$$

где $f_1(x)$, $\varphi_1(x)$ будут некоторые полиномы, которые могут приводиться к постоянному числу.

Принимая во внимание формулы (5) предыдущего параграфа, получим

$$\begin{aligned} R_{k+1} = (-1)^k[Q_1(x)Q_2(x)\cdots Q_k(x)]+ \\ +(-1)^{k+1}[Q(x)Q_1(x)\cdots Q_k(x)]\varphi(x) \end{aligned}$$

или

$$F(x)f(f) + \Phi(x)\varphi(x) = 1, \tag{1}$$

где

$$\begin{aligned} F(x) &= \frac{(-1)^k}{R_{k+1}}\,[Q_1(x)Q_2(x)\cdots Q_k(x)], \\ \Phi(x) &= \frac{(-1)^{k+1}}{R_{k+1}}\,[Q(x)Q_1(x)\cdots Q_k(x)]. \end{aligned} \tag{3}$$

[30] Делители, равные постоянному числу, не принимаются в рассмотрение.

Мы приходим к теореме

Условие необходимое и достаточное для того, чтобы два полинома $f(x)$ и $\varphi(x)$ были взаимно простые состоит в существовали двух новых полиномов $F(x)$ и $\Phi(x)$ таких, чтобы существовала тождество

$$F(x)f(x) + \Phi(x)\varphi(x) = 1.$$

§ 20

Из теоремы предыдущего параграфа можно вывести те же следствия относительно делимости полиномов, какие выводятся относительно чисел[31] в арифметике.

Так например, если произведение

$$f(x)f_1(x)$$

делится на $\varphi(x)$, но полиномы $f(x)$ ц $\varphi(x)$ взаимно простые, то $f_1(x)$ делится на $\varphi(x)$.

В самом деле, по предположение

$$f(x)f_1(x) = \varphi(x)\varphi_1(x).$$

Функции $f(x)$ и $\varphi(x)$ взаимно простые, следовательно, можно подобрать две целые функции $F(x)$ и $\Phi(x)$ такие, чтобы было

$$F(x)f(x) + \Phi(x)\varphi(x) = 1; \tag{2}$$

умножая тождество (2) на $f_1(x)$ и принимая во внимание тождество (1), получим

$$\varphi(x)[F(x)\psi(x) + \Phi(x)f_1(x)] = f_1(x),$$

откуда следует дедимость $f_1(x)$ на $\varphi(x)$.

Пусть степень $f(x)$ есть n, а степень $\varphi(x)$ есть m, тогда можно сделать весьма важное дальнейшее заключение о степенях функций $F(x)$ и $\Phi(x)$, входящих в тождество (2). Обозначим через m_i степень $R_i(x)$.

Степени $Q(x)$, $Q_1(x)$, $Q_2(x)$, $\ldots$, $Q_k(x)$ будут, очевидно,

$$n - m, \quad m - m_1, \quad m_1 - m_2, \ \ldots, \ m_{k-1} - m_k.$$

На оснований формул (2) и (3) § 18 получаем для степени $F(x)$ и $\Phi(x)$ выражения

$$m - m_1 + (m_1 - m_2) + \ldots + (m_{k-1} - m_k) = m - m_k,$$

$$n - m + (m - m_1) + (m_1 - m_2) + \ldots + (m_{k-1} - m_k) = n - m_k.$$

Следовательно, степень $F(x0$ ниже степени $\varphi(x)$, а степень $\Phi(x)$ ниже степени $f(x)$.

[31] Д. Граве. Элементарный курс теории чисел. Киев, 1918. Глава I.

Покажем в заключение, что функции $F(x)$ и $\Phi(x)$ однозначно определяются тождеством (2) и требованием, чтобы их степени были ниже степеней функций $\varphi(x)$ и $f(x)$. Допустим обратное, что кроме $F(x)$ и $\Phi(x)$ существуют еще другая пара подобных функций $F_1(x)$ и $\Phi_1(x)$, при которых существует тождество

$$F_1(x)f(x) + \Phi_1(x)\varphi(x) = 1. \tag{3}$$

Вычитая (3) из (2), получим

$$(F - F_1)f(x) = (\Phi_1 - \Phi)\varphi(x);$$

$f(x)$ и $\varphi(x)$ функции взаимно простыл, следовательно, разность $F(x)-F_1(x)$ должна делиться на $\varphi(x)$, а разность $\Phi_1(x)-\Phi(x)$ на $f(x)$, что невозможно, ибо степени этих разностей ниже степеней тех функций, на которые они должны делиться; значит. мы приходим к двум тождествам

$$F - F_1 = 0, \qquad \Phi_1 - \Phi = 0,$$

и, значить, функции F_1 и Φ_1 не отличаются от F и Φ.

§ 21

Если полиномы, отличающиеся друг от друга постоянными множителями, не считать за различные, то из тождества (1) § 19 вытекает единственность разложения полинома на неразложимые далее множители. Эти множители играют туже роль в делимости полиномов, что и простые числа при делимости чисел.

Вследствие абсолютной разложимости полиномов от одной переменной независимой, неприводимым может быть лишь полином первой степени.

Если, как сказано, не обращать внимание на постоянные множители, то аналогию с простыми числами арифметики составляют двучлены вида

$$x - \alpha. \tag{1}$$

На такого рода двучлены одним только способом разлагается всякая целая функция от одной переменной независимой, причем α есть корень целой функции.

Если давать α все возможные как вещественные, так и мнимые значения, выражение (1) пробежит *неперечислимую*[32] совокупность; простые же числа в арифметике образуют совокупность *перечислимую*.

§ 22

Если мы перейдем к функциям от многих переменных независимых, то тут могут существовать неприводимые функции высших степеней.

Для доказательства теоремы об однозначности разложения целой функции на неприводимые, надо будет рассмотреть, как должно производить выкладки алгоритма Эвклида в этом случае.

Возьмем функцию, разложенную по степеням x

$$f(x, y, z, \ldots) = X_0x^n + X_1x^{n-1} + \ldots + X_{n-1}x + X_n, \tag{1}$$

[32]Д. Граве. Введение в анализ. Киев 1910 г. Заключение. § 3.

где $X_0, X_1, \ldots, X_n$ суть целые функции от остальных переменных независимых.

Докажем теорему:

Необходимое и достаточное условие для того, чтобы функция $f(x, y, z, \ldots)$ имела делитель $\varphi(y, z, \ldots)$ независимый от x, состоит в том, чтобы все коэффициенты X_i делились на $\varphi(y, z, \ldots)$.

В самом деле, достаточность теоремы очевидна. Что касается ее необходимости, то допустим, что f делится на φ, т. е.

$$X_0 x^n + \ldots + X_n = \varphi(y, z, \ldots)[Y_0 x^n + Y_1 x^{n-1} + \ldots + Y_n],$$

где $Y_0, Y_1, \ldots, Y_n$ суть целые функции от $y, z, \ldots$. Сравнивая коэффициенты при различных степенях x, получим

$$X_0 = \varphi Y_0, \quad X_1 = \varphi Y_1, \ \ldots, \ X_n = \varphi Y_n. \tag{2}$$

Так как равенства (2) должны иметь место при всех значениях $y, z, \ldots$, то они должны быть тождествами и, значит, все X_i делятся на φ.

§ 23

Пусть требуется искать общий наибольший делитель двух целых функций

$$\begin{aligned} f(x, y, z, \ldots) &= X_0(y, z, \ldots)x^n + X_1(y, z, \ldots)x^{n-1} + \ldots + X_n(y, z, \ldots), \\ \varphi(x, y, z, \ldots) &= Y_0(y, z, \ldots)x^m + Y_1(y, z, \ldots)x^{m-1} + \ldots + Y_m(y, z, \ldots). \end{aligned} \tag{1}$$

Если $n \geq m$, то при делении f на φ первый член относительно x будет иметь вид

$$\frac{X_0(y, z, \ldots)}{Y_0(y, z, \ldots)} x^{n-m},$$

причем в частном оказываются коэффициенты, которые выражаются дробными рациональными функциями от $y, z, \ldots$. Во избежание дробных коэффициентов можно умножить предварительно функцию f, подлежащую делению, на некоторую, приличным образом выбранную, функцию $R(y, z, \ldots)$ от $y, z, \ldots$.

Мы можем в основу алгоритма Эвклида положить теорему:

Если f и φ суть полиномы от переменных независимых $x, y, z, \ldots$, причем φ не уничтожается тождественно, то можно всегда, подобрать три новые целые функции Q, R, P, из которых последняя P не заключает x и не равна тождественно нулю, такие, что будет иметь место тождество

$$P(y, z, \ldots)f(x, y, z, \ldots) = Q(x, y, z, \ldots)\varphi(x, y, z, \ldots) + +R(x, y, z, \ldots),$$

причем функция R или тождественно равна нулю, или же ее степень относительно x ниже степени φ относительно x.

Если степень f по x меньше степени φ, то можно будет положить $P = 1$, $Q = 0$, $R = f$.

Остается, следовательно, доказать теорему лишь в случае (см. (1)) $n \geq m$, $X_0 \neq 0$, $Y_0 \neq 0$.

Если степень φ не выше степени f, то можно будет подобрать два полинома Q_1, R_1, которые удовлетворяют тождеству

$$Y_0(y, z, \ldots)f(x, y, z, \ldots) = Q_1(x, y, z, \ldots)\varphi(x, y, z, \ldots) + R_1(x, y, \ldots), \tag{2}$$

где R_1 или тождественно равно нулю, или же степень R_1 по букве x меньше степени f. Что это так, следует из того обстоятельства, что можно взять

$$Q_1 = X_0(y, z, \ldots)x^{n-m}.$$

Если степень по x полинома R_1 меньше степени φ, то теорема доказана, если же этого нет, то подбираем новых два полинома Q_1 и R_2 так, чтобы было

$$(3) \qquad Y_0(y, z, \ldots)R_1(x, y, z, \ldots) = Q_2(x, y, z, \ldots)\varphi(x, y, z, \ldots) + R_2(x, y, z, \ldots).$$

Сопоставляя (2) и (3), получим

$$Y_0^2 f = (Y_0 Q_1 + Q_2)\varphi + R_2.$$

Если степень R_2 по x меньше степени φ, то теорема доказана, ибо можно положить

$$P = Y_0^2, \qquad Q = Y_0 Q + Q_2, \qquad R = R_2.$$

Если же степень R_2 выше φ, то продолжаем указанным способом понижение степени, пока не дойдем до полинома R_i, степень которого будет уже ниже степени φ и который будет удовлетворять тождеству

$$Y_0^i = (Y_0^{i-1}Q_1 + Y_0^{i-2}Q_2 + \ldots + Q_i)\varphi + R_i,$$

так что будет

$$P = Y_0^i, \qquad Q = Y_0^{i-1}Q_1 + Y_0^{i-2}Q_2 + \ldots + Q_i, \qquad R = R_i.$$

Полезно заметить, *что за функции P можно принять некоторую степень функции Y_0.*

§ 24

Теперь можем приступить к нахождение общего наибольшего делителя функций (1) § 23.

Получаем систему тождеств

$$(1) \qquad \begin{aligned}
&P(y, z, \ldots)f = Q(x, y, z, \ldots)\varphi + R_1(x, y, z, \ldots)\\
&P_1(y, z, \ldots)\varphi = Q_1(x, y, z, \ldots)R_1(x, y, z, \ldots) + R_2(x, y, z, \ldots)\\
&P_2(y, z, \ldots)R_1(x, y, z, \ldots) = Q_2(x, y, z, \ldots)R_2(x, y, z, \ldots) + R_3(x, y, z, \ldots)\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&P_{k-1}(y, z, \ldots)R_{k-2}(x, y, z, \ldots) = Q_{k-1}(x, y, \ldots)R_{k-1}(x, y, \ldots) + R_k(x, y, \ldots)\\
&P_k(y, z, \ldots)R_{k-1}(x, y, z, \ldots) = Q_k(x, y, z, \ldots)R_k(x, y, z, \ldots) + R_{k+1}(y, z \ldots).
\end{aligned}$$

Степени φ, R_1, R_2, ... относительно буквы x, по которой мы делим, убывают; следовательно, мы доходим до такого остатка R_{k+1},который не заключает буквы x.

Полиномы f и φ будут иметь общий делитель, заключающий букву x, тогда и только тогда, когда $R_{k+1}(y, z, \ldots)$ *тождественно уничтожается.*

Чтобы это доказать, заметим прежде всего, что каждый общий делитель f и φ будет по первому равенству (1) делителем остатка $R_1(x, y, \ldots)$, а тогда по второму равенству (1) он будет также делителем R_2; продолжая рассуждение далее, мы заметим, что этот делитель, заключая букву x, будет делить R_{k+1}, что невозможно (см. § 10). Значить, должен равняться тождественно пулю остаток R_{k+1}.

Для доказательства обратного, а именно, что при тождеств $R_{k+1} = 0$ функции f и φ имеют общие делители, заключающие букву x, и для нахождения общего наибольшего делителя этих функций, будем рассуждать по индукции.

Предположим, что для целых функций, не заключающих буквы x, другими словами, для целых функций, число переменных незавнсимых, которых на единицу меньше, имеет место теория делимости аналогичная арифметической; то отсюда будет следовать не только подлежащее доказательству обратное заключение, но и существование теории, аналогичной арифметической, для полиномов, заключающих также и переменную x. В параграфах 18, 19, 20 мы видели, что арифметическая теория проверяется для функций от одной переменной независимой, следовательно, с этого случая может начаться индукция.

Итак, предполагая существование арифметической теории для функций от переменных независимых $y, z, \ldots$, (без x), мы напомним характерные положения этой теории:

1) Функций одним только способом[33] раскладываются на неприводимые множители.

2) Если произведение ff_1 делится на φ, но f и φ взаимно простые функции, то f_1 делится на φ.

3) Если произведение ff_1 делится на неприводиый множитель φ, то на него должна делиться одна из функций f или f_1.

4) Произведение функций взаимно простых с φ есть сама функция взаимно простая с φ.

§ 25

Если мы возьмем функцию $\varphi(y, z, \ldots)$ без x, то, как мы видели в § 21, для делимости на φ функции, заключающей x, необходимым и достаточным условием является делимость на φ всех коэффициентов при степенях x.

Итак, если у нас задана функция

$$f = X_0x^n + X_1x^{n-1} + \ldots + X_n,$$

то, разложив все коэффициенты X_i на неприводимые множители, можем найти общий наибольший делитель этих коэффициентов.

Пусть этот делитель будет φ, тогда получим

$$f = \varphi f_1,$$

где

$$f_1 = X_0'x^n + X_1'x^{n-1} + \ldots + X_n'.$$

Новые X_i' не имеют уже отличного от постоянного числа общего делителя.

[33] С указанной, конечно, выше оговоркой.

Итак при помощи функции φ выделены уже все неприводимые множители f, *не заключающие* буквы x. Функция же f_1 может раскладываться лишь на множители, заключающее букву x. Функция φ по предцоложению раскладывается одним только способом на неприводимые множители. Остается показать, что такое же единственное разложение на множители имеет место для функций f_1, заключающей букву x?.

Докажем теперь теорему.

Неприводимая функция $\varphi(y, z, \ldots)$, не заключающая x и которая есть делитель произведения ff_1 двух функций, заключающих букву x, должна делить одну из функций f или f_1.

Произведение двух полиномов

$$f = X_0x^n + X_{n-1}x^{n-1} + \ldots$$
$$f_1 = Y_0x^m + Y_1x^{m-1} + \ldots$$

есть

$$ff_1 = X_0Y_0x^{n+m} + (X_0Y_1 + X_1y_0)x^{n+m-1} + (X_0Y_2 + X_1Y_1 + X_2Y_)x^{n+m-2} + \ldots$$

Допустим обратное, что ни одна из функций f и f_1 не делится на φ; тогда не все X_i и не все Y_i делятся на φ. Пусть коэффициенты $X_0, X_1, \ldots, X_{i-1}$ делятся на φ, а X_i не делится на φ (может быть, конечно, $i = 0$); подобным же образом $Y_0, Y_1, \ldots, Y_{j-1}$ делятся на φ, а Y_j не делится на φ. Мы получим коэффициент члена $x^{n-i+m-j}$ произведения ff_1 в таком виде

$$X_0Y_{i+j} + \ldots + X_{i-1}Y_{j+1} + X_iY_j + X_{i+1}Y_{j-1} + \ldots + X_{i+j}Y_0, \tag{1}$$

где X и Y с индексами большими n и m надо считать равными нулю. По предположений теоремы выражение (1) должно делиться на φ. Мы приходим к заключению о делимости на φ произведения X_iY_j, ибо другие члены будут по предположению делиться на φ; но X_i, Y_j, φ не заключают буквы x, следовательно, по предположению приложимости к ним арифметической теории мы приходим к противоречие, ибо ни X_i ни Y_j не делятся на φ[34].

§ 26

Докажем теперь теорему: *если произведение ff_1 двух функций, заключающих букву x, делится на функцию φ, не заключающую x, причем f и φ будут функциями взаимно простыми, то f_1 должно делится на φ.*

Разложим φ на произведение неприводимых множителей

$$\varphi = \varphi_1\varphi_2 \cdots \varphi_k.$$

По предположению мы имеем равенство

$$ff_1 = \varphi_1\varphi_2 \cdots \varphi_k F(x, y, z, \ldots). \tag{1}$$

[34]Мы просим читателя сравнить § 15, 16 главы XIII.

Функция φ_1 делит произведение f и f_1, следовательно, она как неприводимая должна делить или множитель f, или же множитель f_1, но f и φ по предположению взаимно простые, следовательно, φ_1 должна делить f_1 и мы получаем $f_1 = \varphi_1 f_1'$; тогда равенство (1) дает

$$f f_1' = \varphi_2 \cdots \varphi_k F;$$

далее доказываем делимость f_1' на φ_2 и, продолжая далее, убедимся, что f_2 делится на φ, что и требовалось доказать.

§ 27

Переходим теперь к доказательству обратного заключения § 23, а именно, что, если существует тождество $R_{k+1} = 0$, то функций f и φ имеют общие делители, заключающие букву x. Пусть

$$R_k = \omega \cdot S(x, y, z, \ldots),$$

где ω есть полином, не заключающей x и представляющий общий наибольший делитель всех коэффициентов при разных степенях x в R_k.

Тогда на основании последнего из равенств (1) § 24 мы имеем

$$P_k R_{k-1} = Q_k \omega S.$$

Функция P_k взаимно простая с S, ибо не содержит x, следовательно,

$$Q_k \omega = P_k T(x, y, z, \ldots)$$

и мы получаем

$$R_{k-1} = TS.$$

Подставляя в предыдущее равенство, будем иметь

$$P_{k-1} R_{k-2} = (Q_{k-1} T + \omega) S,$$

откуда подобно предыдущему получаем

$$R_{k-2} = T_1 S.$$

Итак, функция S, заключающая обязательно x, ибо первый остаток не заключающий x есть по предположению R_{k+1}, есть делитель обеих функций f и φ.

Покажем. что всякий общий делитель $\psi(x, y, z, \ldots)$ функций f и φ, не имеющий делителей без x, будет делителем функции S. В самом деле, ψ делит все остатки и, следовательно, получается

$$\omega S = \psi(x, y, z, \ldots)\psi_1(x, y, z, \ldots),$$

но ψ и ω взаимно простые, следовательно, ψ делит S, что и требовалось показать.

Итак, *если $R_{k+1} = 0$, то общий наибольший делитель функций f и φ, заключающей x и освобожденный от всяких делителей без x, получится, если из $R_k(x, y, z, \ldots)$ удалить все подобные делители.*

§ 28

Теперь мы подходим к завершению рассуждений последних параграфов, а именно к доказательству справедливости арифметической теории во всех подробностях для функций, заключающих букву x, если справедливость ее известна для функций без x.

Все основывается на теореме:

Если рассматриваются три функции

$$f(x, y, z, \ldots), \qquad \varphi(x, y, z, \ldots), \qquad \psi(x, y, z, \ldots),$$

причем функция ψ не приводимая и делит произведение $f\varphi$, то ψ должна делит одну из функций f или φ.

Если функция ψ не делит функцию f, то функций f и ψ взаимно простые, ибо ψ функция неприводимая. В этом случай, при применении алгоритма § 24 к двум функциям f и ψ мы должны дойти до остатка, не заключающего x и не тождественно равного нулю. Пусть этот остаток будет R_{k+1}. Применяя соображения § 18, мы получим

$$R_{k+1} = f(x, y, z, \ldots)F(x, y, z, \ldots) + \psi(x, y, z, \ldots)\Psi(x, y, z, \ldots), \tag{1}$$

где F и Ψ известным образом подобранные целые функции.

Умножаем тождество (1) на $\varphi(x, y, z, \ldots)$. Получаем в правой части полином, делящийся на ψ так, что будет

$$R_{k+1}(y, z, \ldots)\varphi(x, y, z, \ldots) = \psi(x, y, z, \ldots)\omega(x, y, z, \ldots).$$

На основании неприводимости ψ, эта функций может иметь только постоянный множитель с R_{k+1}, следовательно, φ делится на ψ.

Следствие I. *Если произведение*

$$f_1(x, y, z, \ldots)f_2(x, y, z, \ldots) \cdots f_k(x, y, z, \ldots)$$

делится на неприводимую функцию $\psi(x, y, z, \ldots)$, то один из множителей должен делится на ψ.

Из этой теоремы вытекает на основании соображений, подобных приводимым в теории чисел, единственность разложения целой функций на неприводимые множители, если не считать за различные функции, отличающиеся на постоянный множитель.

§ 29

Если функция φ делит произведение $f_1 f_2 \cdots f_k$, но не делит ни одного множителя f, то функция φ *не может* быть неприводимою.

Рассмотрим для примера тождество

$$\frac{a_1xy + b_1x + c_1y + d_1}{a_2xy + b_2x + c_2y + d_2} = \frac{a_3xy + b_3x + c_3y + d_3}{a_4xy + b_4x + c_4y + d_4}$$

причем не равен нулю определитель

$$\begin{vmatrix} a_1 & b_1 & c_1 & d_1 \\ a_2 & b_2 & c_2 & d_2 \\ a_3 & b_3 & c_3 & d_3 \\ a_4 & b_4 & c_4 & d_4 \end{vmatrix}. \tag{1}$$

Освобождаясь от знаменателей, мы заметим, что функция $a_1xy+b_1x+c_1y+d_1$ делит произведение

$$(a_2xy + b_2x + c_2y + d_2)(a_3xy + b_3x + c_3y + d_3), \tag{2}$$

но в тоже самое время она не может делить ни одного из множителей произведения (2), ибо иначе определитель (1) равнялся бы нулю. Итак, рассматриваемая функция приводимая, то есть

$$a_1xy + b_1x + c_1y + d_1 = (\alpha x + \beta)(\gamma x + \delta).$$

§ 30

Если функция целая φ делить степень f^n, где f функция неприводимая, то

$$\varphi = f^k.$$

Приложим эту теорему к рассмотрению одного определителя.

Пусть задан определитель $A = |a_{ik}|$. Обозначим

$$\mathfrak{a}^{(i)}_{ki} = \begin{pmatrix} a_{ik} & 0 & 0 & \dots & 0 \\ 0 & a_{ik} & 0 & \dots & 0 \\ 0 & 0 & a_{ik} & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & a_{ik} \end{pmatrix},$$

где l обозначает число горизонталей и колонн, все диагональные элементы суть a_{ik}, а остальные — нули.

Требуется вычислить определитель

$$\mathfrak{a}^{(l)} = \begin{vmatrix} \mathfrak{a}^{(l)}_{11} & \mathfrak{a}^{(l)}_{12} & \dots & \mathfrak{a}^{(l)}_{1n} \\ \mathfrak{a}^{(l)}_{21} & \mathfrak{a}^{(l)}_{22} & \dots & \mathfrak{a}^{(l)}_{2n} \\ \dots & \dots & \dots & \dots \\ \mathfrak{a}^{(l)}_{n1} & \mathfrak{a}^{(l)}_{n2} & \dots & \mathfrak{a}^{(l)}_{nn} \end{vmatrix}. \tag{1}$$

Для пояснения этого знака заметим, что, если

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

то при $l = 2$ получим

$$\mathfrak{a}^{(2)} = \begin{vmatrix} a_1 & 0 & a_2 & 0 & a_3 & 0 \\ 0 & a_1 & 0 & a_2 & 0 & a_3 \\ b_1 & 0 & b_2 & 0 & b_3 & 0 \\ 0 & b_1 & 0 & b_2 & 0 & b_3 \\ c_1 & 0 & c_2 & 0 & c_3 & 0 \\ 0 & c_1 & 0 & c_2 & 0 & c_3 \end{vmatrix}.$$

Для вычисления определителя (1) рассмотрим новый, который получается, если все нули оставить на прежних местах, а вместо элементов a_{ik} определителя A подставить их алгебраические дополнения A_{ik}.

Обозначим этот новый определитель через $\mathfrak{a}_1^{(l)}$. Тогда произведение $\mathfrak{a}^{(l)}\mathfrak{a}_1^{(l)}$, как не трудно видеть, будет определителем порядка nl, все диагональные элементы которого будут A, а остальные — нули. Следовательно,

$$\mathfrak{a}^{(l)}\mathfrak{a}_1^{(l)} = A^{nl}.$$

На основании неприводимости буквенного определителя A мы заключаем

$$\mathfrak{a}^{(l)} = A^k.$$

Не трудно однако, сравнивая показатели над одной какой нибудь буквой, получить $k = l$, так что окончательно

$$\mathfrak{a}^{(l)} = A^l.$$

§ 31

Здесь упомянем без доказательства весьма важную и общую теорему Hilbert'a,[35] а именно, *можно во всякой не приводимой целой функции от любого числа переменных независимых подставить вместо любой части этих переменных такие рациональные числа, что функция относительно остальных переменных будет по прежнему неприводимой.*

Свойства целых рациональных инвариантов

§ 32

Приложим теперь выше изложенные теоремы к доказательству ряда весьма важных замечаний, относящихся к целым рациональным инвариантам.

Очевидно, что всякое произведение нескольких целых инвариантов будет опять целым инвариантом, при этом вес произведения равен сумме весов отдельных множителей. Докажем теперь предложение обратное.

Теорема. *Целый рациоиальный инвариант*

$$I(a_1, a_2, \ldots)$$

[35]Hilbert. Ueber die Irreducibilität ganzer rationalen Functionen mit ganz Coöfficienten. Journ. f. r. u. ang. Math. B. 110.

формы $f(a_1, a_2, \ldots; x_1, x_2, \ldots)$ *есть такая функция, каждый целый множитель которой есть также иивариант.*

Очевидно, что достаточно доказать теорему только для неприводимых множителей $\varphi_1, \varphi_2, \ldots, \varphi_k$ инварианта I.

Подвергнем формулу f линейному преобразование модуля c, и пусть $a'_1, a'_2, \ldots$ суть новые коэффициенты. По свойству инвариантов имеем

$$I(a'_1, a'_2, \ldots) = c^\mu I(a_1, a_2, \ldots).$$

Разлагая обе части на неприводимые множители, получим

$$\varphi_1(a'_1, a'_2, \ldots) \cdots \varphi_k(a'_1, a'_2, \ldots) = c^\mu \varphi_1(a_1, a_2, \ldots) \cdots \varphi_k(a_1, a_2, \ldots),$$

ибо определитель общего вида c есть функция неприводимая. Каждый множитель φ_i левой части есть функция, как от элементов определителя, так и от первоначальных коэффициентов $a_1, a_2, \ldots$ формы f.

Следовательно, должно быть

$$\varphi_i(a'_1, a'_2, \ldots) = c^j \psi(a_1, a_2, \ldots), \tag{1}$$

где ψ есть целая функция, равная произведение одной или нескольких функций $\varphi_i(a_1, a_2, \ldots) \cdots \varphi_k(a_1, a_2, \ldots)$.

Применяя тождество (1) к случаю тождественного преобразования $c = 1$, получим

$$a'_1 = a_1, \quad a'_2 = a_2, \ \ldots$$

и, следовательно, равенство (1) дает тождество

$$\varphi_i(a_1, a_2, \ldots) = \psi(a_1, a_2, \ldots),$$

так, что получаем окончательно равенство

$$\varphi_i(a'_1, a'_2, \ldots) = c^j \varphi_i a_1, a_2, \ldots),$$

показывающее, что функция φ_i есть инвариант, и теорема доказана,

§ 33

Если бы мы захотели обобщить понятие инварианта таким образом, что назвали бы инвариантом такую функцию $I(a_1, a_2, \ldots)$ коэффициентов формы f, которая при преобразовании с модулем $c = |c_{ik}|$ получает множителем некоторую целую функцию

$$\psi(c_{11}, c_{12}, \ldots, c_{nn}),$$

то эта функция не может быть ничем иным, как степенью модуля. Таким образом мы не получаем никакого обобщения.

Для доказательства этого обстоятельства приведем предварительно следующую лемму.

Если заданы две целые функции f *и* φ *от произвольного числа переменных независимых, из которых* φ *неприводимая; то если* f *обращается в нуль для всех*

значений переменных независимых, уничтожающих функцию φ, то f делится на φ.

Если f не делится на φ, то функций f и φ взаимно простые. Производя последовательные деления по одной из общих независимых переменных, которую обозначить через x, мы дойдем до неравного тождественно нулю остатка $R(y, z, \ldots)$, заключающая другие переменные независимые $y, z, \ldots$. Так как функция φ заключает по предположению x, то можем написать

$$\varphi(x, y, z, \ldots) = a_0(y, z, \ldots)x^n + a_1(y, z, \ldots)x^{n-1} + \ldots,$$

где $a_0(y, z, \ldots)$ не равна тождественно нулю.

Итак, произведение

$$R(y, z, \ldots) \cdot a_0(y, z, \ldots)$$

не равно тождественно нулю, и, следовательно, можно указать такие значения $y_1, z_1, \ldots$ независимых переменных, что будет

$$R(y_1, z_1, \ldots) \neq 0, \qquad a_0(y_1, z_1, \ldots) \neq 0. \tag{1}$$

Полином $\varphi(x, y, z, \ldots)$ будет заключать x, следовательно он будет обращаться в нуль по крайней мере для одного значения x_1 переменного x

$$\varphi(x_1, y_1, z_1, \ldots) = 0;$$

тогда по предположению $f(x_1, y_1, z_1, \ldots) = 0$, а, следовательно, на основании тождества $R = fF + \varphi\Phi$ и $R = 0$, что противоречить неравенству (4). Итак, f действительно должна делиться на φ.

Обращаемся теперь к доказательству поставленного в начале параграфа утверждения; для этой цели покажем, что функция $\psi(c_{11}, \ldots, c_{nn})$ обращается в нуль только при таких значениях c_{ik}, при которых равняется нулю модуль $c = |c_{ik}|$ преобразования. В самом деле, допустим обратное, а именно, что при некоторых частных значениях γ_{ik} коэффициентов c_{ik} *обращается в нуль* функция ψ, а модуль *с неравен* нулю.

Итак, допустим, что

$$I(a'_1, a'_2, \ldots) = \psi(c_{11}, \ldots, c_{nn})I(a_1, a_2, \ldots). \tag{1}$$

Возьмем такую систему начальных значений коэффициентов $a_1, a_2, \ldots$, при которых

$$I(a_1, a_2, \ldots) \neq 0. \tag{2}$$

Применяя преобразование с коэффициентами γ_{ik}, получим

$$I(a'_1, a'_2, \ldots) = \psi(\gamma_{11}, \ldots, \gamma_{nn})I(a_1, a_2, \ldots) = 0;$$

обозначая через γ'_{ik} коэффициенты преобразования обратного, получим

$$I(a_1, a_2, \ldots) = \psi(\gamma'_{11}, \ldots, \gamma'_{nn})I(a_1,', a'_2, \ldots) = 0,$$

что противоречить неравенству (2). Следовательно, при $\psi = 0$ должно быть также и $c = 0$.

Разложим ψ на неприводимых множителей

$$\psi(c_{11}, \ldots, c_{nn}) = \varphi_1(c_{11}, \ldots) \cdots \varphi_k(c_{11}, \ldots). \tag{3}$$

Если для некоторых значений c_{ik} обращается в нуль один из неприводимых множителей, например, φ_i, то должен тогда обращаться в нуль и модуль c преобразования. На основании доказанной леммы функция φ_i должна быть делителем определителя c, рассматриваемого как функция от c_{ik}. Но определитель есть функция неприводимая, следовательно, φ_i может отличаться только постоянным множителем от c. Значит, тождество (3) можно переписать так: $\psi = Lc^k$, где L постоянная величина.

Перепишем теперь тождество (1) так

$$I(a'_1, \ldots) = Lc^k I(a_1, \ldots)$$

и применим тождественное преобразование, то получим $L = 1$, следовательно, будем иметь окончательно

$$\psi = c^k.$$

Свойство изобаричности

§ 34

Рассмотрим целую функцию от нескольких переменных независимых

$$\sum Ax^\lambda y^\mu z^\nu \cdots t^\rho. \tag{1}$$

Сопоставим каждой переменной независимой некоторое целое число, которое мы назовем ее *весом*.

Пусть переменные

$$x, \quad y, \quad z, \ \ldots, \ t$$

будут иметь веса

$$l, m, n, \ \ldots, \ r.$$

Выражение

$$l\lambda + m\mu + n\nu + \ldots + r\rho$$

мы будем называть *весом члена*

$$Ax^\lambda y^\mu z^\nu \cdots t^\rho.$$

Наибольшей из весов отдельных членов мы назовем *весом* всей целой функции (1).

Как частный случай понятие о весе можно рассматривать данное в § 1 главе I понятие о степени.

Это тот частный случай, когда всем переменным независимым приписывается вес 1, т. е.

$$l = 1, \quad m = 1, \quad n = 1, \ \ldots, \ r = 1. \tag{2}$$

Мы будем функцию (1) называть *изобарическою*, если веса всех ее отдельных членов одинаковы. В случае (2) понятие об изобаричностн совпадает с данным нами в § 2 главы I понятием однородности.

§ 35

Будем рассматривать веса различных членов инварианта

$$I(a_1, a_2, \ldots),$$

представляющего из себя целую функцию от коэффициентов a_i формы

$$\sum a_i x^\lambda y^\mu z^\nu \cdots t^\rho. \tag{1}$$

Будем придавать коэффициентам a_i веса в зависимости от той или другой выбранной переменной независимой. Если выберем переменную независимую x, то установим вес коэффициента a_i по показателю λ над x. Итак, коэффициент a_i имеет вес λ относительно x, вес μ — относительно y, вес ν — относительно z и т. д.

Докажем изобаричность целого инварианта формы относительно каждой переменной независимой.

Будем рассматривать одну из переменных, например, x; то, что будет сказано относительно нее, будет, очевидно, годиться для каждой из остальных.

Если мы сделаем линейное преобразование

$$x = cx', \quad y = y', \quad z = z', \ \ldots, \ t = t' \tag{2}$$

с модулем равным c, то форма (1) преобразуется в такую

$$\sum a'_i x'^\lambda y'^\mu z'^\nu \cdots t'^\rho,$$

где

$$a'_i = a_i c^\lambda.$$

Итак, *вес каждого из коэффициентов a_i формы можно определить как показателя степени величины c, на которую умножается a_i при преобразовать (2).*

Отсюда следует, что изобарический по отношеипо к x полином веса λ приобретает c^λ множителем при преобразовании (2).

Справедливо также обратное свойство, а именно, что, если, полином от коэффициентов формы получает при преобразовали (2) множитель c^λ, то он есть изобарическая относительно x функций веса λ.

Пусть

$$f(a'_1, \ldots) = c^\lambda f(a_1, \ldots). \tag{3}$$

Разобьем функцию f на отдельные изобарические части

$$f(a_1, \ldots) = f_1(a_1, \ldots) + f_2(a_1, \ldots) + \ldots, \tag{4}$$

где f_1 есть совокупность членов веса λ_1, f_2 — веса λ_2 и т. д. Мы будем иметь

$$f(a'_1, \ldots) = c^{\lambda_1} f_1(a_1, \ldots) + c^{\lambda_2} f_2(a_1, \ldots) + \ldots \tag{5}$$

На оснований (3) и (4) получаем

$$f(a'_1, \ldots) = c^{\lambda} f_1(a_1, \ldots) + c^{\lambda} f_2(a_1, \ldots) + \ldots$$

Правая часть последнего равенства должна быть тождественно равна правой части равенства (5), и мы получаем

$$\lambda = \lambda_1 = \lambda_2 = \ldots$$

Мы приходим, действительно, к заключенно: *полином f, составленный из коэффициентов формы, получает при преобразовании (2) множитель c^{λ} тогда и только тогда, когда он изобарический относительно x и имеет вес λ.*

§ 36

На основании соображений предыдущего параграфа мы приходим к следующему заключению:

Целый рациональный инвариант веса λ[36] *есть относительно всякой переменной изобарическая функция веса λ.*

Это свойство нзобаричности сохраняется для инвариантов всякой системы, состоящей из нескольких форм.

Нетрудно убедиться, что всякий целый рациональный инвариант имеет положительный вес, отличный от нуля; стоит для этой цели принять только в соображение, что вес всякого коэффициента a_i не меньше единицы по которой нибудь из букв.

§ 37

Обращаясь к рассмотрению веса ковариантa, можем переписать преобразовало (2) в таком виде

$$x' = c^{-1}x, \quad y' = c^0 y, \quad z' = c^0 z, \ \ldots, \ t' = c^0 t,$$

другими словами, при рассмотрений весов по отношение к букве x придется придавать для когредаентных переменных вес -1 букве аналогичной x и вес 0 всем остальным. При таком условии мы придем к изобаричности всякого ковариантa.

§ 38

Поясним изложенную теорию на примере.

Возьмем квадратичную форму

$$ax^2 + 2bxy + cy^2.$$

Коэффициент a имеет вес 2 по x и вес 0 по y.

[36] В смысле § 6. Гл. VI.

Инвариант $ac - b^2$ будет иметь вес 2 по любой из букв x и y.

Полярная форма

$$ax_1x_2 + b(x_1y_2 + x_2y_1) + cy_1y_2$$

будет ковариантом нулевого веса.

Принцип однородности

§ 39

Рассмотрим сверхповерхность[37] в пространстве $n-1$ измерений определяемую уравнением

$$f(a_1, a_2, \ldots; , x_1, \ldots, x_n) = 0, \tag{1}$$

где форма f относительно x_i. Эта форма будет однородною функциею первой степени относительно коэффициентов a_i. Очевидно, что сверхповерхность не изменяется; если умножить все коэффициенты a_i на одно и тоже отличное от нуля число c; т. е. уравнение

$$f(ca_1, ca_2, \ldots; , x_1, \ldots, x_n) = 0 \tag{2}$$

определяет туже сверхповерхность, что и (1).

На простых примерах можно показать следующий интересный факт, что соотношение между коэффициентами

$$\varphi(a_1, a_2, \ldots) = 0$$

не всегда выделяет из всей совокупности сверхповерхностей некоторый *класс*.

Возьмем уравнение плоскости в трехмерном пространств

$$f(a_1, a_2, a_3, a_4; x, y, z, 1) = 0;$$

это уравнение имеет вид

$$a_1x + a_2y + a_3z + a_4 = 0. \tag{3}$$

Соотношение

$$a_4 = 0$$

выделяет класс плоскостей, проходящих через начало координат.

Соотношение же

$$a_4 = 1 \tag{4}$$

не выделяет никакого класса, ибо через деление уравнения (3) всякой плоскости (не проходящей через начало координат) на a_4 мы удовлетворим соотношений (4).

Приняв сказанное в соображение, предположим, что соотношение

$$\varphi(a_1, a_2, \ldots) = 0 \tag{5}$$

[37]См. стр. 165

выделяет некоторый класс сверхповерхностей.

Мы будем говорить, что соотношение (5) выражает некоторое *геометрическое свойство* сверхповерхностей этого класса.

§ 40

Теорема. *Соотношение $\varphi = 0$, где φ целая рациональная функция от коэффициентов a_i уравнения сверхповерхности тогда и только тогда выражает геометрическое свойство сверхповерхности, когда φ есть однородная функция от a_i.*

Если φ *не однородная* функция, то она раскладывается на сумму однородных

$$\varphi = \varphi_m + \varphi_{m-1} + \ldots + \varphi_1 + \varphi_0,$$

где знаком φ_k? обозначена однородная функция степени k; мы, конечно, предполагаем, что кроме φ_m еще по крайней мере одна из φ_k не равна тождественно нулю.

Представим уравнение сверхповерхности в таком виде

$$f(ca'_1, ca'_2, \ldots; x_1, \ldots, x_n) = 0, \tag{1}$$

где c произвольная переменная величина, а числа $a'_1, a'_2, \ldots$ такие значения коэффициентов $a_1, a_2, \ldots$, при которых не обращаются в нуль φ_m и по крайней мере одна из следующих φ_k.

Соотношение $\varphi = 0$ принимает вид

$$c^m \varphi_m(a'_1, a'_2, \ldots) + c^{m-1}\varphi_{m-1}(a'_1, a'_2 \ldots) + \ldots = 0. \tag{2}$$

Так как в уравнений (2) кроме старшего коэффициента φ_m не равен нулю по крайней мере еще один, то это уравнение имеет по крайней мере один отличный от нуля корень c_1. Возьмем новое значение c_2, не удовлетворяющее уравнение (2). Мы приходим к заключению, что при $c = c_1$ и $c = c_2$ уравнение (1) определяет одну и туже сверхноверхность, между тем как в первом случае соотношение $\varphi = 0$ удовлетворяется, а во втором нет. Следовательно, соотношение $\varphi = 0$ не представляет геометрического свойства.

Можно показать обратное свойство, а именно, что если φ однородная функция степени m, то соотношение $\varphi = 0$ дает геометрическое свойство сверхповерхности (1). Для этой цели надо доказать, что все сверхповерхности распадаются на два класса A и B, причем сверхповерхности класса A удовлетворяют соотношений $\varphi = 0$, а взятые из класса B не удовлетворяют.

Пусть $a'_1, a'_2, \ldots$ будут коэффициенты одной из сверхповерхностей класса A, а $a''_1, a''_2, \ldots$ будут коэффициенты сверхповерхности из класса B. Нужно показать, что два уравнения

$$f(a'_1, a'_2, \ldots; x_1, \ldots, x_n) = 0$$
$$f(a''_1, a''_2, \ldots; x_1, \ldots, x_n) = 0$$

не могут давать одну и туже сверхповерхность, другими словами, что не существует пропорции

$$a''_1 = ca'_1, \quad a''_2 = ca'_2, \ \ldots,$$

где $c \neq 0$.

Из однородности φ следует

$$\varphi(a_1'', a_2'', \ldots) = c^m \varphi(a_1', a_2', \ldots),$$

если мы допустим существование пропорции. Последнее же равенство невозможно, ибо по предположению

$$\varphi(a_1', a_2', \ldots) = 0, \qquad \varphi(a_1'', a_2'', \ldots) \neq 0,$$

и теорема доказана.

§ 41

Итак, мы видим, что в геометрии особое значение имеют однородные инварианты.

Пусть рассматриваются формы

$$\begin{aligned} &f_1(a, \ldots; x_1, \ldots, x_n) = 0 \\ &f_2(b, \ldots; x_1, \ldots, x_n) = 0 \\ &\ldots\ldots\ldots\ldots\ldots\ldots \end{aligned} \tag{1}$$

степеней $m_1, m_2, \ldots$ относительно x_i.

Сделаем преобразование $x = \mathfrak{c}x'$ с матрицей

$$\mathfrak{c} = \|c_{ik}\|,$$

тогда формы (1) перейдут в новые

$$\begin{aligned} &f_1(a', \ldots; x_1', \ldots, x_n') = 0 \\ &f_2(b', \ldots; x_1', \ldots, x_n') = 0 \\ &\ldots\ldots\ldots\ldots\ldots\ldots \end{aligned} \tag{2}$$

Новые коэффициенты a' будут, очевидно, целыми функциями однородными первой степени относительно первоначальных коэффициентов и однородными степени m_i? от c_{ik}. Подобным же образом b' будут первой степени относительно b и степени m_2 относительно c_{ik} и так далее.

§ 42

Рассмотрим инвариант

$$I(a, \ldots; b, \ldots; \ldots)$$

веса λ системы форм (1) § 40. Пусть этот инвариант будет однородной функцией степени α относительно a, однородной функцией степени β относительно b и т. д.

Рассматривая тождество

$$I(a', \ldots; b', \ldots; \ldots) = c^\lambda I(a, \ldots; b, \ldots; \ldots), \tag{1}$$

сравним степени его обеих частей относительно элементов c_{ik} преобразования. Левая часть будет иметь степень

$$m_1\alpha + m_2\beta + \ldots,$$

ибо a' степени m_1, b' степени m_2 и т. д.

Правая же часть равенства (1) имеет относительно c_{ik} степень $n\lambda$. Мы приходим к весьма важному равенству

$$m_1\alpha + m_2\beta + \ldots = n\lambda.$$

§ 43

Теорема. *Если целый рациональный инвариант*

$$I = I_1 + I_2 + \ldots + I_r$$

есть сумма функций I_i, из которых каждая, но не сумма двух из них однородна по отношению к коэффициентам $a, b, \ldots$ каждой из форм в отдельности, то функции

$$I_1, \quad I_2, \ \ldots, \ I_r$$

будут однородными инвариантами системы (1) § 40.

Напишем свойство инвариантности I:

$$\begin{gathered} I_1(a', \ldots; b', \ldots; \ldots) + \ldots + I_r(a', \ldots; b', \ldots; \ldots) = \\ = c^\lambda[I_1(a, \ldots; b, \ldots; \ldots) + \ldots + I_r(a, \ldots; b, \ldots; \ldots)]. \end{gathered}$$

Принимая в соображение, что все a' суть формы первой степени относительно a, что все b' также первой степени относительно b и т. д., и сравнивая однородные функции одинаковых степеней относительно $a, b, \ldots$, получим

$$\begin{gathered} I_1(a'_1, \ldots; b', \ldots; \ldots = c^\lambda I_1(a, \ldots; b, \ldots; \ldots) \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ I_r(a'_1, \ldots; b', \ldots; \ldots = c^\lambda I_r(a, \ldots; b, \ldots; \ldots), \end{gathered}$$

и теорема доказана.

§ 44

Теорема. *Всякий целый рациональный инвариант одной формы есть однородная функция ее коэффициентов.*

Итак, пусть I будет инвариант формы

$$f(a, \ldots; x_1, \ldots, x_n).$$

Разлагая инвариант I на однородные инварианты, получим

$$I = I_1 + I_2 + \ldots + I_r.$$

Пусть степени инвариантов $I_1, I_2, \ldots, I_r$ относительно a будут $\alpha_1, \alpha_2, \ldots, \alpha_r$.

Обозначая через m степень формы f, получим для однородных инвариантов (см. § 41) ряд равенств

$$m\alpha_1 = n\lambda, \quad m\alpha_2 = n\lambda, \ \ldots, \ m\alpha_r = n\lambda,$$

откуда

$$\alpha_1 = \alpha_2 = \ldots = \alpha_r,$$

и теорема доказана.

Глава IX

Симметрические функции

Неизменяемость функции при подстановках переменных

§ 1

Основной задачей настоящей главы будет рассмотрение свойств функций от n букв

$$x_1,\ \ x_2,\ \ldots,\ x_n, \tag{1}$$

не меняющихся при подстановках этих букв.

Здесь надо точно различать два различных случая:

1-ый случай, когда независимые переменные (1) суть буквы, которым никаких определенных численных значений не сопоставляется.

2-ой случай, когда буквы (1), входящие в состав функции, имеют определенные численные значения.

Поэтому, когда мы говорим, что функция не меняется от подстановки букв, то под этим мы разумеем одно из двух: или не меняется вид функций, или не меняется ее численное значение. Так, например, если мы над функцией

$$x_1x_2 + x_3x_4$$

произведем подстановку

$$\begin{pmatrix} x_2 & x_1 & x_4 & x_3 \\ x_1 & x_2 & x_3 & x_4 \end{pmatrix},$$

то вид функции не изменится, т. е. новое выражение будет тождественно равно предыдущему при всяких значениях букв. Если же возьмем Функцию

$$x_1 + x_2x_3 \tag{2}$$

и произведем подстановку

$$\begin{pmatrix} x_2 & x_3 & x_1 \\ x_1 & x_2 & x_3 \end{pmatrix},$$

то функция (2) примет вид

$$x_2 + x_3x_1. \tag{3}$$

Функция (3), очевидно, не равна тождественно функций (2); но, если мы укажем некоторое определенное численное значение переменным x_1, x_2, x_3, то эти

значения могут оказаться такими, что функции (2) и (3) будут одинаковы по численной величине; например, можно принять $x_1 = 1$, $x_2 = 1$, $x_3 = 1$.

§ 2

Рассмотрение функций, не меняющихся от подстановок, играет важную роль при решении уравнений в радикалах. Первый обратил на это внимание Lagrange. Он ограничивался рассмотрением только функций буквенных и понимал неизменность функций при подстановках лишь в смысле неизменности вида. Гениальный французский математик Evariste Galois обобщил теорию Lagrange'a, причем рассматривал также функции численные, а именно тот случай, когда независимый переменные числа и от подстановки независимых переменных не меняется численная величина функций. Получилась важная теория, в которой теория Lagrange'a оказывается лишь частным случаем и которая дает убедительный доказательства теоремы Abel'a о том, что общее уравнение выше 4-ой степени не решается в радикалах.

Функции симметрические

§ 3

Будем рассматривать функции, не меняющиеся при всех N подстановках букв. Такие функции будем называть *симметрическими*. Так как цель нашего исследования есть решение уравнений, то под независимыми переменными симметрической функций мы будем разуметь корни некоторого алгебраического уравнения степени n.

Итак, будем рассматривать алгебраическое уравнение

$$x^n + p_1 x^{n-1} + p_2 x^{n-2} + \ldots + p_{n-1} x + p_n = 0. \tag{1}$$

Обозначая корни этого уравнения через

$$x_1,\ \ x_2,\ \ x_3,\ \ldots,\ x_n,$$

мы видим, что коэффициенты

$$p_1,\ \ p_2,\ \ p_3,\ \ldots,\ p_n$$

будут целыми симметрическими функциями от этих корней.

Мы видели уже (см. стр. 17), что эти функции выражаются следующим образом

$$p_1 = -(x_1 + x_2 + \ldots + x_n) = -\sum x_i$$

$$p_2 = x_1x_2 + x_2x_3 + \ldots = \sum x_ix_j$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$p_n = (-1)^n x_1x_2x_3\cdots x_n.$$

Эти функции называются *простейшими* симметрическими функциями.

Главною целью дальнейших рассуждений будет доказательство теоремы.

Теорема. *Через указанным простейшие симметрические функции* $p_1, p_2, \ldots, p_n$ *выразится рационально всякая рациональная симметрическая функция от корней уравнения.*

Формулы Newton'a

§ 4

Для доказательства теоремы покажем сначала, как выразить через коэффициенты $p_1, p_2, \ldots, p_n$ уравнения сумму одинаковых степеней корней, т. е., другими словами, симметрическую функцию

$$s_k = x_1^k + x_2^k + \ldots + x_n^k \tag{1}$$

при различных целых показателях k.

Для вычисления функции s_k существуют формулы, данные еще Newton'ом (Arithmetica itiversalis).

Для вывода этих формул поступим так: полагая в формуле Lagrange'a (см. стр. 51)

$$\Omega(x) = F'(x),$$

получим

$$\frac{F'(x)}{F(x)} = \sum \frac{1}{x - x_j},$$

под функцией $F(x)$ мы будем разуметь первую часть уравнения

$$F(x) = x^n + p_1 x^{n-1} + \ldots + p_n = (x - x_1)(x - x_2)\cdots(x - x_n) = 0.$$

Отсюда получим формулу

$$F'(x) = \frac{F(x)}{x - x_1} + \frac{F(x)}{x - x_2} + \ldots + \frac{F(x)}{x - x_n}.$$

Так как x_i есть корень функции $F(x)$, то эта функция делится нацело на $x - x_i$; разделяя на самом деле, получим

$$\begin{array}{l|l}
x^n + p_1 x^{n-1} + p_2 x^{n-2} + \ldots + p_{n-1} x + p_n & x - x_i \\
\hline
-x^n - x_i x^{n-1} & x^{n-1} + \omega_1(x_i) x^{n-2} + \ldots + \omega_{n-1}(x_i) \\
\hline
(p_1 + x_i) x^{n-1} + p_2 x^{n-2} & \\
-(p_1 + x_i) x^{n-1} - x_i(x_i + p_1) x^{n-2} & \\
\hline
(x_i^2 + x_i p_1 + p_2) x^{n-2} & \\
\ldots\ldots\ldots\ldots\ldots\ldots & \\
\end{array}$$

где

$$\omega_1(x_i 0 = x_i + p_1, \quad \omega_2(x_i) = x_i^2 + x_i p_1 + p_2, \ \ldots,$$

так что

$$F'(x) = \sum_{i=1}^{i=n} \{x^{n-1} + \omega_1(x_i) x^{n-2} + \omega_2(x_i) x^{n-3} + \ldots + \omega_{n-1}(x_i)\},$$

или

$$F'(x) = nx^{n-1} + x^{n-2}\sum \omega_1(x_i) + x^{n-3}\sum \omega_2(x_i) + \ldots + \sum \omega_{n-1}(x_i). \tag{1}$$

Так как с другой стороны по правилам получения производной целой функции имеем

$$F'(x) = nx^{n-1} + (n-1)p_1x^{n-2} + (n-2)p_2x^{n-3} + \ldots + p_{n-1}, \tag{2}$$

то, сравнивая коэффициенты двух выражений (1) и (2) функции $F'(x)$, получим

$$\begin{aligned}
&\sum \omega_1(x_i) = (n-1)p_i,\\
&\sum \omega_2(x_i) = (n-2)p_2,\\
&\ldots\ldots\ldots\ldots\ldots\ldots,\\
&\sum \omega_{n-1}(x_i) = p_{n-1},
\end{aligned}$$

но

$$\begin{aligned}
&\sum \omega_1(x_i) = s_1 + np_i,\\
&\sum \omega_2(x_i) = s_2 + p_1s_1 + np_2,\\
&\sum \omega_3(x_i) = s_3 + p_1s_2 + p_2s_1 + np_3,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\
&\sum \omega_{n-1}(x_i) = s_{n-1} + p_1s_{n-2} + \ldots + np_{n-1},
\end{aligned}$$

следовательно, сопоставляй эти формулы, получим

$$\begin{aligned}
&s_1 + p_1 = 0,\\
&s_2 + p_1s_1 + 2p_2 = 0,\\
&s_3 + p_1s_2 + p_2s_1 + 3p_3 = 0,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\
&s_{n-1} + p_1s_{n-2} + p_2s_{n-3} + \ldots + (n-1)p_{n-1} = 0,
\end{aligned} \tag{3}$$

и, наконец, замечая тождество $F(x_i) = 0$ и суммируя его по всем корням, получим

$$\sum (x_i^n + p_1x_i^{n-1} + p_2x_i^{n-2} + \ldots + p_{n-1}x_i + p_n) = 0,$$

т. е. другими словами

$$s_n + p_1s_{n-1} + p_2s_{n-2} + \ldots + p_{n-1}s_1 + np_n = 0. \tag{4}$$

Равенства (3) и (4) дают n линейных уравнений для выражения неизвестных $s_1, s_2, \ldots, s_n$ через коэффициенты $p_1, p_2, \ldots, p_n$.

Систему этих линейных уравнений можно решить относительно $s_1, s_2, \ldots, s_n$, потому что определитель этой системы равняется единице. Получаем выражение искомых функций s

$$
\begin{aligned}
&s_1 = -p_1 \\
&s_2 = +p_1^2 - 2p_2, \\
&s_3 = -p_1^3 + 3p_1p_2 - 3p_3, \\
&s_4 = +p_1^4 - 4p_1^2p_2 + 4p_1p_3 + 2p_2^2 - 4p_4, \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots
\end{aligned} \tag{5}
$$

Очень важным является то обстоятельство, что все s выражаются целыми функциями с целыми коэффициентами от $p_1, p_2, p_3, \ldots, p_n$.

Обратно, при помощи формул (3) можно выразить рационально симметрическая функций $p_1, p_2, \ldots, p_n$ через суммы s_k; однако коэффициенты этих выражений будут уже дробные. Итак, получим

$$
\begin{aligned}
p_1 &= -s_1, \\
2p_2 &= \quad s_1^2 - s_2, \\
3p_3 &= -s_1^3 + 3s_1s_2 - 2s_3, \\
&\ldots\ldots\ldots\ldots\ldots\ldots
\end{aligned} \tag{6}
$$

§ 5

В предыдущем параграфе мы видели как вычислить функции s_k, когда значок k принимает целые положительные значения, не превосходящие значка n. Нетрудно убедиться, что малым изменением способа можно вычислить функцию s_k, как для значений $k > n$, так и для значений k отрицательных.

В самом деле, если мы возьмем тождество

$$x_i^{m-n} F(x_i) = 0,$$

где $m > n$, и просуммируем его по корням, т. е. напишем тождество

$$\sum_1^n x_i^{m-n} F(x_i) = 0,$$

то получим

$$s_m + p_1 s_{m-1} + \ldots + p_{n-1} s_{m-n+1} + p_n s_{m-n} = 0.$$

Последняя формула дает возможность вычислить s_m, когда известно выражение n предыдущих функций $s_{m-1}, \ldots, s_{m-n}$; значит, можно начать вычисление с функций s_{n+1}, выразив ее через известные уже $s_n, s_{n-1}, \ldots, s_2, s_1$.

§ 6

Совершенно подобным образом можно будет вычислить s_k с отрицательными значками k. В самом деле, тождество

$$\sum_1^n \frac{1}{x_i} F(x_i) = 0$$

дает

$$s_{n-1} + p_1 s_{n-2} + \ldots + p_{n-1} \cdot n + p_n s_{-1} = 0. \tag{1}$$

Последнее равенство дает возможность выразить s_{-1} через s_k с положительными значками k. Когда известна функция s_{-1} мы получим функцию s_{-2}, рассмотрев тождество

$$\sum_1^n \frac{1}{x_i^2} F(x_i) = 0,$$

которое перепишем так

$$s_{n-2} + p_1 s_{n-3} + \ldots + p_{n-2} \cdot n + p_{n-1} s_{-1} + p_n s_{-2} = 0. \tag{2}$$

Продолжая рассматривать тождество

$$\sum_1^n \frac{1}{x_i^k} F(x_i) = 0$$

с возрастающими положительными значками k, будем получать последовательно

$$s_{-3}, \quad s_{-4}, \quad \ldots$$

Заметим, что формулы (1) и (2), пользуясь формулами (3) § 4, можно переписать так

$$p_{n-1} + p_n s_{-1} = 0, \qquad 2p_{n-2} + p_{n-1} s_{-1} + p_n s_{-2} = 0.$$

Применяя формулы Newton'a к двучленному уравнению

$$x^n - 1 = 0,$$

получим

$$\begin{aligned}
&x_1 + x_2 + x_3 + \ldots + x_n = 0,\\
&x_1^2 + x_2^2 + x_3^2 + \ldots + x_n^2 = 0,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\
&x_1^{n-1} + x_2^{n-1} + x_3^{n-1} + \ldots + x_n^{n-1} = 0,\\
&x_1^n + x_2^n + x_3^n + \ldots + x_n^n = n.
\end{aligned}$$

Выражение симметрической функции от корней через коэффициенты

§ 7

Формулы Newton'a для вычисления функций s_k дают возможность выразить через коэффициенты $p_1, p_2, \ldots, p_n$ уравнения всякую рациональную симметрическую функцию от корней. Так как рациональная функция от корней есть отношение двух целых функций, то, следовательно, покажем, как вычислить целую симметрическую функцию от корней.

Самый общий вид целой функций от корней будет, конечно,

$$\sum A x_1^{\lambda_1} x_2^{\lambda_2} \cdots x_n^{\lambda_n}, \tag{1}$$

где $\lambda_1, \lambda_2, \ldots, \lambda_n$ некоторые целые положительные числа или нули.

Возьмем один из членов этой функций

$$Ax_1^{\lambda_1} x_2^{\lambda_2} \cdots x_n^{\lambda_n}. \tag{2}$$

Если функция симметрична в том смысле, что она не меняет вида от любой подстановки букв $x_1, x_2, \ldots, x_n$, то в составе нашей функции должен находиться всякий член такого вида, который получается из члена (2) от какой-нибудь подстановки корней. Отсюда замечаем, что в состав симметрической функции (1) должно входить выражение

$$A \sum x_1^{\lambda_1} x_2^{\lambda_2} \cdots x_n^{\lambda_n},$$

где под знаком $\sum$ показатели $\lambda_1, \lambda_2, \ldots, \lambda_n$ не меняются при переходе от одного члена к другому, сумма же распространена на всевозможные перемещения корней. Итак, замечаем, что общий вид целой симметрической функции от корней есть следующий

$$A \sum x_1^{\lambda_1} x_2^{\lambda_2} \cdots x_n^{\lambda_n} + B \sum x_1^{\mu_1} x_2^{\mu_2} \cdots x_n^{\mu_n} + \ldots + M \sum x_1^{\rho_1} x_2^{\rho_2} \cdots x_n^{\rho_n}.$$

Значит, задача вычисления целой симметрической функции самого общего вида приводится к вычисление функций

$$\sum x_1^{\lambda_1} x_2^{\lambda_2} \cdots x_n^{\lambda_n},$$

в которой ряд показателей $\lambda_1, \lambda_2, \ldots, \lambda_n$ представляет определенный ряд чисел, каждое из которых или целое положительное, или нуль, а сумма распространена на всевозможные перемещения корней.

§ 8

Рассмотрим функцию $\sum x_1^{\lambda_1} x_2^{\lambda_2} \cdots x_m^{\lambda_m}$, где $m \leq n$ и все показатели различны между собою. Легко убедиться в возможности выразить заданную функцию рационально через коэффициенты p_i, если будем последовательно рассматривать случаи

$$m = 1, \quad m = 2, \ \ldots$$

1-ый случай, $m = 1$.

$$\sum_1^n x_i^{\lambda_i} = s_{\lambda_1},$$

и вычисление функции нам уже известно.

2-ой случай, $m = 2$.

$$\sum x_i^{\lambda_1} x_k^{\lambda_2},$$

где сумма распространена на всевозможные сочетания (i, k) n чисел $1, 2, 3, \ldots, n$ по два. Нашу двойную сумму можно вычислить, производя суммирование сначала по букв k, потом по букве i.

Если желаем суммировать по букве k, надо число i считать определенным числом. Тогда для k возможны все численные значения $1, 2, 3, \ldots, n$, исключая

значение i, потому что мы не рассматриваем сочетаний корней с повторениями индексов; и у нас выходит

$$\sum_{i,k} x_i^{\lambda_1} x_k^{\lambda_2} = \sum_i x_i^{\lambda_1} \left\{ \sum_k x_k^{\lambda_2} - x_i^{\lambda_2} \right\} = \sum_i x_i^{\lambda_1} \cdot \sum_k x_k^{\lambda_2} - \sum_i x_i^{\lambda_1+\lambda_2} =$$

$$= \sum_k x_k^{\lambda_2} \cdot \sum_i x_1^{\lambda_1} - \sum_i x_i^{\lambda_1+\lambda_2} = s_{\lambda_2} s_{\lambda_1} - s_{\lambda_1+\lambda_2},$$

а так как s_k мы умеем вычислить, то и заданная двойная сумма получается, как функция от коэффициентов.

3-ий случай, $m = 3$.

$$\sum_{i,k,l} x_i^{\lambda_1} x_k^{\lambda_2} x_l^{\lambda_3}.$$

Так как перемещения (i, k, l) нндексов должны быть перемещениями без повторений элементов, то, если начнем суммирование по значку l, то ему мы имеем право дать все значения от 1 до n, кроме i и k, и мы получаем

$$\sum_{i,k,l} x_i^{\lambda_1} x_k^{\lambda_2} x_l^{\lambda_3} = \sum_{i,k} x_i^{\lambda_1} x_k^{\lambda_2} \left\{ \sum_l x_l^{\lambda_3} - x_i^{\lambda_3} - x_k^{\lambda_3} \right\} =$$

$$= \sum_l x_l^{\lambda_3} \cdot \sum_{i,k} x_i^{\lambda_1} x_k^{\lambda_2} - \sum_{i,k} x_i^{\lambda_1+\lambda_3} x_k^{\lambda_2} - \sum_{i,k} x_i^{\lambda_1} x_k^{\lambda_2+\lambda_3},$$

и тройную сумму привели к вычислению

$$\sum_l x_l^{\lambda_3} = s_{\lambda_3},$$

и к вычислению трех двойных сумм. На основании формулы предыдущего случая получаем окончательно

$$\begin{aligned} \sum_{i,k,l} x_i^{\lambda_1} x_k^{\lambda_2} x_l^{\lambda_3} &= s_{\lambda_3}(s_{\lambda_1} s_{\lambda_2} - s_{\lambda_1+\lambda_2}) - (s_{\lambda_1+\lambda_3} s_{\lambda_2} - s_{\lambda_1+\lambda_2+\lambda_3}) - \\ &- (s_{\lambda_1} s_{\lambda_2+\lambda_3} - s_{\lambda_1+\lambda_2+\lambda_3}) = s_{\lambda_1} s_{\lambda_2} s_{\lambda_3} - s_{\lambda_1} s_{\lambda_2+\lambda_3} - \\ &- s_{\lambda_2} s_{\lambda_1+\lambda_3} - s_{\lambda_3} s_{\lambda_1+\lambda_2} + 2 s_{\lambda_1+\lambda_2+\lambda_3}. \end{aligned} \tag{1}$$

Наконец, не может представить затруднения рассмотрение случаев $m = 4$, $m = 5$, и т. д.; рассуждения будут те же. Сделав суммирование по одному из m значков с пропуском, конечно, $m-1$ элемента, мы приведем все вычисление сумм m-го порядка к вычислению ряда сумм меньшего порядка.

Итак, можно считать доказанным, что *всякая симметрическая рациональная функция от корней как целая, так и дробная, выражается рационально через коэффициенты уравнения.*

Необходимо сделать весьма важное добавление относящееся к случаю, когда среди показателей $\lambda_1, \lambda_2, \ldots, \lambda_m$ существует k одинаковых. В этом случай надо результат, найденный по общим формулам разделить на $1 \cdot 2 \cdot 3 \cdots k$. В самом деле,

если $\lambda_1 = \lambda_2 = \ldots = \lambda_k$, то от перестановки переменных независимых $x_1, x_2, \ldots, x_k$ получается один и тот же член. Из формулы (1) мы получаем при $\lambda_1 = \lambda_2$

$$\sum x_i^{\lambda_1} x_2^{\lambda_1} x_l^{\lambda_3} = \frac{1}{1 \cdot 2} \{s_{\lambda_1}^2 s_{\lambda_3} - 2 s_{\lambda_1} s_{\lambda_1+\lambda_3} - s_{\lambda_3} s_{2\lambda_1} + 2 s_{2\lambda_1+\lambda_3}\},$$

а при $\lambda_1 = \lambda_2 = \lambda_3$

$$\sum (x_i x_k x_l)^{\lambda_1} = \frac{1}{1 \cdot 2 \cdot 3} \{s_{\lambda_1}^3 - 3 s_{\lambda_1} s_{2\lambda_1} + 2 s_{3\lambda_1}\}.$$

Метода Cauchy

§ 9

Укажем еще один способ вычисления симметрических функций, предложенный Cauchy.

Рассмотрим сперва случай двух корней α и β, т. е. случай квадратного уравнения

$$x^2 + ax + b = (x - \alpha)(x - \beta) = 0.$$

Пусть будет задана целая симметрическая функция

$$G(\alpha, \beta)$$

двух корней; замечая, что $a = -\alpha - \beta$, подставим в $G(\alpha, \beta)$ вместо β величину $-a - \alpha$

$$G(\alpha, -a - \alpha).$$

Расположила G по степеням α, получим

$$G(\alpha, -a - \alpha) = A_0 \alpha^m + A_1 \alpha^{m-1} + \ldots + A_{m-1}\alpha + A_m,$$

где $A_0, A_1, \ldots, A_m$ суть целые функций с целыми коэффициентами от α и от коэффициентов заданной функции G.

Обозначая через $\varphi(x)$ функций

$$A_0 \alpha^m + A_1 \alpha^{m-1} + \ldots + A_{m-1}\alpha + A_m$$

разделим ее на $f(x) = x^2 + ax + b$; тогда, обозначая частное через $Q(x)$, а остаток через $A + Bx$, получим

$$\varphi(x) = f(x) \cdot Q(x) + A + Bx, \tag{1}$$

где A и B суть целые рациональные функции от коэффициентов a и b (это следует из того, что коэффициент при высшем члене x^2 делителя равен единице и коэффициентов функции G.

Подставляя в тождество (1) вместо x корень α функции $f(x)$, получаем

$$\varphi(\alpha) = G(\alpha, \beta) = A + B\alpha. \tag{2}$$

Меняя на основании симметричности функции $G(\alpha, \beta)$ в тождестве (2) порядок букв α и β, получаем

$$G(\alpha, \beta) = A + B\beta. \tag{3}$$

Так как α и β независимые переменные, то B должно равняться нулю, ибо в противном случае тождество

$$A + B\alpha = A + B\beta$$

устанавливало бы зависимость между α и β.

Итак, $B = 0$; тогда

$$G(\alpha, \beta) = A,$$

т. е. симметрическая функция G выражается рационально через коэффициенты a и b, что мы и хотели показать.

Обратимся к доказательству справедливости теоремы при каком угодно числе n корней

$$\alpha_1, \quad \alpha_2, \ \ldots, \ \alpha_n$$

уравнения

$$f(x) = x^n + p_1 x^{n-1} + \ldots + p_{n-1}x + p_n = 0$$

Будем, конечно, предполагать при этом, что все корни различные между собою независимые переменные. Метода будет состоять в том, что предполагая известным способ вычисления для $n-1$ переменной, покажем как произвести вычисление для n переменных.

Возьмем симметрическую фуикцию

$$G(\alpha_1, \alpha_2, \ldots, \alpha_n).$$

Разлагая ее по степеням одного из корней, например, α_1, получаем

$$G = G_0\alpha_1^{\mu} + G_1\alpha_1^{\mu-1} + \ldots + G_{\mu-1}\alpha_1 + G_{\mu}, \tag{4}$$

где

$$G_0, \quad G_1, \ \ldots, \ G_{\mu-1}, \quad G_{\mu}$$

суть, очевидно, целые симметрические функции от остальных $n-1$ корней α_2, $\alpha_3, \ldots, \alpha_n$, т. е., другими словами, от корней уравнения

$$x^{n-1} + p_1'x^{n-2} + p_2'x^{n-3} + \ldots + p_{n-2}'x + p_{n-1}' = 0,$$

первая часть которого происходит от деления $f(x)$ на $x - \alpha_1$. На основании формул § 4 коэффициенты $p_1', p_2', \ldots, p_{n-1}'$ выражаются целыми рациональными функциями от α_1 и коэффициентов $p_1, p_2, \ldots, p_n$, заданного уравнения, а именно,

$$\begin{aligned}
&p_1' = \alpha + p_1,\\
&p_2' = \alpha_1^2 + p_1\alpha_1 + p_2,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\
&p + n - 1' = \alpha_1^{n-1} + p_1\alpha_1^{n-2} + \ldots + p_{n-2}\alpha_1 = p_{n-1}.
\end{aligned}$$

Итак, по предположение справедливости теоремы для $n-1$ переменных, коэффициенты $G_0, G_1, \ldots, G_n$ выражаются рационально через $p'_1, p'_2, \ldots, p'_{n-1}$, а, следовательно, и рационально через α_1, $p_1, p_2, \ldots, p_{n-1}$.

Вычислив эти выражения, подставив в (4) и собрав окончательно коэффициенты при одинаковых степенях α_1, получим

$$G = A_0\alpha_1^m + A_1\alpha_1^{m-1} + \ldots + A_{m-1}\alpha_1 + A_m,$$

где, вообще говоря, m не меньше n, а коэффициенты

$$A_0, \quad A_1, \ \ldots, \ A_m$$

суть целые рациональные функции от $p_1, p_2, \ldots, p_{n-1}$.

Рассмотрим аналогично функцию

$$\psi(x) = A_0x^m + A_1x^{m-1} + \ldots + A_{m-1}x + A_m;$$

деля ее на

$$f(x) = x^n + p_1x^{n-1} + \ldots + p_{n-1}x + p_n,$$

получим некоторое частное $Q(x)$ и остаток не выше $n-1$ степени

$$C_0x^{n-1} + C_1x^{n-2} + \ldots + C_{n-2}x + C_{n-1},$$

где $C_0, C_1, C_2, \ldots, C_{n-1}$ суть целые функции коэффициентов $p_1, p_2, \ldots, p_n$.

Получаем тождество

$$C_0x^{n-1} + C_1x^{n-2} + \ldots + C_{n-2}x + C_{n-1} - \psi(x) - Q(x)\cdot f(x) = 0. \tag{5}$$

Подставляя в тождество (5) вместо x корень α_1, получим

$$C_0\alpha_1^{n-1} + C_1\alpha_1^{n-2} + \ldots + C_{n-2}\alpha_1 + C_{n-1} - G = 0, \tag{6}$$

ибо

$$f(\alpha_1) = 0, \qquad \psi(\alpha_1) = G.$$

Заменяя в тождестве (6) α_1 последовательно через $\alpha_2, \alpha_3, \ldots, \alpha_n$, получим на оснований симметричности функций G ряд новых тождеств

$$\begin{aligned}
&C_0\alpha_2^{n-1} + C_1\alpha_2^{n-2} + \ldots + C_{n-2}\alpha_2 + C_{n-1} - G = 0,\\
&C_0\alpha_3^{n-1} + C_1\alpha_3^{n-2} + \ldots + C_{n-2}\alpha_3 + C_{n-1} - G = 0,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\
&C_0\alpha_n^{n-1} + C_1\alpha_n^{n-2} + \ldots + C_{n-2}\alpha_n + C_{n-1} - G = 0.
\end{aligned} \tag{7}$$

Тождества (6) и (7) можно рассматривать, как систему линейных однородных уравнений с неизвестными

$$C_0, \quad C_1, \ \ldots, \ C_{n-2}, \quad C_{n-1} - G$$

и с определителем

$$\begin{vmatrix}
\alpha_1^{n-1} & \alpha_1^{n-2} & \ldots & \alpha_1 & 1\\
\alpha_2^{n-1} & \alpha_2^{n-2} & \ldots & \alpha_2 & 1\\
\ldots\ldots & \ldots\ldots & \ldots & \ldots\ldots & \ldots\\
\alpha_n^{n-1} & \alpha_n^{n-2} & \ldots & \alpha_n & 1
\end{vmatrix}$$

На оснований § 45 главы IV имеем

$$\begin{aligned} D = {} & (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)\cdots(\alpha_1 - \alpha_{n-1})(\alpha_1 - \alpha_n) \\ & (\alpha_2 - \alpha_3)\cdots(\alpha_2 - \alpha_{n-1})(\alpha_2 - \alpha_n) \\ & \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ & (\alpha_{n-2} - \alpha_{n-1})(\alpha_{n-2} - \alpha_n) \\ & (\alpha_{n-1} - \alpha_n). \end{aligned} \tag{8}$$

Считал все корни $\alpha_1, \alpha_2, \ldots, \alpha_n$ произвольными различными между собою независимыми переменными, заключаем, что D не равно нулю, и, следовательно,

$$C_0 = 0, \quad C_1 = 0, \ \ldots, \ C_{n-2} = 0$$
$$C_{n-1} - G = 0,$$

откуда

$$G = C_{n-1},$$

т. е. получаем выражение симметрической функции через коэффициенты $p_1, p_2, \ldots, p_n$.

Тот же результат можно получить короче, замечая, что функция

$$C_0 x^{n-1} + C_1 x^{n-2} + \ldots + C_{n-2} x + C_{n-1} - G$$

обращается в нуль для n различных значений x, именно для $\alpha_1, \alpha_2, \ldots, \alpha_n$; следовательно, (см. стр. 17) все ее коэффициенты должны тождественно равняться нулю, и, значит,

$$C_{n-1} - G = 0.$$

Понятие о результанте

§ 10

Как первый пример симметрической функции рассмотрим функцию, носящую название результанта двух целых функций.

Пусть заданы две целые функции,

$$f(x) = x^n + p_1 x^{n-1} + p_2 x^{n-2} + \ldots + p_{n-1} x + p_n, \tag{1}$$

$$\varphi(x) = x^m + q_1 x^{m-1} + q_2 x^{m-2} + \ldots + q_{m-1} x + q_m, \tag{2}$$

Обозначим через $\alpha_1, \alpha_2, \ldots, \alpha_n$ корни функций $f(x)$, а через $\beta_1, \beta_2, \ldots, \beta_m$ корни функции $\varphi(x)$. Рассмотрим два следующих произведения

$$\varphi(\alpha_1) \cdot \varphi(\alpha_2) \cdot \varphi(\alpha_3) \cdots \varphi(\alpha_n), \tag{3}$$

$$f(\beta_1) \cdot f(\beta_2) \cdot f(\beta_3) \cdots f(\beta_m). \tag{4}$$

Нетрудно убедиться, что два произведения (3) и (4) могут отличаться друг от друга только знаком, абсолютные же величины у них одинаковы. В самом деле, заметив, что

$$f(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)\cdots(x - \alpha_n),$$

$$\varphi(x) = (x-\beta_1)(x-\beta_2)(x-\beta_3)\cdots(x-\beta_m),$$

мы можем написать произведение (3) в таком виде

$$\prod(\alpha_i - \beta_j), \tag{5}$$

где произведение $\prod$ распространяется на все значения i из ряда $1, 2, 3, \ldots, n$ и на все значения j из ряда $1, 2, 3, \ldots, m$. Совершенно подобным же образом получим для выражения (4)

$$\prod(\beta_j - \alpha_i). \tag{6}$$

Выражение (6) получается из выражения (5) переменою знака каждого множителя, входящего в произведение. Так как число всех множителей равно mn, произведение степеней заданных функций, то, значит, можем написать следующее равенство

$$\varphi(\alpha_1)\cdot\varphi(\alpha_2)\cdot\varphi(\alpha_3)\cdots\varphi(\alpha_n) = (-1)^{mn} f(\beta_1)\cdot f(\beta_2)\cdot f(\beta_3)\cdots f(\beta_m).$$

Если мы не будем обращать внимания на знак выражений (3) и (4), то можем сказать, что эти два выражения представляют одну и ту же величину. Эта величина будет симметрической функцией, как от корней α функций $f(x)$, так и от корней β функции $\varphi(x)$. В этом убеждают нас выражения (3) и (4).

Эта симметрическая функция называется *результантом* двух заданных целых функций $f(x)$ и $\varphi(x)$ и выражается, как мы видим рационально через коэффициенты обеих функций.

Возьмем для примера случай двух квадратных функций

$$f(x) = x^2 + p_1 x + p_2,$$
$$\varphi(x) = x^2 + q_1 x + q_2.$$

Пусть α_1 и α_2 будут корни уравнения $f(x)$, тогда результант,

$$R = (\alpha_1^2 + q_1\alpha_1 + q_2)(\alpha_2^2 + q_1\alpha_2 + q_2) =$$

$$= \alpha_1^2\alpha_2^2 + q_1(\alpha_1^2\alpha_2 + \alpha_2^2\alpha_1) + q_1^2(\alpha_1\alpha_2) + q_2(\alpha_1^2 + \alpha_2^2) + q_1q_2(\alpha_1 + \alpha_2) + q_2^2;$$

но

$$\alpha_1\alpha_2 = p_2, \qquad \alpha_1 + \alpha_2 = -p_1,$$

следовательно, получим

$$R = p_2^2 - p_2p_1q_1 + q_1^2p_2 + q_2(p_1^2 - 2p_2) - p_1q_1q_2 + q_2^2 =$$

$$= (q_2 - p_2)^2 - (q_1 - p_1)(p_1q_2 - p_2q_1).$$

§ 11

Теорема. *Необходимое и достаточное условие для того, чтобы две функции $f(x)$ и $\varphi(x)$ имели общий корень, состоит в том, чтобы равнялся нулю их результант.*

В самом деле, необходимость теоремы следует из того соображения, что, если функция $\varphi(x)$ имеет некоторый корень α_i, принадлежащий функции $f(x)$, то будет тождественно $\varphi(\alpha_i) = 0$, и следовательно, обратится в нуль произведение

$$\varphi(\alpha_1) \cdot \varphi(\alpha_2) \cdots \varphi(\alpha_i) \cdots \varphi(\alpha_n), \tag{1}$$

представляющее собою результант функций $f(x)$ и $\varphi(x)$.

Достаточность же теоремы следует из того, что, если результант равен нулю, т. е., другими словами, равно нулю произведение (1), то должен равняться нулю но крайней мере один из множителей этого произведения; значит, равным нулю оказывается, например, множитель $\varphi(\alpha_i)$, т. е. α_i оказывается общим корнем двух функций $f(x)$ и $\varphi(x)$.

Исключение переменных

§ 12

Предположим, что коэффициенты заданных уравнений

$$x^n + p_1 x^{n-1} + p_2 x^{n-2} + \ldots + p_{n-1} x + p_n = 0, \tag{1}$$

$$x^m + q_1 x^{m-1} + q_2 x^{m-2} + \ldots + q_{m-1} x + q_m \tag{2}$$

суть целые функции от ряда новых независимых переменных $y, z, \ldots$.

Вычислив результант R первых частей заданных уравнений, мы замечаем, что этот результант оказывается целою функциею от новых независимых переменных $y, z, \ldots$.

Если мы напишем равенство

$$R = 0, \tag{3}$$

то это равенство будет алгебраическим уравнением относительно новых переменных $y, z, \ldots$ и будет давать такие значения этим переменным, при которых уравнения (1) и (2) совместимы, т. е., другими словами, имеют один или несколько общих корней относительно x.

По аналогии с тем как в Элементарной Алгебре производится исключение буквы x из двух уравнений способом сравнения неизвестных, говорят, что уравнение (3) представляет из себя результат исключения буквы x из двух заданных уравнений.

Задача исключения x из двух уравнений равносильна задаче вывода условия, при котором два уравнения (1) и (2) имеют общий корень. В этом случае два полинома

$$f(x) \qquad \text{и} \qquad \varphi(x)$$

имеют общий делитель $x - \alpha$, где α общий корень этих полиномов.

Будем производить для отыскания общего делителя последовательные деления как это сказано в § 19 главы VIII пока не дойдем до линейного делителя $Ax + B$. Разделяя предыдущий остаток на $Ax + B$, получим остаток R, независимый от x. Этот остаток будет рациональной функцией от переменных $y, z, \ldots$.

Отсюда мы видим, что необходимым условием существования общего корня двух функций будет равенство

$$R = 0. \tag{4}$$

Если равенство (4) удовлетворяется, то общий корень двух полиномов $f(x)$ и $\varphi(x)$ получается из уравнения

$$Ax + B = 0.$$

Так как A и B выражаются рационально через переменные $y, z, \ldots$, то можно сказать, что общий корень α есть рациональная функция от переменных $y, z, \ldots$.

Теорема Bézout

§ 13

Докажем теорему Bézout, состоящую в том, что *степень результанта двух целых функций общего вида*

$$f(x) = x^n + p_1 x^{n-1} + p_2 x^{n-2} + \ldots + p_{n-1}x + p_n, \tag{1}$$

$$\varphi(x) = x^m + q_1 x^{m-1} + q_2 x^{m-2} + \ldots + q_{m-1}x + q_m, \tag{2}$$

степени n и m равна произведению этих степеней $m \cdot n$.

Предположим, что коэффициенты p и q заданных функций таким образом выражены через новые переменные $y, z, \ldots$, что первые части уравнений (1) и (2) суть целые функций самого общего вида степеней n и m. Значит, в каждой из этих функций должны находиться члены, буквенный выражения которых $x^\lambda y^\mu z^\nu \cdots$ могут принимать всевозможные комбинации неотрицательных показателей, сумма которых не превосходить степени функций. Тогда, очевидно, что коэффициенты p_i и q_k должны быть целыми функциями общего вида, степеней равных значкам i и k.

Рассмотрим теперь некоторый член результанта R. Так как этот результант есть целая функция от коэффициентов обеих функций, то, значит, каждый его член должен иметь вид

$$A p_0^{\lambda_0} p_1^{\lambda_1} p_2^{\lambda_2} \cdots p_n^{\lambda_n} \cdot q_0^{\mu_0} q_1^{\mu_1} q_2^{\mu_2} \cdots q_m^{\mu_m}, \tag{3}$$

где λ_i и μ_k суть целые неопределенный числа, а коэффициент A есть некоторый численный коэффициент.

Так как степень p_i относительно корней $\alpha_1, \alpha_2, \ldots$ есть i, а степень q_j относительно корней $\beta_1, \beta_2, \ldots$ есть j, то член (3) будет функция от корней α и β степени

$$1 \cdot \lambda_1 + 2 \cdot \lambda_2 + \ldots + n\lambda_n + 1 \cdot \mu_1 + 2 \cdot \mu_2 + \ldots m\mu_m,$$

но, с другой стороны, результант

$$R = \prod(\alpha_i - \beta_j)$$

есть однородная функция степени $m \cdot n$ от корней α и β, следовательно,

$$1 \cdot \lambda_1 + 2 \cdot \lambda_2 + \ldots + n\lambda_n + 1 \cdot \mu_1 + 2 \cdot \mu_2 + \ldots m\mu_m = m \cdot n. \tag{4}$$

Но, с другой стороны, степень члена (3) относительно переменных $y, z, \ldots$ есть

$$1 \cdot \lambda_1 + 2 \cdot \lambda_2 + \ldots + n\lambda_n + 1 \cdot \mu_1 + 2 \cdot \mu_2 + \ldots m\mu_m,$$

следовательно, ввиду (4), степень результанта R относительно переменных $y, z, \ldots$ будет $m \cdot n$, что и требовалось доказать.

Это рассуждение показывает, собственно говоря, что степень результанта не выше $m \cdot n$; но может быть эта степень будет ниже $m \cdot n$. Действительно, такое понижение степени результанта возможно, когда коэффициенты при неизвестных $y, z, \ldots$ в функциях p_i, q_k имеют определенные численные значения, причем некоторые могут равняться нулю.

Надо показать однако, что в общем случае буквенных коэффициентов такого понижения не существует. Проще всего показать по крайней мере один численный пример, в котором результант имеет как раз степень $m \cdot n$.

Для этой цели возьмем два уравнения:

$$f(x) = x - y^n = 0, \qquad \varphi(x) = x^m - y - 1 = 0;$$

исключая x, получим

$$R = y^{nm} - y - 1 = 0.$$

§ 14

Поясним геометрически нашу теорию. Рассмотрим исключение координаты y из двух уравнений

$$f(x, y) = 0, \qquad \varphi(x, y) = 0$$

алгебраических кривых. Пусть f будет целою функциею степени n общего вида от x, y с буквенными коэффициентами, а φ — также общего вида степени m.

Мы замечаем, что, приравнивая результант $R(x)$ нулю, получим уравнение

$$R(x) = 0 \tag{1}$$

степени mn, дающее абсциссы точек пересечения кривой $f = 0$ с кривою $\varphi = 0$. Итак, в общем случае уравнение (1) будет иметь mn простых корней и, следовательно, линии будут пересекаться в mn точках. На основании сказанного в конце § 12 ордината точки пересечения будет определяться из уравнения первой степени $Ay + B = 0$, где A и B рациональные функций от корня уравнения (1).

При счете точек надо принимать, конечно, во внимание также и мнимые точки, т. е. точки с мнимыми координатами.

Когда мы переходим от буквенных коэффициентов к численным, то возможны самые разнообразные особенности.

Прежде всего может случиться, что несколько точек пересечения будут иметь одну и туже абсциссу; это будет, конечно, в том случае когда уравнение (1) имеет кратные корни. Рассмотрим случай двукратного корня x_0 уравнения (1), тогда,

если этому корню соответствуют две различный ординаты y, то уравнение $Ay+B$ не должно давать определенного значения для y и мы получим $A=0$, $B=0$. Надо рассмотреть предыдущий остаток второй степени $A_1y^2+B_1y+C_1$, корни которого и будут давать абсциссы двух точек встречи рассматриваемых кривых.

Может далее случиться, что две или несколько точек встречи совпадают, тогда получается касание линий.

Все эти особенности не нарушают степени nm уравнения (1). Дело идет только о кратных корнях этого уравнения и о вычислении y, соответствующего каждому корню x_0 уравнения (1).

Мы должны оставить в стороне случай, когда корню x_0 соответствует бесчисленное множество значений y; это будет в том случае, когда прямая $x-x_0$ входить в состав обеих линий $f=0$ и $\varphi=0$, т. е. когда обе функции f и φ делятся на двучлен $x-x_0$.

Конечно надо предполагать, что функции f и φ взаимно просты, ибо существование общего делителя ψ приводилось бы к тому, что обе алгебраические линии имеют общую часть $\psi=0$.

Понижение степени уравнения (1) на основании соображений § 6 главы II может происходить только в том случае, когда существуют у этого уравнения *бесконечно большие корни*. Геометрически говоря, это будет тот случай, когда обе алгебраическая кривые имеют общими бесконечно далекие точки. Можно привести очень много простых примеров этого обстоятельства. Например, две гиперболы с параллельными асимптотами пересекаются в общих точках с бесконечно далекой прямою, следовательно, они могут иметь только две общие точки на конечном расстоянии. Значит, в случай двух таких гипербол после исключения одной координаты получается уравнение не 4-ой степени ($n=2$, $m=2$), а всего только 2-ой. В самом деле, уравнения 2-х гипербол с параллельными асимптотами имеет вид

$$Ax^2+Bxy+Cy^2+Dx+Ey+F=0,$$
$$Ax^2+Bxy+Cy^2+D_1x+E_1y+F_1=0.$$

Вычитая второе уравнение из первого, получим

$$(D-D_1)x+(E-E_1)y+F-F_1=0;$$

для исключения решаем последнее относительно y

$$y=\frac{D_1-D}{E-E_1}x+\frac{F_1-F}{E-E_1}$$

и, подставляя последнее выражение в уравнение одной из гипербол, получаем квадратное уравнение относительно x как результат исключения y.

Как частный случай является задача нахождения точек пересечения двух кругов

$$\begin{aligned} x^2+y^2+Dx+Ey+F&=0,\\ x^2+y^2+D_1x+E_1y+F_1&=0. \end{aligned} \tag{2}$$

Круги, как известно, имеют две точки встречи (вещественные или мнимые) на конечном расстоянии.

Чтобы проследить механизм того, каким образом мы теряем из виду остальные две бесконечно далекие точки, введем однородные координаты.

Уравнения (2) перепишутся так

$$x^2 + y^2 + z(Dx + Ey + Fz) = 0,$$
$$x^2 + y^2 + z(D_1x + E_1y + F_1z) = 0.$$

Вычитал, мы получаем

$$z[(D - D_1)x + (E - E_1)y + (F - F_1)z] = 0.$$

В предыдущем анализе мы пропускали рассмотрение случая $z = 0$, дающего бесконечно далекую прямую.

Все круги пересекаются с бесконечно далекой прямой в мнимых точках, определяемых двумя уравнениями

$$x^2 + y^2 = 0, \qquad z = 0.$$

Эти точки, каждая в отдельности, определяются уравнениями

$$(x + y\sqrt{-1} = 0, \quad z = 0), \qquad (x - y\sqrt{-1} = 0, \quad z = 0).$$

Это суть известные, так называемые, циклические точки, играющие большую роль в вопрос отличия проективных и метрических свойств геометрических фигур.

Вопрос об указании точной степени результанта в том случае, когда эта степень меньше mn был решен профессором Дерптского Университета Миндингом.[38]

§ 15

Теорема Bézout о степени результанта двух уравнений может быть обобщена на случай какого угодно числа уравнений.

Рассмотрим случай трех уравнений; однако наши соображения будут относиться к произвольному числу уравнений.

Итак, пусть будут заданы три уравнения

$$f(x, y, z) = 0,$$
$$\varphi(x, y, z) = 0,$$
$$\psi(x, y, z) = 0$$

степеней m, n, p.

Исключая букву x из уравнений $f(x, y, z) = 0$ и $\varphi(x, y, z) = 0$, получим

$$F(y, z) = 0; \tag{1}$$

исключая подобным же образом букву x из уравнений $\varphi(x, y, z) = 0$, $\psi(x, y, z) = 0$, получим

$$\Phi(y, z) = 0. \tag{2}$$

[38]Minding. Journal de Math, pures et appliqués. Ser. I. T. VI.

Уравнение (1) будет степени mn, а уравнение (2) степени np. Совместное существование уравнений (1) и (2) выражает условие существования общего корня относительно x у трех заданных уравнений.

Исключая y из двух уравнений (1) и (2), получим уравнение

$$\Omega(z) = 0, \tag{3}$$

которое будет степени $mn \cdot np = mn^2p$, и будет удовлетворяться всеми значениями z, при которых три уравнения

$$f = 0, \qquad \varphi = 0, \qquad \psi = 0 \tag{4}$$

имеют общую систему решений относительно x и y.

Если мы назовем результантом исключения x и y из трех уравнений такую функцию

$$\Pi(z),$$

которая обращается в нуль только при тех значениях z, при которых уравнения (4) имеют общие решения относительно x и y, то оказывается, что функция $\Omega(z)$ не есть результант $\Pi(z)$, а заключает этот результант, как множитель, т. е.

$$\Omega(z) = \Pi(z) \cdot \omega(z).$$

Самый способ получения функции $\Omega(z)$ показывает, что эта функция не есть результант исключонния x и y. В самом деле, исключая x сначала из уравнений

$$f(x, y, z) = 0, \qquad \varphi(x, y, z) = 0,$$

а потом из уравнений

$$\varphi(x, y, z) = 0, \qquad \psi(x, y, z) = 0,$$

получим два уравнения степеней mp и np, откуда через исключение y получим новое уравнение

$$\Omega_1(z) = 0, \tag{5}$$

где $\Omega_1(z)$ есть функция степени mnp^2. Наконец, исключая x сначала из системы

$$f(x, y, z) = 0, \qquad \psi(x, y, z) = 0,$$

а потом из системы

$$f(x, y, z) = 0, \qquad \varphi(x, y, z) = 0,$$

получим два уравнения степеней mp и mn, откуда через исключение y получим уравнение

$$\Omega_2(z) = 0$$

степени m^2np.

Очевидно, что функция наибольшей степени из функций

$$\Omega(z), \quad \Omega_1(z), \quad \Omega_2(z)$$

заключает наверно лишние множители.

Оказывается, что *искомый результант* $\Pi(z)$ *есть общий множитель трех функций*

$$\Omega(z), \quad \Omega_1(z), \quad \Omega_2(z)$$

и его степень есть произведение mnp степеней заданных уравнений.

Докажем, что степень результанта есть mnp, показав, что таково число общих решений наших трех уравнении относительно трех неизвестных x, y, z.

Во избежание упоминаний об исключительных случаях сделаем наши уравнения однородными, вводя четвертую переменную u, именно полагая

$$\frac{x}{u}, \quad \frac{y}{u}, \quad \frac{z}{u}$$

вместо

$$x, \quad y, \quad z.$$

Итак, надо решить относительно x, y, z уравнения

$$\begin{aligned} f(x, y, z, u) &= 0, \\ \varphi(x, y, z, u) &= 0, \\ \psi(x, y, z, u) &= 0. \end{aligned} \tag{6}$$

Рассмотрим сначала случай, когда каждая из трех функций f, φ, ψ есть произведение линейных множителей. Мы получим все возможные решения этих трех уравнений, приравнивая нулю по одному линейному множителю из каждого уравнения.

Число таких комбинаций трех уравнений первой степени будет равно

$$mnp,$$

если мы предполагаем все линейные множители независимыми между собою.

Итак, в этом случае число решений нашей системы будет mnp, и все решения будут различны между собою.

Предполагая теперь в самом общем случае коэффициенты уравнений (6) независимыми между собою переменными, мы замечаем, что результант, происходящий от исключения x и y, не может тождественно равняться нулю, ибо в подобном случае система имела бы всегда бесчисленное множество решений относительно x, y, z, что противоречит только что разобранному случаю разложения на линейные множители, и, следовательно, результант есть некоторая однородная функция двух переменных, степень которой не может меняться при каких-либо частных предположениях относительно коэффициентов (ибо все члены одного и того же измерения).

Так как степень такого результанта равна mnp при предположении разложимости функций на линейные множители, то, следовательно, такая же степень должна быть и в общем случае; это и требовалось доказать.

То, что мы сказали относительно трех уравнений, прилагается и к общему случаю n уравнений. Исключая из таких уравнений те $n-1$ переменных, мы получаем уравнение, степень которого равна произведению степеней этих уравнений.

Приемы исключения при помощи определителей

§ 16

Укажем простейшие способы вычисления результантов в форме определителей; при этом будем помнить, что результантом двух функций от x называется выражение, независящее от x, целое и рациональное относительно коэффициентов обеих функций, обращение которого в нуль представляет условие необходимое и достаточное для того, чтобы, функций имели общий корень.

§ 17

Способ Euler'a. Пусть даны два уравнения

$$f(x) = 0, \qquad \varphi(x) = 0 \tag{1}$$

степеней n и m. Если оба эти уравнения имеют общего линейного множителя, то мы должны получить тождественные результаты, умножим ли мы первое уравнение на $m-1$ остальных линейных множителей второго, или же второе уравнение на $n-1$ оставшихся линейных множителей первого. Следовательно, если мы первое уравнение из (1) умножим на функций $\varphi_1(x)$ степени $m-1$, заключающую m произвольных постоянных, а второе уравнение из (1) умножим на функций $f_1(x)$ степени $n-1$, заключающую n произвольных постоянных, и в полученных уравнениях

$$f(x)\varphi_1(x) = 0,$$
$$\varphi(x)f_1(x) = 0$$

сравним коэффициенты, то для получения результанта функций $f(x)$ и $\varphi(x)$ достаточно будет написать условия, при котором из полученных от сравнения $m+n$ коэффициентов уравнений можно определить вполне $m+n$ введенных постоянных.

Итак, пусть

$$\begin{aligned} f(x) &= a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n, \\ f_1(x) &= \alpha_0x^{n-1} + \alpha_1x^{n-2} + \ldots + \alpha_{n-1} \\ \varphi(x) &= b_0x^m + b_1x^{m-1} + \ldots + b_{m-1}x + b_m \\ \varphi_1(x) &= \beta_0x^{m-1} + \beta_1x^{m-2} + \ldots + \beta_{m-1}, \end{aligned}$$

тогда сравнивая коэффициенты в обоих частях тождества

$$f(x)\varphi_1(x) = \varphi(x)f_1(x)$$

получим следуюшие уравнения

$$\begin{array}{lll} a_0\beta_0 & -b_0\alpha_0 & = 0, \\ a_1\beta_0 + a_0\beta_1 & -b_1\alpha_0 - b_0\alpha_1 & = 0, \\ a_2\beta_0 + a_1\beta_1 + a_0\beta_2 & -b_2\alpha_0 - b_1\alpha_1 - b_0\alpha_2 & = 0, \\ \multicolumn{3}{l}{\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,} \end{array}$$

из которых, как из системы $m+n$ однородных уравнений относительно $m+n$ переменных

$$\alpha_0,\ \ \alpha_1,\ \ldots,\ \alpha_{n-1},\ \ \beta_0,\ \ \beta_1,\ \ldots,\ \beta_{m-1},$$

находим искомый результант в форме определителя $m+n$ порядка

$$R=\begin{vmatrix} a_0 & a_1 & a_2 & \ldots & a_n & 0 & 0 & \ldots & 0 \\ 0 & a_0 & a_1 & \ldots & a_{n-1} & a_n & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & \ldots & \ldots & \ldots & a_{n-1} & a_n \\ b_0 & b_1 & b_2 & \ldots & b_m & 0 & 0 & \ldots & 0 \\ 0 & b_0 & b_1 & \ldots & b_{m-1} & b_m & 0 & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & \ldots & \ldots & \ldots & b_{m-1} & b_m \end{vmatrix},$$

если после исключения вертикали полученного определителя заменим горизонталями, а горизонтали вертикалями.

Пример: найти результант уравнений

$$x^2+3x-4=0,$$
$$2x^3-x^2+4x-1=0.$$

По выведенному правилу находим

$$R=\begin{vmatrix} 1 & 3 & -4 & 0 & 0 \\ 0 & 1 & 3 & -4 & 0 \\ 0 & 0 & 1 & 3 & -4 \\ 2 & -1 & 4 & -1 & 0 \\ 0 & 2 & -1 & 4 & -1 \end{vmatrix}=644.$$

§ 18

Способ Sylvester'a. Способ Sylvester'a дает результант в форме тождественной с формою Euler'a, только приводит к нему посредством других более простых соображений.

Будем рассматривать те же уравнения

$$f(x)=0,\qquad \varphi(x)=0$$

степеней n и m.

Будем умножать уравнение $f(x)=0$ последовательно на

$$x^{m-1},\ \ x^{m-2},\ \ldots,\ x,\ \ 1,$$

а уравнение $\varphi(x)=0$ на

$$x^{n-1},\ \ x^{n-2},\ \ldots,\ x,\ \ 1,$$

тогда получим $n+m$ и уравнений, в которых величины

$$x^{m+n-1},\ \ x^{m+n-2},\ \ldots,\ x^2,\ \ x,\ \ 1$$

могут быть рассматриваемы, как независимые переменные. Исключая эти величины, получим результант в той же форме, что и в предыдущем параграфе.

Пример: найти результант уравнений

$$ax^2 + bx + c = 0,$$
$$a'x^3 + b'x^2 + c'x + d' = 0;$$

умножая первое уравнение на x^2, x, 1, а второе на x, 1, получим систему пяти уравнений

$$\begin{array}{rrrrrl} ax^4 & +bx^3 & +cx^2 & & & = 0, \\ & ax^3 & +bx^2 & +cx & & = 0, \\ & & ax^2 & +bx & +c & = 0, \\ a'x^4 & +b'x^3 & +c'x^2 & +d'x & & = 0, \\ & a'x^3 & +b'x^2 & +c'x & +d' & = 0, \end{array}$$

из которой, исключая x^4, x^3, x^2, x, 1, получим результант

$$R = \begin{vmatrix} a & b & c & 0 & 0 \\ 0 & a & b & c & 0 \\ 0 & 0 & a & b & c \\ a' & b' & c' & d' & 0 \\ 0 & a' & b' & c' & d' \end{vmatrix}.$$

§ 19

Способ Bézout. Этот способ дает результант в форме определителя более удобной для вычисления чем способы Euler'a и Sylvester'a.

Общая идея этого способа уяснится легче всего из рассмотрения частного случая, например, двух уравнений 4-ой степени

$$\begin{aligned} ax^4 + bx^3 + cx^2 + dx + e = 0, \\ a'x^4 + b'x^3 + c'x^2 + d'x + e' = 0. \end{aligned} \tag{1}$$

Умножая первое из этих уравнений на a', второе на a и вычитая второе из первого, получим уравнение

$$(ab')x^3 + (ac')x^2 + (ad')x + (ae') = 0, \tag{2}$$

где, для краткости, положено

$$(ab') = ab' - a'b, \quad (ac') = ac' - a'c, \ \ldots;$$

умножая снова первое из уравнений (1) на $a'x + b'$, второе на $ax + b$ и вычитая, получим

$$(ac')x^3 + \{(ad')(bc')\}x^2 + \{(ae') + (bd')\}x + (be') = 0; \tag{3}$$

умножая теперь первое из уравнений (1) на $a'x^2 + b'x + c'$, второе на $ax^2 + bx + c$ и вычитая, получим

$$(ad')x^3 + \{(ae') + (bd')\}x^2 + \{(be') + (cd')\}x + (ce') = 0; \tag{4}$$

наконец, умножая первое из уравнений (1) на $a'x^3 + b'x^2 + c'x + d'$, второе на $ax^3 + bx^2 + cx + d$ и вычитая, получим

$$(ae')x^3 + (be')x^2 + (ce')x + (de') = 0. \tag{5}$$

Из составленных таким образом четырех уравнений (2), (3), (4) и (5) можем исключить буквы x^3, x^2, x, 1 и получим определитель

$$\begin{vmatrix} (ab') & (ac') & (ad') & (ae') \\ (ac') & (ad') + (bc') & (ae') + (bd') & (be') \\ (ad') & (ae') + (bd') & (be') + cd') & (ce') \\ (ae') & (be') & (ce') & (de') \end{vmatrix}.$$

Применение этого способа к общему случаю двух уравнений n-ой степени настолько очевидно, что нет надобности приводить общего доказательства. Из рассмотрения найденного определителя легко заметить общий закон составления результанта в случае двух уравнений n-ой степени.

Вычисление дискриминанта

§ 20

Как весьма важный пример вычисления симметрических функций, рассмотрим симметрическую функцию, носящую название *дискриминанта*. Рассмотрим функцию P^2, где

$$\begin{aligned} P = (x_1 - x_2)(x_1 - x_3)(x_1 - x_4)\cdots(x_1 - x_n)\cdot \\ (x_2 - x_3)(x_2 - x_4)\cdots(x_2 - x_n)\cdot \\ (x_3 - x_4)\cdots(x_3 - x_4)\cdot \\ \cdots\cdots\cdots\cdots\cdot \\ (x_{n-1} - x_n), \end{aligned}$$

в числе $x_1, x_2, \ldots, x_n$ есть корни уравнения $f(x) = 0$.

Функция P^2, очевидно, остается неизменной при всякой подстановке корней. Эта функция называется *дискриминантом уравнения* $f(x) = 0$.

Для вычисления дискриминанта заметим прежде всего, что функцию P можно представить (см. стр. 101) в виде следующего определителя

$$P = \begin{vmatrix} x_1^{n-1} & x_1^{n-2} & \ldots & x_1 & 1 \\ x_2^{n-1} & x_2^{n-2} & \ldots & x_2 & 1 \\ \cdots\cdots & \cdots\cdots & \cdots & \cdots & \cdots \\ x_n^{n-1} & x_n^{n-2} & \ldots & x_n & 1 \end{vmatrix}$$

или, изменяя порядок следования колонн на обратный, получаем

$$P = (-1)^{\frac{n(n-1)}{2}} \begin{vmatrix} 1 & x_1 & \ldots & x_1^{n-2} & x_1^{n-1} \\ 1 & x_2 & \ldots & x_2^{n-2} & x_2^{n-1} \\ \cdots\cdots & \cdots\cdots & \cdots & \cdots & \cdots \\ 1 & x_n & \ldots & x_n^{n-2} & x_n^{n-1} \end{vmatrix}$$

Возвысим последний определитель в квадрат, производя умножение элементов по колоннам; получим

$$P^2 = \begin{vmatrix} s_0 & s_1 & s_2 & \dots & s_{n-1} \\ s_1 & s_2 & s_3 & \dots & s_n \\ s_2 & s_3 & s_4 & \dots & s_{n+1} \\ \dots & \dots & \dots & \dots & \dots \\ s_{n-1} & s_n & s_{n+1} & \dots & s_{2n-2} \end{vmatrix}.$$

Итак, мы получаем выражение дискриминанта через функции s. Формулы Newton'a (см. § 4) дают возможность выразить дискриминант через коэффициенты уравнения.

Прилагая полученное нами выражение для дискриминанта к квадратному уравнений

$$x^2 + p_1 x + p_2 = 0,$$

получим

$$P^2 = \begin{vmatrix} s_0 & s_1 \\ s_1 & s_2 \end{vmatrix},$$

откуда

$$P^2 = s_0 s_2 - s_1^2 = 2(p_1^2 - 2p_2) - p_1^2 = p_1^2 - 4p_2,$$

т. е. то выражение, которое стоит под корнем квадратным в общей формуле решения квадратного уравнения.

Для кубического уравнения

$$x^3 + p_1 x^2 + p_2 x + p_3 = 0$$

по формулам стр. 238 получаем

$$s_0 = 3, \quad s_1 = -p_1, \quad s_2 = p_1^2 - 2p_2, \quad s_3 = -p_1^3 + 3p_2 p_2 - 3p_3,$$
$$s_4 = p_1^4 - 4p_1^2 p_2 + 4p_1 p_3 + 2p_2^2 - 4p_4,$$

откуда

$$P^2 = \begin{vmatrix} s_0 & s_1 & s_2 \\ s_1 & s_2 & s_3 \\ s_2 & s_3 & s_4 \end{vmatrix} =$$
$$= s_0 s_2 s_4 - s_0 s_3^2 - s_1^2 s_4 - s_2^3 + 2 s_1 s_2 s_3 =$$
$$= p_1^2 p_2^2 + 18 p_1 p_2 p_3 - 4p_2^3 - 4p_1^3 p_3 - 27 p_3^2.$$

В случае $p_1 = 0$, т. е. когда дано уравнение

$$x^4 + p_2 x + p_3 = 0,$$

получаем

$$P^2 = -4p_2^3 - 27p_3^2 = -2^2 \cdot 3^3 \left\{ \frac{p_3^2}{4} + \frac{p_2^3}{27} \right\},$$

т. е. та величина, которая стоить под квадратным корнем в формуле Cardano.

§ 21

Представляя левую часть данного уравнения $f(x) = 0$ в виде

$$f(x) = (x - x_1)(x - x_2) \cdots (x - x_n)$$

и взяв от обеих частей логарифмическую производную, получим

$$\frac{f'(x)}{f(x)} = \frac{1}{x - x_1} + \frac{1}{x - x_2} + \ldots + \frac{1}{x - x_n},$$

или

$$f'(x) = \frac{f(x)}{x - x_1} + \frac{f(x)}{x - x_2} + \ldots + \frac{f(x)}{x - x_n}.$$

Подставляя в это выражение для $f'(x)$ вместо x последовательно $x_1, x_2, \ldots, x_n$, получим

$$\begin{aligned} f'(x_1) &= (x_1 - x_2)(x_1 - x_3) \cdots (x_1 - x_n), \\ f'(x_2) &= (x_2 - x_1)(x_2 - x_3) \cdots (x_2 - x_n), \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ f'(x_n) &= (x_n - x_1)(x_1 - x_2) \cdots (x_1 - x_{n-1}). \end{aligned} \tag{1}$$

Пользуясь этими формулами можно дать другой вид дискриминант P^2. В самом деле, перемножая формулы (1) и замечая, что в полученном таким образом произведений каждый член $x_k - x_i$ вход два раза с разным знаком, получаем

$$\begin{aligned} (-1)^{\frac{n(n-1)}{2}}\ f'(x_1)f'(x_2)\cdots f'(x_n) = (x_1 - x_2)^2(x_1 - x_3)^2 \cdots (x_1 - x_n)^2 \cdot \\ \cdot (x_2 - x_3)^2 \cdots (x_2 - x_n)^2 \cdot \\ \ldots\ldots\ldots\ldots\ldots \\ \cdot (x_{n-1} - x_n)^2, \end{aligned}$$

или короче

$$P^2 = (-1)^{\frac{n(n-1)}{2}}\ f'(x_1)f'(x_2)\cdots f'(x_n). \tag{2}$$

Из этой формулы мы видим, что дискриминант P^2 уравнения $f(x) = 0$ надо рассматривать, как *результант производной функции $f'(x)$ и первоначальной функции $f(x)$, умноженный при этом на множители $(-1)^{\frac{n(n-1)}{2}}$, где n есть степень уравнения $f(x) = 0$.*

Из выражения (2) для дискриминанта ясно видно, что *обращение в нуль дискриминанта является условием необходимым и достаточным для существования кратных корней уравнений.*

§ 22

Говорят, что целая функция $f(x)$ обладает свойством неприводимости в области рациональных чисел, если она не разлагается на множителей с рациональными коэффициентами.

Так, например, функция

$$f(x) = x^4 + 1$$

не разлагается в области рациональных чисел на множителей, но эта функция будет разлагаться на множители, если к рациональным числам присоединим иррациональное число $\sqrt{2}$. В самом деле,

$$x^4 + 1 = x^4 + 2x^2 + 1 - 2x^2 = (x^2 + 1)^2 - 2x^2 =$$
$$= (x^2 + x\sqrt{2} + 1)(x^2 - x\sqrt{2} + 1).$$

Очевидно, что, если к области рациональных чисел мы присоединим все иррациональные, а также все мнимые числа, то в такой новой области всех чисел не существует неприводимых функций выше первой степени, потому что всякая функция степени n разлагается на n линейных множителей.

§ 23

Приведем несколько основных положений относительно неприводимых функций. Так как мы будем ограничиваться только областью рациональных чисел, то функцию будем называть просто неприводимою.

Пусть задана неприводимая функция $f(x)$. Рассмотрим другую целую функцию $F(x)$ с рациональными коэффициентами и будем искать общий наибольший делитель этих двух функции. Пусть этот общий наибольший делитель будет $\varphi(x)$.

Так как нахождение общего наибольшего делителя двух целых функций совершается посредством рациональных операций, то, если коэффициенты двух заданных функций были рациональные, то будут рациональными и коэффициенты функций $\varphi(x)$; отсюда мы видим, что функция $\varphi(x)$ должна быть или постоянным числом, или же равняться $f(x)$, так как по определению неприводимости функция $f(x)$ не может иметь никакого делителя $\varphi(x)$ с рациональными коэффициентами меньшей степени. Таким образом мы видим, что функция $F(x)$ или взаимно простая с $f(x)$, или делится на $f(x)$; отсюда получается теорема.

Теорема. *Если функция $F(x)$ с рациональными коэффициентами обращается в нуль при каком-либо корне неприводимого уравнения $f(x) = 0$, то она должна обращаться в нуль при всех корнях этого уравнения.*

Следствие I. *Если неприводимое уравнение $f(x) = 0$ имеет общий корень с уравнением $\varphi(x) = 0$ низшей степени, то все коэффициенты функции $\varphi(x)$ должны равняться нулю; и, следовательно, уравнение $\varphi(x) = 0$ должно обращаться в тождество.*

В самом деле, $\varphi(x)$ не может быть взаимно простым с $f(x)$ и не может делиться на $f(x)$, потому что степень $\varphi(x)$ меньше.

Следствие II. *Все корни неприводимого уравнения простые.*

В самом деле, обратное допущение приводит к противоречию, потому что, если допустить, что неприводимая функция $f(x)$ имеет кратный корень, то производная $f'(x)$ степени ниже, чем функция $f(x)$, имеет с нею по крайней мере один общий корень и не обращается тождественно в нуль.

Простейший вид рациональной функции от корня неприводимого уравнения

§ 24

Как новое приложение теории симметрических функций, рассмотрим приведение рациональной функций от корня неприводимого уравнения

$$f(x) = x^n + p_1 x^{n-1} + \ldots + p_{n-1}x + p_n \tag{1}$$

в простейшему виду.

Итак, рассмотрим рациональную функцию

$$\frac{\varphi(x)}{\psi(x)}, \tag{2}$$

где x есть корень уравнения (1).

Целые функций $\varphi(x)$ и $\psi(x)$ можно предполагать степеней не выше $n-1$, ибо все высшие степени можно исключить, пользуясь уравнением (1). В самом деле, если бы степень функции $\varphi(x)$ была выше $n-1$, то, деля $\varphi(x)$ на $f(x)$ и обозначая через $\omega(x)$ частное, а через $\varphi_1(x)$ остаток, получим

$$\varphi(x) = f(x)\omega(x) + \varphi_1(x);$$

но так как x есть корень функции $f(x)$, то получим

$$\varphi(x) = \varphi_1(x)$$

и, следовательно, при вычислений рациональной функции (2) от корня уравнения (1) можно заменить функцию $\varphi(x)$ степени выше $n-1$ функциею $\varphi_1(x)$ степени не выше $n-1$. Подобным образом, если функция $\psi(x)$ степени выше $n-1$, то ее можно заменить остатком $\psi_1(x)$ от деления $\psi(x)$ на $f(x)$.

Итак, будем предполагать, что степени функций $\varphi(x)$ и $\psi(x)$ не выше $n-1$. Кроме того будем предполагать, что функция (2) не обращается в ∞ ни при одном из корней уравнения (1). Обозначим корни заданного уравнения через

$$\alpha,\ \ \beta,\ \ \gamma,\ \ldots,\ \mu.$$

Умножим числитель и знаменатель дроби

$$\frac{\varphi(\alpha)}{\psi(\alpha)}$$

на выражение

$$\psi(\beta)\psi(\gamma)\cdots\psi(\mu),$$

тогда получим дробь

$$\frac{\varphi(\alpha)\psi(\beta)\psi(\gamma)\cdots\psi(\mu)}{\psi(\alpha)\psi(\beta)\psi(\gamma)\cdots\psi(\mu)},$$

знаменатель которой есть результант двух функций $\varphi(x)$ и $\psi(x)$.

Обозначим его через R. Произведение

$$\psi(\beta)\psi(\gamma)\cdots\psi(\mu) \tag{3}$$

есть симметрическая функция корней уравнения

$$\frac{f(x)}{x-\alpha} = 0,$$

или (см. стр. **??**)

$$x^{n-1} + \omega_1(\alpha)x^{n-2} + \omega_2(\alpha)x^{n-3} + \ldots + \omega_{n-1}(\alpha) = 0,$$

где

$$\begin{aligned}
&\omega_1(\alpha) = \alpha + p_1\\
&\omega_2(\alpha) + \alpha^1 + p_1\alpha + p_2,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\
&\omega_{n-1}(\alpha) = \alpha^{n-1} + p_1\alpha^{n-2} + \ldots + p_{n-1},
\end{aligned}$$

следовательно, это произведение (3) выражается в виде целой рациональной функции от коэффициентов

$$\omega_1(\alpha),\ \ \omega_2(\alpha),\ \ldots,\ \omega_{n-1}(\alpha),$$

т. е. в виде целой функции от α. Обозначим эту функцию через $\Omega(\alpha)$.

Итак, рациональная функция (2) от корня α уравнения (1) может быть представлена в виде

$$\frac{1}{R}\ \varphi(\alpha)\Omega(\alpha),$$

т. е. в виде целой функции

$$\Pi(\alpha),$$

которую можно предположить, согласно предыдущему, не выше $n-1$ степени. Выскажем теорему.

Теорема. *Самый общий вид рациональной функции от корня α неприводимого уравнения $f(x) = 0$ степени n, не обращающейся в бесконечность ни при одном из корней, есть*

$$C_0\alpha^{n-1} + C_1\alpha^{n-2} + \ldots + C_{n-2}\alpha + C_{n-1},$$

где C суть рациональные числа.

Поясним теорию примером. Пусть надо привести к простейшему виду рациональную функцию

$$\frac{3x^2+3x-1}{x^3-4x+2}$$

от корня уравнения

$$x^2 - x + 1 = 0. \tag{4}$$

Выполняем деления

$$\begin{array}{r|l} 3x^2 + 3x - 1 & x^2 - x + 1 \\ \hline 3x^2 - 3x + 3 & 3 \\ \hline 6x - 4 & \end{array}$$

$$\begin{array}{r|l} x^3 - 4x + 2 & x^2 - x + 1 \\ \hline x^3 - x^2 + x & x + 1 \\ \hline x^2 - 5x + 2 & \\ x^2 - \ x + 1 & \\ \hline -\ 4x + 1 & \end{array}$$

Обозначая корни заданного уравнения (4) через α и β, придется преобразовать выражение

$$\frac{6\alpha - 4}{-4\alpha + 1}.$$

Поступая по правилу, получаем

$$\frac{(6\alpha - 4)(1 - 4\beta)}{(1 - 4\alpha)(1 - 4\beta)} = \frac{(6\alpha - 4)(1 - 4\beta)}{1 - 4(\alpha + \beta) + 16\alpha\beta}; \tag{5}$$

но

$$\alpha + \beta = 1, \qquad \alpha\beta = 1,$$

следовательно, правая часть тождества (5) преобразуется в

$$\frac{(6\alpha - 4)\{1 - 4(1 - \alpha)\}}{1 - 4 + 16} = \frac{1}{13}(6\alpha - 4)(4\alpha - 3) = \frac{1}{13}(24\alpha^2 - 34\alpha + 12).$$

Производя наконец, деление

$$\begin{array}{r|l} 24\alpha^2 - 34\alpha + 12 & \alpha^2 - \alpha + 1 \\ \hline 24\alpha^2 - 24\alpha + 24 & 24 \\ \hline -\ 10\alpha - 12 & \end{array}$$

получим искомое простейшее выражение

$$-\frac{10}{13}\alpha - \frac{12}{13}.$$

Общие формулы, выражающие зависимость между s_i и p_i

§ 25

Формулы Newton'а позволяют вычислять s_i, когда известны коэффициенты p_i и обратно. Дело сводится к решению уравнений первой степени. Можно однако получить сразу явные выражения этих количеств.

Пусть будет

$$x^n + p_1 x^{n-2} + p_2 x^{n-2} + \ldots + p_n = (x - x_1)(x - x_2) \cdots (x - x_n).$$

Разделяя обе части этого тождества на x^n и логарифмируя, получим

$$\lg\left(1 + \frac{p}{x} + \frac{p_2}{x^2} + \ldots + \frac{p_n}{x^n}\right) = \lg\left(1 - \frac{x_1}{x}\right) + \lg\left(1 - \frac{x_2}{x}\right) + \ldots + \lg\left(1 - \frac{x_n}{x}\right);$$

обозначая для краткости

$$\alpha = \frac{p}{x} + \frac{p_2}{x^2} + \ldots + \frac{p_n}{x^n}$$

и раскладывая логарифмы в ряд, получим

$$\alpha - \frac{\alpha^2}{2} + \frac{\alpha^3}{3} - \frac{\alpha^4}{4} + \ldots = -\left\{\frac{s_1}{x} + \frac{s_2}{2x^2} + \ldots + \frac{s_k}{kx^k} + \ldots\right\}.$$

Для получения s_k придется приравнять коэффициенту $\frac{s_k}{k}$ при x^{-k} в правой части коэффициент при той же степени в левой части. Общий член левой части есть

$$\frac{(-1)^{i+1}}{i}\left(\frac{p}{x} + \frac{p_2}{x^2} + \ldots + \frac{p_n}{x^n}\right)^i. \tag{1}$$

По формуле §§ 6, 7 главы I выражение (1) будет иметь вид

$$\frac{(-1)^{i-1}}{i} \sum \frac{(\beta_1 + \beta_2 + \ldots + \beta_n)!}{\beta_1!\beta_2! \cdots \beta_n!}\, p_1^{\beta_1} p_2^{\beta_2} \cdots p_n^{\beta_n}\, x^{-(\beta_1 + 2\beta_2 + \ldots + n\beta_n)},$$

где

$$\beta_1 + \beta_2 + \ldots + \beta_n = i. \tag{2}$$

Нам необходимо обратить внимание только на те его члены, в которых

$$\beta_1 + 2\beta_2 + 3\beta_3 + \ldots + n\beta_n = k. \tag{3}$$

Мы получаем, следовательно такую общую формулу

$$s_k = \sum \frac{(-1)^{\beta_1 + \beta_2 + \ldots + \beta_n}(\beta_1 + \beta_2 + \ldots + \beta_n)!}{\beta_1!\beta_2! \cdots \beta_n!}\, k p_1^{\beta_1} p_2^{\beta_2} \cdots p_n^{\beta_n},$$

где сумма распространяется на такие целые положительные и равные нулю значения β_i, которые удовлетворяют равенству (2).

Для обратного выражения p_i, через s_i будем рассуждать так

$$1 + \frac{p}{x} + \frac{p_2}{x^2} + \ldots + \frac{p_n}{x^n} = e^{-\left(\frac{s_1}{x} + \frac{s_2}{2x^2} + \cdots\right)} = 1 - \frac{\gamma}{1} + \frac{\gamma^2}{1 \cdot 2} - \ldots,$$

откуда находим

$$p_k = \sum \frac{(-1)^{\beta_1 + \beta_2 + \ldots + \beta_n}}{\beta_1!\beta_2! \cdots \beta_n!}\left(\frac{s_1}{1}\right)^{\beta_1}\left(\frac{s_2}{2}\right)^{\beta_2} \cdots \left(\frac{s_n}{n}\right)^{\beta_n}$$

при том же условии (2).

О вычислении симметрических функций

§ 26

Выражение симметрических функций в явном виде через коэффициенты p_i является настолько важной задачей алгебры, что изучение приемов такого выражения интересовало большинство выдающихся математиков, занимавшихся алгеброй. Особенно важны на практике приемы вычисления, которые дают сразу выражение через коэффициенты p_i, не переходя через s_i.

Одна из хороших метод была дана еще Waring'ом.[39]

Она состоит в общих чертах в следующем.

Обозначим корни уравнения через $a, b, c, \ldots, k, l$.

Берем однородную систематическую функцию V этих корней. Пусть α есть наибольший из показателей, стоящих над корнями в отдельных членах функций V. Очевидно, что в функций V будет существовать один или несколько членов, заключающих a^α.

Из всех этих членов выберем такие, где входит корень b в наибольшей степени β. Продолжая процесс выбора далее по порядку следования корней $c, \ldots, k, l$ придем к определенному члену функции V, который будем называть *старшим*; так что будет

$$V = Aa^\alpha b^\beta c^\gamma \cdots k^\varkappa l^\lambda + \ldots,$$

причем

$$\alpha \geq \beta \geq \gamma \geq \ldots \geq \varkappa \geq \lambda.$$

Не трудно видеть по формулам

$$(-1)p_1 = \sum a, \quad (-1)^2 p_2 = \sum ab, \quad (-1)^3 p_3 = \sum abc, \quad \ldots,$$

что функция

$$P_1 A(-1)^{\alpha+\beta+\gamma+\ldots+\varkappa+\lambda} = p_1^{\alpha-\beta} p_2^{\beta-\gamma} \cdots p_{n-1}^{\varkappa-\lambda} p_n^\lambda$$

будет иметь тот же старший член; следовательно, разность

$$V_1 = V - P_1$$

будет иметь старший член, в котором по крайней мере один из показателей $\alpha, \beta, \gamma, \ldots, \lambda$ меньше, чем для функций V. Продолжая с функцией V_1 то, что мы делали с функцией V, придем к новой функции $V_2 = V_1 - P_2$ и т. д. получим

$$V = P_1 + P_2 + \ldots$$

После конечного ряда операций функция будет исчерпана, ибо показатели уменьшаются.

Если считать неизбежными трудности, происходящие от высоких степеней как основного уравнения, так и самой симметрической функции V, то способ Waring'а

[39] Waring. Meditationes algebraicae. Editio tertia p. 13.

приходится считать хорошим для практики, особенно после улучшений последующих ученых.[40]

§ 27

Имеет для практики некоторое значение метода Cauchy, изложенная нами выше. Покажем ее приложение на одном примере.

Требуется вычислить дискриминант уравнения 3-ей степени

$$x^3 + px^2 + qx + r = 0.$$

Этот дискриминант есть

$$V = V_1(a-b)^2(a-c)^2,$$

где V_1 есть дискриминант $(b-c)^2$ квадратного уравнения

$$x^2 + (p+a)x + a^2 + pa + q - 0,$$

как известно,

$$V_1 = (p+a)^2 - 4(a^2+pa+q) = -3a^2 - 2pa + (p^2 - 4q)$$
$$(a-b)(a-c) = f'(a)3a^2 + 2pa + q$$

и, следовательно,

$$V = (-3a^2 - 2pa + p_2 - 4q)(3a^2 + 2pa + q)^2 =$$
$$= -27a^6 - 54pa^5 - 27p^2 \left| \begin{array}{c} a^4 + 4p^3 \\ -72pq \end{array} \right| \left| \begin{array}{c} a^3 + 4p^4 \\ -18p^2q \\ -27q^2 \end{array} \right| \left| \begin{array}{c} a^2 + 4p^3q \\ -18pq^2 \end{array} \right| \left| \begin{array}{c} a + p^2q^2 \\ -4q^3 \end{array} \right| \begin{array}{l} \\ -54q \\ \\ \\ \\ \end{array} .$$

Разделяя это выражение V на $a^3 + pa^2 + qa + r$, получим частное

$$-27a^3 - 27pa^2 - 27qa + 4p^3 + 27r - 18pq$$

и остаток

$$-4q^3 - 27r^2 + 18pqr + p^2q^2 - 4p^3r;$$

последнее выражение и есть искомое выражение для V.

В курсе Serret «Cours d'algébre supérieure» 1910 г. целая глава посвящена общим соображениям о вычислений симметрических функций, где автор излагает приложение известного ряда Lagrange'a, а также некоторые собственные мысли, относящаяся к этому предмету.

§ 28

Я считаю необходимым добавить еще несколько замечаний, помогающих составить для всякой однородной симметрической функций корней ее буквенное

[40] Peterson. Théorie des équations algébriques, Paris 18S7, p. 34.

выражение через p_i с неопределенными коэффициентами, подлежащими дальнейшему определению.

Теорема. *Если считать весом p_i число i, то однородная целая смммметрическая функция степени m от корней x_i должна быть после выражены через p_i изобарическою веса m.*

Будем предполагать корни x_i независимыми переменными, тогда и коэффициенты p_i будут также независимыми переменными, ибо всякое соотношение между p_i выраженное через корни x_i, давало бы зависимость между корнями.

Пусть имеем

$$f(x_1, \ldots, x_n) = \varphi(p_1, p_2, \ldots, p_n).$$

Разобьем функцию φ на изобарические части и возьмем одну из этих частей φ_0 обозначая ее вес через μ.

Эта часть φ_0, не будучи тождественно равной пулю, не может давать тождественно равное нулю выражение, если мы все p_i выразим через корни. В самом деле, φ_0, выраженная в корнях, не будет равна нулю, если мы возьмем корни уравнения с такими коэффициентами, при которых φ_0 равно нулю. Итак, всякая изобарическая часть φ_0 веса μ будет давать однородную функцию от корней степени μ. Так как члены однородных функций разных степеней сокращаться не могут, следовательно, если заданная однородная симметрическая функция f имеет степень m, то она должна быть в p_i изобарическою веса $\mu = m$.

Теорема. *Целая симметрическая функция от корней x_i имеет такую степень в коэффициентах p_i, какой степени она относительно любою из корней.*

Будем рассматривать функцию

$$f(x_1, \ldots, x_n) = \varphi(p_1, p_2, \ldots, p_n)$$

относительно какого нибудь определенного из корней x_1. Пусть относительно этого корня функция f имеет степень m. Обозначим через μ степень φ относительно $p_1, p_2, \ldots, p_n$. Надо доказать равенство

$$m = \mu.$$

Неравенство $m \leq \mu$ следует из того соображения, что всякий коэффициент p_i первой степени относительно x_i. Теперь надо показать, что не может быть $m < \mu$, то есть, что но может тождественно равняться нулю коэффициент при x_1^m.

Обозначим через $q_1, q_2, q_3, \ldots$ сумму сочетания остальных (кроме x_1) корней по одному, по два, по три и т. д. Будем иметь формулы

$$(-1)p_1 = x_1 + q_1, \quad (-1)^2 p_2 = x_1 q_1 + q_2, \quad (-1)^3 p_3 = x_1 q_2 + q_3.$$

Мы видим, что если степень x_1^m происходит из члена $p_1^l p_2^r p_3^s p_4^t$, то независимо от знака коэффициент у x_1^m будет $q_1^r q_2^s q_3^t$, обратно коэффициент $q_1^r q_2^s q_3^t$ может происходить только от члена $p_1^l p_2^r p_3^s p_4^t$, ибо $l + r + s + t = m$. Итак, этот член с x_1^m не может сократиться с членами, происходящими от других членов φ, и, следовательно, $m = \mu$.

§ 29

Когда дело идет об удобных приемах вычисления симметрических функций, то нет возможности обойти молчанием приемы вычисления функций от разностей корней, называемых некоторыми авторами[41] *критическими*. К числу таких функций принадлежат, например, дискриминант.

Критическая функция не меняется, если все корни получают одно и тоже приращение λ. Заменяя в уравнении x на $x+\lambda$, получим

$$x^n + (p_1 + n\lambda)x^{n-1} + \left\{ p_2 + (n-1)\lambda p_1 + \frac{1}{2}n(n-1)\lambda^2 \right\} x^{n-2} + \ldots = 0.!$$

Тогда критическая функция φ, выраженная через p_i, обратится в следующую

$$(1) \qquad \varphi + \left\{ \frac{\partial\varphi}{\partial p_1}\, dp_1 + \frac{\partial\varphi}{\partial p_2}\, dp_2 + \ldots \right\} + \frac{1}{1\cdot 2}\left\{ \frac{\partial^2\varphi}{\partial p_1^2}\, dp_1^2 + \ldots \right\} + \ldots$$

Но приращения $dp_1, dp_2, \ldots$ коэффициентов можно заменить выражениями

$$n\lambda, \quad (n-1)\lambda p_1 + \frac{1}{2}n(n-1)\lambda^2, \ \ldots, !$$

отсюда, располагая выражение (1) но степеням λ, получим

$$(1) \qquad \varphi + \lambda\left\{ n\frac{\partial\varphi}{\partial p_1} + (n-1)p_1\frac{\partial\varphi}{\partial p_2} + (n-2)p_2\frac{\partial\varphi}{\partial p_3} + \ldots \right\} + \lambda^2\{\ldots\} + \ldots$$

Так как функция φ не должна меняться, то мы приходим в *дифференциальному уравнению*

$$(2) \qquad n\frac{\partial\varphi}{\partial p_1} + (n-1)p_1\frac{\partial\varphi}{\partial p_2} + (n-2)p_2\frac{\partial\varphi}{\partial p_3} + \ldots = 0.$$

§ 30

Покажем приложение приемов двух предыдущих параграфов к вычислению дискриминанта

$$V = (x_1 - x_2)^2(x_1 - x_3)^2(x_2 - x_3)^2$$

уравнения третьей степени

$$x^3 + p_1x^2 + p_2x + p_3 = 0.$$

Так как V должна быть функцией изобарической в p_i веса 6 и степени (неоднородной) 4, то она может быть только такого вида

$$(1) \qquad V = Ap_3^2 + Bp_3p_2p_1 + Cp_3p_1^3 + Dp_2^3 + Ep_2^2p_1^2.$$

Составляем дифференциальное уравнение

$$3\frac{\partial V}{\partial p_1} + 2p_1\frac{\partial V}{\partial p_2} + p_2\frac{\partial V}{\partial p_3} = 0.$$

[41] Salmon. Vorlesungen ü. d. Algebra d. lin. Transf. 1877, s. 70.

Получаем

$$(2A+3B)p_3p_2+(2B+9C)p_3p_1^2+(B+6D+6E)p_2^2p_1+(C+4E)p_2p_1^3=0.$$

Это равенство должно быть тождеством, следовательно,

$$2A+3B=0,\quad 2B+9C=0,\quad B+6D+6E=0,\quad C+4E=0,$$

откуда

$$C=-4E,\quad B=18E,\quad A=-27E,\quad D=-4E.$$

Полагая $x_3=0$, а, следовательно, и p_3, получаем на основании (1) $E=1$, так что окончательно

$$V=p_1^2p_2^2+18p_1p_2p_3-4p_2^3-4p_3p_1^3-27p_3^2.$$

Если кубическое уравнение имеет вид

$$x^3+px+q=0,$$

то $p_1=0$, $p_2=p$, $p_3=q$ и, следовательно,

$$V=-(27q^2+p^3).$$

§ 31

Вычислим дискриминант уравнения 4-ой степени

$$x^4+p_1x^3+p_2x^2+p_3x+p_4=0, \tag{1}$$

ибо его выражение понадобится нам в дальнейшем.

Уничтожим по способу § 6 главы III коэффициент при x^3, тогда получим уравнение

$$y^4+ay^2+by+c=0, \tag{2}$$

где

$$\begin{gathered}a=-\frac{3}{8}p_1^2+p_2,\quad b=\frac{1}{8}p_1^3-\frac{1}{2}p_1p_2+p_3\\ c=-\frac{3}{256}p_1^4+\frac{1}{16}p_1^2p_2-\frac{1}{4}p_1p_3+p_4.\end{gathered} \tag{3}$$

Положим

$$2y=u+v+w,$$

и кроме того для сокращения

$$s=u^2+v^2+w^2,\quad t=v^2w^2+u^2w^2+u^2v^2.$$

Тогда

$$4y^2=s+2(vw+uw+uv),$$

$$16y^4 = s^2 + 4s(vw + uw + uv) + 4t + 8uvw(u + v + w).$$

Вставляя в уравнение (2), получим

$$s^2 + 4t + 4as + 16c + 8(uvw + b)(u + v + w) + \\ + 4(s + 2a)(vw + uw + uv) = 0.$$

Две произвольные из трех величин u, v, w подбираем так, чтобы было

$$uvw + b = 0, \qquad s + 2a = 0. \tag{3}$$

Тогда будет

$$s^2 + 4t + 4as + 16c = 0$$

или проще (на оснований (3))

$$t = a^2 - 4c. \tag{4}$$

Сопоставляя (3) и (4), мы получаем

$$u^2 + v^2 + w^2 = -2a$$
$$v^2w^2 + u^2w^2 + u^2v^2 = a^2 - 4c$$
$$u^2v^2w^2 = b^2$$

т. е. u^2, v^2, w^2 оказываются корнями кубического уравнения

$$z^3 + 2az^2 + (a^2 - 4c)z - b^2 = 0.$$

Знаки u, v, w надо так подбирать, чтобы имело место первое из равенств (3). Мы приходим к четырем корням уравнения (2)

$$2y_1 = \quad u + v + w,$$
$$2y_2 = \quad u - v - w,$$
$$2y_3 = -u + v - w,$$
$$2y_4 = -u - v + w.$$

Так как корни x_i уравнения (1) отличаются постоянным числом $\dfrac{p_1}{4}$ от корней y_i уравнения (2), то дискриминанты обоих уравнений одинаковы, и мы можем вычислять дискриминант D для уравнения (2):

$$y_1 - y_2 = v + w, \quad y_3 - y_4 = v - w,$$
$$y_1 - y_3 = w + u, \quad y_4 - y_2 = w - u,$$
$$y_1 - y_4 = u + v, \quad y_2 - y_4 = u - v,$$

откуда

$$D = (v^2 - w^2)^2(w^2 - u^2)^2(u^2 - v^2)^2.$$

То есть D есть также дискриминант уравнения

$$z^3 + 2az^2 + (a^2 - 4c)z - b^2 = 0.$$

Если мы уничтожим коэффициент при z^2, т. е. будем рассматривать уравнение

$$z_1^3 + pz_1 + q,$$

то получим

$$p = -\frac{1}{3}(2a)^2 + (a^2 - 4c),$$
$$27q = 2(2a)^3 - 9 \cdot 2a(a^2 - 4c) + 27(-b^2).$$

Дискриминант будет выражаться так

$$D = -(27q^2 + 4p^3);$$

подставляя сюда вместо p и q сначала a, b, c и затем p_1, p_2, p_3, p_4, получим после шаблонных выкладок равенство

$$27D = 4A^3 - B^2,$$

где

$$A = p_2^2 - 3p_2p_3 + 12p_4,$$
$$B = 27p_1^2p_4 + 27p_3^2 + 2p_2^3 - 72p_2p_4 - 9p_1p_2p_3.$$

Преобразование Tschirnhausen'a

§ 32

Будем рассматривать задачу, поставленную Tschirnhausen'ом, о преобразовании уравнения

$$x^n + p_1x^{n-2} + p_2x^{n-2} + \ldots + p_n == 0 \tag{1}$$

к новой неизвестной y, представляющей из себя рациональную функцию от первоначальной неизвестной x

$$y = \varphi(x). \tag{2}$$

Другими словами, надо составить уравнение

$$y^n + q_1y^{n-1} + q_2y^{n-2} + \ldots + q_n = 0, \tag{3}$$

которого корни суть

$$y_1 = \varphi(x_1), \quad y_2 = \varphi(x_2), \ \ldots, \ y_n = \varphi(x_n),$$

если

$$x_1, \quad x_2, \ \ldots, \ x_n$$

суть корни первоначального уравнения (1).

Очевидно, что коэффициенты q_i нового уравнения будут симметрическими функциями от выражений

$$\varphi(x_1), \quad \varphi(x_2), \ \ldots, \ \varphi(x_n),$$

а, следовательно, они будут также и симметрическими функциями от корней $x_1, x_2, \ldots, x_n$ и мы найдем их выражения через p_i по выше указанным правилам вычисления симметрических функций.

§ 33

Покажем теперь более удобный в практическом отношении прием осуществления преобразования Tschirnhausen'a. Прежде всего, мы можем на основании соображений § 24 рациональную функцию $\varphi(x)$ от корня x представить в простейшем виде

$$y = a_0 + a_1 x + a_2 x^2 + \ldots + a_{n-1} x^{n-1}; \tag{1}$$

умножая равенство (1) на x, получим

$$yx = a_0 x + a_1 x^2 + a_2 x^3 + \ldots + a_{n-1} x^n.$$

На основании уравнения (1) § 32 можно будет заменить x^n на

$$-p_1 x^{n-1} - p_2 x^{n-2} - \ldots - p_{n-2} x^2 - p_{n-1} x - p_n$$

и мы получим

$$yx = a'_0 + a'_1 x + a'_2 x^2 + \ldots + a'_{n-1} x^{n-1},$$

где

$$a'_0 = -a_{n-1} p_n, \quad a'_1 = a_0 - a_{n-1} p_{n-1}, \quad a'_2 = a_1 - a_{n-1} a_{n-2}, \quad \ldots.$$

Подобным же образом, представляя в простейшем виде также выражения $yx^2, yx^3, \ldots, yx^{n-1}$, получим

$$\begin{aligned}
y &= a_0 + a_1 x + a_2 x^2 + \ldots + a_{n-1} x^{n-1}, \\
yx &= a'_0 + a'_1 x + a'_2 x^2 + \ldots + a'_{n-1} x^{n-1}, \\
yx^2 &= a''_0 + a''_1 x + a''_2 x^2 + \ldots + a''_{n-1} x^{n-1}, \\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\
yx^{n-1} &= a_0^{(n-1)} + a_1^{(n-1)} x + a_2^{(n-1)} x^2 + \ldots + a_{n-1}^{(n-1)} x^{n-1}.
\end{aligned}$$

Исключая из этой системы величины $x, x^2, \ldots, x^{n-1}$, получим

$$\begin{vmatrix}
a_0 - y & a_1 & a_2 & \ldots & a_{n-1} \\
a'_0 & a'_1 - y & a'_2 & \ldots & a'_{n-1} \\
a''_0 & a''_1 & a''_2 - y & \ldots & a''_{n-1} \\
\ldots & \ldots & \ldots & \ldots & \ldots \\
a_0^{(n-1)} & a_1^{(n-1)} & a_2^{(n-1)} & \ldots & a_{n-1}^{(n-1)} - y
\end{vmatrix} = 0. \tag{2}$$

Уравнение (2) степени n от y и есть искомое преобразованное по методу Tschirnhausen'a.

§ 34

Tschirnhausen рассматривал преобразование как методу для решения уравнений. Он старался найти вид функции $\varphi(x)$ таким образом, чтобы в преобразованном уравнении уничтожалось возможно большое число коэффициентов q_i. Таким путем можно, например, решить уравнения 3-ей и 4-ой степени.

Для уравнения третьей степени Tschirnhausen и Euler предлагают положить

$$y^2 + \alpha y + \beta = x \tag{1}$$

и подобрать α и β таким образом, чтобы после исключения y из (1) и следующего уравнения

$$y^3 = d \tag{2}$$

получалось заданное уравнение третьей степени.

В случае уравнения третьей степени можно считать простейшим видом рациональной функций от его корня одну из двух функции

$$a_0 + a_1 x + a_2 x^2, \qquad \frac{a_0 + a_1 x}{1 + a_2 x};$$

так что можно было бы приводить заданное уравнение третьей степени к виду (2) не только при помощи соотношения (1), но также и при помощи такого

$$x = \frac{\alpha + \beta y}{1 + y}.$$

Для решения уравнения четвертой степени Tschirnhausen предлагает привести его к виду

$$y^4 + py^2 + q = 0$$

при помощи соотношения

$$y = \alpha + \beta x + x^2.$$

Euler исключает y между двумя уравнениями

$$x = a_0 + a_1 y + a_2 y^2 + a_3 y^3$$
$$y^4 = d$$

и подбирает a_0, a_1, a_2, a_3, d таким образом, чтобы результат исключения совпадал с заданным уравнением.

§ 35

Возвращаясь к общей теории, приведем уравнение

$$x^n + p_1 x^{n-1} + \ldots + p_n = 0 \tag{1}$$

к виду

$$y^n + q_1 y^{n-1} + \ldots + q_n = 0 \tag{2}$$

при помощи соотношения

$$y = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4.$$

Всякая сумма k-ых степеней корней уравнений (2) будет формой степени k относительно a_0, a_1, a_2, a_3, a_4. Следовательно, коэффициенты q_i, выражаясь рационально через коэффициенты уравнения (1), будут в тоже время формами относительно a_i, причем степень каждого q_i относительно a_i будет равна индексу i этого коэффициента.

M. Jerrard показал, что можно свести к решению кубического уравнения задачу выбора a_0, a_1, a_2, a_3, a_4, таким образом, чтобы уничтожились второй, третий и четвертый коэффициенты уравнения, какова бы ни была степень этого уравнения; т. е. чтобы было

$$q_1 = 0, \quad q_2 = 0, \quad q_3 = 0. \tag{3}$$

Начнем с рассмотрения первого уравнения $q_1 = 0$. Так как это уравнение первой степени относительно a_l, то можно будет выразить a_0 линейно через a_1, a_2, a_3, a_4. Подставляя эти выражения в два остальных уравнения (3), получим

$$q_2' = 0, \quad q_3' = 0,$$

где q_2' форма квадратичная относительно a_1, a_2, a_3, a_4, а q_3' форма третьей степени.

Представляя квадратичную форму в виде суммы квадратов линейных функций, перепишем уравнение $q_2' = 0$ в таком виде

$$f^2 + g^2 + h^2 + k^2 = 0, \tag{4}$$

где f, g, h, k линейные формы относительно a_l, уравнение (4) можно будет удовлетворить, полагая

$$f^2 + g^2 = 0, \quad h^2 + k^2 = 0$$

или

$$f = g\sqrt{-1}, \quad h = k\sqrt{-1}. \tag{5}$$

Из уравнений (5) выражаются a_1, a_2 линейно через a_3, a_4. Подставляя эти выражения в последнее уравнение ?, получим

$$q_3'' = 0,$$

где q_3'' кубическая форма относительно двух переменных a_3 и a_4. Одна из этих переменных остается произвольною, другая же определяется из уравнения третьей степени, так что теорема Jerrard'a оказывается справедливою.

Можно было бы совершенно подобным образом достигнуть того чтобы было

$$q_1 = 0, \quad q_2 = 0, \quad q_4 = 0.$$

Мы причем очевидно к уравнению четвертой степени. Итак, мы видим, что решается в радикалах задача уничтожения при помощи преобразования Tschirnhausen'a или коэффициентов p_1, p_2, p_3, или же коэффициентов p_1, p_2, p_4. Заменой x

на $\frac{1}{x}$ мы перенесем соображения, относящаяся к старшим коэффициентам на соображения относящаяся к младшим. Можно будет достигнуть уничтожения, или коэффициентов p_{n-3}, p_{n-2}, p_{n-1}, или же коэффициентов p_{n-4}, p_{n-2}, p_{n-1}.

В применении к уравнениям 5-ой степени мы замечаем, что это уравнение может быть приведено к одному из следующих видов

$$x^5 + px + q = 0,$$
$$x^5 + px^2 + q = 0,$$
$$x^5 + px^3 + q = 0,$$
$$x^5 + px^4 + q = 0.$$

§ 36

Покажем теперь замечательный вид, под которым представляет Hermite преобразование Tschirnhausen'a.

Мы придадим изложению характер приложения символического исчисления. Мы будем предполагать известиями начала этого исчисления по крайней мере в той форме, как это изложено в главе XIV курса теории чисел (второе издание 1913).

Мысль Hermite'a состоит в выражений рациональных функций от корня x неприводимого уравнения

$$f(x) = x^n + p_1x^{n-2} + p_2x^{n-2} + \ldots + p_n = 0$$

в виде

$$y = \alpha_{n-1}\omega_0 + \alpha_{n-2}\omega_1 + \ldots + \alpha_1\omega_{n-2} + \alpha_0\omega_{n-1}, \tag{1}$$

где

$$\omega_0 = 1, \quad \omega_1 = x + p_1, \quad \omega_2 = x^2 + p_1x + p_2, \ \ldots, \ \omega_k = x^k + p_1x^{k-1} + \ldots + p_k, \ \ldots$$

Коэффициенты α_i в выражении (1) суть новые переменные независимые. Так как степени $1, x, x^2, \ldots, x^{n-1}$ выражаются линейно через

$$\omega_0, \quad \omega_1, \ldots, \ \omega_{n-1},$$

то очевидно, что в виде (1) может быть представлена всякая целая функция степени не выше $n-1$ при помощи соответственного выбора коэффициентов α_i. Выражая через ω_i, величину $y\omega_k$ получим

$$y\omega_k = A_0^{(k)}\omega_0 + A_1^{(k)}\omega_1 + \ldots + A_{n-1}^{(k)}\omega_{n-1}. \tag{2}$$

Выписав все уравнения (2) для всех значений ? значка $1, 2, \ldots, (n-1)$ и исключая $\omega_0, \omega_1, \ldots, \omega_{n-1}$, получим преобразованное уравнение для y

$$\begin{vmatrix} A_0^{(0)} - y & A_1^{(0)} & \ldots & A_{n-1}^{(0)} \\ A_0^{(1)} & A_1^{(1)} - y & \ldots & A_{n-1}^{(1)} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ A_0^{(n-1)} & A_1^{(n-1)} & \ldots & A_{n-1}^{(n-1)} - y \end{vmatrix} = 0. \tag{3}$$

Остается показать как вычислить все коэффициенты $A_i^{(k)}$.

Равенство (2) должно быть тождеством относительно x, если только после перемножений в произведении $y\omega_k$ заменить все степени выше x^{n-1} при помощи уравнения $f(x) = 0$. Тождество относительно $\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_{n-1}$ останется тождеством, если заменить нижние значки показателями, то есть, вместо прежних независимых переменных ввести величины $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$. Получим из (2) новое тождество

$$\begin{aligned}[\alpha^{n-1}\omega_0 + \alpha^{n-2}\omega_1 + \ldots + \alpha\omega_{n-2} + \omega_{n-1}\omega_k = \\ = \mathfrak{A}_0^{(k)}\omega_0 + \mathfrak{A}_1^{(k)}\omega_1 + \ldots + \mathfrak{A}_{n-1}^{(k)}\omega_{n-1},\end{aligned} \tag{4}$$

где $\mathfrak{A}_i^{(k)}$ получается из $A_i^{(k)}$ заменой α_i на α^i.

Подставим в тождество (4) $x = \alpha$, не забывая формального правила исключать степени α выше α^{n-1} при помощи уравнения $f(\alpha) = 0$. Пусть обозначен через ω_i' результата подстановки α вместо x в величину ω_i. Равенство (4) перепишется так

$$[\alpha^{n-1}\omega_k' - \mathfrak{A}_0^{(k)}]\omega_0' + [\alpha^{n-2}\omega_k' - \mathfrak{A}_1^{(k)}]\omega_1' + \ldots = 0,$$

отсюда на основании независимости функции ω_i' получим

$$\mathfrak{A}_i^{(k)} = \alpha^{n-i-1}\omega_k'.$$

Таким образом мы получаем символическое равенство

$$A_i^{(k)} \doteqdot \alpha^{n-i-1}\omega_k(\alpha). \tag{5}$$

Это равенство надо понимать так: надо найти остаток

$$a_1\alpha^{n-1} + a_2\alpha^{n-2} + \ldots + a_{n-1}\alpha + a_n$$

от деления $\alpha^{n-i-1}\omega_k(\alpha)$ на $f(\alpha)$ и тогда получится настоящее равенство

$$A_i^{(k)} = a_1\alpha_{n-1} + a_2\alpha_{n-2} + \ldots + a_{n-1}\alpha_1 + a_n\alpha_0,$$

если заменить показатели значками.

§ 37

Поясним теории примером уравнений 3-ей степени

$$f(x) = x^3 + p_2x^2 + p_2x + p_3 = 0$$

$$\omega_0 = 1, \quad \omega_1 = x + p_1, \quad \omega_2 = x^2 + p_1x + p_2$$

$$\begin{aligned}
A_0^{(0)} &= \alpha^2\omega_0 = \alpha_2, \quad A_1^{(0)} = \alpha\omega_0 = \alpha_1, \quad A_2^{(0)} = \omega_0 = 1, \\
A_0^{(1)} &= \alpha^2\omega_1 = \alpha^3 + p_1\alpha^2 = -p_2\alpha - p_3 = -p_2\alpha_1 - p_3\alpha_0, \\
A_1^{(1)} &= \alpha\omega_1 = \alpha^2 + p_1\alpha = \alpha_2 + p_1\alpha_1, \\
A_2^{(1)} &= \omega_1 = \alpha + p_1 = \alpha_1 + p_1\alpha_0, \\
A_0^{(2)} &= \alpha^2\omega_2 = \alpha^4 + p_1\alpha^3 + p_2\alpha^2 = -p_3\alpha = -p_3\alpha_1, \\
A_1^{(2)} &= \alpha\omega_2 = \alpha^3 + p_1\alpha^2 + p_2\alpha = -p_3 - p_3\alpha_0, \\
A_2^{(2)} &= \omega_2 = \alpha^2 + p_1\alpha + p_2 = \alpha_2 + p_1\alpha_1 + p_2\alpha_0.
\end{aligned}$$

Применим символическое вычисление к нахождение кубического уравнения

$$y^3 + P_1 y^2 + P_2 y + P_3 = 0,$$

которому удовлетворяет выражение

$$y = \alpha_2\omega_0 + \alpha_1\omega_1 + \alpha_0\omega_2.$$

Это кубическое уравнение может быть написано в символическом виде так

$$\begin{vmatrix} \alpha^2\omega_0 - y & \alpha\omega_0 & \omega_0 \\ \beta^2\omega_1(\beta) & \beta\omega_1(\beta) - y & \omega_1(\beta) \\ \gamma^2\omega_2(\gamma) & \gamma\omega_2(\gamma) & \omega_2(\gamma) - y \end{vmatrix} = 0, \tag{1}$$

где, после выполнения действий и уничтожения степеней выше второй символов α, β, γ на основании уравнений $f(\alpha) = 0$, $f(\beta) = 0$, $f(\gamma) = 0$, придется подставить $\alpha^i = \beta^i = \gamma^i = \alpha_i$.

Получаем

$$P_1 = \alpha^2\omega_0 + \beta\omega_1(\beta) + \omega_2(\gamma) = \alpha^2 + \alpha(\alpha + p_1) + \alpha^2 + p_1 + p_2 = \\ = 3\alpha^2 + 2p_1\alpha + p_2 = f'(\alpha) = 3\alpha_2 + 2p_1\alpha_1 + p_2\alpha_0.$$

Коэффициент P_2 будет квадратичной формой от α_0, α_1, α_2, а P_3 формой кубичной.

Выберем одну из переменных независимых α_0, α_1, α_2 так, чтобы было $P_1 = 0$, или, что одно и тоже,

$$3\alpha_2 + 2p_1\alpha_1 + p_2\alpha_0 = 0 \tag{2}$$

из этого равенства можно выразить α_2 линейно через α_0 и α_0; подставляя это выражение в коэффициент P_2, мы получим этот последний в виде квадратичной формы от двух букв α_1 и α_0

$$3P_2 = A\alpha_1^2 + B\alpha_1\alpha_2 + C\alpha_2^2.$$

Эта форма по предложению Sylvester'a носить название *безутианты* для заданного уравнения $f(x) = 0$.

Из уравнения (1) имеем

$$P_2 = \beta\omega_1(\beta)\omega_2(\gamma) + \alpha^2\omega_2(\gamma) + \alpha^2\beta\omega_1(\beta) - \gamma^2\omega_2(\gamma) - \alpha\beta^2\omega_1(\beta) - \gamma\omega_2(\gamma)\omega_1(\beta).$$

Можно ограничиться, очевидно, двумя только символическими буквами α, γ

$$P_2 = \alpha\omega_1(\alpha)\omega_2(\gamma) + \alpha^2\omega_2(\gamma) + \alpha^2\gamma\omega_1(\gamma) + p_3\gamma + \gamma(p_2\alpha + p_3) + p_3(\gamma + p_1) = \\ = (3\alpha^2 + p_1\alpha)\omega_2(\gamma) - \alpha^2 p_2 + 3p_3\gamma + p_1p_3 + p_2\alpha\gamma.$$

Но принимая в соображение (2), которое можно переписать в таком символическом виде

$$3\alpha^2 + 2p_1\alpha + p_2 = 0,$$

мы получим

$$3P_2 = -(p_1\alpha + p_2)(p_1\gamma + 2p_2) - 3\alpha^2 p_2 + 9p_3\gamma + 3p_1p_3 + 3p_2\alpha\gamma = \\ = (3\gamma + p_1)(p_2\alpha + 3p_3) - (p_1\alpha + p_2)(p_1\gamma + p_2),$$

или окончательно

$$3P_2 = \begin{vmatrix} 3\alpha_1 + p_1\alpha_0 & p_1\alpha_1 + p_2\alpha_0 \\ p_1\alpha_1 + p_2\alpha_0 & p_2\alpha_1 + 3p_3\alpha_0 \end{vmatrix}. \tag{3}$$

Найденная формула (3) заслуживает внимания.

Приведем первую часть $f(x)$ заданного уравнения в вид бинарной формы

$$f(x, y) = x^3 + p_1x^2y + p_2xy^2 + p_3y^3$$

и составим определитель

$$H(\xi, \eta) = \begin{vmatrix} f''_{xx}(\xi, \eta) & f''_{xy}(\xi, \eta) \\ f''_{yx}(\xi, \eta) & f''_{yy}(\xi, \eta) \end{vmatrix},$$

элементы которого суть вторые частные производные формы $f(x, y)$. Этот определитель носит название *гессиана* формы $f(x, y)$.

Очевидно, что будет

$$3P_2 = H(\alpha_1, \alpha_0)$$

и коэффициенты искомой безутианты будут

$$A = 3p_2 - p_1^2, \quad B = 9p_3 - p_1p_2, \quad C = 3p_1p_3 - p_2^2.$$

Кроме того будет

$$3D = 4AC - B_1^2,$$

где D дискриминант заданного кубического уравнения.

Заметим здесь кстати, что гессиан $H(\xi, \eta)$ есть ковариант веса 2 формы $f(x, y)$.

Приведенные соображения обобщаются на случай безутианты уравнения всякой степени.

Вычислим теперь последний коэффициент P_3

$$-P_3 = \begin{vmatrix} \alpha^2\omega_0 & \alpha\omega_0 & \omega_0 \\ \beta^2\omega_1(\beta) & \beta\omega_1(\beta) & \omega_1(\beta) \\ \gamma^2\omega_2(\gamma) & \gamma\omega_2(\gamma) & \omega_2(\gamma) \end{vmatrix} = \omega_1(\beta)\omega_2(\gamma)(\alpha - \beta)(\alpha - \gamma)(\beta - \gamma);$$

производя перемножение, уничтожая высшие степени α, β, γ и заменяя показатели значками, легко получим окончательное выражение P_3 через α_0, α_1, α_2.

Глава X

Об отделении корней

О пределах модуля корня

§ 1

Покажем, что можно найти два таких положительных числа l и L (при условии $L > l$), что модули всех корней уравнения

$$f(x) = p_0x^n + p_1x^{n-1} + \ldots + p_{n-1}x + p_n = 0$$

будут заключаться между этими числами.

Такие числа l и L называются *пределами* модулей корней заданного уравнения; число l называется *низшим* пределом, а число L называется *высшим*.

§ 2

Рассмотрим функцию самого общего вида

$$f(x) = p_0x^n + p_1x^{n-1} + \ldots + p_{n-1}x + p_n = 0,$$

где коэффициенты $p_0, p_1, \ldots, p_n$ какие угодно вещественные или комплексные числа. Мы видели уже (см. стр. 11), что можно указать такой круг плоскости, что для точек вне этого круга модуль $|f(x)|$ функции будет больше некоторого положительного числа, и, следовательно, корни самой функции будут все лежать внутри этого круга. Их расстояния от начала координат, т. е. модули, будут числа конечные.

Не трудно указать простое правило для вычисления такого положительного числа L, которое больше модулей всех корней.

Обозначим через

$$a_0, \quad a_1, \quad a_2, \quad a_3, \ \ldots, \ a_n$$

модули коэффициентов

$$p_0, \quad p_1, \quad p_2, \quad p_3, \ \ldots, \ p_n$$

и кроме того обозначим через a наибольшее из чисел: $a_1, a_2, a_3, \ldots, a_n$; тогда мы получим по теореме о модуле суммы двух чисел

$$|f(x)| \geq |p_0x^n| - |p_1x^{n-1} + \ldots + p_n|. \tag{2}$$

Обозначая через ρ модуль x, получим

$$|p_0x^n| = a_0\rho^n$$

и кроме того

$$\begin{aligned} |p_1x^{n-1} + p_2x^{n-2} + \ldots + p_n| &\leq a_1\rho^{n-1} + a_2\rho^{n-2} + \ldots + a_n \\ &\leq a(\rho^{n-1} + \rho^{n-2} + \ldots + 1) \\ &\leq a\,\frac{\rho^n - 1}{\rho - 1}. \end{aligned}$$

Отсюда мы получаем

$$|f(x)| \geq a_0\rho^n - a\,\frac{\rho^n - 1}{\rho - 1}. \tag{3}$$

Для получения искомого верхнего предела L модулей корней достаточно указать такое число ρ, чтобы при $|x| = \rho$ модуль $|f(x)|$ был больше нуля. Для этой цели, предполагая

$$\rho > 1, \tag{4}$$

достаточно удовлетворить неравенству

$$a_0\rho^n - a\,\frac{\rho^n - 1}{\rho - 1} > 0. \tag{5}$$

На основании неравенства (4) неравенство (5) может быть переписано так

$$a_0\rho^n(\rho - 1) - a(\rho^n - 1) > 0$$

или

$$a_0\rho^n(\rho - 1) - a\rho^n + a > 0. \tag{6}$$

Неравенство (6) удовлетворится наверно, если мы удовлетворим неравенству

$$a_0\rho^n(\rho - 1) - a\rho^n > 0,$$

или

$$a_0(\rho - 1) - a > 0;$$

отсюда

$$a_0\rho > a_0 + a$$

и, значить,

$$\rho > 1 + \frac{a}{a_0}. \tag{7}$$

Итак, за верхний предел L модулей корней рассматриваемой функции можно принять число $1 + \dfrac{a}{a_0}$.

Если коэффициент p_n не равен нулю, то не существует корней функции равных нулю, и можно будет указать такое число l, что модули всех корней функции будут больше l.

В самом деле введем новую переменную при помощи уравнения

$$x = \frac{1}{y};$$

тогда уравнение относительно новой переменной примет вид

$$p_0 + p_1 y + p_2 y^2 + \ldots + p_{n-1} y^{n-1} + p_n y^n = 0. \tag{8}$$

Обозначили, через b высший предел модулей корней последнего уравнения. На основании предыдущих соображений будем иметь

$$b = 1 + \frac{\alpha}{a_n},$$

где α наибольший из модулей $a_0, a_1, a_2, \ldots, a_{n-1}$.

Очевидно, что за *низший* предел модулей корней заданного уравнения можно принять

$$\frac{1}{b},$$

т. е. число

$$\frac{a_n}{a_n + \alpha}.$$

Итак, мы видим, что, если x есть корень уравнения

$$f(x) = 0,$$

то должны иметь место неравенства:

$$\frac{a_n}{a_n + \alpha} < |x| < 1 + \frac{a}{a_0}.$$

§ 3

Полученный результат можно представить следующим образом геометрически. Если мы из начала координат, как центра, опишем две окружности радиусами, равными высшему и низшему пределам модулей корней, то все корни уравнения должны заключаться в пространстве между этими окружностями. Сами же пределы l и L будут даже пределы для вещественных корней, причем для положительных корней получаются пределы $+l$ и $+L$, а для отрицательных корней пределы $-L$ и $-l$.

О пределах вещественных корней

§ 4

Хотя показанные нами пределы модулей комплексных корней дают непосредственно пределы для вещественных корней, но часто таким путем получаются слишком широкие пределы для вещественных корней.

Покажем несколько простых приемов, дающих возможность получить на практике для вещественных корней уравнения более близкие между собою пределы.

Будем в уравнении

$$p_0x^n + p_1x^{n-1} + \ldots + p_{n-1}x + p_n = 0$$

предполагать старший коэффициент p_0 числом положительным и коэффициенты числами вещественными. Тогда, если все коэффициенты числа положительные, то уравнение, очевидно, не может иметь положительных корней, ибо при всяком положительном x первая часть будет числом положительным отличным от нуля; следовательно, необходимым условием для того, чтобы уравнение имело положительные корни, будет присутствие в первой части уравнения членов с отрицательными коэффициентами. Пусть первый отрицательный коэффициент, начиная от коэффициента p_0 будет p_{n-m}. Обозначим через p наибольшую из абсолютных величин отрицатсльных коэффициентов; тогда, предполагая x положительным, получим

$$f(x) = p_0x^n + p_1x^{n-1} + \ldots + p_{n-m}x^m + \ldots + p_n \geq p_0x^n - p(x^m + \ldots + 1).$$

Вторая часть неравенства, очевидно, не больше первой, ибо она получается через пропуск всех положительных членов между главным и первым отрицательным и через замену всех остальных членов отрицательными членами с наибольшей абсолютной величиной коэффициентов. Нетрудно указать такое число, что при x большем этого числа вторая часть этого неравенства будет оставаться положительным числом; для этого придется удовлетворить неравенству

$$p_0x^n - p(x^m + x^{m-1} + \ldots + 1) > 0,$$

или

$$p_0x^n - p\,\frac{x^{m+1} - 1}{x - 1} > 0.$$

Будем предполагать $x > 1$, тогда придется решить неравенство

$$p_0x^n(x - 1) - px^{m+1} + p > 0.$$

Достаточно удовлетворить такому новому неравенству

$$p_0x^n(x - 1) - px^{m+1} > 0,$$

или

$$p_0x^{n-m-1}(x - 1) - p > 0.$$

Это же последнее неравенство может быть заменено следующим

$$p_0(x - 1)^{n-m-1}(x - 1) - p > 0, !$$

или

$$p_0(x - 1)^{n-m} - p > 0.$$

Решая, будем иметь

$$(x - 1)^{n-m} > \frac{p}{p_0}$$

или

$$x - 1 > \sqrt[n-m]{\frac{p}{p_0}},$$

откуда

$$x > 1 + \sqrt[n-m]{\frac{p}{p_0}}.$$

Отсюда мы видим, что за *верхний* предел положительных корней может быть принято число

$$1 + \sqrt[n-m]{\frac{p}{p_0}}.$$

Нахождение *низшего* предела положительных корней приведется к преобразованию уравнения при помоши подстановки

$$x = \frac{1}{y}$$

и к нахождение высшего предала положительных корней преобразованного уравнения.

Заменяя в уравнении x на $-x$, мы приведем задачу отыскания пределов отрицательных корней к задаче разыскания пределов положительных корней для нового уравнения.

Таким образом, мы замечаем, что основной задачей при разыскании пределов вещественных корней является задача определения высшего предала положительных корней.

§ 5

Покажем еще один способ решения последней задачи. Пусть первая часть рассматриваемого уравнения состоит из ряда положительных членов, следующих за главным, за которыми следуют члены, все имеющие знак минус. Итак, первая часть заданного уравнения $f(x)$ имеет вид

$$f(x) = \varphi(x) - \psi(x),$$

где $\varphi(x)$ и $\psi(x)$ полиномы с положительными коэффициентами. Пусть m будет низшая степень x в функции $\varphi(x)$; тогда в выражении

$$\frac{f(x)}{x^m} = \frac{\varphi(x)}{x^m} - \frac{\psi(x)}{x^m}$$

часть $\dfrac{\varphi(x)}{x^m}$ заключает члены не отрицательных степеней, а часть $\dfrac{\psi(x)}{x^m}$ заключает члены отрицательных степеней. Мы видим, следовательно, что при возрастании положительных значений x первая часть не убывает, а вторая часть убывает. Следовательно, разность

$$\frac{f(x)}{x^m}$$

возрастает. Если эта разность положительна при каком-нибудь значении a независимого переменного x, то она останется положительною и при $x > a$, т. е. функция $f(x)$ не будет иметь корней больших a, и, следовательно,

всякое положительное число a, при котором первая часть заданного уравнения есть число положительное, может быть принято за высший предел положительных корней.

Отсюда получается способ нахождения высшего предела корней в случае произвольного заданного уравнения. Всегда первая часть уравнения может быть представлена в таком виде:

$$f(x) = \varphi_1(x) - \varphi_2(x) + \varphi_3(x) - \varphi_4(x) + \ldots + \varphi_{2k-1}(x) - \varphi_{2k}(x), \tag{1}$$

где полиномы $\varphi_1, \varphi_2, \varphi_3, \ldots, \varphi_{2k}$ имеют положительные коэффициенты. Достаточно подобрать числа

$$a_1, \quad a_2, \quad a_3, \ \ldots, \ a_k,$$

при которых будут положительными полиномы

$$\varphi_1(x) - \varphi_2(x), \quad \varphi_3(x) - \varphi_4(x), \ \ldots, \ \varphi_{2k-1}(x) - \varphi_{2k}(x).$$

Тогда по предыдущему наибольшее из чисел (1) может быть принято за искомый верхний предел.

§ 6

Пусть требуется определить пределы корней уравнения

$$2x^5 - 92x^2 + 2x - 1 = 0.$$

По общему правилу находим, что верхний предел будет $1 + \dfrac{a}{a_0}$, где a есть наибольший из модулей коэффициентов -92, 2, -1, значит, $a = 92$, а $a_0 = 2$. Отсюда получаем $L = 1 + 46 = 47$.

Применяя соображения § 4, получим для верхнего предела выражение $1 + \sqrt[n-m]{\dfrac{p}{p_0}}$. В данном случае $n = 5$, $m = 2$, $p = 92$, $p_0 = 2$; значит $1 + \sqrt[n-m]{\dfrac{p}{p_0}} = 1 + \sqrt[3]{46} = 1 + 3, \ldots = 4, \ldots$.

Но нетрудно видеть, на основании соображений § 5, что за верхний предел положительных корней можно принять число 4. В самом деле, рассматривая функции $2x^5 - 92x^2$, $2x - 1$, мы замечаем, что вторая функция уже положительна при $x = 1$, первая же функция $2x^2(x^3 - 46)$ положительна при $x = 4$, следовательно, 4 можно принять за верхний предел положительных корней.

Чтобы найти нижний предел положительных корней, заменим x на $\dfrac{1}{y}$; получим $y^5 - 2y^4 + 92y^3 - 2 = 0$. Найдем верхний предел положительных корней этого уравнения; рассматривая две функций $y^5 - 2y^4$ и $92y^3 - 2$, мы замечаем, что первая функция $y^4(y - 2)$ делается положительной после $y = 2$; но при $y = 2$ вторая функция тоже положительна; следовательно, число 2 есть верхний предел преобразованного уравнения, а число $l = \dfrac{1}{2}$ будет нижним пределом положительных корней заданного уравнения.

Для нахождения пределов отрицательных корней заменим x на $-x$; получим уравнение $2x^5 + 92x^2 + 2x + 1 = 0$. Последнее уравнение имеет все положительные

коэффициенты, следовательно, оно не имеет положительных корней; потому и заданное уравнение не имеет отрицательных корней.

Способ Newton'a определения высшего предела корней

§ 7

Способ Newton'a определения верхнего предала положительных корней основывается на следующей теореме.

Если при некотором значении a независимого переменного x все функции

$$f(x), \quad f'(x), \quad f''(x), \ \ldots, \ f^{(n)}(x) = 1 \cdot 2 \cdot 3 \cdots n \cdot p_n$$

принимают положительные численные значения, то число a может считаться верхним пределом положительных корней уравнения $f(x) = 0$.

Доказательство этого предложения основывается на рассмотрении формулы Taylor'a

$$f(a+h) = f(a) + hf'(a) + \frac{h^2}{1 \cdot 2} f''(a) + \ldots + \frac{h^n}{n!} f^{(n)}(a).$$

Если все числа

$$f(a), \quad f'(a), \quad f''(a), \ \ldots, \ f^{(n)}(a)$$

положительны, то при произвольном положительном числе h будет положительным также и выражение

$$f(a+h).$$

Другими словами, число $a+h$ не может быть корнем» уравнения $f(x) = 0$.

Нетрудно убедиться также, что при произвольном h будут положительными также числа

$$f'(a+h), \quad f''(a+h), \ \ldots, \ f^{(n-1)}(a+h).$$

Доказательство этого последнего свойства может быть основано на разложении $f^{(k)}(a+h)$ по формуле Taylor'a. В самом деле, имеем

$$f^{(k)}(a+h) = f^{(k)}(a) + \frac{h}{1} f^{(k+1)}(a) + \frac{h^2}{1 \cdot 2} f^{(k+2)}(a) + \\ + \ldots + \frac{h^{n-k}}{(n-k)!} f^{(n)}(a),$$

а числа

$$f^{(k)}(a), \quad f^{(k+1)}(a), \ \ldots, \ f^{(n)}(a)$$

по сделанному выше предположению положительны.

Из этой теоремы получается такой прием вычисления верхнего предала положительных корней. Последняя производная n-го порядка есть число положительное и притом постоянное. Предыдущая производная $f^{(n-1)}(x)$ есть функция первой степени с положительным коэффициентом при x. Увеличивая достаточно x, остановимся на каком-нибудь значений a_1 переменной x, при котором рассматриваемая производная положительна. Подставляем это число a_1 в предыдущую производною $f^{(n-2)}(x)$. Если результат подстановки будет положительный,

то останавливаемся на числе a_1; если же результат подстановки отрицательный, то продолжаешь увеличивать численное значение x, пока вторая производная не сделается положительною. Приходим таким путем к числу a_2, при котором с одной стороны производная $f^{(n-2)}(x)$ число положительное, а, с другой стороны, останется также положительною и производная $f^{(n-1)}(x)$, ибо число a_2 не меньше числа a_1. Подставляешь число a_2 в следующую производную $f^{(n-3)}(x)$ или увеличиваем его до тех пор, пока эта производная не сделается положительною. Такой процесс подстановки чисел возрастающих во все производные и заданную функцию приведет наверно к нахождению такого числа, при котором все функции $f(x), f'(x), f''(x), \ldots, f^{(n)}(x)$ сделаются положительными, и, следовательно, это число может считаться за верхний предел положительных корней уравнения $f(x) = 0$.

Алгоритм Horner'a

§ 8

Нахождение верхнего предала положительных корней по способу Newton'a требует вычисления значений, принимаемых функциями

$$f(x), \quad f'(x), \ \ldots, \ f^{(n)}(x)$$

при $x = a$. Вычисление этих результатов может быть просто выполнено, пользуясь схемой вычислений, носящей название *алгоритма* Horner'a.

Будем делить функцию

$$f(x) = p_0x^n + p_1x^{n-1} + \ldots + p_{n-1}x + p_n = 0$$

на $x - a$ и обозначим частное через

$$\varphi_1(x) = q_0x^{n-1} + q_1x^{n-2} + \ldots + q_{n-1},$$

где

$$\begin{aligned} q_0 &= p_0, \\ q_1 &= aq_0 + p_1, \\ q_2 &= aq_1 + p_2, \\ &\ldots\ldots\ldots\ldots, \\ q_{n-1} &= aq_{n-2} + p_{n-1}, \end{aligned}$$

остаток же равняется

$$q_n = aq_{n-1} + p_n.$$

Последовательное вычисление коэффициентов q_i и остатка q_n может быт расположено следующим образом. Составляем таблицу

$$\left|\begin{array}{c|c|c|c|c|c} p_0 & p_1 & p_2 & \ldots & p_{n-1} & p_n \\ p_0 & q_1 & q_2 & \ldots & q_{n-1} & q_n \\ p_0 & r_1 & r_2 & \ldots & r_{n-1} & \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \end{array}\right|,$$

у которой в первом ряду расположены все коэффициенты заданной функции в порядке убывающих степеней, причем некоторые из этих чисел могут быть нулями; во втором ряду таблицы под первым числом p_0 ставим то же самое число p_0. Затем для получения второго члена этого ряда умножаем первый член второго ряда на a и складываем со вторым членом первого ряда; для получения третьего члена умножаем предыдущий член, т. е. q_1, и прибавляем третий член p_2 первого ряда, и т. д. продолжаем эту операцию до последнего члена q_n. Остаток q_n от деления $f(x)$ на $x-a$ и будет как раз равняться $f(a)$.

На основании сказанного нетрудно получить путем подобных же выкладок значения производных $f'(x), f''(x), \ldots$ рассматриваемой функции. В самом деле, на оснований формулы Taylor'a

$$f(x) = f(a) + (x-a)f'(a) + \ldots + \frac{(x-a)^n}{n!}f^{(n)}(a),$$

замечаем, что частное $\varphi_1(x)$ от деления $f(x)$ на $x-a$ будет

$$\varphi_1(x) = f'(a) + \frac{x-a}{1\cdot 2}f''(a) + \ldots + \frac{(x-a)^{n-1}}{n!}f^{(n)}(a);$$

а отсюда мы замечаем, что $f'(a)$ можно рассматривать как остаток от деления частного $\varphi_1(x)$ на разность $x-a$. Новое частное $\varphi_2(x)$ от этого последнего деления будет

$$\varphi_2(x) = \frac{1}{1\cdot 2}f''(a) + \frac{x-a}{3!}f'''(a) + \ldots$$

Мы видим, следовательно, что остаток от деления второго частного $\varphi_2(x)$ на $x-a$ будет $\dfrac{1}{1\cdot 2}f''(a)$.

Продолжая последовательное деление полученных частных, мы будем получать остатки

$$\frac{1}{3!}f'''(a), \quad \frac{1}{4!}f^{94)}(a), \quad \frac{1}{(n-1)!}f^{(n-1)}(a),$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

Очевидно, что, вписывая в нашу таблицу на предыдущей странице третий ряд чисел $p_0, r_1, r_2, \ldots, r_{n-1}$, которые также получаются по числам второго ряда, как числа второго мы получили но числам первого ряда, то значение $f'(a)$, которое принимает производная $f'(x)$ при $x=a$, будет равно r_{n-1}. Продолжая вписывать в таблицу дальнейшие ряды чисел, будем получать значения производных:

$$\frac{1}{2!}f''(a), \quad \frac{1}{3!}f'''(a), \text{ и т.д.}$$

Пусть дана функция

$$f(x) = x^5 + 2x^4 - 13x^3 - x^2 - 25x + 100,$$

причем принимается $a=-5$. Составим таблицу Horner'a

1	2	−13	−1	−25	100
1	−3	2	−11	30	−50
1	−8	42	−221	1135	
1	−13	107	−756		
1	−18	197			
1	−23				

Из этой таблицы мы видим, что после разделения на $x+5$ получается частное $x^4-3x^3+2x^2-11x+30$ и остаток -50. Кроме того получается

$$f(-5)=-50,\quad f'(-5)=1135,\quad \frac{1}{2}f''(-5)=-756,\quad \frac{1}{6}f'''(-5)=197,$$

$$\frac{1}{24}f^{(4)}(-5)=-23.$$

Об отделении корней

§ 9

Обращаясь к задаче отделении вещественных корней, мы замечаем, что она может быть формулирована следующим образом.

Требуется между пределами l и L вещественных корней вставить ряд $m-1$ возрастающих вещественных чисел

$$l_1,\ \ l_2,\ \ l_3,\ \ldots,\ l_{m-1}$$

таким образом, чтобы в каждом из промежутков между числами

$$l,\ \ l_1,\ \ l_2,\ \ldots,\ l_{m-1},\ \ L$$

существовало не более одного вещественного корня заданного уравнения.

В настоящее время задача отделения корней может быть рассматриваема как в значительной мере устаревшая, ибо существу приемы приближенного вычисления корней, не требуют предварительного их отделения.

Посвящая, однако, целую главу отделению корней, я имел главным образом в виду не самую задачу отделения корней, а различные методы и приемы рассуждения, замечательные по их оригинальности, а также ряд результатов, хотя и стоящих до некоторой степени отдельно друг от друга, но сыгравших известную роль в истории науки.

Теорема. *Если значения $f(a)$ и $f(b)$ разных знаков, то функция $f(x)$ имеет нечетное число корней между a и b. Если же знаки чисел $f(a)$ и $f(b)$ одинаковы, то между числами a и b или не существует корней или число их четное.*

Для всякой пары сопряженных комплексных корней $\lambda+i\mu$ и $\lambda-i\mu$ функция $f(x)$ будет заключать произведение двух линейных множителей $(x-\lambda-i\mu)(x-\lambda+i\mu)=(x-\lambda)^2+\mu^2$, которое имеет положительное значение при всех вещественных значениях x. Выделяя в одну целую функцию $F(x)$ все множители, соответствующие мнимым корням функции $f(x)$, и обозначая через

$$\alpha_1,\ \ \alpha_2,\ \ldots,\ \alpha_k$$

вещественные корни функции $f(x)$, получим

$$f(x)=F(x)(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_k). \tag{1}$$

Функция $F(x)$ будет сохранять знак плюс при всех вещественных значениях x, если только мы предположим положительным коэффициент при высшей степени x в функции $f(x)$.

Подставляя в равенство (1) числа a и b, получим

$$f(a) = F(a)(a-\alpha_1)(a-\alpha_2)\cdots(a-\alpha_k),$$

$$f(b) = F(b)(b-\alpha_1)(b-\alpha_2)\cdots(b-\alpha_k),$$

откуда, разделяя, получаем

$$\frac{f(a)}{f(b)} = \frac{F(a)}{F(b)}\cdot\frac{a-\alpha_1}{b-\alpha_1}\cdot\frac{a-\alpha_2}{b-\alpha_2}\cdots\frac{a-\alpha_k}{b-\alpha_k}.$$

Дробь $\dfrac{F(a)}{F(b)}$ есть число положительное. Рассмотрим дробь

$$\frac{a-\alpha_i}{b-\alpha_i},$$

где i одно из чисел $1, 2, 3, \ldots, k$. Нетрудно видеть, что эта дробь положительна, если корень α_i лежит вне промежутка между числами a и b, и отрицательна, если этот корень лежит внутри указанного промежутка.

Итак, мы видим, что дробь $\dfrac{a}{b}$ будет положительною, если во второй части или не будет отрицательных дробей, или же число их будет четное, и та же дробь будет отрицательна в случай нахождения нечетного числа корней внутри промежутка (a, b), что и доказывает справедливость теоремы.

Теорема. *Если x, возрастая переходит через корень α функции $f(x)$, то выражение $\dfrac{f(x)}{f'(x)}$ переходит через нуль всегда от отрицательных значений к положительными.*

Пусть α будет k-кратный корень функции $f(x)$, т. е.

$$f(\alpha) = 0, \quad f'(\alpha) = 0, \ldots, \ f^{(k-1)}(\alpha) = 0,$$

тогда по формуле Taylor'a получим

$$f(\alpha+h) = \frac{h^k}{k!}f^{(k)}(\alpha) + h^{k+1}A, \tag{2}$$

где A целая функция от h. Применяя формулу Taylor'a к производной $f'(x)$, получим

$$f'(\alpha+h) = \frac{h^{k-1}}{(k-1)!}f^{(k)}(\alpha) + h^k B, \tag{3}$$

где B целая функция от h. Отсюда

$$\frac{f(\alpha+h)}{f'(\alpha+h)} = h\cdot\frac{\dfrac{1}{k!}f^{(k)}(\alpha) + hA}{\dfrac{1}{(k-1)!}f^{(k)}(\alpha) + hB}; \tag{4}$$

второй из множителей, стоящих в правой части формулы (4), стремится при приближении h к нулю к пределу

$$\frac{\frac{1}{k!}f^{(k)}(\alpha)}{\frac{1}{(k-1)!f^{(k)}(\alpha)}},$$

т. е. к пределу

$$\frac{1}{k}.$$

Мы видим, следовательно, что при достаточно малых по абсолютной величине значениях приращения h дробь, стоящая в правой части равенства (4), представляет положительное число (ибо ее предел положительное число). Итак, мы видим, что знак выражения

$$\frac{f(\alpha+h)}{f'(\alpha+h)} \tag{5}$$

совпадает со знаком h при достаточно малых абсолютных значениях h. Итак, в результате мы видим, что, если h переходить через нуль от отрицательных значений к положительным, то и выражение (5) переходит через нуль от отрицательных значений к положительным, что и требовалось доказать.

Задача отделения корней будет просто решена, если в ряде

$$l,\ \ l_1,\ \ l_2,\ \ldots,\ l_{m-1},\ \ L \tag{6}$$

будет $m = n$ и после подстановки двух последовательных чисел ряда (6) в функций $f(x)$, стоящую в первой части рассматриваемого уравнения, получаются результаты разные по знаку. В самом деле, в этом случае в каждом из n промежутков (n есть степень функции $f(x)$ должно существовать не менее одного корня функций $f(x)$, а так как число корней не может быть больше n, то в каждом из промежутков ? будет заключаться только один корень, и, следовательно, корни функции $f(x)$ будут отделены числами ряда (6).

Способ Waring'a и Lagrange'a

§ 10

Waring и Lagrange указали общий способ нахождения ряда чисел

$$l_1,\ \ l_2,\ \ l_3,\ \ldots,\ l_{m-1}, \tag{1}$$

производящего отделение корней, — способ, неоставляющий желать ничего лучшего с теоретической точки зрения.

Будем ряд (1) предполагать арифметическою прогрессией, крайними членами которой пусть будут пределы l и L корней. Обозначая разность прогрессии через h, получим ряд (1) в виде такой прогрессии

$$l,\ \ l+h,\ \ l+2h,\ldots,\ l+(m-1)h,\ \ L. \tag{2}$$

Остается подобрать положительную разность h столь малою, чтобы в каждом из промежутков не могло заключаться более одного корня рассматриваемой функции $f(x)$.

Для этой цели составим, так называемое, *уравнение в квадратах разностей корней* заданного уравнения, т. е. такое уравнение, корнями которого будут квадраты всевозможных разностей корней заданного уравнения

$$(\alpha-\beta)^2,\quad (\alpha-\gamma)^2,\quad (\beta-\gamma)^2,\ \ldots$$

Число корней нового уравнения будет, очевидно,

$$\mu=\frac{n(n-1)}{2}$$

по числу сочетаний из n корней по два.

Предполагая заданное уравнение в виде

$$x^n+p_1x^{n-1}+\ldots+p_{n-1}x+p_n=0,$$

а уравнение в квадратах разностей в виде

$$x^\mu+P_1x^{\mu-1}+\ldots+P_{\mu-1}x+P_\mu=0,$$

мы замечаем, что коэффициенты

$$P_1,\quad P_2,\ \ldots,\ P_{\mu-1},\quad P_\mu,$$

как симметрические функции от корней $\alpha,\beta,\gamma,\ldots$, будут выражаться полиномами относительно коэффициентов

$$p_1,\quad p_2,\ \ldots,\ p_n,$$

причем эти полиномы будут с целыми коэффициентами.

Так, например, первый коэффициент P_1 вычисляется так

$$P_1=\sum(\alpha-\beta)^2.$$

Раскрывая эту сумму, мы замечаем, что в нее войдут удвоенные произведения всевозможных сочетаний корней с знаками минус и сумма квадратов корней, причем квадрат каждого корня повторяется столько раз, сколько остальных корней, т. е. $(n-1)$ раз, и мы получаем

$$P_1=(n-1)\sum\alpha^2+2\sum\alpha\beta.$$

Но $\sum\alpha\beta=p_2$, а по формулам Newton'a (см. стр. 238)

$$\sum\alpha^2=p_1^2-2p_2,$$

следовательно, мы получаем

$$P_1=-(n-1)(p_1^2-2p_2)+2p_2=2np_2-(n-1)p_1^2.$$

Следующие коэффициенты $P_2, P_3, \ldots$ вычисляются уже сложнее: Lagrange указал хороший прием вычисления всех остальных коэффициентов; последний коэффициент P_μ есть не что иное, как дискриминант уравнения, вычисление которого было уже показано на стр. 258.

Метода Waring'a и Lagrange 'a состоит в составлении уравнения в квадратах разностей и в нахождении нижнего предала λ его положительных корней. Нетрудно убедиться, что, если мы возьмем за разность прогрессии $\sqrt{\lambda}$, то в каждом из промежутков между числами (2) не может существовать больше одного, корня уравнения, ибо абсолютная величина разности $\alpha-\beta$ любых двух корней заданного уравнения больше $\sqrt{\lambda}$ (по определению λ, существует для любого α и β неравенство $\lambda < (\alpha-\beta)^2$, а для вещественных корней α и β корень $(\alpha-\beta)^2$ уравнения в квадратах разностей положителен).

Упрощение Cauchy

§ 11

Практическое неудобство способа Waring'a и Lagrange'a состоит в сложности вычислений коэффициентов уравнения в квадратах разностей и еще в том, что в случае малости числа $\sqrt{\lambda}$, число промежутков, подлежащих исследованию оказывается очень значительным. Эти практические недостатки не были устранены и замечательной методой, предложенной Lagrange'ем, для вычисления коэффициентов уравнения в квадратах разностей.

Cauchy упростил задачу, показав, что для нахождения положительного числа, меньшого абсолютной величины разности любых двух вещественных корней заданного уравнения нет надобности составлять все уравнение в квадратах разностей, а достаточно составить только последний коэффициент, т. е. дискриминант.

Обозначая через G^2 модуль этого коэффициента, получим

$$G^2 = |(\alpha-\beta)^2(\alpha-\gamma)^2(\beta-\gamma)^2\cdots|.$$

Введем в рассмотрение верхний предел ρ модулей корней заданного уравнения. Тогда для каждой нары корней получим неравенство

$$|(\beta-\gamma)^2| < (2\rho)^2. \tag{1}$$

Рассматривая определенную пару α и β вещественных корней заданного уравнения и применяя ко всем остальным парам неравенство (1), получим неравенство

$$G^2 < (\alpha-\beta)^2(2\rho)^{n(n-1)-2},$$

ибо число всех разностей между корнями, за исключением разности $\alpha-\beta$, равно

$$\frac{n(n-1)}{2} - 1.$$

Итак, для всякой разности между двумя вещественными корнями получается неравенство

$$(\alpha-\beta)^2 > \frac{G^2}{(2\rho)^{n(n-1)-2}}.$$

Отсюда мы видим, что достаточно взять разность прогрессии h равною или меньшею числа

$$\frac{G}{(2\rho)^{\frac{n(n-1)-2}{2}}}.$$

Особенно просто рассматривается случай, когда коэффициенты

$$p_1, \quad p_2, \ldots, \ p_n$$

числа целые; тогда коэффициенты $P_1, P_2, \ldots, P_\mu$ будут также числа целые, и, следовательно, G^2 будет целое число, т. е. оно будет не меньше единицы; и потому в этом случай можно брать разность прогрессии h непревосходящею числа

$$\frac{1}{(2\rho)^{\frac{n(n-1)}{2}-1}}.$$

В этом случай, очевидно, нет надобности вычислять коэффициент P_μ уравнения в квадратах разностей.

Несмотря однако на упрощение Cauchy, практическое приложение этого способа представляет большие неудобства. Математики после Lagrange'а пытались избежать рассмотрения уравнения в квадратах разностей, но до открытая Budan'ом весьма важной теоремы не было получено удобных в практическом отношений результатов.

Теорема Budan'a

§ 12

В 1811 году была сообщена парижской Академии Наук Budan'ом теорема, весьма важная по приложениям к задаче об отделении корней.

Будем рассматривать ряд функций

$$f(x), \quad f'(x), \ \ldots, \ f^{(n)}(x), \tag{1}$$

где n степень функции $f(x)$. Подставим в ряд (1) вместо x некоторое вещественное число a. Напишем ряд знаков (плюс или минус) численных значений функции ряда (1), который будем называть рядом Budan'a

$$+ \ + \ - \ + \ - \ \ldots \tag{2}$$

Будем говорить, что переход от одного знака ряда (2) к следующему представляет *постоянство* знака, если оба знака одинаковы, и *перемену* знака, если эти знаки различны. Число перемен знака в ряду (2) будем называть *числом перемен знака* ряда Budan'a, соответствующим числу a. Так например, ряд

$$+ \ - \ - \ + \ + \ -$$

имеет три перемены знака, а именно, при переход от первого знака ко второму, от третьего к четвертому и от пятого к шестому.

Теорема Budan'a. *При переходе от вещественного числа a к большему числу ряд Budan'a для функции $f(x)$ теряет такое число перемен знака, которое или*

равно числу вещественных корней $f(x)$ в промежутка (α, β), или больше этого числа на четное число.

Изменение числа перемен знака в ряде Budan'a может происходить только при переходе через корень которой-нибудь из функций ряда. Предположим, что мы непрерывно увеличиваем переменную x от α до β и при таком увеличений переходим через корень γ которой-нибудь из функций ряда, например, $f^{(\mu)}(x)$. Если этот корень γ кратный корень функции $f^{(\mu)}(x)$, то следующие функции ряда должны также его иметь своим корнем; но, так как последняя, функция ряда Budan'a есть постоянное число отличное от нуля, то корень γ не может обратить в нуль все функций, следующие за рассматриваемой. Пусть будет $f^{(\mu+k)}(x)$ первая функция, следующая за рассматриваемой, не обращающаяся в нуль при $x = \gamma$. Таким образом, мы имеем

$$f^{(\mu)}(\gamma) = 0, \ \ldots, \ f^{(\mu+k-1)}(\gamma) = 0, \quad f^{(\mu+k)}(\gamma) \gtrless 0.$$

Рассмотрим два случая.

1-й случай. $f^{(\mu)}(x)$ есть первая функция $f(x)$ ряда Budan'a, т. е. $\mu = 0$, и мы имеем

$$f(\gamma) = 0, \quad f'(\gamma) = 0, \ \ldots, \ f^{(k-1)}(\gamma) = 0, \quad f^{(\mu)}(\gamma) \gtrless 0.$$

Число γ есть k-кратный корень рассматриваемой функции $f(x)$. Чтобы рассмотреть изменения в переменах знака ряда, рассмотрим сначала значения x, меньшие γ и достаточно близкие к этому числу, а потом значения x, большие γ и достаточно близкие к нему. По теореме стр. 289 мы замечаем, что выражение

$$\frac{f^{(\lambda)}(x)}{f^{(\lambda+1)}(x)}$$

где λ одно из чисел $0, 1, 2, \ldots, k-1$, переходит от отрицательных значений к положительным при переходе x от значений меньших γ к значениям большим γ. Таким образом, мы видим, что часть ряда Budan'a

$$f(x), \quad f'(x), \ \ldots, \ f^{(k)}(x)$$

при значениях x, близких к γ и меньших этого числа, представляет одни перемены знака, при значениях же больших γ — одни постоянства знака. Следовательно, при переход через корень γ рассматриваемая часть ряда Budan'a теряет k перемен знака; другими словами, эта часть теряет такое число перемен знака, какова кратность корня γ.

2-й случай. Предположим теперь, что μ отлично от нуля. Рассмотрим часть ряда Budan'a, образованную функциями

$$f^{(\mu-1)}(x), \quad f^{(\mu)}(x), \ \ldots, \ f^{(\mu+k)}(x), \tag{3}$$

причем

$$f^{(\mu-1)}(\gamma) \gtrless 0, \quad f^{(\mu)}(\gamma) = 0, \ \ldots, \ f^{(\mu+k-1)}(\gamma) = 0, \quad f^{(\mu+k)}(\gamma) \gtrless 0.$$

Покажем, что ряд (3) теряет всегда четное число перемен знака. Это число может быть равным нулю. В самом деле, ряд функций

$$f^{(\mu-1)}(x), \ldots, \ f^{(\mu+k)}(x)$$

теряет при переходе x через γ равно k перемен знака, как мы это видели выше. Рассматривая две первые функции

$$f^{(\mu-1)}(x), \quad f^{(\mu)}(x)$$

ряда (3), мы замечаем, что при k четном в этих двух функциях не происходить ни потери, ни приобретения перемен знака: при нечетном же k в этих функциях имеет место или потеря, или приобретение перемен знака. В самом деле, если k четное, то γ есть корень четной кратности функции $f^{(\mu)}(x)$, и, следовательно, эта функция не меняет своего знака при переходе через γ; точно также не меняет своего знака и функция $f^{(\mu-1)}(x)$, ибо она не обращается в нуль при $x = \gamma$. С другой стороны, если k число нечетное, то γ корень нечетной кратности, и, следовательно, при переходе через него функция $f^{(\mu)}(x)$ меняет свой знак; функция же $f^{(\mu-1)}(x)$ знака не меняет, и, следовательно, при переходе через γ в первых двух функциях ряда (3) происходит или потеря, или приобретение перемены знака, так что общее число потерянных перемен знака в ряде (3) при переходе через x будет γ, т. е. число четное.

Итак, мы видим, что теорема Budan'a вполне доказана, ибо общее число перемен знака ряда Budan'a уменьшится при переходе через каждый корень основной функций $f(x)$ на число, равное кратности этого корня; а общее уменьшение числа перемен знака при изменении x в пределах промежутка будет равно числу корней основной функций в данном промежутка плюс число потерь перемен знака, происходящих при переходе через корни промежуточных функций ряда Budan'a, а это последнее число, как мы видели, всегда четное.

Следствие теоремы Budan'a

§ 13

Из теоремы Budan'a легко вывести следующее важное следствие:

Если число вещественных корней функций $f(x)$ в промежутке (α, β) равняется m, а число потерь перемен знака в ряде

$$f(x), \quad f'(x), \ \ldots, \ f^{(n)}(x)$$

равно $m + 2k$, то уравнение $f(x) = 0$ имеет по крайней мере $2k$ мнимых корней.

Рассмотрим три промежутка

$$(-\infty, \alpha), \quad (\alpha, \beta), \quad (\beta, +\infty).$$

Пусть число вещественных корней в этих промежутках будет

$$m' \quad m \quad m_1,$$

а пусть число потерь перемен знака в этих промежутках будет

$$m' + 2k' \quad m + 2k \quad m_1 + 2k_1.$$

Тогда число потерь перемен знака во всем промежутка $(-\infty, +\infty)$ будет равняться сумме

$$m' + m + m_1 + 2(k' + k + k_1);$$

но нетрудно видеть, что при $x = -\infty$ ряд Budan'a представляет одни перемены знака, число которых, очевидно, будет n, а при $x = +\infty$ знаки всех функций Budan'a одинаковы, и, значит, в промежутке $(-\infty, +\infty)$ происходить n потерь перемен знака. Отсюда мы заключаем, что

$$n = m' + m + m_1 + 2(k' + k + k_1). \tag{1}$$

Обозначим через $2y$ число мнимых корней функций $f(x)$. Так как число вещественных корней заданной функций есть $m' + m + m_1$, то мы получаем равенство

$$n = m' + m + m_1 + 2y. \tag{2}$$

Сравнивая (2) с (1), получим

$$y = k' + k + k_1.$$

Но, так как k' и k_1 не отрицательные числа, то получаем и неравенство

$$y \geq k,$$

т. е. число мнимых корней не меньше $2k$.

Правило знаков Descartes'a

§ 14

Как следствие теоремы Budan'a получается весьма важная в практическом отношении теорема, указанная еще Descartes'ом.

Теорема. *Число положительных корней функции $f(x)$ не превосходит числа перемен знака в ряде коэффициентов функции $f(x)$ и, если оно меньше, то на число четное.*

Применяя формулу Maclaurin'a мы можем написать

$$f(x) = f(0) + xf'(0) + \frac{x^2}{1 \cdot 2} f''(0) + \ldots + \frac{x^n}{n!} f^{(n)}(0).$$

Отсюда мы видим, что знаки коэффициентов функций $f(x)$ не отличаются от знаков ряда

$$f(0), \quad f'(0), \ \ldots, \ f^{(n)}(0). \tag{1}$$

Итак, число перемен знака в коэффициентах функции $f(x)$ равно числу перемен знака в ряде Budan'a для этой функции при $x = 0$. По теореме Budan'a число положительных корней функции $f(x)$ может отличаться на четное число от числа потерь перемен знака в ряде $f(x), f'(x), \ldots, f^{(n)}(x)$ при переходе x от 0 до $+\infty$; но при $x = +\infty$ этот ряд представляет одни повторения знака, следовательно, число положительных корней функции $f(x)$ будет отличаться на четное число от числа перемен знака в ряде

$$f(0), \quad f'(0), \ \ldots, \ f^{(n)}(0). \tag{2}$$

Таким образом справедливость теоремы Descartes'a доказана ибо знаки ряда (2) совпадают, со знаками коэффициентов функции $f(x)$.

Из теоремы Deskartes'a вытекают некоторый весьма важные следствия.

Следствие I. *Число отрицательным корней функций $f(x)$ на четное число или нуль меньше числа перемен знака в функции $f(-x)$.*

Следствие II. *Если все корни функции $f(x) = 0$ вещественны, то число положительных корней точно равно числу перемен знака в функции $f(x)$, а число отрицательных корней равно числу перемен знака в функции $f(-x)$.*

Для доказательства рассмотрим разности между степенями каждых двух последовательных членов полинома $f(x)$ расположенного по убывающим степеням.

Пусть будет μ таких случаев, где разность степеней *нечетная*, причем эти разности пусть будут

$$2k_1 + 1, \quad 2k_2 + 1, \ \ldots, \ 2k_\mu + 1.$$

Кроме того пусть будет ν пар членов *разных знаков*, разности степеней которых пусть будут числа *четные*

$$2h_1 + 2, \quad 2h_2 + 2, \ \ldots, \ 2h_\nu + 2;$$

и, наконец, пусть будет ρ пар членов одинакового знака, разности степеней которых пусть будут *четные* числа

$$2g_1, \quad 2g_2, \ \ldots, \ 2g_\rho.$$

Рассмотрим, какое число членов будет в заданном уравнении. Так как число пар первой категории есть μ, второй ν и третьей ρ, то общее число членов будет, очевидно, на единицу более суммы числа пар, т. е. будет $\mu+\nu+\rho+1$. Рассмотрим, какое число членов не будет входит в уравнение. Мы замечаем, что каждая пара членов, разность степеней которой есть k, будет соответствовать пропуску $k-1$ членов, и, следовательно, общее число пропущенных членов будет

$$2k_1 + 2k_2 + \ldots + 2k_\mu + (2h_1 + 1) + (2h_2 + 1) + \ldots + (2h_\nu + 1) +$$

$$+(2g_1 - 1) + (2g_2 - 1) + \ldots + (2g_\rho - 1) = 2s + \nu - \rho,$$

где

$$s = k_1 + k_2 + \ldots + k_\mu + h_1 + \ldots + h_\nu + g_1 + \ldots + g_\rho.$$

Итак, складывая число $\mu + \nu + \rho + 1$ членов, входящих в состав уравнения и $2s + \nu - \rho$, число пропущенных членов, мы должны получить общее число членов $n + 1$ уравнения n-ой степени, т. е.

$$2s + \mu + 2\nu + 1 = n + 1,$$

откуда

$$n = 2s + \mu + 2\nu.$$

Будем рассматривать перемены знака в полиноме $f(x)$ и обозначим их число через V, а через V' число перемен в полиноме $f(-x)$. Тогда нетрудно показать, чему равно $V + V'$. В самом деле, пары членов одного знака с четною разностью степеней не дают перемен знака, ни в составе V, ни в составе V'. Каждая пара с

нечетною разностью степеней, если давала повторение знака при x, будет давать перемену знака при $-x$, и обратно. Следовательно, такой паре будет соответствовать одна перемена знака, входящая или в V, или в V'. Число перемен знака в сумме $V+V'$, введенных такими парами, будет, очевидно, μ, и, наконец, пара членов разных знаков с четною разностью будет давать перемены, как при x, так и при $-x$, и, следовательно, каждая такая пара введет в сумму $V+V'$ две единицы. Таким образом будет

$$V + V' = \mu + 2\nu.$$

Итак, мы получаем

$$n = 2s + V + V'. \tag{2}$$

Обозначим теперь через P число положительных корней заданного уравнения, через P' число отрицательных корней, а через $2y$ число мнимых корней. Тогда общее число корней будет равняться степени n, т. е.

$$n = P + P' + 2y. \tag{3}$$

Сравнивая выражения (2) и (3), получаем

$$2y + P + P' = 2s + V + V',$$

или

$$2y = (V - P) + (V' - P') + 2s. \tag{4}$$

Если мнимых корней в уравнении не существует, то получаем равенство

$$0 = (V - P) + (V' - P') + 2s. \tag{5}$$

Числа $V-P$ и $V'-P'$ не отрицательны, ибо на основании теоремы Descartes'a число положительных корней P не превосходить числа перемен знака V в полиноме $f(x)$, а число отрицательных корней P' не превосходит числа перемен знака V' в полиноме $f(-x)$; число же s не отрицательно, ибо оно равно сумме чисел

$$h_1 + \ldots + k_1 + \ldots + g_1 + \ldots,$$

которые или нули, или числа положительные. Следовательно, равенство (5) может быть удовлетворено только положением

$$P = V, \qquad P' = V', \qquad s = 0,$$

что и доказываешь справедливость нашего следствия.

Следствие III. *Если все корни функций вещественны, то число корней, заключенных между α и β, где $\beta > \alpha$, точно равно числу потерь перемен знака в ряде функций Budan'a*

$$f(x), \quad f'(x), \ \ldots, \ f^{(n)}(x) \tag{6}$$

при переходе от α к β.

В самом деле, число корней уравнения $f(x) = 0$ больше α будет равняться числу положительных корней уравнения $f(x'+\alpha) = 0$, где x' новая переменная; но по второму следствию теоремы Descartos'a число положительных корней уравнения $f(x'+\alpha) = 0$ будет равно числу перемен знака в коэффициентах этого уравнения, а раскрытие по формуле Taylor'a убеждает нас, что эти коэффициенты отличаются только положительными численными множителями от величин

$$f(\alpha), \quad f'(\alpha), \quad f''(\alpha), \ \ldots, \ f^{(n)}(\alpha),$$

следовательно, число положительных корней у $f(x'+\alpha)$ будет равно числу перемен знака в ряде (1) при $x = \alpha$.

Точно таким же образом число корней функции $f(x)$ больших β будет равно числу перемен знака в ряде (6) при $x = \beta$. Отсюда, очевидно, и следует, что число корней, заключающихся между α и β, равно числу потерь перемен знака при переходе от α к β.

Простые признаки существования мнимых корней

§ 15

Из равенства

$$2y = (V - P) + (V' - P') + 2s \tag{1}$$

предыдущего параграфа можно вывести весьма важное следствие относительно нижнего предела числа мнимых корней уравнения.

В самом деле, замечая, что числа $V - P$ и $V' - P'$ не отрицательны, получаем из равенства (1)

$$y \geq s.$$

Отсюда видим, что, если по крайней мере одно из чисел $k_1, k_2, \ldots, h_1, h_2, \ldots, g_1, g_2, \ldots$ отлично от нуля, то s число положительное, и, следовательно, уравнение наверно имеет мнимые корни.

Мы получаем такое предложение.

Если в уравнении имеется пропуск одного члена между членами одного знака, или же пропуск числа членов более одного, то уравнение имеет наверно мнимые корни.

Например, следующие уравнения

$$x^7 + 3x^5 - 4x^4 + x^3 - 2x^2 - x - 1 = 0,$$
$$x^7 + x^3 - x + 1 = 0,$$
$$x^5 - 4x^4 - 5x^2 + 1 = 0,$$
$$x^5 - x^2 + 1 = 0$$

имеют мнимые корни.

Hermite в бытность его учеником в лицее Louis le Grand 1842, указал на такую теорему: *если четыре последовательных коэффициента уравнения $f(x) = 0$ представляют арифметическую прогрессию, то это уравнение имеет непременно мнимые корни.* Для доказательства достаточно заметить, что произведение $f(x)(x^2 - 2x + 1)$ будет иметь пропуск двух членов.

Теорема Rolle'a

§ 16

Теорема. *Между двумя последовательными корнями целой функции лежит по крайней мере один корень ее производной.*

Рассмотрим два последовательных корня a и b функций $f(x)$, причем $b > a$. Предполагая h достаточно малым положительным числом, мы убеждаемся в справедливости двух неравенств

$$\frac{f(a+h)}{f'(a+h)} > 0, \qquad \frac{f(b-h)}{f'(b-h)} < 0. \tag{1}$$

Так как a и b суть два последовательных корня заданной функции, то между числами $a+h$ и $b-h$ не существуешь корней функции $f(x)$, и, следовательно, два результата

$$f(a+h) \quad \text{и} \quad f(b-h)$$

должны иметь один и тот же знак. Но тогда на основании неравенств (1) выражения

$$f'(a+h) \quad \text{и} \quad f'(b-h)$$

должны быть разных знаков, и, следовательно, производная $f'(x)$ должна иметь нечетное число корней в промежутке между числами

$$a+h \quad \text{и} \quad b-h,$$

что и требовалось доказать.

Интерполяционная формула Lagrange'a

§ 17

Поставим себе задачею определить целую функций $f(x)$ степени n, обращающуюся при $n+1$ частных значениях

$$a_0, \quad a_1, \quad a_2, \ \ldots, \ a_n$$

независимого переменного x в наперед заданные численные значения

$$f(a_0), \quad f(a_1), \quad f(a_2), \ \ldots, \ f(a_n).$$

Так как число коэффициентов функций $f(x)$ равно $n+1$, то эти коэффициенты можно будет определить из $n+1$ линейных уравнений, получающихся от приравнивании числам (1) значений функций $f(x)$ при $a_0, a_1, a_2, \ldots, a_n$.

Нетрудно видеть, что существует только одна функция $f(x)$, удовлетворяющая требованиям задачи, ибо, если были бы возможны две искомые функции $f(x)$ и $f_1(x)$, то их разность

$$f(x) - f_1(x)$$

обращалась бы в нуль для значениях x равных

$$a_0, \quad a_1, \quad a_2, \ \ldots, \ a_n$$

и должна была бы тождественно обратиться в нуль, так как степень этой функции n, а число корней $n+1$; значить $f(x)$ совпадает с $f_1(x)$.

Lagrange показал простой способ писать окончательное выражение искомой функций. Введем в рассмотрение следующую функцию степени $n+1$

$$\varphi(x) = (x-a_0)(x-a_1)\cdots(x-a_n),$$

корни которой суть заданные числа $a_0, a_1, a_2, \ldots, a_n$. Обозначим для сокращения

$$\varphi_i(x) = \frac{\varphi(x)}{x-a_i},$$

где i может принимать все значения ряда $0, 1, 2, \ldots, n$. Все функции $\varphi_i(x)$ суть целые функций n-ой степени.

Будем искать функцию $f(x)$ в таком виде:

$$f(x) = A_0\varphi_0(x) + A_1\varphi_1(x) + \ldots + A_n\varphi_n(x), \tag{2}$$

где

$$A_0, \quad A_1, \quad A_2, \ \ldots, \ A_n$$

суть некоторые коэффициенты, которые надо определить.

Нетрудно видеть, что функции $\varphi_i(x)$ обладают следующими свойствами

$$\varphi_i(a_k) = 0,$$

при k отличном от i; это следует из того, что функция $\varphi_i(x)$ имеет корнями все корни функций $\varphi(x)$ кроме a_i. [Далее,]

$$\varphi_i(a_i) = \varphi'(a_i);$$

чтобы показать это, заметим, что

$$\varphi(x) = (x-a_i)\varphi_i(x),$$

откуда

$$\varphi'(x) = \varphi_i(x) + (x-a_i)\varphi_i'(x);$$

подставляя сюда a_i вместо x, получим

$$\varphi'(a_i) = \varphi_i(a_i).$$

Легко видеть, что $\varphi'(a_i)$ отлично от нуля, ибо, согласно определению функций $\varphi(x)$, все ее корни простые. Подставляя в равенство (2) a_i вместо x, получим

$$f(a_i) = A_i\varphi_i(a_i),$$

откуда

$$A_i = \frac{f(a_i)}{\varphi_i(a_i)} = \frac{f(a_i)}{\varphi'(a_i)}.$$

Отсюда получаем окончательное выражение для искомой функций в виде

$$f(x) = \frac{f(a_0)}{\varphi'(a_0)}\,\varphi_0(x) + \frac{f(a_1)}{\varphi'(a_1)}\,\varphi_1(x) + \ldots + \frac{f(a_n)}{\varphi'(a_n)}\,\varphi_n(x). \tag{3}$$

Последняя формула (3) и есть известная интерполяционная формула Lagrange'a.

§ 18

Формулу Lagrange'a (3) можно переписать так

$$f(x) = A_0 \frac{\varphi(x)}{x - a_0} + A_1 \frac{\varphi(x)}{x - a_1} + \ldots + A_n \frac{\varphi(x)}{x - a_n}$$

или

$$\frac{f(x)}{\varphi(x)} = \frac{A_0}{x - a_0} + \frac{A_1}{x - a_1} + \ldots + \frac{A_n}{x - a_n}.$$

Переписанная в таком виде формула Lagrange'a дает разложение рациональной функции $\dfrac{f(x)}{\varphi(x)}$ на простейшие дроби и была нами получена на стр. 51.

О функциях с перемежающимися корнями

§ 19

Рассмотрим функцию $f(x)$ с вещественными коэффициентами, корни которой

$$\alpha_1, \quad \alpha_2, \ \ldots, \ \alpha_n \tag{1}$$

вещественны и различны; пусть кроме того имеют место неравенства

$$\alpha_1 < \alpha_2 < \alpha_3 < \ldots < \alpha_n.$$

Так как число промежутке в между корнями (1) есть $n - 1$, и кроме того у производной, как функции степени $n - 1$, число корней есть также $n - 1$, то, как следствие теоремы Rolle'a, получится, что все корни

$$\beta_1, \quad \beta_2, \ \ldots, \ \beta_{n-1} \tag{2}$$

производной должны быть вещественны и должны заключаться по одному в промежутках между корнями (1); другими словами, между корнями (1) и (2) должны существовать неравенства

$$\alpha_1 < \beta_1 < \alpha_2 < \beta_2 < \alpha_3 < \ldots < \beta_{n-1} < \alpha_n. \tag{3}$$

Неравенства (3) показываюсь, что и обратно в этом случай между каждыми двумя последовательными корнями производной находится корень заданной функции $f(x)$. Говорят, что корни функции $f(x)$, если они все вещественны, *перемежаются* с корнями производной. Обобщая это понятие, мы назовем две функций $f(x)$ и $\varphi(x)$ функциями с перемежающимися корнями, если все корни этих функции вещественны и между каждыми двумя последовательными корнями одной функций лежит корень другой функции.

Очевидно, что функции с перемежающимися корнями должны быть или одинаковых степеней, или, как в выше приведенном случае, степени их могут отличаться на единицу.

Теорема. *Если корни функций $f(x)$ и $\varphi(x)$ перемежающтся, то уравнение*

$$f(x)\varphi'(x) - f'(x)\varphi(x) = 0$$

не имеет вещественных корней.

Предположим, что степень функции $f(x)$ не превосходить степени $\varphi(x)$, тогда по формуле Lagrange'a (см. пред. параграфе) получим

$$\frac{f(x)}{\varphi(x)} = C + \sum_i \frac{f(\alpha_i)}{\varphi'(\alpha_i)} \cdot \frac{1}{x - \alpha_i}, \tag{5}$$

где C постоянная, если степени функций $f(x)$ и $\varphi(x)$ одинаковы, и нулю, если степень $f(x)$ ниже степени $\varphi(x)$.

Дифференцируя тождество (5) по x, получим

$$\frac{\varphi(x)f'(x) - f(x)\varphi'(x)}{[\varphi(x)]^2} = -\sum \frac{f(\alpha_i)}{\varphi'(\alpha_i)} \cdot \frac{1}{(x - \alpha_i)^2}. \tag{6}$$

Нетрудно видеть, что сумма во второй части последнего равенства сохраняет свой знак при всевозможных значениях x. В самом деле, рассмотрим два последовательных корня

$$\alpha_i \quad \text{и} \quad \alpha_{i+1}$$

функции $\varphi(x)$. Так как корни производной $\varphi'(x)$ перемежаются с корнями функции $\varphi(x)$, то числа $\varphi'(\alpha_1)$ и $\varphi'(\alpha_{i+1})$ разных знаков. Подобным же образом будут разных знаков числа $f(\alpha_i)$ и $f(\alpha_{i+1})$, ибо перемежаются по условно также корни функций $f(x)$ с корнями $\varphi(x)$.

Следовательно, дроби

$$\frac{f(\alpha_i)}{\varphi'(\alpha_i)} \quad \text{и} \quad \frac{f(\alpha_{i+1})}{\varphi'(\alpha_{i+1})}$$

одного знака, так что дроби

$$\frac{f(\alpha_i)}{\varphi'(\alpha_i)}$$

имеют один знак при всевозможных значениях i.

Формулу (6) можно будет написать в таком виде

$$\varphi(x)f'(x) - \varphi'(x)f(x) = -\sum \frac{f(\alpha_i)}{\varphi'(\alpha_i)} \{\varphi_i(x)\}^2;$$

последняя формула показывает, что выражение

$$\varphi(x)f'(x) - \varphi'(x)f(x)$$

не меняет своего знака при всевозможных значениях x. Нетрудно видеть, что кроме того это выражение не может обращаться в нуль ни при каком вещественном значений β числа x. В самом деле, такое обращение в нуль могло бы иметь место, если бы β обращала в нуль сразу все функции

$$\varphi_1(x), \quad \varphi_2(x), \ \ldots, \ \varphi_n(x),$$

что невозможно.

Из всего сказанного вытекает, следовательно, что уравнение

$$\varphi(x)f'(x) - \varphi'(x)f(x) = 0$$

не может иметь вещественных корней.

§ 20

Приведем два примера функций с перемежающимися корнями.

Рассмотрим так называемые, *полиномы Legendre'a*, играюшие весьма важную роль в некоторых частях анализа. Назовем полиномом Legendre'a и обозначим его через X_n производную порядка n от функции

$$\varphi(x) = \frac{(x^2-1)^n}{1\cdot 2\cdot 3\cdots n\cdot 2^n},$$

т. е. от такой целой функций степени $2n$

$$\varphi(x) = \frac{1}{2\cdot 4\cdots 2n}\left\{x^{2n} - \frac{n}{1}\,x^{2n-1} + \ldots +\right.$$

$$\left. +(-1)^k\,\frac{n(n-1)\cdots(n-k+1)}{1\cdot 2\cdots k}\,x^{2n-2k} + \ldots \pm \frac{n}{1}\,x^2 \mp 1\right\}.$$

Итак, мы видим, что выражением Legendre'овой функции будет

$$X_n = \frac{2n(2n-1)\cdots(n+1)}{2\cdot 4\cdots 2n}\,x^n - \ldots +$$

$$+(-1)^k\,\frac{(2n-2k)(2n-2k-1)\cdots(n+1)}{2\cdot 4\cdots 2k\cdot 2\cdot 4\cdots(2n-2k)}\,x^{2n-2k} + \ldots$$

Мы замечаем, что X_n есть некоторая целая функция от x; например,

$$X_1 = x, \quad X_2 = \frac{3}{2}\,x^2 - \frac{1}{2}, \ \ldots$$

Не трудно убедиться, прилагая теорему Rolle'a, что все корни Legendre'овой функции X_n, вещественны и различны между собою.

В самом деле, $\varphi(x)$ имеет все корни вещественные, причем этих корней два: $+1$ и -1, и каждый из них кратности n. На основании сказанного в предыдущем §-е производная $\varphi'(x)$ будет иметь корни $+1$ и -1 с кратностями $n-1$ и еще один корень α в промежутке между $+1$ и -1; для функций $\varphi''(x)$ кроме чисел $+1$ и -1 будут еще два вещественных корня β_1 и β_2, заключенных в каждом из промежутков

$$(-1, \alpha), \quad (\alpha, 1);$$

$\varphi'''(x)$ будет иметь корни $+1$ и -1 с кратностями $n-3$ и три новых корня, различных между собою и лежащих по одному в промежутках

$$(-1, \beta_1), \quad (\beta_1, \beta_2), \quad (\beta_2, 1).$$

Продолжая рассуждение дальние, мы замечаем что производная порядка n от $\varphi(x)$, которая представляет не что иное, как функций Legendre'a, уже не будет иметь корней равных $+1$ и -1, а будет иметь n различных между собою корней в промежутки от -1 до $+1$.

Рассмотрим для примера еще функцию

$$V_n = z^n + \frac{1}{z^n},$$

где

$$x = z + \frac{1}{z}.$$

Нетрудно видеть, что V_n будет полиномом степени n от x. В самом деле, рассматривая выражение xV_{n-1}, получим

$$xV_{n-1} = \left(z + \frac{1}{z}\right)\left(z^{n-1} + \frac{1}{z^{n-1}}\right) = z^n + \frac{1}{z^n} + z^{n-2} + \frac{1}{z^{n-2}} = V_n + V_{n-2};$$

откуда получаем такое соотношение между тремя функциями V_{n-2}, V_{n-1} и V_n

$$V_n = xV_{n-1} - V_{n-2}. \tag{1}$$

Соотношение (1) дает возможность вычислять последовательно $V_0, V_1, V_2, V_3, \ldots$; получаем

$$V_0 = 2, \quad V_1 = x,$$
$$V_2 = xV_1 - V_0 = x^2 - 2, \quad V_3 = x^3 - 3x, \ \ldots$$

Нетрудно видеть, что корни двух последовательных функций V_{n-1} и V_n перемежаются. Мы убедимся в справедливости сказанного, показав, что, если корни двух функций V_{n-2} и V_{n-1} перемежаются, то будут перемежаться и корни функций V_{n-1} и V_n. Подставим в уравнение (1) два последовательных корня α, β функций V_{n-1}; тогда результаты подстановок чисел α и β в функцию V_{n-2} должны быть разных знаков, ибо корни V_{n-2} перемежаются с корнями V_{n-1}. Но при x, равном одному из указанных корней, мы имеем из равенства (1)

$$V_n = -V_{n-2},$$

значит различных знаков должны быть результаты, постановки α и β в функцию V_n. Для того, чтобы убедиться, что корни V_n и V_{n-1} перемежаются, остается показать, что функция V_n имеет один корень, больший наибольшего из корней функций V_{n-1}, и один корень, меньший наименьшего из корней последней функций. Так как старшие члены функций V_n и V_{n-2} суть x^n и x^{n-2}, то мы видим (см. стр. **??**), что знаки функций V_n и V_{n-2} одинаковы, как при $x = +\infty$, так и при $x = -\infty$. Применяя равенство (1) к наибольшему корню λ функции V_{n-1}, мы видим, что при $x = \lambda$ функций V_n и V_{n-2} разных знаков. С другой стороны функция V_{n-2} не имеет корня большого λ, следовательно, V_{n-2} не меняет своего знака в промежутков $(\lambda, +\infty)$; значит, должна менять в этом промежутка свой знак функция V_n, и, следовательно, по крайней мере один корень функций V_n должен заключаться в этом промежутке. Подобным же образом мы покажем, что

будет существовать вещественный корень функции V_n в промежутке $(-\infty, \mu)$, где μ есть меньший из корней функций V_{n-1}.

Итак, мы видим, что корни функций V_n и V_{n-1} перемежаются, что и требовалось доказать.

Перемежаемость корней двух рядом стоящих Legendre'овских функций зависит от соотношения

$$nX_n - (2n-1)xX_{n-1} + (n-1)X_{n-2} = 0.$$

Теорема В. А. Маркова

§ 21

Из теоремы предыдущего параграфа вытекает весьма важная теорема, замеченная В. Марковым.

Теорема. *Если корни двух функций $f(x)$ и $\varphi(x)$ перемежаются, то перемежаются также и корни их производных $f'(x)$ и $\varphi'(x)$.*

В самом деле, рассмотрим функцию

$$\varphi(x)f'(x) - f(x)\varphi'(x).$$

Пусть будут α_1 и α_2 два последовательных корня производной $\varphi'(x)$.

По теорем предыдущего §-а мы замечаем, что результаты подстановок чисел α_1 и α_2 в выражение (1) одного знака. Эти результаты суть, очевидно,

$$\varphi(\alpha_1)f'(\alpha_1) \quad \text{и} \quad \varphi(\alpha_2)f'(\alpha_2).$$

Но числа $\varphi(\alpha_1)$ и $\varphi'(\alpha_2)$ разных знаков, следовательно, должны быть разных знаков числа $f'(\alpha_1)$ и $f'(\alpha_2)$, т. е. между каждыми двумя последовательными корнями производной $\varphi'(x)$ должен лежать вещественный корень производной $f'(x)$.

О полиномах наименее уклоняющихся от нуля

§ 22

Совершенно особого характера вопросы на maxima и minima были поставлены и решены П. Л. Чебышевым. Для характеристики этих вопросов решим основную задачу Чебышева о нахождении целой функции степени n со старшим коэффициентом, равным единице, при условии, чтобы эта функция *наименее уклонялась от нуля* в данном промежутке. Под наименьшим уклонением от нуля разумеется требование, чтобы был *наименьшим maximum* абсолютной величины функции в данном промежутке.

Чебышев показал. что такая функция для промежутка $(-1, +1)$ есть не что иное, как функция

$$f(x) = \frac{1}{2^{n-1}} \cos(n \arccos x). \tag{1}$$

Для вычисления этой функции (1) можно будет поступить так. Введем угол φ при помощи равенства $x = \cos\varphi$, тогда мы получим

$$f(x) = \frac{1}{2^{n-1}} \cos n\varphi.$$

Значить, функция Чебышева есть не что иное, как та целая функция степени n, при помощи которой косинус кратной дуги $\cos n\varphi$ выражается через косинус простой дуги $\cos\varphi$. Покажем, что старший коэффициент функций $\cos(n \arccos x)$ есть 2^{n-1}. В самом деле,

$$\cos\varphi + i\sin\varphi = x + \sqrt{x^2-1},$$

$$\cos\varphi - i\sin\varphi = x - \sqrt{x^2-1},$$

откуда

$$\cos n\varphi + i\sin n\varphi = (x + \sqrt{x^2-1})^n,$$
$$\cos n\varphi - i\sin n\varphi = (x - \sqrt{x^2-1})^n.$$

Следовательно

$$\cos n\varphi = \frac{(x+\sqrt{x^2-1})^n + (x-\sqrt{x^2-1})^n}{2} = p_0 x^n + p_1 x^{n-1} + \ldots$$

Разделяя обе части уравнения на x^n, получим

$$p_0 + \frac{p_1}{x} + \ldots = \frac{\left(1+\sqrt{1-\frac{1}{x^2}}\right)^n + \left(1-\sqrt{1-\frac{1}{x^2}}\right)^n}{2}.$$

Полагая $x = \infty$, получим

$$p_0 = \frac{2^n}{2} = 2^{n-1}.$$

Итак, старший коэффициент функций (1) равен единице.

Докажем теперь, следуя академику А. Маркову, что функция (1) есть наименее уклоняющаяся от нуля в промежутка $(-1, +1)$. Допустим, что в этом промежутка другая функция $\psi(x)$ менее уклоняется от нуля. Мы замечаем, что функция (1) уклоняется от нуля на величину $\frac{1}{2^{n-1}}$, так как наибольшая абсолютная величина функции $\cos(n \arccos x)$ есть 1; это уклонение происходит при значениях

$$\varphi = 0,\ \frac{\pi}{n},\ \frac{2\pi}{n},\ \frac{3\pi}{n},\ \ldots,\ \frac{(n-1)\pi}{n},\ \pi!$$

т. е. когда x принимает значения

$$x_0 = 0,\ x_1 = \cos\frac{\pi}{n},\ x_2 = \cos\frac{2\pi}{n}, \ldots,\ x_{n-1} = \cos\frac{n-1}{n}\pi,\ x_n = 1. \tag{2}$$

Так как значения функции $f(x)$ при значениях (2) переменного независимого будут

$$\frac{1}{2^{n-1}},\ -\frac{1}{2^{n-1}},\ \frac{1}{2^{n-1}},\ \ldots,\ (-1)^n \frac{1}{2^{n-1}},$$

то, следовательно, если функция $\psi(x)$ уклоняется от нуля менее чем Чебышевская функция, то будут существовать неравенства

$$f(x_0) - \psi(x_0) > 0, \quad f(x_1) - \psi(x_1) < 0, \quad f(x_2) - \psi(x_2) > 0, \ \ldots$$

Итак, разность

$$f(x) - \varphi(x)$$

будет иметь по крайней мере один корень в каждом промежутке

$$(x_0, x_1), \quad (x_1, x_2), \ \ldots, \ (x_{n-1,n}),$$

что невозможно, ибо разность $f(x) - \psi(x)$ степени $n-1$, так как обе функции $f(x)$ и $\psi(x)$ имеют старший коэффициент равный единице. Итак, функция Чебышева (1) есть, действительно, функция наименее уклоняющаяся от нуля в промежутке $(-1, +1)$, из всех целых функций степени n, имеющих старшим коэффициентом 1.

Очень элегантный способ доказательства дан также Б. Млодзеевским.[42]

§ 23

Чебышевым и его учениками был подвергнут изучению вопрос о наименее уклоняющихся от нуля полиномах вида

$$x^n - \sigma x^{n-1} + p_1 x^{n-2} + \ldots p_n,$$

где σ данное число.

Случай $\sigma = 0$ был разобран впервые самим Чебышевым в мемуаре «Théorie des mécanismes connus sous le nom de parallélogrammes».[43]

Изучению случая σ отличного от нуля посвящен замечательный мемуар Е. И. Золотарева[44] «Приложение эллиптических функций к вопросам о функциях, наименее и наиболее отклоняющихся от нуля».

В сочинении «О функциях наименее уклоняющихся от нуля в данном промежутке» Спб. 1892. покойный В. А. Марков решает вопрос для полиномов

$$p_0 x^n + p_1 x^{n-1} + \ldots + p_n,$$

коэффициенты которых связаны соотношением

$$\alpha_0 p_0 + \alpha_1 p_1 + \ldots + \alpha_n p_n = \alpha.$$

Указанное сочинение В. А. Маркова было его студенчоским сочияением. Оно замечательно целым рядом результатов важного значения. Между прочим, в этом сочинений указана теорема приведенная нами в § 21.

В последнее время А. П. Пшеборский[45] обобщил исследования В. А. Маркова на случай двух соотношений

$$\alpha_0 p_0 + \alpha_1 p_1 + \ldots + \alpha_n p_n = \alpha,$$

[42]Б. Млодзеевский. Математический Сборник XXIX: 1 Москва.

[43]Сочинения III, 1 стр. 111–143.

[44]Приложения к XXX тому Записки Академии Наук за 1877 г.

[45]Пшеборский. О некоторых полиномах, наименее уклоняющихся от нуля в данном промежутка. Сообщения Харьк. Мат. Общ. Сер. 2. Т. XIV.

$$\beta_0 p_0 + \beta_1 p_1 + \ldots + \beta_n p_n = \beta.$$

В последнее время вопросы Чебышева послужили исходной точкой для теории рядов, расположенных по полиномам, теории, связанной с именем Weierstrass'a. В этой теории обратили на себя внимание исследования выдающегося современного математика Сергея Бернштейна. Хотя эти исследования относятся более к анализу бесконечно малых, чем к алгебре, тем не менее, я считаю необходимым сказать о них несколько слов по стольку, по скольку эти исследования относятся к полиномам, наименее уклоняющихся от нуля. С. Бернштейн[46] вводит определение:

Полином

$$P(x) = A_0 x^{\alpha_0} + A_1 x^{\alpha_1} + \ldots + A_n x^{\alpha_n}$$

называется осцилирующим в промежутке $(0, 1)$ *относительно не отрицательных показателей*

$$\alpha_0 < \alpha_1 < \ldots < \alpha_n,$$

если его абсолютная величина достигает своего наибольшего значения $n + 1$ *раз в промежутке.*

Число n Бернштейн называет порядком осцилирующего полинома.

Оказывается, что, если мы зададим численное значение одного из коэффициентов A_i, другие же коэффициенты будем менять, то осцилирующий полином будет наименее уклоняться от нуля, чем все остальные такого же вида.

Пусть, в самом деле, $P(x)$ и $Q(x)$ будут полиномы с теми же показателями α_i (того же порядка), имеющие одинаковый коэффициент A_i, причем полином $P(x)$ осцилирующий, а полином $Q(x)$ произвольный. Допустим, что абсолютная величина $Q(x)$ не превосходить абсолютной величины $P(x)$ в промежутке $(0, 1)$. Тогда для значений

$$x_0, \quad x_1, \ \ldots, \ x_n,$$

дающих maximum абсолютной величины $P(x)$, получим

$$(-1)^{k+\rho}[P(x_k) - Q(x+k)] \geq 0,$$

где ρ есть 0 или 1.

Уравнение

$$P(x) - Q(x) = 0$$

должно иметь, следовательно, n корней; что невозможно, ибо в разности $P(x) - Q(x)$ пропадает член с коэффициентом A_i так что эта разность должна заключать только n членов; поэтому число перемен знаков коэффициентов не может быть больше $n - 1$, а, следовательно, по теорем Descartes'a не может быть больше чем $n - 1$ положительных корней.

Бернштейн заявляет, что ему известен вид осцилирующих полиномов только для того случая, когда показатели $\alpha_0, \alpha_1, \alpha_2, \ldots, \alpha_n$ образуют арифметическую прогрессию и ставит новую задачу нахождения этих полиномов для других случаев. Мы считаем, что задача Бернштейна имеет свой интерес.

[46] S. Bernstein. Sur la meilleure approximation de $|x|$ par des polynomes de degres donnés. Acta Mathematica t. 37.

Метода Fourier

§ 24

Здесь мы изложим методу отделения корней, указанную Fourier и основанную на приложении теоремы Budan'a. Хотя эта метода не решает вполне с теоретической точки зрения задачи об отделении корней, но на практике в большинстве случаев дает простой способ решить эту задачу.

Историческая роль методы Fourier состоять в том, что несомненно, изучая ее, Sturm, ученик Fourier, был приведен к открытию его знаменитой теоремы, которая будет предметом следующей главы.

В основании методы Fourier лежать следующие предложения.

Лемма. *При изменений x в промежутке не заключающем корня производной $f'(x)$, функция*

$$x - \frac{f(x)}{f'(x)}$$

возрастает, если $f(x)$ и $f''(x)$ одного знака, и убывает, если эти функции различных знаков.

В самом деле, обозначая

$$x - \frac{f(x)}{f'(x)} = \varphi(x),$$

получим

$$\varphi'(x) = 1 - \frac{\{f'(x)\}^2 - f(x)f''(x)}{\{f'(c)\}^2} = \frac{f(x)f''(x)}{\{f'(x)\}^2};$$

отсюда мы замечаем, что производная $\varphi'(x)$ остается положительною, если $f(x)f''(x) > 0$, т. е. $f(x)$ и $f''(x)$ одинаковых знаков, и отрицательна, если $f(x)$ и $f''(x)$ разных знаков; отсюда и следует справедливость леммы.

Теорема I. *Если функция $f(x)$ имеет два вещественных корня в промежутке (a, b), первая производная $f'(x)$ имеет один корень в этом промежутке, а вторая производная $f''(x)$ в этом промежутке не имеет корней, то должно иметь место неравенство*

$$\frac{f(b)}{f'(b)} - \frac{f(a)}{f'(a)} < b - a,$$

причем предполагается $b > a$.

Обозначим через x_1 и x_2 корни функции $f(x)$ и предположим, что $x_2 > x_1$. Между этими корнями лежит корень x_0 производной $f'(x)$.

Рассмотрим две функции

(1) $$\frac{f(x)}{f'(x)}$$

и

(2) $$\frac{f'(x)}{f''(x)}.$$

Функция (1) не меняет своего знака в промежутке (a, x_1), ибо в этом промежутка нет корней ни у числителя, ни у знаменателя. Подобным же образом функция

(2) не меняет своего знака в промежутке (a, x_0). Нетрудно убедиться, что знаки обеих функции (1) и (2) в промежутке (a, x_1) одинаковы; в самом деле, на основании теоремы стр. 289, обе дроби (1) и (2) отрицательны: первая для значений x, близких к x_1 и меньших этого числа, вторая для значений x, близких к x_0 и меньших его. Таким образом, обе дроби (1) и (2) отрицательны во всем промежутка (a, x_1). Произведение их

$$\frac{f(x)}{f''(x)}$$

оказывается числом положительным в промежутка (a, x_1), т. е. в этом промежутков функций $f(x)$ и $f''(x)$ одного знака, так что для этого промежутка функция

$$\varphi(x) = x - \frac{f(x)}{f'(x)} \tag{3}$$

есть функция возрастающая, и мы имеем неравенство

$$\varphi(a) < \varphi(x_1). \tag{4}$$

Аналогично может быть трактован промежуток (x_2, b); в самом деле, обе дроби (1) и (2) положительны в этом промежутков, так как, с одной стороны, они не меняют знака: первая в промежутке (x_2, b), вторая в промежутки (x_0, b); с другой стороны, по теореме стр. 289, значения их в этих промежутках должны быть положительными. Итак, будет положительным в промежутка (x_2, b) их произведение

$$\frac{f(x)}{f''(x)}.$$

Значит, в этом промежутке будет возрастать функция (3), и мы получаем неравенство

$$\varphi(x_2) < \varphi(b). \tag{5}$$

Но x_1 и x_2 суть корни функции $f(x)$; следовательно, по равенству (3) мы получим

$$\varphi(x_1) = x_1,$$
$$\varphi(x_2) = x_2;$$

отсюда неравенства (4) и (5) получают вид

$$\varphi(a) < x_1, \qquad x_2 < \varphi(b).$$

Но $x_2 > x_1$, следовательно, подавно

$$\varphi(a) < \varphi(b),$$

то есть

$$a - \frac{f(a)}{f'(a)} < b - \frac{f(b)}{f'(b)},$$

или окончательно

$$\frac{f(b)}{f'(b)} - \frac{f(a)}{f'(a)} < b - a,$$

что и требовалось доказать.

Теорема II. *Если в промежутке (a, b) функция $f(x)$ не имеет вещественных корней, первая же производная имеет один корень, а вторая производная не имеет корня, причем знак этой второй производной совпадает со знаком самой функции в этом промежутке, и если имеет место неравенство*

$$\frac{f(b)}{f'(b)} - \frac{f(a)}{f'(a)} < b - a,$$

то уменьшением промежутка всегда можно будет достигнуть того, что для нового промежутка (a_1, b_1) будет иметь место неравенство

$$\frac{f(b1)}{f'(b_1)} - \frac{f(a_1)}{f'(a_1)} \geq b_1 - a_1.$$

Обозначим через x_0 корень первой производной. Так как $f(x)$ одного знака во всем промежутке, то функция

$$\varphi(x) = x - \frac{f(x)}{f'(x)}$$

будет возрастающая в рассматриваем промежутка (a, b).

Рассмотрим промежуток (a, b_1) и будем давать числу b_1 убывающие численные значения, начиная от числа b и неопределенно приближающиеся к корню x_0. Тогда функция

$$\varphi(b_1) - \varphi(a)$$

будет убывающая, ибо будет убывать первый член $\varphi(b_1)$. Если было положительным первоначальное значение нашей разности

$$\varphi(b) - \varphi(a),$$

то это значение должно будет, убывая, приближаться к $-\infty$, ибо число x_0, к которому приближается число b_1, есть корень знаменателя в выражении функции $\varphi(x)$, и, следовательно, мы дойдем до такого значения b_1, при котором будет иметь место неравенство

$$\varphi(b_1) - \varphi(a) \leq 0,$$

то есть

$$\frac{f(b_1)}{f'(b_1)} - \frac{f(a)}{f'(a)} \geq b_1 - a,$$

что и требовалось доказать.

Можно было бы оставить верхний предать b промежутка (a, b) без перемены, а увеличивать нижний предел a, причем, рассматривая возрастающую функцию $\varphi(x) - \varphi(b)$, можно было бы взять за нижний предел числа a_1 настолько близкое к корню x_0, чтобы было

$$\frac{f(b)}{f'(b)} - \frac{f(a_1)}{f'(a_1)} \geq b - a_1.$$

Обращаясь к приложение теоремы Budan'a к отделению корней, введем понятие о, так называемых, указателях функции ряда Budan'a. Будем называть *указателем функции* $f^{(\mu)}(x)$ на промежутке (α, β) число потерь перемен знака в ряде

$$f^{(\mu)}(x), \quad f^{(\mu+1)}(x), \ \ldots, \ f^{(n)}(x),$$

соответствующее промежутку (α, β), и будем обозначать его Δ_μ; тогда всякому промежутку будет соответствовать ряд указателей

$$\Delta_0, \quad \Delta_1, \ \ldots, \ \Delta_n.$$

За Δ_n можно принять число нуль.

Очевидно, что два рядом стоящие указателя могут отличаться не более, чем на 1, так что может быть одно из трех

$$\Delta_{\mu+1} = \Delta_\mu, \qquad \Delta_{\mu+1} = \Delta_\mu + 1,$$

$$\Delta_{\mu+1} = \Delta_\mu - 1.$$

Если первый указатель $\Delta_0 = 0$, то по теореме Budan'a не существует корней заданной функции $f(x)$ в промежутке (α, β). Когда $\Delta_0 = 1$, то по той же теореме должен существовать непременно один простой корень, который таким образом оказывается отделенным числами α и β. Все, очевидно, сводится к указанию правил, как надо рассуждать в случае $\Delta_0 \geq 2$.

Рассмотрим первый слева указатель, равный единице; существование такого указателя очевидно из того соображения, что первый указатель не меньше числа 2, (ибо мы рассматриваем случай $\Delta_0 \geq 2$), а последний равен нулю, два же рядом стоящих не могут отличаться больше, чем на единицу. Итак допустим, что $\Delta_\mu = 1$.

Метода Fourier, состоит в том, что показывается, что уменьшением промежутков можно первый, равный единице, указатель передвинуть влево, т. е., другими словами, уменьшите значение μ. Таким образом в конце концов можно указатель, равный единице, поместить на первое место, или же достигнуть того, чтобы первый указатель был равен нулю.

Рассмотрим предыдуший указатель $\Delta_{\mu-1}$. Очевидно, что этот указатель должен равняться числу 2, ибо, если бы он равнялся единице, то Δ_μ не был бы первым, равным единице указателем. Если же $\Delta_{\mu-1} = 0$, то перед указателем $\Delta_{\mu-1}$ должен бы существовать указатель, равный единице, ибо первый указатель не меньше 2. Будем рассматривать следующий указатель $\Delta_{\mu+1}$. Сближая пределы α и β, можно достигнуть того, чтобы указатель $\Delta_{\mu+1}$ сделать равным нулю. В самом деле, равенство

$$\Delta_\mu = 1$$

показывает по теореме Budan'a, что $f^{(\mu)}(x)$ имеет один только корень, причем этот корень простой; следовательно, указывая два числа α_1 и β_1, достаточно близкие с двух сторон к этому корню, можно достигнуть того, что в промежутке (α_1, β_1) не будет корней производной $f^{(\mu+1)}(x)$.

Итак, для промежутка (α_1, β_1) указатель $\Delta_{\mu+1}$ может быть или нуль, или два; но так как функция $f^{(\mu=1)}(x)$ в промежутке (α_1, β_1) не меняет своего знака, функция же $f^{(\mu)}(x)$ меняет свой знак, проходя через единственный свой корень, то ряд функций

$$f^{(\mu)}(x), \quad f^{(\mu+1)}(x)$$

представляет перемену знака до корня функции $f^{(\mu)}(x)$ и повторение знака после этого корня. Другими словами, в этой паре функций происходит потеря одной перемены знака при переходе от α_1 к β_1, значит, указатель функции $f^{(\mu)}(x)$ должен быть на единицу больше указателя функции $f^{(\mu+1)}(x)$, и, следовательно, для промежутка (α_1, β_1) имеет место следуюшдй ряд указателей

$$\Delta_{\mu-1} = 2, \quad \Delta_\mu = 1, \quad \Delta_{\mu+1} = 0.$$

Что касается двух других промежутков (α, α_1) и (β_1, β), которые остаются от промежутка (α, β) после выделения, то, очевидно, что в этих двух промежутках будет $\Delta_\mu = 0$. В самом деле, в этих промежутках нет корней функции $f^{(\mu)}(x)$, ибо эта функция имеет единственный корень в среднем промежутке (α_1, β_1). По теореме Budan'a указатель функции в каждом из двух последних промежутков должен или равняться нулю, или быть больше нуля на число четное; с другой стороны указатель Δ_μ на всем промежутке (α, β) равен сумме указателей (что следует из определения), соответствующих трем частям промежутка; а так как указатель равен единице для всего промежутка и для средней его части, то он должен, очевидно, равняться нулю для каждой из двух крайних частей, и, следовательно, для каждой из двух этих крайних частей первый указатель, равный единице, будет левее от указателя Δ_μ.

Итак, весь вопрос, следовательно, сводится к рассмотрению случая

$$\Delta_{\mu-1} = 2, \quad \Delta_\mu = 1, \quad \Delta_{\mu+1} = 0.$$

В этом случае мы видим, что функция $f^{(\mu+1)}(x)$, которая есть не что иное, как вторая производная функции $f^{(\mu-1)}(x)$, не имеет корня в рассматриваемом промежутка. Предыдущая функция $f^{(\mu)}(x)$, (первая производная от $f^{(\mu-1)}(x)$) имеет один корень; функция же $f^{(\mu-1)}(x)$ должна иметь или два корня, или ни одного (теорема Budan'a). Называя через α и β границы нашего промежутка, мы видим, что, если

$$\frac{f^{(\mu-1)}(\beta)}{f^{(\mu)}(\beta)} - \frac{f^{(\mu-1)}(\alpha)}{f^{(\mu)}(\alpha)} \geq \beta - \alpha,$$

то функция $f^{(\mu-1)}(x)$ не имеет корня в данном промежутке; это следует из приведенных ранее теорем. В этом случай функция $f^{(\mu-1)}(x)$ не меняет своего знака в промежутке (α, β).

Так как в теореме Budan'a существенную роль играет не то обстоятельство, что последняя функция не меняет своего знака в данном промежутке, то, наследуя промежуток, можно прилагать теорему Budan'a к ряду функций

$$f(x), \quad f'(x), \ \ldots, \ f^{(\mu-1)}(x),$$

остановленному на функции, не меняющей своего знака в промежутке. Следовательно, рассматривая указатели последнего ряда, можно будет последний указатель считать равным нулю. Очевидно, что ряд новых указателей

$$\Delta_0, \quad \Delta_1, \ \ldots, \ \Delta_{\mu-1}$$

будет представлять числа на две единицы меньше прежних, ибо последнее число будет 0, вместо числа 2.

Итак, в новом ряде указателей указатель, равный единице, будет стоять налево от указателя $\Delta_{\mu-1}$. Если же будет

$$\frac{f^{(\mu-1)}(\beta)}{f^{(\mu)}(\beta)} - \frac{f^{(\mu-1)}(\alpha)}{f^{(\mu)}(\alpha)} < \beta - \alpha,$$

то нельзя сказать ничего определенного об этом промежутке; придется этот промежуток уменьшить введением произвольных промежуточных чисел. Продолжая такое деление, мы обыкновенно приходим к промежуткам, относительно которых можно высказать определенное суждение: или, в случай неравенства

$$\frac{f^{(\mu-1)}(\beta)}{f^{(\mu)}(\beta)} - \frac{f^{(\mu-1)}(\alpha)}{f^{(\mu)}(\alpha)} \geq \beta - \alpha,$$

в промежутке не будет существовать вещественных корней, или же будет заключаться один корень функции $f^{(\mu-1)}(x)$, который таким образом оказывается отделенными. В этом последнем случае указатель $\Delta_{\mu-1}$ промежутка с отделенным корнем должен, очевидно, равняться единице, ибо во всем первоначальном промежутке этот указатель равнялся числу 2 и, следовательно, в новом промежутке указатель не может быть больше числа 2. Итак, мы видим, что в этом случае $\Delta_{\mu-1} = 1$, т. е. указатель, равный единице, передвинуть на одно место влево.

Продолжая таким образом последовательное перемещение налево указателя, равного единице, мы достигнем того, что этот указатель поместится на первое место, т. е. будет $\Delta_0 = 1$; тогда в соответственном промежутке будет существовать один только корень заданной функций $f(x)$, который таким образом и будет отделен.

Может случиться, что для некоторых из рассматриваемых промежутков будет $\Delta_0 = 0$; тогда в этих промежутках не будет корней у заданной функции.

§ 26

Изложенный способ Fourier отделения корней, как мы видим, заключает слабый пункт, а именно, может случиться, что при рассмотрений трех указателей

$$\Delta_{\mu-1} = 2, \quad \Delta_\mu = 1, \quad \Delta_{\mu+1} = 0$$

эти числа будут оставаться для соответственных промежутков, как бы далеко мы ни производили разбития промежутка на меньшие.

Такой случай будет иметь место, когда в промежутке (α, β) функция будет иметь двукратный корень $f^{(\mu-1)}(x)$, который, следовательно, будет простым корнем функции $f^{(\mu-1)}(\beta)$, причем кроме x_0 три функции

$$f^{(\mu-1)}(x), \quad f^{(\mu)}(x), \quad f^{(\mu+1)}(x)$$

не имеют других корней (функция $f^{(\mu+1)}(x)$ при этом предположении, очевидно, совсем не имеет корней в этом промежутке). Очевидно, что как бы ни уменьшали промежуток, заменяя его новыми (α_1, β_1), заключающими корень x_0, в этом промежутке будут заключаться два корня равных x_0 функции $f^{(\mu-1)}(x)$, один корень

у функций $f^{(\mu)}(x)$ и ни одного корня у функций $f^{(\mu+1)}(x)$; следовательно, для всех таких промежутков числа

$$\Delta_{\mu-1}, \quad \Delta_\mu, \quad \Delta_{\mu+1}$$

останутся равными 2, 1, 0. В этом случае, как бы далеко ни производить уменьшения промежутка, нельзя достигнуть перемещения налево указателя, равного единице; но в таком, особенно неблагоприятном, случае всегда можно убедиться в существовании кратного корня функции $f^{(\mu-1)}(x)$ приемами нахождения кратных корней, указанными на стр. **??**, и след., или же в крайнем случай трактовать такой неудобный для рассмотрения случай при помощи теоремы Sturm'a (стр. 324).

§ 27

Покажем, как поступать в том случай, если при подстановки некоторого числа α в ряд функций

$$f(x), \quad f'(c), \ \ldots, \ f^{(n)}(x)$$

несколько функций подряд обращаются в нуль; пусть эти функции будут

$$f^{(\mu)}(x), \quad f^{(\mu+1)}(x), \ \ldots, \ f^{(\mu+k-1)}(x).$$

Рассмотрим еще следующую функцию $f^{(\mu+k)}(x)$, не обращающуюся в нуль при $x = a$. Очевидно, что придется брать вместо числа a два числа $a + h$ и $a - h$, достаточно близкие к a по обе стороны ($h > 0$). При этом, если a есть нижняя граница промежутка, то число a заменять числом $a + h$, и числом $a - h$ в случае верхней границы; h можно выбрать настолько малым, что не будет равно нулю ни одно из чисел

$$(1) \qquad f^{(\mu)}(a+h), \quad f^{(\mu+1)}(a+h), \ \ldots, \ f^{(\mu+k-1)}(a+h), \quad f^{(\mu+k)}(a+h),$$

и

$$(2) \qquad f^{(\mu)}(a-h), \quad f^{(\mu+1)}(a-h), \ \ldots, \ f^{(\mu+k-1)}(a-h), \quad f^{(\mu+k)}(a-h).$$

Но мы уже знаем, что первый ряд должен представлять одни повторения знака, второй же ряд одни перемены знака; следовательно, по знаку последней функции $f^{(\mu+k)}(x)$ можно будет определить знак всех остальных. Пусть будет написан ряд знаков при $x = a$, причем вместо соответственного знака написано число нуль для всех тех функций, которые обращаются в нуль при $x = a$; тогда, если условимся над цифрою нуль писать тот знак, который соответственная функция получает при $a + h$, а под цифрою нуль знак, соответствующий $a - h$, то легко указать на основании сказанного все, как верхние, так и нижние знаки. Например, если имеется ряд знаков

$$- \ + \ 0 \ 0 \ - \ -0 \ 0 \ 0 \ 0 \ +,$$

то получим, например, такой ряд знаков

$$\begin{array}{cccccccccccc}
a+h & & & - & - & & & + & + & + & + & \\
a & - & + & 0 & 0 & - & - & 0 & 0 & 0 & 0 & + \\
a-h & & & - & + & & & + & - & + & - &
\end{array}$$

Указанное правило носит название *правила двойного знака.*

§ 28

Рассмотрим теперь численные примеры и будем применять способ Fourier отделения корней.

Пример I. Пусть дано уравнение

$$x^6 + x^5 - x^4 - x^3 + x^2 - x + 1.$$

Имеем ряд функций

$$\begin{aligned}
f(x) &= x^6 + x^5 - x^4 - x^3 + x^2 - x + 1,\\
f'(x) &= 6x^5 + 5x^4 - 4x^3 - 3x^2 + 2x - 1,\\
\frac{f''(x)}{1\cdot 2} &= 15x^4 + 10x^3 - 6x^2 - 3x + 1,\\
\frac{f'''(x)}{1\cdot 2\cdot 3} &= 20x^3 + 10x^2 - 4x - 1,\\
\frac{f^{IV}(x)}{1\cdot 2\cdot 3\cdot 4} &= 15x^2 + 5x - 1,\\
\frac{f^{V}(x)}{1\cdot 2\cdot 3\cdot 4\cdot 5} &= 6x + 1\\
\frac{f^{VI}(x)}{1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6} &= 1.
\end{aligned}$$

Действительные корни заданного уравнения $f(x) = 0$ заключаются между числами -1 и $+1$. Подставляя числа

$$-1, \quad -\frac{1}{2}, \quad 0, \quad \frac{1}{2}, \quad +1$$

в ряд функций

$$f(x), \quad f'(x), \quad f''(x), \quad f'''(x), \quad f^{IV}(x), \quad f^{V}(x), \quad f^{VI}(x),$$

получаем следующие результаты

x	$f(x)$	$f'(x)$	$f''(x)$	$f'''(x)$	$f^{IV}(x)$	$f^{V}(x)$	$f^{VI}(x)$
-1	$+$	$-$	$+$	$-$	$+$	$-$	$+$
$\frac{1}{2}$	$+$	$-$	$+$	$+$	$+$	$-$	$+$
0	$+$	$-$	$+$	$-$	$-$	$+$	$+$
$\frac{1}{2}$	$+$	$-$	$+$	$+$	$+$	$+$	$+$
$+1$	$+$	$+$	$+$	$+$	$+$	$+$	$+$

.

Произошло две потери перемен знака при переход от -1 до $-\frac{1}{2}$, две от 0 к $\frac{1}{2}$ и две от $\frac{1}{2}$ к 1. Мы немедленно можем заключить, что между $\frac{1}{2}$ и 1 действительных корней нет, так как мы имеем

$$f\left(\frac{1}{2}\right) = \frac{39}{64}, \quad f'\left(\frac{1}{2}\right) = -\frac{48}{64}, \quad f(1) = 1, \quad f'(1) = 5,$$

что дает

$$\frac{f(1)}{f'(1)} - \frac{f\left(\frac{1}{2}\right)}{f'\left(\frac{1}{2}\right)} > 1 - \frac{1}{2}.$$

В промежутке $\left(0, \frac{1}{2}\right)$ ряд указателей есть

$$2, \quad 2, \quad 2, \quad 1, \quad 0, \quad 0.$$

Первый указатель 1, сопровождаемый другим, равным единице, заставляет нас сузить пределы. Подстановка $\frac{1}{4}$ дает результаты

$$+ \ - \ + \ - \ + \ + \ +,$$

откуда видно, что нет никакой потери при переходе от нуля к $\frac{1}{4}$ достаточно рассмотреть промежуток $\left(\frac{1}{4}, \frac{1}{2}\right)$; соответствующий ряд указателей будет

$$2, \quad 2, \quad 2, \quad 1, \quad 0, \quad 0, \quad 0.$$

Так как мы имеем

$$f''\left(\frac{1}{4}\right) = \frac{13}{126}, \quad f'''\left(\frac{1}{4}\right) = -\frac{51}{8}, \quad f''\left(\frac{1}{2}\right) = \frac{3}{8}, \quad f'''\left(\frac{1}{2}\right) = 12,$$

то будет

$$\frac{f''\left(\frac{1}{2}\right)}{f'''\left(\frac{1}{2}\right)} - \frac{f''\left(\frac{1}{4}\right)}{f'''\left(\frac{1}{4}\right)} > \frac{1}{2} - \frac{1}{4}$$

отсюда заключаем, что уравнение

$$f''(x) = 0$$

не имеет корней между $\frac{1}{4}$ и $\frac{1}{2}$; следовательно, данное уравнение тоже не имеет их в этом промежутка. Наконец, рассматривая ряд указателей для промежутка $\left(-1, \frac{1}{2}\right)$, получим

$$2, \quad 2, \quad 2, \quad 1, \quad 0, \quad 0, \quad 0.$$

Так как мы имеем

$$f''(-1) = 6, \quad f'''(-1) = -42, \quad f''\left(-\frac{1}{2}\right) = \frac{31}{8}, \quad f'''\left(-\frac{1}{2}\right) = 6,$$

то будет

$$\frac{f''\left(-\frac{1}{2}\right)}{f'''\left(-D\frac{1}{2}\right)} - \frac{f''(-1)}{f'''(-1)} > -\frac{1}{2} + 1,$$

что указывает на то, что уравнение $f''(x) = 0$ не имеет корней между $-\frac{1}{2}$ и -1, следовательно, и сама данная функция не имеет корней в этом промежутке.

Итак шесть корней нашего уравнения мнимые.

Пример II. Пусть дано уравнение

$$x^6 - 12x^5 + 60x^4 + 123xx^2 + 4567x - 89012 = 0,$$

рассмотренное самим Fourier.

Получаем для этого уравнения ряд функций

$$\begin{aligned}
f(x) &= x^6 - 12x^5 + 60x^4 + 123xx^2 + 4567x - 89012,\\
f'(x) &= 6x^5 - 60x^4 + 240x^3 + 246x + 4567,\\
\frac{f''(x)}{1\cdot 2} &= 15x^4 - 120x^3 + 360x^2 + 123,\\
\frac{f'''(x)}{1\cdot 2\cdot 3} &= 20x^3 - 120x^2 + 240x,\\
\frac{f^{IV}(x)}{1\cdot 2\cdot 3\cdot 4} &= 15x^2 - 60x + 60,\\
\frac{f^{V}(x)}{1\cdot 2\cdot 3\cdot 4\cdot 5} &= 6x - 1\\
\frac{f^{VI}(x)}{1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6} &= 1.
\end{aligned}$$

Выберем положительную и сколь угодно малую величину h. Подставляя ряд чисел

$$-10,\quad -1,\quad -h,\quad +h,\quad +1,\quad +10;$$

получим следующие результаты

x	$f(x)$	$f'(x)$	$f''(x)$	$f'''(x)$	$f^{IV}(x)$	$f^{V}(x)$	$f^{VI}(x)$
-10	$+$	$-$	$+$	$-$	$+$	$-$	$+$
-1	$-$	$-$	$+$	$-$	$+$	$-$	$+$
$-h$	$-$	$+$	$+$	$-$	$+$	$-$	$+$
$+h$	$-$	$+$	$+$	$+$	$+$	$-$	$+$
$+1$	$-$	$+$	$+$	$+$	$+$	$-$	$+$
$+10$	$+$	$+$	$+$	$+$	$+$	$+$	$+$

.

Так как мы замечаем в промежутке $(-10, 10)$ шесть потерь перемен знака, то отсюда заключаем. что все действительные корни заключены между числами -10 и $+10$.

Между -10 и -1 произошла одна потеря перемены знака, следовательно, между этими числами существует всего один корень, который таким образом отделен.

Между $-h$ и h мы замечаем две потери, что показывает, что существуют два мнимых корня.

Наконец, между $+1$ и $+10$ три потери, следовательно, между этими границами находится один или три действительных корня.

Ряд указателей функций $f(x)$, отнесенный к промежутку между числами 1 и 10, есть

$$3,\quad 2,\quad 2,\quad 2,\quad 2,\quad 1,\quad 0;$$

вычислением находим, что

$$\frac{f^{IV}(10)}{f^{V}(10)} - \frac{f^{IV}(1)}{f^{V}(1)} < 10 - 1.$$

Этот результат показывает, что промежуток между 1 и 10 слишком значителен, чтобы можно было судить о природе корней по одной только операции.

Прежде чем уменьшить этот промежуток, нужно посмотреть, не имеет ли уравнение $f^{IV}(x) = 0$ равных корней между 1 и 10. Действительно, мы замечаем, что $x-2$ есть общий делитель между $f^{V}(x)$ и $f^{IV}(x)$; с другой стороны этот бином не делит функций

$$f'''(x), \quad f''(x), \quad f'(x), \quad f(x),$$

предшествующих $f^{IV}(x)$; значить, можно будет уменьшить на 2 пять первых указателей. Получим новый ряд

$$1, \quad 0, \quad 0, \quad 0, \quad 0, \quad 1, \quad 0,$$

который показывает, что отделение корней закончено. Итак, предложенное уравнение имеет только два действительных корня; один между -10 и -1, другой между $+1$ и $+10$.

Теорема Newton'a. Доказательство Sylvester'a

§ 29

В заключение упоминаем об одной теорем Newton'a.[47] Эта теорема была дана без доказательства и доказана была в первый раз Sylvester'ом.[48]

Рассмотрим уравнение

$$p_0 x^n + p_1 x^{n-1} + p_2 x^{n-2} + \ldots + p_n = 0$$

с вещественными коэффициентами.

Составим два ряда чисел

$$(1) \qquad \begin{array}{c} p_0, \ p_1, \ p_2, \ \ldots, \ p_n, \\ q_0, \ q_1, \ q_2, \ \ldots, \ q_n, \end{array}$$

при чем первый ряд составлен из коэффициентов заданного уравнения, а второй ряд указан формулами

$$q_0 = q_n = 1, \quad q_i = p_i^2 - \frac{(i+1)(n-i+1)}{i(n-i)}\, p_{i-1} p_{i+1}.$$

Каждые четыре числа

$$(2) \qquad \begin{array}{cc} p_i & p_{i+1} \\ q_i & q_{i+1} \end{array}$$

[47] Is. Newton. Arithmetica universalis.

[48] Sylvester. Transactions of R. Irish. Acad. t. 24 (1871).

представляюсь относительно знаков один из шестнадцати случаев

$$\begin{array}{ll} a) & \begin{matrix}++\\++\end{matrix},\ \begin{matrix}++\\--\end{matrix},\ \begin{matrix}--\\++\end{matrix},\ \begin{matrix}--\\--\end{matrix},\\ b) & \begin{matrix}++\\+-\end{matrix},\ \begin{matrix}++\\-+\end{matrix},\ \begin{matrix}--\\+-\end{matrix},\ \begin{matrix}--\\-+\end{matrix},\\ c) & \begin{matrix}+-\\+-\end{matrix},\ \begin{matrix}+-\\-+\end{matrix},\ \begin{matrix}-+\\+-\end{matrix},\ \begin{matrix}-+\\-+\end{matrix},\\ d) & \begin{matrix}+-\\++\end{matrix},\ \begin{matrix}+-\\--\end{matrix},\ \begin{matrix}-+\\++\end{matrix},\ \begin{matrix}-+\\--\end{matrix}. \end{array}$$

Эти случаи мы будем указывать следующими выражениями и символами.

a) Постоянство — постоянство $\ldots PP$,
b) Постоянство — перемена $\ldots PV$,
c) Перемена — перемена $\ldots VV$,
d) Перемена — постоянство $\ldots VP$.

Теорема Newton'a. *Число положительных корней уравнения не превосходит числа VP в рядах* (1)*, а если меньше, то на число четное.*

Число отрицательных корней не превосходит числа PP, а если меньше, то на четное число.

Доказательство Sylvester'a состоит в том, что он доказывает новую теорему, из которой теорема Newton'a получается таким же образом, как теорема Descartes'a из теоремы Budan'a.

Теорема Sylvester'a. *Пусть будет задано уравнение n-ой степени $f(x) = 0$. Полагая*

$$F(x) = [f(x)]^2, \quad F_n(x) = [f^{(n)}(x)]^2,$$

$$F_i(x) = [f^{(i)}(x)]^2 - \frac{n-i+1}{n-i} f^{(i-1)}(x) f^{(i+1)}(x),$$

оставим два ряда функций

$$\begin{matrix} f(x), & f'(x), & f''(x), & \ldots, & f^{(n)}(x), \\ F(x), & F_1(x), & F_2(x), & \ldots, & F_n(x). \end{matrix} \tag{3}$$

Число лежащих между a и b корней $f(x)$ или равно или на четкое число меньше, чем число потерь перемен — постоянств VP в рядах (3) *при переходе от a к $b > a$.*

Число лежащих между a и b корней $f(x)$ или равно или на четное число меньше, чем число приобретений постоянств — постоянств PP в рядах (3) *при переходы от a к $b > a$.*

Мы получим из теоремы Sylvester'a теорему Newton'a, если применим теорему к промежутку $(0, \infty)$, ибо

$$F_i(0) = (1 \cdot 2 \cdots i)^2 \left[p_{n-1}^2 - \frac{(n-i+1)(i+1)}{(n-i)i} p_{n-i-1} p_{n-i+1} \right].$$

Мы не будем останавливаться на доказательстве теоремы Sylvester'a. Читатель найдет подробное доказательство в книге Юл. Сохоцкого. *Высшая алгебра.* Более

короткое доказательства можно найти в книге H. Weber'a, Lehrbuch der Algebra, а также в книге Petersen, Théorie des équations algébriques 1897. Лучше же всего посоветовать обратиться к мемуару самого Sylvester'a.

Теоремы Sylvester'a и Newton'a часто в приложениях дают лучшие результаты чем теоремы Budan'a и Descartes'a, ибо по этим теоремам может получиться более низкий предел для числа корней, заключающихся в данном промежутков. Это понижение предела происходит потому, что при теореме Budan'a рассматриваются только перемены знака первого ряда функций, а при теореме Sylvester'a откидываются из них те, при которых второй ряд дает также перемену знака. Указанному преимуществу теоремы Sylvester'a перед теоремой Budan'a я придаю мало значения, ибо я лично считаю сомнительным практическое значение всех приемов отделения корней вместе взятых.

Глава XI

Теорема Sturm'a

§ 1

Будем рассматривать уравнение $f(x) = 0$ с вещественными коэффициентами и простыми корнями. Обозначая для сокращения $f(x)$ через V, мы заметим, что у функции V и ее производной V' не будет общих делителей.

Будем относительно функции V и V' производить выкладку нахождения общего наибольшего делителя при помощи последовательного деления.

От деления V на V' получим остаток, степень которого не выше $n-2$, где n — степень функции V.

Изменим знаки у всех членов остатка; тогда остаток обратится в функцию, которую назовем V_2.

Будем делить производную V' на V_2 и обозначим через V_3 остаток с измененным знаком. Затем будем делить функцию V_2 на функцию V_3 и продолжать деление далее, изменяя всякий раз знак у остатка.

Получаем ряд остатков

$$V_2,\ \ V_3,\ \ V_4,\ \ldots,\ V_r \qquad (r < n),$$

степени которых убывают. Последний остаток V_r должен быть постоянным числом, ибо V и V' не имеют общих делителей.

Указанный способ вычисления приводит к ряду функций

$$V,\ \ V',\ \ V_2,\ \ V_3,\ \ldots,\ V_r, \tag{1}$$

который мы для сокращения будем называть *рядом функций Sturm'a*, соответствующим функции V.

Обозначая через

$$Q_1,\ \ Q_2, \ldots,\ Q_{r-1}$$

частные в последовательном делений, получим между функциями Sturm'a соотношения

$$V = V'Q_1 - Q_2,\ \ V' = V_2Q_2 - V_3,\ \ldots,\ V_{r-2} = V_{r-1}Q_{r-1} - V_r.$$

§ 2

Подставим некоторое вещественное число α вместо x в ряд функции Sturm'a и напишем ряд знаков результатов подстановки в таком же порядке, в каком расположены функции Sturm'a.

Будем называть число перемен знака в ряду функции Sturm'a, получающихся после подстановки числа α — числом перемен, соответствующим α.

Теорема Sturm'a

§ 3

Число перемен знака в ряду функций Sturm'a, соответствующих меньшему числу α, не менее числа перемен, соответствующих большему числу β; при чем число потерь перемен знака при переходы от α к β точно равно числу вещественных корней функции $V = f(x)$, заключающихся между числами α и β.

Применяя соображения, аналогичные тем, которые мы производили при доказательстве теоремы Budan'a (см. § 12 глава X), мы должны будем заставлять независимую переменную x непрерывно возрастать от α до β. При этом мы должны принимать во внимание изменение знака всякой функции V, если только переменная x перейдет через корень этой функции.

Придется рассматривать два предположения: 1)изменение числа перемен знака при переходе через корень первой функций V, 2) изменение числа перемен знака при переходе через корень одной из промежуточных функций $V', V_2, \ldots, V_{r-1}$ (V_r — не меняет знака, как число постоянное).

Докажем, что при переходе независимой переменной x через корень функции V всегда теряется одна перемена знака.

На основании теоремы § 9 главы X замечаем, что отношение

$$\frac{V}{V'}$$

при переходе x через корень a от меньших значений к большим переходит от отрицательных значений к положительным; значит, для значений $x = a + h$ будем иметь при достаточно малых по абсолютной величин значениях h неравенства

$$h < 0, \quad \frac{V}{V'} < 0,$$
$$h > 0, \quad \frac{V}{V'} > 0.$$

Итак, мы видим, что две функций V и V' разных знаков при значениях x меньших корня a и достаточно близких к нему и одного знака при значениях x, непосредственно следующих за корнем a уравнения $V = 0$. Итак, до корня a первые два знака в ряду Sturm'a будут давать перемену, после же корня — повторение и, следовательно, при переходе через корень уравнения $V = 0$ происходит потеря одной перемены знака в ряду Sturm'a, если пока не обращать внимания на то, что происходить в следующих функциях ряда Sturm'a.

Покажем теперь, что при переходе через корень одной из промежуточных функций не происходит изменения числа перемен знаков. В самом деле, не трудно убедиться, что для значения b, обращающего в нуль функцию V_m, не могут обращаться в нуль рядом стоящие функции V_{m-1} и V_m. Предположим обратное, т. е., что при $x = b$ две рядом стоящие функции V_{m-1} и V_m обращаются в нуль. Тогда на основании равенства

$$V_{m-1} = V_m Q_m - V_{m+1} \tag{1}$$

должна обратиться в нуль при $x = b$ и следующая функция V_{m+1}. Прилагая подобное рассуждение, заметим, что обращаются в нуль все следующие функции $V_{m+2}, V_{m+3}, \ldots, V_r$, что невозможно, ибо V_r отличное от нуля постоянное число.

Полагая в равенстве (1) $x = b$, где b корень функции V_m, мы получим

$$V_{m-1} = -V_{m+1}$$

и, следовательно, результаты подстановок корня b в рядом стоящие функций V_{m-1} и V_{m+1} разных знаков. Отсюда мы видим, что, какие бы знаки ни имела функция V_m при значениях x соседних по обе стороны с корнем b, в ряду функции

$$V_{m-1}, \quad V_m, \quad V_{m+1}$$

будет всегда одна перемена знака, ибо крайние функции — разных знаков, а знак средней (при $x = b-h$ и $x = b+h$) будет в обоих случаях совпадать со знаком одной из крайних. Итак, мы видим, что при переходе через корень одной из средних функций не происходит изменения перемен знака в ряду Sturm'a.

Резюмируя все сказанное, мы видим, что при непрерывном возрастании x от α до β могут происходить изменения числа перемен знака только при переходе x через корень первой функций V, причем при переходе через каждый корень происходить одна потеря перемены знака в первых двух функциях. Следовательно, общее число потерь перемен знака при изменении x от α до β будет равно числу корней функции V, заключенных в промежутке от α до β.

§ 4

По поводу доказанной теоремы упомянем о трех замечаниях, принадлежащих самому Sturm'у.

1-ое замечание. При последовательном вычислении остатков имеем право умножать или делить на произвольные положительные числа все делимые и все делители; от этого функции Sturm'a получать положительные множители, что не отразится на их знаках. Надо избегать лишь введения отрицательных множителей.

2-ое замечание. Условие, чтобы последняя функция V_r обязательно была постоянным числом, не играет никакой роли в доказательстве. Доказательство предполагает только, что последняя функция V_r не меняет знака, когда x изменяется от α до β. Отсюда следует, что если какая нибудь промежуточная функция V_i, не имеет корня между α и β, то на этой функций можно оборвать ряд Sturm'a и следующих функции $V_{i+1}, V_{i+2}, \ldots, V_r$ не рассматривать.

3-е замечание. Может случиться, что для одного из пределов α, β обращается в нуль одна или несколько функций Sturm'a; это обстоятельство не производить однако никакого недоразумения при счете числа перемен знака. Достаточно заменить в этом случае α на $\alpha - h$ и β на $\beta + h$, где h сколь угодно малая величина. Если первая функция V обращается в нуль для одного из пределов α или β, то две первые функций V, V' будут представлять перемену знака при $x = \alpha - h$ и постоянство знака при $x = \beta + h$. Что касается обращения в нуль при α или β одной из промежуточных функций V_i, то при $x = \alpha - h$ или $x = \beta + h$ будет одна только перемена знака в ряде трех функций V_{i-1}, V_i, V_{i+1}. Практически дело сводится к отбрасыванию функций V_i равной нулю, ибо ту же самую одну перемену знака представляет последовательность V_{i-1}, V_{i+1}.

§ 5

Теорема Sturm'a прилагается без видоизменения также к случаю уравнений, имеющих кратные корни. При этом необходимо кратный корень считать за один.

В самом деле, пусть $X = 0$ будет подлежащее изучению уравнение с кратными корнями, и обозначим через X' производную его первой части. Будем искать при помощи последовательного деления общий наибольший делитель функции X и ее производной X', не позабывая менять знак у всякого остатка. Мы получим ряд функций

$$X,\ \ X',\ \ X_2, \ldots,\ X_{r-1},\ \ X_r, \tag{1}$$

из которых последняя не будет постоянною, а будет общим наибольшим делителем функций X, X' и будет, следовательно, делить все остальные функции.

Между функциями (1) существуют соотношения

$$X_{i-1} = X_i Q_i - X_{i+1}, \tag{2}$$

где Q_i целая функция.

Если мы обозначим через D произведение общих линейных множителей D и D', то деля на D все функции ряда (1), получим ряд следующих целых функций

$$V,\ \ V_1,\ \ V_2,\ \ldots,\ V_{r-1},\ \ V_r, \tag{3}$$

из которых последняя приводится к постоянному числу. Ряд (3) удовлетворяет всем свойствам теоремы Sturm'a, ибо во первых на основании (2) будут иметь место соотношения

$$V_{i-1} = V_i Q_i - V_{i+1},$$

а кроме того отношеник $\dfrac{V}{V_1} = \dfrac{X}{X'}$ по теореме § 9 главы X переходить через корень функции X всегда от отрицательных значений к положительным. Итак, число корней X в промежутке α, β можно исследовать по переменам знака в ряде (3), но число перемен знака в этом ряде тоже, что и в ряде (1), функции которого отличаются от функции (3) одним и тем же множителем D.

Таким образом ряд (3) можно заменить рядом (1).

§ 6

Поясним теорему Sturm'a на примере. Найдем число вещественных корней уравнения

$$(x + a)^p (x - a)^q = b, \tag{1}$$

где a положительное число, p и q числа, натуральные, а b вещественное число, которое может быть как положительным, так и отрицательным.

Для нахождения числа всех вещественных корней уравнения (1) достаточно принять $\alpha = -\infty$, $\beta = +\infty$.

Итак будем наследовать корни функции

$$V = (x + a)^p (x - a)^q - b;$$

ее производная будет

$$V' = (x+a)^{p-1}(x-a)^{q-1}\{(p+q)x-(p-q)a\}.$$

Деля V на V' и изменяя знак у остатка, получим

$$V_2 = (x+a)^{p-1}(x-a)^{q-1} + \frac{b}{a^2}\,\frac{(p+q)^2}{4pq}.$$

Деля далее V' на V_2 и продолжая процесс последовательного деления, получим остальные две функции Sturm'a

$$V_3 = b\{(p+q)x-(p-q)x\},$$

$$V_4 = (-1)^q\,\frac{p^pq^q}{(p+q)^{p+q}} - \frac{b}{(2a)^{p+q}}.$$

Разберём отдельно четыре случая.

I) p — четное, q — четное.

α) $b > 0$.

1) $\dfrac{b}{(2a)^{p+q}} < \dfrac{p^pq^q}{(p+q)^{p+q}}$:

	V	V'	V_2	V_3	V_4	Число перемен	
$+\infty$	$+$	$+$	$+$	$+$	$+$	0	4 вещественных корня
$-\infty$	$+$	$-$	$+$	$-$	$+$	4	

2) $\dfrac{b}{(2a)^{p+q}} > \dfrac{p^pq^q}{(p+q)^{p+q}}$:

	V	V'	V_2	V_3	V_4	Число перемен	
$+\infty$	$+$	$+$	$+$	$+$	$-$	1	2 вещественных корня
$-\infty$	$+$	$-$	$+$	$-$	$-$	3	

3) $\dfrac{b}{(2a)^{p+q}} = \dfrac{p^pq^q}{(p+q)^{p+q}}$:

	V	V'	V_2	V_3	V_4	Число перемен	
$+\infty$	$+$	$+$	$+$	$+$	0	0	3 вещественных корня
$-\infty$	$+$	$-$	$+$	$-$	0	3	

В этом случае $V_4 = 0$, следовательно, корень

$$x = \frac{p-q}{p+q}\,a$$

функции V_3 будет двукратным корнем V.

β) $b < 0$:

	V	V'	V_2	V_3	V_4	Число перемен	
$+\infty$	$+$	$+$	$+$	$-$	$+$	2	Нет вещественных корней
$-\infty$	$+$	$-$	$+$	$+$	$+$	2	

Остальные случаи укажем, не выписывая подробно знаков функций Sturm'a.

II) p — нечетное, q — четное.

α) $b > 0$.

1) $\dfrac{b}{(2a)^{p+q}} < \dfrac{p^p q^q}{(p+q)^{p+q}}$: 3 вещественных корня.

2) $\dfrac{b}{(2a)^{p+q}} > \dfrac{p^p q^q}{(p+q)^{p+q}}$: один вещественный корень.

3) $\dfrac{b}{(2a)^{p+q}} = \dfrac{p^p q^q}{(p+q)^{p+q}}$: 1 двукратный корень $\dfrac{p-q}{p+q}\,a$.

β) $b < 0$; один вещественный корень.

III) p — четное, q — нечетное.

α) $b > 0$; один вещественный корень.

β) $b < 0$.

1) $\dfrac{b}{(2a)^{p+q}} < \dfrac{p^p q^q}{(p+q)^{p+q}}$: 3 вещественных корня.

2) $-\dfrac{b}{(2a)^{p+q}} > \dfrac{p^p q^q}{(p+q)^{p+q}}$: один вещественный корень.

3) $-\dfrac{b}{(2a)^{p+q}} = \dfrac{p^p q^q}{(p+q)^{p+q}}$: 1 двукратный корень $\dfrac{p-q}{p+q}\,a$.

IV) p — нечетное, q — нечетное.

α) $b > 0$. Два вещественных корня.

β) $b < 0$

1) $-\dfrac{b}{(2a)^{p+q}} < \dfrac{p^p q^q}{(p+q)^{p+q}}$: 2 вещественных корня.

2) $-\dfrac{b}{(2a)^{p+q}} > \dfrac{p^p q^q}{(p+q)^{p+q}}$: нет корней.

3) $-\dfrac{b}{(2a)^{p+q}} = \dfrac{p^p q^q}{(p+q)^{p+q}}$: 1 двукратный корень $\dfrac{p-q}{p+q}\,a$.

Итак, мы видим, что данное уравнение не может иметь более 4-х вещественных корней.

§ 7

Теорема Sturm'a может быть изменена таким образом, что вместо последовательных остатков от деления функции на ее производную можно за функции Sturm'a выбирать полиномы, составляемые другим образом. Такое видоизменение увеличивает практическое и теоретическое значение теоремы Sturm'a. Нетрудно видеть, что при доказательстве теоремы Sturm'a играло роль не то обстоятельство, что функции Sturm'a составлялись последовательным делением, а следующие четыре свойства функций Sturm'a:

1) последняя функция V_r не меняет своего знака между рассматриваемыми пределами;

2) когда при некотором значении $x = a$ обращается в нуль одна из промежуточных функций, то рядом стоящие по обе стороны функции должны принимать значения разных знаков;

3) ни для какого частного значения x в данном промежутка не могут обратиться в нуль две рядом стоящие функции Sturm'a;

4) при переходе через корень первой функции V от значений меньших к большим отношение $\frac{V}{V_1}$, где V_1 вторая функция ряда Sturm'a, может и не быть производною от V, переходит от отрицательных к положительным.

Очевидно, что, каким бы образом ни составлен был ряд функций

$$V,\ \ V_1,\ \ V_2,\ \ldots,\ V_r, \tag{1}$$

число корней первой функций V, лежащих между α и $\beta > \alpha$, равняется числу потерь перемен знака при переход от α к β, если только функций (1) удовлетворяют, поставленным выше четырем свойствам.

§ 8

Часто могут быть употреблены с пользой ряды функций, неудовлетворяющие указанным четырем свойствам. Мы рассмотрим случай приложения таких рядов, которые, удовлетворяя трем первым свойствам, не удовлетворяют четвертому.

В самом деле, если отношение

$$\frac{V}{V_1}$$

переходить через нуль, как от положительных значений к отрицательным, так и от отрицательных к положительным, то в ряду функций Sturm'a при изменении x от α до β может произойти одно из трех: или число перемен знака не изменится, или произойдешь потеря некоторого числа перемен, или же, наконец, увеличение числа перемен; при этом всегда будет происходить потеря перемен знака при переходе через корень функций V, при котором отношение $\frac{V}{V_1}$ переходит от отрицательных значений к положительным, и, наоборот, одно приобретение перемены знака при переход через корень другой категории, а именно такой, что отношение переходит от положительных значений к отрицательным.

Если при переходе через корень V отношение $\frac{V}{V_1}$ не меняет знака, то не происходит изменения числа перемен знака.

Назовем корень *принадлежащим к первой категории*, если отношение (1) переходит от положительных значений к отрицательным, и обратно назовем его *принадлежащим ко второй категории*, если отношение (1) переходит от отрицательных значений к положительным.

Пусть Δ обозначает избыток числа корней первой категории над числом корней второй.

Если через k обозначить натуральное число, на которое изменится число перемен знака в ряде Sturm'a при переходе от α к β, то очевидно, будем иметь

$$\Delta = \pm k,$$

где знак + должен быть, когда ряд Sturm'a *приобретает* k перемен при изменении x от α до β, и знак $-$, когда теряется k перемен.

Если число k равняется n, степени функций V, то, очевидно, что уравнение $V = 0$ имеет все корни вещественные и кроме того при непрерывном изменении x от α до β отношение (1), проходя через нуль, переходит всякий раз или от

отрицательных значений к положительным ($\Delta = -n$) или же всякий раз от положительных значений к отрицательным ($\Delta = +n$). Отсюда следует, что между двумя последовательными корнями функций V должен существовать по крайней мере один корень функций V_1. Если эта последняя функция имеет степень $n-1$, то ее корни перемежаются с корнями $V = 0$.

§ 9

Рассмотрим теперь условия необходимые и достаточные, для того чтобы при обыкновенном применении теоремы Sturm'a уравнение $V = 0$ имело все корни вещественные.

Обозначим через k число перемен знака в ряду Sturm'a при $x = -\infty$, а через k_1 число перемен знака при $x = +\infty$.

Для числа вещественных корней мы получаем выражение

$$k - k_1.$$

Если все n корней функций V вещественны, то получим

$$k - k_1 = n. \tag{1}$$

Если ряд Sturm'a есть

$$V,\ \ V',\ \ V_2,\ \ldots,\ V_r,$$

то числа k и k_1 не могут превосходить числа r; но $r \leq n$, следовательно, равенству (1) возможно не иначе удовлетворить, как полагая

$$k = n, \qquad k_1 = 0,$$

ибо, если $k_1 > 0$, то для числа k получим значение большее n, что невозможно. Отсюда выводим $r = n$, то есть, *для функции V, имеющей все вещественные корни, ряд функций Sturm'a должен обязательно состоять из $n+1$ функций*, ибо при $x = -\infty$ число перемен знака k должно равняться n и, следовательно, число самих функций должно быть $n+1$.

Кроме того, ряд функций Sturm'a не должен иметь перемен знака при $x = +\infty$, и, следовательно, во всех функциях Sturm'a коэффициенты при старших членах должны быть числа положительные, если мы предположим, что коэффициент p_0 старшего члена функции V число положительное. Так как коэффициенты старших членов функций V и ее производной V' суть p_0 и np_0, то условия, необходимые и достаточные для вещественности всех корней функций V, будут состоять в том, чтобы старшие коэффициенты всех остальных $n-1$ функций Sturm'a были числами положительными.

Получаются таким образом $n-1$ неравенств между коэффициентами функций V. Из этих неравенств некоторые могут быть следствиями остальных, так что число условий может быть меньше $n-1$.

Для примера рассмотрим уравнение 3-ей степени

$$V = x^3 + px + q,$$

$$V' = 3x^2 + p.$$

Будем делить V на V', и, чтобы не вводить дробных чисел, умножим, согласно замечании 2 § 4, функций V на 3

$$\begin{array}{r|l} 3x^3+3px+3q & 3x^2+p \\ \hline 3x^3+px & x \\ \hline 2px+3q & \end{array}$$

Отсюда за функций V_2 можем выбрать

$$V_2 = -2px - 3q.$$

Будем делить V' на V_2, умножив предварительно V' на $4p^2$:

$$\begin{array}{r|l} 12p^2x^2+4p^3 & -2px-3q \\ \hline 12p^2x^2+18pqx & -6px+9q \\ \hline -18pqx+4p^3 & \\ -18pqx-27q^2 & \\ \hline 27q^2+4p^3 & \end{array}$$

Отсюда за функций V_3 можно принять $-27q^2 - 4p^3$.

Так как общее число функций в данном случай равно $n+1=4$, то условием вещественности будут неравенства, число которых равно $n-1=2$

$$-2p > 0, \qquad -27q^2 - 4p^3 > 0.$$

Нетрудно видеть, что неравенство $p<0$ есть простое следствие неравенства $27q^2+4p^3<0$, ибо это неравенство, очевидно, не имеет места при p положительном или $p=0$. Итак, для вещественности корней уравнения

$$x^3 + px + q = 0$$

получается одно условие

$$\frac{q^2}{4} + \frac{p^3}{27} < 0,$$

как это мы видели в § 9 Главы III.

Связь с непрерывными дробями

§ 10

По ходу вычисления функций Sturm'a, представляющего алгоритм Эвклида для разложения дроби

$$\frac{f'(x)}{f(x)}$$

в непрерывную, видна связь теоремы Sturm'a с теорией непрерывных дробей. Углубимся несколько более в эту связь, причем начнем с замечательных исследований академика А. Маркова,[49] публикованных в мемуаре «О функциях, получаемых при обращении рядов в непрерывные дроби» 1894.

[49]Приложение к LXXIV тому Записок Импер. Академии Наук.

Будем рассматривать бесконечный ряд

$$f = \frac{s_0}{x} + \frac{s_1}{x^2} + \frac{s_2}{x^3} + \dots$$

причем предположим, что $s_0 \neq 0$.

Рассматривая обратную функцию, получим

$$\frac{1}{f} = \frac{1}{\frac{s_0}{x} + \frac{s_1}{x^2} + \frac{s_2}{x^3} + \dots} = \frac{\frac{x}{s_0}}{1 + \frac{s_1}{s_0}\frac{1}{x} + \frac{d_2}{s_0}\frac{1}{x^2} + \dots} =$$

$$= \frac{x}{s_0}\left\{1 - \frac{s_1}{s_0}\frac{1}{x} - \frac{s_2}{s_0}\frac{1}{x^2} - \dots + \left(\frac{s_1}{s_0}\frac{1}{x} + \frac{s_2}{s_0}\frac{1}{x^2} + \dots\right)^2 - \dots\right\} = q_1 - f_1,$$

где

$$q_1 = \frac{1}{s_0}x - \frac{s_1}{s_0^2}, \qquad f_1 = \frac{\sigma_0}{x} + \frac{\sigma_1}{x^2} + \frac{\sigma_2}{x^3} + \dots$$

где

$$\sigma_0 = \frac{1}{s_0^2}\begin{vmatrix} s_0 & s_1 \\ s_1 & s_2 \end{vmatrix}.$$

Если $\sigma_0 \neq 0$, то подобным же образом получим

$$\frac{1}{f_1} = q_2 - f_2,$$

где

$$q = \frac{1}{\sigma_0}x - \frac{\sigma_1}{\sigma_0^2}.$$

Продолжая далее, разложим f в непрерывную дробь

$$f = \cfrac{1}{q_1 - \cfrac{1}{q_2 - \cfrac{1}{q_3 - \ddots}}}.$$

Параметрам

$$s_0, \quad s_1, \quad s_2, \dots, \quad s_{2m-2}, \quad s_{2m-1}$$

мы будем давать вещественные значения; при том только такие, чтобы ни один из определителей

$$\Delta_1 = s_0, \quad \Delta_2 = \begin{vmatrix} s_0 & s_1 \\ s_1 & s_2 \end{vmatrix}, \quad \Delta\begin{vmatrix} s_0 & s_1 & s_2 \\ s_1 & s_2 & s_3 \\ s_2 & s_3 & s_4 \end{vmatrix}, \ \dots,$$

$$\Delta_m = \begin{vmatrix} s_0 & s_1 & s_2 & \dots & s_{m-1} \\ s_1 & s_2 & s_3 & \dots & s_m \\ \dots & \dots & \dots & \dots & \dots \\ s_{m-1} & s_m & s_{m+1} & \dots & s_{2m-2} \end{vmatrix}$$

не обращался в нуль.

Мы будем в дальнейшем изложений употреблять обозначение

$$\Delta_m = |s_i|_m.$$

В таком случае

$$q_1,\ \ q_2,\ \ldots,\ q_k,\ \ldots,\ q_m$$

целые функции первой степени относительно x.

Обращая дроби

$$\frac{1}{q_1},\ \ \frac{1}{q_1 - \dfrac{1}{q_2}},\ \ldots,\ \frac{1}{q_1 - \dfrac{1}{q_2 - \ddots - \dfrac{1}{q_k}}},\ \ldots,\ \frac{1}{q_1 - \dfrac{1}{q_2 - \ddots - \dfrac{1}{q_m}}}$$

в обыкновенные

$$\frac{\varphi_1(x)}{\psi_1(x)},\ \ \frac{\varphi_2(x)}{\psi_2(x)},\ \ldots,\ \frac{\varphi_k(x)}{\psi_k(x)},\ \ldots,\ \frac{\varphi_m(x)}{\psi_m(x)},$$

мы можем получить

$$\psi_k(x) = P_{0,k} + P_{1,k}x + P_{2,k}x^2 + \ldots + P_{k,k}x^k$$

и определять отношения

$$\frac{P_{0,k}}{P_{k,k}},\ \ \frac{P_{1,k}}{P_{k,k}},\ \ldots,\ \frac{P_{k-1,k}}{P_{k,k}}$$

из уравнений

$$\begin{gathered}
s_0P_{0,k} + s_1P_{1,k} + s_2P_{2,k} + \ldots + s_{k-1}P_{k-1,k} + s_kP_{k,k} = 0,\\
s_1P_{0,k} + s_2P_{1,k} + s_3P_{2,k} + \ldots + s_kP_{k-1,k} + s_{k+1}P_{k,k} = 0,\\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
s_{k-1}P_{0,k} + s_kP_{1,k} + s_{k+1}P_{2,k} + \ldots + s_{2k-2}P_{k-1,k} + s_{2k-1}P_{k,k} = 0.
\end{gathered}$$

Эти уравнения получаются из того соображения, что выражение

$$\psi_k(x)\left\{\frac{s_0}{x} + \frac{s_1}{x^2} + \frac{s_2}{x^3} + \ldots\right\}$$

не должно заключать членов

$$\frac{1}{x},\ \ \frac{1}{x^2},\ \ldots,\ \frac{1}{x^k},$$

т. е. другими словами должно быть

$$\psi_k(x)f = \varphi_k(x) + \frac{\alpha}{x^{k+1}} + \frac{\beta}{x^{k+2}} + \ldots,$$

ибо[50]

$$f - \frac{\varphi_k(x)}{\psi_k(x)} = \frac{\pm 1}{\psi_k(x)\{\varphi_k(x)(q_{k+1} - f_{k+1}) - \varphi_{k-1}(x)\}}.$$

[50]Д. Граве. Элементарный курс теории чисел. 1913 г. Второе изд. Стр. 187.

Решая уравнение (1), получим

$$P_{ik} = \frac{(-1)^{k-i} P_{k,k}}{\Delta_k} \begin{vmatrix} s_0 & s_1 & \dots & s_{i-1} & s_{i+1} & \dots & s_k \\ s_1 & s_2 & \dots & s_i & s_{i+2} & \dots & s_{k+1} \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ s_{k-1} & s_k & \dots & s_{k+i-2} & s_{k+i} & \dots & s_{2k-1} \end{vmatrix}.$$

Когда функция $\psi_k(x)$ составлена, нетрудно уже составить и функцию

$$\varphi_k(x) = Q_{0,k} + Q_{1,k}x + Q_{2,k}x^2 + \ldots + Q_{k-1,k}x^{k-1},$$

которая должна быть равна целой части произведения $\psi_k(x)f$.

Именно, в силу только что указанного требования можем написать следущие формулы

$$\begin{array}{rcl} Q_{0,k} & = & s_0P_{1,k} + s_1P_{2,k} + \ldots + s_{k-1}P_{k,k}, \\ Q_{1,k} & = & s_0P_{2,k} + \ldots + s_{k-2}P_{k,k}, \\ \multicolumn{3}{c}{\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots,} \\ Q_{k-1,k} & = & s_0P_{k,k}. \end{array} \tag{2}$$

Коэффициент $P_{k,k}$ остается пока неопределенным. Конечно эта неопределенность пропадает в выражений дроби

$$\frac{\varphi_k(x)}{\psi_k(x)}.$$

Если же мы хотим, чтобы числитель и знаменатель дроби получались по известным формулам

$$\begin{array}{c} \psi_1(x) = q_1, \quad \psi_2(x) = q_2\psi_1(x) - 1, \ \ldots, \ \psi_m(x) = q_m\psi_{m-1}(x) - \psi_{m-2}(x), \\ \varphi_1(x) = 1, \quad \varphi_2(x) = q_2, \ \ldots, \ \varphi_m(x) = q_m\varphi_{m-1}(x) - \varphi_{m-2}(x), \end{array} \tag{3}$$

то должны удовлетворить уравнениям следующего вида

$$\begin{array}{c} (s_0P_{1,k} + s_1P_{2,k} + \ldots + s_{k-1}P_{k,k})P_{0,k-1} - \\ -P_{0,k}(s_0P_{1,k-1} + s_1P_{2,k-1} + \ldots + s_{k-2}P_{k-1,k-1}) = 1, \end{array}$$

т. е.

$$\varphi_k(0)\psi_{k-1}(0) - \varphi_{k-1}\psi_k(0) = 1. \tag{4}$$

При рассмотрении последнего уравнения полезно ввести определитель

$$\Delta = \begin{vmatrix} s_0 & s_1 & s_2 & \dots & s_{k-1} & s_k \\ s_1 & s_2 & s_3 & \dots & s_k & s_{k+1} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ s_{k-1} & s_k & s_{k+1} & \dots & s_{2k-2} & s_{2k-1} \\ 0 & 0 & 0 & \dots & 0 & 1 \end{vmatrix}$$

и его миноры

$$\Delta_{i,j}. \tag{5}$$

Под $\Delta_{i,j}$ мы подразкмеваем произведение $(-1)^{i+j}$ на определитель, получаемый из (3) вычеркиванием $j+1$-ой горизонтали (считая сверху) и $i+1$-ой колонны (считая слева). Заметим кстати, что $\Delta = \Delta_k = \Delta_{k,k}$.

Введя такие обозначения, мы можем представить отношения

$$\frac{P_{0,k}}{P_{k,k}},\ \frac{P_{1,k}}{P_{k,k}},\ \ldots,\ \frac{P_{k-1,k}}{P_{k,k}}$$

под видом дробей

$$\frac{\Delta_{0,k}}{\Delta},\ \frac{\Delta_{1,k}}{\Delta},\ldots,\ \frac{\Delta_{k-1,k}}{\Delta},$$

а отношения

$$\frac{P_{0,k-1}}{P_{k-1,k-1}},\ \frac{P_{1,k-1}}{P_{k-1,k-1}},\ \ldots,\ \frac{P_{k-2,k-1}}{P_{k-1,k-1}}$$

под видом дробей

$$\frac{\Delta_{0,k-1}}{\Delta_{k-1,k-1}},\ \frac{\Delta_{1,k-1}}{\Delta_{k-1,k-1}},\ \ldots,\ \frac{\Delta_{k-2,k-1}}{\Delta_{k-1,k-1}}.$$

Уравнение (2) принимает вид

$$(s_0\Delta_{1,k} + s_1\Delta_{2,k} + \ldots + s_{k-1}\Delta_{k,k})\Delta_{0,k-1} -$$
$$-\Delta_{0,k}(s_0\Delta_{1,k-1} + s_1\Delta_{2,k-1} + \ldots + s_{k-2}\Delta_{k-1,k-1}) = \frac{\Delta_k\Delta_{k-1}}{P_{k,k}P_{k-1,k-1}},$$

или

$$s_0(\Delta_{1,k}\Delta_{0,k-1} - \Delta_{0,k}\Delta_{1,k-1})s_1(\Delta_{2,k}\Delta_{0,k-1} - \Delta_{0,k}\Delta_{2,k-1}) + \ldots$$
$$+s_{k-2}(\Delta_{k-1,k}\Delta_{0,k-1} - \Delta_{0,k}\Delta_{k-1,k-1}) + s_{k-1}(\Delta_{k,k}\Delta_{0,k-1}) = \frac{\Delta_k\Delta_{k-1}}{P_{k,k}P_{k-1,k-1}}. \tag{4}$$

На основании § 41 главы IV, получим

$$\Delta_{1,k}\Delta_{0,k-1} - \Delta_{0,k}\Delta_{1,k-1} = \Delta\begin{vmatrix} s_2 & s_3 & \ldots & s_k \\ s_3 & s_4 & \ldots & s_{k+1} \\ \ldots & \ldots & \ldots & \ldots \\ s_k & s_{k+1} & \ldots & s_{2k-2} \end{vmatrix},$$

$$\Delta_{2,k}\Delta_{0,k-1} - \Delta_{0,k}\Delta_{2,k-1} = -\Delta\begin{vmatrix} s_1 & s_3 & s_4 & \ldots & s_k \\ s_2 & s_4 & s_5 & \ldots & s_{k+1} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ s_{k-1} & s_{k+1} & s_{k+2} & \ldots & s_{2k-2} \end{vmatrix},$$

$$\Delta_{3,k}\Delta_{0,k-1} - \Delta_{0,k}\Delta_{3,k-1} = \Delta\begin{vmatrix} s_1 & s_2 & s_4 & s_5 & \ldots & s_k \\ s_2 & s_3 & s_5 & s_6 & \ldots & s_{k+1} \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ s_{k-1} & s_k & s_{k+2} & s_{k+3} & \ldots & s_{2k-2} \end{vmatrix},$$

$$\Delta_{k-1,k}\Delta_{0,k-1} - \Delta_{0,k}\Delta_{k-1,k-1} = (-1)^{k-2}\Delta\begin{vmatrix} s_1 & s_2 & \ldots & s_{k-2} & s_k \\ s_2 & s_3 & \ldots & s_{k-1} & s_{k+1} \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ s_{k-1} & s_k & \ldots & s_{2k-4} & s_{2k-2} \end{vmatrix},$$

$$\Delta_{k,k}\Delta_{0,k-1} = (-1)^{k-1}\Delta \begin{vmatrix} s_1 & s_2 & \dots & s_{k-1} \\ s_2 & s_3 & \dots & s_k \\ \dots & \dots & \dots & \dots \\ s_{k-1} & s_k & \dots & s_{2k-3} \end{vmatrix},$$

и кроме того

$$s_0 \begin{vmatrix} s_2 & s_3 & \dots & s_k \\ s_3 & s_4 & \dots & s_{k+1} \\ \dots & \dots & \dots & \dots \\ s_k & s_{k+1} & \dots & s_{2k-2} \end{vmatrix} - s_1 \begin{vmatrix} s_1 & s_3 & s_4 & \dots & s_k \\ s_2 & s_4 & s_5 & \dots & s_{k+1} \\ \dots & \dots & \dots & \dots & \dots \\ s_{k-1} & s_{k+1} & s_{k+2} & \dots & s_{2k-2} \end{vmatrix} + \dots +$$

$$+(-1)^{k-1}s_{k-1} \begin{vmatrix} s_1 & s_2 & \dots & s_{k-1} \\ s_2 & s_3 & \dots & s_k \\ \dots & \dots & \dots & \dots \\ s_{k-1} & s_k & \dots & s_{2k-3} \end{vmatrix} = \Delta = \Delta_k = \Delta_{k,k}.$$

Поэтому уравнение (2) или что одно и тоже (4) приводить к следующему равенству

$$\Delta_k^2 = \frac{\Delta_k\Delta_{k-1}}{P_{k,k}P_{k-1,k-1}}. \tag{5}$$

Вместе с тем мы видели в самом начале, что надо положить

$$P_{1,1} = \frac{1}{s_0} = \frac{1}{\Delta_1}$$

для того, чтобы было $\varphi_1(x) = 1$.

Уравнение (5) дает

$$P_{k,k}P_{k-1,k-1} = \frac{\Delta_{k-1}}{\Delta_k}.$$

Отсюда цоследовательно выводим

$$P_{2,2} = \frac{\Delta_1^2}{\Delta_2}, \quad P_{3,3} = \frac{\Delta_2^2}{\Delta_1^2\Delta_3}, \quad P_{4,4} = \frac{\Delta_1^2\Delta_3^2}{\Delta_2^2\Delta_4}$$

и вообще

$$P_{2l,2l} = \frac{\Delta_1^2\Delta_3^2\cdots\Delta_{2l-1}^2}{\Delta_2^2\Delta_4^2\cdots\Delta_{2l-2}^2\Delta_{2l}}, \quad P_{2l+1,2l+1} = \frac{\Delta_2^2\Delta_4^2\cdots\Delta_{2l}^2}{\Delta_1^2\Delta_3^2\cdots\Delta_{2l-1}^2\Delta_{2l+1}}.$$

Таким образом функции $\psi_k(x)$ и $\varphi_k(x)$ нами определены вполне. Наконец мы можем определить

$$q_1, \quad q_2, \ \dots, \ q_k, \ \dots, \ q_m,$$

как целые части дробей

$$\frac{\psi_1(x)}{1}, \quad \frac{\psi_2(x)}{\psi_1(x)}, \ \dots, \ \frac{\psi_k(x)}{\psi_{k-1}(x)}, \ \dots, \ \frac{\psi_m(x)}{\psi_{m-1}(x)}.$$

Не останавливаясь на этом, заметим только, что коэффициент при x в выражении q_k равен отношению

$$\frac{P_{k,k}}{P_{k-1,k-1}}.$$

Обратимся теперь к корням уравнения

$$\psi_k(x) = 0, \tag{6}$$

которые условимся обозначать символом

$$x_{i,k},$$

отличая их друг от друга индексом i.

Исключая из рассмотрения случай кратных корней, будем иметь формулу

$$\frac{\varphi_k(x)}{\psi_k(x)} = \sum \frac{R_{i,k}}{x - x_{i,k}},$$

где

$$R_{i,k} = \frac{\varphi_k(x_{i,k})}{\psi_k'(x_{i,k})}.$$

Разлагая нашу сумму

$$\sum \frac{R_{i,k}}{x - x_{i,k}}$$

в ряд по целым отрицательным степеням x и ограничиваясь теми членами, где $\frac{1}{x}$ входит в степени меньшей чем $2k+1$, мы должны получить

$$\frac{s_0}{x} + \frac{s_1}{x^2} + \frac{s_2}{x^3} + \ldots + \frac{s_{2k-1}}{x^{2k}}.$$

Отсюда вытекают уравнения

$$s_0 = \sum R_{i,k}, \quad s_1 = \sum R_{i,k} x_{i,k}, \quad s_2 = \sum R_{i,k} x_{i,k}^2, \ \ldots, \ s_{2k-1} = \sum R_{i,k} x_{i,k}^{2k-1}.$$

Если мы ограничим параметры

$$s_0, \quad s_1, \quad s_2, \ \ldots, \ s_{2m-2}$$

неравенствами

$$\Delta_1 > 0, \quad \Delta_2 > 0, \ \ldots, \ \Delta_k > 0, \ \ldots, \ \Delta_m > 0,$$

то все коэффициенты

$$P_{1,1}, \quad P_{2,2}, \quad P_{3,3}, \ldots, \ P_{m,m}$$

будут числами положительными и, следовательно, ряд функций

$$\psi_m(x), \quad \psi_{m-1}(x), \quad \psi_{m-2}(x), \ldots, \ \psi_1(x), \quad 1$$

будет обладать всеми свойствами функций Sturm'a и ни одно из уравнений

$$\psi_m(x) = 0, \quad \psi_{m-1}(x) = 0, \ldots, \ \psi_k(x) = 0, \ldots, \ \psi_i(x) = 0$$

не будет допускать *ни мнимых, ни кратных корней.*

На оснований соображений § 8 можно утверждать, что корни всякой функции $\psi_k(x)$ перемежаются с корнями соседних двух $\psi_{k-1}(x)$, $\psi_{k+1}(x)$.

Из формул (1) мы выводим

$$\varphi_m(x)\psi_{m-1}(x) - \psi_m(x)\varphi_{m-1} = \varphi_{m-1}(x)\psi_{m-2}(x) - \psi_{m-1}(x)\varphi_{m-2}(x) =$$

$$= \ldots = \varphi_2(x)\psi_1(x) - \psi_2(x)\varphi_1(x) = 1,$$

так что

$$\varphi_k(x)\psi_{k-1}(x) - \psi_k(x)\varphi_{k-1}(x) = 1, \tag{7}$$

отсюда

$$\varphi_k(x_{i,k})\psi_{k-1}(x_{i,k}) = 1,$$

числа

$$R_{i,k} = \frac{\varphi_k(x_{i,k})}{\psi_k'(x_{i,k})} = \frac{1}{\psi_{k-1}(x_{i,k})\psi_k'(x_{i,k})}$$

будут положительными, так как $\psi_{k-1}(x_{i,k})$ и $\psi_k'(x_{i,k})$ одного знака.

Нетрудно написать условия, чтобы все корни уравнений

$$\psi_m(x) = 0, \quad \psi_{m-1}(x) = 0, \ldots, \ \psi_k(x) = 0, \ldots, \ \psi_1(x) = 0$$

были положительными. Для этой цели ряд чисел

$$\psi_m(0), \quad \psi_{m-1}(0), \ldots, \ \psi_1(0), \quad 1,$$

или что одно и тоже

$$P_{0,m}, \quad P_{0,m-1}, \ldots, \ P_{0,1}, \quad 1,$$

представлял *все* перемены знака.

Нетрудно видеть, что должны иметь место неравенства

$$s_1 > 0, \quad \begin{vmatrix} s_1 & s_2 \\ s_2 & s_3 \end{vmatrix} > 0, \quad \begin{vmatrix} s_1 & s_2 & s_3 \\ s_2 & s_4 & s_4 \\ s_3 & s_4 & s_5 \end{vmatrix} > 0 \quad \text{и т.д.}$$

§ 11

Переходя к случаю разложения в непрерывную дробь

$$\frac{f(x)}{f'(x)},$$

мы получаем, как частный случай, исследования M. Sylvester'a, публикованные без доказательства в Philosophical Magazine (Декабрь 1839). Sturm доказал формулы Sylvester'a в VII томе журнала Liouville'a. В XII томе того же журнала находятся замечательные исследования о том же вопросе Borchardt'a.

Итак, выведем эти результаты из теории Маркова. Мы будем иметь

$$\frac{f'(x)}{f(x)} = \frac{s_0}{x} + \frac{s_1}{x^2} + \frac{s_2}{x^3} + \ldots, \tag{1}$$

причем

$$s_k = x_1^k + x_2^k + \ldots + x_m^k, \tag{2}$$

где $x_1, x_2, \ldots, x_k$ корни уравнения $f(x) = 0$, которое мы предполагаем освобожденным от кратных корней.

В этом случае разложение дроби (1) дает конечную непрерывную дробь, так что последним знаменателем $\psi_m(x)$ подходящих дробей можно считать функцию $f(x)$ и мы приходим к теореме:

Условие необходимое и достаточное для вещественности всех корней уравнения $f(x) = 0$ *состоит в неравенствах*

$$\begin{vmatrix} s_0 & s_1 \\ s_1 & s_2 \end{vmatrix} > 0, \quad \begin{vmatrix} s_0 & s_1 & s_2 \\ s_1 & s_2 & s_3 \\ s_2 & s_3 & s_4 \end{vmatrix} > 0, \ldots, \quad \begin{vmatrix} s_0 & s_1 & s_2 & \ldots & s_{m-1} \\ s_1 & s_2 & s_3 & \ldots & s_m \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ s_{m-1} & s_m & s_{m+1} & \ldots & s_{2m-2} \end{vmatrix} > 0. \tag{3}$$

Очевидно, что

$$\Delta_k = 0$$

при $k > m$.

Обозначим

$$V = f(x), \quad V_1 = f'(x),$$

$$V = V_1 q_1 - V_2, \quad V_1 = V_2 q_2 - V_3, \ldots, \ V_{m-2} = V_{m-1} q_{m-1} - V_m.$$

Мы оставляем в силе предположение $\Delta_i \neq 0$ при $i \leq m$.

Будем иметь

$$\varphi_1(x) = 1, \quad \varphi_2(x) = q_2, \quad \varphi_3(x) = q_2 q_3 - 1,$$

$$\psi_1(x) = q_1, \quad \psi_2(x) = q_1 q_2 - 1, \quad \psi_3(x) = q_1 q_2 q_3 - q_1 - q_3.$$

Получаем формулу

$$V_{k+1} = V_1 \psi_k(x) - V \varphi_k(x) = f'(x)\psi_k(x) - f(x)\varphi_k(x). \tag{4}$$

Это соотношение дает возможность выразить в явном виде V_{k+1}.

§ 12

На оснований (1) и (2) § 10 получаем

$$\varphi_k(x) = \frac{P_{k,k}}{\Delta_k} \begin{vmatrix} 0 & \mu_1(x) & \mu_2(x) & \ldots & \mu_k(x) \\ -s_0 & -s_1 & -s_2(x) & \ldots & -s_k \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ -s_{k-1} & -s_k & -s_{k+1} & \ldots & -s_{2k-1} \end{vmatrix}, \tag{1}$$

где

$$\mu_1(x) = s_0, \quad \mu_i(x) = s_0 x^{i-1} + s_1 x^{i-2} + \ldots + s_{i-1}.$$

Функция $\mu_i(x)$ есть не что иное как целая часть рациональной функции

$$\frac{x^i f'(x)}{f(x)}.$$

Подобным же образом

$$\psi_k(x) = \frac{P_{k,k}}{\Delta_k} \begin{vmatrix} 1 & x & x^2 & \dots & x^k \\ -s_0 & -s_1 & -s_2 & \dots & -s_k \\ \dots & \dots & \dots & \dots & \dots \\ -s_{k-1} & -s_k & -s_{k+1} & \dots & -s_{2k-1} \end{vmatrix}. \tag{2}$$

Преобразуем теперь выражение (2). Умножим первую колонну на $-x$ и приложим ко второй, умножим вторую в ее первоначальном виде на $-x$ и приложим к третьей; продолжая таким образом до последней колонны получим

(3)

$$\psi_k(x) = \frac{1}{\lambda} \begin{vmatrix} s_0x - s_1 & s_1x - s_2 & \dots & s_{k-1}x - s_k \\ \dots & \dots & \dots & \dots \\ s_{k-1}x - s_k & s_kx - s_{k+1} & \dots & s_{2k-2}x - s_{2k-1} \end{vmatrix} = \frac{1}{\lambda_k} \left| \sum \alpha^{i-1}(x-\alpha) \right|_k;$$

сумма $\sum$ распространяется на все корни $\alpha_1, \alpha_2, \dots, \alpha_m$ уравнения $f(x) = 0$, а

$$\lambda_k = \frac{\Delta_k}{P_{k,k}}.$$

Очевидно, что формула (3) представляет $\psi_k(x)$ при помощи произведения двух матриц

$$\begin{Vmatrix} x-\alpha_1 & \dots & x-\alpha_m \\ \alpha_1(x-\alpha_1) & \dots & \alpha_m(x-\alpha_m) \\ \dots & \dots & \dots \\ \alpha_1^{k-1}(x-\alpha_1) & \dots & \alpha_m^{k-1}(x-\alpha_m) \end{Vmatrix} \cdot \begin{Vmatrix} 1 & \dots & 1 \\ \alpha_1 & \dots & \alpha_m \\ \dots & \dots & \dots \\ \alpha_1^{k-1} & \dots & \alpha_m^{k-1} \end{Vmatrix}.$$

Получаем, следовательно, (см. § 26 Главы IV)

$$\psi_k(x) = \frac{1}{\lambda_k} \begin{vmatrix} 1 & 1 & \dots & 1 \\ \alpha_1 & \alpha_2 & \dots & \alpha_k \\ \dots & \dots & \dots & \dots \\ \alpha_1^{k-1} & \alpha_2^{k-1} & \dots & \alpha_k^{k-1} \end{vmatrix}^2 (x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_k).$$

Обозначая дискриминант функции $(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_k)$ через

$$D(\alpha_1, \alpha_2, \dots, \alpha_k) = (\alpha_1-\alpha_2)^2(\alpha_1-\alpha_3)^2\cdots(\alpha_{k-1}-\alpha_k)^2,$$

получим

$$\psi_k(x) = \frac{1}{\lambda_k} \sum D(\alpha_1, \alpha_2, \dots, \alpha_k)(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_k). \tag{4}$$

Здесь сумма распространяется на все сочетания m корней α_i по k.

§ 13

Для вычисления выражения функции V_{k+1} примем в соображение формулу (4) § 11 и формулы (1) и (2) § 12. Будем иметь

$$\frac{V_{k+1}}{f(x)} = \frac{1}{\lambda_k}\begin{vmatrix} \dfrac{f'(x)}{f(x)} & \dfrac{xf'(x)}{f(x)} - \mu_1 & \dfrac{x^2f'(x)}{f(x)} - \mu_2 & \dots & \dfrac{x^kf'(x)}{f(x)} - \mu_k \\ -s_0 & -s_1 & -s_2 & \dots & -s_k \\ \dots & \dots & \dots & \dots & \dots \\ -s_{k-1} & -s_k & -s_{k+1} & \dots & -s_{2k-1} \end{vmatrix}.$$

Имея в виду соотношение

$$\mu_i x + s_i = \mu_{i+1},$$

после простых преобразовать получим

$$\frac{V_{k+1}}{f(x)} = \frac{1}{\lambda_k}\left|\frac{x^if'(x)}{f(x)} - \mu_i(x)\right|.$$

Но известно, что

$$\frac{x^if'(x)}{f(x)} - \mu_i(x) = \sum \frac{\alpha^i}{x-\alpha},$$

следовательно,

$$V_{k+1} = \frac{f(x)}{\lambda_k}\left|\sum \frac{\alpha^i}{x-\alpha}\right|, \tag{1}$$

и мы получаем произведение матриц

$$\left\|\begin{matrix} \dfrac{1}{x-\alpha_1} & \dots & \dfrac{1}{x-\alpha_m} \\ \dfrac{\alpha_1}{x-\alpha_1} & \dots & \dfrac{\alpha_m}{x-\alpha_m} \\ \dots & \dots & \dots \\ \dfrac{\alpha_1^k}{x-\alpha_1} & \dots & \dfrac{\alpha_m^k}{x-\alpha_m} \end{matrix}\right\| \cdot \left\|\begin{matrix} 1 & \dots & 1 \\ \alpha_1 & \dots & \alpha_m \\ \dots & \dots & \dots \\ \alpha_1^k & \dots & \alpha_m^k \end{matrix}\right\|,$$

т. е.

$$V_{k+1} = \frac{1}{\lambda_k}\sum D(\alpha_1, \alpha_2, \dots, \alpha_k, \alpha_{k+1})(x-\alpha_{k+2})\cdots(x-\alpha_m).$$

Эта формула и формула (4) § 12 суть как раз формулы, указанный Sylvester'ом.

§ 14

Множители λ_k выражаются но формулам

$$\lambda_{2k} = \left(\frac{\Delta_2\Delta_4\cdots\Delta_{2k}}{\Delta_1\Delta_3\cdots\Delta_{2k-1}}\right)^2, \qquad \lambda_{2k+1} = \left(\frac{\Delta_1\Delta_3\cdots\Delta_{2k+1}}{\Delta_2\Delta_4\cdots\Delta_{2k}}\right)^2.$$

При вещественных значениях s_i множители суть числа положительные.

Сравнивая коэффициенты при старших степенях в уравнении (4), § 12. получим

$$P_{k,k} = \frac{1}{\lambda_k} \sum D(\alpha_1, \alpha_2, \ldots, \alpha_k);$$

отсюда получаем

$$\Delta_k = \sum D(\alpha_1, \alpha_2, \ldots, \alpha_k),$$

что очевидно на основании возвышения в квадрат матрицы

$$\left\| \begin{array}{ccc} 1 & \ldots & 1 \\ \alpha_1 & \ldots & \alpha_m \\ \ldots\ldots\ldots\ldots\ldots & & \\ \alpha_1^{k-1} & \ldots & \alpha_m^{k-1} \end{array} \right\|.$$

При применении теоремы Sturm'а можно откинуть положительные множители λ_k. Число μ вещественных корней уравнения $V = f(x) = 0$ будет равно числу потерь перемен знака при переход от ряда

$$V(-\infty),\ \ V_1(-\infty), \ldots,\ V_{m-1}(-\infty),\ \ V_m(-\infty) \tag{1}$$

к ряду

$$V(+\infty),\ \ V_1(+\infty), \ldots,\ V_{m-1}(+\infty),\ \ V_m(+\infty). \tag{2}$$

Знаки ряда (1) укажутся рядом величин

$$(-1)^m,\ \ (-1)^{m-1}\Delta_1,\ \ldots,\ -\Delta_{m-1},\ \ \Delta_m, \tag{3}$$

а знаки ряда (2) будут совпадать со знаками ряда

$$1,\ \ \Delta_1,\ \ldots,\ \Delta_{m-1},\ \ \Delta_m. \tag{4}$$

Пусть ξ обозначает число перемен знаков в ряде (3), а η число перемен знаков в ряде (4).

Получаем два равенства

$$\xi - \eta = \mu, \qquad \xi + \eta = m,$$

откуда

$$\mu = m - 2\eta;$$

таким образом мы приходим к теореме: *число пар мнимых корней уравнения* $V = 0$ *равно числу перемен знаков в ряде величин*

$$1,\ \ \Delta_1,\ \ \Delta_2,\ \ldots,\ \Delta_m.$$

Так что, если эти величины все положительные, то мы приходим к нашему прежнему заключению об отсутствии мнимых корней уравнения.

Приложение теоремы Sturm'a к одному классу уравнений

§ 15

Приложим теорему Sturm'a к доказательству вещественности корней одного замечательного уравнения, а именно, характеристического уравнения симметрической матрицы, все элементы которой вещественные

$$(1)\qquad \begin{vmatrix} a_{ii}-g & a_{21} & \dots & a_{n1} \\ a_{12} & a_{22}-g & \dots & a_{n2} \\ \dots & \dots & \dots & \dots \\ a_{1n} & a_{2n} & \dots & a_{nn}-g \end{vmatrix} = 0,$$

где $a_{ik} = a_{ki}$.

Это уравнение заключает как частный случаи уравнение третьей степени, от которого зависит нахождение осей поверхности второго порядка, а также уравнения при помощи которых определяются возмущения эллиптических элементов движения небесных тел.

Дано разными авторами очень много доказательств того, что корни уравнения (1) вещественные. Мы приведем доказательство Borchardt'a,[51] модернизируя несколько его изложение.

Нетрудно составить уравнение, которому будут удовлетворять k-ые степени g^k корней g уравнения (1). На основании теоремы Cayley – Hamilton'a,[52] гласящей, что матрица $\mathfrak{a} = \|a_{ij}\|$ удовлетворяет символически (в смысле действий над матрицами) ее характеристическому уравнению, мы получим уравнение для g^k, если составим характеристическое уравнение для матрицы

$$\mathfrak{a}^k = \|a_{ij}^{(k)}\|,$$

то есть уравнение

$$\begin{vmatrix} a_{ii}^{(k)}-x & a_{21}^{(k)} & \dots & a_{n1}^{(k)} \\ a_{12}^{(k)} & a_{22}^{(k)}-x & \dots & a_{n2}^{(k)} \\ \dots & \dots & \dots & \dots \\ a_{1n}^{(k)} & a_{2n}^{(k)} & \dots & a_{nn}^{(k)}-x \end{vmatrix} = 0,$$

Очевидно, что элементы $a_{ij}^{(k)}$ матрицы, представляющей k-ую степень заданной $\mathfrak{a}$, выражаются однородными целыми функциями k-ой степени через элементы a_{ij} матрицы $\mathfrak{a}$.

Дадим элементарное доказательство высказанного предложения независимое от теоремы Hamilton'a – Cayley. В самом деле, рассмотрение характеристического уравнения (1) равносильно с рассмотрением преобразования

$$(2)\qquad \begin{aligned} gx_1 &= a_{11}x_1 + a_{21}x_2 + \dots + a_{n1}x_n, \\ gx_2 &= a_{12}x_1 + a_{22}x_2 + \dots + a_{n2}x_n, \\ &\dots\dots\dots\dots\dots\dots\dots\dots, \\ gx_n &= a_{1n}x_1 + a_{2n}x_2 + \dots + a_{nn}x_n. \end{aligned}$$

[51] Journ. de Mathematiques pures et apepliquées. t. XVI.

[52] Д. Граве. Элементарный курс теории чисел. Второе изд. Глава XIII.

Умножим уравнения (2) на g и подставим во вторых частях вместо

$$gx_1, \quad gx_2, \ \ldots, \ gx_n \tag{3}$$

их выражения из тех же уравнений (2); получим

$$\begin{aligned} g^2x_1 &= a_{11}^{(2)}x_1 + a_{21}^{(2)}x_2 + \ldots + a_{n1}^{(2)}x_n, \\ g^2x_2 &= a_{12}^{(2)}x_1 + a_{22}^{(2)}x_2 + \ldots + a_{n2}^{(2)}x_n, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ g^2x_n &= a_{1n}^{(2)}x_1 + a_{2n}^{(2)}x_2 + \ldots + a_{nn}^{(2)}x_n. \end{aligned} \tag{4}$$

Нетрудно видеть, что матрица коэффициентов правых частей уравнений (4) будет $\mathfrak{a}^2$, если $\mathfrak{a}$ будет матрица коэффициентов уравнения (2). Итак, мы видим, что теорема справедлива для случая $k = 2$. Умножая (4) на g и выражая (3) при помощи (2), убедимся в справедливости теоремы для $k = 3$, и т. д.

§ 16

Раскрывая определитель (1) § 15 по степеням g, мы получим для суммы корней характеристического уравнения выражение

$$s_1 = g_1 + g_2 + \ldots + g_n = a_{11} + a_{22} + \ldots + a_{nn} = \sum a_{ii},$$

составленное из элементов главной диагонали матрицы $\mathfrak{a}$.

Подобным же образом получим

$$s_k = g_1^k + g_2^k + \ldots + g_n^k = a_{11}^{(k)} + a_{22}^{(k)} + \ldots + a_{nn}^{(k)} = \sum a_{ii}^{(n)}.$$

Введем для аналогии обозначения

$$a_{ij}^{(1)} = a_{ij}$$
$$a_{ii}^{(0)} = 1, \qquad a_{ij}^{(0)} = 0 \quad (i \neq j).$$

Очевидно, что $a_{ij}^{(0)}$ будут элементами единичной матрицы

$$\mathfrak{a}^0 = I.$$

Можно будет написать $s_0 = n = \sum a_{ii}^{0)}$, $s_1 = \sum a_{ii}^{(1)}$.

§ 17

Тождество

$$\mathfrak{a}^{k+l} = \mathfrak{a}^k\mathfrak{a}^l$$

дает по правилам умножения симметрических матриц

$$a_{ij}^{(k+l)} = \sum_{h=1}^{h=n} a_{hi}^{(k)} a_{hj}^{(l)},$$

отсюда

$$s_{k+i} = \sum_{r=1}^{r=n} a_{rr}^{(k+l)} = \sum_{h=1}^{h=n}\sum_{r=1}^{r=n} a_{hr}^{(k)} a_{hr}^{(l)}.$$

Мы видим, что определитель

$$\Delta_\mu = \begin{vmatrix} s_0 & s_1 & \dots & s_{\mu-1} \\ \dots & \dots & \dots & \dots \\ s_{\mu-1} & s_\mu & \dots & s_{2\mu-2} \end{vmatrix}$$

имеет матрицу

$$s_0 = \sum\sum a_{hr}^{(0)} a_{hr}^{(0)}, \quad s_1 = \sum\sum a_{hr}^{(0)} a_{hr}^{(1)}, \ \dots, \ s_{\mu-1} = \sum\sum a_{hr}^{(0)} a_{hr}^{(\mu-1)}$$
$$s_1 = \sum\sum a_{hr}^{(0)} a_{hr}^{(1)}, \quad s_2 = \sum\sum a_{hr}^{(1)} a_{hr}^{(1)}, \ \dots, \ s_\mu = \sum\sum a_{hr}^{(1)} a_{hr}^{(\mu-1)}$$
$$\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$$

следовательно, он происходит от возвышения в квадрат матрицы

$$\left\| a_{rh}^{(0)} \quad a_{rh}^{(1)} \quad \dots \quad a_{rh}^{\mu-1} \right\|;$$

различные горизонтали последней матрицы получаются, если индексами r и h давать все возможные значения $1, 2, \dots, n$.

Итак $\Delta_\mu > 0$, ибо Δ_μ есть сумма квадратов различных определителей матрицы, все же элементы этих определителей числа вещественные, как рациональные функции элементов основной матрицы $\mathfrak{a}$.

На оснований доказанного выше положительность всех определителей Δ_μ влечет за собой вещественность всех корней уравнения (1) § 15 и теорема доказана.

Исследования Hermite'a

§ 18

Глубокое значение теоремы Sturm'a в алгебре выеснилось с особою рельефностью после замечательных исследований Hermite'a.[53] Знаменитый ученый показал связь теоремы Sturm'a с теорией квадратичных форм; из этой связи вытекли самые разнообразный следствия, относящиеся к другим частям алгебры: к теории инвариантов, к преобразованиям Tschirnhausen'a и т. п. Надо обратить особенное внимание на замечательные исследования Darboux.[54] посвященный тому же вопросу. Не имея возможности изложить исследования Hermite'a в полном их объеме, мы обратим внимание на их характерные пункты.

Прежде всего Hermite показывает, что функции Sturm'a V_h (см. (2) § 13) можно представить в виде дискриминантов некоторых квадратичных форм.

Рассмотрим форму

$$(1) \qquad G = \frac{1}{\alpha_1 - x} Y_1^2 + \frac{1}{\alpha_2 - x} Y_2^2 + \dots + \frac{1}{\alpha_n - x} Y_n^2,$$

[53] Ch. Hermite. Remarques sur le théorème de M. Sturm. Comtes rendues de l'Acad. de Paris T. 36 (1853).

[54] G. Darboux: Sur le théorème de Sturm. Bulletin de Sciences Math. 1875.

где $\alpha_1, \alpha_2, \ldots, \alpha_n$ суть корни заданного уравнения

$$f(x) = 0$$

а

$$Y_k = y_0 + \alpha_k y_1 + \alpha_k^2 y_2 + \ldots + \alpha_k^{n-1} y_{n-1},$$

величины

$$y_0, \quad y_1, \quad y_2, \quad \ldots, \quad y_{n-1} \tag{2}$$

суть произвольно выбранные независимые переменные. Очевидно, что относительно величин (2) функции (1) будет квадратичной формой

$$G = \sum a_{ij} y_i y_j \qquad \begin{pmatrix} i = 0, \ldots, n-1 \\ j = 0, \ldots, n-1 \end{pmatrix},$$

где

$$a_{ij} = \frac{\alpha_1^{i+j}}{\alpha_1 - x} + \frac{\alpha_2^{i+j}}{\alpha_2 - x} + \ldots + \frac{\alpha_n^{i+j}}{\alpha_n - x} = \sum \frac{\alpha^{i+j}}{\alpha - x}.$$

Очевидно, что дискриминант Δ_n (см. § 12 главы VII) выразится по формуле

$$\Delta_n = \left| \sum \frac{\alpha^i}{\alpha - x} \right|_n,$$

то есть мы получаем формулу (1) § 13.

Итак

$$\Delta_n = \frac{D(\alpha_1, \alpha_2, \ldots, \alpha_n}{(-1)^n f(x)};$$

Δ_n отлично от нуля, если все корни α_i различны между собой. Итак, если все корни α_i различны между собой, то форма (1) имеет ранг n.

Нетрудно видеть, что вообще говоря будет

$$\Delta_k = \left| \sum \frac{\alpha^i}{\alpha - x} \right|_k$$

или

$$\Delta_k = \frac{(-1)^k}{f(x)} \sum D(\alpha_1, \alpha_2, \ldots, \alpha_k)(x - \alpha_k)(x - \alpha_{k+1}) \cdots (x - \alpha_n).$$

Коэффициенты α_{ij} квадратичной формы (1), будучи симметрическими функциями корней α_i будут величинами вещественными, если вещественны коэффициенты уравнения $f(x) = 0$ и также дадим вещественное значение числу x, не совпадающее ни с одним корнем α_i.

На основании формул M. Sylvester'a

$$\frac{V_1}{V} = -\rho_1 \frac{\Delta_1}{1}, \quad \frac{V_2}{V_1} = -\rho_2 \frac{\Delta_2}{\Delta_1}, \quad \ldots, \quad \frac{V_n}{V_{n-1}} = -\rho_n \frac{\Delta_n}{\Delta_{n-1}},$$

где все ρ_i числа положительные.

Число перемен знака в ряде

$$V,\ \ V_1,\ \ V_2, \ldots,\ V_n \tag{3}$$

равняется числу положительных величин в ряде

$$\frac{\Delta_1}{1},\ \ \frac{\Delta_2}{\Delta_1},\ \ldots,\ \frac{\Delta_n}{\Delta_{n-1}}.$$

В § 12 главы VII мы видели, что разложение квадратичной формы на сумму квадратов имеет вид

$$G = \frac{\Delta_1}{1}\,\mathfrak{Y}_1^2 + \frac{\Delta_2}{\Delta_1}\,\mathfrak{Y}_2^2 + \ldots + \frac{\Delta_n}{\Delta_{n-1}}\,\mathfrak{Y}_n^2, \tag{4}$$

где $\mathfrak{Y}_i$ есть линейная функция от y_i с вещественными коэффициентами.

Итак, число перемен знака в ряде Sturm'a (3) при $x = a$ будет равняться числу квадратов разложения (4), имеющих *положительные* коэффициенты.

§ 19

Поставим задачу Hermite'a самым общим образом. т. е. рассмотрим квадратичную форму

$$G = H(\alpha_1)Y_1^2 + H(\alpha_2)Y_2^2 + \ldots + H(\alpha_n)Y_n^2, \tag{1}$$

где $H(\alpha)$ есть произвольно выбранная рациональная функция от корня α с вещественными коэффициентами.

Коэффициенты формы G будут теперь

$$a_{ij} = \sum H(\alpha)\alpha^{i+j}. \tag{2}$$

Дискриминант формы G будет

$$\Delta_n = |H(\alpha)\alpha^i|_n;$$

другими словами

$$\Delta_n = H(\alpha_1)H(\alpha_2)\cdots H(\alpha_n)D(\alpha_1, \alpha_2, \ldots, \alpha_n).$$

Подобным же образом получим

$$\Delta_k = \sum D(\alpha_1, \alpha_2, \ldots, \alpha_k)H(\alpha_1)H(\alpha_2)\cdots H(\alpha_k),$$

где сумма распространяется на все сочетания корней по k.

Дискриминант формы Δ_n отличен от нуля если все корни α_i различные, а также ни один из них не обращает функцию $H(\alpha)$ в нуль.

Коэффициенты (2) формы G, будучи симметрическими функциями от корней α_i, будут величинами вещественными.

Если все корни α_i вещественные, то формулу (1) можно рассматривать, как канонический вид формы, ибо функции Y_i все независимые между собой, так как их определитель есть $D(\alpha_1, \alpha_2, \ldots, \alpha_n)$, а корни α_i мы считаем все различными.

Вещественному корню α_i будет соответствовать вещественный квадрат линейной функции

$$H(\alpha_i)Y_i^2.$$

Двум мнимым сопряженным корням α_i, α_k будет соответствовать совокупность двух квадратов

$$H(\alpha_i)Y_i^2 + H(\alpha_k)Y_k^2 = [Y_i\sqrt{H(\alpha_i)}]^2 + [Y_k\sqrt{H(\alpha_k)}]^2 = \\ = (u+iv)^2 + (u-iv)^2 = 2u^2 - 2v^2,$$

где u и v линейные функции от y_i с вещественными коэффициентами.

Предполагая корни α_i различными, мы замечаем, что ранг формы может битв меньше n лишь в том случае, когда несколько из $H(\alpha)$ равны нулю.

Обозначая через ρ дополнение ранга до n, через π число положительных квадратов в каноническом представлении формы, а через ν число квадратов со знаком минус, получаем

$$n = \rho + \pi + \nu.$$

Каждая пара мнимых сопряженных корней α_i, α_k дает один положительный квадрат $2u^2$ и один отрицательный $-2v^2$.

Мы приходим к такой общей теореме.

Число ρ равно числу равных нулю выражений $H(\alpha_i)$.

Число π равно числу пар мнимых корней увеличенному на число вещественных корней уравнения, удовлетворяющих неравенству

$$H(\alpha_i) > 0.$$

Число ν равно числу пар мнимых корней увеличенному на число вещественных корней уравнения, удовлетворяющих неравенству

$$H(\alpha_i) < 0.$$

§ 20

Делая различным образом выбор функций H, будем получать различные результаты.

Так например, полагая $H = 1$, придем к теореме, которую мы доказали уже другим способом:

Число пар мнимых корней равно числу отрицательными квадратов в форме

$$Y_1^2 + Y_2^2 + \ldots + Y_n^2,$$

т. е. равно числу перемен знака в ряде чисел

$$1, \quad \Delta_1, \quad \Delta_2, \quad \ldots, \Delta_n.$$

§ 21

Предположение $H(\alpha) = \dfrac{1}{\alpha - x}$, как мы видели, уже сводить дело к функциям V_k и к обычной формулировке теоремы Sturm'a.

Так как число перемен знака в ряде Sturm'a равно числу положительных квадратов в каноническом представлении Hermite'овской квадратичной формы, то мы приходим к теореме:

Число перемен знака в ряду Sturm'a при $x = a$ равно числу вещественных корней больших a, сложенному с числом пар мнимых корней.

§ 22

Так как функций ψ_k (см. § 10) обладают свойствами функций Sturm'a, то Hermite рассматривает также соответствующий этим функциям случай $H = \alpha - x$.

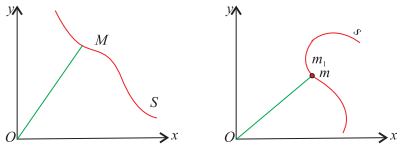
Отделение мнимых корней

§ 23

По аналогии с случаем вещественных корней мы должны будем формулировать задачу отделения мнимых корней следующим образом. Мы будем говорить, что мнимый корень отделен, если в плоскости независимого переменного x указан такой сомкнутый контур, внутри которого лежать только один этот корень. Подобно тому, как для отделения вещественных корней важно было знать точное число корней в каждом данном промежутке, так для случая мнимых корней является важным знать приемы для нахождения точного числа мнимых корней внутри данного сомкнутого контура. Распространение соображений, связанных с теоремой Sturm'a для случая вещественных, корней, на случай мнимых корней принадлежит Cauchy.

§ 24

Рассмотрим две плоскости, соответствующие независимому переменному $z = x + iy$ и целой функции $f(z) = X + iY$, где X и Y суть целые функции с вещественными коэффициентами от вещественных независимых переменных x и y. Если независимая переменная z будет перемещаться в своей плоскости по некоторой непрерывной кривой s, определяемой уравнениями



Черт. 7

$$x = \varphi(t), \qquad y = \psi(t),$$

где t независимая переменная, с изменением которой изменяется положение точки на кривой s, то аффикс $f(z)$ в другой плоскости будет перемещаться по некоторой кривой S, определяемой уравнениями

$$X = \Phi(t), \qquad Y = \Psi(t).$$

Функции Φ и Ψ получатся через подстановку функций φ и ψ вместо x и y

в выражения функции X и Y. Вследствие непрерывности целой функции (см. стр. 13) мы замечаем, что непрерывному движение точки m на кривой s будет соответствовать непрерывное перемещение точки M по кривой S.

Вычисление модуля функции, т. е. расстояния точки M от начала координат, не представляет затруднения.

Аргумент функций есть, как известно, одна из дуг, тангенс которой равен $\frac{Y}{X}$. Затруднение при вычислений аргумента представляется в неопределенности функции $\operatorname{arctg}\frac{Y}{X}$, т. е. в указании кратности периода 2π, которую нужно прибавить к значению arctg, заключенному между $-\frac{\pi}{2}$ и $+\frac{\pi}{2}$, для получения требуемого в задаче. Во всем дальнейшем мы обойдем это затруднение, рассматривая не самый аргумент функции, а приращение этого аргумента, соответствующее непрерывному перемещение точки m вдоль по кривой s. Очевидно, что, на основании непрерывности функции, приращение аргумента функций не зависит от кратности периода у начального значения arctg, соответствующего начальной точке m.

Мы будем рассматривать такие кривые s плоскости независимого переменного z, которые не проходят ни через один из корней целой функции $f(z)$. Тогда для таких кривых s соответственная кривая S не проходит через соответствующее ей начало, координат. Для таких кривых аргумент функции изменяется непрерывно.

Аргумент функций претерпевает разрыв непрерывности только в том случае, когда кривая S проходит через свое начало координат. В этом случай аргумент при переходе точки M через начало координат претерпевает разрыв непрерывности, причем получает сразу приращение равное $+\pi$ или $-\pi$.

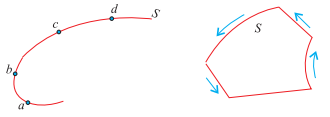
Итак, будем во всем дальнейшем рассматривать такие контуры s, которые не проходят через корни функции $f(z)$.

Теорема Cauchy

§ 25

Лемма I. *Приращение аргумента целой функции, соответствующее некоторой дуге ad контура S равняется сумме приращений аргументов частей этой дуги ab, bc, cd. Контур S может иметь угловые точки и прямолинейные части. Рассматривая сомкнутые контуры мы условимся движение вдоль сомкнутого контура считать положительным, если это движение оставляет слева часть плоскости, ограниченную этим контуром.*

Лемма II. *Если мы заданный сомкнутый контур $ABCD$ разобьем на несколько новых, проводя различные секущие линии $BE, FD, AE, CF, \ldots$, то приращение аргумента функции, соответствующее положительному перемещению вдоль всего контура, будет равно сумме приращений аргумента функций, получаемых при положительных обходах всех частичных контуров.*



Черт. 8

Справедливость леммы следует из того, что при таком обходе частичных контуров, каждая из секущих линий, проведенных внутри заданного контура, проходится два раза в обратных направлениях.

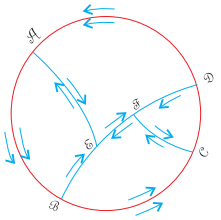
Лемма III. *Приращение аргумента произведения ряда целых функций*

$$f_1(z), \quad f_2(z), \ \ldots, \ f_n(z)$$

соответствующее перемещение по некоторой линии S, равняется сумме приращений аргументов отдельных множителей.

Справедливость леммы следует из того, что аргумент произведения равен сумме аргументов множителей.

Рассмотрим приращение аргумента линейной функций $z-a$, где a некоторое постоянное число. Указывая точки a и z на плоскости комплексного переменного, мы замечаем, что аргумент разности $z-a$ (с точностью до кратности 2π) равняется углу, образованному с положительным направлением оси x-ов вектором az, начало которого есть a. Условимся отсчитывать углы векторов с осью x-ов в том же смысле, как мы определили положительное направление при обходе замкнутых контуров.



Черт. 9

Лемма IV. *Приращение аргумента разности $z-a$ при обходе точкою z сомкнутого контура равно 0, если контур не включает точки a, и равно 2π, если точка a внутри контура.*

Это почти очевидно из чертежа, В самом деле, в каком бы месте ни находилась точка a внутри контура S, или вне его, всегда аргумент разности $z-a$ равняется углу zax, и, очевидно, когда точка z обойдет контур в положительном направлении и вернется в начальное положение, то угол zax изменяясь непрерывно, получит или приращение 2π или 0, смотря по тому, будет ли точка a лежать внутри или вне контура S.

На основании доказанных лемм можно просто доказать основную теорему Cauchy.

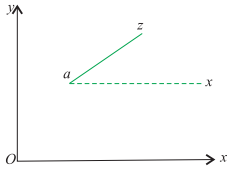
Теорема. *Приращение аргумента целой функций $f(z)$, соответствующее обходу точкою z некоторого сомкнутого контура, равно $2k\pi$, где целое число k равно числу корней функции $f(z)$, лежащих внутри этого контура.*

В самом деле, пусть

$$f(z) = p_0(z-a_1)(z-a_2)\cdots(z-a_n),$$

где $a_1, a_2, \ldots, a_n$ суть корни функции $f(z)$. Получаем

$$\arg f(z) = \arg p_0 + \arg(z-a_1) + \ldots + \arg(z-a_n).$$



Черт. 10

Каждый из аргументов $z-a_k$ получает приращение равное 0 или 2π, судя по тому, лежит ли корень вне контура, или внутри контура. Отсюда аргумент функции получает приращение такой кратности 2π, сколько корней лежит внутри контура.

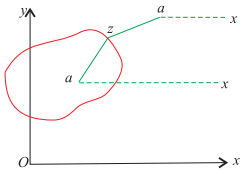
§ 26

Будем называть *внешним контуром совокупности n точек* плоскости такой замкнутый многоугольник без входящих углов, вершины которого находятся в заданных точках и все заданные точки лежат или внутри его или на его сторонах но не вне этого контура.

Очевидно, что легко для всякого расположения точек построить их внешний контур. Понятие о внешнем контуре может быть обобщено на случай бесчисленного множества точек.[55]

Теорема. *Корни производной $f'(z)$ находятся внутри внешнего контура, соответствующим корням самой функций $f(z)$.*

Для доказательства теоремы предположим, что за ось x-ов взята одна из сторон внешнего контура, а ось y-ов направлена под прямым углом в ту сторону, с которой лежит сам контур. Тогда все корня $x_k = \alpha_k + \beta_k i$ функции $f(x)$ имеют не отрицательные мнимые коэффициенты β_k, причем по крайней мере два из них равны нулю и кроме того, если мы не предполагаем всех корней вещественными, то надо допустить, что среди не отрицательных чисел β_k есть отличные от нуля.



Черт. 11

Равенство

$$\frac{f'(x)}{f(x)} = \sum \frac{m_k}{x - x_k},$$

где m_k есть натуральное число, *выражающее* кратность корня x_k, дает, если в него подставить корень $\xi + i\eta$ производной

$$\sum \frac{m_k}{(\xi - \alpha_k) + i(\eta - \beta_k)} = 0.$$

Приравнивая нулю коэффициент при i, получим

$$\sum \frac{(\beta_k - \eta)m_k}{(\xi - \alpha_k)^2 + (\eta - \beta_k)^2} = 0.$$

Очевидно, что число η не может быть *не положительным* и теорема доказана.

§ 27

Как частный случай предыдущей теоремы получаем.

Теорема. *Для уравнений третьей степени $f(x)$ корни производной $f'(x)$ дают фокусы эллипса Steiner'a, вписанного в треугольник, образованный как вершинами корнями заданного уравнения.*

Мы напомним, что эллипс Stainer'a обладает следующими свойствами: (1) он касается сторон треугольника в их серединах, (2) центр его совпадает с пересечением медиан треугольника, (3) он имеет наибольшую площадь из всех эллипсов, вписанных в треугольник.

[55] Д. Граве. Об основных предложениях теории функций двух вещественных переменных. Сообщения Харьковского Математ. Общ. т. VI.

§ 28

Покажем теперь правило для вычисления приращения аргумента целой функции при обходе независимым переменным некоторого сомкнутого контура.

Обозначая $f(z) = X + iY$ мы замечаем, что аргумент $f(z)$ есть одно из значений угла, имеющего тангенсом функцию $\frac{Y}{X}$. Для определенности рассуждений рассмотрим случай, когда начальное значение X, соответствующее некоторой точке описываемого точкою z контура, есть число положительное; тогда за начальное значение φ_0 аргумента функции можно будет принять дугу, имеющую тангенсом $\frac{Y_0}{X_0}$ и заключенную в границах от $-\frac{\pi}{2}$ до $+\frac{\pi}{2}$, ибо $X = \rho\cos\varphi_0$, где ρ есть модуль функции.

Если при перемещении точки z по контуру функция X не обращается в нуль, то дробь $\frac{Y}{X}$, которая есть функция от независимого переменного t (см. стр. 350), не обращается в ∞; а потому аргумент, изменяясь непрерывно, остается в границах от $-\frac{\pi}{2}$ до $+\frac{\pi}{2}$, и, следовательно, если мы обозначим через φ_1 конечное значение аргумента, где число φ_1 заключается в тех же границах от $-\frac{\pi}{2}$ до $+\frac{\pi}{2}$, то полное приращение аргумента равно $\varphi_1 - \varphi_0$.

Остается рассмотреть случай, когда аргумент функций, изменяясь непрерывно, будет переходить через крайние пределы $-\frac{\pi}{2}$ и $+\frac{\pi}{2}$. Аргумент функций перейдет через $+\frac{\pi}{2}$, непрерывно возрастая, в том случае, если дробь $\frac{Y}{X}$ переходит через ∞ от значений положительных к значениям отрицательным; в этом случай можно сказать, что новое значение аргумента, большее чем $+\frac{\pi}{2}$, может быть выражено по формуле $\varphi = \pi + \psi$, где ψ есть угол, лежащий в границах от $-\frac{\pi}{2}$ до $+\frac{\pi}{2}$. В самом деле, если $\varphi = \frac{\pi}{2} + \varepsilon$, где ε некоторое малое положительное число, то $\psi = \varphi - \pi = -\frac{\pi}{2} + \varepsilon = -\left(\frac{\pi}{2} - \varepsilon\right)$. Подобным же образом, если дробь $\frac{Y}{X}$ переходит через бесконечность от отрицательных значений к положительным, то аргумент φ, убывая, переходить через $-\frac{\pi}{2}$, причем новое значение аргумента может быть написано так $\varphi = -\pi + \psi$, где ψ угол, заключающейся в тех же границах от $-\frac{\pi}{2}$ до $+\frac{\pi}{2}$. Итак, мы видим, что при переходе дроби $\frac{Y}{X}$ через ∞ новое значение аргумента может быть выражено так: $\varphi = \varepsilon_1\pi + \psi$, где ε_1 есть $+1$ при переходе от положительных значений к отрицательным и есть -1 при переходе от отрицательных значений к положительным. Если при дальнейшем перемещении z по контуру дробь $\frac{Y}{X}$ второй раз обратится в ∞, изменяя свой знак, то аргумент φ получит новое приращение $\varepsilon_2\pi$, где ε_2 есть $+1$ или -1, так что $\varphi = \varepsilon_1\pi + \varepsilon_2\pi + \psi$, где ψ заключается между $-\frac{\pi}{2}$ и $+\frac{\pi}{2}$. Предположим, что независимая переменная z, обойдя контур, возвращается в начальную точку, причем дробь $\frac{Y}{X}$ меняет свой

знак, проходя p раз через ∞; тогда получаем для искомого аргумента такое число

$$\varphi = \varepsilon_1\pi + \varepsilon_2\pi + \ldots + \varepsilon_p\pi + \psi_0,$$

где число ψ_0, очевидно, должно равняться начальному значений аргумента φ_0. Отсюда мы видим, что полное приращение аргумента $\varphi - \varphi_0$ выражается по формуле

$$\varphi - \varphi_0 = \varepsilon_1\pi + \varepsilon_2\pi + \ldots + \varepsilon_p\pi. \tag{1}$$

Обозначая через k число корней функции, заключенных внутри контура, описанного независимым переменным k, получаешь по теореме Cauchy

$$\varphi - \varphi_0 = 2k\pi. \tag{2}$$

Сравнивая формулы (1) и (2), получаешь для числа корней k выражение

$$k = \frac{\varepsilon_1 + \varepsilon_2 + \ldots + \varepsilon_p}{2}.$$

Если дробь $\dfrac{Y}{X}$ переходя p раз через ∞, переходить m раз от положительных значений к отрицательным и n раз от отрицательных к положительным, то среди чисел ε_i будет m равных $+1$ и n равных -1, и, следовательно, получим

$$k = \frac{m-n}{2}.$$

Случай обращения функции $\dfrac{Y}{X}$ в ∞ без перемены знака не влияет на приращение аргумента.

Рассуждения останутся теми же, если мы значение аргументов φ и ψ будем рассматривать в другой половине, между $\dfrac{\pi}{2}$ и $\dfrac{3\pi}{2}$.

§ 29

Будем, по примеру Cauchy, называть число $\varepsilon_1 + \varepsilon_2 + \ldots + \varepsilon_p$ *индексом* функции $f(z)$ по контуру C, описанному точкою. Обозначая через t_0 и t_1 начальное и конечное значение переменного t, при непрерывном изменении которого линия C была пройдена точкою t, будем обозначать индекс функции так

$$I_{t_0}^{t_1}\left(\frac{Y}{X}\right), \qquad I_{t_0}^{t_1}\{F(t)\}.$$

Из определения индекса вытекает, что индекс функции по некоторой линии C равен сумме индексов, соответствующих частям этой линии при этом предполагается, что все части линии C проходятся в том же направлении, в каком была пройдена вся линия C.

Cauchy показал, что вычисление индекса может быть сведено к соображениям, имеющим прямую связь с теоремою Sturm'a в тех случаях, когда X и Y суть целые функций от t.

Символ индекса обладает следующими основными свойствами.

Если степень целой функции относительно Y выше степени X, и мы обозначим через Y_1 остаток от деления полинома Y на полином X, то будет

$$I\left(\frac{Y}{X}\right) = I\left(\frac{Y_1}{X}\right).$$

В самом деле, обозначая через Q частное, получим

$$Y = QX + Y_1;$$

отсюда

$$\frac{Y}{X} = Q + \frac{Y_1}{X}.$$

Так как целая функция сохраняет конечные значения при всевозможных значениях независимого переменного, то две функции $\frac{Y}{X}$ и $\frac{Y_1}{X}$ обращаются одновременно в бесконечность, причем достаточно большие значения этих функций совпадают по знаку, и, следовательно, у обеих дробей

$$\frac{Y}{X} \quad \text{и} \quad \frac{Y_1}{X}$$

будут одинаковые индексы.

Рассмотрим две обратные дроби

$$\frac{Y}{X}, \qquad \frac{X}{Y}.$$

Обозначим через I индекс первой дроби, а через I_1 индекс второй дроби. Покажем, что

$$I + I_1 = \varepsilon,$$

где ε одно из чисел 0, +1, −1. Рассматривая первую дробь $\frac{Y}{X}$, мы замечаем, что для вычисления индекса I надо рассматривать перемены знака дроби $\frac{Y}{X}$ при переходе через бесконечность, а I_1 будет соответствовать случаям перемены знака той же дроби при переходе ее через нуль. Мы видим, что сумма $I + I_1$ будет равна разности между числом переходов дроби $\frac{Y}{X}$ от положительных значений к отрицательным и числам переходов от отрицательных значений к положительным. Очевидно, что, если полиномы одного знака, как при начальном значении t_0 независимого переменного, так и при конечном значений t_1, то дробь $\frac{Y}{X}$ положительна в обоих случаях, и, следовательно, эта дробь проходить столь же раз от положительных значений к отрицательным, как и обратно. Это значить, что сумма индексов, или, что одно и то же, число ε должно равняться нулю. Если дробь $\frac{Y}{X}$ при начальном значении t_0 была положительна, а при конечном отрицательна, то общее число переходов дроби от положительных значений к отрицательным

должно на единицу превышать число обратных переходов т. е. $\varepsilon = 1$; и, наконец, $\varepsilon = -1$, если начальное значение дроби отрицательное, а конечное значение положительное.

Рассмотрим дробь $\dfrac{X}{X_1}$, где степень числителя будем предполагать выше степени знаменателя. Разделим X на X_1 и обозначим остаток от этого деления с переменой знака через X_2; подобным же образом через X_3 обозначим остаток с обратным знакомь от деления X_1 на X_2. Продолжаем последовательное вычисление функций $X_4, X_5, \ldots$ пока не дойдем до остатка X_n, равного постоянному числу. На основании выведенного раньше свойства, получаем

$$I\left(\frac{X_1}{X}\right) + I\left(\frac{X}{X_1}\right) = \varepsilon_1,$$

где ε_1 есть одно из чисел 0, +1, −1; кроме того имеем

$$I\left(\frac{X}{X_1}\right) = I\left(\frac{-X_2}{X_1}\right) = -I\left(\frac{X_2}{X_1}\right),$$

значить, получаем

$$I\left(\frac{X_1}{X}\right) - I\left(\frac{X_2}{X_1}\right) = \varepsilon_1.$$

Рассуждая подобным же образом, получаем ряд равенств

$$\begin{gathered}
I\left(\frac{X_2}{X_1}\right) - I\left(\frac{X_3}{X_2}\right) = \varepsilon_2, \\
I\left(\frac{X_3}{X_2}\right) - I\left(\frac{X_4}{X_3}\right) = \varepsilon_3 \\
\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\
I\left(\frac{X_{n-1}}{X_{n-2}}\right) - I\left(\frac{X_n}{X_{n-1}}\right) = \varepsilon_{n-1} \\
I\left(\frac{X_n}{X_{n-1}}\right) + I\left(\frac{X_{n-1}}{X_n}\right) = \varepsilon_n.
\end{gathered}$$

Так как X_n число постоянное, отличное от нуля, то дробь $\dfrac{X_{n-1}}{X_n}$ не обращается в бесконечность, и, следовательно, $I\left(\dfrac{X_{n-1}}{X_n}\right) = 0$.

Отсюда, складывая полученные нами равенства, найдем

$$I\left(\frac{X_1}{X}\right) = \varepsilon_1 + \varepsilon_2 + \ldots + \varepsilon_n.$$

На основании равенства

$$I\left(\frac{X_p}{X_{p-1}}\right) + I\left(\frac{X_{p-1}}{X_p}\right) = \varepsilon_p,$$

мы замечаем что $\varepsilon_p = 0$, когда две функций X_{p-1} и X_p представляют или повторение знака, как при начальном значении t_0, так и при конечном значений t_1 или

же в обоих случаях перемену знака; $\varepsilon_p = +1$, если две функции X_{p-1} и X_p при начальном значении представляют повторение знака, а при конечном перемену, и $\varepsilon_p = -1$, если, обратно, начальному значений соответствует перемена знака, а конечному повторение знака. Итак, если мы рассмотрим ряд функций

$$X, \quad X_1, \quad X_2, \ \ldots, \ X_n, \tag{1}$$

то составляя два ряда численных значений этих функций при t_0 и t_1, мы замечаем, что индекс $I\left(\frac{X}{X_1}\right)$ будет равен

$$P_v - V_p,$$

где P_v есть число повторений знака ряда для t_0, перешедших в перемены в ряду для t_1, а V_p число перемен знака ряда для t_0, перешедших в повторение знака для t_1. Обозначая через V число перемен знака в ряде для t_0, а через V_1 число перемен знака в ряде для t_1, мы, очевидно, получим

$$V_1 = V + P_v - V_p,$$

следовательно,

$$P_v - V_p = V_1 - V.$$

Итак, получаем

$$I\left(\frac{X_1}{X}\right) = V_1 - V,$$

т. е. *индекс дроби* $\frac{X_1}{X}$ равняется числу приобретений перемен знака в ряде функций (1) при переходе от t_0 в t_1.

§ 31

Самым удобным способом на практике для отделения мнимых корней является рассмотрение прямоугольника со сторонами параллельными вещественной и мнимой оси, причем ставится задачею найти число корней уравнения

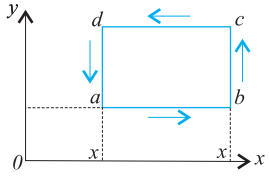
$$f(z) = \varphi(x, y) + i\psi(x, y) = 0,$$

лежащих в каждом из таких прямоугольников.

Например, если мы рассмотрим прямоугольник $abca$ со сторонами определяем уравнениями

$$\begin{aligned} ab &\qquad y = y_0 \\ bc &\qquad x = x_1 \\ cd &\qquad y = y_1 \\ da &\qquad x = x_2, \end{aligned}$$

то при рассмотрении изменения аргумента функции вокруг такого прямоугольника, нам придется на стороне ab брать $X = \varphi(x, y_0)$, $Y = \psi(x, y_0)$, где X и Y суть полиномы от одного независимого переменного x, и нужно будет вычислить $I\left(\frac{Y}{X}\right)$ при изменении независимого переменного x от



Черт. 12

x_0 до x_1. Подобным же образом на прямой bc придется положить $X = \varphi(x_1, y)$, $Y = \psi(x_1, y)$ и рассматривать изменение y от y_0 до y_1. На третьей стороне cd будет $X = \varphi(x, y_1)$, $Y = \psi(x, y_1)$ и x будет изменяться от x_1 до x_0. Наконец, на четвертой стороне da будет $X = \varphi(x_0, y)$, $Y = \psi(x_0, y)$ и y меняется от y_1 до y_0.

Число корней внутри прямоугольника равно полусумме индексов для всех сторон прямоугольника.

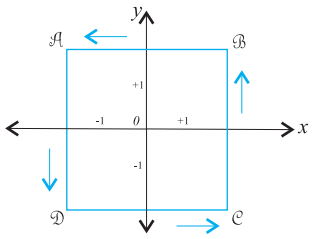
§ 32

Рассмотрим численный пример. Пусть дано уравнение

$$z^4 - 5z + 1 = 0,$$

где $z = x + iy$. Поставим себе задачею найти число корней заданного уравнения, заключающихся в квадрате, образованном прямыми

$$x_0 = -1, \qquad x_1 = +1,$$
$$y_0 = -1, \qquad y_1 = +1.$$



Черт. 13

Наше уравнение можно представить в виде

$$(x + ij)^4 - 5(x + iy) + 1 = 0,$$

или

$$x^4 - 6x^2y^2 + y^4 - 5x + 1 + i(4x^3y - 4xy^3 - 5y) == 0.$$

Рассматривая сторону DC, соответствующую $y = -1$, получим

$$X = x^4 - 6x^3 - 5x + 2,$$
$$X_1 = -4x^3 + 4x + 5.$$

Остаток от деления X на X_1, взятый с обратным знаком, будет

$$X_2 = 20x^3 + 15x - 8.$$

Следующий остаток с обратным знаком будет $X_3 = -3x - 124$, и, наконец, $X_4 = -301868$. Подставим в ряд функций

(1) $$X, \quad X_1, \quad X_2, \quad X_3, \quad X_4,$$

-1 и $+1$ и выпишем ряд получившихся знаков

-1	$+$	$+$	$-$	$-$	$-$
$+1$	$-$	$+$	$+$	$-$	$-$

Из этой таблицы видно, что число приобретений перемен знака в ряду функций (1) при переходе x от -1 до $+1$ равно 1, следовательно, индекс для стороны DC равен 1.

Для стороны BA, где $y = +1$, мы можем не вычислять ряда функций, а, заметив, что она проходится в направлении обратном DC, написать знаки обратные знакам предыдущей таблицы

$$\begin{array}{c|cccc} -1 & - & - & + & + & + \\ +1 & + & - & - & + & + \end{array}$$

Для стороны BA индекс равняется также 1.

Рассмотрим сторону CB, соответствующую $x = +1$. Получим

$$\begin{aligned} X &= y^4 - 6y^2 - 3, \\ X_1 &= -4y^3 - y, \\ X_2 &= 25y^2 + 12, \\ X_3 &= -23y, \\ X_4 &= -276. \end{aligned}$$

Ряд знаков будет

$$\begin{array}{c|cccc} -1 & - & + & + & + & - \\ +1 & - & - & + & - & - \end{array}$$

Число приобретений перемен знака здесь равняется нулю; следовательно, индекс для стороны CB равен нулю.

Для стороны AD, соответствующей $x = -1$, получим

$$\begin{aligned} X &= y^4 - 6y^2 + 7, \\ X_1 &= 4y^3 - 9y, \\ X_2 &= 15y^2 - 28, \\ X_3 &= 23y, \\ X_4 &= 614. \end{aligned}$$

Ряд знаков будет

$$\begin{array}{c|cccc} +1 & + & - & - & + & + \\ -1 & + & + & - & - & + \end{array}$$

Индекс для этой стороны также равен нулю.

Так как число корней равно полусумме индексов для всех сторон прямоугольника $ABCD$, то в рассматриваемом нами прямоугольнике число корней будет 1.

§ 33

Изложенные исследования Cauchy завершаются знаменитым обобщением на случай произвольной функций $f(z)$ комплексного переменного z.

Если функция $f(z)$ регулярная для всех точек внутри контура C, то, обозначая через N число нулей $f(z)$ внутри C, получим

$$N = \frac{1}{2\pi i} \int \frac{f'(z)}{f(z)}\, dz,$$

где интеграл распространяется на контур C[56]

Теория Kronecker'a

§ 34

Теория Cauchy оказалась частным случаем более общей теории, созданной Kronecker'ом и названной им теорией *характеристик*. Эта теория занимательна тем, что распространяет соображения связанные с теоремой Sturm'a на случай функций многих переменных независимых.

Пусть заданы две вещественные алгебраические линии уравнениями

$$\varphi(x, y) = 0, \qquad \psi(x, y) = 0.$$

Во всех элементарных курсах приложений дифференциального исчисления к геометрии доказываются формулы

$$\frac{dx}{ds} = \frac{\psi_2}{\sqrt{\psi_1^2 + \psi_2^2}}, \qquad \frac{dy}{ds} = \frac{\psi_1}{\sqrt{\psi_1^2 + \psi_2^2}}, \tag{1}$$

где для сокращения обозначено

$$\psi_1 = \frac{\partial \psi}{\partial x}, \qquad \psi_2 = \frac{\partial \psi}{\partial y},$$

а дифференциалы dx, dy берутся при положительности дифферещала ds, т. е. они выражают перемещение вдоль по кривой $\psi = 0$ соответствующее возрастанию дуги. Мы будем предполагать, что все алгебраические кривые $f = 0$, которые мы будем рассматривать, заданы так, что функция f, равная нулю вдоль по кривой отрицательна с одной стороны и положительна с другой ее стороны. Если мы будем предполагать кривую $f = 0$ замкнутою и делящего всю плоскость на две части: *внутреннюю* и *внешнюю*, то мы будем предполагать существование неравенства $f < 0$ для внутренней части. Мы знаем, что таким свойством обладают простейшие уравнения круга и эллипса.

Если считать корень квадратный в формулах (1) *положительным*, то получится тот обход по контуру $\psi = 0$, при котором внутренняя часть контура ($\psi < 0$) остается налево.

Рассмотрим дифференциал

$$d\varphi = \varphi_1 dx + \varphi_2 dy$$

и подставим сюда значения дифференциалов, взятые из (1); получим

$$d\varphi = \frac{ds}{\sqrt{\psi_1^2 + \psi_2^2}} \, |\psi_1 \varphi_2|, \tag{2}$$

где

$$|\psi_1 \varphi_2| = \psi_1 \varphi_2 - \varphi_1 \psi_2.$$

[56] Д. Граве. Элементы теории эллиптических функций 1910, стр. 53.

Мы введем обозначение зн. u, причем под этим символом будем разуметь $+1$, если u число положительное, и -1, если u — отрицательно. Символ зн. u будем читать — *знак величины* u. Формула (2) в связи с выше поставленными предположениями даст

$$\text{зн. } d\varphi = \text{зн. } |\psi_1\varphi_2|.$$

§ 35

Двигаясь по замкнутому контуру $\psi = 0$ в указанном направлении, мы будем встречать линию $\varphi = 0$ в некоторых точках M.

Если в точке M будет существовать неравенство $\psi_1\varphi_2 - \varphi_1\psi_2 > 0$, то будет также $d\varphi > 0$ и значит при переходе через точку M мы идем из части плоскости, где $\varphi < 0$, в ту часть, где $\varphi > 0$. При $\psi_1\varphi_2 - \varphi_1\psi_2 < 0$ происходить явление обратное.

Случаи $\psi_1\varphi_2 - \varphi_1\psi_2$ мы не будем рассматривать, ибо не будем никогда предполагать в нашем изложений, что три алгебраическая кривые встречаются в одной точке.

Очевидно, что при движении по замкнутому обходу, когда это движение оканчивается в той же точке, из которой началось, будет иметь место равенство

$$\sum \text{зн. } d\varphi = 0. \tag{1}$$

В самом деле, если путешественник при своем движении переходит несколько раз через границу двух соседних стран A и B, причем оканчивает движение в той же стране, из которой начал, то он должен перейти столько же раз границу из страны A в страну B сколько раз из B в A. В левой части равенства (1) будет столько же членов $+1$, сколько -1.

Мы можем написать равенство

$$\sum \text{зн. } |\psi_1\varphi_2| = 0, \tag{2}$$

равносильное равенству (1).

§ 36

Возьмем теперь кроме алгебраических линий $\varphi = 0$, $\psi = 0$ еще третью $f(x, y) = 0$.

Будем предполагать кривую f замкнутою и будем рассматривать ее точки встречи с кривою

$$\varphi\psi = 0,$$

представляющею совокупность двух кривых $\varphi = 0$, $\psi = 0$.

Очевидно, что равенство (1) § 34 напишется так

$$\sum \text{зн. } d(\varphi\psi) = 0;$$

$$(f = 0, \quad \varphi\psi = 0)$$

нижними формулами мы подчеркиваем тот факт, что сумма распространяется на все точки встречи двух линий $f = 0$ и $\varphi\psi = 0$. Разделяя эти точки встречи на две части: на точки встречи $f = 0$, $\varphi = 0$ и на точки встречи $f = 0$, $\psi = 0$, получим

$$\sum_{(f=0,\ \varphi=0)} \text{зн.}\, d(\varphi\psi) \quad + \quad \sum_{(f=0,\ \psi=0)} \text{зн.}\, d(\varphi\psi) \quad = 0 \ .$$

Но при $\varphi = 0$

$$d(\varphi\psi) = \varphi d\psi + \psi d\varphi = \psi d\varphi,$$

а при $\psi = 0$

$$d(\varphi\psi) = \varphi d\psi + \psi d\varphi = \varphi d\psi.$$

Следовательно

$$\sum_{(f=0,\ \varphi=0)} \text{зн.}\, \psi d\varphi \quad + \quad \sum_{(f=0,\ \psi=0)} \text{зн.}\, \varphi d\psi \quad = 0 \ ,$$

или иначе

$$\sum_{(f=0,\ \varphi=0)} \text{зн.}\, \psi|f_1\varphi_2| \quad + \quad \sum_{(f=0,\ \psi=0)} \text{зн.}\, \varphi|f_1\psi_2| \quad = 0$$

или, что одно и тоже,

$$(1) \qquad \sum_{(f=0,\ \varphi=0)} \text{зн.}\, \psi|f_1\varphi_1| \quad = \quad \sum_{(f=0,\ \psi=0)} \text{зн.}\, \varphi|\psi_1 f_2| .$$

Сделаем транспозицию функций f и φ оставляя ψ без изменения

$$\sum_{(f=0,\ \varphi=0)} \text{зн.}\, \psi|f_1\varphi_2| \quad = \quad \sum_{(f=0,\ \psi=0)} \text{зн.}\, f|\psi_1\varphi_2| .$$

или иначе

$$(2) \qquad \sum_{(f=0,\ \varphi=0)} \text{зн.}\, \psi|f_1\varphi_2| \quad = \quad \sum_{(f=0,\ \psi=0)} \text{зн.}\, f|\varphi_1\psi_2| .$$

Сопоставляя (1) и (2), получим тройную формулу

$$\sum \text{зн.}\, \psi[f_1\varphi_2| = \sum \text{зн.}\, \varphi|\psi_1 f_2| = \sum \text{зн.}\, f|\varphi_1\psi_2| = -2k,$$

где через $-2k$ обозначена общая величина трех равных между собою сумм.

Оказывается, что число k всегда целое; это число Kronecker называет *характеристикой* системы функций $(f; \varphi, \psi)$.

Для того чтобы доказать, что число k целое, достаточно показать, что сумма

$$\sum_{(\varphi=0, \psi=0)} \text{зн.}\, f|\varphi_1\psi_2|$$

число всегда четное.

Разобьем все точки встречи $\varphi = 0$ и $\psi = 0$ на две категории, когда $f < 0$ и $f > 0$.

Имеем

$$(3)\qquad \begin{aligned} \sum_{(\varphi=0,\psi=0)} \text{зн. } f|\varphi_1\psi_2| &= \sum_{(f>0)} \text{зн. } f|\varphi_1\psi_2| + \sum_{(f<0)} \text{зн. } f|\varphi_1\psi_2| \\ \sum \text{зн. } f|\varphi_1\psi_2| &= \sum_{(f>0)} \text{зн. } f|\varphi_1\psi_2| - \sum_{(f<0)} \text{зн. } f|\varphi_1\psi_2| \end{aligned}$$

Равенство (2) § 34 можно будет переписать так

$$(4)\qquad 0 = \sum_{(f>0)} \text{зн. } |\varphi_1\psi_2| + \sum_{(f<0)} \text{зн. } \varphi_1\psi_2|$$

Вычитая (4) из (3), получим

$$\sum \text{зн. } f|\varphi_1\psi_2| = -\sum_{(f<0)} \text{зн. } |\varphi_1\psi_2|$$

откуда приходим окончательно к равенству

$$(5)\qquad k = \sum_{(f<0,\ \varphi=0,\ \psi=0)} \text{зн. } |\varphi_1\psi_2|$$

показывающему, что характеристика есть действительно целое число.

§ 37

Применим теперь понятие о характеристике к нахождение мнимых корней уравнения

$$(1)\qquad F(x+iy) = \varphi(x,y) + i\psi(x,y) = 0,$$

лежащих внутри сомкнутого контура

$$f(x,y) = 0.$$

Дифференцируя тождество (1) по x и y, получим

$$F'(x+iy) = \varphi_1 + i\psi_1,$$
$$iF'(x,+iy) = \varphi_2 + i\psi_2,$$

откуда

$$i\varphi_1 - \psi_1 = \varphi_2 + i\psi_2,$$

так что

$$\psi_1 = -\varphi_2, \qquad \psi_2 = \varphi_1.$$

В этом случае

$$|\varphi_1\psi_2| = \varphi_1\psi_2 - \varphi_2\psi_1 = \varphi_1^2 + \varphi_2^2 > 0,$$

формула (5) предыдущего параграфа дает

$$k = \sum(+1)$$
$$(f < 0, \varphi = 0, \psi = 0).$$

И мы приходим к теореме.

Число корней уравнения $F(z) = \varphi + i\psi = 0$, лежащих внутри сомкнутого контура $f = 0$ равно характеристике системы трех функций $(f; \varphi, \psi)$.

§ 38

Очевидно, что кривые $\varphi = 0$, $\psi = 0$, представляющие вещественную и мнимую часть алгебраического уравнения $F(x + iy) = 0$, не могут быть сомкнутыми, ибо равенство

$$\sum \text{зн.}\, |\varphi_1\psi_2| = 0$$

не может удовлетворяться по причине $|\varphi_1\psi_2| > 0$.

Действительно, обе кривые $\varphi = 0$, $\psi = 0$ имеют бесконечные ветви с прямолинейными асимптотами. Направления асимптот найдутся из следующих соображений.

Пусть

$$F(z) = z^n + p_1 z^{n-1} + p_2 z^{n-2} + \ldots$$

и положим

$$z = r(\cos b\theta + i \sin\theta),$$

тогда получим

$$\varphi = r^n \cos n\theta + p_1 r^{n-1} \cos(n-1)\theta + \ldots,$$
$$\psi = r^n \sin n\theta + p_1 r^{n-1} \sin(n-1)\theta + \ldots;$$

уравнения $\varphi = 0$ и $\psi = 0$ по разделению на r^n примут вид

$$\cos n\theta + p_1 \frac{1}{r} \cos(n-1)\theta + p_2 \frac{1}{r^2} \cos(n-2)\theta + \ldots = 0,$$
$$\sin n\theta + p_1 \frac{1}{r} \sin(n-1)\theta + p_2 \frac{1}{r^2} \sin(n-2)\theta + \ldots = 0.$$

При $r = \infty$, получаем

$$\cos n\theta = 0, \qquad \sin n\theta = 0. \tag{1}$$

Линия $\varphi = 0$ имеет асимптоты, проходящие через начало координат и определяемые уравнением $\cos n\theta = 0$, что дает

$$n\theta = \frac{\pi}{2} + k\pi.$$

Получается *звезда* прямых линий, делящих окружность 2π на $2n$ равных частей. Асимптоты для $\psi = 0$ определяются уравнением $\sin n\theta = 0$ и дают звезду, состоящую из биссекторов углов предыдущей звезды.

Нетрудно видеть, что наш результат, полученный при вещественных p_i, имеет место и в общем случае комплексных p_i, ибо уравнения (1) получаются из старших членов предыдущих уравнений.

§ 39

Соображения предыдущего параграфа в связи с теорией характеристик дают простое доказательство теоремы, что всякое уравнение n-ой степени имеет n корней. Это доказательство по идее своей близко к первому доказательству Gauss'a, публикованному им в 1799 в его докторской диссертации: Demonstratio nova Theorematis omnem functionem algebraicam rationalem integram unius variabilis in factores reales primi el secundi gradus resolvi posse. Helmstatii.

Первая попытка строго доказать основную теорему алгебры принадлежит D'Alembert'y[57]. Gauss в своей диссертации указывает на недостатки доказательств его предшественников: D'Alembert'a, Euler'a, de Foncenex и Langrange'a. Впоследствии Gauss[58] дал три новых доказательства той же теоремы. Мы дали в § 1 Главы II доказательство принадлежащее Cauchy и основанное на приложении теоремы Weiertrass'a.

Докажем теперь туже теорему при помощи теории характеристик.

Возьмем за контур $f = 0$ круг бесконечно большого радиуса с центром в начале координат. На основании соображений § 35 мы видим, что

$$k = -\frac{1}{2}\sum \text{зн. } d(\varphi\psi) \quad (f = 0, \varphi = 0).$$

При бесконечно большом радиусе круга бесконечные ветви кривых $\varphi = 0$, $\psi = 0$ могут быть заменены звездами асимптот.

Не трудно сообразить, что, если мы будем двигаться по кругу в таком направлений, что внутренняя его часть будет находиться налево, то мы будем пересекать бесконечные ветви кривой $\varphi = 0$ таким образом, что в этих точках пересечения произведение $\varphi\psi$ будет менять свой знак в смысле перехода от положительных значений к отрицательным

$$\text{зн. } d(\varphi\psi) = -1 \quad (f = 0, \varphi = 0).$$

Принимая во внимание, что число асимптот есть n, что круг встречает каждую из них два раза, получим

$$k = -\frac{1}{2}(-2n) = n,$$

и теорема доказана.

[57] D'Alembert. Recherches sur le calcul intégrale. Histoire de l'acad. de Berlin.

[58] Gauss. Ges. Werke. B. III, s. 31, 57, 71.

§ 40

Теория Kronecker'a может быть обобщена на случай n мерного пространства. Можно рассматривать n сверхповерхностей

$$\varphi = 0, \quad \psi = 0, \ldots, \ \omega = 0$$

и искать, сколько их точек пересечения заключаются внутри сомкнутой сверхповерхности $f = 0$.

Исследования Hurwitz'a

§ 41

Рассмотрим, как последнее применение характеристик интересные исследования Hurwitz'a[59] об уравнениях, все корни которых имеют отрицательные вещественные части. Задача эта была Hurwitz'у предложена техником Stodola по поводу одного вопроса, касающегося турбин.

Очевидно, что в рассматриваемом случае все корни лежать внутри полукруга, ограниченном полуокружностью бесконечно большого радиуса и осью y-ов.

Как мы видели, на этой полуокружности окажется n точек встречи с линией $\varphi = 0$ таких, что

$$\text{зн. } d(\varphi\psi) = -1,$$

а потому для получения формулы

$$\sum \text{зн. } d(\varphi\psi) = -2n,$$

необходимо допустить, что существует n точек встречи оси y-ов с линией $\varphi = 0$, причем надо двигаться по оси y-ов от $y = -\infty$ до $y = +\infty$.

Для того чтобы все корни функций $\varphi(0, y)$ были вещественные и чтобы при каждом корне y_0 дифференциал $d(\varphi(0, y)\psi(0, y))$ имел знак $-$, необходимо, чтобы корни функций $\varphi(0, y)$ и $\psi(0, y)$ перемежались. Разделяя функцию меньшей степени на функций большей, получим

$$\frac{\psi(0, y)}{\varphi(0, y)} = \frac{s_0}{y} + \frac{s_1}{y^2} + \frac{s_2}{y^3} + \ldots \tag{1}$$

Равенства (7) § 10 показывают, что, если перемежаются корни полиномов $\varphi(0, y)$ и $\psi(0, y)$, то будут перемежаться корни всех рядом стоящих полиномов ряда знаменателей подходящих дробей непрерывной дроби, в которую разлагается дробь (1).

Необходимым и достаточным условием сказанного будет очевидно, положительность всех определителей Δ_k Маркова (см. § 10). Выражая в этом случае определители Δ_k через коэффициенты p_i полинома

$$F(z) = \varphi + i\psi = x^n + p_1 x^{n-1} + p_2 x^{n-2} + \ldots + p_n$$

и предполагая все p_i вещественными, придем к теореме Hurwitz'a.

[59] Mathematische Annalen, B. 46

Необходимыми и достаточным условием для того, чтобы уравнение $F(z) = 0$ *имело только такие корни, у которых вещественная часть отрицательная, состоит в том, чтобы были положительны определитель*

$$\begin{vmatrix} p_1 & 1 & 0 & 0 & 0 & 0 & \dots \\ p_3 & p_2 & p_1 & 1 & 0 & 0 & \dots \\ p_5 & p_4 & p_3 & p_2 & p_1 & 1 & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \end{vmatrix}$$

и все его главные миноры, образованные некоторым числом горизонталей и тем же числом верхних колонн.

Глава XII

О вычислении корней

§ 1

В предыдущих главах мы изучили много свойств корней алгебраических уравнений, причем существование этих корней нами было доказано в двух местах. Теперь мы займемся рассмотрением приемов численного вычисления корней уравнений, у которых коэффициенты заданы численно.

Существует довольно много приемов такого вычисления, данных в разное время различными авторами. Все существующие приемы вычисления корней можно подразделить на две главные категории: одни приемы совершенно общего характера и относятся одинаково как к алгебраическим так и к трансцендентным уравнениям; другие же основаны на специальных свойствах уравнений алгебраических.

Казалось бы, что в курсе алгебры должны быть помещены главным образом эти вторые приемы. Я был однако другого мнения при выборе материала этой главы. Считаю необходимым высказать суждения, которыми я руководился.

Если главу о вычислении корней понимать в том смысле, что ее цель дать изучающему наиболее практичный способ приближенного вычисления корней, тогда надо изложить тот способ, практическое значение которого в настоящее время, действительно, вне всякого сомнения, т. е., способ Gräffe, усовершенствованный Enke.

Не желая однако излагать его в моей книге во всей подробности, я руководствовался такими соображениями. Основанный на простой мысли, способ Enke тогда лишь заслуживает внимания, когда при изложении показан подробно процесс вычисления корней на ряде численных примеров. Такое изложение этого способа находится в книге, известного знатока всевозможных приемов приближенного вычисления и конструктора машин для решения труднейших вопросов интегрального исчисления профессора морской Академии А. Н. Крылова под заглавием: «Лекций о приближенных вычислениях» СПБ. 1911. Для меня не оставалось бы ничего другого, как переписать прекрасное и достаточно подробное изложение автора, занимающее в его книге 47 страниц. Этого я не могу сделать, во первых, потому что моя книга имеет и без того большой объем, во вторых, потому что я предназначаю мою книгу для изучающих чистую математику, а не для техников.

Изучающим чистую математику важнее познакомиться не с техникой вычисления, а с идеями, на которых основан сам прием вычисления. Лицам, желающим быстро вычислять по семизначным логарифмам вещественные и мнимые корни заданного уравнения, можно порекомендовать книгу Крылова, тем более, что эта книга заслуживает внимания не только по изложение способа Gräffe, но также и

по богатству других сведений, которые она дает.

Предназначая далее мою книгу для учащихся в русских университетах, которым читается *исчисление конечных разностей*, как особенный предмет, я считаю возможным не излагать приемов вычисления корней, основанного на применении разностного исчисления.

Итак, я изложу лишь приемы, имеющие значение по важным следствиям, а также сыгравшие известную роль в истории науки, или же связанные с именами первоклассных ученых.

Для более подробного знакомства с историей приемов приближенного вычисления корней можно посоветовать статью Runge «Separation und Approximation der Wurzeln», помещенную в Encyklopedie der Math. Wiss. Band. I. Teil I. Heft 4.

Нахождение соизмеримых корней

§ 2

Рассматривая уравнения с рациональными коэффициентами, мы можем, освободившись от знаменателей, привести всегда такие уравнения к такому виду, что все их коэффициенты будут целые.

Итак, будем рассматривать уравнения с целыми коэффициентами, причем будем предполагать, конечно, что не существуешь общих делителей у коэффициентов.

Покажем, что, *если коэффициент у старшей степени равен единице, а все остальные коэффициенты целые, то, если уравнение имеет рациональные корни, то эти корни могут быть только целые.*

В самом деле, рассмотрим уравнение

$$x^n + p_1 x^{n-1} + p_2 x^{n-2} + \ldots + p_{n-1} x + p_n = 0.$$

Допустим, что это уравнение имеет рациональный корень

$$x = \frac{b}{a},$$

где дробь $\frac{b}{a}$ несократимая, а число $a > 1$.

Покажем, что тогда приходим к противоречию. В самом деле, подставляя $\frac{b}{a}$ в уравнение и умножая на a^{n-1}, получим

$$\frac{b^n}{a} = -p_1 b^{n-1} - p_2 b^{n-2} a - \ldots - p_{n-1} b a^{n-2} - p_n a^{n-1};$$

последнее равенство невозможно, ибо оно дает равенство несократимой дроби, стоящей в левой части, целому числу, стоящему в правой.

Мы видим, следовательно, что знаменатель a должен равняться единице, и рациональный корень должен быть целым.

Если коэффициент при старшей степени будет целое число, отличное от единицы, тогда уравнение с целыми коэффициентами не может иметь рациональных целых корней, а только дробные.

Покажем, что всегда можно свести разыскание рациональных решений на разыскание целых. В самом деле, пусть будет задано уравнение с целыми коэффициентами

$$p_0x^n + p_1x^{n-1} + p_2x^{n-2} + \ldots + p_{n-1}x + p_n = 0. \tag{1}$$

Умножая уравнение (1) на α^n, где α некоторое целое число, и заменяя

$$x\alpha = y,$$

получим

$$y^n + \frac{p_1\alpha}{p_0}y^{n-1} + \ldots + \frac{p_{n-1}\alpha^{n-1}}{p_0}y + \frac{p_n\alpha^n}{p_0} = 0. \tag{2}$$

Остается подобрать α таким образом, чтобы были числами целыми такие выражения

$$\frac{p_1\alpha}{p_0},\quad \frac{p_2\alpha^2}{p_0},\ \ldots,\ \frac{p_n\alpha^n}{p_0},$$

тогда, очевидно, уравнение (2) может иметь только целые рациональные корни. Что касается выбора числа α, то, очевидно, что за это число можно принять p_0, но иногда бывает возможным указать число меньшее.

Итак, займемся решением задачи нахождения целых корней уравнения с целыми коэффициентами

$$x^n + p_1x^{n-1} + \ldots + p_{n-1}x + p_n = 0, \tag{3}$$

где первый коэффициент равен единице.

Если уравнение (3) имеет целый корень a, то первая его часть делится на $x-a$; обозначим частное, происходящее от деления так

$$\varphi(x) = x^{n-1} - q_1x^{n-2} - q_2x^{n-3} - \ldots - q_{n-1},$$

тогда, умножая частное на $x - a$ и сравнивая с коэффициентами уравнений (3), получим ряд равенств

$$\begin{aligned}
p_n &= aq_{n-1},\\
p_{n-1} &= aq_{n-2} - q_{n-1},\\
&\ldots\ldots\ldots\ldots\ldots,\\
p_2 &= aq_1 - q_2,\\
p_1 &= -a - q_1.
\end{aligned}$$

Отсюда получаем, переписывая эти равенства в таком виде

$$\begin{aligned}
q_{n-1} &= \frac{p_n}{a},\\
q_{n-2} &= \frac{p_{n-1} + q_{m-1}}{a},\\
q_{n-3} &= \frac{p_{n-2} + q_{n-2}}{a},\\
&\ldots\ldots\ldots\ldots\ldots,\\
q_1 &= \frac{p_2 + q_2}{a},\\
-1 &= \frac{p_1 + q_1}{a},
\end{aligned} \tag{4}$$

следующее правило для проверки, будет ли целое число a корнем рассматриваемого уравнения. Составляем следующую таблицу, в которой в первом ряду пишем по порядку убывания степени коэффициенты рассматриваемого уравнения

$$\begin{array}{cccccccc} 1 & p_1 & \dots & p_{n-2} & p_{n-1} & p_n & a \\ \hline & +1 & \dots & -q_{n-3} & -q_{n-2} & -q_{n-1} & \end{array}.$$

Первое из равенств (4) показывает, что корень a должен быть делителем последнего коэффициента p_n; частное q_{n-1} от деления даст после перемены знака последний коэффициент функций $\varphi(x)$, который напишем на последнем месте во втором ряде таблицы. Вычитая этот последний член второго ряда таблицы из предпоследнего члена p_{n-1} первого ряда, мы должны получить разность $p_{n-1} + q_{n-1}$, которая делится нацело на a; если такое деление нацело не совершится, то число a не будет корнем рассматриваемого уравнения. Обозначая через q_{n-2} частное от деления $p_{n-1} + q_{n-1}$ на a, получим второй с конца коэффициент $-q_{n-2}$ функции $\varphi(x)$, который помещаем на втором месте справа во втором ряду таблицы. Вычитая этот коэффициент из третьего справа коэффициента первого ряда, деля на a полученную разность и переменяя знак, получим третий справа коэффициент второго ряда. Продолжая таким образом далее, мы убедимся, что целое число a есть корень уравнения в том случае, когда все последовательные деления совершатся нацело и когда n-ый коэффициент второго ряда будет равен $+1$.

Отсюда получается такой способ находить целые корни уравнения: выписываем все делители последнего коэффициента p_n с тем и другим знаком; из этих делителей, очевидно, могут быть корнями только те, которые лежат в границах, указываемых пределами вещественных корней, — только такие делители подлежат проверке указанным выше путем.

Обозначая первую часть заданного уравнения через $f(x)$, получим

$$\frac{f(x)}{x-a} = \varphi(x);$$

подставляя сюда, вместо x значения $+1$ или -1. получим

$$\frac{f(\pm 1)}{a \pm 1} = -\varphi(\pm 1),$$

но $\varphi(\pm 1)$ есть число целое, поэтому прежде чем проверять, будет ли делитель a корнем, по вышеприведенному приему, следует рассмотреть, делится ли нацело на $a-1$ целое число $f(+1)$, а также на $a+1$ целое число $f(-1)$; если которое-нибудь из двух последних делений не совершается нацело, то такой делитель a но будет корнем. Итак, для проверки остаются лишь те делители коэффициента p_n, которые не выходят из пределов вещественных корней и при которых два последних деления совершаются нацело.

§ 3

Поясним теорию примером. Пусть дано уравнение

$$f(x) = x^5 - 34x^3 + 29x^2 + 212x - 300 = 0;$$

имеем

$$f(+1) = -92, \qquad f(-1) = -450.$$

За пределы корней данного уравнения можно взять числа -6 и $+6$.

Придется испробовать следующих делителей числа 300: ± 2, ± 3, ± 4, ± 5.

Число $+3$ не годится, ибо $f(-1)$ не делится на $3+1 = 4$. Точно также не годятся числа: -2, ± 4, -5, ибо $f(+1)$ не делится ни на одно из этих чисел, уменьшенных единицей. Остаются для проверки делители: 2, -3, 5.

Начинаем с делителя 2. Оказывается, число 2 есть корень. Второй

$+1$	0	-34	$+29$	$+212$	-300	2
	$+1$	$+2$	-30	-31	$+150$	2
		1	$+4$	-22	-75	-3
			$+1$	$+1$	-25	5
					$+5$	

ряд таблиц дает коэффициенты функций $\dfrac{f(x)}{x-2}$. Проверяем еще раз делитель 2, ибо 150 продолжат еще делиться на 2. Совершаем проверку над вторым рядом таблицы; получаем третий ряд, дающий коэффициенты функции

$$\frac{f(x)}{(x-2)^2};$$

так как последит коэффициент -75 третьего ряда не делится на 2, то переходим к проверке следующего делителя -3. Этот делитель оказывается корнем, и четвертый ряд таблицы дает коэффициенты функции

$$\frac{f(x)}{(x-2)^2(x+3)}.$$

Следующая проверка делителя 5 приведет уже к отрицательному результату.

Итак, уравнение $f(x) = 0$ может быть переписано так

$$(x-2)^2(x+3)(x^2+x-25) = 0.$$

Уравнение

$$x^2 + x - 25 = 0$$

уже не имеет рациональных корней.

§ 4

Мы видим, что при решении уравнений с какими-угодно коэффициентами можно ограничиться рассмотрением уравнений с рациональными коэффициентами, ибо при иррациональных коэффициентах придется рассматривать приближенные значения таких коэффициентов, которые суть числа рациональные.

Первая задача решения уравнений с рациональными коэффициентами будет состоять в возможном упрощении уравнения; из таких упрощений обязательны прежде всего два следующих: необходимо освободиться от кратных корней, а также найти все соизмеримые корни, тогда, откидывая множители, соответствующее

соизмеримым корням, мы приведем задачу к решению одного или нескольких уравнений с рациональными коэффициентами, не имеющих уже рациональных корней, так что придется вычислить лишь иррациональные корни последних уравнений.

Regula falsi

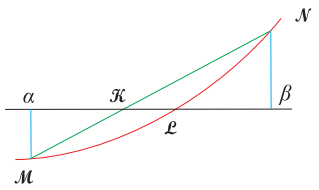
§ 5

Если корень отделен, то найдены два числа α и β таких, что $f(\alpha)$ и $f(\beta)$ разных знаков. Для ясности будем рассматривать задачу геометрически. Будем рассматривать линию, соответствующую уравнению

$$y = f(x) \tag{1}$$

в прямоугольных координатах; тогда абсциссам α и β будут соответствовать ординаты разных знаков. Корень, лежаший в промежутке (α, β) будет абсциссой точки L, в которой кривая пересекает ось x-ов.

Если границы промежутка достаточно близки, то проводя хорду MN, соединяющую точки кривой с абсциссами α и β, можно принять за приближенное значение корня абсциссу точки K встречи с осью x-ов хорды MN. Другими словами, мы принимаем за приближенное значение абсциссу точки, делящей отрезок $\alpha\beta$ пропорционально абсолютным величинам $f(\alpha)$ и $f(\beta)$.



Черт. 14

Уравнение хорды MN, очевидно, будет

$$\frac{y - f(\alpha)}{f(\beta) - f(\alpha)} = \frac{x - \alpha}{\beta - \alpha}.$$

Абсцисса точки встречи ее с осью x-ов получится, полагая $y = 0$, т. е. из уравнения

$$-\frac{f(\alpha)}{f(\beta) - f(\alpha)} = \frac{x - \alpha}{\beta - \alpha},$$

или окончательно

$$x = \frac{\alpha f(\beta) - \beta f(\alpha)}{f(\beta) - f(\alpha)}.$$

Взяв это приближенное значение вместо одного из пределов промежутка (α, β), можем повторить для нового промежутка ту же операцию и таким образом приблизиться к искомому корню. Сказанное вычисление, повторенное достаточное число раз, дает возможность вычислить корень с любою точностью.

§ 6

Newton'ом был предложен способ, носящий название *способ подкасательных*. Мы изложим этот классичесюй прием, годящийся одинаково как для алгебраических уравнений так и для трансцендентных.

Если задано уравнение $f(x) = 0$, то будем рассматривать соответствующую ему линию

$$y = f(x). \tag{1}$$

Решение уравнения состоит в нахождении точки встречи кривой (1) с осью x-ов, имеющей уравнение $y = 0$.

Пусть найдено некоторое приближенное значение α корня уравнения. Если число α не корень, но очень близко к нему, то соответствующее значение $y_\alpha = f(\alpha)$ будет близко к нулю. Точка с координатами $\alpha, f(\alpha)$ будет близка оси x-ов. Применяя общий принцип дифференциального исчисления, состоящий в замене кривой линии вблизи некоторой точки касательною к этой кривой, мы приходим к мысли искать точку встречи касательной, проведенной через точку $\alpha, f(\alpha)$, с осью x-ов. Эта точка встречи дает число более близкое к искомому корню чем α. В этом состоит идея способа Newton'a.

Для осуществления способа напишем уравнение касательной

$$y - f(\alpha) = f'(\alpha)(x - \alpha); \tag{2}$$

для нахождения абсциссы точки встречи с осью x-ов полагаем $y = 0$ и решаем полученное уравнение относительно x

$$x = \alpha - \frac{f(\alpha)}{f'(\alpha)}. \tag{3}$$

Выражение (3) и есть искомое новое приближенное к корню.

Изложим теперь найденный геометрически способ аналитическим путем.

Пусть известно приближенное значение α некоторого корня, тогда сам корень будет выражаться по формуле

$$x = \alpha + u,$$

где u малая поправка, которую нужно придать к неверному значению α корня, чтобы получить его настоящую величину.

Имеем

$$f(\alpha + u) = 0.$$

Раскладывая по формуле Taylor'a, мы получим

$$f(\alpha) + uf'(\alpha) + \frac{u^2}{2!} f''(\alpha) = \ldots = 0.$$

Решая последнее уравнение относительно первой степени u, получим

$$u = -\frac{f(\alpha)}{f'(\alpha)} - \frac{u^2}{2!} \frac{f''(\alpha)}{f'(\alpha)} - \ldots$$

Если приближенное значение α достаточно близко к корню, то число u будет малым числом, высшими степенями которого можно пренебречь в первом приближении; тогда можно считать

$$u = -\frac{f(\alpha)}{f'(\alpha)}$$

и мы приходим к выражению (3).

§ 7

Итак, способ Newton'a состоит в следующем: берется приближенное значение α корня, далее вычисляется новое приближенное значение α_1 по формуле

$$\alpha_1 = \alpha - \frac{f(\alpha)}{f'(\alpha)},$$

по этому значению α_1 составляется новое приближение α_2 по такой же формуле

$$\alpha_2 = \alpha_1 - \frac{f(\alpha_1)}{f'(\alpha_1)}.$$

Продолжая далее вычисление последовательных чисел $\alpha_1, \alpha_2, \alpha_3, \ldots$ по указанным формулам, мы будем приближаться к искомому корню заданного уравнения.

Весьма важное обстоятельство состоит в том, что способ Newton'a был первым примером одного довольно широкого метода современной математики — метода так называемой *итерации* (повторения операций).

Метод итерации состоит в следующем. Берется некоторое число α (безразлично вещественное или комплексное) и некоторая функция $\varphi(x)$ и составляется ряд чисел

$$\alpha_1 = \varphi(\alpha), \quad \alpha_2 = \varphi(\alpha_1), \quad \alpha_3 = \varphi(\alpha_2), \ \ldots;$$

задача состоит в изучении вопроса, когда ряд чисел

$$\alpha, \quad \alpha_1, \quad \alpha_2, \ \ldots$$

имеет предел.

Я лично склонен методу итерации придавать большое значение и считать, не смотря на существование известной литературы, этот метод недостаточно оцененным и разработанным.

§ 8

Приведение в порядок изложенного способа Newton'a требует решения двух основных вопросов: 1) действительно ли последовательное приближение имеет своим пределом корни уравнения и 2) если предел существует, то необходимо оценить погрешность, которую мы делаем, останавливаясь на каком нибудь приближении.

Полный ответ на эти два вопроса был дан Fourier. Чтобы сделать изложение вопроса наиболее ясным, обратимся к геометрическим соображениям. Допустим, что корень, подлежащий вычислению, отделен. Если отделение сделано но методе Fourier, то допустил, что первые указатели суть, например, $1, 0, 0$; тогда в рассматриваемом промежутке (α, β) функция $f(x)$ имеет один простой корень, а $f'(x)$ и

$f''(x)$ сохраняют в промежутке свой знак. Если $f'(x) > 0$, то функция $f(x)$ возрастает, при $f'(x) < 0$ она убывает. Если $f''(x) > 0$, то вогнутость линии $y = f(x)$ внутри промежутка (α, β) направлена кверху, при $f''(x)$ — она направлена книзу.

Докажем теорему.

Если $f'(x)f''(x) < 0$, то вычисление по методу Newton'a, начатое с нижнего предела α промежутка, будет давать числа

$$\alpha_i = \alpha_{i-1} - \frac{f(\alpha_{i-1})}{f'(\alpha_{i-1})}$$

возрастающие, причем $\alpha_i < x_1$, где x_1 корень функции $f(x)$ в промежутке.

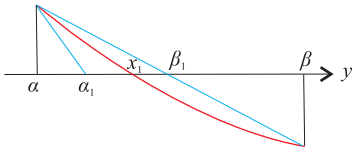
Если же $f'(x)f''(x) > 0$, то можно начать с верхнего предела β и получится ряд чисел убывающих

$$\beta_1 = \beta - \frac{f(\beta)}{f'(\beta)}, \quad \beta_2 = \beta_1 - \frac{f(\beta_1)}{f'(\beta_1)}, \ \ldots,$$

причем $\beta_i > x_1$.

Эта теорема, почти очевидная из геометрических соображений, может быть также просто доказана аналитически. В самом деле, рассмотрим функцию

$$\varphi(x) = x - \frac{f(x)}{f'(x)};$$



Черт. 15

эта функция будет возрастающая в промежутке (α, x_1), если будет иметь место неравенство $f'(x)f''(x) < 0$. На основании доказанного в § 9 главы X видим, что в рассматриваемом промежутке дробь $\dfrac{f(x)}{f'(x)}$ отрицательная, следовательно, $f(x)$ имеет тот же знак что и $f''(x)$; значить, действительно, функция $\varphi(x)$ (см. § 24 главы X) возрастает. Имеем, следовательно, $\varphi(\alpha_1) < \varphi(x_1)$ или, что одно и тоже, $\alpha_1 < x_1$; с другой стороны $\dfrac{f(\alpha)}{f'(\alpha)} < 0$, следовательно, $\alpha_1 > \alpha$ и первая часть теоремы доказана. Подобным же образом докажем и вторую часть теоремы, соответствующую случаю неравенства $f'(x)f''(x) > 0$.

Итак, из только что доказанной теоремы следует, что числа α_i возрастают с возрастанием значка i, но остаются меньше числа x_1; тогда на оснований известной теоремы[60] теории пределов переменное число α_i стремится к пределу. Этот предел будет не чем иным, как корнем x_1, ибо этот предел будет удовлетворять уравнению

$$x = x - \frac{f(x)}{f'(x)}.$$

§ 9

Покажем теперь степень приближения, получаемую при способе Newton'a. Я изменю несколько способ рассуждения моих предшественников, сопоставляя способ подкасательных с правилом regula falsi.

[60] Д. Граве. Введение в анализ 1910. стр. 50.

Ограничимся рассмотрением случая $f'(x)f''(x) < 0$. Нетрудно показать, что если мы обозначим через β_1 выражение

$$\frac{\alpha f(\beta) - \beta f(\alpha)}{f(\beta) - f(\alpha)},$$

то искомый корень x_1 будет внутри промежутка (α_1, β_1). В самом деле, достаточно доказать неравенство $\beta_1 > x_1$. Рассмотрим функцию

$$\psi(x) = \frac{\alpha f(x) - x f(\alpha)}{f(x) - f(\alpha)};$$

первая производная от этой функции будет

$$\psi'(x) = \frac{f(\alpha)}{[f(x) - f(\alpha)]^2} \{f(\alpha) - f(x) - (\alpha - x)f'(x)\} = \frac{f(\alpha)(\alpha - x)f''(\xi)}{2[f(x) - f(\alpha)]^2},$$

где ξ заключается между α и x. Значение $f(\alpha)$, очевидно, обратно по знаку со значением производной $f'(x)$, — значит, $f(\alpha)$ одного знака с $f''(\xi)$. Итак, функция $\psi(x)$ возрастающая; следовательно,

$$\psi(x_1) < \psi(\beta)$$
$$x_1 < \beta_1.$$

Для нахождения степени приближения к корню x_1 рассмотрим разность $\beta_1 - \alpha_1$; получаем

$$\beta_1 - \alpha_1 = \frac{\alpha f(\beta) - \beta f(\alpha)}{f(\beta) - f(\alpha)} - \alpha + \frac{f(\alpha)}{f'(\alpha)} = \frac{(\alpha - \beta)f(\alpha)}{f(\beta) - f(\alpha)} + \frac{f(\alpha)}{f'(\alpha)} =$$
$$= \frac{f(\alpha)[f(\beta) - f(\alpha) - (\beta - \alpha)f'(\alpha)}{f'(\alpha)[f(\beta) - f(\alpha)]} = \frac{f(\alpha)(\beta - \alpha)^2 f''(\eta)}{2(\beta - \alpha)f'(\zeta)f'(\alpha)},$$

где числа ζ и η заключаются между α и β, но

$$\frac{f(\alpha)}{f'(\alpha)} = \alpha - \alpha_1,$$

следовательно, получим

$$\beta_1 - \alpha_1 = (\alpha_1 - \alpha)(\beta - \alpha)\left[- \frac{f''(\eta)}{2f'(\zeta)}\right].$$

Если мы обозначим через m наибольшее значение абсолютной величины второй производной в данном промежутки, а через p наименьшее значение абсолютной величины первой производной, то положительное число

$$-\frac{f''(\eta)}{2f'(\zeta)}$$

меньше $\dfrac{m}{2p} = M$. Кроме того $\alpha_1 - \alpha < \beta - \alpha$, следовательно,

$$\beta_1 - \alpha_1 < (\beta - \alpha)^2 M. \tag{1}$$

Повторив операцию методы Newton'a и правило regula falsi, т. е. взяв числа

$$\alpha_2 = \alpha_1 - \frac{f(\alpha_1)}{f'(\alpha_1)}, \qquad \beta_2 = \frac{\alpha_1 f(\beta_1) - \beta f(\alpha_1)}{f(\beta_1) - f(\alpha_1)},$$

получим

$$\beta_2 - \alpha_2 < (\beta_1 - \alpha_1)^2 M. \tag{2}$$

Продолжая таким образом далее, мы получим

$$\beta_m - \alpha_m < (\beta_{m-1} - \alpha_{m-1})^2 M. \tag{m}$$

Возвышая неравенство (1) в степень 2^{m-1}, неравенство (2) в степень 2^{m-2} и т. д., наконец, неравенство (m) в степень 2^0, получим

$$\begin{aligned}
(\beta_1 - \alpha_1)^{2^{m-1}} &< (\beta - \alpha)^{2^m} M^{2^{m-1}}, \\
(\beta_2 - \alpha_2)^{2^{m-2}} &< (\beta_1 - \alpha_1)^{2^{m-1}} M^{2^{m-2}}, \\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots, \\
(\beta_m - \alpha_m) &< (\beta_{m-1} - \alpha_{m-1})^2 M.
\end{aligned}$$

Перемножая эта неравенства, получим

$$\beta_m - \alpha_m < (\beta - \alpha)^{2^m} M^{1+2+2^2+\ldots+2^{m-1}}$$

или

$$\beta_m - \alpha_m < (\beta - \alpha)[(\beta - \alpha)M]^{2^{m-1}}.$$

Можно всегда выбрать первоначальный промежуток (α, β) столь малым, что будет сразу

$$\beta - \alpha < \varepsilon, \qquad (\beta - \alpha)M < \varepsilon,$$

где ε правильная дробь, а тогда получим

$$\beta_m - \alpha_m < \varepsilon^{2^m}.$$

Мы приходим к весьма важному заключению, что приближение величины α_m к искомому корню x_1 меньше ε^{2^m}.

Способ Lagrange'a

§ 10

Способ Lagrange'a состоит в разложении вещественных корней уравнения с рациональными коэффициентами в непрерывные дроби.

Возьмем уравнение

$$f(x) = p_0 x^n + p_1 x^{n-1} + \ldots + p_{n-1} x + p_n = 0. \tag{1}$$

Будем рассматривать только положительные корни, ибо в случае отрицательных корней можно заменить x на $-x$.

Положим, что между двумя натуральными числами a и $a+1$ существует один или несколько последовательных корней уравнения (1); мы имеем всегда возможность предполагать, что таких корней будет только один, ибо умножением x на некоторое достаточно большое число k можно достигнуть того, что новое уравнение относительно kx будет иметь такие корни, что все разности между двумя последовательными корнями будут не менее единицы, а тогда между каждыми двумя натуральными числами, стоящими рядом, будет существовать не больше одного корня.

Итак, предположим, что в промежутке $(a, a+1)$ существует один корень уравнения (1). Этот корень можно будет написать в таком виде

$$x = a + \frac{1}{x_1}, \tag{2}$$

где x_1 неправильная дробь. Подставим выражение (2) в уравнение (1), получим новое уравнение относительно x_1 той же степени n. Пусть это уравнение будет иметь вид

$$f_1(x_1) = p_0^{(1)} x_1^n + p_1^{(1)} x_1^{n-1} + \ldots + p_n^{(1)} = 0. \tag{3}$$

Уравнение (3) будет иметь только один корень больший единицы, ибо, если бы оно имело более одного корня, большего единицы, то уравнение (1) имело бы более одного корня, лежащего в промежутка $(a, a+1)$.

Пусть корень уравнения (3) заключается между двумя целыми положительными числами a_1 и $a_1 + 1$; тогда этот корень можно будет выразить формулой

$$x_1 = a_1 + \frac{1}{x_2}. \tag{4}$$

Подставляя последнее выражение в уравнение (3), получим новое уравнение

$$f_2(x_2) = p_0^{(2)} x_2^n + p_1^{(2)} x_2^{n-1} + \ldots + p_n^{(2)} = 0. \tag{5}$$

Продолжая таким образом далее получим разложение корня в непрерывную дробь

$$a + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots}}.$$

Если корень рациональный, то непрерывная дробь оканчивается. В этом обстоятельстве заключается преимущество способа Lagrange'a, ибо при других способах, как бы далеко ни продолжать приближение к корню, нельзя будет заметить рациональности вычисляемого корня, если таковая случайно имеет место и мы предварительно не нашли по приемам §§ 2–4 всех рациональных корней. Если непрерывная дробь бесконечная, то мы получаем способ приближенного вычисления корня, состоящий в вычислении подходящих дробей $\frac{P_m}{Q_m}$.

Lagrange показал, как вычислять последовательные уравнения

$$f_1(x_1) = 0, \quad f_2(x_2) = 0, \ \ldots, \ f_m(x_m) = 0, \ \ldots$$

В самом деле, имеем

$$f_i(x_i) = f_i\left(a_i + \frac{1}{x_{i+1}}\right) = f_i(a_i) + \frac{1}{x_{i+1}} f_i'(a_i) + \ldots + \frac{1}{x_{i+1}^n} \frac{f_i^{(n)}}{1 \cdot 2 \cdots n},$$

следовательно, преобразованное уравнение $f_{i+1}(x) = 0$ имеет вид (здесь мы пропускаем у x_{i+1} значок $i+1$)

$$x^n f_i(a_i) + x^{n-1} f_i'(a_i) + \ldots + \frac{f_i^{(n)}(a_i)}{1 \cdot 2 \cdots n} = 0,$$

так что

$$p_0^{(i+1)} = f_i(a_i), \quad p_1^{(i+1)} = f_i'(a_i), \ \ldots, p_n^{(i+1)} = \frac{1}{n!} f_i^{(n)}(a_i).$$

Понимая, что описанное разложение корня в непрерывную дробь сопровождается довольно громоздкими выкладками, Lagrange усовершенствовал свой способ, указав на очень хороший прием продолжения вычисления ряда чисел

$$a, \quad a_1, \quad a_2, \ \ldots$$

когда известны несколько первых.

§ 11

Поясним теорию Lagrange'а примером.

Возьмем уравнение

$$x^3 - 7x + 7 = 0;$$

применяя теорию Lagrange'а, получим три корня в таком виде

$$x_1 = 1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{4 + \cfrac{1}{\omega}}}}, \qquad x_2 = 1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{4 + \cfrac{1}{\omega}}}},$$

$$x_3 = 3 + \frac{1}{\omega},$$

где ω есть неполное частное общее для всех трех непрерывных дробей. Число ω будет корнем уравнения

$$\omega^3 - 20\omega^2 - 9\omega - 1 = 0.$$

Начиная с места ω, во всех трех непрерывных дробях будут следовать неполные частные в одной и той же последовательности.

Мы опять приходим к новому преимуществу методы Lagrange'а, помогающему заметить свойство заданного уравнения, что все три его корня выражаются рационально через ω

$$x_1 = \frac{19\omega + 4}{14\omega + 3}, \quad x_2 = \frac{22\omega + 5}{13\omega + 3}, \quad x_3 = \frac{-1 - 3\omega^2}{\omega}.$$

Исключая ω, получим

$$x_1 = \frac{7-4x_3}{5-3x_3}, \qquad x_2 = \frac{7-5x_3}{4-3x_3};$$

итак, метода Lagrange'a дает возможность заметить свойство заданного уравнения, которое мы будем в дальнейшем называть свойством *нормальности* и которое состоит в том, что через один его корень выражаются рационально остальные корни.

§ 12

Поставим теперь задачу: *найти все нормальные уравнения третьей степени*

$$x^3 + p_1x^2 + p_2x + p_3 = 0, \tag{1}$$

где p_1, p_2, p_3 целые числа.

Обозначая через Δ дискриминант, получим

$$\Delta = (x-x_1)^2(x-x_2)^2(x_1-x_2)^2 =$$
$$= -(4p_2^3 + 27p_3^2) + 18p_1p_2p_3 + p_1^2p_2^2 - 4p_1^3p_3.$$

В последней формул через x, x_1, x_2 обозначены три корня уравнения (1).

Умножая тождество

$$\sqrt{\Delta} = (x-x_1)(x-x_2)(x_1-x_2)$$

на $x_1 - x_2$, получим

$$(x_1-x_2)\sqrt{\Delta} = [(x_1-x_2)(x_1-x)]\,[(x_2-x)(x_2-x_1)].$$

По $(x_1-x)(x_1-x_2)$ есть значение, которое принимает производная первой части уравнения (1) при корн x_1, следовательно,

$$(x_1-x)(x_1-x_2) = 3x_1^2 + 2p_1x_1 + p_2;$$

подобным же образом

$$(x_2-x)(x_2-x_1) = 3x_2^2 + 2p_1x_2 + p_2.$$

Отсюда

$$(x_1-x_2)\sqrt{\Delta} = (3x_1^2 + 2p_1x_1 + p_2)(3x_2^2 + 2p_1x_2 + p_2)$$
$$= 9x_1^2x_2^2 + 6p_1x_1x_2(x_1+x_2) + 3p_2(x_1+x_2)^2 + (4p_1^2 - 6p_2)x_1x_2 + \tag{2}$$
$$+2p_1p_2(x_1+x_2) + p_2^2.$$

Кроме того имеем

$$x_1 + x_2 = -x - p_1, \quad x_1x_2 = -(x_1+x_2)x + p_2 = x^2 + p_1x + p_2. \tag{3}$$

Формулы (3) дают возможность выразить правую часть уравнения (2) через корень x

$$(x_1 - x_2)\sqrt{\Delta} = 9x^4 + 12p_1x^3 + (15p_2 + p_1^2)x^2 + \\ +(10p_1p_2 - 2p_1^3)x + 4p_2^2 - p_1^2p_2.$$

Мы можем понизить при помощи уравнения (1) на дее единицы степень последняго выражения

$$(x_1 - x_2)\sqrt{\Delta} = (6p_2 - 2p_1^2)x^2 - (9p_3 - 7p_1p_2 + 2p_1^3)x + \\ +4p_2^2 - p_1^2p_2 - 3p_1p_3.$$

Решая относительно x_1 и x_2 последнее уравнение и первое из (3), получим для этих корней выражения по формуле

$$\frac{1}{2\sqrt{\Delta}}\,[(6p_2 - 2p_1^2)x^2 - (9p_3 - 7p_1p_2 + 2p_1^3 + \sqrt{\Delta})x + \\ +4p_2^2 - p_1^2p_2 - 3p_1p_3 - p_1\sqrt{\Delta}],$$

полагая последовательно в ней $\sqrt{\Delta}$ равным его обоим значениям.

Итак, мы видим, что *рационалное выражение одного корня через другой получится, если* Δ *— число положительно и полный квадрат целого числа.*

Так в примере § 11 $p_1 = 0$, $p = -7$, $p_3 = 7$ и мы получаем

$$\Delta = 7^2.$$

§ 13

В предыдущих параграфах мы подчеркнули характер методы Lagrange'a, дающий возможность судить об арифметической природе подлежащего вычисление корня. Этот характер проявился с особенной рельефностью при приложений методы к уравнениям второй степени с рациональнымн коэффициентами. Оказался поразительный факт, что корни таких уравнений (и конечно только таких) разлагаются в *периодические* непрерывные дроби.

Эта теорема Lagrange'a заставила математиков в продолжении всего 19-го столетия искать новый способ приближенного вычисления корней алгебраических уравнений, приводящий к периодическому алгоритму, представляющему для кубических уравнений обобщение алгоритма непрерывных дробей.

Заслуга нахождения этого алгоритма принадлежит выдающемуся русскому математику г. Вороному, изложившему свой способ в трактате «Об одном обобщении алгоритма непрерывных дробей» Варшава 1896.

Преждевременная смерть прекратила научную деятельность, носившую отпечаток гениальности. Долг русских ученых продолжить исследования Вороного, ибо все говорить в пользу возможности дальнейших обобщений на уравнения высших степеней.

Наконец, нельзя не упомянуть о том, что в связи с разложением корней алгебраических уравнений в непрерывные дроби была замечена в первый раз Liouville'-ем[61] возможность доказательства существования чисел трансцендентных.

На основании сказанного в § 16 главы III *алгебраическим числом* называется корень всякого уравнения

$$f(x) = p_0x^n + p_1x^{n-1} + \ldots + p_n = 0, \tag{1}$$

коэффициенты которого целые числа.

Будем раскладывать иррациональный вещественный корень α уравнения (1) в непрерывную дробь

$$\alpha = a\cfrac{1}{a_1 + \cfrac{1}{a_2+\ddots}}.$$

Рассмотрим промежуток $(\mathfrak{a}, \mathfrak{b})$, в котором находится корень α. Пусть $\dfrac{P_n}{Q_n}$ некоторая подходящая дробь, настолько близкая к корню α, что она также находится внутри промежутка $(\mathfrak{a}, \mathfrak{b})$.

Для всех значений x в промежутке $(\mathfrak{a}, \mathfrak{b})$ будет

$$|f'(x)| < M,$$

где M величина исключительно зависящая от промежутка.

Применяя теорему Lagrange'a[62], получим

$$f\left(\frac{P_n}{Q_n}\right) = \left(\frac{P_n}{Q_n} - \alpha\right) f'\left[\alpha + \theta\left(\frac{P_n}{Q_n} - \alpha\right)\right], \qquad 0 < \theta < 1.$$

Так как величина $\alpha + \theta\left(\dfrac{P_n}{Q_n} - \alpha\right)$ находится также внутри интервала $(\mathfrak{a}, \mathfrak{b})$, то мы получим

$$\left|f\left(\frac{P_n}{Q_n}\right)\right| < \left|\frac{P_n}{Q_n} - \alpha\right| M;$$

отсюда

$$\left|\frac{P_n}{Q_n} - \alpha\right| > \frac{\left|f\left(\frac{P_n}{Q_n}\right)\right|}{M}. \tag{2}$$

Из теории непрерывных дробен известно[63]

$$\frac{P_n}{Q_n} - \alpha = \frac{(-1)^n}{Q_n(Q_n\alpha_n + Q_{n-1})}, \qquad \alpha_n = a_n + \cfrac{1}{a_{n+1}+\ddots}.$$

[61] Journal de Liouville, t. XVI.

[62] Д. Граве. Энциклопедия математики 1912. стр. 189.

[63] Д. Граве. Элементарный курс теории чисел. 1913 г. Стр. 187.

Отсюда, принимая во внимание $\alpha_n > a_n$, получим

$$\left|\frac{P_n}{Q_n} - \alpha\right| < \frac{1}{a_n Q_n^2}. \tag{3}$$

Сопоставляя (2) и (3), получим

$$a_n < \frac{M}{Q_n^2 \left| f\left(\frac{P_n}{Q_n}\right)\right|}.$$

Далее мы имеем

$$\frac{P_n}{Q_n} = \frac{A}{Q_n^r},$$

где A некоторое целое положительное или отрицательное число; значит

$$\left| f\left(\frac{P_n}{Q_n}\right)\right| \geq \frac{1}{Q_n^r},$$

и мы приходим к неравенству Liouville'a

$$a_n < M Q_n^{r-2}. \tag{4}$$

Стоит только написать такую непрерывную дробь, у которой неравенство (4) не удовлетворяется, чтобы быть уверенным что такая дробь не может быть алгебраическим числом. Эта дробь будет числом новой природы, которое называется *трансцендентным.*

Метода Gauss'a для трехчленных уравнений

§ 15

Трехчленными называются уравнения вида

$$x^{q+p} + 2ax^q + \beta = 0,$$

которые заключают только три члена. Такие уравнения часто встречаются. Кроме случаев квадратного и кубического уравнения мы можем напомнить (§ 35 главы IX) преобразовало Jerrard'a, которое приводить общее уравнение 5-ой степени к трехчленному виду.

Я говорю в моей книге о трехчленных уравнениях, потому что C. Fr. Gauss обратил внимание на эти уравнения и дал[64] прекрасный способ их решения. В 1896 году Gundelfingen[65] публиковал таблицы, облегчающие выкладки этого решения. Я покажу здесь мое видоизменение способа Gauss'a, относящееся к вычисление вещественных корней трехчленных уравнений. Мой способ основан на

[64]Gauss Werke, Bd. III, s. 85. Beitrage zur Theorie der algebraischen Gleichungen. Zweite Abhandlung. (1849).

[65]Gundelfingen. Tafeln zur Berechnung der reellen Wurzeln sammtlicher trinomiscben Gleichungen (Leipzig 1896).

применении метода итераций. Этот способ еще в бытность мою студентом Петербургского Университета 1883 г. я показывал товарищам. Я ничего не публиковал о нем, ибо подробное теоретическое проведение не привело меня к новым в идейном отношении результатам. Способ рассуждения не отличался по существу от тех соображений, с которыми связано приложение известиого ряда Lagrange'a[66].

Здесь я привожу мой способ, ибо при практическом вычислении он не хуже способа Gauss'a, но имеет преимущество в мнемоническом отношений и его буквально нельзя забыть, если он был один раз известен.

Возвысим уравнение

$$x^q(x^p + 2a) = -\beta$$

в степень p

$$x^{pq}(x^p + 2a)^p = (-1)^p\beta^p$$

и положим

$$x^p + a = z, \tag{1}$$

тогда уравнение принимает вид

$$(z + a)^p(z - a)^q = b, \tag{2}$$

где

$$b = (-1)^p\beta^p.$$

Итак, мы пришли к уравнение (2), которое мы уже исследовали по теореме Sturm'a (см. § 6 главы XI). На основании (1) всякому вещественному корню заданного трехчленного уравнения будет соответствовать вещественный же корень преобразованного уравнения (2). Применяя теорему Sturm'a, мы видели, что это уравнение не может иметь четырех вещественных корней.

Уравнение (2) можно преобразовать так[67]

$$z = a + \frac{\sqrt[q]{b}}{\frac{p}{q}(a + z)} \tag{3}$$

Подставляя в скобках знаменателя вместо z все выражение (3) придем к бесконечному периодическому алгоритму

$$z = a + \frac{\sqrt[q]{b}}{\frac{p}{q}(2a + \frac{\sqrt[q]{b}}{\frac{p}{q}(2a + \ddots}}. \tag{4}$$

Подобным же образом, преобразуя уравнение (2) так

$$z = -a + \frac{\sqrt[q]{b}}{\frac{q}{p}(-a + z)}, \tag{5}$$

[66]Э. Гурса. Курс математического анализа. Перев. Некрасова под ред. Млодзеевского, Москва (1911). Стр. 433.

[67]Здесь показатель $\frac{p}{q}$ для удобства написан с левой стороны.

получим другой алгоритм

$$z = -a + \cfrac{\sqrt[q]{b}}{\frac{q}{p}(-2a + \cfrac{\sqrt[q]{b}}{\frac{q}{p}(-2a + \ddots}}. \tag{6}$$

Этот алгоритм представляет обобщение непрерывных дробей в том смысле, что при непрерывных дробях чередуются две операции: деление и сложение; здесь же чередуются три операции: возвышение в степень с показателем $\frac{q}{p}$, деление и сложение.

При q четном в алгоритме (4) можно брать радикал $\sqrt[q]{b}$ с тем или другим знаком, подобным же образом при p четном можно изменить знак при радикале $\sqrt[q]{b}$ в алгоритме (6).

Оказывается, что при помощи четырех, получаемых таким образом алгоритмов можно вычислить все вещественные корни уравнения (2).

Покажем приложение этой методы к численному уравнению.

Вычислим вещественные корни уравнения

$$x^5 - 4x - 2 = 0,$$

полагая

$$x^4 - 2 = z,$$

получим новое уравнение в том виде

$$(z+2)(z-2)^4 = 16. \tag{7}$$

По соображениям § 6 главы XI уравнение (7) должно иметь только три вещественных корня.

Мы получаем действительно следующих три алгоритма для вычисления этих трех корней z_1, z_2, z_3:

$$\frac{z_1+2}{4} = 1 + \cfrac{\cfrac{1}{2\sqrt{2}}}{\sqrt[4]{1 + \cfrac{\cfrac{1}{2\sqrt{2}}}{\sqrt[4]{1+}\ddots}}}, \tag{8}$$

$$\frac{z_2+2}{4} = 1 - \cfrac{\cfrac{1}{2\sqrt{2}}}{\sqrt[4]{1 - \cfrac{\cfrac{1}{2\sqrt{2}}}{\sqrt[4]{1-}\ddots}}}, \tag{9}$$

$$\frac{-z_3+2}{4} = 1 - \cfrac{2^{-6}}{{}^4(1 - \cfrac{2^{-6}}{{}^4(1-\ddots}}. \tag{10}$$

Теперь я покажу подробно, как вычислить по моему алгоритму корни. Мы возьмем семизначные логарифмические таблицы, а также таблицы Gauss'овых логарифмов, носящих заглавие: «Tafeln der Additions und Substractions Logarithmen für sieben Stellen». Berechnet von I. Zech. Berlin. 1863.

Изобретение Gauss'ом логарифмов сумм и разностей показывает, что этот «princeps mathematicorum», провидевший орлиным взором глубочайшие современные теории, не гнушался, когда дело шло о практическом вычислении, предлагать действительно удобные в практическом отношении приемы. Таков удел гения, который велик как в теории так и на практики.

Начнем с вычисления алгоритма (8) § 15

$$\lg \frac{1}{2\sqrt{2}} = 9,5484550.$$

Логарифм числа $1 + \dfrac{1}{2\sqrt{2}}$ вычисляем, применяя Zech'овские логарифмы сумм. По этим логарифмам действие производится так. Положим, что требуется вычислить $\lg(A + B)$, где $A > B$. Находим $\lg A$ и $\lg B$; вычисляем разность $g = \lg - \lg B$; по числу g ищем соответственное число G в таблицы Zech'а, относящейся к сложению (в указанном издании таблица № XII стр. 636). Искомый логарифм будет

$$\lg(A + B) = \lg A + G.$$

Итак, для нашего случая $g = \lg 1 - \lg \dfrac{1}{2\sqrt{2}} = 0 - 9,5484550 = 0.4525450$. По таблице получаем $G = 0,1314754$, значит, $\lg\left(1 + \dfrac{1}{2\sqrt{2}}\right) = \lg 1 + G = 0,1314754$. Извлекаем корень четвертой степени, тогда получим

$$k_1 = \lg \sqrt[4]{1 + \frac{1}{2\sqrt{2}}} = 0,0328688.$$

Повторяем операцию моего алгоритма т. е. вычисляем по Zech'овским таблицам

$$\lg \left\{ 1 + \frac{\dfrac{1}{2\sqrt{2}}}{\sqrt[4]{1 + \dfrac{1}{2\sqrt{2}}}} \right\}.$$

Не объясняя подробно всех действий я приведу полное вычисление логарифма величины

$$\frac{z_1 + 2}{4}$$

до семи знаков.

Вторая итерация:

$$\lg\frac{1}{2\sqrt{2}} = 9,5484550$$
$$k_1 = 0,0328688$$
$$9,5155862$$
$$\text{доп.} = 0,4888138$$
$$G_1 = 0,1231271$$
$$\text{дел. на } 4 = 0,0307818 = k_2$$

Третья итерация:

$$\lg\frac{1}{2\sqrt{2}} = 9,5484550$$
$$k_2 = 0,0307818$$
$$9,5176732$$
$$\text{доп.} = 0,4823268$$
$$G_2 = 0,1236432$$
$$\text{дел. на } 4 = 0,0309108 = k_3$$

Четвертая итерация:

$$\lg\frac{1}{2\sqrt{2}} = 9,5484550$$
$$k_3 = 0,0309108$$
$$9,5175442$$
$$\text{доп.} = 0,4824558$$
$$G_3 = 0,1236113$$
$$\text{дел. на } 4 = 0,0309048 = k_4$$

Пятая итерация:

$$\lg\frac{1}{2\sqrt{2}} = 9,5484550$$
$$k_4 = 0,0309028$$
$$9,5175522$$
$$\text{доп.} = 0,4824478$$
$$G_4 = 0,1236133$$

Шестая итерация уменьшает лишь на единицу последнюю цифру

$$\lg\frac{z_1+2}{4} = 0,1236132.$$

Получаем

$$z_1 + 2 = x_1^4 = 5,31708.$$

Уравнение

$$(x_1^4 - 4)x_1 = 2$$

показывает, что корень x_1 должен быть числом положительным; получаем

$$x_1 = 1,518512. \tag{1}$$

Подобным же образом мы вычислим оба других алгоритма (9), (10) § 15, применяя таблицу логарифмов разностей (таблицу Zech'a № XII стр. 681). По этой таблице для вычисления $\lg(A-B)$, вычисляется разность $g = \lg A - \lg B$, но g находится соответственное число G таблицы и окончательно $\lg(A-B) = \lg A - G$.

Я привожу здесь полное вычисление обоих алгоритмов.

Алгоритм (9) § 15.

Первая итерация:

$$9,5484550$$
$$g = 0,4515450$$
$$G = 0,1894672$$
$$\text{доп.} = 9,8105328$$
$$\frac{1}{4}\cdot = 9,9526332 = k_1$$

Вторая итерация:

$$9,5484550$$
$$k_1 = 9,9526332$$
$$9,5958218$$
$$g_1 = 0,4041782$$
$$G_1 = 0,2177392$$
$$\text{доп.} = 9,7822608$$
$$\frac{1}{4}\cdot = 9,9455652 = k_2$$

Третья итерация:

$$9,5484550$$
$$k_2 = 9,9455652$$
$$9,6028898$$
$$g_2 = 0,3971102$$
$$G_2 = 0,2224029$$
$$\text{доп.} = 9,7775971$$
$$\frac{1}{4}\cdot = 9,9443993 = k_3$$

Четвертая итерация:

$$\begin{array}{r} 9548550 \\ {}_3 = 99443993 \\ 9,6040557 \\ \hline g_3 = 0,3959443 \\ \hline G_3 = 0,2232844 \\ \hline \text{доп. } = 9,7767156 \end{array}$$

$$\frac{1}{4}\cdot = 9,9441789 \quad = k_4$$

Пятая итерация:

$$\begin{array}{r} 9,5484550 \\ k_4 = 9,9441789 \\ \hline 9,6042761 \\ g_4 = 0,3957239 \\ \hline G_4 = 0,2233325 \\ \hline \text{доп. } = 9,7766675 \end{array}$$

$$\frac{1}{4}\cdot = 9,9441669 \quad = k_5$$

Шестая итерация:

$$\begin{array}{r} 9,5484550 \\ k_5 = 9,9441669 \\ \hline 9,6042881 \\ g_5 = 0,3957119 \\ \hline G_5 = 0,2233405 \\ \hline \text{доп. } = 9,7766595 \end{array}$$

Седьмая итерация дает окончательно

$$\lg \frac{z_2 + 2}{4} = 9,7766592.$$

Получаем

$$z_2 + 2 = x_2^4 = 2,391769,$$

откуда искомый корень z_2 будет

$$x_2 = -1,243597. \tag{2}$$

Алгоритм (10) § 15.

$$\lg 2^{-6} = 8,1938200.$$

Первая итерация:

$$\begin{array}{r} 8,1938200 \\ g = 1,8061800 \\ \hline G = 0,0068405 \\ \hline \text{д. } = 9,9931595 \end{array}$$

$$4\cdot = 9,9726380 \quad = k_1$$

Вторая итерация:

$$\begin{array}{r} 8,1938200 \\ k_1 = 9,9726380 \\ \hline 8,2211820 \\ g_1 = 1,7788180 \\ \hline G_1 = 0,0072880 \\ \hline \text{д. } = 9,9927120 \end{array}$$

$$4\cdot = 9,9708480 \quad = k_2$$

Третья итерация:

$$\begin{array}{r} 8,1938200 \\ k_1 = 9,9708480 \\ 8,2229720 \\ g_2 = 1,7770280 \\ \hline G_2 = 0,0073197 \\ \hline \text{д. } = 9,9926803 \end{array}$$

$$4\cdot = 9,9707212 \quad = k_3$$

Четвертая итерация:

$$\begin{array}{r} 8,1938200 \\ k_3 = 9,9707212 \\ \hline 8,2230988 \\ g_3 = 1,7769012 \\ \hline G_3 = 0,0073215 \\ \hline \text{д. } = 9,9926785 \end{array}$$

Пятая итерация дает окончательно

$$\lg \frac{-z_3 + 2}{4} = \lg \frac{4 - x_3^4}{4} = 9,9926786,$$

откуда

$$x_3 = -0,5087044. \tag{3}$$

Итак, все три вещественных корня заданного уравнения вычислены.

Обращаясь теперь к вычисление мнимых корней трехчленного уравнения, мы возьмем способ Gauss'a, ибо этот способ едва ли подлежит упрощению в общем случае.

Итак, нам надо найти мнимые корни уравнения

$$x^{q+p} + 2ax^q + \beta = 0, \tag{1}$$

где a и β числа вещественные.

Полагая $x = r(\cos\varphi + i\sin\varphi)$, подставляя в уравнение (1) и приравнивая нулю коэффициент при i, получим

$$r^p = -\frac{2a\sin q\varphi}{\sin(p+q)\varphi}. \tag{2}$$

Перепишем теперь уравнение (1) так

$$x^p + 2a + \beta x^{-q} = 0. \tag{3}$$

Если мы относительно (3) сделаем туже операцию, то получим

$$r^p = \beta\,\frac{\sin q\varphi}{\sin p\varphi}, \tag{4}$$

исключая r из уравнений (2) и (4), получим

$$\Omega(\varphi) = \lambda, \tag{5}$$

где

$$\lambda = (-1)^{p+q}\,\frac{(2a)^{p+q}}{\beta^p}, \qquad \Omega(x) = \frac{[\sin(p+q)x]^{p+q}}{[\sin px]^p\,\sin[qx]^q}.$$

Подчеркнем главнейшие свойства функции $\Omega(x)$.

I. Ее производная определяется из уравнения

$$\frac{\Omega'(x)}{\Omega(x)}\,\frac{\sin(p+q)x}{\sin px\,\sin qx} = -(p+q)^2 - (p\operatorname{ctg} px - q\operatorname{ctg} qx)^2,$$

из которого следует, что знак производной $\Omega'(x)$ совпадет со знаком выражения

$$-\frac{\sin(p+q)x}{\sin px\,\sin qx}\,\Omega(x).$$

II.

$$\Omega(-x) = \Omega(x), \qquad \Omega(\pi - x) = \Omega(x).$$

Эти равенства показывают, что достаточно рассмотреть значения x, заключающаяся между 0 и π.

III.

$$\Omega(0) = \frac{(p+q)^{p+q}}{p^p\,q^q}. \tag{6}$$

IV. В промежутке $\left(0, \frac{\pi}{p+q}\right)$ функция $\Omega(x)$ убывает от значения (6) до нуля.

Когда найдены все значения φ, удовлетворяющие уравнению (5) и лежашие в промежутке $(0, \pi)$, то из них надо откинуть те, по которым получается из уравнений (2) и (4) для величин r^p или r^{p+q} числа отрицательные. Gauss обратил внимание на следующее обстоятельство. Если мы прологарифмируем уравнением (5), ограничиваясь случаем $\lambda > 0$, то получаем

$$\lg \Omega(\varphi) = \lg \lambda.$$

Выражение $\lg \Omega(\varphi)$ вычисляется просто без пропорционального интерполирования для тех значений угла φ, для которых в таблице $\lg \sin x$ указаны соответствующие числа, ибо, если φ_0 есть некоторое табличное число, то и $\lg \sin p\varphi_0$, $\lg \sin q\varphi_0$, $\lg \sin(p+q)\varphi_0$ находятся прямо в таблице (без интерполирования). Итак, для всякого табличного угла φ_0 вычисление $\lg \Omega(\varphi)$ производится очень просто. Gauss предлагает найти два рядом стоящие табличные числа φ_0 и φ_1 такие, чтобы было

$$\lg \Omega(\varphi_0) \geq \lg \lambda, \qquad \lg \Omega(\varphi_1) \leq \lg \lambda;$$

другими словами, чтобы корень φ уравнения (5) заключался между числами φ_0 и φ_1. Для семизначных таблиц разность $\varphi_1 - \varphi_0$, как известно, равна $10''$. Обыкновенно небольшое число проб приводить к нахождению чисел φ_0 и φ_1; окончательное же вычисление корня φ совершается по правилу regula falsi, т. е. пропорциональным интерполированием.

§ 18

Покажем на численном примере способ вычисления мнимых корней. Возьмем тоже самое уравнение

$$x^5 - 4x - 2 = 0,$$

$$p = 4, \quad q = 1, \quad a = -2, \quad \beta = -2.$$

Уравнения (2) и (4) § 17 имеют в данном случае вид

$$r^4 = \frac{4 \sin \varphi}{\sin 5\varphi}, \qquad r^5 = -2 \frac{\sin 4\varphi}{\sin 5\varphi},$$

следовательно, должно быть

$$\sin \varphi > 0, \quad \sin 5\varphi > 0, \quad \sin 4\varphi < 0.$$

По этим неравенствам получаются следующих два возможных промежутка для искомого корня

$$(72^\circ, 90^\circ), \qquad (144^\circ, 180^\circ).$$

Но промежуток $(144^\circ, 180^\circ)$ откидывается, ибо в нем функция $\Omega(\varphi)$ изменяется от 0 до $\frac{5^5}{4^4} = 12,19$, тогда как по уравнению (5) должно быть

$$\Omega(\varphi) = 64.$$

Итак, искомый аргумента одного из двух мнимых сопряженных корней должен быть в промежутке $(72°, 90°)$. Рассмотрение производной показывает, что в этом промежутки функция $\Omega(x)$ возрастает.

Приходится рассматривать функций

$$5 \lg \sin \varphi - \lg \sin \varphi - 4 \lg \sin 4\varphi - \lg 64. \tag{1}$$

Когда я приготовлял для книги эти вычисения, то я пробовал сначала $\varphi = 80°$. Функция (1) оказалась числом отрицательным. Тогда я попробовал $\varphi = 85°$; число оказалось также отрицательное, но уже малое. Проба $\varphi = 86°$ привела к положительному числу; следовательно, корень заключается между 85° и 86°. Применение правил regula falsi дало около $85°20'$. Две дальнейшие пробы показали, что корень заключается между $85°21'$ и $85°22'$. Интерполируя по правилу regula falsi и производя еще пару проб, мы получаем окончательно два, рядом стоящиея в таблице, числа

$$85°21'20'', \qquad 85°21'30'',$$

которым соответствуют значения функции (1)

$$-0,0011532, \ +0,0000735.$$

Пропорциональное интерполирование дает окончательно

$$\varphi = 85°21'29'',37.$$

По уравнению (2) § 17 получим значение модуля мнимого корня

$$r = 1,443181.$$

Откуда искомых два мнимых корня будут

$$0,116792\ldots \pm i \cdot 1,438448\ldots$$

§ 19

Метода Gauss'a подверглась обобщению на случай четырехчленных уравнений в работе A. Wiener'a[68]

Способ Graeffe

§ 20

Способ Graeffe основан на довольно простой мысли, которая восходит еще к Dan. Bernoulli[69].

Пусть $x_1, x_2, \ldots, x_n$ корни уравнения $f(x) = 0$.

Полагая по обыкновенно $s_k = x_1^k + x_2^k + \ldots + x_n^k$, будем иметь

$$\frac{s_k}{s_{k-1}} = x_1 \frac{1 + \left(\frac{x_2}{x_1}\right)^k + \ldots + \left(\frac{x_n}{x_1}\right)^k}{1 + \left(\frac{x_2}{x_1}\right)^{k-1} + \ldots + \left(\frac{x_n}{x_1}\right)^{k-1}}.$$

[68]Zeitschrift f. Math. Phys. 31 (1886), s. 65, 192.

[69]D. Bernoulli. Comm. Petrop. 3. 1728. p. 92.

Если корень x_1, имеет наибольший модуль, то при беспредельном возрастании k мы будем иметь

$$\lim \frac{s_k}{s_{k-1}} = x_1.$$

Таким образом наибольший по модулю корень может быть найден как предел $\frac{s_k}{s_{k-1}}$.

Euler в своем знаменитом сочинопш «Introductio in analysin infinitorum». (T. I, Кар. 17) стремился придать идеям Bernoulli практическое значение и развил способ вычислять корни численных уравнений при помощи возвратных рядов. Идеи Euler'а были развиты позднейшими авторами[70].

Идея возвышения корней в бесконечно большие степени привела к действительно удобному на практике способу решения уравнений лишь после исследование Graeffe, развитых позднейшими авторами[71].

[70] *Fourier.* Anal, des équ. det. Ostwalds Klass. № 127. *Stern.* Journ. f. r. u. ang. Math. 11 (1834). *Jacobi* ibidem. 13 (1835). *Cohn.* Math. Ann. 44 (1894).

[71] *Graeffe.* Die Aufl. d. höh. num. Gleich. 1837. *Encke.* Journ. f. r. u. ang. Math 22 (1841). *Carvallo.* Ann. d. la fac. de Toulouse 1882). *А. Крылов.* Лекции о приб. вычисл. С.-Петербург 1911.

Глава XIII

Двучленные уравнения

Двучленные уравнения

§ 1

Будем рассматривать уравнения вида

$$x^n - 1 = 0, \tag{1}$$

где n натуральное число. Из элементов известно, что корни этого уравнения имеют вид

$$r_k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n} = e^{\frac{2k\pi}{n}i}. \tag{2}$$

Давая значку k значения

$$0,\ \ 1,\ \ 2,\ \ldots,\ n-1,$$

получим все n корней уравнения (1)

$$r_0 = 1,\ \ r_1,\ \ r_2,\ \ldots,\ r_{n-1}. \tag{3}$$

Из формулы (2) вытекает, что

$$r_k = \left\{e^{\frac{2\pi i}{n}}\right\}^k = r_1^k;$$

таким образом, мы видим. что все корни (3) получаются, как степени одного корня r_1, и, следовательно, ряду чисел (3) можно дать вид

$$r_1^0,\ \ r_1^1,\ \ r_1^2,\ \ldots,\ r_1^{n-1}. \tag{4}$$

§ 2

Только что мы видели, что, если возвышать корень r_1 в последовательные степени $1, 2, 3, \ldots, n-1$, то будут получаться отличные от единицы различные корни двучленного уравнения, и n-ая степень будет наименьшая из степеней, удовлетворяющая равенству

$$r_1^n - 1 = 0.$$

Будем корни (3) § 1 называть *корнями степени n из единицы*; назовем *первообразным* корни степени n из единицы, такой корень, что наименьшая его степень, обращающаяся в единицу, будет n.

Мы видели уже, что но крайней мере один такой корень существует, потому что корень r_1 как раз обладает этим свойством и есть, следовательно, первообразный.

§ 3

Поставим себе вопрос, существуют-ли кроме корня r_1 еще первообразные корни[72]. Нетрудно убедиться, что первообразным будет всякий корень

$$r_k,$$

где число k взаимно простое с n. В самом деле, рассмотрим какую-нибудь целую степень x этого корня

$$r_k^x = \left\{ e^{\frac{2k\pi}{n} i} \right\}^x = e^{\frac{2kx\pi}{n} i}$$

и будем искать наименьшее целое число, при котором имеет место равенство

$$r_k^x = 1. \tag{1}$$

Для того, чтобы это равенство имело место, надо положить

$$kx = nl, \tag{2}$$

где l целое число, ибо тогда

$$e^{\frac{2kx\pi}{n} i} = e^{2l\pi i} = 1.$$

Таким образом, мы видим, что произведение kx делится на n, но k число взаимно простое с n, следовательно, x должно делиться на n, и мы получаем

$$x = n\xi,$$

где ξ число целое. Так как наименьшее значение целого числа есть 1, то получаем наименьшее значение x, удовлетворяющего (1), равным n, и, следовательно, корень r_k при k взаимно простом с n есть первообразный.

Покажем дальние, что, если k будет иметь общего наибольшего с n делителя d, отличного от 1, то корень r_k, не будет первообразный. В самом деле, в этом случае можно положить

$$k = dk_1, \qquad n = dn + 1,$$

где k_1 и n_1 целые взаимно простые числа, и кроме того

$$r_k = e^{\frac{2k\pi}{n} i} = e^{\frac{2k_1\pi}{n_1} i},$$

[72] Я предлагаю читателю сравнить рассуждения этой главы с изложением в моей книге «Элементарный курс теории чисел» (вт. изд. 1913).

следовательно, получаем

$$r_k^{n_1} = e^{2k_1\pi i} = 1;$$

таким образом, мы видим, что в этом случае существует такой показатель n_1, при возвышении в степень которого получается 1, но этот показатель меньше n; значит, в этом случае корень r_k непервообразный.

Получается следующая теорема:

Существует столько первообразных корней степени n из единицы, сколько существует чисел меньших n и взаимно простых с n.

Будем обозначать во всем дальнейшем число первообразных корней символом

$$\varphi(n)$$

$\varphi(n)$ есть некоторая числовая функция, имеющая смысл, только при целых значениях аргумента n и принимающая только целые значения. Так как существует только один первообразный корень из единицы первой степени, а именно сама единица, то считают

$$\varphi(1) = 1.$$

Функция $\varphi(n)$, на основании только что приведенной теоремы, имеет еще другое значение: она представляет число чисел, меньших n и взаимно простых с ним.

Это даст возможность вычислять значения функции $\varphi(n)$ для различных численных значений n; так, например, $\varphi(6) = 2$, ибо существуют только два числа 1 и 5 взаимно простыл с числом 6.

Если число n простое, то оно взаимно простое со всеми числами меньшими его, а таких чисел будет $n-1$, поэтому при n простом

$$\varphi(n) = n - 1.$$

§ 4

Покажем теперь, что для всякого первообразного корня r_k имеет место то же самое свойство, которое мы видели для первообразного корня r_1, а именно n *степеней*

$$r_k^0, \quad r_k^1, \quad r_k^2, \ \ldots, \ r_k^{n-1} \tag{1}$$

будут все корни (3) § 1 из единицы.

В самом деле, будем рассматривать произведения

$$k \cdot 0, \quad k \cdot 1, \quad k \cdot 2, \ \ldots, \ k \cdot l, \ \ldots \ k \cdot (n-1); \tag{2}$$

будем делить произведения (2) на число n и составлять остатки от этого деления: пусть эти остатки будут

$$\rho_0, \quad \rho_1, \quad \rho_2, \ \cdots, \ \rho_{n-1}, \tag{3}$$

так что ρ_l обозначает остаток от деления на n числа kl; очевидно, что

$$\rho_0, \quad \rho_1 = k,$$

так как k меньше n. Заметив, что

$$kl = nm + \rho_l,$$

где m целое число, получим, очевидно,

$$r_k^l = e^{\frac{2kl\pi}{n}i} = e^{\frac{(2(nm+\rho_l)\pi}{n}i} = e^{2m\pi i} \cdot e^{\frac{2\rho_l\pi}{n}i} = e^{\frac{2\rho_l\pi}{n}i} = r_{\rho_l}.$$

Отсюда мы видим, что числа ряда (1) будут представлять собою ряд чисел

$$r_{\rho_0},\ \ r_{\rho_1},\ \ r_{\rho_2},\ \ldots,\ r_{\rho_{n-1}}. \tag{4}$$

Мы желаем доказать, что ряд (4) дает все корни степени n из единицы. Для этой цели достаточно убедиться, что среди остатков (3) не будет одинаковых; итак покажем, что невозможно равенство

$$\rho_i = \rho_j;$$

предположим. что это равенство имело бы место, тогда два числа

$$ki \quad \text{и} \quad kj$$

при делении на n давали бы одинаковые остатки, а, значит, их разность

$$k(i-j)$$

давала бы в остатке нуль, но число k взаимно простое с n, следовательно, должно делиться на n число $i-j$, что невозможно.

Итак, все остатки

$$r_{\rho_0},\ \ r_{\rho_1},\ \ r_{\rho_2},\ \ldots,\ r_{\rho_{n-1}}$$

различны между собою. Значить, доказана теорема:

Всякий первообразный корень степени n из единицы обладает свойством давать все корни степени n из единицы при возвышении в степени $0, 1, 2, \ldots, n-1$.

§ 5

Рассмотрим теперь какой нибудь непервообразный корень r_k степени n из единицы. Предположим опять, что число k имеет общий наибольший делитель d с n, так что

$$k = d \cdot k_1, \qquad n = d \cdot n_1;$$

мы видели уже, что наименьшая степень корня r_k, дающая единицу, уже меньше n и равна n_1; будем говорить, что наш корень *принадлежит к показателю n_1.*

Получаем теорему:

Всякий непервообразный корень степени n из единицы принадлежит к некоторому показателю n_1, который есть делитель числа n.

Посмотрим теперь, сколько существует корней степени n, принадлежащих к определенному показателю n_1.

Так как

$$r_k = e^{\frac{2k_1\pi}{n_1}i},$$

где k_1 число взаимно простое с n_1 и меньшее этого числа, ибо $k < n$, то мы заключаем, что всякий корень степени n, принадлежащий показателю n_1, есть первообразный корень из единицы степени n_1, и, значит, число корней степени n, принадлежащих показателю n_1, будет $\varphi(n_1)$.

§ 6

Рассмотрим всевозможные делители числа n и рассмотрим сумму

$$\sum \varphi(n_i),$$

распространенную на всех делителей числа n.

Нетрудно убедиться, что *эта сумма есть* n.

В этом убеждаемся простым счетом корней; всякий корень принадлежит непременно к какому-нибудь показателю n_1, следовательно, при счете он дает единицу в состав соответственной функций $\varphi(n_1)$. Значить, перебрав все корни, мы с одной стороны получим число n, а с другой сумму всех функций $\varphi(n_i)$. Получаем, следовательно, равенство

$$n = \sum \varphi(n_i).$$

Например, если $n = 12$, то делители будут

$$1, \quad 2, \quad 3, \quad 4, \quad 6, \quad 12,$$

и, значить,

$$12 = \varphi(1) + \varphi(2) + \varphi(3) + \varphi(4) + \varphi(6) + \varphi(12),$$

что легко проверить, ибо

$$\varphi(1) = 1, \quad \varphi(2) = 1, \quad \varphi(3) = 2,$$
$$\varphi(4) = 2, \quad \varphi(6) = 2, \quad \varphi(12) = 4.$$

§ 7

Возьмем какой-нибудь первообразный корень r_k, и пусть число n раскладывается на два взаимно простые множителя a и b, так что

$$n = a \cdot b. \tag{1}$$

Из элементов известно, что можно подобрать бесчисленное множество пар чисел x и y, удовлетворяющих уравнению

$$ax + by = 1. \tag{2}$$

При этом очевидно, что число x взаимно простое с b, ибо, если бы эти два числа имели делителя δ, то на этого делителя должна бы делиться единица, что невозможно; точно также y взаимно простое с a. Получаем

$$r_k = e^{\frac{2k\pi}{n}i} = e^{\frac{2k(ax+by)\pi}{n}i} = e^{\frac{2kx\pi}{n}i} = \cdot e^{\frac{2ky\pi}{n}i} = r' \cdot r'',$$

где

$$r' = e^{\frac{2kx\pi}{n}i}, \qquad r'' = e^{\frac{2ky\pi}{n}i}.$$

Итак, мы представили первообразный корень степени n в виде произведения двух корней r' и r'', из которых первый степени b, а второй степени a, причем оба эти корня первообразные, потому что число k взаимно простое с обоими множителями a и b, и, следовательно, kx взаимно простое с b, а ky взаимно простое с a.

Отсюда получаем следующее правило составления всех первообразных корней степени ab, если известны все первообразные корни степени a и степени b, в случае a и b взаимно простых между собою:

Перемножим каждый из корней степени a на каждый из корней степени b и получим все первообразные корни степени ab, и выходит, что

$$\varphi(ab) = \varphi(a) \cdot \varphi(b). \tag{3}$$

Равенство (3) дает возможность получить общую формулу для вычисления функции $\varphi(n)$ для любого целого значения n.

§ 8

В самом деле, равенство (3) можно написать для какого угодно числа множителей. Так, если задан ряд каких угодно взаимно простых чисел

$$a, \quad b, \quad c, \quad \ldots,$$

то получим

$$\varphi(a \cdot b \cdot c \cdots) = \varphi(a) \cdot \varphi(b) \cdot \varphi(c) \cdots$$

Напишем разложение заданного числа n на простые множители

$$n = p_1^{\lambda_1} \cdot p_2^{\lambda_2} \cdot p_2^{\lambda_3} \cdots,$$

где $p_1, p_2, p_3, \ldots$ простые числа, входящие в состав n, а $\lambda_1, \lambda_2, \lambda_3, \ldots$ некоторые целые числа, тогда получаем

$$\varphi(n) = \varphi(p_1^{\lambda_1}) \cdot \varphi(p_2^{\lambda_2}) \cdot \varphi(p_3^{\lambda_3}) \cdots$$

Остается, следовательно, показать, как вычислять функцию

$$\varphi(p^{\lambda}),$$

где p простое число.

Рассмотрим p^λ последовательных натуральных чисел

$$1,\ \ 2,\ \ 3,\ \ldots,\ p^\lambda - 1,\ \ p^\lambda;$$

из этих чисел взаимно простыми с p будут те числа, которые не делятся на простое число p. Значить, чтобы сосчитать число этих чисел, надо выкинуть из нашего ряда все числа, делящиеся на p, т. е. следующие

$$p,\ \ 2p,\ \ 3p,\ \ldots,\ (p^{\lambda-1}p,\ \ p^{\lambda-1}p;$$

таким образом, надо выкинуть $p^{\lambda-1}$ чисел не взаимно простых с p, и мы получаем, что число взаимно простых чисел, меньших p^λ будет

$$\varphi(p^\lambda) = p^\lambda - p^{\lambda-1} = p^\lambda\left(1 - \frac{1}{p}\right),$$

откуда получаем

$$\varphi(n)p^{\lambda_1}\left(1 - \frac{1}{p_1}\right)p_2^{\lambda_2})\left(1 - \frac{1}{p_2}\right)\cdots,$$

или окончательно

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots$$

Это выражение для функций φ показывает, что для вычисления этой функции не надо знать показателей λ_i, а надо знать лишь все различные простые числа, входящая в состав числа n.

§ 9

Пусть

$$k_1,\ \ k_2,\ \ k_3,\ \ldots,\ k_{\varphi(n)} \tag{1}$$

будут все числа взаимно простые с n и меньшие n.

Возьмем какое-нибудь из этих чисел, например, k, тогда ряд чисел

$$kk_1,\ \ kk_2,\ \ldots,\ kk_{\varphi(n)} \tag{2}$$

при делении этих чисел на n даст ряд остатков

$$l_1,\ \ l_2,\ \ldots,\ l_{\varphi(n)}. \tag{3}$$

Нетрудно показать, что ряд (3) состоит из тех же чисел, что и ряд (1), только расположенных в другом порядке.

В самом деле, очевидно, что все числа ряда (3) взаимно простые с n, ибо эти числа происходят от деления чисел (2) взаимно простых с n на n, а при таком делении, если бы остаток имел общий делитель с n, то такого общего делителя имело бы делимое. Итак, числа (3) суть числа меньшие n и взаимно простые с n. Остается показать, что эти числа различны между собою.

В самом деле, предположим, что

$$l_i = l_j,$$

тогда разность двух чисел

$$kk_i \quad \text{и} \quad kk_j$$

должна бы делиться на n, а это невозможно, потому что эта разность имеет вид

$$k(k_i - k_j)$$

и есть произведение числа k взаимно простого с n и разности двух чисел меньших n. Итак, ряд остатков (3) совпадает с рядом (1). Отсюда получаются две следуюшие весьма важные теоремы.

Теорема I. *Если мы возведем все первообразные корни*

$$r_{k_1}, \quad r_{k_2}, \ldots, \; r_{k_{\varphi(n)}}$$

степени n из единицы в степень, показатель которой k есть число взаимно простое с n, то получим те же самые первообразные корни, только расположенные в другом порядке.

В самом деле, эти корни будут

$$r_{l_1}, \quad r_{l_2}, \ldots, \; r_{l_{\varphi(n)}}.$$

Теорема II. *Если мы возвысим какой нибудь первообразный корень r_k степени n из единицы в степени, показатели которые, будут числа*

$$k_1, \quad k_2, \ldots, \; k_{\varphi(n)},$$

взаимно простыл с n и меньшие n, то мы получим все первообразные корни, степени n из единицы.

§ 10

Пусть

$$f(\alpha, \beta, \gamma, \ldots) \tag{1}$$

будет произвольно взятая целая функция от какого-нибудь числа корней степени n из единицы с целыми коэффициентами.

Составим ряд функций

$$f_1, \quad f_2, \quad f_3, \; \ldots, f_{n-1}, \quad f_n,$$

который получаются из функций (1) заменою корней $\alpha, \beta, \gamma, \ldots$ последовательными их степенями, так, что

$$\begin{aligned} f_1 &= f(\alpha, \; \beta, \; \gamma, \; \ldots), \\ f_2 &= f(\alpha^2, \beta^2, \gamma^2, \ldots), \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ f_n &= f(\alpha^n, \beta^n, \gamma^n, \ldots). \end{aligned}$$

Можно показать, что сумма

$$f_1 + f_2 + \ldots + f_n$$

будет всегда целое число, делящееся на n. Покажем это.

Возьмем какой-нибудь первообразный корень r из единицы, тогда все корни $\alpha, \beta, \gamma, \ldots$, какое бы их число ни было, будут степенями этого первообразного корня. Подставляя эти степени корня r вместо $\alpha, \beta, \gamma, \ldots$, в функцию f_1, и, уничтожая все степени r выше $n-1$ на основании равенства

$$r^n = 1$$

представим нашу функцию в таком виде

$$f_1 = A + A_1 r + A_2 r^2 + \ldots + A_{n-1} r^{n-1}, \tag{2}$$

где все коэффициенты

$$A, \quad A_1, \quad A_3, \ \ldots, \ A_{n-1}$$

числа целые. Заменим корни $\alpha, \beta, \gamma, \ldots$ какими-нибудь их степенями

$$\alpha^k, \quad \beta^k, \quad \gamma^k, \ \ldots;$$

это все равно, что заменить первообразный корень r его степенью r^k, и тогда мы получим еще $n-1$ равенств

$$\begin{gathered} f_2 = A + A_1 r^2 + A_2 (r^2)^2 + \ldots + A_{n-1} (r^2)^{n-1}, \\ f_3 = A + A_1 r^3 + A_2 (r^3)^2 + \ldots + A_{n-1} (r^3)^{n-1}, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ f_n = A + A_1 r^n + A_2 (r^n)^2 + \ldots + A_{n-1} (r^n)^{n-1}. \end{gathered}$$

Складывая эти равенства с равенством (2), получим следующее равенство

$$f_1 + f_2 + \ldots + f_n = n \cdot A, \tag{3}$$

потому что числа

$$r, \quad r^2, \quad r^3, \ \ldots, \ r^n$$

суть все корни $\alpha, \beta, \gamma, \ldots$ из единицы, а суммы различных степеней всех этих корней до $(n-1)$-ой на основании стр. 239 равны нулю. Теорема таким образом доказана, ибо A целое число.

§ 11

Перейдем теперь к рассмотрению многочленов, корни которых суть только первообразные корни какой-нибудь степени n из единицы.

Для получения такой функции, нужно из функций

$$f(x) = x^n - 1$$

удалить все непервообразные корни. Мы видели, что всякий непервообразный корень есть непременно корень другого уравнения

$$x^{n_i} - 1 = 0,$$

где n_1 есть делитель числа n. Значит, в функции $f(x)$ останутся только одни первообразные корни, если мы удалим из нее все общие множители, которые эта функция может иметь с функциями низших степеней

$$x^{n_1} - 1, \quad x^{n_2} - 1, \ \ldots,$$

где $n_1, n_2, \ldots$ суть все делители числа n.

Так как нахождение общего делителя двух функций совершается при помощи последовательного деления, то, очевидно, что коэффициенты всех целых функций, которые будут входить при сказанном процессе удаления общих множителей будут рациональны.

Будем во всем дальнейшем обозначать через

$$X_n$$

такой многочлен, который имеет только первообразные корни степени n из единицы. Очевидно, что этот многочлен будет степени $\varphi(n)$, и мы получим

$$X_n = x^{\varphi(n)} + ax^{\varphi(n)-1} + bx^{\varphi(n)-2} + \ldots,$$

где $a, b, c, \ldots$ рациональные коэффициенты.

§ 12

Покажем на примерах первых 12-ти чисел, как находить функцию X_n.

1°. $n = 1$, $\varphi(1) = 1$;
так как можно считать, что существует только один первообразный корень первой степени из единицы, а именно сама единица, то

$$X_1 = x - 1.$$

2°. $n = 2$, $\varphi(2) = 1$;
в этом случае из функции $x^2 - 1$ надо удалить корень первой степени, т. е. разделить эту функций на $x - 1$, и мы получим

$$X_2 = x + 1.$$

3°. $n = 3$, $\varphi(3) = 2$;
так как 3 число простое, то все корни функции $x^3 - 1$ кроме 1 суть первообразные, и, значит, разделяя на $x - 1$, получим

$$X_3 = x^2 + x + 1.$$

4°. $n = 4$, $\varphi(4) = 4 \cdot \dfrac{1}{2} = 2$;
в этом случай из функции $x^4 - 1$ надо удалить корни второй степени, т. е разделить эту функцию на $x^2 - 1$, и мы получим

$$X_4 = x^2 + 1.$$

5°. $n = 5$, $\varphi(5) = 4$;

получаем

$$X_4(x) = x^4 + x^3 + x^2 + x + 1.$$

6°. $n = 6$, $\varphi(6) = 6 \cdot \frac{1}{2} \cdot \frac{2}{3} = 2$;
из функции $x^6 - 1$ надо удалить все корни третьей степени, значит, надо разделить ее на $x^3 - 1$ и получим $x^3 + 1$; но еще надо разделить на $x + 1$ и мы получим

$$X^6 = x^2 - x + 1.$$

7°. $n = 7$, $\varphi(7) = 6$;
получаем

$$X_7 = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1.$$

8°. $n = 8$, $\varphi(8) = 8 \cdot \frac{1}{2} = 4$;
удаляя из функции $x^8 - 1$ все корни 4-ой степени, т. е. разделяя на $x^4 - 1$, получим

$$X_8 = x^4 + 1.$$

9°. $n = 9$, $\varphi(9) = 9 \cdot \frac{2}{3} = 6$;
разделяя $x^9 - 1$ на функцию $x^3 - 1$, получим

$$X_9 = x^6 + x^3 + 1.$$

10°. $n = 10$, $\varphi(10) = 10 \cdot \frac{1}{2} \cdot \frac{4}{5} = 4$;
разделяя $x^{10} - 1$ на $x^5 - 1$, получим $x^5 + 1$, а разделяя еще на $x + 1$, получим

$$X_{10} = x^4 - x^3 + x^2 - x + 1.$$

11°. $n = 11$, $\varphi(11) = 10$;
получим

$$X_{11} = x^{10} + x^9 + x^8 + \ldots + x^3 + x^2 + x + 1.$$

12°. $n = 12$, $\varphi(12) = 12 \cdot \frac{1}{2} \cdot \frac{2}{3} = 4$;
разделяя $x^{12} - 1$ на $x^6 - 1$, получим $x^6 + 1$, а раздедяя еще на $x^2 + 1$, получим

$$X_{12} x^4 - x^2 + 1.$$

§ 13

На предыдущих примерах мы видели, что коэффициенты функций X_n оказываются не только рациональными, но и целыми: это свойство, как нетрудно показать, принадлежит функции X_n при всяком значении n.

В этом очень просто убедиться, если принять в соображение следующие леммы относительно целых функций, указанные Gauss'ом и имеющим большое применение в разных частях Алгебры.

§ 14

Будем рассматривать полиномы с целыми коэффициентами

$$a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n.$$

Если обший наибольший делитель всех коэффициентов этой функции есть 1, то будем называть эту функцию *первоначальною*. Нетрудно показать справедливость следующей теоремы:

Если две целые функции

$$a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n,$$
$$b_0x^m + b_1x^{m-1} + \ldots + b_{m-1}x + b_m$$

первоначальны, то их произведение

$$c_0x^{m+n} + c_1x^{m+n-1} + \ldots + c_{m+n}$$

будет первоначально.

Допустим обратное: допустим, что произведение непервоначально; тогда все коэффициенты $c_0, c_1, \ldots, c_{m+n}$ имеют некоторый делитель $\delta > 1$. Этот делитель должен заключать в себе по крайней мере простой множитель p; допустим, следовательно, что все коэффициенты $c_0, c_1, \ldots, c_{m+n}$ делятся на некоторое простое число p, отличное от единицы. Невозможность этого допущения обнаруживается сразу. В самом деле, пусть первый по счету слева коэффициент, не делящийся на p в первом множителе будет a_r, а во втором b_s, тогда получаем

$$c_{r+s} = a_rb_s + a_{r+1}b_{s-1} + a_{r+2}b_{s-2} + \ldots + aa_{r-1}b_{s+1} + a_{r-2}b_{s+2} + \ldots,$$

а так как все коэффициенты

$$b_{s-1},\quad b_{s-2},\ \ldots,\ a_{r-1},\quad a_{r-2},\ \ldots$$

делятся на p, то во второй части последнего равенства все члены кроме первого a_rb_s, делятся на p. Итак, оказывается, что c_{r+s} не может делиться на p.

§ 15

Из теоремы предыдущего §-а можно вывести, как следствие следующую новую теорему:

Если две целые функции

$$\varphi(x) = x^n + \alpha_1x^{n-1} + \alpha_2x^{n-2} + \ldots$$
$$\psi(x) = x^m + \beta_1x^{m-1} + \beta_2x^{m-2} + \ldots$$

с рациональными коэффициентами дают в произведении функцию

$$x^{m+n} + \gamma_1x^{m+n-1} + \gamma_2x^{m+n-2} + \ldots,$$

у которой коэффициенты $\gamma_1, \gamma_2, \ldots$ целые числа, то целыми должны быть также коэффициенты $\alpha_1, \alpha_2, \ldots$ и $\beta_1, \beta_2, \ldots$ функций φ и ψ.

Допустим обратное, а именно, что коэффициенты у функций $\varphi(x)$ и $\psi(x)$ дробные. Обозначим через α_0 наименьший общий знаменатель всех коэффициентов

$\alpha_1, \alpha_2, \ldots$, а через β_0 наименьшей общий знаменатель коэффициентов $\beta_0, \beta_1, \ldots$. Тогда две функций $\alpha_0\varphi(x)$ и $\beta_0\psi(x)$ будут с целыми коэффициентами. Очевидно, что эти функции будут первоначальными, потому что, если бы после умножения на α_0 функции $\varphi(x)$ оказался у всех коэффициентов этой функций какой-нибудь общий множитель, то в этом случае число α_0 не могло бы быть общим наименьшим знаменателем. Итак, обе функции

$$\alpha_0\varphi(x), \qquad \beta_0\psi(x)$$

первоначальны, а, значить, первоначальной функцией должно было бы быть их произведение

$$\alpha_0\beta_0(x^{n+m} + \gamma_1 x^{n+m-1} + \ldots);$$

но так как все коэффициенты $\gamma_1, \gamma_2, \ldots$ числа целые, то для того, чтобы последняя функция была первоначальною, необходимо, чтобы равнялся единице общий множитель $\alpha_0\beta_0$ всех коэффициентов; итак, выходит

$$\alpha_0\beta_0 = 1,$$

откуда

$$\alpha_0 = 1, \qquad \beta_0 = 1;$$

следовательно, все α_i и β_i числа целые, что и требовалось доказать.

§ 16

Обращаемся теперь к более близкому рассмотрению функций X_n.

Возьмем функцию

$$x^n - 1.$$

Так как каждый из корней этой функций принадлежит всегда к некоторому показателю n_1, который есть делитель числа n, то нетрудно убедиться в существование тождества

$$x^n - 1 = \prod X_{n_1}, \tag{1}$$

где произведение распространяется на все делители числа n. В справедливости формулы (1) убеждаемся следующим образом:

Так как во второй части мы рассматриваем все делители n_1 числа n, то для каждого делителя n_1 мы можем взять только первообразные корни степени n_1.

Сравнивая высшие степени в левой и правой частях, мы получаем соотношение

$$n = \sum \varphi(n_1).$$

Из формулы (1) мы получаем следующее важное заключение: так как произведение функций X_n есть целая функция с целыми коэффициентами, а мы знаем, что коэффициенты функций X_n рациональны, то мы приходим к заключений, что коэффициенты функции X_n должны быть числами целыми.

Если мы применим формулу (1) к случаю $n = 12$, то получим делители

$$1, \quad 2, \quad 3, \quad 4, \quad 5, \quad 6,$$

следовательно,

$$x^{12}-1=(x-1)(x+1)(x^2+x+1)(x^2+1)(x^2-x+1)(x^4-x^2+1).$$

Неприводимость функции X_n при n простом

§ 17

Целые функций X_n обладают свойством неприводимости в области рациональных чисел. Далее мы докажем это свойство в общем случае, а теперь пока можно ограничиться доказательством его лишь для n простого. Мы приведем доказательство Gauss'a (Disqilisitiones arithmeticae).

§ 18

Докажем, что функция

$$X_n=\frac{x^n-1}{x-1}=x^{n-1}+x^{n-2}+\ldots+x^2+x+1$$

неприводима, причем будем предполагать n простым.

Предположим обратное. Предположим, что функция X_n имеет множитель $\varphi_1(x)$ с рациональными, а, значит, целыми коэффициентами. Пусть степень этого множителя будет

$$m<n-1.$$

Разлагая функцию $\varphi_1(x)$ на линейные множители, получим

$$\varphi_1(x)=(x-r)(x-s)(x-t)\cdots=x^m+a_1x^{m-1}+\ldots+a_m,$$

где $r,s,t,\ldots$ суть некоторые из m корней функций φ_1, а коэффициенты

$$a_1,\quad a_2,\ \ldots,\ a_m$$

суть целые числа. Составим теперь ряд функций

$$\varphi_2,\quad \varphi_3,\ \cdots,\ \varphi_{n-1},$$

корни которых будут квадраты, кубы, ..., $n-1$-ые степени корней функций $\varphi_1(x)$, т. е.

$$\begin{gathered}\varphi_2=(x-r^2)(x-s^2)(x-t^2)\cdots,\\ \varphi_3=(x-r^3)(x-s^3)(x-t^3)\cdots,\\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots,\\ \varphi_{n-1}=(x-r^{n-1})(x-s^{n-1})(x-t^{n-1})\cdots\end{gathered}$$

Нетрудно видеть, что все коэффициенты функций

$$\varphi_2,\quad \varphi_3,\ \cdots,\ \varphi_{n-1}$$

суть числа целые; в самом деле, эти коэффициенты суть целые симметрические функции от корней $r,s,t,\ldots$ с целыми коэффициентами, значит, выражаются целыми рациональными функциями от $a_1,a_2,\ldots,a_m$ с целыми коэффициентами.

Подставляя во все эти выражения 1 вместо ?, мы получим целые числа, которые обозначим буквами

$$\varphi_1(1) = p_1, \quad \varphi_2(1) = p_2, \ \ldots, \ \varphi_{n-1}(1) = p_{n-1}.$$

Нетрудно, видеть, что все эти числа положительны. В самом деле, корни каждой из функций $\varphi_i(x)$ мнимые, а, следовательно, функция φ_i сохраняет свой знак при всевозможных вещественных значениях x; но, так как старший коэффициент этой функций есть $+1$, то для достаточно больших вещественных значений x функция φ_i имеет знак $+$, значит, она положительна и для всех остальных вещественных значений, и, следовательно, все числа

$$p_1, \quad p_2, \ \ldots, \ p_{n-1}$$

числа целые и положительные.

Из выражения

$$\varphi_1(1) = (1-r)(1-s)(1-t)\cdots$$

мы видим, что $\varphi_1(1)$ есть целая рациональная функция с целыми коэффициентами от m величин $r, s, t, \ldots$. Обозначим эту функцию через $\omega(r, s, t, \ldots)$, тогда мы имеем равенства

$$\begin{gathered} \varphi_1(1) = \omega(r, s, t, \ldots) = p_1, \\ \varphi_2(1) = \omega(r^2, s^2, t^2, \ldots) = p_2, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ \varphi_{n-1}(1) = \omega(r^{n-1}, s^{n-1}, t^{n-1}, \ldots) = p_{n-1}, \end{gathered} \tag{1}$$

и, наконец,

$$\omega(r^n, s^n, t^n, \ldots) = p_n = 0. \tag{2}$$

Перемножив равенства (1), получим

$$\begin{gathered} \{(1-r)(1-r^2)\cdots(1-r^{n-1})\}\ \{(1-t)(1-t^2)\cdots(1-t^{n-1})\} \\ \{(1-t)(1-t^2)\cdots(1-t^{n-1})\cdots = p_1 p_2 \cdots p_{n-1}; \end{gathered}$$

каждый из множителей в фигурных скобках представляет из себя не что иное, как результат подстановки единицы в функцию X_{n-1} и мы получаем

$$\{X_n(1)\}^m = p_1 \cdot p_2 \cdots p_{n-1}. \tag{3}$$

Так как число n простое, то получаем

$$n^m = p_1 \cdot p_2 \cdots p_{n-1};$$

таким образом каждое из целых чисел p_i может быть только или самым числом n, или единицею, причем наверно будет несколько чисел p_i равных единице, ибо в правой части (3) множителей больше чем m и притом число равных единиц чисел не меньше $n-1-m$; а если мы предположим что которые-нибудь из чисел p_i суть более высокие степени числа n, то число равных единице чисел p_i должно быть

еще больше. Итак, наверно существует ρ чисел p_i равных единице; причем число ρ удовлетворят неравенствам

$$n-1-m \leq \rho \leq n-2.$$

Остальные коэффициенты p_i должны делиться на n, и мы получаем следующую формулу

$$p_1 + p_2 + \ldots p_{n-1} = \rho + nA,$$

где A целое число. Но на основании теоремы § 10 сумма

$$p_1 + p_2 + \ldots + p_{n-1} + p_n$$

должна быть целым числом, делящимся на n, следовательно, мы получаем

$$nB = \rho + nA.$$

Мы приходим к противоречие, что целое число ρ, меньшее n, должно делиться на n, что невозможно, ибо ρ не нуль. Стало быть, предположение, что функция X_n имеет множитель $\varphi_1(x)$, ошибочно; значит, функция X_n при n простом неприводима.

Вычисление функций X_n при n составном

§ 19

Обращаемся теперь к рассмотрению случая, когда n есть степень некоторого простого числа p, т. е. пусть

$$n = p^\lambda.$$

Можно написать

$$n = p \cdot p_1,$$

где $p_1 = p^{\lambda-1}$. Нетрудно видеть, что мы получим все первообразные корни степени n, если из всех корней степени n выкинем все корни степени p_1; отсюда получаем

$$X_n = \frac{x^{pp_1}-1}{x^{p_1}-1} = x^{p_1(p-1)} + \ldots + x^{2p_1} + x^{p_1} + 1. \tag{1}$$

Если $p_1 > 1$, то между первым и вторым членами функции (1) заключается пропуск по крайней мере одного члена. Отсюда получается такое свойство:

Сумма всех первообразных корней степени n, где n есть степень простого числа выше первой, равняется нулю.

Обращаясь к общему случаю, употребим способ рассуждения, который прилагался при выводе функции $\varphi(n)$; предположим, что мы умеем вычислить функции X_n, если в нее входить некоторое число $m-1$ различных простых множителей, и покажем, как вычислить эту функцию, если число различных простых множителей будет на единицу больше, т. е. будет m.

Итак, пусть вычислена функция X_n при некотором значении n.

Пусть p простое число, не входящее в состав числа n; рассмотрим, как вычислить функцию $X_{n'}$, где

$$n' = np^\lambda.$$

Пусть x будет корень функции $X_n(x)$; тогда мы замечаем, что получим корни $X_{n'}(x)$, если умножим все корни r на первообразные корни степени p^λ (см. § 7). Значить, если мы обозначим

$$p^\lambda = p \cdot p_1,$$

то мы получим все первообразные корни степени p^λ, если отбросим из всех корней α степени p^λ все корни β степени p_1; значит, мы получим все корни $X_n(x)$, если из всех корней $r\alpha$ отбросим все корни $r\beta$. Нетрудно видеть, что $r\alpha$ будут корнями функции

$$X_n(x^{p^\lambda});$$

в самом деле,

$$(r\alpha)^{p^\lambda} = r^{p^\lambda} \cdot \alpha^{p^\lambda} = r^{p^\lambda},$$

но так как p^λ число взаимно простое с n, а возвышение первообразного корня r степени n в степень простую с n дает опять первообразный корень степени n, то r^{p^λ} будет также первообразным корнем степени n, и мы получаем

$$X_n(r^{p^\lambda}) = 0.$$

Это тождество можно переписать так

$$X_n\{(r\alpha)^{p^\lambda}\} = 0,$$

значит, действительно, $r\alpha$ есть корень уравнения

$$X_n(x^{p^\lambda}) = 0. \tag{2}$$

Так как различных значений первообразного корня r степени n есть $\varphi(n)$, а различных значений всех корней α степени p^λ есть p^λ, то, значит, различных $r\alpha$ будет

$$p^\lambda \varphi(n);$$

а так как этому же числу равна степень уравнения (2), то $r\alpha$ и будут все корни уравнения (2). Подобным же образом $r\beta$ будут все корни уравнения

$$X_n(x^{p^{\lambda-1}}) = 0. \tag{3}$$

Следовательно, разделяя первую часть уравнения (2) на первую часть уравнения (3), мы должны получить как раз функцию $X_{n'}$ и, значит, получаем тождество

$$X_{npp_1}(x) = \frac{X_n(x^{pp_1})}{X_n(x^{p_1})}. \tag{4}$$

§ 20

Формула (4) предыдущего параграфа дает возможность получать функцию X_n в самом общем случае.

Применимь ее к случаю двух простых множителей p и q, так что

$$n = q^\mu = q \cdot q_1,$$

где $q_1 = q^{\mu-1}$, а

$$n_1 = p^\lambda q^\mu = p^\lambda \cdot n = n \cdot p \cdot p_1,$$

где $p_1 = p^{\lambda-1}$.

Получаем

$$X_{n_1} = \frac{X_n(x^{pp_1})}{X_n(x^{p_1})}; \tag{1}$$

но на основании соображений предыдущего параграфа мы видим, что

$$X_n(x) = \frac{x^{qq_1}-1}{x^{q_1}-1},$$

значить, по формуле (1) будем иметь

$$X_{n_1} = \frac{x^{pp_1qq_1}-1}{x^{pp_1q_1}-1} : \frac{x^{qp_1q_1}-1}{x^{p_1q_1}-1} = \frac{(x^{pp_1qq_1}-1)(x^{p_1q_1}-1)}{(x^{pp_1q_1}-1)(x^{qp_1q_1}-1)},$$

или иначе

$$X_{n_1} = \frac{(x^{n_1}-1)(x^{\frac{n_1}{pq}}-1)}{(x^{\frac{n_1}{p}}-1)(x^{n_1}q-1)}. \tag{2}$$

Эта формула может быть обобщена. Обозначая через μ_1 всевозможные частные от деления заданного n на всевозможные произведения, состоящие из четного числа различных простых множителей, входящих в состав числа n, а через μ_2 всевозможные частные от деления числа n на нечетное число различных простых множителей, входящих в состав числа n, получим

$$X_n = \frac{\prod(x^{\mu_1}-1)}{\prod(x^{\mu_2}-1)} = \frac{(x^n-1)\prod(x^{\frac{n}{pq}}-1)\cdots}{\prod(x^{\frac{n}{p}}-1)\ \prod(x^{\frac{n}{pqr}}-1)\cdots}. \tag{3}$$

Доказательство будет состоять в том, что мы предположим формулу (3) справедливою для такого числа n, в которое входит $m-1$ различных простых множителей, и докажем справедливость этой формулы для числа

$$n' = n \cdot pp_1,$$

где p новое простое число, не входящее в состав числа n. В моей книге «Элементарный курс теории чисел» (втор. изд. 1913 г.) помещено более простое доказательство формулы (3) основанное на арифметических соображениях.

§ 21

Укажем еще несколько весьма важных свойств функций X_n.

Рассмотрим функций $X_n(x)$, где n число нечетное. Так как числа 2 и n взаимно простые, то мы получим все первообразные корни степени $2n$, если умножим все первообразные корни степени n на первообразные корни 2-ой степени; но так как существует только один первообразный корень второй степени, именно -1,

то, если через r обозначим все первообразные корни степени n, то $-r$ будут первообразными корнями степени $2n$, и получается тождество

$$X_{2n}(x) = X_n(-x). \tag{1}$$

Так, например,

$$X_3 = x^2 + x + 1,$$

поэтому

$$X_6 = x^2 - x + 1;$$

например,

$$X_5 = x^4 + x^3 + x^2 + x + 1,$$

поэтому

$$X_{10} = x^4 - x^3 + x^2 - x + 1.$$

Если n есть степень числа 2, т е. $n = 2^\lambda$ то получаем

$$X_n = \frac{x^n - 1}{x^{\frac{n}{2}} - 1} = x^{\frac{n}{2}} + 1. !$$

Например,

$$X_4 = x^2 + 1,$$
$$X_8 = x^4 + 1, \quad \text{и т.д.}$$

§ 22

Если мы поставим 1 вместо x в функцию $X_n(x)$, то мы видим, что для первых значений числа n получим значения

$$X_2(1) = 2, \quad X_3(1) = 3, \quad X_4(1) = 2, \quad X_5(1) = 5, \ \ldots$$

Можно доказать теорему:

При $n > 1$ значение $X_n(1)$ равняется простому числу p, если $n = p^\lambda$, равняется единице, если в состав числа n входит больше одного простого множителя.

В самом деле. на оснований формулы (4) § 19

$$X_{npp_1}(x) = \frac{X_n(x^{pp_1})}{X_n(x^{p_1})}$$

мы замечаем, что, если значок npp_1 содержит больше одного простого множителя, то мы имеем

$$X_{npp_1}(1) = \frac{X_n(1)}{X_n(1)} = 1.$$

Если же n есть степень

$$p^\lambda = p \cdot p_1,$$

то по формуле (1) § 19, получаем

$$X_{p^\lambda}(1) = p.$$

§ 23

Выведем теперь весьма важную теорему, указанную Eisenstein'ом[73]. На этой теореме Eisenstein основал доказательство, интересующей теперь нас, задачи о неприводимости X_n.

Теорема. *Если в целой функции*

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n$$

целые коэффициенты $a_0, a_1, \ldots, a_n$ таковы, что a_0 не делится на некоторое простое число p, все остальные коэффициенты $a_1, a_2, \ldots, a_n$ делятся на p, причем последний коэффициент a_n не делится на p^2, то функция $f(x)$ неприводимая.

Допустим обратное, а именно, что функция $f(x)$ приводима, т. е.

$$f(x) = (\alpha_0x^h + \alpha_1x^{h-1} + \ldots + \alpha_h)(\beta_0x^k + \beta_1x^{k-1} + \ldots + \beta_k);$$

числа h и k оба больше нуля и дают в сумме n.

Так как $\alpha_h\beta_k = a_n$, то из двух множителей α_h и β_k должен только один делиться на p, а другой не должен делиться. Пусть делится на p коэффициент β_k, а α_h не делится. Все β не могут делиться на p, ибо иначе делился бы коэффициент a_0, что противоречить предположению. Итак, пусть β_λ не делится на p, а все следующие $\beta_{\lambda+1}, \beta_{\lambda+2}, \ldots, \beta_k$ делятся. Составляя коэффициент при $x^{k-\lambda}$ в произведении обоих полиномов, получаем

$$\alpha_h\beta_k + \alpha_{h-1}\beta_{\lambda+1} + \ldots$$

Этот коэффициент, очевидно, на p не делится.

Приходится предположить, что $k - \lambda = n$, а это невозможно, ибо $k < n$.

§ 24

Применим теорему Eisenstein'а к доказательству неприводимости функции

$$X_p = \frac{x^p - 1}{x - 1}$$

при p простом. Положим $x = z + 1$, тогда получим

$$X_p(z+1) = \frac{1}{z}\,[((z+1)^p - 1] = z^{p-1} + pz^{p-2} + \frac{p(p-1)}{1\cdot 2}\,z^{p-3} + \ldots + p.$$

В правой части все коэффициенты кроме первого делятся на p, причем последний делится только на первую степень p. Значит, $X_p(z+1)$ есть функция неприводимая, а, следовательно, тоже самое будет иметь место также для функции $X_p(x)$, что и требовалось доказать.

§ 25

[73] Crelle's Journal, Bd. 39, (1850).

Подобным образом можно доказать справедливость теоремы о неприводимости X_n при $n = p^k$, где p простое число.

Мы имеем

$$X_n(x) = \frac{x^{p^k} - 1}{x^{p^{k-1}} - 1}.$$

Полагая $x = z + 1$, мы видим, что $X_n(z+1)$ получаем от деления $x^{p^k} - 1 = z^{p^k} + p\varphi(z)$ на $x^{p^{k-1}} - 1 = z^{p^{k-1}} + p\psi(z)$, где функции $\varphi(z)$ и $\psi(z)$ имеют целые коэффициенты. Обдумывая механизм выкладки деления, мы придем к заключению, что

$$X_n(z+1) = z^{p^{k-1}} + p\omega(z), \tag{1}$$

где $\omega(z)$ также целая функция с целыми коэффициентами. Для приложения теоремы Eisenstein'a необходимо убедиться, что независимый от z член в функций (1) не делится на p^2. Это, действительно, имеет место, ибо подставляя $z = 0$, мы должны припомнить формулу $X_n(1) = p$ § 22.

О неприводимости X_n в общем случае

§ 26

Доказательство неприводимости X_n при произвольном n вначале представило математикам значительные трудности; эти трудности были однако превзойдены и мы в настоящее время имеем ряд доказательств, предложенных различными авторами. Мы приведем здесь доказательства Dedekind'a, Ardt'a и Petersen'a.

Предварительно мы дадим несколько основных теорем, относящихся к теории функциональных сравнений по простому модулю p.

Мы будем писать сравнение

$$F(x) \equiv 0 \pmod p,$$

если все целые коэффициенты целой функции $F(x)$ делятся на p, т. е., иначе говоря, сравнимы с нулем по модулю p[74]

Сравнение

$$f(x) \equiv \varphi(x) \pmod p$$

должно обозначать, что коэффициенты при одинаковых степенях x в $f(x)$ и в $\varphi(x)$ сравнимы между собой по модулю p. Например,

$$2x^2 - x + 3 \equiv 7x^2 + 4x - 2 \pmod 5.$$

Теорема Schönemann'a. *При произвольных переменных независимых* $u, v, w, \ldots$ *имеет место сравнение*

$$(u + v + w + \ldots)^p = u^p + v^p + w^p + \ldots \pmod p.$$

[74]Д. Граве Элементарным курс теории чисел, вт. изд. 1913. Глава III.

Доказательство этой теоремы основано на свойстве полиномиального коэффициента (см. § 6: Глава I)

$$\frac{p\cdot(p-1)\cdot(p-2)\cdots 2\cdot 1}{1\cdot 2\cdots a\ 1\cdot 2\cdots b\ \ldots\ 1\cdot 2\cdots d},$$

где $a+b+\ldots+d=p$, делиться на простое число p, ибо простого числа p нет среди множителей знаменателя.

Из этой теоремы вытекаст ряд важных следствий.

Рассмотрим уравнение

$$f(x)=x^n+a_1x^{n-1}+a_2x^{n-2}+\ldots+a_n=0 \tag{1}$$

с *целыми* коэффициентами $a_1,a_2,\ldots,a_n$.

Мы имеем

$$-a_1=\sum\alpha,\quad a_2=\sum\alpha\beta,\quad -a_3=\sum\alpha\beta\gamma,\quad \ldots, \tag{2}$$

где через $\alpha,\beta,\gamma,\ldots$ обозначены корни (1).

Пусть p обозначает произвольное простое число. Составим уравнение

$$F(x)=x^n+A_1x^{n-1}+A_2x^{n-2}+\ldots+A_n=0, \tag{3}$$

корни которого суть p-ые степени корней заданного (1), т. е.

$$F(x)=(x-\alpha^p)(x-\beta^p)(x-\gamma^p)\cdots$$

Значит,

$$-A_1=\sum\alpha^p,\quad A_2=\sum\alpha^p\beta^p,\quad -A_3=\sum\alpha^p\beta^p\gamma^p,\quad \ldots, \tag{4}$$

Сравнивая (4) и (2) и принимая во внимание теорему Schönemann'a, получим

$$A_1\equiv a_1^p,\ A_2\equiv a_2^p,\ A_3\equiv a_3^p,\ \ldots\ (\mathrm{mod}\,p), \tag{5}$$

где, очевидно, числа $A_1,A_2,A_3,\ldots$ суть целые, ибо на оснований (4) эти числа как симметрические функции от корней $\alpha,\beta,\gamma,\ldots$ выражается в виде целых функции от $a_1,a_2,\ldots,a_n$ с целыми коэффициентами.

На основании теоремы Fermat'a[75] можно будет сравнения (5) переписать так

$$A_1\equiv a_1,\ A_2\equiv a_2,\ A_3\equiv a_3,\ \ldots\ (\mathrm{mod}\,p).$$

Сопоставляя же эти сравнения с (1) и (3) получим сравнение

$$F(x)\equiv f(x)\ (\mathrm{mod}\,p), \tag{6}$$

выражающее весьма важную теорему.

[75]Д. Граве Элементарным курс теории чисел, вт. изд. 1913. Глава III § 9.

§ 27

Начнем с доказательства Petersen'a[76]

Если X_n приводимая функция, т. е. если

$$X_n(x) = \psi_1(x)\psi_2(x)\cdots, \tag{1}$$

где $\psi_i(x)$ суть неприводимые целые функции с целыми коэффициентами со старшим коэффициентом равным единице, то, 1) *все функции* $\psi_1(x), \psi_2(x), \ldots$? *имеют одну и ту же степень,* 2) *корни всякой функции* $\psi_i(x)$ *будут получаться от возвышения в некоторую степень корней* $\psi_1(x)$.

В самом деле, пусть α будет корень функций $\psi_1(x)$; по определенно функции X_n корень α будет первообразным степени n корнем из единицы.

Пусть β будет какой нибудь корень функций $\psi_2(x)$; так как β будет другим первообразным корнем степени n из единицы, то мы будем иметь $\beta = \alpha^k$, где k число взаимно простое с n.

Составим уравнение $\psi(x)$, корни которого получаются от возвышения в степень k корней уравнения $\psi_1(x) = 0$. Два уравнения $\psi(x) = 0$, $\psi_2(x) = 0$ имеют один общий корень α^k, следовательно, на основании неприводимости $\psi_2(x)$ функция $\psi(x)$ должна делиться на $\psi_2(x)$. Значить, степень $\psi(x)$ не ниже $\psi_2(x)$, то есть, степень $\psi_1(x)$ не ниже степени $\psi_2(x)$. Меняя ролями функции ψ_1 и ψ_2, приходим к убеждению, что обе эти функции имеют одну и туже степень.

§ 28

Приложим теорему § 27 к доказательству неприводимости X_n при $n = p^k$.

Подставляя $x = 1$ в равенство (1) § 27, получим

$$p = \psi_1(1)\psi_2(1)\cdots$$

Откуда один из множителей $\psi_i(1)$ должен равняться $\pm p$, а остальные ± 1. Пусть $\psi_1(1) = \pm p$, $\psi_2(1) = \pm 1$. Если мы положим

$$\psi_1(x) = (x-\alpha)(x-\beta)(x-\gamma)\cdots,$$

то будет

$$\psi_2(x) = (x-\alpha^k)(x-\beta^k)(x-\gamma^k)\cdots$$

Получаем далее

$$\frac{1}{p} = \pm\frac{\psi_2(1)}{\psi_1(1)} = \pm\frac{1-\alpha^k}{1-\alpha}\cdot\frac{1-\beta^k}{1-\beta}\cdot\frac{1-\gamma^k}{1-\gamma}\cdots = \\ = \pm(1+\alpha+\ldots+\alpha^{k-1})(1+\beta+\ldots+\beta^{k-1})\cdots$$

Последнее равенство *невозможно*, ибо левая часть $\dfrac{1}{p}$ — есть правильная дробь, тогда как правая часть будет целым числом, ибо эта правая часть, есть целая симметрическая функция от корней ψ_1 с целыми коэффициентами.

[76] Petersen. Théorie des équations algébraiques. 1897. p. 349

§ 29

Приступаем теперь к доказательству неприводимости X_n в общем случае. Допустим приводимость

$$X_n = \psi_1(x)\psi_2(x)\cdots$$

И рассмотрим все возможные разности

$$\psi_i(x) - \psi_k(x). \tag{1}$$

Пусть m будет целое число, выбранное под двумя условиями: 1) чтобы было $m > n$, 2) чтобы было m больше всякого делителя всех целых коэффициентов всех разностей (1).

Пусть корни $\psi_2(x)$ происходят от корней $\psi_1(x)$ через возвышение в степень k, где k число взаимно простое с n. Возьмем целое число

$$t = ASn + k, \tag{2}$$

где A есть произведение простых чисел, не превосходящих m и не входящих k. Если мы разложим число t на простые множители

$$t = q_1 q_2 q_3 \cdots,$$

то все эти простые множители $q_1, q_2, \ldots$ должны быть больше m.

Через возвышение корней ψ_1 в степень t получается, очевидно, на основании (2), функция ψ_2. Будем теперь возвышать корни функций ψ_1 последовательно в степени $q_1, q_2, \ldots$. Так как произведение t переводит ψ_1 в ψ_2, то не может ψ_1 остаться без изменений при возвышении ее корней в степень всякого одного из множителей q. Пусть при возвышении в степень q_1 функция переходит в другую ψ_1, тогда, применяя теорему § 26, получим

$$\psi_1 \equiv \psi_i \pmod{q_1},$$

что невозможно, ибо $q_1 > m$.

§ 30

Приведем теперь доказательство Dedekind'a[77]

Для доказательства неприводимости X_n поступим так. Пусть $f(x)$ будет один из неприводимых множителей полинома X_n, если мы допустим приводимость функции X_n. Пусть α один из корней $f(x)$.

Корень α есть в тоже время корень X_n, т. е. первообразный корень степени n из единицы. Если мы докажем, что α^μ будет корнем функции $f(x)$ при всяком числе μ взаимно простом с n, то отсюда вытечет $f(x) = X_n$ и неприводимость X_n будет доказана.

Достаточно показать справедливость сказанного для случая $\mu = p$, где p простое число, не входящее в состав числа n; ибо в случае μ составного мы можем повторить рассуждение относительно всех его простых делителей взятых в известном порядке.

[77]Dedekind. Beweis für die Irreducibilität der Kreisteilungsgleichungen. Crelle J. Bd. 54.

Возвысим все корни

$$\alpha, \quad \beta, \quad \gamma, \quad \ldots$$

функции $f(x)$ в степень p

$$\alpha^p, \quad \beta^p, \quad \gamma^p, \quad \ldots \tag{1}$$

Очевидно, что числа (1) все различные между собой, ибо обозначая через p' число удовлетворяющее сравнений $p'p \equiv 1 \pmod n$, можем возвысить равенство $\alpha^p = \beta^p$ в степень p' и получим $\alpha = \beta$, что противоречило бы предположению неприводимости $f(x)$.

Пусть $F(x)$ будет та функция, которой корнями являются числа (1).

Нетрудно убедиться, что функция $F(x)$ неприводимая.

Допустим обратное и пусть будет $F_1(x)$ тот из неприводимых множителей функции $F(x)$, который имеет корень α^p, так что $F_1(\alpha^p) = 0$. Мы видим, следовательно, что уравнение $F_1(x^p) = 0$ удовлетворяется одним из корней α неприводимой функции $f(x)$; значит, это уравнение должно удовлетворяться всеми остальными корнями

$$F_1(\alpha^p) = 0, \quad F_1(\beta^p) = 0, \quad F_1(\gamma^p) = 0, \quad \ldots$$

то есть функция $F_1(x)$ совпадает с $F(x)$, что и требовалось показать.

Если функция $f(x)$ первоначальная, то такова же будет и функция $F(x)$. Две неприводимые функции $f(x)$ и $F(x)$ одной степени должны или совпадать или быть взаимно простыми. Допустим второе предположение. Если функции $f(x)$ и $F(x)$ не имеют общих множителей, то они представляют из себя два различных делителя функции $x^n - 1$ и мы приходим к тождеству

$$x^n - 1 = f(x)F(x)\varphi(x), \tag{1}$$

где $\varphi(x)$ функция с целыми коэффициентами.

На основании теоремы Schönemann'a (6) § 26 получаем

$$F(x) \equiv f(x) \pmod p,$$

следовательно, равенство (1) может быть переписано так

$$x^n - 1 = [f(x)]^2\varphi(x) + p\omega(x), \tag{2}$$

отсюда, дифференцируя, получим

$$nx^{n-1} = f(x)X(x) + p\lambda(x), \tag{3}$$

где $\omega(x)$, $X(x)$, $\lambda(x)$ целые функций с целыми коэффициентами. Умножая (2) на $-n$, а (3) на x и складывая, получим *невозможное* сравнение

$$n \equiv f(x)\Phi(x) \pmod p, \tag{4}$$

где $\Phi(x)$ функция с целыми коэффициентами. Так как число n не делится на p, то нельзя предполагать все коэффициенты $\Phi(x)$ делящимися на p, а значит в правой части сравнения (4) должен существовать по крайней мере один член, содержащий x с неделящимся на p коэффициентом и сравнение (4) невозможно.

Итак $F(x) = f(x)$, мы получаем, следовательно, $f(\alpha^p) = 0$ и теорема доказана.

§ 31

Приведем, наконец, доказательство Arndt'a[78].

Будем доказывать справедливость теоремы для уравнения

$$X_n = 0,$$

где $n = p^\alpha \cdot n'$, предполагая доказанною неприводимость $X_{n'}$ для числа n', заключающего меньшее число различных между собой простых множителей. Мы предполагаешь, что простое число p не входить в состав числа n'.

Допустим обратное, а именно, что функция X_n разлагается на два целочисленных множителя

$$X_n = \varphi(x)\psi(x).$$

Пусть

$$\Phi(x) = 0, \qquad \Psi(x) = 0$$

будут уравнения, которым удовлетворяют p^α степени корней соответственных уравнений

$$\varphi(x) = 0, \qquad \psi(x) = 0.$$

На основании теоремы Schönemann'a получаем

$$\varphi(x) \equiv \Phi(x),\ \psi(x) \equiv \Psi(x) \pmod p. \tag{1}$$

Всякий первообразный корень r из единицы степени n может быть представлен в виде

$$r = \rho r',$$

где ρ есть первообразный корень степени p^α, а r' первообразный корень степени n'.

Очевидно, что

$$r^{p^\alpha} = r'^{p^\alpha}$$

будет первообразным корнем степени n'.

Возьмем произвольный из корней r' неприводимого на основании нашего допущения уравнения $X_{n'} = 0$.

Итак, мы видим, что каждое из уравнений $\Phi(x) = 0$, $\Psi(x) = 0$ имеет корень $r^{p^\alpha} = r'^{p^\alpha}$ общий с уравнением $X_{n'} == 0$. На основании допущенной неприводимости последнего уравнения получим

$$\varphi(r') \equiv 9,\ \psi(r') \equiv 0 \pmod p$$

или, что одно и тоже,

$$X_n(r') = p^2 f(r'), \tag{2}$$

[78] *Arndt.* Einfacher Beweis für die Irreducibilität einer Gleichung in der Kreisteilung. Crelle Journ. Bd. 56. *Lebesgue.* Demostration de l'irrediicibilité de l'équation aux racines primitives de l'unité. Journ. de Liouville T. 4. Serie II.

где r' произвольный корень уравнения $X_{n'} = 0$.

Мы видели уже, что

$$x^n - 1 = \prod X_d(x), \qquad x^{\frac{n}{p}} - 1 = \prod X_\delta(x),$$

где значок d распространяется на все делители числа n; а значок δ на все делители числа $\dfrac{n}{p}$. Отсюда мы видим, что δ не может равняться n, тогда как среди d существует значок равный n. Итак, целая функция

$$\frac{x^n - 1}{x^{\frac{n}{p}} - 1}$$

должна делиться на X_n и мы получаем

$$\frac{x^n - 1}{x^{\frac{n}{p}} - 1} = X_n(x) \cdot \omega(x),$$

полагая $x = r'$ получаем

$$p = X_n(r')\omega(r').$$

Сопоставляя же с (2), получим

$$1 = pd(r')\omega(r').$$

Удаляя из произведения $f(r')\omega(r')$ все степени r' выше $\varphi(n')$ при помощи уравнения $X_{n'} = 0$, придем к равенству

$$1 = p(a_0 + a_1 r' + a_2 r'^2 + \ldots),$$

дающему невозможное равенство

$$1 = pa_0,$$

ибо все числа $a_0, a_1, a_2, \ldots$ целые. И теорема, подлежавшая доказательству, оказывается справедливою.

Относительная приводимость целых функций

§ 32

Скажем теперь несколько слов об одном очень важном понятии, о так называемой, *относительной приводимости* функций. Можно доказать такую теорему.

Теорема. *Заданы две неприводимым целые функции $f(x)$, $\varphi(x)$. Если одна из них $f(x)$ делается приводимою от присоединения корня η другой $\varphi(x)$, то и вторая $\varphi(x)$ сделаетсл приводимою при присоединении корня ξ первой функций $f(x)$.*

Итак, по предположению функция $f(x)$ делается приводимою от присоединения корня η второй, следовательно, имеем

$$f(x) = f_1(x, \eta) f_2(x, \eta)$$

Целые функции f_1, f_2 от двух аргументов x, η можно предполагать относительно η степени меньшей степени функции φ, ибо все высшие степени можно уничтожить при помощи уравнения $\varphi(\eta) = 0$.

Если ξ есть корень функции $f(x)$, то мы имеем

$$f_1(\xi, \eta) f_2(\xi, \eta) = 0.$$

Итак, уравнение

$$f_1(\xi, y) f_2(\xi, \eta) = 0$$

имеет один общий корень η с уравнением $\varphi(y) = 0$.

Очевидно, что предположение о том, что функция $\varphi(x)$ остается неприводимой при присоединении ξ, падает, ибо функция

$$f_1(\xi, y) f_2(\xi, \eta)$$

должна делиться на неприводимую функцию $\varphi(y)$ между тем как ни один из множителей f_1, f_2 будучи функцией низшей степени не может делиться.

§ 33

Итак, мы видим, что каждые две функции $f(x)$ и $\varphi(x)$ либо остаются неприводимыми при присоединении к одной корня другой, или же они суть взаимно приводимые.

Покаажем на примере случай взаимной неприводимости.

Функции X_n, X_m взаимно неприводимы, если числа n и m суть числа взаимно простые[79].

Обозначим через ν один из корней X_n, а через μ один из корней X_m.

Выражение $\rho = \nu\mu$ будет первообразным корнем степени mn из единицы.

Подберем два целых рациональных числа x и y, удовлетворяющие равенству

$$nx + my = 1.$$

Получим

$$\nu = \rho^{my}, \qquad \mu = \rho^{nx}.$$

Допустим взаимную приводимость X_n и X_m. Пусть

$$\varphi(x, \mu)$$

будет множитель X_n, предполагая, что последняя функция сделалась приводимою от присоединения корня μ функций X_m. Очевидно, что по крайней мере для одного из корней ν функций X_n будет удовлетворяться уравнение

$$\varphi(\nu, \mu) = 0,$$

которое можно переписать еще так

$$\varphi(\rho^{my}, \rho^{nx}) = 0. \tag{1}$$

[79] *Kronecker*. Mém. sur les facteurs irréductibles de l'expression $x^n - 1$. Journ. de Liouville. T. 19. (1854).

Вследствие доказанной неприводимости X_{mn} в области рациональных чисел, можно подставить в уравнение (1) вместо ρ другой корень ρ^h, где h число взаимно простое с mn:

$$\varphi(\rho^{hmy}, \rho^{hnx}) = 0. \tag{2}$$

Возьмем совершенно произвольное число s, взаимно простое с n и подберем h так, чтобы было[80]

$$h \equiv s \pmod{n},\ h \equiv 1 \pmod{n},$$

тогда равенство (2) примет вид

$$\varphi(\nu^s, \mu) = 0$$

и, следовательно, $\varphi(x, \mu)$ делится на X_n. Отсюда получается неприводимость X_n, которая остается после присоединения μ, т. е. другими словами получается взаимная неприводимость функций X_n, X_m.

§ 34

Относительно функций взаимно приводимых можно доказать ряд дальнейших свойств. Обе функции раскладываются на одинаковое число множителей причем степени этих множителей в одной функции пропорциональны степеням их в другой.

Landsberg показываот в 132 томе журнала Crelle'a связь этого вопроса с разложением групп по двойному модулю.

Вычисление дискриминанта X_n

§ 35

В книге Weber'a Lehrbuch der Algebra дается вычисление дискриминанта уравнения $X_n = 0$ только для случая $n = p^k$, где p простое число; между тем как вычисление дискриминанта также для общего случая производится совершенно элементарно[81] на основании тех же самых соображений.

Мы имеем

$$X_n(x) = \frac{(x^n - 1)\prod(x^{\frac{n}{pq}} - 1)\cdots}{\prod(x^{\frac{n}{p}} - 1)\prod(x^{\frac{n}{pqr}} - 1)\cdots}\ .$$

Для получения дискриминанта составляем произведение

$$\varepsilon \prod X_{n'}(r), \tag{1}$$

где $\varepsilon = (-1)^{\frac{n_1(n_1-1)}{2}}$, $n_1 = \varphi(n)$, а произведение $\prod$ распространяется на все $\varphi(n)$ корней r уравнения $X_n = 0$.

[80] Д. Граве. Элементарный курс теории чисел. Втор. изд. 1913 г. Стр. 54.

[81] Rados. Crelle's Journ. 131, 49 (1906).

Очевидно, что при вычислений произведения (1) достаточно заменить производную $X_n'(x)$ выражением

$$(2) \qquad \frac{nx^{n-1}\prod(x^{\frac{n}{pq}}-1)\cdots}{\prod(x^{\frac{n}{p}}-1)\prod(x^{\frac{n}{pqr}}-1)\cdots},$$

происходящим от дифференцировании только одного первого множителя x^n-1 выражения X_n.

Подставим вместо x в выражение (2) последовательно все корни $r_1, r_2, \ldots, r_{n_1}$ уравнения $X_n = 0$ и перемножим полученные результаты. Получаем прежде всего в числителе

$$n^{\varphi(n)}.$$

Кроме того будет иметь место равенство

$$(r_1 r_2 \cdots r_{n_1})^{n-1} = 1,$$

ибо равно единице произведение всех первообразных корней из единицы[82].

Точно также дадут единицу в произведении части $\prod(r_i^{\frac{n}{pq}}-1)$, $\prod(r_i^{\frac{n}{pqr}}-1)$, ..., а потому остается лишь рассмотреть часть знаменателя

$$\prod(x^{\frac{n}{p}}-1).$$

Рассмотрим выражение

$$(3) \qquad (r_1^{\frac{n}{p}}-1)(r_2^{\frac{n}{p}}-1)\cdots(r_{n_1}^{\frac{n}{p}}-1) = (-1)^{n^2}\prod(1-r_i^{\frac{n}{p}}).$$

Но $r_i^{\frac{n}{p}}$ есть первообразный корень степени p из единицы, следовательно, выражение (3) имеет вид

$$(-1)^{n_1}\cdot[X_p(1)]^{\nu} = (-1)^{n_1}\cdot p^{\nu},$$

где ν обозначает число одинаковых из чисел

$$r_i^{\frac{n}{p}}.$$

Обозначая $r_i = r^i$, где r один определенный из первообразных корней. Мы получаем $r_k^{\frac{n}{p}} = r_l^{\frac{n}{p}}$, если $\frac{n}{p}\,k \equiv \frac{n}{p}\,l \pmod n$ или $k \equiv k \pmod p$. Итак, надо посмотреть, сколько из чисел

$$k = l + px$$

взаимно простых с n или, что одно и тоже, с $\frac{n}{p}$, если x пробегает полную систему вычетов по модулю $\frac{n}{p}$.

На основании классической[83]) теоремы теории чисел мы имеем

$$\nu = \frac{\varphi\left(p\frac{n}{p}\right)}{\varphi(p)} = \frac{\varphi(n)}{\varphi(p)}.$$

[82]Д. Граве. Элементарный курс теории чисел. Вт. изд. 1913 г., стр. 177.
[83]Д. Граве. Элементарный курс теории чисел. Вт. изд. 1913 г., стр. 50.

Итак, получаем окончательное выражение для дискриминанта

$$\frac{(-1)^{\frac{\varphi(n)}{2}} n^{\varphi(n)}}{p_1^{\frac{\varphi(n)}{\varphi(p_1)}} p_2^{\frac{\varphi(n)}{\varphi(p_2)}} \cdots p_l^{\frac{\varphi(n)}{\varphi(p_l)}}},$$

где $p_1, p_2, \ldots, p_n$ суть простые числа, входящие в состав числа n.

В заключение мы намекнем читателю, почему обратятся в единицу части $\prod(x^{\frac{n}{pq}} - 1)$, $\prod(x^{\frac{n}{pqr}} - 1)$, ...

Это произойдет вследствие существований равенства $X_{pq}(1) = 1$, $X_{pqr} = 1$, ...

Глава XIV

Теория полей

§ 1

Совокупность всех рациональных чисел обладает, как известно из элементарной алгебры, следующими свойствами.

Все рациональные числа образуют абелеву группу (см. стр. 117) относительно *сложения*, ибо существуют свойства

$$a + b = b + a, \qquad (a + b) + c = a + (b + c).$$

Существует одна единица этой группы, а именно число 0 (нуль).

Всякому элементу a группы соответствует ему обратный $-a$, ибо

$$a + (-a) = 0.$$

На оснований сказанного в главе V, в группе всегда возможно решение уравнения первой степени

$$a + x = b,$$

то есть всегда выполняется действие вычитания, как операция, обратная сложению.

§ 2

На основании сказанного мы можем назвать совокупность рациональных чисел *аддитивной группой*. Единицей этой группы является число нуль. Если мы это число *отбросим*, то получим совокупность чисел, представляющих абелеву группу относительно *действия умножения*, ибо существуют свойства

$$ab = ba, \qquad (ab)c = a(bc).$$

Единицей этой группы является число 1; всякому элементу a соответствует обратный $\dfrac{1}{a}$, ибо

$$a\,\frac{1}{a} = 1.$$

В этой группе (без числа 0), которую мы назовем *мультипликативною*, всегда возможно решение уравнения первой степени

$$ax = b,$$

то есть всегда возможно действие деления.

Нельзя делить только на 0, то есть на *единицу* аддитивной группы.

§ 3

Число 0, умноженное на любое число рассматриваемой совокупности дает 0:

$$0 \cdot a = 0.$$

Действия сложения и умножения удовлетворяют *распределительному* (дистрибутивному) закону

$$(a + b)c = ac + bc.$$

§ 4

Совокупность чисел, обладающих свойствами указанными в §§ 1, 2, 3, мы будем называть *числовым полем.*

Рациональные числа образуют поле.

Элементарная алгебра дает еще два примера подобных полей чисел: 1) поле вещественных (рациональных и иррациональных), 2) поле чисел комплексных.

Общее понятие поля

§ 5

Современная математика требует введения в рассмотрение более общего понятая о *поле* (Körper) совершенно абстрактного характера. Поле могут образовать не только числа, но и предметы какой угодно природы, которые мы будем называть *элементами* поля.

Поле должно представлять из себя группу относительно двух операций, которые мы назовем *сложением* и *умножением*, совершенно независимо от их природы. Мы эти операции будем обозначать теми же знаками, что и в элементарной алгебре. Вся суть будет состоять в том, что операции производимые над элементами поля должны удовлетворять всем вышеприведенным (§ 1, 2, 3) основным законам рациональных действий элементарной алгебры.

Таким образом мы приходим к такому общему определенно поля.

Полем мы будем называть всякую совокупность таких предметов $a, b, c, \ldots$, *названных его элементами, которые можно подчинить двум различным приемам групповой композиции, из которых один назовем сложением* $(a+b)$, *а другой умножением* ab, *причем имеют место следующие постулаты:*

I. *Все элементы поля образуют группу относительно сложения, единицу которой обозначим через* 0.

II. *Все элементы поля за исключением* 0 *образуют группу относительно умножения.*

III. *Имеет место распределительный закон*

$$(a + b)c = ac + bc.$$

IV. *Для всякого элемента a имеет место*

$$0 \cdot a = 0.$$

V. *Обе группы аддитивная и мультипликативная суть абелевы*

$$a + b = b + a, \qquad ab = ba.$$

§ 6

Сделаем несколько весьма важных замечаний по поводу только данного определения поля.

Вследствие группового характера поля действие вычитания в нем всегда возможно. Что касается до действия деления, то оно возможно для всех элементов за исключением случая деления на единицу аддитивной группы. Эта единица обладает в поле всеми свойствами числа 0 элементарной алгебры.

Произведение нескольких множителей в поле может тогда и только тогда равняться аддитивной единице, если один из множителей равен этой единице.

§ 7

Рассматривая внимательно указанные в § 5 пять постулатов, мы можем заметить, что в постулате V достаточно требовать *только, чтобы мультипликативная группа была перестановочною*, тогда можно доказать, что при существовании четырех первых постулатов и аддитивная группа будет перестановочна.

В самом деле, возьмем единицу мультипликативной группы [1] и два произвольных элемента a и b. Будем иметь на основании первых постулатов

$$\begin{gathered} a+b+a+b = (a+b)+(a+b) = [1](a+b)+[1](a+b) = \\ = \{[1]+[1]\}(a+b) = (a+b)\{[1]+[1]\} = a\{[1]+[1]\}+b\{[1]+[1]\} = \\ = \{[1]+[1]\}a+\{[1]+[1]\}b = a+a+b+b, \end{gathered}$$

итак,

$$a+b+a+b = a+a+b+b.$$

Прибавляя к обеим частям слева $-a$ и справа $-b$, получим

$$b+a = a+b,$$

т. е. получаем коммутативность аддитивной группы.

§ 8

Рассматривая три поля, известных из элементарной алгебры, мы замечаем, что первое поле *рациональных чисел* заключается как часть в двух остальных: поле *вещественных чисел* и поле *комплексных чисел*.

Если элементы поля Ω входят в состав другого поля Ω_1, то поле Ω носит название *делителя* поля Ω_1. Так, например, поле вещественных чисел есть делитель поля комплексных чисел.

Не трудно показать, что поле рациональных чисел есть делитель всякого поля. В самом деле, возьмем какой нибудь элемент ω поля Ω, тогда поле Ω должно заключать элемент $\frac{\omega}{\omega}$, т. е. число единицу; из единицы же можно получить все целые числа при помощи сложения, вычитания и умножения, из целых же чисел происходят дробные через деление.

Более строгая формулировка только что указанного свойства получится, если мы введем весьма важное понятие о так называемом *изоморфизме* полей.

Так как элементами поля могут быть предметы какой угодно природы, не обязательно числа, то мы считаем за одно поле два так называемых изоморфных поля, т. е. таких, что всякому рациональному соотношению

$$f(a, b, c, \ldots) = 0$$

элементов $a, b, c, \ldots$ одного поля соответствует тождественное соотношение

$$f(a', b', c', \ldots) = 0$$

соответственных элементов $a', b', c', \ldots$ другого.

Такой изоморфизм двух полей устанавливает однозначное соответствие каждому элементу a первого поля некоторый определенный элемента a' другого.

Если поле таково, что его элементы не числа, а предметы другой природы, то мультипликативная единица [1] поля может не быть числом 1, тогда получаем теорему, что всякое поле Ω имеет делителем некоторое другое поле R, изоморфное с полем рациональных чисел; это поле R назовем *арифметическою частью* поля Ω.

§ 9

Пусть задано числовое поле Ω и некоторое число α, не входящее в состав поля Ω. Рассмотрим теперь поле, образованное числами поля Ω, а также всевозможными новыми, получаемыми от комбинирования числа α с числами поля Ω при помощи основных действий.

Очевидно, что всякое число нового поля будет вида

$$\frac{\varphi(\alpha)}{\psi(\alpha)},$$

где $\varphi(\alpha)$ и $\psi(\alpha)$ суть целые функции от α с коэффициентами, принадлещиими полю Ω.

Будем обозначать новое поле так

$$\Omega(\alpha)$$

и говорить, что оно происходит от *присоединения* к полю Ω числа α.

Если к полю $\Omega(\alpha)$ присоединим новое число β, то получим поле

$$\Omega(\alpha, \beta),$$

которое происходить из поля Ω через присоединсние двух чисел α и β.

Подобным же образом можно присоединить любое число чисел.

§ 10

Рассмотрим целую рациональную функцию

$$f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n$$

с коэффициентами

$$a_0, \quad a_1, \ \ldots, \ a_{n-1}, \quad a_n$$

принадлежащими к некоторому полю Ω.

Будем называть такую функций *принадлежащею полю* Ω, или просто *функцией поля* Ω.

Если функция $f(x)$ разлагается на два множителя

$$\varphi(x) \quad \text{и} \quad \psi(x),$$

так что

$$f(x) = \varphi(x)\psi(x),$$

причем целые функции $\varphi(x)$ и $\psi(x)$ принадлежать тому же полю Ω, то будем говорить, что функция $f(x)$ *приводимая в поле* Ω, т. е. нахождение ее корней приводится к нахождение корней функции $\varphi(x)$ и $\psi(x)$ меньших степеней.

Если разложение функции $f(x)$ на множители, принадлежащие тому же полю, невозможно, то говорить, что функция *неприводима* в поле Ω.

Одна и та же функция может быть неприводимою в одном поле и приводимою в другом. Так например, функция

$$x^4 + 1$$

неприводима в поле рациональных чисел и приводима в таком поле, которое получается от присоединения к рациональным числам числа

$$\sqrt{2},$$

ибо

$$x^4 + 1 = (x^2 + \sqrt{2}x + 1)(x^2 - \sqrt{2}x + 1).$$

В поле всех чисел как вещественных, так и комплексных, всякая функция выше первой степени приводима и раскладывается на линейные множители, что составляет основную теорему алгебры.

§ 11

Необходимо обратить внимание, что формула Taylor'a для целых функций остается справедливою и для целых функции некоторого поля, ибо эта формула

$$f(x+h) = f(x) + hf'(x) + \frac{h^2}{1\cdot 2}f''(x) + \ldots + \frac{h^n}{1\cdot 2\cdot 3\cdots n}f^{(n)}(x)$$

происходит от разложения $f(x+h)$ по степеням h; для целых же функций такое разложение совершается при помощи рациональных действий.

Раз формула Taylor'a сохраняется в поле, то отсюда вытекает для поля все те же следствия относительно кратных корней, которые излагаются в алгебре.

§ 12

При общих исследованиях о полях имеет большое значение, введенное Steinitz'ом[84] понятие о так называемой *характеристике* поля.

Это понятие можно ввести таким образом.

Возьмем мультипликативную единицу ε поля. Можно положить

$$\varepsilon = 1\varepsilon, \quad \varepsilon + \varepsilon = 2\varepsilon, \quad 2\varepsilon + \varepsilon = 3\varepsilon, \ldots$$

Числа $\varepsilon, 2\varepsilon, 3\varepsilon, \ldots$ называются *натуральными кратными* элемента ε; здесь $1, 2, 3, \ldots$ не суть элементы поля, а лишь знаки. Для отрицательного целого числа $-n$ можно будет положить

$$-(n\varepsilon) = (-n)\varepsilon.$$

Итак элемент $m\varepsilon$ определен для всякого целого значения m как положительного так и отрицательного. Возможны два случая полей.

Равенство

$$m\varepsilon = m'\varepsilon \tag{1}$$

может или иметь место исключительно при существовании другого равенства

$$m = m', \tag{2}$$

или же может случиться, что для справедливости (1) нет надобности удовлетворять равенству (2).

Мы подчеркнем тот факт, что равенство (1) есть равенство символическое, имеющее место на основании свойств конструкции поля, равенство же (2) есть обыкновенное арифметическое.

Если поле таково, что всякое равенство вида (1) влечет за собою равенство (2), то мы будем говорить, что поле имеет *характеристику нуль*.

Поле имеет характеристику нуль, если все кратные $m\varepsilon$ мультипликативной единицы различны между собой.

Обратимся теперь к рассмотрению полей другого рода, когда равенство (1) имеет место без равенства (2). Равенство (1) можно будет переписать так

$$(m - m')\varepsilon = 0.$$

Итак, в этом случае среди кратных $m\varepsilon$ должны быть равные нулю. Пусть будет первое из ряда кратных $\varepsilon, 2\varepsilon, 3\varepsilon, \ldots$ равное нулю соответствовать целому числу p

$$p\varepsilon = 0.$$

Покажем, 1) что элементы

$$\varepsilon, \quad 2\varepsilon, \quad 3\varepsilon, \ \ldots, \ (p-1)\varepsilon$$

[84] E. Steinitz. Algebraische Theorie der Körper. Grelles Journ. B. 137. Heft

различны между собой и 2) что p число простое.

В самом деле, если бы число p было не простым

$$p = qr$$

то мы имели бы

$$p\varepsilon = (q\varepsilon)(r\varepsilon) = 0$$

и по § 6 выходило бы, или $q\varepsilon = 0$, или $r\varepsilon = 0$. Оба эти предположения противоречат допущению, что p есть наименьшее число, при котором уничтожается $p\varepsilon$.

Простое число p называется *характеристикой* поля.

В теории чисел[85] мы познакомились с замечательным представителем поля характеристики p, которое мы назвали *конечным*.

Поля с характеристикой отличной от нуля обладают особенными свойствами, а потому во всем дальнейшем мы будем предполагать равною нулю характеристику поля.

§ 13

Теорема. *Неприводимая в поле Ω функция $f(x)$ не имеет общего делителя с другою $F(x)$ того же поля, если $F(x)$ не делится на $f(x)$.*

Эта теорема, имеющая большое значение, почти очевидна. В самом деле, будем искать общий наибольший делитель полиномов

$$F(x) \quad \text{и} \quad f(x)$$

последовательным делением. Очевидно, что коэффициенты этого общего делителя происходят при помощи рациональных операций из коэффициентов функций $F(x)$ и $f(x)$, следовательно, общий делитель должен принадлежать тому же полю Ω. Но заданная функция $f(x)$ не имеет в поле Ω других делителей кроме самого себя и постоянного числа. Отсюда, общий наибольший делитель должен быть равным самой функции $f(x)$ или быть постоянным.

Следствие I. *Неприводимая функция не может иметь кратных корней*[86]

В самом деле, если бы существовал кратный корень, то производная $f'(x)$, имея общий делитель с неприводимой функцией $f(x)$, должна была бы делиться на $f(x)$, что невозможно, ибо степень производной ниже степени самой функции.

Следствие II. *Если функция $F(x)$ обращается в нуль при одном из корней неприводимой функции $f(x)$, то она уничтожается и при всех остальных корнях функции $f(x)$.*

Следствие III. *Если степень целой Функции $F(x)$ ниже степени неприводимой функции $f(x)$ и если $F(x)$ обращается в нуль при одном корне функции $f(x)$, то функция $F(x)$ должна тождественно обращаться в нуль, т. е. все ее коэффициенты должны равняться нулю).*

Следствие IV. *Приводимая функция разлагается одним только способом на неприводимые множители. При этом две целых функции, отличающиеся постоянными множителем, не считаются различными.*

[85] Д. Граве. Элементарный курс теории чисел. Вт. изд. 1913. Главы VIII.

[86] Это свойство может оказаться несправедливым при полях с отличной от нуля характеристикой. Steinitz, Crelles Journ. B. 137, H. I, S. 219.

§ 14

Присоединения новых величин разделяются на две категории: присоединения *алгебраические* и присоединения *трансцендентные*.

Присоединение называется трансцендентным, если между различными степенями присоединяемой буквы x не устанавливается никаких соотношений. Поле, получаемое от присоединения к полю Ω трансцендентной величины x, является совокупностью всех рациональных функции от x с коэффициентами из поля Ω.

Гораздо более простой вид имеет поле, когда между различными степенями присоединяемой буквы x имеет место линейное соотношение, т. е., другими словами, когда присоединяемая величина α есть корень алгебраического уравнения

$$F(x) = 0, \tag{1}$$

где $F(x)$ неприводимая в основном поле Ω функция.

Мы будем называть также и уравнение (1) *неприводимым* в поле Ω. Через присоединение к полю Ω корня α уравнения (1) получается поле $\Omega(\alpha)$, которое называется *алгебраическим полем*.

§ 15

Пусть уравнение $F(x) = 0$ имеет вид

$$x^n + a_1 x^{n-1} + \ldots + a_{n-1}x + a_n = 0,$$

где $a_1, a_2, \ldots, a_{n-1}, a_n$ суть числа поля Ω.

Степень n последнего уравнения носит название степени алгебраического поля $\Omega(\alpha)$.

Самый общий вид числа Θ поля $\Omega(\alpha)$ есть

$$\Theta = \frac{\varphi(\alpha)}{\psi(\alpha)},$$

где φ и ψ целые функции с коэффициентами из поля Ω.

Из § 24 главы IX известно, что всякая рациональная функция от корня неприводимого уравнения n-ой степени может быть представлена при помощи рациональных выкладок в виде целой функций степени не выше $n-1$, т. е.

$$\Theta = c_0 + c_1\alpha + c_2\alpha^2 + \ldots + c_{n-1}\alpha^{n-1}, \tag{1}$$

где коэффициенты

$$c_0, \quad c_1, \quad c_2, \quad \ldots, \quad c_{n-1}$$

принадлежат также к полю Ω.

Такое представление (I) элемента Θ возможно одним способом, ибо, если бы существовало другое представление

$$\Theta = c_0' + c_1'\alpha + c_2'\alpha^2 + \ldots + c_{n-1}'\alpha^{n-1}, \tag{2}$$

то корень α неприводимого уравнения степени n поля Ω удовлетворял бы уравнению

$$(c_0 - c_0') + (c_1 - c_1')\alpha + (c_2 - c_2')\alpha^2 + \ldots + (c_{n-1} - c_{n-1}')\alpha^{n-1} = 0$$

того же поля, откуда на основании следствия III § 13 получаем

$$c'_0 = c_0, \quad c'_1 = c_1, \ \ldots, \ c'_{n-1} = c_{n-1}.$$

Итак, поле $\Omega(\alpha)$ есть совокупность чисел Θ, определяемых формулой (1), где коэффициенты

$$c_0, \quad c_1, \quad c_2, \ \ldots, \ c_{n-1}$$

суть всевозможные элементы поля.

§ 16

Мы будем рассматривать алгебраически поля более общего вида

$$\Omega(\alpha, \beta, \gamma, \ldots),$$

получаемые от присоединения к полю Ω корней

$$\alpha, \quad \beta, \quad \gamma, \ldots$$

одного или нескольких уравнений поля Ω.

Докажем теперь весьма важное предложение, состоящее в том, что одновременное присоединено нескольких корней одного или нескольких уравнений равносильно присоединению *одного* корня *одного* уравнения. Таким путем мы приходим к заключению, что самый общий вид алгебраического поля дает поле, происходящее от присоединения к основному одного только алгебраического числа.

§ 17

Докажем предварительно лемму.

Лемма. *Пусть*

$$\Phi_1(x, y, z, \ldots), \quad \Phi_2(x, y, z, \ldots), \quad \Phi_3(x, y, z, \ldots), \ \ldots$$

суть целые рациональные функции переменных $x, y, z, \ldots$ с произвольными коэффициентами. Если ни у одной из этих функций все коэффициенты не обращаются сразу в нуль, то можно на бесчисленное число способов дать переменным такие рациональные значения, что ни одна из функций не обратится в нуль.

Предложите очевидно для случая, когда функции зависят от одной независимой переменной. Очевидно, что в этом случай функции будут обращаться в нуль только при своих корнях, число же таких корней конечное, а потому, если независимому переменному дадим значение, отличное от этих корней, то ни одна из функций

$$\Phi_1, \quad \Phi_2, \quad \Phi_3, \ \ldots$$

не обратится в нуль.

Что касается большого числа независимых переменных, то нетрудно убедиться в справедливости леммы в случае m переменных, если лемма доказана для $m-1$ переменных.

Каждую из функции можно представить в виде полинома от одной из переменных, напр., x, с коэффициентами, которые будут целыми фуцкциями от $m-1$ остальных переменных

$$y, \quad z, \quad \ldots$$

По предположению справедливости леммы в случай $m-1$ переменных, можно будет буквам

$$y, z, \ldots$$

на бесчисленное число способов придать такие рациональные значения, что не уничтожатся сразу коэффициенты каждой из этих функций, а тогда остальной переменной можно дать такое значение, что все функций будут отличны от нуля.

§ 18

Рассмотрим поле

$$\Omega(\alpha, \beta, \gamma, \ldots)$$

Возьмем линейную функций

$$\xi = x\alpha + y\beta + z\gamma + \ldots,$$

где α — корень некоторого уравнения

$$A(x) = 0 \tag{1}$$

из поля Ω, β — корень уравнения

$$B(x) = 0, \tag{2}$$

γ — корень уравнения

$$C(x) = 0 \quad \text{и т.д.} \tag{3}$$

Обозначая через $\alpha_1, \beta_1, \gamma_1, \ldots$ другую комбинацию корней соответственных уравнений, положим

$$\xi_1 = x\alpha_1 + y\beta_1 + z\gamma_1 + \ldots.$$

Составим подобным образом новые выражения $\xi_2, \xi_3, \ldots$ Число таких выражений будет равно произведению степеней функций $A(x), B(x), C(x), \ldots$. Заметим кстати, что нет надобности предполагать все уравнения (1), (2), (3), ... различными.

Разности

$$\xi - \xi_1, \quad \xi - \xi_2, \quad \xi - \xi_3, \quad \ldots$$

суть линейные функций от $x, y, z, \ldots$, причем ни одна из них не равна тождественно нулю, ибо мы, очевидно, предполагаем уравнения (1), (2), (3), ... неприводимыми и, следовательно, не имеющими кратных корней.

По лемме § 15 можно дать $x, y, z, \ldots$ такие рациональные численные значения, чти всевозможные разности, составленные из функций $\xi, \xi_1, \xi_2, \ldots$ будут отличны от нуля, а, следовательно, и все значения $\xi, \xi_1, \xi_2, \ldots$ будут различны между собой.

Обратим теперь внимание, что всякая функция, симметричная относительно корней каждого из уравнений (1), (2), (3), ..., по известной теореме алгебры будет выражаться рационально через коэффициенты этих уравнений. Следовательно, такая величина есть число поля Ω.

К подобным функциям принадлежать, очевидно, коэффициенты полинома

$$F(t) = (t-\xi)(t-\xi_1)(t-\xi_2)\cdots .$$

Уравнение $F(t) = 0$ есть, следовательно, уравнение поля Ω, не имеющее кратных корней. Один из корней этого уравнения есть ξ.

Пусть Θ будет какой нибудь элемент поля

$$\Omega(\alpha, \beta, \gamma, \ldots)$$

и, следовательно, целая функция от корней

$$\alpha, \quad \beta, \quad \gamma, \quad \ldots$$

Обозначим через

$$\Theta_1, \quad \Theta_2, \quad \ldots$$

величины, которые происходят из величины Θ через замену корней

$$\alpha, \quad \beta, \quad \gamma, \quad \ldots$$

новыми комбинациями корней

$$\begin{array}{l} \alpha_1, \quad \beta_1, \quad \gamma_1, \quad \ldots \\ \alpha_2, \quad \beta_2, \quad \gamma_2, \quad \ldots \\ \ldots\ldots\ldots\ldots\ldots \end{array}$$

Рассмотрим функцию

$$F(t)\left[\frac{\Theta}{t-\xi} + \frac{\Theta_1}{t-\xi_1} + \frac{\Theta_2}{t-\xi_2} + \ldots\right].$$

Очевидно, что эта функция есть целая относительно t. Коэффициенты ее суть симметрические функции корней уравнений (1), (2), (3), ..., а потому эта целая функция, которую мы обозначим через $\psi(t)$, принадлежит к полю Ω.

Отсюда мы получаем

$$\frac{\psi(t)}{F(t)} = \frac{\Theta}{t-\xi} + \frac{\Theta_1}{t-\xi_1} + \frac{\Theta_2}{t-\xi_2} + \ldots$$

По теореме Lagrange'a мы знаем, что

$$\Theta = \frac{\psi(\xi)}{F'(\xi)}.$$

Итак, Θ выражается рациональною функциею от ξ с коэффициентами, принадлежащими к полю Ω. Следовательно, всякая величина поля $\Omega(\alpha, \beta, \gamma, \ldots)$ принадлежит полю $\Omega(\xi)$. С другой стороны очевидно, что всякая величина поля $\Omega(\xi)$

есть в тоже время элемент поля $\Omega(\alpha, \beta, \gamma, \ldots)$, ибо ξ выражается рационально через $\alpha, \beta, \gamma, \ldots$.

Итак, мы заключаем о полной тождественности двух полей, что можно выразить равенством

$$\Omega(\xi) = \Omega(\alpha, \beta, \gamma, \ldots).$$

§ 19

Kronecker'у мы обязаны гениальными соображениями, относящимися к трансцендентным присоединениям и находящимися в известной аналоги с теоремой, доказаной в предыдущем параграфе. В знаменитом мемуаре «Grundzge einer arithmetischen Theorie der algebraischen Grössen» Kronecker вводит в рассмотрение рациональные функций от любого числа переменных независимых с коэффициентами, принадлежациими к данному полю. У Kronecker'а получается теория, которая также не зависит от числа присоединенных переменных. Коренное различие состоит в том, что Kronecker пользуется трансцендентным присоединением для изучения свойств основного поля, которое он предполагает алгебраическим. Weber во втором томе своей алгебры дает хорошее изложение теории Kronecker'а, причем называет эту теорию *теорией функционалов*.

§ 20

Поставим вопрос, когда два алгебраических поля изоморфны. Мы будем предполагать у обоих полей основным полем *рациональное поле* Ω.

Пусть одно поле будет $\Omega(\alpha)$; если это поле изоморфно другому Ω_1, то элементу α первого поля должен соответствовать элемент α_1 другого. Рассмотрим неприводимое уравнение

$$a_0\alpha^n + a_1\alpha^{n-1} + \ldots + a_{n-1}\alpha + a_n = 0; \tag{1}$$

очевидно, что на основании принципа изоморфности этому уравнению в другом поле должно соответствовать такое

$$a_0\alpha_1^n + a_1\alpha_1^{n-1} + \ldots + a_{n-1}\alpha_1 + a_n = 0,$$

ибо рациональным числам одного поля должны соответствовать те же самые числа в другом.

Итак, мы получаем

$$\Omega_1 = \Omega(\alpha_1),$$

т. е. алгебраическому полю $\Omega(\alpha)$ соответствует как изоморфное поле $\Omega(\alpha_1)$, где α_1 другой корень того же самого уравнения (1).

§ 21

Присоединяя последовательно корни

$$\alpha, \quad \alpha_1, \quad \alpha_2, \quad \ldots$$

одного и того же неприводимого уравнения, получим ряд полей

$$\Omega(\alpha),\ \ \Omega(\alpha_1),\ \ \Omega(\alpha_2),\ \ldots$$

изоморфных между собой, которая называются *сопряженными* с полем

$$\Omega(\alpha).$$

Если все сопряженные поля тождественны между собой, то поле $\Omega(\alpha)$ носит название *нормальнаго* поля.

§ 22

Итак, мы видели ряд примеров на бесконечные поля. Основными являются три главных поля элементарной алгебры. Затем имеют важное значение поля, получаемый от присоединения новых элементов. Исчерпываются ли этими примерами все мыслимые поля? Ответ на этот вопрос оказывается отрицательным. В последнее время дан пример нового вида поля. Такое поле образуют символы новой природы, введенные в науку K. Hensel'ем под названием *p-адических чисел*. Я считаю необходимым сказать несколько слов об этих числах.

§ 23

Возьмем некоторое простое число p и будем рассматривать системные (десятичные) дроби при системе счисления, имеющей основанием число p. Так, например, системная дробь

$$b_4b_3b_2b_1b_0,\ \ a_1a_2a_3a_4\ldots, \tag{1}$$

где цифры $b_4, b_3, b_2, b_1, b_0, a_1, \ldots$ суть целые числа меньшие p или нули, обозначает как известно сумму

$$b_4p^4 + b_3p^3 + b_2p^2 + b_1p + b_0 + \frac{a_1}{p} + \frac{a_2}{p^2} + \frac{a_3}{p^3} + \ldots$$

Hensel предлагает употреблять под названием p-адических чисел, те же самые символы (1), но только производить над этими числами действия сложения, вычитания, умножения и деления по другим правилам.

Изменение правил простейших действий, указанное Hensel'ем, состоит в том, что разряды, которым соответствуют цифры в обычной арифметике возрастают справа налево. Hensel же предполагает разряды возрастающими слева направо, т. е. как будто бы символ (1) обозначал сумму

$$\frac{b_4}{p^4} + \frac{b_3}{p^3} + \frac{b_2}{p^2} + \frac{b_1}{p} + b_0 + a_1p + a_2p^2 + a_3p^3 + \ldots \tag{2}$$

Таким образом в правиле сложения, если при сложении соответствующих цифр накопляется единица высшего разряда, то ее надо прибавлять к ближайшей цифре *направо*, а не к левой цифре как в арифметике. Подобным же образом при вычитании, если необходимо занять единицу высшего разряда, то ее надо занимать из ближайшей направо стоящей цифры.

Могут возразить, что при бесконечном числе цифр p-адического числа сумма (2) представляет ряд расходящийся и потому не допустима к употреблению. Но дело в том, что мы можем вовсе не отождествлять p-адическое число с суммой (2), а лишь пользоваться видом этой суммы для установления действий над p-адическими числами.

Вообще говоря p-адические числа суть символы, с которыми *не совмещается никакого понятая о величине*, и для которых понятия больше и меньше отпадают.

Глава XV

Теория Lagrange'a

§ 1

С этой главы мы начнем заниматься одною из самых важных задач алгебры, решением уравнений в радикалах.

Умение решать уравнения первой степени относится к временам самой глубокой древности; так например, мы их находим в старой египетской книге Ahmes (1700 г. до Р. Х.). Уравнения второй степени решались уже греческими математиками. Решение этих уравнений в геометрической форме можно видеть в Эвклидовых элементах (300 л. до Р. Х.).

В алгебраической форме уравнения второй степени встречаются в старейшем памятнике греческой алгебры — Диофантовой «Арифметике» (300 л. по Р. Х.). Уравнения третьей и четвертой степени были решены итальянскими математиками XVI столетия: Scipione del Ferro, Tartaglia, Cardano и Ferrari.

Все попытки решить общее уравнение пятой степени остались тщетными. Знаменитый математик Langrange в своем бессмертном мемуаре: «Réflexions sur la résolution algèbrique des équations» (1770) излагает результаты своих попыток в этом направлены. Он поставил себе целью изучить и внимательно рассмотреть все существовавшие до него способы решения уравнений 3-ей и 4-ой степени, для того чтобы сделать догадки относительно решения уравнений высших степеней.

Несмотря на массу новых и важных идей, результат работы Lagrange'a явился неутешительным.

Lagrange обратил внимание на то обстоятельство, что во всех разобранных им приемах решения уравнений 3-ей и 4-ой степени дело сводилось к решению уравнений низших степеней. Lagrange дал прием приведения решения заданного уравнения к решению некоторого нового, вспомогательного уравнения, которое он назвал «équation résolvente».

Это вспомогательное уравнение оказывается 2-ой степени для уравнений 3-ей степени и 3-ей степени для уравнений 4-ой; *для уравнений 5-ой степени оно оказалось 6-ой степени.* Поэтому способ, дававший результат для уравнений 3-ей и 4-ой степеней, переставал быть полезным для уравнений 5-ой степени.

Так как это обстоятельство, повышения степени вспомогательного уравнения, продолжает сохраняться для уравнений всякой степени выше 5-ой, то в одном месте мемуара Lagrange пишет знаменательную фразу, в которой он говорить, что обобщение соображений, касающихся решения уравнений первых 4-х степеней на уравнения высших степеней ему кажется «почти невозможным».

Руководствуясь идеями Lagrange'a, Ruffini[87] и Abel[88] доказали, что *общее уравнение выше четвертой степени, не решается алгебраически, т. е. корни его не могут быть выведены из коэффициентов при помощи следующих алгебраических действий: сложения, вычитания, умножения, деления и извлечения радикалов.*

Различие между уравнениями буквенными и численными

§ 2

Обратим внимание на главнейшие идеи, введенные в науку Lagrange'ем. Прежде всего является существенным, что Lagrange подчеркнул разницу между, так называемыми, *буквенными* уравнениями и *численными*[89].

Уравнение

$$x^n + p_1 x^{n-1} + p_2 x^{n-2} + \ldots + p_n = 0 \tag{1}$$

называется *буквенным*, если все его коэффициенты $p_1, p_2, \ldots, p_n$ представляют из себя буквы, которым не придано никаких особенных численных значений; другими словами, если эти коэффициенты суть независимые переменные. Корни $x_1, x_2, \ldots$, x_n буквенного уравнения можно также рассматривать как независимые переменные, ибо на основании существования равенств

$$\begin{gathered} x_1, x_2, \ldots, x_n = \sum x_1 = -p_1, \\ x_1x_2 + x_1x_3 + \ldots + x_{n-1}x_n = \sum x_1x_2 = p_2, \\ x_1x_2x_3 + \ldots \sum x_1x_2x_3 = -p_3, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ x_1x_2x_3 \cdots x_n = (-1)^n p_n \end{gathered} \tag{2}$$

всякой системе численных значений[90] корней $x_1, x_2, \ldots, x_n$ будет соответствовать некоторая определенная система численных значений коэффициентов $p_1, p_2, \ldots, p_n$. Из соображений главы II мы знаем, что и обратно всякой системе численных значений коэффициентов $p_1, p_2, \ldots, p_n$ соответствует определенная система численных значений корней.

§ 3

Если корни уравнения суть независимые переменные, то между этими корнями могут существовать только такие соотношения.

$$\Omega(x_1, x_2, \ldots, x_n) = 0, \tag{1}$$

[87] Ruffini. Teoria generale delle equazioni in cui si dimostra impossibile la soluzione algebraica delle equazioni generali di grado superiore al quarto. Bologna. (1799).

[88] Abel. Beweis der Unmöglichkeit, algebraische Gleichungen von höheren Graden als dem vierten allgemein aufzulösen. Creles Journ. B. I. (1820).

[89] Д. Граве. Об основных положениях теории Galois. Матом. Сборн. 1914.

[90] Численные значения во всем дальнейшем мы будем рассматривать самого общего вида т. е. и комплексные: $a + bi$

в которых функция Ω тождественно равняется нулю, т. е. при всяких значениях $x_1, x_2, \ldots, x_n$, ибо иначе уравнение (1) определяло бы один из корней как функцию от других. Тождества вида (1) мы будем называть *буквенными* в отличие от тождеств *численных*. Так например, тождество $(x_1+x_2)^2-x_1^2-2x_1x_2-x_2^2=0$ есть буквенное, а тождество $1+2=3$ есть численное.

Буквенные тождества между корнями не нарушают свойства корней оставаться независимыми переменными.

Если мы напишем между корнями соотношение

$$x_1 + x_2 + \ldots + x_n = 0, \tag{2}$$

то, чтобы удовлетворить этому соотношение нельзя считать все корни независимыми переменными, ибо равенство (2) налагает на численные значения корней некоторое ограничение.

Итак, *буквенным* уравнения можно определить как такие, которые не допускают соотношений вида (1) буквенно не тождественных. Если же между корнями существуют не тождественные буквенные соотношения, то уравнение мы будем называть *численным*. Крайним случаем численной определенности численных уравнений являются уравнения, в которых между корнями существует равное степени уравнения число не тождественных буквенных соотношений. Тогда все корни численно определены, а, значить, и коэффициенты уравнения имеют определенные числовые значения.

§ 4

Для придания нашей теории большей определенности возьмем в основу наших рассуждений некоторое поле Ω и будем рассматривать *лишь такие соотношения между корнями*

$$\Pi(x_1, x_2, \ldots, x_n) = \sum a x_1^{\lambda_1} x_2^{\lambda_2} \cdots x_n^{\lambda_n} = 0, \tag{1}$$

где Π *есть целая функция от корней, коэффициенты которой* a *принадлежать полю* Ω.

На основании соображений главы VIII соотношения (1) будут буквенно тождественны лишь в случае равенства нулю всех коэффициентов a.

Рациональные функции от корней

§ 5

Мы займемся в настоящей главе, следуя Lagrange'у, исключительно буквенными уравнениями.

Присоединим к основному полю Ω коэффициенты $p_1, p_2, \ldots, p_n$ буквенного заданного уравнения, получим поле, которое обозначим через $\Omega(p)$ и которое получается, очевидно, от трансцендентного расширения поля Ω, ибо коэффициенты p_i независимые переменные.

Рассмотрим в поле $\Omega(p)$ некоторую *рациональную* функцию

$$\varphi(x_1, x_2, \ldots, x_n),$$

от корней, коэффициенты числителя и знаменателя которой, следовательно, суть или элементы поля Ω или рациональные функции от $p_1, p_2, \ldots, p_n$ с коэффициентами из поля Ω.

§ 6

Будем в заданной рациональной функции $\varphi(x_1, x_2, \ldots, x_n)$ производить *подстановки* (см. глава V) корней $x_1, x_2, \ldots, x_n$ и обратим внимание на тот случай, когда функция не меняется от такой подстановки.

Выражение, что функция не меняется надо понимать здесь в таком смысле; значение функции после подстановки должно быть буквенно тождественным с первоначальным значением. Например, Функция $x_1x_2 + x_3x_4$ не меняется от круговой подстановки корней $(x_1x_3x_2x_4)$.

Мы приходим к очевидной теореме.

Подстановки, не меняющие рациональную функцию, образуют группу.

В самом деле, если каждая из двух подстановок приводит функцию к ее первоначальному виду, то и обе подстановки, произведенная одна за другой, приведут функцию к ее первоначальному виду.

Так например, подстановки, не менякнция функцию $x_1x_2+x_3x_4$ образуют группу восьмого порядка

$$\begin{gathered} 1, \quad (x_1x_2), \quad (x_3x_4), \quad (x_1x_2)(x_3x_4), \quad (x_1x_3)(x_2x_4), \quad (x_1x_4)(x_2x_3), \\ (x_1x_3x_2x_4), \quad (x_1x_4x_2x_3). \end{gathered} \tag{1}$$

Не трудно убедиться, что всякая подстановка, не входящая в эту группу, меняет функцию, так например, подстановка $(x_1x_2x_3)$ обращает функцию $x_1x_2 + x_3x_4$ в $x1x_4 + x_2x_3$.

§ 7

Если функция φ *не меняется* от подстановок группы G, а *меняется* от всякой подстановки, *не* входящей в группу G, то мы будем говорить, что функция *принадлежит группе* G.

При подстановках, не принадлежащих группе G, функция ? может принимать другой вид. Пусть разные значения, принимаемые функцией при всевозможных подстановках, будут

$$\varphi, \quad \varphi_1, \quad \varphi_2, \quad \ldots, \quad \varphi_{k-1}.$$

Эти значения мы будем называть *сопряженными значениями функции* φ.

Если группа G, к которой принадлежит функция, будет состоять из всех $n!$ подстановок, то функция носит название *симметрической*. В главе V мы назвали *симметрическою* также группу всех подстановок. Система сопряженных значений симметрической функции состоит только из одной функции.

Другой крайний случай представляет функция. принадлежащая к *единичной* группе, т. е. к группе, состоящей из единственной тождественной подстановки. Такая функция меняется при всех подстановках и мы ее во всем дальнейшем будем называть *функцией Galois*.

Функция Galois имеет очевидно $n!$ сопряженных значений.

Примером функций Galois может служить линейное выражение

$$\alpha_1 x_1 + \alpha_2 x_2 + \ldots + \alpha_n x_n,$$

в котором коэффициенты $\alpha_1, \alpha_2, \ldots, \alpha_n$ различные между собой числа.

§ 8

На всяком частном примере нетрудно составить сопряженные значения функций. Так, например, функция $x_1x_2 + x_3x_4$ дает место трем значениям

$$x_1x_2 + x_3x_4, \quad x_1x_3 + x_2x_4, \quad x_1x_4 + x_2x_3.$$

§ 9

Мы теперь проследим внимательно связь свойств рациональных функций по отношению к подстановкам независимых переменных с теорией групп подстановок. Таким образом мы придем к новому выводу предложений, с которыми мы познакомились еще в главе V.

Итак, возьмем функцию φ, принадлежащую к группе

$$G = \{S_1 = 1,\ S_2,\ S_3,\ \ldots,\ S_m\} \tag{1}$$

порядка m. Пусть эта функция при помощи некоторой подстановки T_1, не входящей в группу G, переходит в другое значение φ_1. Посмотрим, не существует ли других подстановок, кроме подстановки T_1, переводящих функцию φ в функцию φ_1.

Нетрудно убедиться, что таковыми будут все следующие подстановки

$$S_1T_1 = T_1, \quad S_2T_1, \quad S_3T_1, \ \ldots, \ S_mT_1. \tag{2}$$

Эти подстановки, очевидно, различны между собой, ибо равенство $S_kT_1 = S_lT_1$ влекло бы за собой $S_k = S_l$, что невозможно ибо мы предполагаем, что подстановки (1) все различны.

Нетрудно убедиться, что кроме подстановок (2) не существует подстановок, переводящих φ в φ_1.

В самом деле, пусть будет Σ какая нибудь подстановка, переводящая φ в φ_1; тогда, очевидно, произведение подстановок ΣT_1^{-1} оставляет без перемены функцию φ, ибо Σ переводит φ в φ_1, а T_1^{-1} переводит обратно φ_1 в φ. Так как, с другой стороны, не существует по предположеию других подстановок, не меняющих функции φ, кроме подстановок группы G, то будем иметь

$$\Sigma T_1^{-1} = S_i, \quad \text{или} \quad \Sigma = S_iT_1,$$

т. е. подстановка Σ входит в состав системы (2).

Будем систему (2) обозначать символом

$$GT_1$$

и называть *системой сопряженною с группой G и относящейся к значению φ_1*.

Если системами подстановок G и GT_1 не исчерпываются все $N = n!$ подстановок, то должно существовать по крайней мере еще одно значение функции φ_2, которое функция принимает при подстановках сопряженной системы GT_2:

$$S_1T_2 = T_2, \quad S_2T_2, S_3T_2, \ldots, \ S_mT_2, \tag{3}$$

очевидно, что подстановки (3) все различны между собой и различны от подстановок (1) и (2).

Продолжая наше рассуждение далее, мы замечаем, что, если через k обозначить число различных значений

$$\varphi, \quad \varphi_1, \quad \varphi_2, \ \ldots, \ \varphi_{k-1}.$$

принимаемых функцией φ, то все N подстановок симметрической группы должны разбиться на k сопряженных систем

$$G, \quad GT_1, \quad GT_2, \ \ldots, \ GT_{k-1}. \tag{4}$$

Из этих систем образует группу только первая G; остальные системы, очевидно, не группы, ибо в них нет единичной подстановки, которая входит только в группу G.

Присоединяясь к терминологии § 31 главы V, получаем теорему.

Число сопряженных значений функции φ, принадлежащей группе G, равно индексу этой группы G по отношению ко всей симметрической группе.

§ 10

Соображения предыдущего параграфа важны в том отношений, что они привели к более общей теореме § 28 главы V и распространяются на теорию каких угодно групп.

Возьмем произвольную группу H каких угодно предметов (не обязательно подстановок). Если некоторые из этих элементов образуют новую группу G, то, как нам уже известно, эта группа G называется *делителем* группы H, или *подгруппой* H.

Приходим к теореме.

Порядок k подгруппы G конечной группы H есть делитель (в арифметическом смысле слова] порядка K группы H.

Доказательство может быть проведено совершенно аналогично с тем, что мы видели в § 28 главы V.

Мы можем группу H разложить на сопряженные системы

$$\begin{aligned} &1, \quad A_2, \quad A_3, \ \ldots, \ A_k, \\ &B_1, \quad A_2B_1, \quad A_3B_1, \ \ldots, \ A_kB_1, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ &B_{q-1}, \quad A_2B_{q-1}, \quad A_3B_{q-1}, \ \ldots, \ A_kB_{q-1}, \end{aligned} \tag{1}$$

из которых первая есть подгруппа G. Разложение (1) мы будем называть *разложением группы H на сопряженные системы по подгруппе G* и обозначать символически

$$H = G + GB_1 + GB_2 + \ldots + GB_{q-1};$$

получаем, очевидно,

$$K = kq,$$

откуда н следует справедливость вышеприведенной теоремы.

§ 11

Подобным же образом можно было бы найти элементы ?, умножением на которые слева получим разложение группы ? на сопряженные системы

$$\begin{aligned}
&1, \quad A_2, \quad A_3, \ \ldots, \ A_k,\\
&C_1, \quad C_1A_2, \quad C_1A_3, \ \ldots, \ C_1A_k,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\
&C_{q-1}, \quad C_{q-1}A_2, \quad C_{q-1}A_3, \ \ldots, \ C_{q-1}A_k,
\end{aligned}$$

что можно указать символического формулой

$$H = G + C_1G + C_2G + \ldots + C_{q-1}G.$$

Если найдены элементы $1, B_1, B_2, \ldots, B_{q-1}$, дающие равенство

$$H = G + GB_1 + GB_2 + \ldots + GB_{q-1},$$

то, очевидно, что за элементы $1, C_1, C_2, \ldots, C_{q-1}$ можно будет принять элементы $1, B_1^{-1}, B_2^{-1}, \ldots, B_{q-1}^{-1}$ и получить

$$H = G + B_1^{-1}G + B_2^{-1}G + \ldots + B_{q-1}^{-1}G.$$

Справедливость последнего соображения следует из того, что замена элементов группы их обратными дает ту же труппу.

§ 12

Возвращаемся теперь к сопряженным значениям $\varphi, \varphi_1, \ldots, \varphi_{k-1}$ функции φ, принадлежащей к группе подстановок G.

Очевидно, что, если мы во всех функциях ряда

$$\varphi, \quad \varphi_1, \quad \varphi_2, \ \ldots, \ \varphi_{k-1} \tag{1}$$

произведем некоторую подстановку S корней, то в этих функциях ряда (1) произойдет некоторая перестановка этих функций; потому что функциями ряда (1) исчерпываются, с одной стороны, все возможные значения функций φ, принимаемые ею при различных подстановках корней, с другой стороны, две различные из числа функций φ_i не могут обратиться в одну и ту же функцию, ибо тогда обратная подстановка из одной функций делала бы две различные, что невозможно. Итак, всякая подстановка S, перемещающая n корней $x_1, x_2, \ldots, x_n$, сопровождается в тоже самое время некоторой подстановкой сопряженных значений (1) функции φ.

§ 13

То обстоятельство, что подстановка корней производить подстановку сопряженных значений функции наводит нас на мысль о существовании такой теоремы, относящейся к теории каких угодно конечных форм.

Умножением справа на произвольный элемент B группы H сопряженных систем

$$G,\ \ GB_1,\ \ GB_2, \ldots,\ GB_{q-1} \tag{1}$$

осуществляет некоторая подстановка этих систем, т. е. системы

$$GB,\ \ GB_1B,\ \ GB_2B, \ldots,\ GB_{q-1}B$$

представляют из себя те же системы, что и (1)*, только, быть может, в другом порядке.*

Совершенно подобным образом умножением слева на произвольный элемент C группы H ряда сопряженных систем

$$G,\ \ C_1G,\ \ C_2G,\ \ldots,\ C_{q-1}G$$

достигается некоторая подстановка в этих системах.

§ 14

Покажем, что сопряженный $\varphi, \varphi_1, \ldots, \varphi_{k-1}$ значения суть корни уравнения степени k с коэффициентами из поля $\Omega(p)$.

В самом деле, составим уравнение

$$(y-\varphi)(y-\varphi_1)\cdots(y-\varphi_{k-1}) = 0, \tag{1}$$

которое можно будет переписать в таком виде

$$y^k + P_1y^{k-1} + P_2y^{k-2} + \ldots + P_k = 0. \tag{2}$$

Коэффициенты $P_1, P_2, \ldots, P_k$, будучи симметрическими функциями от $\varphi, \varphi_1, \ldots, \varphi_{k-1}$, будут в тоже время симметрическими функциями от $x_1, x_2, \ldots, x_n$, ибо всякая подстановка корней $x_1, x_2, \ldots, x_n$ сопровождается подстановкой величин $\varphi, \varphi_1, \ldots, \varphi_{k-1}$, следовательно, коэффициенты $P_1, P_2, \ldots, P_k$ не меняются; итак, на основании теоремы § 8 главы IX, коэффициенты P_i уравнения (2) выражаются рационально через коэффициенты p_i первоначального уравнения и коэффициенты функции φ. Другими словами, коэффициенты P_i принадлежать полю $\Omega(p)$.

§ 15

Покажем на примере функции $\varphi = x_1x_2 + x_3x_4$, как составить уравнение (2) § 14.

Пусть задано основное уравнение 4-ой степени

$$x^4 + p_1x^3 + p_2x^2 + p_3x + p_4 = 0,$$

корни которого будут $x_1, x_2, x_3.x_4$. Коэффициенты нашего уравнения p_1, p_2, p_3, p_4 будем считать величинами известными, ибо эти величины будут элементами поля $\Omega(p)$.

Мы имеем

$$\begin{aligned} p_1 &= -x_1 - x_2 - x_3 - x_4, \\ p_2 &= x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4, \\ p_3 &= -x_1x_2x_3 - x_1x_2x_4 - x_1x_3x_4 - x_2x_3x_4, \\ p_4 &= x_1x_2x_3x_4. \end{aligned}$$

В данном случае $k = 3$, ибо

$$\varphi = x_1x_2 + x_3x_4, \qquad \varphi_1 = x_1x_3 + x_2x_4, \qquad \varphi_2 = x_1x_4 + x_2x_3. \tag{1}$$

Требуемое уравнение (2) § 14 будет иметь вид

$$y^3 + P_1y^2 + P - 2y + P_3 = 0,$$

где

$$P_1 = -\varphi - \varphi_1 - \varphi_2, \qquad P_2 = \varphi\varphi_1 + \varphi\varphi_2 + \varphi_1\varphi_2, \qquad P_3 = -\varphi\varphi_1\varphi_2.$$

Покажем теперь, что, как и следует из общей теории, можно будет выразить коэффициенты P_1, P_2, P_3 через величины известные p_1, p_2, p_3, p_4.

В самом деле, после простых выкладок

$$\begin{gathered} P_1 = -\varphi - \varphi_1 - \varphi_2 = -x_1x_2 - x_3x_4 - x_1x_3 - x_2x_4 - x_1x_4 - x_2x_3 = -p_2, \\ P_2 = \varphi\varphi_1 + \varphi\varphi_2 + \varphi_1\varphi_2 = (x_1x_2 + x_3x_4)(x_1x_3 + x_2x_4) + \\ (x_1x_2 + x_3x_4)(x_1x_4 + x_2x_3) + (x_1x_3 + x_2x_4)(x_1x_4 + x_2x_3) = p_1p_3 - 4p_4, \\ P_3 = \varphi\varphi_1\varphi_2 = p_4p_1^2 - 4p_4p_2 + p_3^2. \end{gathered}$$

Итак, мы получаем окончательно уравнение

$$y^3 - p_2y^2 + (p_1p_3 - 4p_4)y + p_1^2p_4 + -4p_2p_4 + p_3^2 = 0, \tag{2}$$

которому удовлетворяет функция $y = x_1x_2 + x_3x_4$.

§ 16

Теорема. *Если функция ψ не меняется от всех подстановок группы G, которой принадлежит функция φ, то функция ψ выражается рационально через функций φ.*

Пусть сопряженные значения функции φ будут

$$\varphi, \quad \varphi_1, \quad \varphi_2, \ \ldots, \ \varphi_{k-1} \tag{1}$$

и положим, что этим значениям соответствуют подстановки сопряженных систем

$$G, \quad GT_1, \quad GT_2, \ldots, \ GT_{k-1}. \tag{2}$$

Все подстановки системы GT_i обращают, очевидно, функцию ψ в одну и туже ψ_1, ибо подстановка из группы G не меняет по предположению функции ψ и

остается подстановка T_i, которая дает значение ψ_i. Применяя к функции ψ подстановки ряда систем (2), получим ряд функций

$$\psi, \quad \psi_1, \quad \psi_2, \ \ldots, \ \psi_{k-1}. \tag{3}$$

Все функции ряда (3) будут различны между собой, если функция ψ принадлежит к той же группе G, что и φ. Если функций ряда (3) не все различны, то функция ψ будет принадлежать к более обширной группе, в которую группа G входит как подгруппа.

Для доказательства нашей теоремы совершенно безразлично, одинаковы или различны значения (3).

Для нас существенно важно только, что различны функции φ_i, ибо функция φ принадлежит как раз группе G.

Умножением систем (2) справа на подстановку Σ достигается некоторая подстановка этих систем, то, следовательно. применение подстановки Σ к корням $x_1, x_2, \ldots, x_n$, от которых зависят рациональные функции (1) и (3), производит одну и туже подстановку, как в ряде функций (1), так и в ряде функций (3).

Рассмотрим теперь такую сумму дробей

$$\frac{\psi}{t-\varphi} + \frac{\psi_1}{t-\varphi_1} + \ldots + \frac{\psi_{k-1}}{t-\varphi_{k-1}}, \tag{4}$$

где t новая независимая переменная. Эта сумма дробей есть некоторая функция от независимой переменной t и от корней $x_1, x_2, \ldots, x_n$, которые входят в функции φ_i и ψ_i. Очевидно, что это есть функция симметрическая от корней $x_1, x_2, \ldots, x_n$, ибо при любой подстановке Σ корней функции φ и ψ одинаково перемещаются, так что в сумме (4) перемещаются слагаемые дроби, а сумма их не меняется.

Если мы сумму (4) представим в виде одной дроби, то эта дробь будет иметь вид

$$\frac{F(t)}{\Omega_0(t)},$$

где $\Omega_0(t) = (t-\varphi)(t-\varphi_1)\cdots(t-\varphi_{k-1})$, а числитель $F(t)$ будет целой функцией степени $k-1$ от t. На оснований теоремы, относящейся к симметрическим функциям, заключающим произвольный параметр мы заключаем, что все коэффициенты целых функций $F(t)$ и $\Omega_0(t)$ суть элементы поля $\Omega(p)$, ибо они суть симметрические функций корней. Итак, мы имеем тождество

$$\frac{F(t)}{\Omega_0(t)} = \frac{\psi}{t-\varphi} + \frac{\psi_1}{t-\varphi_1} + \ldots$$

На основании теоремы Lagrange'а получаем

$$\psi = \frac{F(\varphi)}{\Omega_0'(\varphi)} \tag{5}$$

и теорема доказана.

Оказывается, что ψ выражается в поле $\Omega(p)$ рационально через φ. Для возможности применения формулы (5) необходимо, чтобы функция $\Omega_0(t)$ не имела кратных корней, ибо если φ будет кратным корнем функции $\Omega_0(t)$, то $\Omega_0'(\varphi) = 0$

и формула (5) перестает иметь место. Поэтому было необходимо предположение, что φ принадлежит группе G.

Как очевидное следствие вытекает такая теорема.

Если две функций принадлежите к одной и той же группе, то каждая функция выражается рационально через другую.

§ 17

Поясним приведенную теорию примером.

Функции

$$\varphi = x_1x_2 + x_3x_4, \qquad \psi = x_1^3x_2^3 + x_3^3x_4^3$$

принадлежать, очевидно, к одной и той же группе; значит, они должны выражаться одна через другую. Выразить ψ через φ проще; в самом деле, возвышая функцию φ в куб, получим

$$\varphi^3 = \psi + 3(x_1^2x_2^2x_3x_4 + x_1x_2x_3^2x_4^2) = \psi + 3p_4\varphi,$$

откуда окончательно

$$\psi = \varphi^3 - 3p_4\varphi. \tag{1}$$

Чтобы выразить обратно φ через ψ, поступим так: на основании уравнения (2) § 15 можно будет формулу (1) переписать так

$$\psi = p_2\varphi 629p_4 - p_1p_3)\varphi + p_1^2p_4 - 4p_2p_4 + p_3^2, \tag{2}$$

умножая обе части последнего уравнения (2) на φ и пользуясь уравнением (2) § 15, получим

$$\begin{gathered}\psi\varphi = \varphi^2(p_2^2 - p_1p_3 + p_4) + \varphi(p_1^2p_4 + p_3^2 - p_1p_2p_3) + \\ + p_1^2p_2p_4 + p_2p_3^2 - 4p_2^2p_4.\end{gathered} \tag{3}$$

Рассматривая уравнения (2) и (3) как уравнения первой степени относительно φ и φ^2, получим для φ такое выражение

$$\varphi = \frac{A + B\psi}{C + D\psi},$$

где

$$\begin{aligned}A &= p_1^3p_3p_4 - p_1^2p_4^2 - p_1p_2p_3p_4 + 4p_2p_4^2 + p_1p_3^2 - p_3^2p_4,\\ B &= p_2^2 - p_1p_3 + p_4,\\ C &= p_2^2p_4 - 2p_1p_3p_4 + p_4^2 + p_1^2p_3^2 - p_1^2p_2p_4 - p_2p_3^2,\\ D &= p_2.\end{aligned}$$

§ 18

Теорема. *Функция ψ, принадлежащая к подгруппе G группы H, к которой принадлежит функция φ, есть корень алгебраического уравнения, коэффициенты*

которого выражаются рационально через функцию φ, и степень которого равна индексу подгруппы G. Функция же φ выражается рационально через ψ.

Последнее утверждение теоремы о томе, что функция φ выражается рационально через ψ следует непосредственно из теоремы § 16, ибо φ не меняется от всех подстановок группы функции ψ.

Покажем теперь справедливость первой части теоремы. Разложим группу H на сопряженные системы при помощи подгруппы G. Пусть эти системы будут

$$G,\ \ GS_1,\ \ GS_2,\ \ldots,\ GS_{q-1}, \tag{1}$$

где q есть индекс подгруппы G. Этим системам соответствуют различные значения ψ. Обозначим эти значения так

$$\psi,\ \ \psi_1,\ \ \psi_2,\ \ldots,\ \psi_{q-1}.$$

Эти все значения различны между собой, ибо мы предположили, что функция ψ принадлежит как раз подгрупп G. Что касается функции φ, то она не меняется от всех подстановок, входящих во все системы (1), ибо совокупность этих систем и есть группа H функций φ. Рассмотрим функцию

$$(t-\psi)(t-\psi_1)\cdots(t-\psi_{q-1}) = t^q + Q_1 t^{q-1} + \ldots + Q_q,$$

где t есть новая независимая переменная, а $Q_1, Q_2, \ldots, Q_q$ симметрические функции от величин $\psi, \psi_1, \ldots, \psi_{q-1}$. Очевидно, что всякий из коэффициентов Q_i не меняется от всех подстановок группы H, ибо всякая подстановка этой группы влечет за собой лишь перестановку величин $\psi, \psi_1, \ldots, \psi_{q-1}$; поэтому на основании теоремы § 16 мы можем утверждать, что Q_i выражается рационально через φ, что и требовалось доказать.

§ 19

Обращаемся теперь к рассмотрений групп, к которым принадлежат сопряженные значения функции.

Возьмем функцию φ, принадлежащую группе G, тогда, как мы видели уже, ее сопряженные значения

$$\varphi,\ \ \varphi_1,\ \ \varphi_2,\ \ldots,\ \varphi_{q-1}$$

соответствуют сопряженным системам

$$G,\ \ GT_1,\ \ GT_2,\ \ldots,\ GT_{q-1}!$$

Посмотрим теперь, какие подстановки не меняют значение φ_i. Очевидно, что всякая подстановка вида

$$T_i^{-1} S T_i, \tag{1}$$

где S подстановка из группы G, не будет менять φ_i. В самом деле, подстановка T_i^{-1} переводит φ_i в φ, подстановка S не меняет φ и, наконец, подстановка T_i переводить φ обратно в φ_i.

Покажем, что и, обратно, всякая подстановка Σ, не меняющая функции φ_i будет иметь вид (1). В самом деле, подстановка

$$T_i \Sigma T_i^{-1}$$

очевидно не меняет функции φ, а потому она должна совпадать с некоторою подстановкой S группы G

$$T_i \Sigma T_i^{-1} = S,$$

откуда окончательно

$$\Sigma = T_i^{-1} S T_i,$$

что и требовалось доказать.

Итак, мы видим, что *группа функции φ_i будет не что иное как преобразование*

$$T_i^{-1} G T_i$$

группы G при помощи подстановки T_i.

Мы просим читателя еще раз внимательно просмотреть §§ 18, 19, 20, 42, 43, 44, 45, 46, 47 главы V; теперь мы можем яснее себе представить происхождение изложенных там теорем.

Так как функция φ_i есть, можно сказать, та же функция, что и φ, только переменные независимые имеют другие обозначения, так сказать, другие названия; то очевидно, что группа $T_i^{-1} G T_i$ должна быть совершенно изоморфна с группой G.

Теперь нам делается совершенно ясным, почему преобразование $T_i^{-1} S T_i$ подстановки S совершается при помощи замены обозначения элементов в циклах подстановки S при помощи подстановки T_i.

§ 20

Итак, если G есть *нормальный* делитель симметрической группы, то все преобразования

$$T_1^{-1} G T_1, \quad T_2^{-1} G T_2, \ \ldots, \ T_{k-1}^{-1} G T_{k-1}$$

совпадают с группой G, значит, все сопряженные значения

$$\varphi, \quad \varphi_1, \quad \varphi_2, \ \ldots, \ \varphi_{k-1} \tag{1}$$

принадлежат к одной и той же группе G. На оснований теоремы § 16 мы получаем в этом случае, что все значения (1) суть рациональные функции от одного из них, например, φ:

$$\varphi_1 = \theta_1(\varphi), \quad \varphi_2 = \theta_2(\varphi), \ \ldots, \ \varphi_{k-1} = \theta_{k-1}(\varphi). \tag{2}$$

Мы будем называть *нормальным* уравнение

$$t^k + P_1 t^{k-1} + \ldots + P_k = 0, \tag{3}$$

которому удовлетворяют величины (1), если имеют место равенства (2), то есть, все они выражаются рационально через одну.

§ 21

Поясним вышеизложенную теорию на примере общего уравнения 4-ой степени. Интересно, что, показывая на уравнении 4-ой степени приложение изложенных теорем, мы систематически придем в полному решению уравнений 4-ой степени.

Начнем с рассмотрения двух функции

$$\varphi = x_1x_2 + x_3x_4, \qquad \psi = (x_1 - x_3)(x_2 - x_4).$$

Первую функцию мы уже рассматривали в § 15.

Что касается до функции ψ, то мы замечаем, что она принадлежит группе (Vierergruppe) подстановок

$$1, \quad (x_1x_2)(x_3x_4), \quad (x_1x_3)(x_2x_4), \quad (x_1x_4)(x_2x_3),$$

которая входит делителем в группу (1) § 6 функции φ; так как индекс этой подгруппы равен $\frac{8}{4} = 2$, то будут существовать два сопряженных значения функции при восьми подстановках группы (1) § 6. Эти значения будут

$$\psi = (x_1 - x_3)(x_2 - x_4), \qquad \psi_1 = (x_2 - x_3)(x_1 - x_4).$$

Если мы введем обозначения § 15, то можно будет написать

$$\psi = \varphi - \varphi_2, \qquad \psi_1 = \varphi - \varphi_1.$$

Если мы рассмотрим функцию

$$(t - \psi)(t - \psi_1) = t^2 + Q_1t + Q_2,$$

то надо будет показать, как выразить Q_1 и Q_2 рационально через φ.

Мы имеем

$$\begin{aligned} Q_1 &= -\psi - \psi_1 = -(\varphi - \varphi_2) - (\varphi - \varphi_1) = -3\varphi + (\varphi + \varphi_1 + \varphi_2) = \\ &= -3\varphi - P_1 = -3\varphi + p_2, \\ Q_2 &= \psi\psi_1 = (\varphi - \varphi_2)(\varphi - \varphi_1) = \Omega_0'(\varphi), \end{aligned}$$

где

$$\Omega_0(t) = (t - \varphi)(t - \varphi_1)(t - \varphi_2) = t^3 + P_1t^2 + P_2t + P_3$$

и, следовательно, получаем

$$Q_2 = 3\varphi^2 + 2p_1\varphi + P_2 = 3\varphi^2 - 2p_2\varphi + p_1p_3 - 4p_4.$$

§ 22

Рассмотрим общую симметрическую группу 4-х независимых переменных x_1, x_2, x_3, x_4. Для сокращения мы будем писать только индексы $1, 2, 3, 4$.

Напишем таблицу всех 24 перемещений 4-х индексов:

1234	2134	3124	4123
1243	2143	3142	4132
1324	2314	3214	4213
1342	2341	3241	4231
1423	2413	3412	4312
1432	2431	3421	4321

,

мы получим все 24 подстановки симметрической группы, если укажем переход от первоначального перемещения ко всякому другому.

Эти подстановки будут

(1)

1	(12)	(132)	(1432)
(34)	(12)(34)	(1342)	(142)
(23)	(123)	(13)	(143)
(234)	(1234)	(134)	(14)
(243)	(1243)	(13)(24)	(1423)
(24)	(124)	(1324)	(14)(23)

.

Вследствие существования формулы

$$(1234\cdots n) = (12)(13)\cdots(1n)$$

мы заключаем, что в знакопеременную группу одиночные циклы могут входить только в том случае, если они состоят из нечетного числа элементов. Знакопеременная группа (см. стр. 152) будет состоять из следующих 12 подстановок

(2)
$$1,\ (12)(34),\ (13)(42),\ (14)(23)$$
$$(123),\ (132),\ (124),\ (142),\ (134),\ (143),\ (234),\ (243).$$

Эта группа имеет нормальным делителем Vierergruppe

(3)
$$1,\quad (12)(34),\quad (13)(24),\quad (14)(23).$$

В самом деле, преобразование всякой подстановки вида $(\alpha\beta)(\gamma\delta)$ будет иметь тот же вид $(\alpha_1\beta_1)(\gamma_1\delta_1)$.

Наконец, мы можем указать группу, состоящую из двух подстановок

(4)
$$1,\quad (12)(34),$$

которая будет, очевидно, нормальным делителем группы (3).

§ 23

В связи с указанными в § 22 подгруппами можно будет поступить так. Рассмотрим функции корней уравнения 4-ой степени, принадлежащая группам (1), (2), (3), (4). Изучение связи между этими функциями приведет нас к полному алгебраическому решению буквенного уравнения 4-ой степени.

О функциях, принадлежащих к симметрической группе (1) говорить не стоить, ибо симметрические функции мы считаем величинами известными. Функция,

принадлежащая к знакопеременной группе (2), будет корнем квадратного уравнения с известными коэффициентами.

Проще всего взять знакопеременную функцию

$$\tau = (x_1 - x_2)(x_1 - x_3)(x_1 - x_4)(x_2 - x_3)(x_2 - x_4)(x_3 - x_4).$$

Эта функция, очевидно, удовлетворяет квадратному уравнению

$$\tau^2 = D,$$

где D — дискриминант данного уравнения

$$x^4 + p_1x^3 + p_2x^2 + p_3x = p_4 = 0.$$

В § 31 Главы IX мы видели, что

$$27D = 4A^3 - B^2,$$

где

$$\begin{aligned} A &= p_2^2 - 3p_1p_3 + 12p_4, \\ B &= 27p_1^2p_4 + 27p_3^2 + 2p_2^3 - 72p_2p_4 - 9p_1p_2p_3. \end{aligned}$$

Мы видели уже в § 21 пример функции, принадлежащей к Vierergruppe (3), а именно

$$\psi = (x_1 - x_3)(x_2 - x_4).$$

Так как Vierergruppe имеет индекс 3 относительно знакопеременной, то функция должна быть корнем кубического уравнения, коэффициенты которого должны выражаться рационально через функцию τ, принадлежащую знакопеременной группе.

Разлагая знакопеременную группу на сопряженные системы по Vierergruppe V, получим

$$\begin{aligned} V &= 1,\ (12)(34),\ (13)(24),\ (14)(23) \\ V(123) &= (123),\ (134),\ (243),\ (142), \\ V(132) &= (132),\ (234),\ (124),\ (143). \end{aligned}$$

Этим системам соответствуют значения

$$\begin{aligned} \psi &= (x_1 - x_3)(x_2 - x_4) = \varphi - \varphi_2, \\ \psi_1 &= (x_2 - x_1)(x_3 - x_4) = \varphi_2 - \varphi_1, \\ \psi_2 &= (x_3 - x_2)(x_1 - x_4) = \varphi_1 - \varphi, \end{aligned} \tag{1}$$

где φ, φ_1, φ_2 обозначеюя § 15.

Функция ψ есть корень кубического уравнения, коэффициенты которого вычисляются следующим образом

$$\begin{aligned} \psi + \psi_1 + \psi_2 &= 0, \\ \psi\psi_1 + \psi\psi_2 + \psi_1\psi_2 &= -(\varphi^2 + \varphi_1^2 + \varphi_2^2) + (\varphi\varphi_1 + \varphi\varphi_2 + \varphi_1\varphi_2), \\ \psi\psi_1\psi_2 &= \tau. \end{aligned}$$

Далее, придерживаясь обозначений § 15, получим

$$\varphi^2 + \varphi_1^2 + \varphi_2^2 = P_1^2 - 2P_2 = p_2^2 - 2(p_1p_3 - 4p_4),$$
$$\varphi\varphi_1 + \varphi\varphi_2 + \varphi_1\varphi_2 = P_2 = p_1p_3 - 4p_4,$$

следовательно,

$$\psi\psi_1 + \psi\psi - 2 + \psi_1\psi_2 = -p_2^2 + 3(p_1p_3 - 4p_4) = -A.$$

Итак, кубическое уравнение, которому удовлетворяет функция ψ, имеет вид

$$\psi^3 - A\psi - \tau = 0. \tag{2}$$

Переходим теперь к функции ω, принадлежащей к группе (4). За такую функцию можно взять

$$\omega = x_1 - x_3 + x_2 - x_4.$$

Так как группа (4) имеет индекс 2 относительно группы (3), то ω должна удовлетворять квадратному уравнению, коэффициенты которого выражаются рационально через ψ. Раскладывая Vierergruppe на сопряженные системы по отношений к группе (4) получим

$$1, \quad (12)(34); \quad (13)(24), \quad (14)(23.$$

Этим системам соответствуют два сопряженные значения функции ?

$$\omega = x_1 - x_3 + x_2 - x_4, \qquad \omega_1 = x_3 - x_1 + x_4 - x_2 = -\omega.$$

Функция ω удовлетворяет квадратному уравнению

$$\omega^2 - k = 0, \tag{3}$$

где

$$k = (x_1 - x_3 + x_2 - x_4)^2 = x_1^2 + x_2^2 + x_3^2 + x_4^2 + 2\varphi - 2\varphi_1 - 2\varphi_2 =$$
$$= p_1^2 - 2p_2 - 2p_2 + 4\varphi = p_1^2 - 4p_2 + 2\varphi,$$

но из уравнений (1), получаем

$$\psi - \psi_1 = 2\varphi - \varphi_1 - \varphi_2 = 3\varphi - p_2,$$

откуда

$$\varphi = \frac{1}{3}(p_2 + \psi - \psi_2).$$

Итак уравнение (3) принимает окончательно вид

$$\omega^2 - p_1 + \frac{8}{3}p_2 + \frac{4}{3}(\psi_2 - \psi) = 0.$$

После того как найдена функция ω, можно будет окончательно найти все 4 корня заданного уравнения при помощи квадратных уравнений. В самом деле, мы имеем

$$\omega = x_1 - x_3 + x_2 - x_4 = p_1 + 2(x_1 + x_2) = -p_1 - 2(x_3 + x_4).$$

Значит,

$$x_1 + x_2 = \frac{\omega - p_1}{2}, \qquad x_3 + x_4 = \frac{-\omega - p_2}{2}.$$

Но произведения x_1x_2 и x_3x_4 суть корни квадратного уравнения вида

$$\xi^2 - \varphi\xi + p_4 = 0,$$

или

$$\xi^2 - \frac{1}{3}(p_2 + \psi - \psi_2)\xi + p_4 = 0. \tag{4}$$

Корни x_1 и x_2 найдутся при помощи квадратного уравнения, ибо известны сумма их $x_1 + x_2$ и произведение x_1x_2. Подобным же образом найдем x_3 и x_4 при помощи квадратного уравнения. Итак, последовательное рассмотрение функций τ, ψ, ω, ξ приводит нас к полному решению в радикалах уравнения 4-ой степени. Это решение сводится к цепи уравнений

$$\tau^2 = D, \qquad \psi^3 - A\psi - \tau = 0, \qquad \omega^2 - p_1^2 + \frac{8}{3}p_2 + \frac{4}{3}(\psi_2 - \psi) = 0$$

$$\xi^2 - \frac{1}{3}(p_3 + \psi - \psi_2)\xi + p_4 = 0$$

и наконец

$$x^2 + \frac{p_1 - \omega}{2}x + \xi_1 = 0, \qquad x^2 + \frac{p_1 + \omega}{2}x + \xi_2 = 0,$$

где ξ_1 и ξ_2 суть корни уравнения (4).

§ 24

Изложенный в предыдущем параграфе способ решения уравнения 4-ой степени наводит нас на дальнейшие весьма важные рассуждения.

В § 13 главы III мы видели самый простой способ решения буквенного уравнения 4-ой степени. Если мы припомним, что по этому способу решение приводится к решению уравнения 3-ей степени, то, принимая во внимание формулы Cardano, мы замечаем, что радикальное выражение является 4-х этажным, причем трем этажам соответствуют квадратные радикалы, а одному — кубические. Этот вид может быть указан схематически так

$$\sqrt{\cdots\sqrt{\cdots\sqrt[3]{\cdots\sqrt{\cdots}}}}.$$

Полученное нами в предыдущем параграфе решение кажется нам уклоняющимся от указанной схемы. Во первых, можно подумать, что под корнем кубическим должно быть 2 квадратных радикала: один $\sqrt{D}$, а другой вводимый формулами Cardano. С другой стороны можно подумать, что над корнем кубическим должны быть 3 этажа квадратных радикалов. Нетрудно, однако, убедиться, что квадратный радикал соответствующий формулами Cardano пропадает, ибо кубическое уравнение ψ имеет особенный вид; с другой стороны, один из верхних квадратных радикалов пропадает вследствие того, что квадратное уравнение для ξ имеет корни, рационально выражающиеся через ω.

§ 25

Остановимся сначала на втором замечании, что корни $\xi_1 = x_1x_2$, $\xi_2 = x_3x_4$ квадратного уравнения (4) § 23 выражаются рационально через функцию ω. На основании рассмотрения групп это очевидно, ибо ξ_1 и ξ_2 не меняются от группы $1, (12)(34)$ функции ω. Но нетрудно убедиться к этом и на самом деле при помощи вычисления

$$\begin{gathered}(x_1x_2 - x_3x_4)\omega = (x_1x_2 - x_3x_4)(x_1 - x_3 + x_2 - x_4) = \\ = p_3 + x_1x_2(x_1 + x_2) + x_3x_4(x_3 + x_4) - p_1\varphi = \\ = (x_1x_2 + x_3x_4)(x_1 + x_2 + x_3 + x_4) = \\ = -p_3 + x_1x_2(x_1 + x_2) + x_3x_4(x_3 + x_4);\end{gathered}$$

отсюда

$$x_1x_2 - x_3x_4 = \frac{2p_3 - p_1\varphi}{\omega},$$

кроме того,

$$x_1x_2 + x_3x_4 = \varphi,$$

и окончательно

$$\begin{aligned}\xi_1 = x_1x_2 &= \frac{1}{2}\left\{\varphi + \frac{2p_3 - p_1\varphi}{\omega}\right\}, \\ \xi_2 = x_3x_4 &= \frac{1}{2}\left\{\varphi - \frac{2p_3 - p_1\varphi}{\omega}\right\}.\end{aligned}$$

§ 26

Обращаемся теперь к рассмотрению кубического уравнения

$$\psi^3 - A\psi - \sqrt{d} = 0. \tag{1}$$

Так как Vierergruppe есть нормальный делитель знакопереыенной, то уравнение принадлежит к числу нормальных, если мы будем считать выражение $\tau = \sqrt{D}$, присоединенным к полю $\Omega(p)$. Но Vierergruppe есть нормальный делитель также и для всей симметрической группы, то уравнение

$$(\psi^3 - A\psi)^2 - D = 0$$

будет также нормальным в поле $\Omega(p)$ без присоединения τ.

Мы видели уже в § 12 главы XII, что у нормальных кубическкх уравнений

$$x^3 + ax^2 + bx + c = 0$$

должен быть полным квадратом дискриминант

$$\Delta = -(4b^3 + 27c^2) + 18abc + a^2b^2 - 4a^3c.$$

Это как раз имеет место для кубического уравнения (1), ибо

$$\Delta = 4A^3 - 27D.$$

Откуда (см. стр. 454)

$$\Delta = B^2.$$

Применяя формулы Cardano, получим

$$\psi = \sqrt[3]{\frac{\sqrt{D}}{2} + B\,\frac{i\sqrt{3}}{2^2\,9^2}} + \sqrt[3]{\frac{\sqrt{D}}{2} - B\,\frac{i\sqrt{3}}{2^2\,9^2}}.$$

Второй корень квадратный $\sqrt{3}$ является от присоединения корня кубического из единицы

$$\alpha = \frac{-1 + i\sqrt{3}}{2}.$$

§ 27

Покажем теперь, как на самом деле выражаются корни уравнения (1) § 26 одни через другие.

Проще всего будем следовать общей теории § 16 и рассмотрим выражение

$$\frac{\psi_1}{t-\psi} + \frac{\psi_2}{t-\psi_1} + \frac{\psi}{t-\psi_2}, \tag{1}$$

где ψ, ψ_1, ψ_2 суть корни рассматриваемого кубического уравнения. Выражение (1) может быть переписано так

$$\frac{t\mathfrak{A} + \mathfrak{B}}{t^3 - at - \tau}, \tag{2}$$

где

$$\begin{aligned}\mathfrak{A} &= -(\psi_1+\psi_2)\psi_1(\psi=\psi_2)\psi_2 - (\psi+\psi_1)\psi = \\ &= \psi\psi_1 + \psi_1\psi_2 + \psi_2\psi = -A.\end{aligned}$$

Вычисление $\mathfrak{B}$ несколько сложнее:

$$\mathfrak{B} = \psi_1^2\psi_2 + \psi_2^2\psi + \psi^2\psi_1.$$

Введем вспомогательную величину

$$\lambda = \psi_1\psi_2^2 + \psi_2\psi^2 + \psi\psi_1^2.$$

Тогда

$$\mathfrak{B} + \lambda = \psi_1\psi_2(\psi_1+\psi_2) + \psi_2\psi(\psi_2+\psi) + \psi\psi_1(\psi+\psi+1) = -3\psi\psi_1\psi_2 = -3\tau. \tag{3}$$

С другой стороны

$$\mathfrak{B} - \lambda = \psi_1\psi_2(\psi_1-\psi_2) + \psi_2\psi(\psi_2-\psi) + \psi\psi_1(\psi-\psi_1),$$

но

$$\begin{aligned}&\psi_1 - \psi_2 = \varphi + \varphi_1 - 3\varphi_1 = p_2 - 3\varphi_1,\\ &\psi_2 - \psi = p_2 - 3\varphi,\\ &\psi - \psi_1 = p_2 - 3\varphi_2,\end{aligned}$$

кроме того

$$\psi_1\psi_2 = \Omega_0'(\varphi_1), \qquad \psi_2\psi = \Omega_0'(\varphi), \qquad \psi\psi_1 = \Omega_0'(\varphi_2),$$

где $\Omega_0'(y)$ обозначает первую часть уравнения (1) § 15. Итак, выражение

$$\mathfrak{B} - \lambda = \Omega_0'(\varphi)(p_2 - 3\varphi) + \Omega_0'(\varphi_1)(p_2 - 3\varphi_1) + \Omega_0'(\varphi_2)(p_2 - 3\varphi_2) \tag{1}$$

будучи симметрической функцией трех корней φ, φ_1, φ_2 уравнения $\Omega_0'(y) = 0$ выражается просто в поле $\Omega(p)$; пусть это выражение будет $\mathfrak{K}$. Мы получаем, сопоставляя (3) и (4),

$$\mathfrak{B} = -\frac{3}{2}\,\tau + \frac{1}{2}\,\mathfrak{K}.$$

Окончательное выражение ψ_1 через ψ имеет вид

$$\psi_1 = \frac{-A\psi + \mathfrak{B}}{3\psi^2 - A}.$$

Глава XVI

Теория Galois

§ 1

В основу моего изложения теории Galois я положу мысли, приведенные мною в статье «Об основных положениях теории Galois». Матем. Сборн. Москва 1914.

Теория Galois принадлежит настолько исключительная роль в математике, что я считаю необходимым остановиться несколько на личности автора этой теории.

Evariste Galois родился 25 окт. 1811 г. вблизи Парижа. В 1823 году покинул родительский дом, чтобы поступить в коллегию Louis-le-Grand. Уже с пятнадцати лет обнаружились в нем выдающиеся способности к математике, причем на классических творениях Lagrange'a он воспитал свои природные наклонности алгебраиста. — Можно думать, что уже к семнадцати годам он обладал своими наиболее важными идеями. Но об этом можно делать только догадки, ибо два мемуара, представленные им в парижскую Академию Наук, не только удостоились ответа, но даже оказались потерянными. Этот удивительный факт в высшей степени характерен для оффициальных научных организаций, которые всегда относятся с известным недоверием к начинающим авторам. После двух неудачных попыток поступить в Политехническую Школу Galois поступил в 1829 году в Нормальную Школу, которую принужден был оставить уже в следующем году. Последние годы жизни он провел довольно бурно, участвуя в политической жизни страны, и умер 31 мая 1832 г. от раны, полученной на дуэли.

§ 2

Если обычно принято приписывать Galois начало применения теории групп к изучение алгебраических уравнений, то это справедливо только до известной степени, ибо надо признать, что случай буквенных уравнений, как это мы видели в предыдущей главе, достаточно подробно изучен уже Lagrange'ем. Galois принадлежит лишь честь создания удивительной по глубине теории, которая, с одной стороны, является распространением теории Langrange'a на численные уравнения, с другой стороны, заключает теорию Langrange'a как частный случай.

Не смотря на большую разработанность теории Galois мне не случилось до самого последнего времени встретить такое изложено ее принципов, которое бы удовлетворило меня с точки зрения простоты, строгости и общности. Скажу более, часто изложение теории страдает такими неясностями и недомолвками, что изучающей эту теории в первый раз может составить себе совершенно превратное понятие о предмете.

§ 3

В основу моего изложения я ставлю *точную* формулировку различия между буквенными и численными уравнениями.

Уравнение

$$x^n + p_1 x^{n-1} + p_2 x^{n-2} + \ldots + p_n = 0$$

я буду называть *численным*, если между его корнями *существуют* соотношения вида

$$\Pi(x_1, x_2, \ldots, x_n) = 0, \tag{1}$$

где Π целая функция от независимых переменных $x_1, x_2, \ldots, x_n$ с отличными от нуля и принадлежащими к полю Ω коэффициентами.

Я напомню, что мы согласились в главе XIV рассматривать только поля с равной нулю характеристикой.

Соотношения (1) с отличными от нуля коэффициентами будем называть для сокращения *нетождественными*, сохраняя название *тождественных* для соотношений (1) в случай равенства нулю всех коэффициентов.

Говоря кратко, мы назовем численными такие уравнения, которые допускают не тождественные соотношения между корнями.

Если все коэффициенты p_i уравнения суть определенные числа, принадлежащие к полю Ω, то уравнение будет очевидно, численным, ибо существуют между корнями не тождественные соотношения

$$\sum x_i + p_1 = 0, \quad \sum x_1 x_2 - p_2 = 0, \ \ldots$$

Этот случай есть, так сказать, крайний в смысле числовой определенности уравнения. По моей терминологии численным уравнением будет называться также и такое, где, например, p_1, а все остальные коэффициенты $p_2, p_3, \ldots, p_n$ независимые переменные, ибо тогда существует между корнями не тождественное соотношение

$$x_1 + x_2 + \ldots + x_n = 0.$$

Вообще говоря, будет численным всякое уравнение, коэффициенты которого удовлетворяют соотношениям вида $\Pi(p_1, p_2, \ldots, p_n) = 0$.

§ 4

Рассмотрим совокупность G всех подстановок из которых *каждая* не нарушает справедливости *всякого* соотношения между корнями. Докажем, что эта совокупность есть группа.

Пусть выписаны все возможные соотношения между корнями[91]

$$\Pi = 0, \ \ \Pi_1 = 0, \ \ \Pi_2 = 0, \ \ldots \tag{1}$$

Применим к произвольному из них, например к Π, одну из подстановок S данной совокупности. Так как подстановка S не должна нарушать справедливости

[91]Целыми индексами при буквах Π я не имею желания подчеркивать необходимости для совокупности соотношений быть обязательно перечислимою.

соотношения $\Pi = 0$, то это последнее после подстановки должно обратиться в новое соотношение также верное. Это новое соотношение должно находиться среди соотношений (1), пусть оно будет $\Pi_k = 0$. Применим теперь к последнему другую подстановку T нашей совокупности G. Пусть соотношение $\Pi_k = 0$ перейдет в новое $\pi_l = 0$. Очевидно, что подстановка ST переводит соотношение $\pi = 0$ в $\Pi_l = 0$, но соотношение $\Pi_l = 0$ есть также верное соотношение, следовательно, подстановка ST принадлежать к G, ибо эта подстановка не нарушает произвольно выбранного соотношения $\Pi = 0$. Итак, G есть группа.

Группа G носит название группы Galois для данного уравнения или, просто, группы уравнения.

§ 5

Нетрудно видеть, что для буквенного уравнения группой Galois является вся симметрическая группа всех подстановок корней, ибо можно сказать, что между корнями буквенная» уравнения существуют только тождественные соотношения, эти же соотношения не нарушаются от любой подстановки.

§ 6

Если соотношения между корнями численного уравнения таковы, что требование не нарушать их заставляет отбрасывать известные подстановки, то группа Galois уменьшается и делается подгруппой симметрической группы. Следуя Kronecker'у, мы скажем, что в таком случае уравнение имеет *аффект*. Буквенные уравнения суть уравнения без аффекта.

§ 7

Покажем на простом примере, что существуют *численные* уравнения без аффекта.

Рассмотрим, например, уравнение (см. § 15 главы XII)

$$x^5 - p^2x - p = 0, \tag{1}$$

где p произвольное простое число, и возьмем за основное поле Ω поле рациональных чисел.

Так как первая часть уравнения имеет при $-\infty$, -1, 0, $+\infty$, знаки $-$, $+$, $-$, $+$, то существуют три вешественных корня уравнения. Остальные два корня обязательно *мнимые*, ибо в уравнении имеется пропуск трех членов со степенями x^4, x^3, x^2 (см. стр. 299).

Так как числа основного поля вещественные, то всякое соотношение между корнями будет иметь вид $a + ib = 0$, откуда $a = 0$, $b = 0$, а, следовательно, и $a - ib = 0$. Другими словами, всякое соотношение между корнями не нарушается от изменения знака перед i.

Если мы обозначим через 1 и 2 мнимые корни, то изменение знака перед i осуществляется при помощи транспозиции (12). Итак мы видим, что транспозиция (12) должна входить в группу Galois. По теореме Eisenstein'а (см. стр. 413) уравнение (1) неприводимо в основном поле, то, следовательно, как мы увидим далее, его

группа транзитивна. Мы видели в § 39 главы V, что, если транзитивная группа заключает транспозицию (12), то она или симметрическая или же импримитивная. Уравнение задано простой степени, значит, число корней есть простое, а потому группа подстановок этих корней не может быть импримитивною. Итак, мы видим, что группа Galois для уравнения (1) есть симметрическая, т. е. уравнение (1) не имеет аффекта.

§ 8

Будем теперь рассматривать рациональные функции

$$\varphi(x_1, x_2, \ldots, x_n)$$

от корней $x_1, x_2, \ldots, x_n$ с коэффициентами из основного поля Ω.

Основным вопросом является изучение условий *неизменяемости* функции φ при подстановках корней. Эту неизменяемость можно понимать двояко: при буквенных уравнениях дело идет о функциоиальной неизменяемости, т. е. неизменяемости *вида*; при численных же уравнениях дело идет о неизменяемости *численного значения* функции, хотя бы вид ее и изменялся при подстановки.

Несмотря на кажущееся большое различие этих двух понятий теория Galois сближает их в одно гармоническое целое.

Поясним сказанное примером. Функция $x_1x_2 + x_3x_4$ не меняет своего вида при подстановке (1324), но меняет вид при подстановке (123), ибо от последней подстановки Функция принимает вид $x_2x_3 + x_1x_4$; если у нас рассматривается численное уравнение, среди соотношений которого существует $x_2 = x_4$, то численное значение функции $x_1x_2 + x_3x_4$ не меняется при обеих подстановках (1324) и (123).

§ 9

При буквенных уравнениях мы имели очевидную теорему: *подстановки не изменяющие вида функции, образуют группу.*

Эта теорема падает, если мы потребуешь вместо неизменяемости вида функций неизменяемость численного значения. Можно доказать для численных уравнений, *что подстановки, не изменяющиея численного значения функции, могут и не образовать группы.*

В последнем мы легко убеждаемся на самых простых примерах. Возьмем, например, уравнение

$$x^6 + x^5 + \ldots + x^2 + x + 1 = 0,$$

корни которого суть

$$x_k = e^{\frac{2k\pi i}{7}}.$$

Очевидно, что $x_1x_6 = 1$. Произведение x_1x_6 не меняет своей численной величины, т. е. остается равным единице, при двух подстановках

$$S = (12)(56), \qquad T = (16)(23),$$

ибо от подстановки S оно переходить в $x_2x_4 = 1$, а от T оно переходит в $x_6x_1 = 1$. Подстановка же ST переводить первоначальную функцию x_1x_6 в x_3x_5, а эта величина уже не равна единице и, значить, произведение подстановок S и T, не

менявших численного значения функции, представляет подстановку, уже меняющую численное значение.

Теорема о том, что подстановки, не меняюшие функций, образуют группу, *восстановляется* для численных уравнений, если будем выбирать подстановки не произвольно, а только лишь *из группы Galois*.

Мы приходим к теорем имеющей место для численных уравнений.

Подстановки из группы Galois, не меняющая численно функции образуют группу.

Пусть функция $\varphi(x_1, x_2, \ldots, x_n)$, которую мы обозначим для краткости $\varphi(x)$, не меняет своего численного значения от двух подстановок S и T, взятых из группы Galois. Обозначим то выражение, в которое переходить функция $\varphi(x)$ при подстановке S, знаком $\varphi(x|S)$.

Получим два равенства

$$\varphi(x|S) = \varphi(x), \qquad \varphi(x|T) = \varphi(x). \tag{1}$$

Так как подстановки из группы Galois можно применять ко всякому соотношение между корнями, то, применяя подстановку T к первому из равенств (1), а S ко второму, получим

$$\varphi(x|ST) = \varphi(x|T), \qquad \varphi(x|TS) = \varphi(x|). \tag{2}$$

Сравнивая (1) и (2), получим

$$\varphi(x|ST) = \varphi(x|TS) = \varphi(x),$$

и теорема доказана.

§ 10

Примыкая к идеям Kronecker'a, возьмем выражение

$$\xi = t_1x_1 + t_2x_2 + \ldots + t_nx_n,$$

где $t_1, t_2, \ldots, t_n$ независимые переменные. Корни $x_1, x_2, \ldots, x_n$ мы можем предполагать различными между собой, ибо в случае кратных корней мы можем освободить от них уравнение при помощи рациональных действий, т. е., другими словами, не выходя из основного поля.

Пусть

$$\xi, \quad \xi', \quad \xi'', \ \ldots, \ \xi^{(N-1)} \qquad (N = 1 \cdot 2 \cdot 3 \cdots N) \tag{1}$$

будут те выражения, которых получаются из ξ от различных N подстановок корней $x_1, x_2, \ldots, x_n$, оставляя на месте величины $t_1, t_2, \ldots, t_n$.

Так, например,

$$\xi^{(i)} = t_1x_{i_1} + t_2x_{i_2} + \ldots + tnx_{i_n},$$

где

$$i_1, \quad i_2, \ \ldots, \ i_n$$

некоторое перемещение индексов $1, 2, \ldots, n$.

Величины (1), рассматриваемые как функции от независимых переменных t_i, все *различны* между собой, ибо различны все $x_1, x_2, \ldots, x_n$.

§ 11

Рассмотрим функцию

$$G(\eta) = (\eta - \xi)(\eta - \xi') \cdots (\eta - \xi^{(N-1)}) = \eta^N + T_1\eta^{N-1} + T_2\eta^{n-2} + \ldots + T_N,$$

где, очевидно, T_k есть форма степени k от независимых переменных t_i с коэффициентами симметрическими функциями от x_i. Другими словами, T_k будет форма степени k от t_i с коэффициентами, принадлежащими к полю $\Omega(p)$; так например,

$$T_1 = \frac{N}{n}\, p_1(t_1 + t_2 + \ldots + t_n),$$

где p_1 первый коэффициент заданного уравнения.

§ 12

Покажем, что уравнение $G(\eta) = 0$ *неприводимо* в поле $\Omega(p, t)$, полученном от присоеднненния $t_1, t_2, \ldots, t_n$ к $\Omega(p)$, если предположить корни x_i *независимыми переменнымы*.

Допустим обратное, а именно, что уравнение приводимо. Пусть $G_1(\eta)$ будет некоторый неприводимый множитель функции $G(\eta)$. Мы, конечно, должны предполагать, что коэффициенты функции $G_1(\eta)$ суть формы от t_i с коэффициентами из $\Omega(p)$. Указанный характер коэффициентов $G_1(\eta)$ происходит оттого, что эта функция должна быть произведением разностей $\eta - \xi^{(i)}$, где i не пробегает полной системы значений $0, 1, 2, \ldots, N-1$. Пусть $G_1(\eta)$ будет тот из неприводимых множителей функции $G(\eta)$, который имеет корень ξ.

Имеет место тождество $G_1(\xi) = 0$. Это тождество будет буквенным, если предположить корни x_i независимыми переменными. Так как буквенное тождество не нарушается при всех подстановках переменных, то мы получим тождество

$$G_1(\xi^{(i)}) = 0,$$

где i пробегает всю систему чисел $0, 1, 2, \ldots, N-1$.

Итак, неприводимый множитель $G_1(\eta)$ должен заключать все различные между собой N корней функции $G(\eta)$, т. е. $G_1(\eta)$ должен совпадать с $G(\eta)$ и, следовательно, $G(\eta)$ неприводимо.

§ 13

Покажем прежде всего, что корни $x_1, x_2, \ldots, x_n$ заданного уравнения выражаются рационально через ξ в таком смысле, что корень x_i есть рациональная функция от ξ, коэффициенты которой принадлежать полю $\Omega(p, t)$.

Рассмотрим следующие N линейных уравнений

$$x_{i_r} = \sum A_h(t_1 x_{i_1} + t_2 x_{i_2} + \ldots = t_n x_{i_n})^h, \tag{1}$$

где сумма $\sum$ распространяется на все значения $0, 1, \ldots, N-1$ показателя h. Коэффициенты A_h подлежат определению из N уравнений первой степени, которые получаются из уравнения (1), если под $i_1, i_2, \ldots, i_n$ разуметь все возможные перемещения индексов $1, 2, \ldots, n$.

Решим при помощи определителей систему N уравнений с N неизвестными A_h и покажем, что эти неизвестные окажутся элементами поля $\Omega(p, t)$.

Мы получаем, очевидно,

$$\Theta A_h = \Delta_h,$$

где Θ есть определитель

$$\begin{vmatrix} (t_1 x_{i_1} + t_2 x_{i_2} + \ldots = t_n x_{i_n})^{N-1} & (t_1 x_{i_1} + t_2 x_{i_2} + \ldots = t_n x_{i_n})^{N-2} & \ldots & 1 \\ \ldots & \ldots & \ldots & \ldots \end{vmatrix}.$$

В этом определителе горизонтали получаются из первой при помощи подстановок корней x_i.

Определитель же Δ_h, получается из Θ заменой h-ой колонны колонной корней x_{i_r}. Так как при всякой подстановка корней x_i горизонтали в Θ и Δ_h перемещаются одинаково, то будут симметрическими функциями от корней x_i два выражения Θ^2 и $\Theta\Delta_h$. Отсюда окажется симметрической функцией от корней x_i коэффициент

$$A_h = \frac{\Theta\Delta_h}{\Theta^2}.$$

Подставляя полученные выражения коэффициентов A_h в равенство (1) и применяя это равенство к первоначальному расположению индексов $1, 2, \ldots, n$, получим

$$x_r = \sum A_h \xi^h,$$

т. е. всякий корень x_r рационально выражается через ξ в поле $\Omega(p, t)$.

§ 14

Если x_i будут корнями численного уравнения, то функция $G(\eta)$ § 11 может *сделаться приводимой*. Мы покажем, что, если обозначить через $g(\eta)$ неприводимый в $\Omega(p, t)$ множитель функции $G(\eta)$, то степень уравнения $g(\eta) = 0$ будет равна порядку группы Galois. Уравнение $g(\eta) = 0$ называется *резольвентой Galois*. Тогда будет очевидно, что для уравнения без аффекта резольвента Galois обращается в уравнение $G(\eta) = 0$.

Пусть резольвента $g(\eta)$ тот неприводимый множитель функции $G(\eta)$,который имеет корень ξ. Тождество $g(\eta) = 0$ удовлетворяется таким образом: первая часть есть функция рациональная от t_i и x_i. Все коэффициенты при степенях t_i в числителе должны уничтожаться на основании соотношений между корнями x_i. Итак, рассматривая в равенстве $g(\eta) = 0$ величины t_i как произвольные постоянные, мы можем к нему применить любую подстановку S_i корней x_i, взятую из группы Galois. Пусть подстановка S_i обращает ξ в $\xi^{(i)}$, значит, получим новое справедливое равенство $g(\xi^{(i)}) = 0$. Итак, подстановки группы Galois можно характеризовать как такие, которые переводят один корень ξ резольвенты в другой. Но быть может таким образом не исчерпываются все корни $\xi^{(i)}$ резольвенты. Для доказательства обратного покажем, что переход от ξ ко всякому другому корню $\xi^{(k)}$

резольвенты дает подстановку корней из группы Galois. Для этой цели возьмем любое соотношение-

$$\Pi(x_1, x_2, \ldots, x_n) = 0 \tag{1}$$

между корнями. Выражая корни через ξ, получим

$$\Pi(\xi) = 0.$$

Здесь $\Pi(\xi)$ есть целая функция от ξ с коэффициентами из поля $\Omega(p,t)$. Если уравнению $\Pi(\xi) = 0$ удовлетворяет один корень ξ неприводимого в поле $\Omega(p,t)$ уравнения $g(u) = 0$, то ему должен удовлетворять также всякий другой корень $\xi^{(k)}$ того же уравнения $g(u) = 0$ и мы имеем $\Pi(\xi^{(k)}) = 0$. Другими словами, соотношение (1) между корнями не нарушается от подстановки $(\xi, \xi^{(k)})$ переводящей ξ в $\xi^{(k)}$.

Так как соотношение (1) выбрано произвольно, то подстановка $(\xi, \xi^{(k)})$ принадлежит группе Galois, что и требовалось доказать.

Резюмируя сказанное, мы замечаем, что группа Galois состоит из подстановок

$$(\xi, \xi), \quad (\xi, \xi'), \quad (\xi, \xi''), \quad \ldots, \quad (\xi, \xi^{(\nu-1)}),$$

где $\xi, \xi', \ldots, \xi^{(\nu-1)}$ суть все корни резольвенты Galois.

§ 15

Теперь я перейду к указанию способа рассуждения, который сводит численную неизменяемость непосредственно к рассмотрению буквенной неизменяемости.

Для этой цели покажем, что переход от

$$\xi = t_1 x_1 + t_2 x_2 + \ldots + t_n x_n$$

к

$$\xi^{(i)} = t_1 x_{i_1} + t_2 x_{i_2} + \ldots + t_n x_{i_n}$$

может быть воспроизведен подстановкой, букв t_i оставляя x_i на местах. Чтобы найти соответственную подстановку величин t_i будем рассуждать так: обозначим через

$$\sigma = \begin{pmatrix} i_1 & i_2 & \ldots & i_n \\ 1 & 2 & \ldots & n \end{pmatrix}$$

подстановку $(\xi, \xi^{(i)})$ корней x_i. Произведем в выражении $\xi^{(i)}$ ту же подстановку σ индексов у величин t_i, оставляя корни x_i на местах, тогда выражение $\xi^{(i)}$ обратится в $t_{i_1} x_1 + t_{i_2} x_2 + \ldots + t_{i_n} x_n$, т. е. в ξ.

Итак, переход от ξ к $\xi^{(i)}$ производится при помощи обратной подстановки σ^{-1} величин t_i.

§ 16

Если подстановка σ пробегает группу Galois, то ту же группу пробегает и обратная подстановка σ^{-1}. Итак, мы имеем право вместо подстановок корней x_i рассматривать подстановки независимых переменных t_i. Если мы не будем выходить из группы Galois, то мы достигнем полного сведения теории численных уравнений к теории Lagrange'a.

В самом деле, всякое соотношение

$$\Pi(x_1, x_2, \ldots, x_n) = 0$$

после подстановки вместо x_i их выражений через ξ обратится в

$$\Pi'(t_1, t_2, \ldots, t_n) = 0, \tag{1}$$

которое должно быть *тождеством относительно* t_i, ибо эти величины суть независимые переменные.

Конечно равенство (1) не будет тождеством, если сохранить обозначения корней x_i; все его коэффициенты обратятся в нуль лишь на основании соотношений, существующих между корнями численного уравнения. Поэтому я и сказал, что (1) есть тождество только относительно t_i.

Если функция $\varphi(x_1, x_2, \ldots, x_n)$ не изменяет численного значения при подстановка σ, при чем вид свой она изменяет и обращается в $\varphi_1(x_1, x_2, \ldots, x_n)$, то мы имеем равенство

$$\varphi(x_1, x_2, \ldots, x_n) = \varphi_1(x_1, x_2, \ldots, x_n), \tag{2}$$

которое будет одним из существующих соотношений между корнями. Выразим теперь x_i через ξ, тогда получим из равенства (2) другое

$$\varphi'(t_1, t_2, \ldots, t_n) = \varphi'_1(t_1, t_2, \ldots, t_n). \tag{3}$$

Так как t_i суть независимые переменные, то обе функции

$$\varphi'(t_1, t_2, \ldots, t_n) \quad \text{и} \quad \varphi'_1(t_1, t_2, \ldots, t_n)$$

рассматриваемые как функций от t_i должны быть равны тождественно, принимая во внимание, конечно, существуюшие между x_i соотношения. Функция $\varphi'(t_1, t_2, \ldots, t_n)$ не изменяет, следовательно, своего вида относительно t_i при подстановка σ^{-1} этих величин t_i.

§ 17

Для завершения полного сведения численных уравнений к теории Lagrange'а необходимо доказать для *численных* уравнений теорему, аналогичную основной теореме теории симметрических функций.

Эта теорема может быть формулируема так:

Теорема. *Функция φ от корней x_i с коэффициентами из основного поля Ω, не меняющаяся численно при всех подстановках группы Galois, есть величина из поля $\Omega(p)$.*

Пусть резольвента Galois $g(u) = 0$ имеет степень ν и пусть ее корни будут $\xi, \xi', \xi'', \ldots, \xi^{(\nu-1)}$. Выразим функцию φ через ξ:

$$\varphi = \Phi(\xi).$$

На оснований неизменяемости функций φ при всех подстановках группы Galois получим

$$\varphi = \Phi(\xi) = \Phi(\xi') = \ldots = \Phi(\xi^{(\nu-1)}),$$

откуда

$$\varphi = \frac{1}{\nu}\,[\Phi(\xi) + \Phi(\xi') + \ldots + \Phi(\xi^{(\nu-1)})].$$

Итак, φ выражается симметрической функцией от корней резольвенты, значит, эта функция есть элемент поля $\Omega(p,t)$. С другой стороны, φ не заключает переменных независимых t_i, следовательно, она должна быть величиною из $\Omega(p)$, что и требовалось доказать.

§ 18

Из сказанного вытекает справедливость следующих теорем самого общего вида, в которых неизменяемость функций и их принадлежность к группе должна быть понимаема в том или другом смысле, судя по тому, какое уравнение рассматривается, буквенное или численное.

I. Подстановки из группы Galois, *не меняющие* (буквенно при буквенных уравнениях и численно при численных) рациональной функции φ от корней, образуют всегда некоторую группу H.

II. Функция φ, *принадлежащая* группе H, являющейся настоящим (меньшего порядка) делителем группы Galois, *изменяется* при подстановках группы Galois, не входящих в состав подгруппы H, при чем она получает новое значение (новый вид при буквенных уравнениях и новое численное значение при численных) при подстановках сопряженной системы $H\Sigma$ и только при них.

III. Функция, *не меняющаяся* от всех подстановок группы Galois, есть величина из $\Omega(p)$.

IV. Число *различных* значений функций φ, принимаемых при всех подстановках группы Galois, равно индексу j подгруппы H по отношению к группе Galois.

V. Функция φ, *принадлежащая* группе H индекса j, есть корень уравнения степени j

$$\varphi^j + M_1\varphi^{j-1} + \ldots + M_j = 0,$$

где коэффициенты M_i принадлежать $\Omega(p)$.

VI. Если функция ψ *не меняется* при подстановках группы H другой функции φ, то она выражается рационально в поле $\Omega(p)$ через φ.

VII. Если две функции φ и ψ принадлежат к одной группе, то каждая из них выражается рационально через другую.

VIII. Если функция ψ принадлежать к подгруппе K группы H другой функции φ, то она есть корень алгебраического уравнения

$$\psi^\lambda + L_1\psi^{\lambda-1} + \ldots + L_\lambda = 0$$

степени λ, равной индексу подгруппы K по отношению к группе H, причем коэффициенты L_i суть рациональные в поле $\Omega(p)$ функции от φ.

Глава XVII

Дальнейшие свойства резольвент

О резольвенте Galois

§ 1

В предыдущей главе мы дали определение понятая группы Galois. Особенное значение имеет группа Galois в вопросе об алгебраическом решений уравнений. Оказывается, что, если уравнение решается в радикалах, то его группа обладает *особенными свойствами* и носит в случай наличности этих свойств название *группы разрешимой*. Разрешимость группы уравнения, или, лучше сказать, *наличность* тех *свойств*, по которым группу называют разрешимою, является условием необходимым и достаточным для возможности алгебраического решения уравнения. Существующее среди не специалистов алгебры некоторое предубеждение против теории Galois основано на недоразумении. За всю столетнюю после Galois историю вопроса об алгебраическом решении уравнений не было случая, чтобы решение уравнения в радикалах не сопровождалось указанием, соответствующей уравнению, группы и обратно, чтобы знание разрешимой группы не приводило к полному решению уравнения. Поэтому изучение группы Galois для алгебраического решения уравнения является не только теорией, но и практическим приемом для проведения до конца выкладки решения уравнения.

§ 2

Поставив в предыдущей главе задачу самым общим образом, поведем однако дальнейшее изложение ближе к обычной теории численных уравнений, трактующей вопрос несколько уже.

Пусть коэффициенты заданного уравнения

$$x^n + p_1 x^{n-1} + p_2 x^{n-2} + \ldots + p_n = 0 \tag{1}$$

суть *определенных числа, принадлежащие* к полю Ω, которое мы будем считать основным. Числа основного поля мы будем считать числами *известными*.

В настоящей главе будет обращено особенное внимание на тот важный факт, что группа Galois зависит органически от того *поля*, которое принято за основное. Если поле изменяется при помощи расширения через присоединение новых величин, или же мы переходим от первоначального поля к его делителю, то группа уравнения *может* измениться.

Если для некоторого поля группа Galois сведется к одной только тождественной подстановке (сведется к единице), то можно сказать, что *в таком поле задан-*

ное уравнение решается вполне. В самом деле, в этом случае каждый корень в отдельности

$$x_i$$

может считаться за функцию, не изменяющуюся от всех подстановок группы Galois, ибо эта группа состоит из одной только тождественной подстановки. Итак, на оснований теоремы § 17 главы XVI корень x_i должен принадлежать к нашему полю. Мы предполагаем, что при всяком изменении поля коэффициенты p_i заданного уравнения в нем находятся.

Из сказанного следует основной прием приложения теории Galois к решению уравнений.

Вся задача состоит в том, чтобы приличным изменением поля придти окончательно к такому полю, для которого группа Galois обращается в единицу; тогда, очевидно, уравнение окажется решенным.

§ 3

На простом примере можно показать возможность такого расширения основного поля Ω, чтобы в новом поле данное уравнение (1) § 2 решалось вполне. В самом деле, если мы присоединить к основному полю Ω все корни $x_1, x_2, \ldots, x_n$ данного уравнения, то, очевидно, что в полученном таким образом расширенном поле

$$\Omega(x_1, x_2, \ldots, x_n) \tag{1}$$

заданное уравнение решается вполне. Все корни x_i находятся в этом новом поле (1), припоминая же соглашение § 2 считать числа всякого рассматриваемого поля за известные, мы можем сказать, что вей корни x_i оказываются известными в новом поле.

Приведенные соображения могут с первого взгляда показаться тривиальными и как бы игрой слов; тем не менее в этих соображениях лежит глубокий смысл и ключ ко всей теории Galois.

Припоминая теорему § 18 главы XIV, мы замечаем, что одновременное присоединение нескольких алгебраических чисел $x_1, x_2, \ldots, x_n$ равносильно присоединению одного ξ, и можем сказать, что поле (1) есть не что иное как

$$\Omega(\xi)$$

где ξ есть корень некоторого неприводимого уравнения

$$g(\xi) = 0 \tag{2}$$

с коэффициентами из поля Ω.

§ 4

Покажем весьма важные свойства вспомогательного уравнения (2) $g(\xi) = 0$ предыдущего параграфа.

Так как корни $x_1, x_2, \ldots, x_n$ суть элементы поля (1) § 3, которое есть не что иное как $\Omega(\xi)$, то корни x_i будут рациональными функциями от ξ

$$x_1 = \Theta_1(\xi), \quad x_2 = \Theta_2(\xi), \ \ldots, \ x_n = \Theta_n(\xi)$$

коэффициенты всех функций Θ_i принадлежат к основному полю Ω. С другой стороны, величина ξ есть элемент поля (1) § 3, значит,

$$\xi = \varphi(x_1, x_2, \ldots, x_n), \tag{1}$$

где φ рациональная функция от x_i с коэффициентами из поля Ω. Припоминая, как мы в § 18 главы XIV указывали функцию ξ, мы придем к дальнейшим весьма важным замечаниям. Я повторю в несколько иных выражениях соображения § 18 главы XIV.

Функция $\varphi(x_1, x_2, \ldots, x_n)$ может быть взята совершенно произвольно лишь бы она менялась численно от всех подстановок корней. Такую функцию мы будем по примеру § 7 главы XV называть функцией Galois. Там мы рассматривали буквенную изменяемость функции. Теперь придется убедиться, что существуют функции Galois при численных уравнениях, т. е. что существует такая функция, *численные* значения которой получаемые при *всех* подстановках корней все различны между собой.

В § 10 главы XVI мы построили линейную функцию

$$t_1x_1 + t_2x_2 + \ldots + t_nx_n \tag{2}$$

от корней x_i численного уравнения с коэффициентами произвольными переменными независимыми. Если все корни x_i различны, то функция (2) будет уже функцией Galois. В дальнейшем мы не желаем рассматривать трансцендентных расширений поля при помощи переменных t_i, а потому надо сообразить, нельзя ли выбором численных значений t_i из поля Ω достигнуть того, чтобы выражение (2) оставалось функцией Galois также и при определенных численных значениях t_i. Прилагая рассуждения § 17 главы XIV, заметим, что всегда можно задать *даже* рациональные значения коэффициентам t_i чтобы выражение (2) было функцией Galois.

Единственное и вполне *естественное* требование мы накладываем на заданное уравнение, чтобы все его корни были *простые*.

Пусть

$$\xi, \quad \xi', \quad \xi'', \ \ldots, \ \xi^{(N-1)} \qquad (N = 1 \cdot 2 \cdot 3 \cdots n) \tag{3}$$

будут выражения получаемые при всех подстановках корней из

$$\xi = \varphi(x_1, x_2, \ldots, x_n),$$

где φ есть функция Galois.

Рассмотрим уравнение

$$G(\eta) = (\eta - \xi)(\eta - \xi') \cdots (\eta - \xi^{(N-1)}) = \eta^N + A_1\eta^{N-1} + A_2\eta^{N-2} + \ldots,$$

в котором все коэффициенты A_i, будучи симметрическими функциямн корней x_i, представляют из себя элементы поля Ω.

Неприводимая функция $g(\eta)$, (см. (2) § 3) будет, очевидно, делителем $G(\eta)$, ибо $G(\eta)$ имеет своим корнем корень ξ функции $g(\eta)$. Итак, мы видим, что корнями функции $g(\eta)$ будут некоторые из выражений (3). Пусть эти корни будут

$$\xi, \quad \xi_1, \quad \xi_2, \ \ldots, \ \xi_{\nu-1}.$$

Повторяя рассуждение § 12 главы XVI, докажем. что *группа Galois есть не что иное как группа подстановок x_i, соответствующих перепереходу от ξ в остальные значения ξ_k*:

$$(\xi, \xi), \quad (\xi, \xi_1), \ \ldots, \ (\xi, \xi_{\nu-1}.$$

Уравнение $g(\eta) = 0$, осуществляющее своими корнями группу Galois, носит название, как мы уже сказали *резольвенты Galois.*

Корни $\xi, \xi_1, \ldots, \xi_{\nu-1}$ резольвенты, будучи рациональными функциями от корней x_i, суть элементы поля (1) § 3, или, что одно и тоже, поля $\Omega(\xi)$; итак, все корни резольвенты Galois выражаются рационально через один из них ξ:

$$\xi = \xi, \quad \xi_1 = \omega_1(\xi), \quad \xi_2 = \omega_2(\xi), \ \ldots, \xi_{\nu-1} = \omega_{\nu-1}(\xi).$$

Резюмируя все сказанное, мы можем характеризовать резольвенту Galois таким образом.

Резольвента Galois $g(\eta) = 0$ для уравнения $f(x) = 0$, не имеющего кратных корней, есть уравнение из той же основной области Ω, обладающее следующими свойствами:

1) *Все корни данного уравнения $f(x) = 0$ выражаются рационально через один из корней резольвенты*

$$x_1 = \Theta_1(\xi), \quad x_2 = \Theta_2(\xi), \ \ldots, \ x_n = \Theta_n(\xi 0.$$

2) *Все корни резольвенты рационально выражаются через все корни заданного уравнения*

$$\xi = \varphi(x_1, x_2, \ldots, x_n), \quad \xi_1 = \varphi_1(x_1, x_2, \ldots, x_n), \ \ldots, \ \xi_{\nu-1} = \varphi_{\nu-1}(x_1, x_2, \ldots, x_n).$$

3) *Все корни резольвенты рационально выражаются через один из них*

$$\xi = \xi, \quad \xi_1 = \omega_1(\xi), \ \ldots, \ \xi_{\nu-1} = \omega_{\nu-1}(\xi).$$

Название *резольвенты* дано уравнению $g(\eta) = 0$ потому, что достаточно знание одного из корней ξ этого уравнения, чтобы вполне решить заданное уравнение $f(x) = 0$.

§ 5

Резольвента Galois есть нормальное (см. § 20 главы XV) уравнение, ибо все ее корни выражаются рационально через ξ. Этого можно было сразу ожидать,

ибо корень ξ, как функция Galois, принадлежать единичной группе, единичная же группа есть нормальный делитель всякой другой.

Понятие о резольвенте Galois заключает большой произвол, ибо все зависит от выбора функции Galois $\xi = \varphi(x_1, x_2, \ldots, x_n)$. Если мы выберем другую функцию $\varphi_0(x_1, x_2, \ldots, x_n)$, то эта новая функция будучи элементом поля $\Omega(\xi)$ будет рациональною функцией от первоначальной ξ. Так что новая функция $\eta = \vartheta(\xi)$ окажется корнем новой резольвенты Galois $g(\eta) = 0$. Эта новая резольвента происходить из первоначальной при помощи преобразования $\eta = \vartheta(\xi)$ Tschirnhausen'a.

Итак, в этой теории резольвенты Galois, как уравнения происходяшие одно из другого при помощи преобразования Tschirnhausen'a, считаются одной трудности в смысле решения.

Выбор резольвенты не влияет на группу Galois, ибо соответственные корни различных резольвент связаны между собой рационально, а потому принадлежать одной и той же группе.

§ 6

Взглянем на связь группы Galois с резольвентой еще с другой точки зрения.

Так как $\xi_i = \omega_i(\xi)$ есть корень уравнения $g(u) = 0$, то мы получим $g(\omega_i(\xi)) = 0$, то есть, другими словами, уравнение $g(\omega_i(u)) = 0$ имеет общий корень ξ с неприводимым уравнением $g(u) = 0$. На основании свойств неприводимых уравнений мы замечаем, что и всякий другой корень ξ_k неприводимого уравнения $g(u) = 0$ будет удовлетворять уравнению $g(\omega_i(u)) = 0$ и мы получаем

$$g(\omega_i(\xi_k)) = 0,$$

т. е. $\omega_i(\xi_k)$ есть также корень уравнения ?

$$\omega_i(\xi_k) = \xi_i,$$

что можно написать подробнее так

$$\omega_i(\omega_k(\xi)) = \omega_i(\xi).$$

Итак, если функции $\omega_1, \omega_2, \omega_3, \ldots, \omega_{\nu-1}$ рассматривать как некоторые операции, производимые над аргументом, причем присоединим к ним еще операции $\omega_0(\xi) = \xi$ (единичную операцию), то формула (1) показывает, что эти операции образуют группу. Эта группа, конечно, изоморфна с группой Galois.

Транзитивные группы и неприводимость

§ 7

Пусть заданное уравнение $f(x) = 0$ степени n *приводимо* в поле Ω и пусть $f_1(x) = 0$ некоторый неприводимый в поле Ω множитель функции $f(x)$. Пусть степень $f_1(x)$ есть m, где $m < n$.

Обозначим корни множителя $f_1(x)$ через

$$x_1, \quad x_2, \ \ldots, \ x_m, \tag{1}$$

а через

$$x_{m+1},\ \ x_{m+2},\ \ \ldots,\ x_n, \tag{2}$$

остальные корни уравнения $f(x) = 0$.

Обозначим через x' один из корней (1), а через x'' один из корней (2).

Мы имеем тождество

$$f_1(x') = 0. \tag{3}$$

Предположим, что группа Galois заданного уравнения $f(x) = 0$ *транзитивная* (см. § 37 глава V), тогда должна в группе быть по крайней мере одна подстановка Σ, переводящая корень x' в x''.

Так как подстановки группы Galois прилагаются ко всякому соотношению между корнями. Прилагая Σ к соотношение (3), получим

$$f_1(x'') = 0,$$

что противоречить предположению. Итак мы приходим к теореме.

Если уравнение неприводимо, то его группа транзитивна, в случае же приводимости группа должна быть интранзитивна.

Докажем теперь теорему обратную. Пусть группа уравнения интранзитивна, причем пусть она перемещает между собой только корни (1), тогда функция

$$f_1(x) = (x - x_1)(x - x_2)\cdots(x - x_m)$$

не меняется при всех подстановках группы Galois, значит, коэффициенты $f_1(x)$ принадлежат полю Ω (см. § 15 главы XVI). Итак $f_1(x)$ оказывается множителем в поле Ω функций $f(x)$ и уравнение $f(x) = 0$ приводимо. Получается окончательная теорема.

Условием необходимым и достаточным для приводимости или неприводимости уравнения является иитранзитивность или транзитивность его группы.

Примитивные группы и уравнения

§ 8

В § 38 главы V мы дали понятие об *импримитивности* группы. Покажем теперь, какими свойствами обладает уравнение, когда оно имеет импримитивную группу Galois.

Для большей ясности будем параллельно рассматривать *три понятия* 1) некоторое *уравнение* $f(x) = 0$ с коэффициентами из поля Ω, не имеющее кратных корней. 2) его *группу Galois*, 3) *поле* $\Omega(\alpha)$, образованное от присоединения к полю Ω корня α уравнения $f(x) = 0$.

Что такое мы понимаем под импримитивностью или, обратно, примитивностью группы, было сказано в § 38 главы V.

Мы будем называть неприводимое в поле Ω уравнение $f(x) = 0$ *импримитивным*, если оно делается приводимым и раскладывается на несколько множителей

$$f(x) = f_1(x)f_2(x)\cdots f_\mu(x)$$

в расширенном поле $\Omega(\tau)$, где все множители $f_i(x)$ *одной и той, же степени*, а τ есть корень некоторого уравнения

$$\varphi(x) = 0$$

степени ν с коэффициентами из Ω.

Так как число μ должно быть делителем степени n, то *импримитивным может быть только уравнение составной степени.*

Если невозможно сведение решения неприводимого уравнения $f(x) = 0$, на решение ряда уравнений $\varphi(x) = 0$ и

$$f_1(x) = 0, \quad f_2(x) = 0, \ \ldots, \ f_\mu(x) = 0$$

такого рода, как было выше сказано, то уравнение $f(x) = 0$ носит название *примитивного*. Очевидно, что *всякое уравнение простой степени примитивное.*

§ 9

Введем теперь понятие об *импримитивности* поля $\Omega(\alpha)$, получаемого от присоединения к полю Ω корня уравнения

$$f(x) = 0, \tag{1}$$

неприводимого в поле Ω.

Пусть корни уравнения (1) будут

$$\alpha, \quad \alpha_1, \quad \alpha_2, \ \ldots, \ \alpha_{n-1}.$$

Рассмотрим поля

$$\Omega(\alpha), \quad \Omega(\alpha_1), \quad \Omega(\alpha_2), \ \ldots, \ \Omega(\alpha_{n-1}) \tag{2}$$

Поля (2) имеют общим делителем Ω, основное поле, и называются полями, *сопряженными* с полем $\Omega(\alpha)$.

Если уравнение (1) нормальное (см. § 20 главы XV), то все поля (2) тождественны между собой.

Может существовать случай промежуточный, когда общим наибольшим делителем полей (2) будет поле

$$\Omega(\beta), \tag{3}$$

где β не заключается в поле Ω.

В случай нормального уравнения поле (3) совпадает с каждым из полей (2).

Будем рассматривать элементы поля $\Omega(\alpha)$; эти элементы суть, очевидно, рациональные функции $\psi(\alpha)$.

Будем называть *сопряженными* величинами элемента $\psi(\alpha)$ числа

$$\psi(\alpha), \quad \psi(\alpha_1), \quad \psi(\alpha_2), \ \ldots, \ \psi(\alpha_{n-1}). \tag{4}$$

Если числа (4) *все различны между собой, то мы будем называть элемент* $\psi(\alpha)$ *поля* $\Omega(\alpha)$ *примитивным элементом поля* $\Omega(\alpha)$.

Если среди чисел (4) существуют равные, то элемент $\psi(\alpha)$ носит названия *импримитивного.*

Так, например, если все сопряженные значения (4) одинаковы, то элемент $\psi(\alpha)$ есть элемент поля Ω, ибо в этом случай

$$\psi(\alpha) = \frac{1}{n}\left[\psi(\alpha) + \psi(\alpha_1) + \ldots + \psi(\alpha_{n-1})\right].$$

Итак, во всяком поле $\Omega(\alpha)$ существуют импримитивные элементы из поля Ω.

Если кроме элементов поля Ω поле $\Omega(\alpha)$ не имеет других импримитивных элементов, то поле называется примитивным.

Обратно, поле $\Omega(\alpha)$ будет импримитивным при наличности в нем импримитивных элементов β, не заключающихся в поле Ω.

§ 10

Покажем, что три данные нами определения импримитивности: группы, уравнения и поля совершенно тождественны между собой.

Начнем с сопоставления понятия об импримитивности уравнения и его группы Galois.

Если группа уравнения $f(x) = 0$ импримитивна, то, как мы видели в § 38 главы V, все n корней уравнения $f(x) = 0$ могут быть расположены в прямую матрицу

$$(1)\qquad \begin{array}{l} A = \alpha,\ \alpha_1,\ \ldots,\ \alpha_{r-1} \\ B = \beta,\ \beta_1,\ \ldots,\ \beta_{r-1} \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ S = \sigma,\ \sigma_1,\ \ldots,\ \sigma_{r-1} \end{array},$$

состоящую из s горизонталей ($n = rs$). Каждая из этих горизонталей состоит из корней, образующих систему импримитивности.

Возьмем симметрическую функцию $\psi(x, x_1, \ldots, x_{r-1})$ такую, чтобы значения

$$(2)\qquad \begin{array}{ll} y & = \psi(\alpha, \alpha_1, \ldots, \alpha_{r-1}) \\ y_1 & = \psi(\beta, \beta_1, \ldots, \beta_{r-1}) \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & \\ y_{s-1} & = \psi(\sigma, \sigma_1, \ldots, \sigma_{r-1}) \end{array}$$

были *различны* между собой.

Чтобы видеть возможность сказанного, возьмем, например, за выражения (2) следующие

$$(3)\qquad \begin{array}{c} \psi(t, A) = (t-\alpha)(t-\alpha_1)\cdots(t-\alpha_{r-1}), \\ \psi(t, B) = (t-\beta)(t-\beta_1)\cdots(t-\beta_{r-1}), \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ \psi(t, S) = (t-\sigma)(t-\sigma_1)\cdots(t-\sigma_{r-1}) \end{array}$$

достаточно вместо t *подобрать* такое *рациональное* значение, чтобы все величины (3) были различны между собой.

Рассмотрим функцию

$$\varphi(\eta) = (\eta - y)(\eta - y_1)\cdots(\eta - y_{s-1}), \tag{4}$$

где η переменная независимая.

Так как по свойству импримитивности группа перемещает только корни отдельных систем импримитивности и кроме того перемещает между собой самые системы, то все коэффициенты функции $\varphi(\eta)$ не меняются и, значит, функция $\varphi(\eta)$ принадлежит полю Ω.

Величины (2) оказываются корнями уравнения

$$\varphi(\eta) = 0 \tag{5}$$

степени s.

Нетрудно видеть, что уравнение (5) *неприводимое*, ибо, вследствие предполагаемой *транзитивности* группы Galois, корень α может переходить в любой из корней $\beta_i, \ldots, \sigma_i$, следовательно, система A должна переходить в любую из следующих $B, \ldots, S$, то есть, корни $y, y_1, \ldots, y_{r-1}$ перемещаются *транзитивно*.

Очевидно, что, если мы обозначим через ω произвольную симметрическую функцию корней $\alpha, \alpha_1, \alpha_2, \ldots, \alpha_{r-1}$, то рассматривая целую функцию

$$\varphi(\eta)\left\{\frac{\omega}{\eta - y} + \frac{\omega_1}{\eta - y_1} + \ldots + \frac{\omega_{s-1}}{\eta - y_{s-1}}\right\}$$

с коэффициентами из Ω по способу, уже несколько раз нами применявшемуся, мы покажем, что ω выражается рационально через y.

Мы можем написать

$$\psi(\eta, A) = \psi(\eta, y), \tag{6}$$

что будет выражать то обстоятельство, что коэффициенты $\psi(\eta, A)$, будучи симметрическими функциями от $\alpha, \alpha_1, \alpha_2, \ldots, \alpha_{r-1}$, выражаются рационально через y.

Мы получаем

$$f(x) = \psi(x, y)\psi(x, y_1)\cdots\psi(x, y_{s-1}). \tag{7}$$

Итак, мы видим, что уравнение $f(x) = 0$ оказалось импримитивным в указанном выше смысле слова.

Данные нами определения импримитивности группы и уравнения друг другу соответствуют.

Покажем, что уравнение $\psi(\eta, y) = 0$ неприводимо в поле $\Omega(y)$.

Корни уравнения $\psi(\eta, y) = 0$ суть (см. (3)) $\alpha, \alpha_1, \alpha_2, \ldots, \alpha_{r-1}$.

Допустим приводимость уравнения и пусть $\psi_1(\eta, y)$ будет тот неприводимый множитель, который имеет корень α.

Если мы к соотношению

$$\psi_1(\alpha, y) = 0$$

применим все подстановки группы Galois и примем во внимание, что y симметрическая функция от корней $\alpha, \alpha_1, \alpha_2, \ldots, \alpha_{r-1}$, то получим

$$\psi_1(\alpha_i, y) = 0,$$

вследствие транзитивности группы Galois i может принимать все значения $0, 1, 2, \ldots, r-1$, следовательно, ψ_1 совпадает с ψ и неприводимость уравнения $\psi(\eta, y) = 0$ доказана.

§ 11

Теперь остается показать, что понятие о импримитивности группы и поля друг другу соответствуют.

Рассмотрим сопряженные величины

$$\psi(\alpha), \quad \psi(\alpha_1), \quad \psi(\alpha_2), \ \ldots, \ \psi(\alpha_{n-1}) \tag{1}$$

элемента $\psi(\alpha)$ поля $\Omega(\alpha)$.

Очевидно, что величина $\psi(\alpha)$ есть корень уравнения

$$(t - \psi(\alpha)) \cdots (t - \psi(\alpha_{n-1}) = F(t) = 0, \tag{2}$$

получаемого от преобразования Tschirnhausen'a

$$t = \psi(x),$$

получаемого к заданному неприводимому уравнений

$$f(x) = 0, \tag{3}$$

корни которого суть $\alpha, \alpha_1, \alpha_2, \ldots, \alpha_{n-1}$.

Посмотрим, что можно сказать о приводимости уравнения (2).

Пусть уравнение (2) будет приводимым и пусть $\varphi(t)$ будет неприводимый множитель функции $F(t)$, у которого предположим равным единице старший коэффициент.

Очевидно, что уравнение $\varphi(t) = 0$ удовлетворяется по крайней мере для одной из величин (1).

Пусть, например,

$$\varphi(\psi(\alpha)) = 0,$$

тогда уравнение $\varphi(\psi(x)) = 0$ имеет один общий корень α с уравнением $f(x) = 0$. Вследствие неприводимости уравнения $f(x) = 0$ все его корни должны обращать в нуль функцию $\varphi(\psi(x))$ и мы получаем

$$\varphi(\psi(\alpha)) = 0, \quad \varphi(\psi(\alpha_1)) = 0, \quad \varphi(\psi(\alpha_2)) = 0, \ \ldots, \ \varphi(\psi(\alpha_{n-1})) = 0. \tag{4}$$

Если все величины (1) различны между собой, то $\varphi(t)$ совпадает с $F(t)$ и уравнение (2) неприводимо.

Пусть $\psi(\alpha)$ будет *импримитивный* элемент поля $\Omega(\alpha)$, тогда среди величин существуют *одинаковые*. Пусть различные между собой из этих величин будут

$$\psi_1 = \psi(\alpha_{i_1}), \quad \psi_2 = \psi(\alpha_{i_2}), \ \ldots, \psi_s = \psi(\alpha_{i_s}) \tag{5}$$

остальные величины пусть совпадают с одною из величин (5).

На основании (4) корнями неприводимого множителя $\varphi(t)$ должны быть все величины (5) и каждая, очевидно, по одному разу, ибо $\varphi(t)$ как функция неприводимая не может имеет кратных корней.

Итак

$$\varphi(t) = (t - \psi_1)(t - \psi_2) \cdots (t - \psi_s).$$

Всякий другой неприводимый множитель функции $F(t)$ должен совпадать с $\varphi(t)$, ибо он должен иметь корнем по крайней мере одну из величин (5).

Итак, мы получаем

$$F(t) = [\varphi(t)]^r,$$

где $n = sr$.

§ 12

Резюмируя сказанное в § 11, мы замечаем, что все корни уравнения $f(x) = 0$ можно будет расположить в s систем

$$\begin{array}{c} A = \alpha,\ \alpha_1,\ \alpha_2,\ \ldots,\ \alpha_{r-1} \\ B = \beta,\ \beta_1,\ \beta_2,\ \ldots,\ \beta_{r-1} \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ S = \sigma,\ \sigma_1,\ \sigma_2,\ \ldots,\ \sigma_{r-1} \end{array} \tag{1}$$

по отношению к импримитивному элементу $\psi(\alpha)$ поля $\Omega(\alpha)$.

Системы (1) взяты так, что

$$\begin{array}{c} \psi_1 = \psi(\alpha) = \psi(\alpha_1) = \ldots = \psi(\alpha_{r-1}) \\ \psi_2 = \psi(\beta) = \psi(\beta_1) = \ldots = \psi(\beta_{r-1}) \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \psi_s = \psi(\sigma) = \psi(\sigma_1) = \ldots = \psi(\sigma_{r-1}), \end{array} \tag{2}$$

причем величины (2) суть корни уравнения

$$\varphi(t) = 0$$

неприводимого в поле Ω.

Нетрудно убедиться, что группа Galois уравнения $f(x) = 0$ импримитивна, то есть, не отделяет корней каждой из систем $A, B, \ldots, S$, а каждая подстановка этой группы перемещает лишь корни внутри каждой из систем и переставляет сами системы.

Допустим обратное, что некоторая подстановка S группы Galois распределяет корни одной системы по разным системам. Пусть эта подстановка переводит корень α в β, а корень α_1 в σ.

Применяя подстановку S к соотношению

$$\psi(\alpha) = \psi(\alpha_1)$$

между корнями заданного уравнения, получим

$$\psi(\beta) = \psi(\sigma),$$

что невозможно, ибо мы предполагаем величины ψ_2 и ψ_s, различными между собой.

Итак, мы приходим к теореме.

Импримитивное поле $\Omega(\alpha)$ имеет импримитивную группу.

§ 13

Остается убедиться в справедливости предложения обратного, а именно, что импримитивная группа соответствует импримитивному полю.

Для этой цели достаточно показать, что поле $\Omega(\alpha)$ будет иметь импримитивные элементы, не входящде в состав Ω. Другими словами, достаточно указать элемент поля $\Omega(\alpha)$ удовлетворяющей неприводимому в Ω уравнению, степень которого не равна единице и есть *настоящий* делитель числа n.

Если группа импримитивна, то имеют место соображения § 10. Покажем, что величина y есть как раз такой импримитивный элемент поля $\Omega(\alpha)$, для этой цели достаточно убедиться что функция y, будучи функцией $\alpha, \alpha_1, \alpha_2, \ldots, \alpha_{r-1}$, есть в тоже время *рациональная функция только от одного корня α.*

Рассмотрим уравнение (см. § 10)

$$\psi(\alpha, y) = 0.$$

Величины

$$\psi(\alpha, y_1), \quad \psi(\alpha, y_2), \ \ldots, \ \psi(\alpha, y_{s-1})$$

отличны от нуля, ибо равенство $\psi(\alpha, y_1) = 0$ показывало бы, что α есть корень уравнения $\psi(t, y_1) = 0$, корни которого суть $\beta, \beta_1, \ldots, \beta_{r-1}$. Это невозможно, ибо α не совпадет ни с одним из корней β_i.

Итак, уравнение

$$\psi(\alpha, u) = 0, \tag{1}$$

где u величина неизвестная имеет один только общий корень y с уравнением (4) § 10

$$\varphi(u) = 0. \tag{2}$$

Итак, общий наибольший делитель функций $\psi(\alpha, u)$ и $\varphi(u)$ будет $u - y$. Так как нахождение общего делителя при помощи алгоритма Эвклида сопровождается только рациональнымн выкладками, то y выразится рационально через α, что и требовалось доказать. Итак, обратная теорема оказывается справедливой. Ее можно формулировать так.

Примитивное поле имеет примитивную группу.

§ 14

Докажем следующую в высшей степени важную для дальнейшего теорему.

Теорема. *Транзитивная группа имеет отличного от единицы интранзитивного нормального делителя только в том случае, если она импримитивна.*

Пусть транзитивная группа G имеет интранзитивного нормального делителя H и пусть одна из систем интранзитивности группы H будет

$$A = \alpha,\ \alpha_1,\ \ldots,\ \alpha_{r-1},$$

причем элементы этой системы связаны между собой транзитивно.

Вследствие транзитивности заданной группы G в ней должна существовать подстановка S, переводящая элемент α в произвольный элемент β. Пусть подстановка S переводить элементы системы A в новые

$$B = \beta,\ \beta_1,\ \beta_2,\ \ldots,\ \beta_{r-1}.$$

Очевидно, что должно произойти одно из двух, или системы A и B совпадают, или они не имеют общих элементов. В самом деле, группа H есть нормальный делитель группы G, следовательно, $S^{-1}HS = H$ и значит элементы B будут также перемещаться между собой подобно элементам α. Если существуют в двух системах A и B общие элементы, то обе системы должны совпадать. В самом деле, допустив, что в системе B существуют элементы как из системы A так и новые, мы приходим к невозможному заключению, что элементы системы A могут переходить в элементы, не входящие в состав системы A.

Группа G оказывается, действительно, импримитивною, причем *системы интранзитивности* $A, B, \ldots$ *группы* H *являются системами импримитивности группы* G.

Группа резольвенты

§ 15

Мы сказали уже, что группа уравнения зависит от основного поля Ω, теперь мы будем заниматься вопросом о том, как изменяется группа уравнения от присоединения к полю Ω новых элементов.

Присоединим к основному полю Ω некоторую функцию $\varphi(x_1, x_2, \ldots, x_n)$, принадлежащую к подгруппе H группы Galois заданного уравнения.

Если положено в основу рассуждений некоторое поле Ω, то его элементы и только эти элементы носят название *рациональных величин*, всякая величина, не заключающаяся в поле Ω, будет так называемой *иррациональностью*.

Понятие об иррациональности есть, как мы видим, понятие относительное и зависит от основного поля.

Функция $\varphi(x_1, x_2, \ldots, x_n)$ является иррациональностью, ибо, принадлежа к подгруппе группы уравнения, она не может заключаться в поле Ω.

Иррациональность, подобную функции φ, представляющую из себя рациональную функцию от корней заданного уравнения с *коэффициентами* из Ω мы будем называть *натуральною иррациональностью*. Мы будем называть *побочною* иррациональностью всякую иррациональность другого рода. Так, например, побочными иррациональностями будут корни других уравнений, не выражающиеся

рационально через корни заданного, а также мы будем побочною иррациональностью называть рациональную функций от корней заданного уравнения, в коэффициенты которой входят побочные иррациональности.

§ 16

Посмотрим, что произойдет с группой уравнения от присоединения натуральной иррациональности $\varphi(x_1, x_2, \ldots, x_n)$, принадлежащей точно к подгруппе H.

Покажем прежде всего, что *в новом поле* $\Omega(\varphi)$ *заданное уравнение будет иметь* H *в качестве группы Galois.*

Мы имеем соотношение между корнями $x_1, x_2, \ldots, x_n$ заданного уравнения в новом поле

$$\varphi(x_1, x_2, \ldots, x_n) = k, \tag{1}$$

где k величина из нового поля.

Очевидно, что соотношение (1) *нарушается* от всякой подстановки, не принадлежащей группе H, ибо функция φ численно меняется. Значит при новом поле из группы Galois должны быть *откинуты* все подстановки, не входящие в состав H. Покажем теперь, что группа Galois, соответствующая новому полю будет как раз H. Для этой цели надо убедиться, что всякая подстановка из H не нарушает всех соотношений между корнями с коэффициентами из нового поля.

Пусть выписаны все возможные соотношения между корнями, как *прежние*

$$\mathfrak{a} = 0, \quad \mathfrak{b} = 0, \ldots \tag{2}$$

т. е. имеющие коэффициентами числа основного поля Ω, так и новые

$$\mathfrak{a}' = 0, \quad \mathfrak{b}' = 0, \ldots, \tag{3}$$

т. е. имеющие коэффициентами элементы нового поля $\Omega(\alpha)$.

Рассмотрим одно из новых соотношений (3)

$$\sum \Phi x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n} = 0, \tag{4}$$

в котором коэффициенты Φ суть рациональные функции от φ с коэффициентами из Ω. Заменяя коэффициенты Φ их выражениями через $x_2, x_2, \ldots, x_n$ обратим соотношение (4) в одно из (2). Это соотношение не нарушается от каждой подстановки группы H, ибо эта подстановка есть в тоже время одна из подстановок группы Galois данного уравнения. Кроне того подстановка H не изменяет, очевидно, численной величины коэффициентов Φ, следовательно, соотношение (4) рассматриваемое как соотношение вида (3), т. е. при постоянных Φ не будет тоже нарушаться. Следовательно, группа H будет группой Galois для нового поля.

§ 17

Функция φ будет корнем некоторого уравнения

$$F(\varphi) = 0 \tag{1}$$

степени l, равной индексу группы H по отношению к первоначальной группе Galois.

При решении уравнений 4-ой степени в главе XV мы видели пользу подобных уравнений (1), поэтому естественно, что уравнения, которым удовлетворяют натуральные иррациональности, носят название *резольвент*, то есть уравнений помогающих при решении заданного.

Напомним известные уже нам свойства резольвенты (1).

1) Коэффициенты уравнения (1) суть элементы поля Ω.

2) Все корни $\varphi, \varphi_1, \varphi_2, \ldots, \varphi_{l-1}$ уравнения (1) различны.

3) φ обращается в φ_i при помощи подстановки из сопряженной системы HS_i.

4) Если группа G, соответствующая первоначальному полю разлагается так

$$G = H + HS_1 + HS_2 + + \ldots + HS_{l-1},$$

то все корни $\varphi, \varphi_1, \varphi_2, \ldots, \varphi_{l-1}$ принадлежать группам

$$H, \quad S_1^{-1}HS_1, \quad S_2^{-1}HS_2, \ \ldots, \ S_{l-1}^{-1}HS_{l-1}.$$

В заключение покажем, что уравнение (1) неприводимо в поле Ω. Допустим обратное, а именно, что

$$F(t) = F_1(t)F_2(t).$$

Пусть $F_1(t)$ тот неприводимый в Ω множитель, который имеет корень φ, тогда

$$F_1(\varphi) = 0 \tag{2}$$

будет соотношение между корнями $x_1, x_2, \ldots, x_n$ с коэффициентами из Ω, значит, к этому соотношение» применимы все подстановки первоначальной группы G. Применяя к (2) по одной подстановке из каждой сопряженной системы HS_i, получим

$$F_1(\varphi) = 0, \quad F_1(\varphi_1) = 0, \ \ldots, \ F_1(\varphi_{l-1}) = 0,$$

то есть, $F_1(t)$ имеет все корни функций F, а, так как эти корни различны, то $F_1(t) = F(t)$ и уравнение (1) неприводимо.

§ 18

Найдем теперь группу Galois для резольвенты

$$F(t) = 0.$$

Другими словами, нам надо указать подстановки величин (корней)

$$\varphi, \quad \varphi_1, \ \ldots, \ \varphi_{l-1},$$

не нарушающие всякое существующее между этими величинами соотношение

$$\sum \Psi\varphi^{\beta}\varphi_1^{\beta_1} \cdots \varphi_{l-1}^{\beta_{l-1}} = 0, \tag{1}$$

где Ψ принадлежит к Ω.

Выражая соотношение (1) через $x-1, x_2, \ldots, x_n$, получим соотношение, к которому применимы все подстановки G. Значить, мы приходим к такой теореме.

Группа $\mathfrak{G}$ резольвенты $F(t)=0$ состоит из подстановок ее корней

$$\varphi, \quad \varphi_1, \quad \varphi_2, \ \ldots, \ \varphi_{l-1},$$

которые получаются, если произвести над корнями первоначального уравнения $x_1, x_2, \ldots, x_n$ все подстановки группы G этого уравнения.

§ 19

Рассмотрим группы

$$H, \quad S_1^{-1}HS_1, \quad S_2^{-1}HS_2, \ \ldots, \ S_{l-1}^{-1}HS_{l-1},$$

к которым принадлежать корни

$$\varphi, \quad \varphi_1, \quad \varphi_2, \ \ldots, \ \varphi_{l-1} \tag{1}$$

резольвенты.

Общее пересечение R этих групп есть: 1) нормальный делитель (см. § 46 главы V) группы G, 2) совокупность *тех и только тех* подстановок, при которых не изменяются все величины (1).

Расположим группу G на сопряженные системы по подгруппе R, тогда получим

$$G = R + RT_1 + RT_2 + \ldots + RT_{q-1}.$$

Группа Galois для уравнения $F(t)=0$ имеет, очевидно, порядок q и состоит из тех подстановок, которые производятся в величинах (1) при помощи подстановок

$$I, \quad T_1, \quad T_2, \ \ldots, \ T_{q-1}$$

корней $x_1, x_2, \ldots, x_n$.

Эта группа носит название *Hölder'овского дополнения* нормального делителя R. Мы будем ее обозначать знаком деления групп

$$\frac{G}{R} \quad \text{или} \quad G : R.$$

§ 20

Начнем со случая, когда группа R сводится к единице. Тогда группа резольвенты будет $G : I = G$.

Если мы присоединюсь к Ω все корни $\varphi, \varphi_1, \ldots, \varphi_{l-1}$ резольвенты, то группа уравнения должна понизиться до той, которая оставляет без изменения все эти корни (каждый в отдельности); но $R = I$, следовательно, присоединение всех корней резольвенты сводит группу на единицу и заданное уравнение оказывается решенным.

Такие резольвенты ($R = I$) будем называть *полными*, подчеркивая этим названием ту мысль, что решение заданного уравнения равносильно решений такой полной резольвенты.

Так как группой полной резольвенты является группа G заданного уравнения, то с точки зрения теории Galois решение обоих уравнений является задачей одинаковой трудности. Хотя степени заданного уравнения и полной резольвенты могут быть различны, но им соответствует та же самая группа. Отсюда вытекает, что рассмотрение полных резольвент не подвигает задачу решения уравнения, ибо сводит эту задачу на задачу ей равносильную.

§ 21

Мы будем называть резольвенту *частною*, если группа R не сводится к единице. В этом случае происходить понижение порядка группы уравнения с одной стороны, а с другой стороны достигается та выгода, что группа $G : R$ резольвенты также ниже группы G первоначального уравнения.

Мы замечаем, следовательно, что одновременное присоединение корней частной резольвенты равносильно присоединений одной функции ω принадлежащей группе R. Мы видели уже, что группа R есть нормальный делитель группы G и, значить, ω будет корнем нормального уравнения, т. е. такого, у которого все корни выражаются рационально через один. Итак, от присоединения корня ω некоторого нормального уравнения получается полное решение рассматриваемой частной резольвенты. После решения частной резольвенты и присоединения всех ее корней группа заданного уравнения понижается до R.

§ 22

Задача делается гораздо проще, если R будет совпадать с H, так что подгруппа H сама будет нормальным делителем группы уравнения. В этом случай частная резольвента будет уже сама нормальным уравнением и происходит понижение порядка группы от присоединения одного из ее корней.

§ 23

Будем называть уравнение *простым*, когда его группа простая и *составным*, когда его группа составная (см. § 47 главы V). Очевидно, что простое уравнение может иметь только полные резольвенты, ибо простые группы не имеют отличных от единицы нормальных делителей. Следовательно, нельзя достигнуть понижения группы, какие бы ни присоединять натуральные иррациональности.

Если мы возьмем буквенное уравнение степени выше 4-ой, то после присоединения знакопеременной функции группа сводится на знакопеременную. Вследствие доказанной нами простоты знакопеременной группы рассмотрение резольвент не может принести пользы.

§ 24

Докажем теперь одну теорему относительно группы Hölder'a, которая понадобится в дальнейшем изложении.

Будем называть нормальный делитель H группы G *наибольшим*, если не существует другого нормального делителя $\mathfrak{H}$ заключающего H.

Возможно существование у группы G нескольких различных между собой наи-

больших нормальных делителей.

Теорема. *Если H есть наибольший нормальный делитель группы G, то Hölder'овская группа $G:H$ простая.*

Hölderr'овскую группу можно рассматривать, как группу подстановок сопряженных систем

$$H,\quad HS_1,\quad HS_2,\ \ldots,\ HS_{l-1}, \tag{1}$$

происходящих от умножения справа на подстановки T группы G

$$HT,\quad HS_1T,\quad HS_2T,\ \ldots,\ HS_{l-1}T.$$

Можно еще иначе рассуждать, если установить понятие о *композиции частей* группы G.

Пусть $\mathfrak{A}$ и $\mathfrak{B}$ две совокупности элементов группы G. Не предполагая совокупности $\mathfrak{A}$ и $\mathfrak{B}$ непременно подгруппами, мы можем назвать их *частями* группы G.

Обозначим символом

$$\mathfrak{AB}$$

совокупность выражений

$$AB$$

где элемент A пробегает часть $\mathfrak{a}$, а элемент B часть $\mathfrak{B}$.

Очевидно, что совокупность $\mathfrak{AB}$ будет новою частью группы, которая может быть подгруппой или даже совпадать с G.

Если H есть подгруппа, то, очевидно, будет

$$HH = H.$$

Сопряженные системы (1) будут частями группы G, их можно будет считать элементами Hölder'овской группы, если под композицией этой группы понимать композицию частей, ибо

$$(HS_i)(HS_k) = HHS_iS_k = HS_m.$$

Допустим, что группа $G:H$ не простая, а имеет нормальный делитель

$$H,\quad H\Sigma_1,\quad H\Sigma_2,\ \ldots,\ H\Sigma_{\lambda-1}\qquad(\lambda<l). \tag{2}$$

Покажем, что группа

$$\mathfrak{G} = H + H\Sigma_1 + H\Sigma_2 + \ldots + H\Sigma_{\lambda-1} \tag{3}$$

будет тогда нормальным делителем G и, следовательно, приходим к противоречие с требованием, чтобы H был наибольшим нормальным делителем.

Группа (2) есть нормальный делитель группы (1); будем преобразовывать ее элементы $H\Sigma_i$ при помощи произвольная) элемента HS группы (1).

Элемент H играет в Hölder'оской группе роль единицы; посмотрим, как для элемента HS составить ему обратный HS_0

$$HS_0HS_0 = H,\qquad HHS_0S = HS_0S = H$$

и окончательно

$$HS_0 = HS^{-1}.$$

Итак, преобразовывая при помощи $H\Sigma_i$, получим

$$HS^{-1}H\Sigma_i HS = H\Sigma_k, \tag{4}$$

ибо (2) есть нормальный делитель группы (1).

Равенство (4) можно переписать так

$$S^{-1}H\Sigma_i S = H\Sigma_k.$$

Последнее же равенство равносильно ряду таких равенств

$$S^{-1}T_\alpha\Sigma_i S = T_\beta\Sigma_k, \tag{5}$$

где T_α и T_β суть элементы H.

Равенства (5) показывают, что группа $\mathfrak{G}$ есть нормальный делитель группы G.

Понижение группы от присоединений

§ 25

Мы видели уже случаи, когда рассмотрение натуралькых иррациональностей не приносит пользы для решения уравнения. Является естественным вопрос, не могут ли в таких случаях помочь делу побочные иррациональности. Ответ получается отрицательный, ибо можно показать что *всякое понижение, группы при помощи присоединения побочной иррациональности может быть с таким же успехом достигнуто присоединением натуральной.*

§ 26

Покажем прежде всего, что можно всегда составить рациональную функцию от корней уравнения с коэффициентами из Ω, принадлежащую ко всякой подгруппе H группы Galois.

Составим сначала функцию Galois V, меняющуюся при всех подстановках. Эта функция, очевидно, будет принимать различные значения при всех подстановках группы Galois.

Пусть $V, V_1, V_2, \ldots, V_{q-1}$ суть значения, принимаемые функцией V при подстановках подгруппы H.

Рассмотрим функцию

$$\varphi(u, x_1, x_2, \ldots, x_n) = (u - V)(u - V_1)(u - V_2)\cdots(u - V_{q-1}),$$

где u новая переменная независимая.

Очевидно, что функция φ не меняется от подстановок группы H, ибо от этих подстановок переставляются величины V_i.

От различных сопряженных систем $HS', HS'', \ldots$ будут получаться уже другие функции

$$\varphi' = (u - V')(u - V_1')(u - V_2') \cdots (u - V_{q-1}')$$
$$\varphi'' = (u - V'')(u - V_1'')(u - V_2'') \cdots (u - V_{q-1}'')$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

Подбираем u таким образом, чтобы не удовлетворялось ни одно из уравнений

$$\varphi - \varphi' = 0, \quad \varphi - \varphi'' = 0, \quad \varphi' - \varphi'' = 0, \ \ldots \tag{1}$$

Такой подбор можно сделать на бесчисленное число способов, даже давая букве u рациональные значения, ибо ни в одном из уравнений (1) буква, рассматриваемая как переменная, не может сократиться.

Итак функция φ *точно* принадлежит группе H.

§ 27

Допустим теперь, что произошло понижение группы уравнения от присоединения побочной иррациональности ζ, которую мы будем предполагать корнем уравнения

$$F(\zeta) = 0 \tag{1}$$

степени m с коэффициентами из поля Ω, которое для общности мы будем предполагать или первоначалым или расширенным при помощи таких иррациональностей, которые не изменили группы уравнения.

Введем в рассмотрение *резольвенту Galois*.

Пусть ξ есть функция Galois (см. § 3).

Возьмем основную функцию

$$G(\eta) = (\eta - \xi)(\eta - \xi') \cdots (\eta - \xi^{N-1}).$$

Если уравнение имеет аффект, то функция G приводима в поле Ω. Ее неприводимый множитель $g(\eta)$ дает резольвенту Galois

$$g(\eta) = 0.$$

Если обозначить через j индекс группы уравнения по отношению ко всей симметрической группе, то нетрудно показать, что функция $G(\eta)$ раскладывается на j неприводимых множителей

$$G(\eta) = g(\eta) g_1(\eta) g_2(\eta) \cdots g_{j-1}(\eta)$$

одинаковых степеней.

Рассмотрим, в самом деле, множитель $g_(\eta)$, пусть один из корней этого множителя будет $\xi^{(\alpha)}$, но, принимая во внимание, что $\xi^{(\alpha)}$ есть рациональная функция от корней x_i, а эти последние выражаются рационально через ξ, то мы получаем

$$\xi^{(\alpha)} = \vartheta(\xi),$$

где $\vartheta(t)$ знак рациональной в Ω функции от переменного независимого t.

Итак, мы имеем тождество

$$g_i(\vartheta(\xi)) = 0. \tag{2}$$

Применяя к соотношению (2) все подстановки группы Galois, получим

$$g_i(\theta(\xi)) = 0, \quad g_i(\vartheta(\xi')) = 0, \ \ldots, \ g_i(\vartheta(\xi^{\nu-1})) = 0, \tag{3}$$

где $\xi, \xi', \ldots, \xi^{\nu-1}$ суть все корни резольвенты Galois $g(\eta) = 0$.

Соотношения (3) показывают, что будет

$$g_i(\eta) = [\eta - \vartheta(\xi)][\eta - \vartheta(\xi')] \cdots [\eta - \vartheta(\xi^{\nu-1}],$$

ибо правая часть, будучи симметрической функцией корней резольвенты $g(\eta) = 0$, будет целою в Ω функцией степени ν от независимой переменной η.

Итак, все множители $g_i(\eta)$ имеют одну и ту же степень ν и неприводимы на основании формул (3), поэтому за резольвенту Galois можно выбрать любой из них

$$g_i(\eta) = 0. \tag{4}$$

Покажем, что группа Galois не зависит от выбора значка i. Это очевидно из того соображения, что переход от одного корня $\vartheta(\xi)$ новой резольвенты (4) к другим ее корням $\vartheta(\xi'), \vartheta(\xi''), \ldots$ равносилен переходу от корня ξ первоначальной резольвенты к ее другим корням $\xi', \xi'', \ldots$.

§ 28

Предположим, что присоединение ζ понизило группу уравнения с G на ее подгруппу H индекса l.

Покажем, что при понижении порядка группы *неприводимая* в первоначальном поле резольвента $g(\eta) = 0$ должна сделаться *приводимою* в новом поле. В самом деле, полагая $\nu = l\mu$, где μ порядок подгруппы H, обозначим подстановки H таким образом

$$[\xi, \xi], \quad [\xi, \xi_1], \ \ldots, \ [\xi, \xi_{\mu-1}], \tag{1}$$

где $\xi, \xi_1, \ldots, \xi_{\mu-1}$ суть некоторые из корней $g(\eta) = 0$.

Не трудно видеть, что в новом поле будет иметь рациональные коэффициенты целая функция

$$(\eta - \xi)(\eta - \xi_1) \cdots (\eta - \xi_{\mu-1}), \tag{2}$$

ибо применение подстановок группы (1) не изменяет функции (2), а тогда по теореме § 15 главы XVI функции (2) имеет коэффициенты из нового поля $\Omega(\zeta)$. Обозначим поэтому функцию (2) так

$$g(\eta, \zeta), \tag{3}$$

не забывая, что степень ее равна μ (порядку группы H). Функция (3), очевидно, неприводимая, ибо, если бы мы обозначили в обратном случае ее неприводимый множитель через $g_1(\eta, \zeta)$ причем того, который обращает в нуль при $\eta = \xi$, получили бы тождество

$$g_1(\xi, \zeta) = 0; \tag{4}$$

к тождеству (4) можно применить подстановки новой группы Galois H и мы получим

$$g_1(\xi, \zeta) = 0, \quad g_1(\xi_1, \zeta) = 0, \ \ldots, \ g_1(\xi_{\mu-1}, \zeta) = 0,$$

т. е. g_1 совпадает с g.

Повторяя рассуждение § 24, замечаем, что резольвента Galois $g(\eta) = 0$, распадается в новом поле $\Omega(\zeta)$ на l неприводимых множителей степени μ каждый

$$g(\eta) = g(\eta, \zeta) g_1(\eta, \zeta) \cdots g_{l-1}(\eta, \zeta),$$

приравнивая один из этих множителей нулю, получаем новую резольвенту Galois

$$g(\eta, \zeta) = 0 \tag{5}$$

для нового поля $\Omega(\zeta)$.

Пусть множители

$$g(\eta, \zeta), \quad g_1(\eta, \zeta), \ \ldots, \ g_{l-1}(\eta, \zeta) \tag{6}$$

соответствуют сопряженным системам

$$H, \quad HS_1, \ \ldots, \ HS_{l-1}. \tag{7}$$

Возьмем *натуральную* иррациональность φ относящуюся по коэффициентам к полю Ω и принадлежащую *точно* к групп H.

Пусть различные значения φ, относящиеся к системам (7), будут

$$\varphi, \quad \varphi_1, \ldots, \ \varphi_{l-1};$$

по теореме о функциях относящихся к одной и той же группе получим

$$g(\eta, \zeta) = \gamma(\eta, \varphi), \quad g_1(\eta, \zeta) = \gamma(\eta, \varphi_1), \ \ldots, \ g_{l-1}(\eta, \zeta) = \gamma(\eta, \varphi_{l-1}),$$

γ есть знак рациональной функции от φ, причем вследствие произвольности η, функция γ остается функцией степени μ от η.

Функции (6) от η все различные, поэтому можно подобрать такое рациональное значение a для η, чтобы были различными все числа

$$g(a, \zeta), \quad g_1(a, \zeta), \ldots, \ g_{l-1}(a, \zeta).$$

Очевидно, что, если мы обозначим через $\Phi(u) = 0$, то уравнение из поля Ω, которому удовлетворяет натуральная иррациональность φ, то уравнение

$$g(a, \zeta) = \gamma(a, u)$$

имеет один только общий корень φ с уравнением $\Phi(u) = 0$; отыскивая общий наибольший делитель $u - \varphi$ двух уравнений при помощи последовательного деления, выразим φ рационально через ζ.

Итак, φ есть элемент поля $\Omega(\zeta)$.

Если φ будет *примитивный* элемент поля, то поле $\Omega(\zeta) = \Omega(\varphi)$, так что ζ есть рациональная функция от φ. В этом случае ζ есть *натуральная* иррациональность и мы имеем $m = l$.

Если ζ будет *побочною* иррациональностью, то φ будет *импримитивным* элементом поля $\Omega(\zeta)$. На основании сказанного в § 10 получаем

$$m = l\lambda, \tag{8}$$

где λ целое число.

Если число m простое, то уравнение (8) возможно лишь в случае $\lambda = 1$ и мы приходим к теореме, которую мы применним в дальнейшем изложении.

Если группа понижается от присоединения корня ζ простой степени, то ζ есть натуральная иррациональность.

§ 29

Резюмируя сказанное в предыдущем параграфе, приходим в теореме.

I. *Всякое возможное понижение группы Galois можно произвести присоединением натуральной иррациональности.*

II. *Если l есть индекс пониженной группы по отношению к первоначальной, то понижение возможно только через присоединение корня уравнения, степень которого есть число кратное l.*

III. *Если степень уравнения есть l, то присоединяемый его корень есть натуральная иррациональность.*

§ 30

В заключение дадим еще одно более простое доказательство теоремы § 82 главы XIII.

Пусть α, β суть корни двух неприводимых в Ω уравнений.

Поле $\Omega(\alpha, \beta)$ получается, или от присоединения к полю $\Omega(\alpha)$ корня β, или же от присоединения к полю $\Omega(\beta)$ корня α.

Если от присоединения к полю $\Omega(\alpha)$ корня β получится инпримитивное поле, то таково же будет поле, получаемое от присоединения α к полю $\Omega(\beta)$.

§ 31

Теорема. *Если группа G подстановок корней заданного уравнения обладает двойным свойством:* 1) *каждая из ее подстановок не нарушает всех соотношений между корнями и* 2) *функция, не изменяющаяся от всех подстановок G, есть элемент основного поля; то группа G есть группа Galois для заданного уравнения.*

Из первого свойства следует, что группа G является делителем группы Galois. Остается убедиться, что второе свойство влечет как следствие тождественность

группы G с группой Galois. Возьмем функцию ξ (см. § 3 главы XVII) и пусть ее значения, соответствующая подстановкам G, будут

$$\xi,\ \ \xi_1,\ \ \xi_2,\ \ldots,\ \xi_{m-1}. \tag{1}$$

Тогда целая функция

$$g(t) = (t-\xi)(t-\xi_1)\cdots(t-\xi_{m-1})$$

будет *действительно*, резольвентой Galois, ибо на оснований второго свойства функция $g(t)$ принадлежит к основному полю. Она неприводима в этом поле, ибо величины (1) изменяются транзитивно от подстановок группы G.

Глава XVIII

Классические виды уравнений, решаемых в радикалах

Нормальные уравнения

§ 1

В следующей главе мы докажем теорему Abel'я, что буквенные уравнения выше четвертой степени не решаются в радикалах. Так как решимость в радикалах, как мы в следующей главе увидим, связана неразрывно с известными свойствами группы уравнения, то теорему Abel'я можно будет формулировать так: *уравнения выше четвертой степени и без аффекта не решаются в радикалах.*

Является задачей первостепенной важности указать на численные уравнения, *имеющие аффект* и решающиеся в радикалах. В настоящей главе мы будем рассматривать наиболее важные виды уравнений, решающихся в радикалах.

§ 2

Мы назвали *нормальным* неприводимое уравнение, все корни которого выражаются рационально через один из них.

Рассмотрим конструкцию группы нормального уравнения.

Если мы обозначим через G_0 подгруппу группы G неприводимого уравнения, оставляющую на месте корень x_0, то получим следующее разложение на сопряженные системы

$$G = G_0 + G_0S_1 + G_0S_2 + \ldots + G_0S_{n-1},$$

где S_1 подстановка, переводящая корень x_0 в x_1, S_2 переводит x_0 в x_2, и так далее, наконец, S_{n-1} переводит x_0 в x_{n-1}.

Так как группа неприводимого уравнения *транзитивна*, то подстановки $S_1, S_2, \ldots, S_{n-1}$ должны в ней существовать.

Итак, мы приходим к теореме.

Группа неприводимою уравнения имеет порядок, делящийся на степень n уравнения.

Если мы эту теорему желаем высказать относительно групп подстановок без связи с уравнениями, то получаем следующую формулировку.

Порядок всякой транзитивной группы подстановок делится на число переставляемых элементов.

§ 3

Если неприводимое уравнение *нормально*, то подгруппа G_0, оставляющая без изменения корень x_0, *должна сводиться к единичной подстановке*, ибо при неизменности корня x_0 должны оставаться без изменения и остальные корни $x_1, x_2, \ldots, x_{n-1}$, выражающееся рационально через x_0. Группа уравнения будет состоять, следовательно, из подстановок

$$G = I + S_1 + S_2 + \ldots + S_{n-1},$$

и мы приходим к теореме.

Группа нормального уравнения имеет порядок, равный степени уравнения.

Абелевы уравнения

§ 4

Определение. Мы назовем Abel'евым всякое уравнение n-ой степени $f(x) = 0$, если каждый из корней его выражается рационально через один. Причем, если это рациональное выражение имеет вид

$$x_1 = \mathfrak{D}(x_0), \quad x_2 = \mathfrak{D}_2(x_0), \ \ldots, \ x_{n-1} = \mathfrak{D}_{n-1}(x_0),$$

то между функциями $\mathfrak{D}_i$ должна существовать зависимость

$$\mathfrak{D}_i[\mathfrak{D}_k(x_0)] = \mathfrak{D}_k[\mathfrak{D}_i(x_0)], \tag{1}$$

имеющая место для каждых двух функций $\mathfrak{D}_i$ и $\mathfrak{D}_k$.

Конечно, коэффициенты рациональных функций $\mathfrak{D}_i$ должны принадлежать к некоторому основному полю Ω.

Так, например, уравнение $x^n - 1 = 0$ деления круга есть Abel'ево при основном поле рациональных чисел, ибо, если мы обозначим через r первообразный корень, то всякий другой корень будет иметь вид $\mathfrak{D}_i(r) = r^i$ и, следовательно, соотношение (1) удовлетворяется

$$\mathfrak{D}_i\mathfrak{D}_k(r) = \mathfrak{D}_k\mathfrak{D}_i(r) = r^{ik}.$$

Подобным же образом всякое двучленное уравнение

$$x^n - a = 0 \tag{2}$$

будет Abel'евым, если основное поле Ω заключает корни n-ой степени из единицы. Обозначая первообразный из этих корней через r, мы можем сказать, что корни уравнения (2) выражаются рационально через один

$$\mathfrak{D}_i(x_0) = r^i x_0,$$

и соотношение (1) имеет место

$$\mathfrak{D}_i\mathfrak{D}_k(x_0) = \mathfrak{D}_k\mathfrak{D}_i(x_0) = r^{ik}x_0.$$

§ 5

Покажем теперь, что группа Abel'ева уравнения коммутативная[92].

Пусть $\varphi(x)$ будет неприводимый множитель первой части $f(x)$ Abel'ева уравнения, причем этот множитель тот, которому удовлетворяет корень x_0. Пусть остальные корни функции $\varphi(x)$ будут $x_1, x_2, \ldots, x_{m-1}$. Тогда мы имеем по определению

$$x_1 = \mathfrak{D}_1(x_0), \quad x_2 = \mathfrak{D} + 2(x_0), \ \ldots, \ x_{m-1} = \mathfrak{D}_{m-1}(x_0).$$

Уравнение $\varphi(x) = 0$, будучи нормальным, имеет группу, состоящую из преобразований

$$\Sigma_0 = (x_0 x_0), \quad \Sigma_1 = (x_0 x_1), \ \ldots, \ \Sigma_{m-1} = (x_0 x_{m-1}).$$

Эта группа, очевидно, коммутативная, ибо

$$\Sigma_i = (x_0 x_i) = [x_0, \mathfrak{D}_i(x_0)],$$
$$\Sigma_k = (x_0, x_k) = [x_0, \mathfrak{D}_k(x_0)].$$

Отсюда

$$\Sigma_i \Sigma_k = [x_0, \mathfrak{D}_i(x_0)][\mathfrak{D}_i(x_0), \mathfrak{D}_i\mathfrak{D}_k(x_0)] = [x_0, \mathfrak{D}_i\mathfrak{D}_k(x_0)],$$
$$\Sigma_k \Sigma_i = [x_0, \mathfrak{D}_k(x_0)][\mathfrak{D}_k(x_0), \mathfrak{D}_k\mathfrak{D}_i(x_0)] = [x_0, \mathfrak{D}_k\mathfrak{D}_i(x_0)].$$

На основами (1) § 4 получим

$$\Sigma_i \Sigma_k = \Sigma_k \Sigma_i,$$

и группа оказывается, действительно, коммутативною.

§ 6

Теорема. *Неприводимое уравнение $\varphi(x) = 0$ с коммутативною группой будет Abel'евым.*

Пусть G_0 будет подгруппа группы нашего уравнения, оставляющая без изменения корень x_0. На основании транзитивности группы G Galois имеем

$$G = G_0 + G_0 S_1 + G_0 S_2 + \ldots + G_0 S_{n-1},$$

где подстановка S_i перемещает корень x_0 в x_i.

Очевидно, что группа, оставляющая корень x_i без перемены будет (см. § 19, глава XV)

$$S_i^{-1} G_0 S_i.$$

На основании коммутативности группы G имеем

$$S_i^{-1} G_0 S_i = S_i^{-1} S_i G_0 = G_0,$$

то есть, группа G_0 не меняет также x_i. Так как значок i взят произвольно, то группа G_0 не меняет всех корней и сводится к единице.

[92] Отсюда происходит название Abel'евой группы. Надо принять, кроме того, в соображение, что Abel'ево уравнение нормальное, и следовательно, резольвентой является один из его неприводимых множителей.

Итак, группа Galois заданного уравнения будет

$$I, \quad S_1, \quad S_2, \ \ldots, \ S_{n-1}.$$

Если мы присоединим к основному полю Ω корень x_0 уравнения $\varphi(x) = 0$, то группа должна сводиться к единице, значит, в поле $\Omega(x_0)$ должны заключаться все остальные корни.

Уравнение $\varphi(x) = 0$ оказывается нормальным и является своей собственной резольвентой Galois.

Если мы положим $x_i = \mathfrak{D}_i(x_0)$, то группа Galois будет состоять из подстановок

$$\Sigma_i = [x_0, \mathfrak{D}_i(x_0)].$$

Мы имеем

$$\Sigma_i\Sigma_k = [x_0, \mathfrak{D}_i\mathfrak{D}_k(x_0)], \qquad \Sigma_k\Sigma_i = [x_0, \mathfrak{D}_k\mathfrak{D}_i(x_0)];$$

вследствие коммутативности группы получаем

$$\mathfrak{D}_i\mathfrak{D}_k(x_0) = \mathfrak{D}_k\mathfrak{D}_i(x_0),$$

и уравнение Abel'ево.

§ 7

Приводимое уравнение с коммутативной группой может и не быть Abel'евым. Мы приходим к теореме.

Если приводимое уравнение $f(x) = 0$ имеет коммутативную группу, то всякий неприводимый множитель φ функции $f(x)$ дает Abel'ево уравнение $\varphi = 0$.

В самом деле, пусть группа заданного уравнения $f(x) = 0$ есть G. Мы получим группу уравнения $\varphi(x) = 0$, если рассмотрим совокупность G' подстановок, которые происходят среди корней $\varphi(x) = 0$ от применения подстановок группы G. Очевидно, что если группа G коммутативна, то такова же и группа G'.

Сведение Abel'евых уравнений на циклические

§ 8

Мы видели уже, что в транзитивной Abel'евой группе не существует кроме единицы другой подстановки, оставляющей без изменения один из корней. Рассмотрим разложение подстановки S Abel'евой группы на циклы

$$S = C_1C_2\cdots C_s;$$

пусть C_1 есть цикл, порядок которого r не выше порядков других циклов. В нашей группе должна существовать подстановка

$$S^r = C_1^rC_2^r\cdots C_s^r.$$

Но $C_1^r = I$ и не меняет корней, входящих в состав цикла C_1, следовательно, $S^r = I$. То есть, все циклы S должны иметь один и тот же порядок r и мы приходим к теореме.

Всякая подстановка, входящая в состав транзитивной Abel'евой группы должна быть правильною (см. § 15 главы V).

§ 9

Итак, рассмотрим одну из подстановок

$$S = C_1 C_2 \cdots C_s$$

рассматриваемой группы заданного Abel'ева уравнения $f(x) = 0$, где циклы C_i суть

$$\begin{aligned} C_1 &= (\alpha, \alpha_1, \ldots, \alpha_{r-1}, \\ C_2 &= (\beta, \beta_1, \ldots, \beta_{r-1}), \\ &\ldots\ldots\ldots\ldots\ldots\ldots, \\ C_s &= (\sigma, \sigma_1, \ldots, \sigma_{r-1}) \qquad (\alpha_i, \beta_i, \sigma_i \text{ суть корни } x_0, x_1, \ldots, x_{n-1}. \end{aligned}$$

В § 20 главы V мы видели, что всякая другая подстановка T нашей группы, перестановочная, следовательно, с S, должна производить только циклическое перемещение букв каждого цикла C_i, и подстановку самих циклов. Так как при этом не будет происходить смещения букв различных циклов, то при $s > 1$ группа нашего уравнения будет, очевидно, *импримитивная*.

§ 10

Функцию $\omega(\xi_1, \xi_2, \ldots, \xi)$ мы будем называть *циклическою*, если она не изменяется от циклической подстановки $(\xi_1, \xi_2, \ldots, \xi)$.

Обозначим

$$(1)\quad \omega = \omega(\alpha, \alpha_1, \ldots, \alpha_{r-1}),\quad \omega_1 = \omega(\beta, \beta_1, \ldots, \beta_{r-1}),\ \ldots,\ \omega_{s-1} = \omega(\sigma, \sigma_1, \ldots, \sigma_{r-1}).$$

Эти величины суть корни уравнения

$$(2)\qquad F(\eta) = 0$$

степени s, коэффициенты которого, будучи симметрическими функциями от величин $\omega, \omega_1, \ldots, \omega_{s-1}$, не меняются при всех подстановках группы Galois заданного Abel'ева уравнения. Итак, это уравнение (2) есть уравнение в поле Ω. На основании соображений § 9 главы XVII оно будет неприводимо.

Группой уравнения (2) будет совокупность подстановок величин (1) при применении к ним подстановок S_i группы заданного уравнения. Коммутативность группы заданного уравнения влечет, очевидно, за собой коммутативность группы уравнения (2).

Итак, *уравнение* (2) *есть Abel'ево, ибо оно неприводимое и имеет коммутативную группу.*

Присоединение к основному полю Ω величины со разбивает заданное уравнение на s множителей

$$f(x) = f(x, \omega) f(x, \omega_1) \cdots f(x, \omega_{s-1}) = 0.$$

Уравнение $f(x,\omega)=0$ имеет корни $\alpha,\alpha_1,\ldots,\alpha_{r-1}$, причем его группа состоит из периода одного цикла

$$C_1=(\alpha,\alpha_1,\ldots,\alpha_{r-1}).$$

Тоже самое относится и к другим множителям. Корни $f(x,\omega_1)=0$ будут $\beta,\beta_1,\ldots,\beta_{r-1}$, и так далее.

§ 11

Мы будем называть *циклическим* уравнение, когда его группа состоит из *степеней одного цикла.*

В предыдущем параграфе мы видели, что первоначальное Abel'ево уравнение $f(x)=0$ степени $n=rs$ привелось к решению одного Abel'ева уравнения $F(\eta)=0$ степени s и ряда циклических уравнений $f(x,\omega_i)=0$ степени r. Мы можем подобным же образом свести задачу решения Abel'ева уравнения $F(\eta)=0$ степени $s=s_1s_2$ на решение Abel'ева уравнения степени s_1, и на решение s_1 циклических уравнений степени s_2.

Продолжая далее, мы можем придти к решению *Abel'ева уравнетя простой степени* p, которое будет само *циклическим*, ибо можно доказать теорему.

Всякое нормальное уравнение простой степени есть циклическое.

Пусть S есть одна из отличных от единицы подстановок группы такого уравнения. Порядок подстановки S должен быть делителем порядка группы. Порядок же группы есть простое число, равное степени p уравнения. Единственным делителем p отличным от единицы является само число p, следовательно, группа уравнения состоит из степеней $I,S,S^2,\ldots,S^{p-1}$ и уравнение циклическое.

Итак, мы приходим к следующему окончательному выводу.

Решение Abel'ева уравнения приводится к решению ряда циклических, степени которых суть делители степени заданного Abel'ева уравнения.

§ 12

Покажем теперь, *что можно привести циклическое уравнение составной степени к решению ряда циклических уравнений простой степени.*

Возьмем некоторое циклическое уравнение $f(x)=0$ составной степени $n=ef$, его группа G состоит из степеней одного цикла

$$S=(x_0,x_1,\ldots,x_{n-1}).$$

Подстановка S^e распадается на e циклов порядка f:

$$S^e=C_0C_1C_2\cdots C_{s-1},$$

где

$$\begin{aligned}
C_0 &= (x_0,x_e,x_{2e},\ldots,x_{(f-1)e}),\\
C_1 &= (x_1,x_{e+1},x_{2e+1},\ldots,x_{(f-1)e+1}),\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\
C_{e-1} &= (x_{e-1},x_{2e-1},x_{3e-1},\ldots,x_{n-1}).
\end{aligned}$$

Возьмем циклическую функцию $\omega(\xi_1, \xi_2, \ldots, \xi_f)$ и обозначим

$$(1)\qquad \begin{aligned} \eta &= \omega(x_0, x_e, x_{2e}, \ldots, x_{(f-1)e}),\\ \eta_1 &= \omega(x_1, x_{e+1}, x_{2e+1}, \ldots, x_{(f-1)e+1}),\\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\ \eta_{e-1} &= \omega(x_{e-1}, x_{2e-1}, x_{3e-1}, \ldots, x_{n-1}). \end{aligned}$$

Величины $\eta, \eta_1, \ldots, \eta_{s-1}$ все различны между собой, ибо они суть корни неприводимого в Ω уравнения

$$(2)\qquad F(t) = (t-\eta)(t-\eta_1)\cdots(t-\eta_{e-1}) = 0$$

степени e. Неприводимость уравнения (2) следует из транзитивности группы G, ибо корень x_0 переходить в x_i от подстановки S^i, значить, η должна переходить во все остальные величины (1).

Что коэффициенты уравнения (2) находятся в поле Ω, следует из того соображения, что подстановка S производит циклическое перемещение величин $\eta, \eta_1, \eta_2, \ldots, \eta_{e-1}$. *Уравнение* (2) *циклическое.*

Все величины η_i выражаются рационально через одну из них, например, η, так что присоединение к полю Ω величины η равносильно присоединению всех остальных. Сказанное следует из того, что всякое *циклическое* уравнение есть в тоже время *Abel'ево.*

В поле $\Omega(\eta)$ заданное уравнение $f(x) = 0$ разбивается на e множителей

$$f(x) = f(x,\eta)f(x,\eta_1)\cdots f(x,\eta_{e-1}) = 0,$$

где

$$f(x,\eta_i) = (x-x_i)(x-x_{e+i})\cdots(x-x_{(f-1)e+i}).$$

Каждое из уравнений

$$f(x,\eta_i) = 0$$

есть циклическое, ибо его группа Galois состоит из степеней цикла G_i.

Резюмируя сказанное, приходим к заключению, *что всякое циклическое уравнение степени n приводится к решению ряда циклических уравнений, степени которых суть простые множители числа n.*

Если степень n есть 2^k, то решение приведет к формуле заключающей только квадратные радикалы. Таким путем была решена Gauss'ом[93] задача построения правильного 17-ти угольника, или иначе, задача деления окружности на 17 равных частей.

§ 13

Перейдем теперь к доказательству возможности решения в радикалах циклического уравнения простой степени. Таким путем будет доказано, что всякое Abel'ево уравнение решается в радикалах.

[93] Gauss. Disquisitiones arithmeticae. Sectio VII.

§ 14

Рассмотрим функцию

$$(\varepsilon, x_0) = x_0 + \varepsilon x_1 + \ldots + \varepsilon^{n-1} x_{n-1}, \tag{1}$$

где n есть некоторое простое число, ε первообразный корень n-ой степени из единицы, а $x_0, x_1, \ldots, x_{n-1}$ суть корни заданного циклического уравнения степени n.

От применения к функции (1) циклической подстановки

$$S = (x_0, x_1, \ldots, x_{n-1})$$

эта функция получает, очевидно, множитель ε^{-1}, то есть, она обращается после подстановки в величину

$$\varepsilon^{-1}(\varepsilon, x_0).$$

Из сказанного вытекает, что функция

$$(\varepsilon, x_0)^n \tag{2}$$

не меняется от подстановок группы заданного уравнения.

В дальнейшем изложении мы покажем, что всякий корень ε простой степени n из единицы выражается в радикалах. Присоединим теперь к полю Ω корень ε и будем рассматривать новое поле $\Omega(\varepsilon)$.

Так как в формуле (2) безразлично, который из первообразных корней взять за ε, то мы можем ε заменить на ε^r. На основании неизменности величины (2) от подстановок x_i группы данного уравнения замечаем, что величина (2) есть элемент поля $\Omega(\varepsilon)$.

Мы получаем, следовательно,

$$(\varepsilon^r, x_0^n) = B_r,$$

где B_r есть элемент поля $\Omega(\varepsilon)$, то есть, на основании сказанного величина, выражающаяся в радикалах.

Мы приходим к равенствам

$$\begin{aligned}
&(1, x_0) = x_0 + x_1 + x_2 && + \ldots + x_{n-1} && = -a_1,\\
&(\varepsilon, x_0) = x_0 + \varepsilon x_1 + \varepsilon^2 x_2 && + \ldots + \varepsilon^{n-1} x_{n-1} && = \sqrt[n]{B_1}\\
&(\varepsilon^2, x_0) = x_0 + \varepsilon^2 x_1 + \varepsilon^4 x_2 && + \ldots + \varepsilon^{2(n-1)} x_{n-1} && = \sqrt[n]{B_2},\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\
&(\varepsilon^{n-1}, x_0) = x_0 + \varepsilon^{n-1} x_1 + \varepsilon^{2(n-1)} x_2 && + \ldots + \varepsilon^{(n-1)^2} x_{n-1} && = \sqrt[n]{B_{n-1}},
\end{aligned} \tag{3}$$

где a_1 — коэффициент заданного уравнения при неизвестном в степени $n-1$.

Принимая во внимание очевидное равенство

$$1 + \varepsilon^r + \varepsilon^{2r} + \ldots + \varepsilon^{(n-1)r} = \frac{\varepsilon^{nr} - 1}{\varepsilon^r - 1} = 0 \qquad (r < n)$$

и складывая наши уравнения (3), мы получаем

$$nx_0 = -a_1 + \sqrt[n]{B_1} + \sqrt[n]{B_2} + \ldots + \sqrt[n]{B_{n-1}}. \tag{4}$$

Подобным образом, умножая уравнения (3) на $1, \varepsilon^{-r}, \varepsilon^{-2r}, \ldots, \varepsilon^{-(n-1)r}$ и складывая, находим

$$nx_r = -a_1 + \varepsilon^{-r}\sqrt[n]{B_1} + \varepsilon^{-2r}\sqrt[n]{B_2} + \ldots + \varepsilon^{-(n-1)r}\sqrt[n]{B_{n-1}}. \tag{5}$$

Итак, корни x_i заданного циклического уравнения выражаются в радикалах.

§ 15

Решение в радикалах циклического уравнения простой степени, данное в предыдущем параграфе, заслуживает некоторого весьма важного добавления.

С первого взгляда может показаться, что в уравнений (5) предыдущего параграфа слишком много радикалов, но не трудно убедиться, что все радикалы $\sqrt[n]{B_i}$ выражаются рационально через один из них, например, $\sqrt[n]{B_1}$.

В самом деле, выражение

$$(\varepsilon^r, x_0)(\varepsilon, x_0)^{n-r} \tag{1}$$

не меняется от подстановки группы G, ибо подстановка S соответствует, как было сказано, умножение функции (ε, x_0) на ε^{-1} и, следовательно, функция (1) получает множитель

$$\varepsilon^{-r} \cdot (\varepsilon^{-1})^{n-r} = \varepsilon^{-n} = 1.$$

Итак, выражение (1) должно быть элементом C_r поля $\Omega(\varepsilon)$.

Мы получаем

$$(\varepsilon^r, x_0)(\varepsilon, x_0)^{n-r} = C_r,$$

т. е.

$$\sqrt[n]{B_r} \cdot \sqrt[n]{B_1^{n-r}} = C_r,$$

или окончательно

$$\sqrt[n]{B_r} = \frac{C_r}{B_1}(\sqrt[n]{B_1})^r.$$

Значит, мы получаем следующее выражение для корня

$$x_r = \frac{1}{n}\left\{ -a_1 + \varepsilon^{-r}\sqrt[n]{B_1} + \varepsilon^{-2r}\frac{C_2}{B_1}(\sqrt[n]{B_1})^2 + \ldots + \varepsilon^{-(n-1)r}\frac{C_{n-1}}{B_1}(\sqrt[n]{B_1})^{n-1} \right\}. \tag{2}$$

Это выражение заключает один только радикал $\sqrt[n]{B_1}$, и, следовательно, давая радикалу n его различных значений получим все n корней заданного циклического уравнения.

§ 16

Так как величина B_1 находится в знаменателях дробных выражений формулы (2) § 15, то нужно показать, что она не равна нулю. Другими словами надо

показать, что выбором первообразного корня ε можно сделать B_1 отличным от нуля.

Мы имеем, очевидно,

$$nx_0 = \sum_{\lambda=0}^{\lambda=n-1} (\varepsilon^\lambda, x_0), \qquad nx_k = \sum_{\lambda=0}^{\lambda=n-1} \varepsilon^{-\lambda k}(\varepsilon^\lambda, x_0).$$

Откуда

$$n(x_k - x_0) = \sum_{\lambda=1}^{\lambda=n-1} (\varepsilon^{-\varepsilon k} - 1)(\varepsilon^\lambda, x_0).$$

Все функции $(\varepsilon^\lambda, x_0)$ не могут равняться нулю, ибо тогда было бы $x_k = x_0$, что противоречить неприводимости заданного циклического уравнения.

Значит, при некотором значений λ_0 функция $(\varepsilon^{\lambda_0}, x_0)$ отлична от нуля, эту то функцию и можно принять за B_1, а за ε взять ε^{λ_0}.

§ 17

Нетрудно видеть, что решение циклического уравнения, приведенное в §§ 14, 15, 16 сохраняется во всех деталях и при n — составном.

В этом случай можно убедиться также, что выбором первообразного корня ε можно достигнуть неравенства нулю выражения B_1.

Доказательство этого обстоятельства при n — составном было дано Weber'ом[94].

Резольвенты Lagrange'а

§ 18

Резольвентами Lagrange'а называются выражения

$$(\varepsilon, x_0) = x_0 + \varepsilon x_1 + \ldots + \varepsilon^{m-1} x_{m-1},$$

где ε есть *произвольный* корень m-ой степени из единицы.

Мы имеем

$$\sum_\varepsilon \varepsilon^k = m,$$

или

$$\sum_\varepsilon \varepsilon^k = 0,$$

где суммы распространены на все корни ε m-ой степени из единицы. Причем сумма будет равна m, если k делится на m и равняться нулю, если k не делится на m (См. § 6 главы IX).

Отсюда, как мы видели раньше, получаем:

$$(1) \qquad \begin{aligned} mx_0 &= \sum_\varepsilon (\varepsilon, x_0), \\ mx_k &= \sum_\varepsilon \varepsilon^{-k}(\varepsilon, x_0). \end{aligned}$$

[94]Weber. Lehrbuch der Algebra. 1898. B. I, S. 590.

Если ε — первообразный корень, то формулы (1) можно переписать так

$$(2)\qquad \begin{aligned} mx_0 &= \sum_{\lambda}(\varepsilon^{\lambda}, x_0),\\ mx_k &= \sum_{\lambda}\varepsilon^{-\lambda k}(\varepsilon^{\lambda}, x_0). \end{aligned}$$

Итак, мы видим, что, если резольвенты Lagrange'а известны, то известны также и легко определяются и корни по формулам (1) и (2).

§ 19

Резольвенты Lagrange'а представляют из себя весьма важный алгоритм для вычисления функций от корней, обладающих известными свойствами.

Итак, будем резольвенту обозначать

$$(\varepsilon, x_0) = \sum_{h=0}^{h=m-1} \varepsilon^h x_h;$$

причем во всем дальнейшем будем употреблять обозначение x_i корня также в том случае, когда число $i > m$; причем будем писать

$$\begin{aligned} x &= x_0 = x_m,\\ x_h &= x_k, \end{aligned}$$

если $h \equiv k \pmod m$; т. е. другими словами, если значки образуют один класс по модулю m, то соответствующее им корни — одинаковы.

Мы видели уже, что циклическая подстановка

$$S = (x_h, x_{h+1}, \ldots, x_{m+h-1})$$

переводит резольвенту

$$(\varepsilon, x) \quad \text{в} \quad \varepsilon^{-1}(\varepsilon, x).$$

Очевидно, что подстановка S^k переведет резольвенту

$$(\varepsilon, x) \quad \text{в} \quad \varepsilon^{-k}(\varepsilon, x).$$

Будем все корни x_i считать переменными независимыми, с одним лишь выше-сделанным ограничением относительно значков, и рассмотрим выражение

$$(\varepsilon, x)^{\nu}.$$

Тогда возвышая резольвенту в степень ν по известным формулам, и замечая, что все степени ε, выше m, заменяются соответственными вычетами по модулю m, мы получаем

$$(1)\qquad (\varepsilon, x)^{\nu} = X_0^{(\nu)} + \varepsilon X_1^{(\nu)} + \ldots + \varepsilon^{m-1} X_{m-1}^{(\nu)} = \sum_h \varepsilon^h X_h^{(\nu)},$$

где $X_i^{(\nu)}$ суть формы степени ν от независимых переменных x_i.

Например, если $m = 3$, то $(\varepsilon, x)^2 = (x_0 + \varepsilon x_1 + \varepsilon^2 x_2)^2 = X_0^{(2)} + \varepsilon X_1^{(2)} + \varepsilon^2 X_2^{(2)}$, где $X_0^{(2)} = x_0^2 + 2x_1x_2$, $X_1^{(2)} = x_2^2 = 2x_0x_1$ и $X_2^{(2)} = x_1^2 + 2x_0x_2$.

Для значков форм $X_i^{(\nu)}$ мы будем придерживаться того же условия, что

$$X_h^{(\nu)} = X_k^{(\nu)},$$

если $h \equiv k \pmod m$.

Подстановка S, очевидно, производите над функциями

$$X_0^{(\nu)}, \quad X_1^{(\nu)}, \ldots, \ X_{m-1}^{(\nu)}$$

циклическую подстановку

$$(0, \nu, 2\nu, 3\nu, \ldots),$$

т. е. $X_h^{(\nu)}$ переходить в $X_{h+\nu}^{(\nu)}$.

В самом деле, для доказательства мы замечаем, что

$$mX_h^{(\nu)} = \sum_{\varepsilon} \varepsilon^{-h}(\varepsilon, x)^{\nu}. \tag{2}$$

Последнее равенство следует из того, что $(\varepsilon, x)^{\nu}$ есть новая резольвента, где роль переменных x_i играют $X_i^{(\nu)}$.

Делая в правой части равенства (2) подстановку S, мы получаем в этой части новую сумму

$$\sum_{\varepsilon} = \varepsilon^{-h-\nu}(\varepsilon, x)^{\nu}.$$

Значить, левая часть должна перейти в $mX_{h+\nu}^{(\nu)}$.

§ 20

Соображениями аналогичными с теми, что в предыдущем параграфе, можно доказать такую же самую теорему общего характера, если рассматривается функция

$$(\varepsilon, x)^{\nu}(\varepsilon^{\lambda_1}, x)^{\nu_1}(\varepsilon^{\lambda_2}, x)^{\nu_2} \cdots = \sum_h \varepsilon^h \Xi_h,$$

где Ξ_h суть формы некоторой степени $\nu + \nu_1 + \nu_2 + \ldots$ относительно x_i.

Отсюда

$$m\Xi_h = \sum \varepsilon^{-h}(\varepsilon, x)^{\nu}(\varepsilon^{\lambda_1}, x)^{\nu_1}(\varepsilon^{\lambda_2}, x)^{\nu_2} \cdots \tag{1}$$

Очевидно, что производство в правой части равенства (1) подстановки S обращает под знаком $\sum$ множитель ε^{-h} в множитель $\varepsilon^{-h-\nu-\nu_1\lambda_1-\nu_2\lambda_2-\cdots}$, т. е., другими словами, форма Ξ_h, переходит от этой подстановки в форму $\Xi_{h+\nu+\nu_1\lambda_1+\nu_2\lambda_2+\ldots}$.

Периоды Gauss'a

§ 21

Gauss показывает в своем сочинении Disquisitiones Arithmeticae удобные в практическом отношении и важные в теоретическом приемы решения двучленных уравнений.

Сущность его методы сводится к рассмотрению резольвенты Lagrange'a (ε, x) в том случае, когда ε — не первообразный корень.

Пусть $m = e \cdot f$ и пусть ε будет корень степени m из единицы, принадлежащий к показателю e. Тогда резольвенту Lagrange'a можно написать так

$$\begin{aligned}(\varepsilon, x) \quad &= x_0 + \varepsilon x_1 + \ldots + \varepsilon^{e-1} x_{e-1} + \\ &+ x_e + \varepsilon x_{e+1} + \ldots + \varepsilon^{e-1} x_{2e-1} + \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ &+ x_{e(f-1)} + \varepsilon x_{e(f-1)+1} + \ldots + \varepsilon^{e-1} x_{m-1}.\end{aligned}$$

Следуя Gauss'y, мы назовем *периодами* такие функций корней

$$\begin{aligned}&\eta_0 = x_0 + x_e + x_{2e} + \ldots + x_{e(f-1)}, \\ &\eta_1 = x_1 + x_{e+1} + \ldots + x_{e(f-1)+1}, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ &\eta_{e-1} = x_{e-1} + x_{2e-1} + \ldots + x_{m-1}.\end{aligned} \tag{1}$$

Тогда получается выражение резольвенты Lagrange'a через периоды Gauss'a в таком виде

$$(\varepsilon, x) = x_e + x_{2e-1} + \ldots + x_{m-1}. \tag{2}$$

Будем выражение (2) также обозначать (ε, η). Будем рассматривать циклическую подстановку $S = (x_0, x_1, \ldots, x_{n-1}$. Так как подстановка S дает циклическое перемещение периодов

$$(\eta_0, \eta_1, \eta_2, \ldots, \eta_{e-1}),$$

то очевидно, что теоремы §§ 19, 20 будут справедливы н относительно коэффициентов выражений

$$(\varepsilon, \eta)^\nu = H_0^{(\nu)} + \varepsilon H_1^{(\nu)} + \ldots + \varepsilon^{e-1} H_{e-1}^{(\nu)}$$

и

$$(\varepsilon, \eta)^\nu (\varepsilon^{\lambda_1}, \eta)^{\nu_1} (\varepsilon^{\lambda_2}, \eta)^{\nu_2} \cdots .$$

Двучленные уравнения и деление круга

§ 22

Из элементов известно, что корни уравнения

$$x^n - 1 = 0 \tag{1}$$

имеют вид

$$x = e^{\frac{2k\pi}{n}i}.$$

Отсюда видно, что задача решения уравнения (1) равносильна задачи деления окружности на n равных частей, или задаче вписывания в круг правильного многоугольника.

Древним математикам были известны построения циркулем и линейкой вписанных правильных многоугольников, имеющих число сторон, выражаемое одной из следующих формул

$$2^k, \quad 3 \cdot 2^k, \quad 5 \cdot 2^k, \quad 3 \cdot 5 \cdot 2^k.$$

Новый шаг в вопрос построения правильных многоугольников циркулем и линейкой был сделан Gauss'ом в его знаменитом сочинений «Disquisitiones Arithmeticae» (в §§ 365–366).

Gauss дает такую теорему: для решимости уравнения $x^n - 1 = 0$ в квадратных радикалах необходимо и достаточно, чтобы было одно из трех:

1) число n простое, вида $2^h + 1$;

2) $n = 2^m$;

3) число n есть произведение чисел предыдущих видов.

Gauss добавляет весьма важное соображение, состоящее в том, что для чисел, для которых можно делить циркулем и линейкой окружность круга, можно также делить на равные части и обвод кривой линии — *лемнискаты*.

§ 23

Очевидно, что число h, фигурирующее в теореме Gauss'а должно иметь вид

$$h = 2^k,$$

ибо, если $h = 2^k \cdot (2r + 1)$, то число

$$2^h + 1 = \left[2^{2^k}\right]^{2r+1} + 1$$

делится на

$$2^{2^k} + 1$$

и, следовательно, не может быть простым числом, так что простые числа надо будет искать среди чисел

$$2^{2^k} + 1.$$

Относительно этих чисел Fermat сделал предположение (оказавшееся неверным), что все эти числа простые.

Действительно, оказалось, что получаются простыл числа при $k = 0, 1, 2, 3, 4$, а именно

$$3, \quad 5, \quad 17, \quad 2576, \quad 65537.$$

Случай 17 разобран у Gauss'а в Disquisitiones Arithmeticae.

Построение циркулем многоугольника с числом сторон = 257 произвел по методе Gauss'а Richelot[95]. И, наконец, случай 65537 сделан Hermes'ом[96].

[95] Journal für die reine und angewandte Mathematik A. L. Crelle; 9, 1, 1832.

[96] Gött. Nachr. 1894.

Далее, для числа $k = 5$ Euler показал, что получается число составное, а именно

$$2^{2^5} + 1 = 4294967297 = 641 \cdot 6700417.$$

Затем сложность чисел показали далее Landry для числа

$$2^{2^6} + 1,$$

а затем священник И. М. Первушин для

$$2^{2^{12}} + 1 \quad \text{и} \quad 2^{2^{23}} + 1 \qquad (Lucas).$$

Остается вопрос открытым, будет ли конечным число простых чисел в ряде

$$2^{2^M} + 1,$$

или нет.

§ 24

Ограничимся рассмотрением случая n простого.

Итак, будем рассматривать решение уравнения

$$X_p(x) = x^{p-1} + x^{p-2} + + \ldots + x + 1 = 0. \tag{1}$$

Если обозначим через r первообразный корень степени p из единицы, то все корни уравнения (1) будут иметь вид

$$r, \quad r^2, \quad r^3, \ \ldots, \ r^{p-1}; \tag{2}$$

число p мы предполагаем простым, значит $p - 1$ число составное.

Покажем теперь, что уравнение (1) циклическое, т. е. что его группа Galois состоит из степеней одной и той же циклической подстановки.

Возьмем первообразный корень g простого числа p. Тогда, очевидно, что по модулю p все числа

$$1, \quad g, \quad g^2, \ \ldots, \ g^{p-2}$$

отличаются только порядком от чисел

$$1, \quad 2, \quad 3, \ \ldots, \ (p-1).$$

Значит ряд чисел

$$r, \quad r^g, \quad r^{g^2}, \ldots, \ r^{g^{p-2}} \tag{3}$$

отличается только порядком от чисел (2). Значит, числа (3) дают также все корни уравнения (1).

Обозначим $r^{g^h} = r_h$.. Тогда числа (3) можно иначе записать так

$$r, \quad r_1, \quad r_2, \ \ldots, \ r_{p-2}. \tag{4}$$

Если мы обозначим через $\theta(x)$ рациональную функцию x^g, т. е.

$$\theta(x) = x^g,$$

то, очевидно, что

$$r_i = \theta^i(r),$$

и, значит, корни (4) представляют собою такой ряд

$$r, \quad \theta(r), \quad \theta^2(r), \quad \theta^3(r), \ \ldots, \ \theta^{p-2}(r), \tag{5}$$

что показываешь, что группа Galois есть циклическая, образованная степенями подстановки

$$S = (r, r_1, r_2, \ldots, r_{p-2}).$$

§ 25

Рассмотрим поле $\Omega(r)$, получаемое от присоединения корня r к полю Ω рациональных чисел. Всякое число этой области будет, очевидно, представлять из себя рациональную функцию $\varphi(r)$ с рациональными коэффициентами.

Так как всякую рациональную функцию от корня уравнения можно представить в целом виде, причем эта целая функция будет в степени на единицу меньше, чем степень уравнения, то мы получаем

$$\varphi(r) = b_0 \cdot 1 + b_1 r + \ldots + b_{p-2} r^{p-2}, \tag{1}$$

где $b_0, b_1, b_2, \ldots$ суть рациональные числа. Давая этим коэффициентам всевозможные рациональные значения, воспроизведем все поле $\Omega(r)$.

Так как мы имеем из уравнения (1) § 24.

$$1 = -r - r^2 - \ldots - r^{p-2}, \tag{2}$$

то мы получаем

$$\varphi(r) = (b_1 - b_0)r + (b_2 - b_0)r^2 + \ldots (b_{p-2} - b_0)r^{p-2} - b_0 r^{p-1}.$$

Но так как числа степеней отличаются только порядком от чисел (4) предыдущего §-фа, то можно представить всякое число в таком виде

$$\varphi(r) = ar + a_1 r_1 + \ldots + a_{p-2} r_{p-2}. \tag{3}$$

Не трудно убедиться, что всякое число рассматриваемого поля представляется только одним способом в виде (3). Для этой цели достаточно убедиться, что равенство

$$\varphi(r) = 0 \tag{4}$$

возможно только тогда, когда все коэффициенты a_i равны 0.

В самом деле, рассматривая выражение (1), мы замечаем, что равенство (4) влечет, как следствие, равенство нулю всех коэффициентов

$$b_0, \quad b_1, \quad b_2, \ \ldots, \ b_{p-2},$$

ибо нам известно, что уравнение

$$X_p(x) = 0$$

неприводимое.

Если коэффициенты b_i равняются нулю, то будут, очевидно, обращаться в нуль и коэффициенты a_i.

§ 26

Группа рассматриваемого уравнения есть

$$G = (I, S, S^2, \ldots, S^{p-2}),$$

образованная степенями круговой подстановки

$$S = (r, r_1, r_2, \ldots, r_{p-2}).$$

Очевидно, что эта группа состоять из таких преобразований чисел $\varphi(r)$, где корень r заменяется корнями

$$r, \quad r_1, \quad r_2, \ \ldots, \ r_{p-2},$$

так что элементы этой группы можно обозначить так

$$(r, r), \quad (r, r_1), \ \ldots, \ (r, r_{p-2}),$$

при этом мы видим, что подстановка (r, r_k) равносильна подстановке (r, r_{h_k}).

Обращаемся теперь к рассмотрению делителей группы G. Очевидно, что эти делители получатся следующим образом. Раскладывая число $p-1$ на множители, пусть имеем

$$p - 1 = e \cdot f.$$

Тогда не трудно видеть, что для всякого делителя e числа $p-1$ будет соответствовать подгруппа

$$G_1 = (I, S^e, S^{2e}, \ldots, S^{(f-1)e}). \tag{1}$$

Эта подгруппа имеет порядок f.

Не трудно составить функции, принадлежащие этой подгруппе. К числу таких функций принадлежат Gauss'овы периоды

$$\begin{aligned} &\eta = r + r_r + r_{2e} + \ldots + r_{(f-1)e}, \\ &\eta_1 = r_1 + r_{e+1} + r_{2e+1} + \ldots + r_{(f-1)e+1}, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ &\eta_{e-1} = r_{e-1} + r_{2e-1} + \ldots + r_{p-2}. \end{aligned} \tag{2}$$

Очевидно, что каждая из этих функций не меняется от подстановок подгруппы (1).

Что касается подстановок, переводящих Gauss'овы периоды одни в другие, то придется рассмотреть сопряженный системы

$$G_1, \quad G_1(r, r_1), \quad G_1(r, r_2), \ldots, \ G_1(r, r_{e-1}).$$

Подстановки этих сопряженных систем переводят период первый η в периоды

$$\eta, \quad \eta_1, \quad \eta_2, \ \ldots, \eta_{e-1}.$$

§ 27

Все функций η_i различны между собою, потому что равенство

$$\eta_k = \eta_i$$

влекло бы за собой линейное соотношение между r_i, что не возможно.

Применяя соображения общей теории (см. главу XVI), мы приходим к такому выводу: Gauss'овы периоды $\eta, \eta_1, \eta_2, \ldots, \eta_{e-1}$ суть корни некоторого уравнения степени e с рациональными коэффициентами.

Если присоединить один из периодов, например, η к полю Ω, то корень r первоначального уравнения будет в новом поле корнем уравнения степени

$$\frac{p-1}{e} = f.$$

§ 28

Теорема. *Всякая функция от корня r первоначального поля, не меняющаяся от подстановки (r, r_e), будет принадлежать к полю $\Omega(\eta)$ и будет выражаться линейно через периоды*

$$\eta, \quad \eta_1, \ \ldots, \ \eta_{e-1}.$$

В самом деле, мы видели, что всякая функция $\varphi(r)$ может быть представлена в таком виде:

$$\varphi(r) = \sum_h a_h r_h. \tag{1}$$

Производя в равенстве (1) подстановку (r, r_e), мы получаем

$$\varphi(r_e) = \sum_h a_h r_{h+e} = \sum_h a_{h-e} r_h.$$

Равенство

$$\varphi(r_e) = \varphi(r)$$

влечет, как следствие, равенство

$$a_h = a_{h-e},$$

имеющее место при всяком h.

Значить, мы получаем

$$a_h = a_{h+e} = a_{h+2e} = \ldots;$$

следовательно, мы получаем

$$\varphi(r) = a \cdot \{r + r_e + \ldots\} + a_1\{r_1 + r_{e+1} + \ldots\} + \ldots =$$
$$= a\eta + a_1\eta_1 + \ldots + a_{e-1}\eta_{e-1},$$

где коэффициенты a_i суть рациональные числа.

Очевидно, что если коэффициенты выражений $\varphi(r)$ будут целыми числами, то и коэффициенты a_i должны быть целыми числами.

§ 29

Рассмотрим теперь уравнение

$$F_e(x) = (x-\eta)(x-\eta_1)\cdots(x-\eta_{e-1}), \tag{1}$$

которому удовлетворяют Gauss'овы периоды.

Из общей теории мы знаем, что коэффициенты этого уравнения должны быть все рациональные.

Не трудно убедиться, что коэффициенты этого уравнения будут числа целые (и рациональные), так что период Gauss'а η есть то, что называется *целым алгебраическим числом.* — Целым алгебраическим числом называется корень уравнения, коэффициенты которого целые числа, а старший коэффициент равен единице.

Для того, чтобы в этом убедиться, составим произведение

$$\eta_k\eta_h.$$

Так как оба множителя принадлежать к подгрупп $G-1$, то и все произведение принадлежит к той же подгруппе, а, следовательно, на оснований теоремы § 28, это произведение должно выражаться линейно через периоды, так что будет

$$\eta_k\eta_h = \alpha\eta + \alpha_1\eta_1 + \ldots + \alpha_{e-1}\eta_{e-1}.$$

Так как множители η_k и η_h суть суммы корней r_i то имеем коэффициенты равные единице. Значит, в произведений коэффициенты будут целые, а, значить, и числа

$$\alpha,\quad \alpha_1,\ldots,\ \alpha_{e-1}$$

будут целыми.

Предположим, что мы имеем удобные приемы для вычисления коэффициентов

$$\alpha,\quad \alpha_1,\ldots,\ \alpha_{e-1}.$$

Тогда получаем ряд равенств

$$\begin{aligned}
\eta\eta &= a_0^{(0)}\eta + a_1^{(0)}\eta_1 + \ldots + a_{e-1}^{(0)}\eta_{e-1},\\
\eta\eta_1 &= a_0^{(1)}\eta + a_1^{(1)}\eta_1 + \ldots + a_{e-1}^{(1)}\eta_{e-1},\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,\\
\eta\eta_{e-1} &= a_0^{(e-1)}\eta + a_1^{(e-1)}\eta_1 + \ldots + a_{e-1}^{(e-1)}\eta_{e-1}.
\end{aligned}$$

Исключая из этих e однородных уравнений буквы

$$\eta,\quad \eta_1,\quad \eta_2,\ldots,\ \eta_{e-1},$$

получим

$$(1)\qquad \begin{vmatrix} a_0^{(0)}-\eta & a_1^{(0)} & \dots & a_{e-1}^{(0)} \\ a_0^{(1)} & a_1^{(1)}-\eta & \dots & a_{e-1}^{(1)} \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ a_0^{(e-1)} & a_1^{(e-1)} & \dots & a_{e-1}^{(e-1)}-\eta \end{vmatrix} = 0.$$

Получим уравнение $F_e(\eta)=0$, обладающее всеми сказанными свойствами.

Посмотрим, как, считая известными корни

$$\eta,\quad \eta_1,\quad \eta_2,\dots,\ \eta_{e-1}$$

уравнения (1) вычислить окончательно корень r заданного уравнения.

Составим для этой цели уравнение степени F, имеющее корни

$$r,\quad r_e,\quad r_{2e},\ \dots,\ r_{(f-1)e},$$

а именно уравнение

$$(2)\qquad \Phi_e(x)=(x-r)(x-r_e)(x-r_{2e})\cdots(x-r_{(f-1)e})=0.$$

Чтобы показать, что коэффициенты уравнения (2) выражаются через периоды, рассмотрим сумму степеней с показателем g^{h}[97] корней уравнения (2), а именно

$$r^{g^h}+r_e^{g^h}+\dots+r_{(f-1)e}^{g^h}=r_h+r_{e+h}+r_{2e+h}+\dots+r_{(f-1)e+1}=\eta_h.$$

Значит, все суммы степеней корней, к вычисление которых по формулам Newton'a приводится вычисление коэффициентов, суть не что иное, как периоды, и, значит, по формулам Newton'a по этим периодам мы вычислим коэффициенты уравнения (2).

§ 30

Итак, задача привелась к решений уравнения (2). Для рассмотрения этого уравнения, разложим показатель его степени па множители

$$f=e'f',$$

и возьмем новый делитель G_2 подгруппы G_1, имеющий порядок f', а индекс e'.

Этот делитель будет состоять из подстановок

$$(I, S^{ee'}, S^{2ee'}, \dots, S^{(f'-1)ee'}).$$

Тогда придется взять такие новые периоды

$$\eta'=r+r_{ee'}+r_{2ee'}+\dots+r_{f'-1)ee'}.$$

Можно показать, что в поле $\Omega(\eta)$ период η' удовлетворяет уравнению

$$F_{e'}(\eta')=0$$

[97] Числа gh сравнимы по модулю p с рядом чисел $1,2,\dots,p-1$.

степени e'.

Когда это уравнение уже решено, то корни

$$r, \quad r^{ee'}, \quad r^{2ee'}, \ \ldots$$

получаются уже из уравнения

$$\Phi_{e'}(x) = 0$$

степени f'.

Относительно всех этих новых уравнений имеют место соображения, аналогичные с предыдущими, с тою лишь разницею, что абсолютное поле рациональных чисел Ω заменяются полем $\Omega(\eta)$.

§ 31

На основании сказанного можно привести задачу деления окружности на простое число p равных частей на решение ряда AЬel'евых уравнений простой степени, ибо раскладывая число $(p-1)$ на простые множители

$$p - 1 = ee'e'' \cdots ,$$

приведем задачу к последовательному вычисление периодов

$$\eta, \quad \eta', \quad \eta'', \ \ldots,$$

удовлетворяющих Abel'евым уравнениям простых степеней

$$e, \quad e', \quad e'', e''', \ \ldots$$

Abel'евы уравнения простых степеней $e, e', e'', \ldots$ требуют для своего решения, как это мы видели в §§ 14, 15, 16 присоединения первообразных корней из единиц степеней $e, e', e'', \ldots$. Итак, мы видим, что выражение в радикалах первообразиого корня степени p привелось к выражению корней из единиц меньших степеней, которые суть делители числа $p-1$. Такое постепенное понижение приведет к полному выражению в радикалах корня степени p.

Метода Gauss'а вычисления резольвент

§ 32

Пусть будет иметь место сравпеп1е

$$\lambda \equiv g^h \pmod{p},$$

так что $h = \operatorname{ind}\lambda$. Тогда

$$r^\lambda = r^{g^h} = r_h = r_{\operatorname{ind}\lambda}.$$

Будем рассматривать периоды η_h при произвольных целых значениях числа h. Причем мы будем заменять значки большие $p-1$ вычетами по модулю $p-1$.

Введем, следуя Gauss'у, новое обозначение

$$\eta^{(\lambda)} = \eta_h = \eta_{\operatorname{ind}\lambda},$$

причем, конечно, будет иметь место при всяких целых значениях h равенство

$$\eta_h = r_h + r_{h+e} + r_{h+2e} + \ldots + r_{h+(f-1)e}. \tag{1}$$

Введем для всякого целого числа λ ряд новых чисел

$$\lambda' \equiv \lambda g^e, \quad \lambda'' \equiv \lambda g^{2e}, \quad \lambda''' \equiv \lambda g^{3e}, \ \ldots, \ (\mathrm{mod}\, p).$$

Тогда будут иметь место такие сравнения

$$\begin{aligned} &\mathrm{ind}\, \lambda' \equiv \mathrm{ind}\, \lambda + e, \\ &\mathrm{ind}\, \lambda'' \equiv \mathrm{ind}\, \lambda + 2e, \quad (\mathrm{mod}\, p-1). \\ &\ldots\ldots\ldots\ldots\ldots \end{aligned}$$

Значит, формула (1) перепишется так

$$\eta_{\mathrm{ind}\, \lambda} = r_{\mathrm{ind}\, \lambda} + r_{\mathrm{ind}\, \lambda'} + r_{\mathrm{ind}\, \lambda''},$$

т. е., другими словами,

$$\eta^{(\lambda)} = r^{\lambda} + r^{\lambda'} + r^{\lambda''} + \ldots \tag{2}$$

§ 33

Рассмотрим два периода

$$\eta^{(\lambda)} = r^{\lambda} + r^{\lambda'} + r^{\lambda''} + \ldots, \tag{1}$$

$$\eta^{(\mu)} = r^{\mu} + r^{\mu'} + r^{\mu''} + \ldots, \tag{2}$$

где числа $\mu', \mu'', \ldots$ также определяются по числу μ, как в прошлом §-фе определялись $\lambda', \lambda'', \ldots$ по числу λ, т. е.

$$\mu' \equiv \mu g^e, \quad \mu'' =\equiv \mu g^{2e}, \ \ldots$$

Можно будет формулы (1) и (2) переписать так

$$\begin{aligned} \eta^{(\lambda)} &= \sum_{s=0}^{s=f-1} r^{\lambda g^{se}}, \\ \eta^{(\mu)} &= \sum_{t=0}^{t=f-1} r^{\mu g^{te}}. \end{aligned}$$

Рассмотрим теперь произведение

$$\eta^{(\lambda)}\eta^{(\mu)} = \sum_s \sum_t r^{\lambda g^{se} + \mu g^{te}}. \tag{3}$$

Будем сначала суммировать по t, считая s постоянным.

Очевидно, что когда t пробегает полную систему вычетов по модулю f, то $s+t$ при всяком s пройдет туже самую систему вычетов, значить, под знаком суммы можно заменить t на $s+t$, и мы имеем

$$\eta^{(\lambda)}\eta^{(\mu)} = \sum_s \sum_t r^{(\lambda+\mu g^{te})g^{se}}.$$

Переменяя порядок суммирования, получим

$$\eta^{(\lambda)}\eta^{(\mu)} = \sum_s \sum_t r^{(\lambda+\mu g^{te})g^{se}} = \sum_t \eta^{\lambda+\mu g^{te}}.$$

Итак, мы получаем

$$\eta^{(\lambda)}\eta^{(\mu)} = \eta^{\lambda+\mu} + \eta^{\lambda+\mu'} + \eta^{\lambda+\mu''} + \ldots \tag{4}$$

Поменяв ролями λ и μ, можно написать туже самую формулу иначе

$$\eta^{(\lambda)}\eta^{(\mu)} = \eta^{\lambda+\mu} + \eta^{\lambda'+\mu} + \eta^{\lambda''+\mu} + \ldots \tag{5}$$

Символ $\eta^{(\lambda)}$, определенный формулой (2) § 32, будет давать постоянное число, если $\lambda = 0$, или, вообще,

$$\lambda \equiv 0 \pmod{p},$$

потому что при $\lambda = 0$ и $\lambda \equiv \pmod{p}$, $\lambda' \equiv \pmod{p}$, $\lambda'' \equiv \pmod{p}$, $\ldots$, и, следовательно,

$$\eta^{(\lambda)} = r^0 + r^0 + \ldots = f.$$

Так что формулы, в которые входят символы $\eta^{(\lambda)}$ — *неоднородные* относительно периодов η. Но во всякой такой неоднородной формуле можно будет восстановить однородность из того соображения, что

$$\eta_1 + \eta_2 + \ldots + \eta_{e-1} = -1.$$

Последняя формула есть не что иное, как формула (2) § 25.

И, значить, всякий постоянный член a, не заключающий периодов, можно заменить через

$$-a(\eta_1 + \eta_2 + \ldots + \eta_{e-1}).$$

§ 34

Пример. Рассмотрим случай $p = 13$, $g = 2$; следовательно $p - 1 = 12$. Пусть $e = 3$, $f = 4$. Тогда имеем таблицу

$\operatorname{ind}\lambda$	0	1	2	3	4	5	6	7	8	9	10	11	12
λ	1	2	4	8	3	6	12	11	9	5	10	7	1

.

По определению Gauss'овых периодов (см. § 26) имеем

$$\eta = r + r_3 + r_6 + r_9,$$
$$\eta_1 = r_1 + r_4 + t_7 + r_{10},$$
$$\eta_2 = r_2 + r_5 + r_8 + r_{11}.$$

По таблице находим

$$\eta = r + r^8 + r^{12} + r^5 = r^1 + r^{1\cdot 2^3} + r^{1\cdot 2^6} + r^{1\cdot 2^9} = \eta^{(1)},$$
$$\eta_1 = r^2 + r^3 + r^{11} + r^{10} = r^2 + r^{2\cdot 2^3} + r^{2\cdot 2^6} + r^{2\cdot 2^9} = \eta^{(2)},$$
$$\eta_2 = r^4 + r^6 + r^9 + r^7 = r^4 + r^{4\cdot 2^3} + r^{4\cdot 2^6} + r^{4\cdot 2^9} = \eta^{(4)}.$$

Очевидно, что будут иметь место следующие равенства

$$\eta^{(1)} = \eta^{(8)} = \eta^{(12)} = \eta^{(5)}$$
$$\eta^{(2)} = \eta^{(3)} = \eta^{(11)} = \eta^{(10)}$$
$$\eta^{(4)} = \eta^{(6)} = \eta^{(9)} = \eta^{(7)}.$$

Значит, числа $\lambda, \lambda', \lambda'', \lambda'''$ суть или

$$1, \quad 8, \quad 12, \quad 3$$

или

$$2, \quad 3, \quad 11, 10,$$

или

$$4, \quad 6, \quad 9, \quad 7.$$

Для нахождения кубического уравнения, которому удовлетворяют периоды η, вычислим три произведения

$$\eta\eta, \quad \eta\eta_1, \quad \eta\eta_2.$$

Получаем

$$\eta\eta = \eta^{(1)}\eta^{(1)},$$

или по формулам (4) предыдущего параграфа получаем

$$\eta\eta = \eta^{(1)}\eta^{(1)} = \eta^{(1+1)} + \eta^{(1+8)} + \eta^{(1+12)} + \eta^{(1+5)} = \eta^{(2)} + \eta^{(9)} + \eta^{(0)} + \eta^{(6)} =$$
$$= \eta^{(2)} + \eta^{(4)} + 4 + \eta^{(4)} = 4 + \eta_1 + 2\eta_2,$$

но $\eta + \eta_1 + \eta_2 = -1$, следовательно,

$$\eta\eta = -4(\eta + \eta_1 + \eta_2) - \eta_1 + 2\eta_2 = -4\eta - 3\eta_1 - 2\eta_2,$$

т. е.

$$\eta\eta = 4\eta - 3\eta_1 - 2\eta_2. \tag{1}$$

Далее имеем

$$\eta\eta_1 = \eta^{(1)}\eta^{(2)} = \eta^{(1+2)} + \eta^{(1+3)} + \eta^{(1+11)} + \eta^{(1+10)} = \eta^{(3)} + \eta^{(4)} + \eta^{(12)} + \eta^{(11)} =$$
$$= 2\eta^{(2)} + \eta^{(4)} + \eta^{(1)} = 2\eta_1 + \eta_2 + \eta.$$

Мы могли бы вычислить иначе произведение $\eta\eta_1$, а именно

$$\eta\eta_1 = \eta^{(1)}\eta^{(2)} = \eta^{(2+1)} + \eta^{(2+8)} + \eta^{(2+12)} + \eta^{(2+5)} = \eta^{(3)} + \eta^{(10)} + \eta^{(1)} + \eta^{(7)} =$$
$$= 2\eta^{(2)} + \eta^{(1)} + \eta^{(4)} = 2\eta^{(1)} + \eta + \eta_2.$$

Итак, имеем

$$\eta\eta_1 = \eta + 2\eta_1 + \eta_2. \tag{2}$$

Наконец, найдем произведение $\eta\eta_2$:

$$\eta\eta_2 = \eta^{(1)}\eta^{(4)} = \eta^{(1+4)} + \eta^{(1+6)} + \eta^{(1+9)} + \eta^{(1+7)} = \eta^{(5)} + \eta^{(7)} + \eta^{(10)} + \eta^{(8)} =$$
$$= 2\eta^{(1)} + \eta^{(4)} + \eta^{(2)} = 2\eta + \eta_2 + \eta_1.$$

Итак,

$$\eta\eta_2 = 2\eta + \eta_1 + \eta_2. \tag{3}$$

Из уравнений (1), (2) и (3) получается такое кубическое уравнение

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

Итак, находим

$$\eta^3 + \eta^2 - 4\eta + 1 = 0.$$

Остается получить уравнение 4-й степени, которому удовлетворяют числа

$$r, \quad r^{12} = r^{-1}, \quad r^5, \quad r^8 = r^{-5}.$$

Мы могли бы составить новые периоды, соответствующие $e' = 2$, а именно

$$\xi = r + r^{12} = r + r^{-1} = 2cs\,\frac{2\pi}{13}$$
$$\xi_1 = r^8 + r^5 = r^5 + r^{-5} = 2cs\,\frac{10\pi}{13}.$$

Не трудно составить квадратное уравнение, которому удовлетворяет период ξ. Получаем

$$\xi + \xi_1 = \eta,$$
$$\xi\xi_1 = \eta_2.$$

Итак, получаем квадратное уравнение

$$\xi^2 - \eta\xi + \eta_2 = 0.$$

Это квадратное уравнение заключает ранее вычисленные периоды в своем основном поле.

И, наконец, зная ξ, мы вычислим окончательно корень r заданного уравнения при помощи квадратного уравнения

$$r + r^{-1} = \xi,$$

или

$$r^2 - \xi r + 1 = 0.$$

Если бы мы не хотели рассматривать промежуточный период ξ, то получили бы прямо из уравнения четвертой степени

$$(r + r^{-1})^2 - \eta(r + r^{-1}) + \eta_2 = 0.$$

Решение имело бы несколько другой вид, если бы мы за первый простой множитель числа $p - 1$ взяли не число 3, а число 2.

Будем производить решение иначе. Пусть $e = 2$, а тогда $f = 6$.

Тогда имеем

$$\eta = 1 + r_2 + r_4 + r_6 + r_8 + r_{10} = r + r^4 + r^3 + r^{12} + r^9 + r^{10} = \eta^{(1)},$$
$$\eta_1 = r_1 + r_3 + r_5 + r_7 + r_9 + r_{11} = r^2 + r^8 + r^6 + r^{11} + r^5 + r^7 = \eta^{(2)}.$$

Очевидно $\eta + \eta_1 = -1$.

Для нахождения квадратного уравнения, которому удовлетворяют периоды η и η_1, достаточно вычислить произведение корней $\eta\eta_1$.

Имеем

$$\eta\eta_1 = \eta^{(1)}\eta^{(2)} = \eta^{(3)} + \eta^{(9)} + \eta^{(7)} + \eta^{(12)} + \eta^{(6)} + \eta^{(8)} =$$
$$= \eta^{(1)} + \eta^{(1)} + \eta^{(2)} + \eta^{(1)} + \eta^{(2)} =^{(2)}= 3\eta^{(1)} + 3\eta^{(2)} = -3.$$

Итак, квадратное уравнение будет

$$\eta^2 + \eta - 3 = 0.$$

Остается получить уравнение 6-ой степени, которому удовлетворяют числа

$$r, \quad r^{12} = r^{-1}, \quad r^3, \quad r^{10} = r^{-3}, \quad r^4, \quad r^9 = r^{-4}.$$

Мы могли бы составить новые периоды соответствующее числу $e' = 3$, а именно,

$$\xi = r + r^{12} = r + r^{-1},$$
$$\xi_1 = r^3 + r^{10} = r^3 + r^{-3},$$
$$\xi_2 = r^4 + r^9 = r^4 + r^{-4}.$$

Не трудно составить кубическое уравнение которому удовлетворяют период ξ.

Имеем

$$\xi + \xi_1 + \xi_2 = \eta.$$

Составим произведения

$$\xi\xi_1 = r^4 + r^2 + r^{11} + r^9,$$
$$\xi\xi_2 = r^5 + r^3 + r^{10} + r^8,$$
$$\xi_1\xi_2 = r^7 + r + r^{12} + r^6.$$

Теперь находим

$$\xi\xi_1 + \xi\xi_2 + \xi_1\xi_2 = \eta + \eta_1 = -1.$$

Наконец, находим произведение

$$\xi\xi_1\xi_2 = \eta_1 + 2.$$

Итак, искомое кубическое уравнение будет

$$\xi^3 - \eta\xi^2 - \xi - (\eta_1 + 2) = 0.$$

Определив ξ, мы вычислим окончательно корень r заданного уравнения при помощи квадратного

$$r + r^{-1} = \xi,$$

или

$$r^2 - \xi r + 1 = 0.$$

§ 35

Вернемся теперь к вычислению резольвент и рассмотрим выражение

$$(\varepsilon^\lambda, r) = \sum \varepsilon^{\lambda h} r_h = \sum_{h=0}^{h=p-2} \varepsilon^{\lambda h} r^{g^h}, \tag{1}$$

где ε — примитивный корень степени $p-1$ из единицы. Или, обозначая

$$g^h \equiv s \pmod p$$

так что

$$h \equiv \operatorname{ind} s \pmod{p-1},$$

получаем

$$(\varepsilon^\lambda, r) = \sum_{s=1}^{s=p-1} \varepsilon^{\lambda \operatorname{ind} s} r^s. \tag{2}$$

Рассмотрим выражение

$$(\varepsilon^\lambda, r)(\varepsilon^\mu, r) = \sum_s \sum_t r^{s+t} \varepsilon^{\lambda \operatorname{ind} s + \mu \operatorname{ind} t}. \tag{3}$$

Если вместо t мы подставим st, ибо s принимает значения, несравнимые с нулем по модулю p, то при данном s выражения t и st пробегают одну и туже полную систему классов но модулю p за исключением класса $s = 0$.

Тогда формула (3) дает

$$(\varepsilon^\lambda, r)(\varepsilon^\mu, r) = \sum_s \sum_t r^{s(1+t)} \varepsilon^{(\lambda+\mu) \operatorname{ind} s + \mu \operatorname{ind} t}. \tag{4}$$

§ 36

Рассмотрим сначала случай I, $\mu + \lambda \equiv 0 \pmod{p-1}$, т. е., другими словами, можно будет в формулах (4) предыдущего §-фа положить $\mu = -\lambda$. Тогда имеем

$$(\varepsilon^\lambda, r)(\varepsilon^{-\lambda}, r) = \sum_s \sum_t r^{s(1+t)} \varepsilon^{-\lambda \operatorname{ind} t}.\lambda$$

Будем рассматривать значение λ, не удовлетворяющее сравнению $\lambda \equiv 0 \pmod{p-1}$. Тогда получаем

$$(\varepsilon^{\lambda}, r)(\varepsilon^{-\lambda}, r) = \sum_{t} \varepsilon^{\lambda \operatorname{ind} t} \sum r^{s(1+t)}.$$

Что касается суммы $\sum r^{s(1+t)}$, то, как известно из элементов, будем иметь

$$\sum_{s} r^{s(1+t)} = \sum_{3} (r^{1+t})^{s} = -1,$$

если $t = 1, 2, \ldots, p-2$.

А если $t = p-1$, то

$$\sum_{s} (r^{1+t})^{s} = \sum_{s} 1^{s} = p-1.$$

Итак, мы можем написать

$$(\varepsilon^{\lambda}, r)(\varepsilon^{-\lambda}, r) = -\sum_{t=1}^{t=p-2} \varepsilon^{-\lambda \operatorname{ind} t} + (p-1) \cdot \varepsilon^{-\lambda \operatorname{ind} (p-1)}.\lambda$$

Но известно, что

$$\operatorname{ind} (p-1) = \frac{p-1}{2};$$

следовательно

$$(\varepsilon^{\lambda}, r)(\varepsilon^{-\lambda}, r) = -\sum_{t=1}^{t=p-2} \varepsilon^{-\lambda \operatorname{ind} t} + p\varepsilon^{-\lambda \frac{p-1}{2}}.$$

Так как $\operatorname{ind} t$ под знаком последней суммы пробегает все значения

$$0, \quad 1, \quad 2, \ \ldots, \ p-2,$$

то

$$\sum_{t} \varepsilon^{\lambda \operatorname{ind} t} = 0.$$

Кроме того

$$\varepsilon^{\frac{p-1}{2}} = -1,$$

потому что ε есть первообразный корень степени $p-1$.

Итак, мы получаем такую основную формулу

$$(\varepsilon^{\lambda}, r)(\varepsilon^{-\lambda}, r) = p \cdot (-1)^{\lambda}. \tag{1}$$

Если же λ делится на $p-1$, то

$$(\varepsilon^{\lambda}, r) = (\varepsilon^{-\lambda}, r) = (1, r) = -1.$$

§ 37

Обращаемся теперь к случаю II, $\lambda + \mu$ не 0 $((\operatorname{mod} p-1))$.

Тогда имеем

$$(\varepsilon^{\lambda}, r)(\varepsilon^{\mu}, r) = \sum_{s}\sum_{t} r^{s(t+1)}\varepsilon^{(\lambda+\mu)\operatorname{ind} s}\cdot\varepsilon^{\mu\operatorname{ind} t} =$$
$$\sum_{t=1}^{t=p-2}\sum_{s=1}^{s=p-1} r^{s(t+1)}\varepsilon^{(\lambda+\mu)\operatorname{ind} s}\varepsilon^{\mu\operatorname{ind} t} + (-1)^{\mu}\sum_{s=1}^{s=p-1}\varepsilon^{(\lambda+\mu)\operatorname{ind} s}.$$

Так как $\lambda+\mu$ не делится на $p-1$, то

$$\sum_{s}\varepsilon^{(\lambda+\mu)\operatorname{ind} s} = 0, \lambda$$

и получаем

$$(\varepsilon^{\lambda}, r)(\varepsilon^{\mu}, r) = \sum_{t=1}^{t=p-2}\varepsilon^{\mu\operatorname{ind} t}\sum_{s} r^{s(t+1)}\varepsilon^{(\lambda+\mu)\operatorname{ind} s} =$$
$$= \sum_{t=1}^{t=p-2}\varepsilon^{\mu\, t-(\lambda+\mu)\operatorname{ind}(t+1)}\sum_{s} r^{s(t+1)}\varepsilon^{\lambda+\mu)\operatorname{ind} s(t+1)}.$$

Произведение $s(t+1)$ пробегает полную приведенную систему вычетов, когда s пробегает таковую по модулю p. Итак, имеем

$$\sum_{s} r^{s(t+1)}\varepsilon^{(\lambda+\mu)\operatorname{ind}(t+1)s} = \sum_{s}\varepsilon^{(\lambda+\mu)\operatorname{ind} s}\, r^{s} = (\varepsilon^{\lambda+\mu}, r).$$

Значит, мы получаем следующую формулу

$$\text{(II)}\qquad \frac{(\varepsilon^{\lambda}, r)(\varepsilon^{\mu}, r)}{(\varepsilon^{\lambda+\mu}, r)} = \psi_{\lambda,\mu}(\varepsilon),$$

где

$$\text{(I)}\qquad \psi_{\lambda,\mu}(\varepsilon) = \sum_{t=1}^{t=p-2}\varepsilon^{\mu\operatorname{ind} t-(\lambda+\mu)\operatorname{ind}(t+1)}.$$

Не надо забывать, что при выводе формулы (II) мы не предполагали сравнимости с нулем по модулю $p-1$ ни одного из чисел λ, μ, $\lambda+\mu$.

§ 38

Jacobi в своих лекциях по теории чисел показал, что решение двучленных уравнений сводится к рассмотрению функций $\psi_{\lambda,\mu}(\varepsilon)$.

При этом он вывел основные свойства этих функций. Следуя методе Jacobi, один из его слушателей, Rosenhain, показал подробный ход вычисления при решении двучленных уравнений простой степени для простых чисел до 103 включительно.

Мы ограничимся здесь самыми основными соображениями теории Jacobi.

Прежде всего мы видим, что всякая функция $\psi_{\lambda,\mu}(\varepsilon)$ есть линейная функция от корней уравнения

$$\varepsilon^{p-1} - 1 = 0$$

с целыми коэффициентами, которые вычисляются очень просто при помощи таблицы индексов.

§ 39

Метод Jacobi состоит в том, что если мы будем считать двучленные уравнения степеней ниже p решенными, то можем считать ε величиной известной, уже выраженной в радикалах, и тогда все резольвенты Lagrange'a

$$(\varepsilon^{\lambda}, r) = \sum \varepsilon^{\lambda h} r_h,$$

которые необходимы для нахождения искомого корня r уравнения $x^p - 1 = 0$, выражаются в радикалах через функций $\psi_{\lambda,\mu}(\varepsilon)$.

§ 40

Итак, рассмотрим некоторый свойства функций $\psi_{\lambda,\mu}(\varepsilon)$.

Прежде всего мы видим на основании уравнения (II) § 37, что

$$\psi_{\lambda,\mu} = \psi_{\mu,\lambda}.$$

Это можно проверить и непосредственно.

Рассмотрим корень t' сравнения

$$tt' \equiv 1 \,(\mathrm{mod}\, p)$$

Не трудно убедиться, что когда t пробегает приведенную систему вычетов по модулю p, то t' пробегает ту же систему. Тогда имеем

$$\mathrm{ind}\,(t+1) \equiv \mathrm{ind}\,(t+tt') \equiv \mathrm{ind}\, t(1+t') \equiv \mathrm{ind}\, t + \mathrm{ind}\,(1+t').$$

Кроме того, очевидно, что

$$\mathrm{ind}\, t \equiv -\mathrm{ind}\, t'.$$

Умножая первое из написанных сравнений на $-(\lambda+\mu)$, а второе на μ, и складывая, получаем

$$\mu\,\mathrm{ind}\, t - (\lambda+\mu)\mathrm{ind}\,(t+1) \equiv \mu(-\mathrm{ind}\, t') - (\lambda+\mu)(-\mathrm{ind}\, t') -$$
$$-(\lambda+\mu)\mathrm{ind}\,(1+t') \equiv \lambda\,\mathrm{ind}\, t' - (\lambda+\mu)\mathrm{ind}\,(1+t'),$$

т. е. мы имеем

$$\sum_t \varepsilon^{\mu\,\mathrm{ind}\, t - (\lambda+\mu)\mathrm{ind}\,(t+1)} = \sum_{t'} \varepsilon^{\lambda\mathrm{ind}\, t' - (\lambda+\mu)\mathrm{ind}\,(t'+1)},$$

т. е., другими словами.

$$\psi_{\lambda,\mu} = \psi_{\mu,\lambda}.$$

§ 41

Чтобы вернуться к Gauss'овым периодам, предположим по прежнему, что

$$p - 1 = ef.$$

Положим

$$\mu = f,$$

а в формулах для функции $\psi_{\lambda,\mu}$ вместо λ подставим $\mu \cdot \lambda$.

Тогда, если обозначим

$$\alpha = \varepsilon^{\mu} = \varepsilon^{f},$$

то

$$\psi_{\lambda,\mu}(\varepsilon) = \sum_{1}^{p-2} \alpha^{\operatorname{ind} t - (\lambda+1)\operatorname{ind}(t+1)};$$

α будет, конечно, корнем уравнения

$$\alpha^{e} - 1 = 0.$$

Будем во всем дальнейшем обозначать

$$\psi_{\lambda}(\alpha) = \sum_{1}^{p-2} \alpha^{\operatorname{ind} t - (\lambda+1)\operatorname{ind}(t+1)}.$$

Будем λ рассматривать, конечно, по модулю e. Формула (II) § 37 перепишется так

$$(\alpha^{\lambda}, r)(\alpha, r) = (\alpha^{\lambda+1}, r) \cdot \psi_{\lambda}(\alpha). \tag{III}$$

Эта формула имеет место при всяком λ, так что, если в ней будем считать $\alpha = \varepsilon^{\mu}$, то, если μ взаимно простое с $p-1$, то в формуле (III) можно придавать λ значения

$$1, \quad 2, \quad 3, \quad \ldots, \quad p - 3.$$

Если же $\mu = f$ есть делитель числа $p - 1$, то тогда λ принимает одно из следующих значений

$$1, \quad 2, \quad 3, \quad \ldots, \quad e - 2,$$

ибо ни λ, ни $\lambda + 1$ не должно делиться на e.

§ 42

Формула (I) подлежит следующему видоизменению

$$(\alpha^{\lambda}, r)(\alpha^{-\lambda}, r) = (-1)^{\mu\lambda} p. \tag{IV}$$

Формулы (III) и (IV) достаточны для выражения в радикалах не только корня r, но и всех периодов η, так как вычисление r это есть частный случай вычисления периода η, когда число его членов $f = 1$. Ограничимся поэтому вычислением периода η.

Итак, $\mu = f$, и мы имеем

$$(\alpha^\lambda, r) = r + \alpha^\lambda r_1 + \alpha^{2\lambda} r_2 + \ldots + \alpha^{(p-2)\lambda} r_{p-2}.$$

Получаем

$$\begin{gathered}(\alpha^\lambda, r) = (r + r_e + r_{2e} + \ldots) + \alpha^\lambda (r_1 + r_{e+1} + \ldots) + \ldots = \\ = \eta + \alpha^\lambda \eta_1 + \alpha^{2\lambda} \eta_2 + \ldots + \alpha^{(e-1)\lambda} \eta_{e-1} = (\alpha^\lambda, \eta).\end{gathered}$$

Теперь формулы (III) н (IV) перепишутся так

$$(\alpha^\lambda, \eta)(\alpha, \eta) = (\alpha^{\lambda+1}, \eta)\psi_\lambda(\alpha), \qquad (\alpha^\lambda, \eta)(\alpha^{-\lambda}, \eta) = (-1)^{f\lambda} p.$$

Получаем следующий ряд равенств

$$\begin{aligned}(\alpha, \eta)(\alpha, \eta) &= (\alpha^2, \eta)\psi_1(\alpha), \\ (\alpha^2, \eta)(\alpha, \eta) &= (\alpha^3, \eta)\psi_2(\alpha), \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \\ (\alpha^{e-2}, \eta)(\alpha, \eta) &= (\alpha^{e-1}, \eta)\psi_{e-2}(\alpha).\end{aligned}$$

Перемножая и замечая. что $\alpha^{e-1} = \alpha^{-1}$, находим

$$(\alpha, \eta)^{e-1} = (\alpha^{-1}, \eta) \cdot \psi_1(\alpha) \cdot \psi_2(\alpha) \cdots \psi_{e-2}(\alpha).$$

Умножая обе части последнего равенства на (α, η), получаем

$$(\alpha, \eta)^e = (-1)^f p \cdot \psi_1(\alpha) \cdot \psi_2(\alpha) \cdots \psi_{e-2}(\alpha),$$

откуда находим резольвенту

$$(\alpha, \eta) = \sqrt[e]{(-1)^f p \cdot \psi_1(\alpha) \cdot \psi_2(\alpha) \cdots \psi_{e-2}(\alpha)}.$$

Отсюда радикальное выражение для периодов η, получается по обыкновенной методе Lagrange'a (см. § 18), если мы в последней резольвенте будем давать букве α значения, равные всем корням уравнения

$$x^e - 1 = 0.$$

В случае $\mu = f = 1$ получаем

$$(\varepsilon, r) = \sqrt[p-1]{-p\psi_1(\varepsilon) \cdot \psi_2(\varepsilon) \cdots \psi_{p-3}(\varepsilon)}.$$

Свойства функции $\psi_{\lambda,\mu}$

§ 43

Так как $\psi_{\lambda,\mu}$ не меняется от перестановки λ и μ, то получится та же самая функция $\psi_\lambda(\alpha)$, если мы вместо (λ, μ) подставим $(\lambda f, f)$ и $(f, \lambda f)$.

Так что

$$\psi_\lambda(\alpha) = \sum \alpha^{\operatorname{ind} t-(\lambda+1)\operatorname{ind}(t+1)} = \sum \alpha^{\lambda \operatorname{ind} t-(\lambda+1)\operatorname{ind}(t+1)}.$$

Обозначая через λ' целое число, удовлетворяющее сравнению

$$\lambda\lambda' \equiv 1 \,(\operatorname{mod} e),$$

получаем

$$\psi_\lambda(\alpha^{\lambda'}) = \sum \alpha^{\lambda'\lambda \operatorname{ind} t-(\lambda'\lambda+\lambda)\operatorname{ind}(t+1)} = \sum \alpha^{\operatorname{ind} t-(\lambda')\operatorname{ind}(t+1)},$$

откуда

$$\psi_\lambda(\alpha^{\lambda'}) = \psi_{\lambda'}(\alpha). \tag{1}$$

Заменяя λ на $(-\lambda-\mu)$, находим

$$\frac{(\varepsilon^{-\lambda-\mu}, r)}{(\varepsilon^{-\lambda}, r)} = \psi_{-\lambda-\mu,\mu}(\varepsilon),$$

или, умножая левую часть на

$$\frac{(\varepsilon^{\lambda+\mu}, r)(\varepsilon^{\lambda}, r)}{(\varepsilon^{\lambda+\mu}, r)(\varepsilon^{l}, r)},$$

получаем

$$\psi_{-\lambda-\mu,\mu}(\varepsilon) = \frac{(-1)^{\lambda+\mu} p(\varepsilon^{\lambda}, r)(\varepsilon^{\mu}, r)}{(-1)^{\lambda} p(\varepsilon^{\lambda+\mu}, r)},$$

откуда

$$\psi_{-\lambda-\mu,\mu}(\varepsilon) = (-1)^{\mu} \cdot \psi_{\lambda,\mu}(\varepsilon). \tag{2}$$

Из этой формулы выводится сразу соответственная формула для $\psi_\lambda(\alpha)$.

В самом деле, заменим числа (λ, μ) на $(\lambda f, f)$ и, кроме того, возьмем корень λ'' сравнения

$$\lambda + \lambda'' + 1 \equiv (\operatorname{mod} e).$$

Тогда получаем

$$\psi_\lambda(\alpha) = (-1)^f \psi_{\lambda''}(\alpha). \tag{3}$$

Формулы (1), (2) и (3) сводят вычисление всех функций ψ_λ на вычисление приблизительно $\frac{1}{6}$ части.

Далее, имеем,

$$\psi_{\lambda,\mu}(\varepsilon) \cdot \psi_{\lambda,\mu}(\varepsilon^{-1}) = \frac{(\varepsilon^{\lambda}, r)(\varepsilon^{\mu}, r)(\varepsilon^{-\lambda}, r)(\varepsilon^{-\mu}, r)}{(\varepsilon^{\mu+\lambda}, r)(\varepsilon^{-\mu-\lambda}, r)} = \frac{(-1)^{\lambda} p \cdot (-1)^{\mu} p}{(-1)^{\lambda+\mu} p} = p.$$

Итак, получаем

$$\psi_{\lambda,\mu}(\varepsilon) \cdot \psi_{\lambda,\mu}(\varepsilon^{-1}) = p. \tag{4}$$

Отсюда, заменяя (λ, μ) на $(\lambda f, f)$, получаем

$$\psi_\lambda(\alpha) \cdot \psi_\lambda(\alpha^{-1}) = p. \tag{5}$$

Введем три, неделящихся на $p-1$, числа λ, μ и ν такие, что суммы $\lambda+\mu$ и $\lambda+\mu+\nu$ не делятся на $p-1$. Тогда

$$\psi_{\lambda,\mu}(\varepsilon)\psi_{\lambda+\mu,\mu}(\varepsilon) = \frac{(\varepsilon^\lambda, r)(\varepsilon^\mu, r)(\varepsilon^{\lambda+\mu}, r)(\varepsilon^\nu, r)}{(\varepsilon^{\lambda+\mu}, r)(\varepsilon^{\lambda+\mu+\nu})} = \frac{(\varepsilon^\lambda, r)(\varepsilon^\mu, r)(\varepsilon^\nu, r)}{(\varepsilon^{\lambda+\mu+\nu}, r)},$$

т. е.

$$\psi_{\lambda,\mu}(\varepsilon)\psi_{\lambda+\mu,\nu}(\varepsilon) = \frac{(\varepsilon^\lambda, r)(\varepsilon^\mu, r)(\varepsilon^\nu, r)}{(\varepsilon^{\lambda+\mu+\nu}, r)}.$$

Итак, мы видим, что произведение $\psi_{\lambda,\mu}\psi_{\lambda+\mu,\nu}$, симметрично относительно трех букв λ, μ и ν не меняется, если эти числа как угодно переставлять.

Так. например, получаем

$$\psi_{\lambda,\mu} \cdot \psi_{\lambda+\mu,\nu} = \psi_{\mu,\nu} \cdot \psi_{\mu+\nu,\lambda}.$$

Отсюда, заменяя (λ, μ, ν) на $(2\lambda f, f, f)$ и принимая во внимание, что

$$\psi_{2f,2\lambda f}(\varepsilon) = \psi_\lambda(\alpha^2),$$

получаем

$$\psi_{2\lambda}(\alpha) \cdot \psi_{2\lambda+1}(\alpha) = \psi_\lambda(\alpha)\psi_\lambda(\alpha^2).$$

Приведенными 6-ю формулами исчерпываются формулы, позволяющие сводить вычисление ψ_λ при одних значениях λ? на вычисление тех же функций при других.

Jacobi сделал попытку при помощи этих формул для всякого заданного простого числа l выразить все $(l-2)$ функции $\psi_\lambda(\alpha)$ через сопряженные величины одной из них, т. е. через $\psi_1(\alpha), \psi_1(\alpha^2), \psi_1(\alpha^3), \ldots$. Его попытка оказалась удачной для всех простых чисел до $l = 23$. Jacobi поэтому высказал предположение, что это обстоятельство всегда имеет место.

Однако Kronecker высказал предположение, что общая теорема Jacobi, вероятно, несправедлива.

Теорема Jacobi

§ 44

Рассмотрим теперь выражение

$$\psi_{\lambda,\mu}(g),$$

где g — первообразный корень, представляющий основание таблицы индексов, при помощи которой вычисляется сама функция ψ_λ.

Получаем

$$\psi_{\lambda,\mu}(g) = \sum_{t=1}^{t=p-2} g^{\mu \operatorname{ind} t + \nu \operatorname{ind}(t+1)};$$

здесь λ и μ мы будем считать положительными числами, не превосходяциими $p-1$, а ν есть число удовлетворяющее сравнению

$$\lambda + \mu + \nu \equiv 0 \,(\mathrm{mod}\, p-1)$$

и меньшее, чем $p-1$.

Итак, имеем

$$\psi_{\lambda,\mu}(g) \equiv \sum_{1}^{p} -2t^{\mu}(t+1)^{\nu} \,(\mathrm{mod}\, p).$$

Не трудно видеть, что сумму в правой части сравнения можно распространить на все числа

$$1, \quad 2, \quad 3, \ \ldots, \ p-1,$$

ибо при $t = p-1$, $t+1 = p$.

Так что получаем окончательно

$$\psi_{\lambda,\mu}(g) \equiv \sum_{1}^{p-1} t^{\mu}(t+1)\nu \,(\mathrm{mod}\, p), \tag{1}$$

или, применяя формулу бинома Newton'a, находим

$$\psi_{\lambda,\mu}(g) \equiv \sum_{h=1}^{h=\nu} \sum_{t=1}^{t=p-1} t^{\mu+h} \,(\mathrm{mod}\, p). \tag{2}$$

Из теории чисел известно, что

$$\sum t^{\mu+h} \equiv 0 \,(\mathrm{mod}\, p), \tag{3}$$

если $\mu + h$ не делится на $p-1$ и

$$\sum t^{\mu+h} \equiv -1 \,(\mathrm{mod}\, p), \tag{4}$$

если $\mu + h$ делится на $(p-1)$.

Покажем теперь, что если $\lambda + \mu < p-1$, то случай (4) не встретится, а, если $\lambda + \mu > p-1$, то этот случай встретится только один раз.

Итак, рассмотрим $\lambda + \mu < p-1$; число ν будет $= p-1-\lambda-\mu$.

Показатель $\mu + h$ пробегает следующая значения

$$\mu, \quad \mu+1, \ \ldots, \ p-1-\lambda = \mu+\nu.$$

Все эти значения суть целые положительные числа и меньшие $p-1$. Значит, ни одно из чисел не делится на $p-1$.

Во втором случае $\lambda + \mu > p-1$ и $\nu = 2(p-1) - \lambda - \mu$. Тогда показатель $\mu + h$ пробегает ряд значений

$$\mu, \quad \mu+1, \quad \mu+2, \ldots, \ 2(p-1)-\lambda.$$

В этом случае будет существовать одно число h, а именно $h = p-1-\mu$, при котором $\mu + h$ делится на $(p-1)$, и мы получаем следующую теорему Jacobi.

Функция $\psi_{\lambda,\mu}(g) \equiv 0 \pmod p$, *если* $\lambda+\mu < p-1$, *а* $\psi_{\lambda,\mu}(g) \equiv -C^{p-1-\mu}_{2(p-1)-\lambda-\mu} \pmod p$ *при* $\lambda + \mu > p - 1$.

Gauss'овы суммы

§ 45

Рассмотрим один из самых важных частных случаев вышеприведенной теории, а именно $e = 2$.

Тогда мы имеем два периода

$$\eta = r + r_2 + r_4 + \ldots + r_{p-3},$$
$$\eta_1 = r_1 + r_3 + r_5 + \ldots + r_{p-2}.$$

Эти два периода носят название Gauss'овых сумм.

Рассмотрим резольвенту

$$(-1, r) = \eta - \eta_1.$$

Не трудно видеть, что

$$\eta = \sum r^s \quad \text{и} \quad \eta_1 = \sum r^b,$$

где показатели: a пробегает совокупность квадратичных вычетов; b — совокупность невычетов; ибо, как известно, index'ы квадратичных вычетов суть числа четные, а index'ы квадратичных невычетов суть числа нечетные.

Итак, имеем

$$(-1, r) = \sum r^a - \sum r^b = \sum_{s=1}^{s=p-1} \left(\frac{s}{p}\right) r^s.$$

Будем рассматривать более общую сумму

$$S_k = \sum_{s=1}^{s=p-1} \left(\frac{s}{p}\right) r^{ks}.$$

Тогда $S_k = (-1, r^k)$. На оснований формулы (I) § 36 мы получаем

$$(-1, r)^2 = (-1)^{\frac{p-1}{2}} p,$$

откуда

$$S_1 = (-1, r) = \pm\sqrt{(-1)^{\frac{p-1}{2}} p}.$$

Указание знака в последней формуле представило Gauss'у, по его собственному признанию, большие затруднения. Оказывается, что этот знак зависит от корня r. Gauss публиковал свое решение вопроса о знаке в последней формуле в мемуаре: Summatio quarundam serierum singularium.

Мы не будем здесь заниматься этой задачей и отошлем читателя к книге проф. Д. А. Граве «Арифметическая теория алгебраических величин» т. I, в которой вопрос о знаке разобран со всей подробностью.

Применим Gauss'овы суммы к доказательству закона взаимности.

Итак, возьмем формулу

$$S_1^2 = (-1)^{\frac{p-1}{2}} \cdot p.$$

Пусть q будет другое простое (нечетное) число. Возвысим обе части последнего равенства в степень $\dfrac{q-1}{2}$.

Получим

$$S_1^{q-1} = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \cdot p^{\frac{q-1}{2}},$$

или

$$S_1^q = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} p^{q-1} 2 \cdot S_1. \tag{1}$$

Рассмотрим выражение[98]

$$S_k\left(\frac{k}{p}\right),$$

где k не делится на p.

Получаем

$$S_k\left(\frac{k}{p}\right) = \sum\left(\frac{ks}{p}\right) \cdot r^{ks}.$$

Если s пробегает полную систему вычетов по модулю p, то число $s' = sk$ будет пробегать ту же систему вычетов, и мы имеем

$$S_k\left(\frac{k}{p}\right) = \sum\left(\frac{s'}{p}\right) r^{s'} = S_1,$$

или иначе

$$S_k = \left(\frac{k}{p}\right) \cdot S_1. \tag{2}$$

Теперь на основании равенств (1) и (2) имеем

$$S_1^q - S_q = \left[(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} p^{\frac{q-1}{2}} - \left(\frac{q}{p}\right)\right] \cdot S_1. \tag{3}$$

Левая часть последнего равенства представляет из себя формулу

$$\left(\sum\left(\frac{s}{p}\right) r^s\right)^q - \sum\left(\frac{s}{p}\right) r^{qs}.$$

Но, так как q нечетное простое число, то

$$\left(\frac{s}{p}\right)^q = \left(\frac{s}{p}\right).$$

Значит, в последней разности при вычитании степени q отдельных членов пропадают. Значит, остаются только такие члены, у которых биномиальные коэффициенты имеют вид

$$\frac{q(q-1)\cdots 2\cdot 1}{1\cdot 2\cdot 3\cdots\alpha\cdot 1\cdot 2\cdots\beta\cdots 1\cdot 2\cdots\gamma},$$

[98] Свойства символа Legendre'а можно найти в книге Д. Граве. Элементарный курс теории чисел. 1913 г.

где

$$\alpha + \beta + \ldots + \gamma = q.$$

Эти коэффициенты суть целые числа, делящиеся на q, ибо простой множитель q в знаменателя совсем не входит, так как все числа $\alpha, \beta, \ldots, \gamma$ меньше q.

Значит, все коэффициенты при разных степенях r в правой части (3) делятся на q и мы получаем

$$(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} p^{q-1} 2 \equiv \left(\frac{q}{p}\right) (\mathrm{mod}\, q).$$

Но

$$p^{\frac{q-1}{2}} \equiv \left(\frac{p}{q}\right) (\mathrm{mod}\, q);$$

следовательно, имеем

$$(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \left(\frac{p}{q}\right) \equiv \left(\frac{q}{p}\right) (\mathrm{mod}\, q).$$

Так как обе части последнего сравнения суть единицы взятые с тем или другим знакомь, а модуль $q \neq 2$, то сравнение обращается в равенство, и мы получаем закон взаимности

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

§ 46

Что касается двух дополнений к закону взаимности, то первое дополнение состоящее в том, что

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

следует из самого определения (из так называемого эйлеровского критериума).

Второе дополнение будет состоять в формуле

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}},$$

т. е. число 2 есть квадратичный вычет простых чисел вида $8n \pm 1$ и невычет чисел вида $8n \pm 3$.

В самом деле, так как

$$\sum r^{ka} + \sum r^{kb} = -1$$

и

$$\sum r^{ka} - \sum r^{kb} = S_k = \left(\frac{k}{p}\right) S_1,$$

то отсюда находим сумму

$$\sum r^{ka} = \frac{1}{2}\left[-1 + \left(\frac{k}{p}\right)\cdot S_1\right],$$

что при $k = 2$ дает

$$\sum r^{2a} = \frac{1}{2}\left[-1 + \left(\frac{2}{p}\right) S_1\right].$$

Рассмотрим теперь разность

$$\left(\sum r^a\right)^2 - \sum r^{2a}. \tag{1}$$

Найдем сначала

$$\left(\sum r^a\right)^2.$$

Так как

$$\eta + \eta_1 = -1 \quad \text{и} \quad \eta - \eta_1 = S_1,$$

то

$$\eta = \frac{1}{2}(-1 + S_1).$$

Следовательно,

$$\left(\sum r^a\right)^2 = \eta^2 = \left[\frac{1}{2}(-1 + S_1)\right]^2.$$

Теперь разность (1) перепишется так:

$$\left(\sum r^a\right)^2 - \sum r^{2a} = \left[\frac{1}{2}(-1 + S_1)\right]^2 - \frac{1}{2}\left[-1 + \left(\frac{2}{p}\right)S_1\right],$$

или

$$\left(\sum r^a\right)^2 - \sum r^{2a} = \frac{1}{4} - \frac{S_1}{2} + \frac{S_1^2}{4} + \frac{1}{2} - \frac{1}{2}\left(\frac{2}{p}\right)S_1.$$

Но

$$A_1^2 = (-1)^{\frac{p-1}{2}} \cdot p;$$

следовательно,

$$\left(\sum r^a\right)^2 - \sum r^{2a} = \frac{3 + (-1)^{\frac{p-1}{2}} \cdot p}{4} - \frac{1}{2}\left[1 + \left(\frac{2}{p}\right)\right]S_1,$$

или, полагая $S_1 = \sum r^a - \sum r^b$, получим

$$\left(\sum r^a\right)^2 - \sum r^{2a} = \left\{\frac{1}{2}\left[1 + \left(\frac{2}{p}\right)\right] - \frac{3 + (-1)^{\frac{p-1}{2}}}{4}\right\} \cdot \sum r^b - \\ - \left\{\tfrac{1}{2}\left[1 + \left(\tfrac{2}{p}\right)\right] + \tfrac{3+(-1)^{\frac{p-1}{2}} \cdot p}{4}\right\} \cdot \sum r^a,$$

ибо $\sum r^b + \sum r^a = -1$.

Заметим, что в разности (1) все коэффициенты должны быть числа целые и четные.

Поэтому из последней формулы следует

$$2\left[1 + \left(\frac{2}{p}\right)\right] \equiv 3 + (-1)^{\frac{p-1}{2}} \cdot p \,(\mathrm{mod}\, 8).$$

Из этого сравнения видим, что для простых чисел p формы $8n \pm 1$ должно быть $\left(\frac{2}{p}\right) = +1$; а для чисел вида $8n \pm 3$, $\left(\frac{2}{p}\right) = -1$. Отсюда имеем

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Разложение простых чисел вида $4n+1$ на сумму двух квадратов

§ 47

Euler доказал очень важную теорему относительно простых чисел вида $4n+1$, а именно он показал, что простые числа этого вида раскладываются на сумму двух квадратов. причем это разложение совершается одним только способом.

Из этой теоремы получается дальнейшее следствие, состоящее в том, что если некоторое число вида $4n+1$ раскладывается двумя способами на сумму квадратов, то оно не может быть простым. Так например, $65 = 1^2 + 8^2$ и $65 = 7^2 + 4^2$, и, следовательно, это число не может быть простым.

В единственности разложения простого числа p на сумму двух квадратов можно будет убедиться так. Пусть число p раскладывается двумя способами на сумму квадратов, т. е.

$$p = x^2 + y^2$$

и

$$p = \xi^2 + \eta^2.$$

Тогда из тождества

$$(x^2 + y^2)(\xi^2 + \eta^2) = (x\xi + y\eta)^2 + (x\eta - y\xi)^2$$

имеем

$$p^2 = (x\xi + y\eta)^2 + (x\eta - y\xi)^2. \tag{1}$$

Переставляя буквы ξ и η, получим

$$p^2 = (x\xi - y\eta)^2 + (x\eta + y\xi)^2. \tag{2}$$

Кроме того,

$$(x\eta + y\xi)(x\eta - y\xi) = x^2\eta^2 - y^2\xi^2 = (p - y^2)\eta^2 - y^2(p - \eta^2) = p(\eta^2 - y^2);$$

так что окончательно имеем

$$p)\eta^2 - y^2) = (x\eta = y\xi)(x\eta - y\xi). \tag{3}$$

Из формулы (3) мы замечаем, что одно из целых чисел

$$x\eta + y\xi, \qquad x\eta - y\xi \tag{4}$$

должно делится на p.

Но по формулам (1) и (2) мы замечаем, что эти числа не превосходят числа p. Оба они не могут равняться p, потому что тогда первая часть равенства (3) делилась бы на p^2, что невозможно, ибо $\eta^2 - y^2$ по численной величин меньше p, так как оба числа η^2 и y^2 меньше p.

Значит, одно из чисел (4) должно равняться нулю, и мы получаем

$$x\eta = \pm y\xi,$$
$$x^2\eta^2 = y^2\xi^2,$$
$$(p - y^2)\eta^2 = (p - \eta^2)y^2,$$

откуда

$$\eta^2 = y^2 \quad \text{и} \quad \xi^2 = x^2,$$

и значить два разложения оказываются тождественными.

Теория функций ψ_λ дает общее решение задачи разложения простого числа вида $4n + 1$ на квадраты. В самом деле, по формуле

$$\psi_2(i)\psi_2(i^{-1}) = p$$

получаем

$$\psi_2(i) = A + Bi = \sum i^{\operatorname{ind} t - 3\operatorname{ind}(t+1)} = \sum i^{\operatorname{ind}(t^2+t)},$$

где A и B числа целые, и

$$\psi_2(i^{-1}) = A - Bi,$$

отсюда

$$p = A^2 + B^2.$$

Построение правильного 17-угольника

§ 48

Построение правильного 17-угольника, равносильное делению окружности на 17 равных частей, сводится аналитически на решение уравнения

$$\xi^{16} + \xi^{15} + \ldots + \xi^2 + \xi + 1 = 0.$$

Решая его, как возвратное, получим равенство

$$\xi + \frac{1}{\xi} = x$$

и уравнение

$$x^8 + x^7 - 7x^6 - 6x^5 + 15x^4 - 10x^3 - 10x^2 - 4x + 1 = 0. \tag{1}$$

Полагая

$$a = \frac{2\pi}{17},$$

получим

$$\xi = \cos ka + i \sin ka, \qquad \frac{1}{\xi} = \cos ka - i \sin ka,$$

так что

$$x = 2\cos ka. \tag{2}$$

При подстановке в выражение (2) значений

$$k = 1,\ 2,\ 3,\ \ldots,\ 16,$$

получим только восемь различных значений

$$2\cos a,\quad 2\cos 2a,\ \ldots,\ 2\cos 8a;$$

остальные выражения при $k > 8$ не дают новых корней, ибо

$$\cos ka = \cos(17 - k)a.$$

Формула

$$2\cos\alpha\cos\beta = \cos(\alpha + \beta) + \cos(\alpha - \beta)$$

показывает, что произведение двух из корней (2) § 47 дает сумму других двух из них

$$[2\cos ka]\ [2\cos la] = 2\cos(k + l)a + 2\cos(k - l)a.$$

§ 49

Покажем теперь, что абсолютные значения корней $2\cos ka$ уравнения (1) § 47 будут равны различным значениям сторон правильного вписанного 34-угольника.

Разделим полуокружность на 17 равных частей и поставим у точек деления числа

$$0,\quad 1,\quad 2,\ \ldots,\ 17.$$

Обозначим через ρ_k длину прямой, соединяющей 0 с k; число k будет взаимно простое с 34 тогда, когда оно будет нечетным и неравным 17; мы получим следующие восемь длин

$$\rho_1,\quad \rho_3,\quad \rho_5,\quad \rho_7,\quad \rho_9,\quad \rho_{11},\quad \rho_{13},\quad \rho_{15},$$

которые будут сторонами различных (звездчатых) правильных вписанных 34-угольников.

Мы замечаем, что

$$\rho_4 = 2\sin\frac{k\pi}{34}.$$

Тогда получается следующее выражение для корня уравнения (1) § 47.

$$2\cos ka = 2\sin\left(\frac{\pi}{2} - ka\right) = 2\sin\left(\frac{\pi}{2} - \frac{2k\pi}{17}\right) = 2\sin\frac{17 - 4k}{34}\pi = \pm\rho_{17-4k}.$$

Мы получаем

$$\begin{aligned} 2\cos a &= \rho_{13}, & 2\cos 5a &= -\rho_3,\\ 2\cos 2a &= \rho_9, & 2\cos 6a &= -\rho_7,\\ 2\cos 3a &= \rho_5, & 2\cos 7a &= -\rho_{11},\\ 2\cos 4a &= \rho_1, & 2\cos 8a &= -\rho_{15}. \end{aligned}$$

Полагая[99]

$$y = \rho_{13} - \rho_{15} + \rho_1 + \rho_0 = 2\cos a + 2\cos 3^2 a + 2\cos 3^4 a + 2\cos 3^6 a,$$
$$y_1 = \rho_6 - \rho_{11} - \rho_3 - \rho_7 = 2\cos 3a + 2\cos 3^3 a + 2\cos 3^5 a + 2\cos 3^7 a,$$

получим

$$y + y_1 = 1, \qquad yy_1 = -4.$$

Но y_1 число отрицательное, потому что $\rho_{11} > \rho_5$, следовательно, полагая $y_1 = -y'$, получим

$$y - y' = 1, \qquad yy' = 4. \tag{1}$$

Далее положим

$$z = \rho_{13} + \rho_1 = 2\cos a + 2\cos 3^4 a,$$
$$z_1 = -\rho_{15} + \rho_9 = 2\cos 3^2 a + 2\cos 3^6 a.$$

Очевидно, что z_1 отрицательно, ибо $\rho_{15} > \rho_9$, следовательно, полагая $z_1 = -z'$, получим

$$z - z' = y, \qquad zz' = 1. \tag{2}$$

Проделаем тоже самое для y_1:

$$u = \rho_5 - \rho_3 = 2\cos 3a + 2\cos 3^5 a,$$
$$u_1 = -\rho_{11} - \rho_7 = 2\cos 3^3 a + 2\cos 3^7 a.$$

Число u положительное, а число u_1 отрицательное. Полагая $u_1 = -u$, получим

$$u' - u = y', \qquad uu' = 1. \tag{3}$$

Наконец, имеем

$$x = \rho_{13}, \qquad x_1 = \rho_1,$$

откуда получаем

$$x + x_1 = z, \qquad xx_1 = u. \tag{4}$$

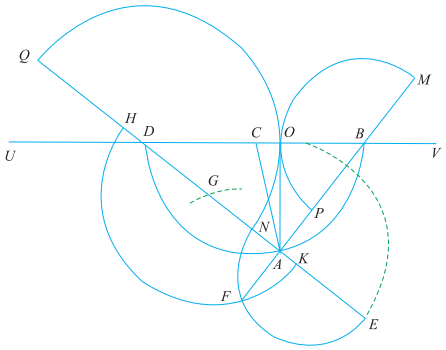
Построив x и x_1, получим ρ_1, сторону правильного 34-угольника, а, значить, и сторону правильного 17-угольника.

§ 50

Получаем следующее построение формулы (1), (2), (3), (4) предыдущего параграфа.

От точки C, взятой на произвольной прямой VU, откладываем отрезок CO, равный по величине $\frac{1}{4}$ произвольно выбранной единицы. Из точки O восставляем к прямой VU перпендикуляр и откладываем на нем единицу длины до точки A. Из

[99] Число 3 есть первообразный корень числа 17.



Черт. 16

точки C, как из центра, описываем окружность радиусом равным CA; обозначим его точки встречи с прямой VU буквами B и D. Нетрудно видеть, что

$$OB = \frac{y}{2}, \qquad OD = \frac{y'}{2};$$

в самом деле, имеем

$$\begin{aligned} 2OD - 2OB &= 4OC = 1, \\ 2OD \cdot 2OB &= 4OA^2 = 4. \end{aligned} \tag{1}$$

Соединим точку A с точками B и D прямыми AB и AD и продолжим каждую в обе стороны; из точки B, как из центра, радиусом равным длине OB опишем окружность, которая встретит прямую AB в точках P и M.

Нетрудно видеть, что

$$AM = z, \qquad AP = z';$$

в самом деле, имеем

$$\begin{aligned} AM - AP = PM &= 2OB = y, \\ AM \cdot AP &= OA^2 = 1, \end{aligned} \tag{2}$$

значит, равенства (2) § 49 имеют место.

Подобным же образом из точки D, как из центра, радиусом равным длине OD опишем окружность, которая встретит прямую DA в точках N и Q; нетрудно видеть, что

$$AN = u, \qquad AQ = u';$$

в самом деле, имеем

$$\begin{aligned} AQ - AN = NQ &= 2DO = y', \\ AN \cdot AQ &= OA^2 = 1, \end{aligned}$$

следовательно, наши равенства (3) § 49 имеют место.

Далее из точки A, как из центра, радиусом, равным $OA = 1$, опишем окружность пересекающуюся в точке E с прямою AD; на прямой EN, как на диаметре, построим круг, который пересечет продолжение прямой AB в точке F; из точки F, как из центра, радиусом, равным половине отрезка AM, делаем на прямой AD засечку в точке G; из точки G, как из центра, тем же радиусом описываем окружность; эта окружность проходит, очевидно, через точку F и встречает в точках K и H прямую AD.

Нетрудно видеть, что

$$AK = x_1, \qquad AH = x;$$

в самом деле,

$$AK + AH = 2KG = 2 \cdot \frac{MA}{2} = AM = z,$$

$$AK \cdot AH = FA^2 = AN \cdot AE = u \cdot 1 = u,$$

и, следовательно, AK есть сторона вписанного в круг тридцатичетыреугольника.

Полученная сторона AK соответствует тридцатичетыреуголнику, вписанному в круг радиуса равного единице, т. е. AO на нашем чертеже.

Глава XIX

Решение уравнений в радикалах

§ 1

Обращаемся теперь к задаче *алгебраического решения* уравнений, в которой требуется выразить корни заданного уравнения при помощи ряда радикалов. Теория групп делает замечательно простыми все относящиеся к этой задаче соображения.

§ 2

Если мы пожелаем ясно представить себе задачу, то придется рассуждать так: надо расширить основное поле Ω через последовательное присоединение ряда радикалов таким образом, чтобы в окончательно полученном поле заключались или все корни заданного уравнения, или, по крайней мере, некоторая часть этих корней.

Здесь являются два вопроса: 1) возможно ли такое расширение поля, 2) если оно возможно, то как осуществить это расширение.

Всякий новый присоединяемый радикал Z есть корень уравнения вида

$$Z^m = A, \tag{1}$$

где m натуральное число, а A величина из того поля, к которому радикал Z присоединяется.

Итак, указанное расширение поля совершается при помощи корней *двучленных* уравнений (1).

§ 3

Если неприводимое уравнение решается в радикалах, то его группа после присоединиения всех этих радикалов должна приводиться к единице.

Если выражается в радикалах только часть корней, то после присоединения этих радикалов уравнение должно сделаться приводимым, следовательно, его группа должна перестать быть транзитивною.

Мы знаем уже, что изменение группы от присоединения может состоять только в понижении ее порядка, поэтому в обоих случаях, решается ли уравнение вполне или получаются только некоторые корни, должно происходить понижение порядка группы.

§ 4

Присоединимся к способу рассуждения, предложенному Jordan'ом[100]. Так как всякое двучленное уравнение есть Abel'ево, то его решение сводится к решению ряда циклических уравнений простой степени. Надо напомнить, что при решении циклических уравнений вводятся корни из единицы, но эти корни суть сами корни Abel'евых уравнений и, следовательно, их выражение через радикалы сводится к ряду новых *циклических уравнений простой степени*.

Итак, можно сказать, что если корень заданного уравнения может быть выражен в радикалах, то он находится в поле, получаемом от присоединения к основному Ω ряда корней циклических уравнений простой степени.

§ 5

Итак, предположим, что мы произвели все необходимые для алгебраического вычисления корня заданного уравнения присоединения корней циклических уравнений. Группа понизилась. Пусть первое понижение порядка группы G заданного уравнения совершилось при присоединении некоторого определенного из ряда присоединенных корней. Таким образом мы приходим к задаче:

Найти условия, при которых возможно понижение порядка группы G данного уравнения при присоединении корня циклического уравнения простой степени p.

Для общности можно заданное уравнение не предполагать неприводимым, достаточно требование лишь неравенства корней.

Итак, пусть понижение группы G совершается от присоединения корня ξ циклического уравнения $\varphi(x) = 0$ простой степени p. Мы будем предполагать, что поле Ω, к которому мы присоединяем ξ, получено из основного через все предшествовавшие присоединения.

Пусть корни уравнения $\varphi(x) = 0$ будут

$$\xi, \quad \xi_1, \quad \xi_2, \ \ldots, \ \xi_{p-1}.$$

Так как циклическое уравнение есть Abel'ево, то мы имеем

$$\xi_1 = \mathfrak{D}(\xi), \quad \xi_2 = \mathfrak{D}_2(\xi), \ \ldots, \ \xi_{p-1} = \mathfrak{D}_{p-1}(\xi).$$

Итак, пусть присоединение ξ сводит группу G на ее делитель G_1 с индексом j; значит, в поле $\Omega(\xi)$ группа Galois для заданного уравнения будет G_1.

В § 26 главы XVII мы видели, что индекс j должен быть делителем p, но p число простое, следовательно, $j = p$. В том же параграфе мы видели, что корень ξ должен быть натуральною иррациональностью

$$\xi = \omega(x_0, x_1, \ldots, x_{p-1}).$$

Функция ω принадлежит к группе G_1. Если мы разложим группу G на сопряженные системы по подгруппе G_1, то получим

$$G = G_1 + G_1S_1 + G_1S_2 + \ldots + G_1S_{p-1},$$

[100] C. Jordan. Traité des substitution. P. 386.

где подстановка S_i переводить корень ξ в ξ_i.

Группа, к которой принадлежит корень ξ_i, есть

$$S_i^{-1} G_1 S_i.$$

Так как корни ξ и ξ_i, на основании свойств Abel'евых уравнений выражаются рационально один через другой, то, значить, они принадлежать к одной и той же группе

$$G_1 = S_i G_1 S_i.$$

Так как последнее равенство имеет место при всяком значений i, то подгруппа G_1 есть нормальный делитель группы G. Мы приходим к следующей основной теореме:

Для возможности решения в радикалах уравнения необходимо, чтобы его группа G имела нормальный делитель G_1 простого индекса.

О разрешимых группах

§ 6

Обращаемся теперь к нахождение *необходимого и достаточного* условия для полной решимости в радикалах заданного уравнения. Если все корни уравнения выражаются в радикалах, то группа уравнения присоединения всех этих радикалов должна свестись к единице.

Мы видели уже, что группа G разрешимого в радикалах уравнения должна иметь нормальный делитель G_1 простого индекса p. Если $G_1 = I$, то группа G есть циклическая простого порядка. Если же группа G_1 отлична от единицы, то мы можем применить к ней те же самые рассуждения и получить, что эта группа G_1 должна иметь новый нормальный делитель G_2 простого индекса p_1 и т. д.

Определение. Мы будем называть разрешимою всякую группу G, для которой можно составить ряд подгрупп

$$G, \quad G_1, \quad G_2, \ \ldots, \ G_{\mu-1}, \quad I,$$

в котором каждая следующая группа G_{i+1} есть нормальный делитель предыдущей G_i, имеющий простой индекс p_i ($G_0 = G$, $p_0 = p$.

§ 7

Теорема. *Необходимым и достаточным условием возможности алгебраического решения уравнения является свойство разрешимости его группы.*

Свойство разрешимости группы надо понимать в смысли определения предыдущего параграфа.

Необходимость теоремы следует непосредственно из соображений §§ 5, 6. Обращаемся теперь к доказательству ее достаточности.

Итак, пусть группа G данного уравнения *разрешимая*, докажем, что все корни уравнения выражаются в радикалах.

Мы имеем ряд подгрупп

$$G, \quad G_1, \quad G_2, \ \ldots, \ G_{\mu-1}, \quad I$$

простых индексов.

Пусть индекс G_1 относительно G есть простое число p. Берем функцию $\omega(x_0, x_1, \ldots, x_{n-1})$ корней заданного уравнения, принадлежащую *точно* подгруппе G_1, тогда, применяя к функции ω все подстановки группы G, получим выражения

$$\omega, \quad \omega_1, \quad \omega_2, \ \ldots, \ \omega_{p-1}, \tag{1}$$

которые будут корнями некоторого уравнения

$$\varphi(x) = 0 \tag{2}$$

степени p неириводимого в основном поле Ω.

Вследствие нормальности подгруппы G_1 все величины (1) принадлежать одной и той же группе G_1, следовательно, все они выражаются рационально через одну ω. Уравнение (2) Abel'ево и в тоже время, будучи простой степени, циклическое. Присоединение ω к полю Ω сводится на основании § 15 главы XVII группу уравнения G к подгруппе G_1. Но величина ω, как корень циклического уравнения выражается в радикалах, следовательно, понижение группы на подгруппу G_1 совершается через присоединение радикалов. Подобным же образом можно будет далее понизить группу до подгруппы G_2 через присоединение новых радикалов и так далее до конца, когда группа обратится в единицу и получится полное алгебраическое решение заданного уравнения.

§ 8

Остается сказать два слова относительно случая, когда некоторые из корней заданного уравнения выражаются в радикалах.

Если не предполагать *неприводимости* уравнения, то ни каких заключений сделать нельзя, ибо возможны самые разнообразный явления.

Перемножим два уравнения

$$f_1(x) = 0, \qquad f_2(x) = 0;$$

тогда получим новое

$$f(x) = f_1(x) f_2(x) = 0. \tag{1}$$

Если уравнение $f_1(x) = 0$ решается вполне в радикалах, то часть корней уравиения (I) выражается в радикалах, причем, если $f_2(x) = 0$ решается также в радикалах, то имеет место случай полного решения уравнения (1). Если же уравнение $f_2(x) = 0$ не решается в радикалах, то не будет существовать полного решения в радикалах уравнения (1).

Если мы будем рассматривать неприводимые уравнения, то для них существует теорема, замеченная Abel'ем.

Если один корень неприводимого уравнении получается через решение ряда циклических уравнений, то уравнение допускает полное алгебраическое решение.

Не смотря на большую важность этой теоремы Abel'я, мы не будем останавливаться на ее доказательстве, отсылая читателя к доказательству, данному профессором Д. Ф. Селивановым[101].

[101] D. Seliwanoff. Acta Mathematica t. 19, 1895.

§ 9

Примером разрешимой группы может служить симметрическая группа G подстановок четырех букв. Если мы обозначим через A ее знакопеременную группу, через V — Vierergruppe и, наконец, через Q — группу (4) § 22 главы XV.

Мы будем иметь ряд подгрупп

$$G, \quad A, \quad V, \quad Q, \quad I$$

с индексами

$$2, \quad 3, \quad 2, \quad 2.$$

Так как эти индексы суть *простые* числа, то группа G *разрешимая* и общее уравнение 4-й степени решается в радикалах.

Приведенное нами в § 23 главы XV полное решение уравнения 4-ой степени есть не что иное, как осуществление на конкретном примере соображений доказательства, приведенного в § 7.

§ 10

Определение *разрешимой* группы находится в связи со следующими весьма важными рассуждениями Jordan'a.

Пусть рассматривается произвольно взятая группа G. Если она простая и не имеет нормальных делителей, то пишем только два знака

$$G, \quad I.$$

Допустим, что группа G имеет нормальный делитель G_1, обладающий свойством не заключаться в другом нормальном делителе большего порядка. Для группы G_1 составляем подобный же нормальный делитель G_2 и продолжаем далее пока не дойдем до простой группы $G_{\mu-1}$, имеющей, следовательно, единицу единственным нормальным делителем.

Полученный ряд последовательных нормальных делителей

$$G, \quad G_1, \quad G_2, \ \ldots, \ G_{\mu-1}, \quad I \tag{1}$$

носит название *ряда Jordan'a, для заданной группы* G.

Пусть будет соответствующий ряду (1) ряд индексов

$$p, \quad p_1, \quad p_2, \ \ldots, \ p_{\mu-1}. \tag{2}$$

Определение *разрешимости* состоит в том, что числа ряда (2) все простые.

Jordan доказывает относительно ряда (1) следующую весьма важную теорему:

Разложение группы G *в ряд* (1) *по нормальным делителям может быть произведено на несколько способов, но при всех этих различных разложениях ряд* (2) *состоит всегда из тех же чисел, только, быть может, расположенных в другом порядке.*

Можно сказать, что, если группа G заданного уравнения имеет ряд (1) нормальных делителей, то решение заданного уравнения сводится к решений ряда нормальных уравнений

$$\varphi(x) = 0, \quad \varphi_1(x) = 0, \ \ldots, \ \varphi_{\mu-1}(x) = 0 \tag{3}$$

степеней $p, p_1, p_2, \ldots, p_{\mu-1}$.

Если числа (2) все простые, то уравнения (3) все циклические и происходит полное алгебраическое решение заданного уравнения. Если степень p_i некоторого уравнения $\varphi_i(x) = 0$ число *не простое*, то это уравнение не решается в радикалах. В самом деле. Hölder'овская группа $\dfrac{G_i}{G_{i1}}$ уравнения $\varphi_i(x) = 0$ простая, ибо G_{i+1} есть нормальный делитель G_i, не заключающийся в большем (см. § 23 главы XVII). Следовательно, не имея других нормальных делителей кроме единицы и будучи составного порядка, группа уравнения $\varphi_i(x) = 0$ не может быть разрешимою.

Теорема Jordan'a о неизменности ряда индексов может иметь значение в том смысле, что трудность решения уравнения не меняется, как бы не вести само решение, ибо придется проходить через нормальные уравнения тех же степеней.

Я не буду останавливаться на доказательстве теоремы Jordan'a по следующим соображениям. Если уравнение не решается в радикалах, то теорема Jordan'a имеет мало практического значения. Если уравнение алгебраически решается, то теорема Jordan'a имеет значение главным образом при сравнении разных радикальных выражений одного и того же корня. Последний вопрос имеет мало значения для нашего элементарного изложения.

Теорема Abel'я

§ 11

Теорема. *Уравнения выше четвертой степени, не имеющие аффекта, не решаются в радикалах.*

На основании доказанного в § 51 главы V мы видим, что симметрическая группа G подстановок более четырех элементов не имеет других нормальных делителей кроме знакопеременной группы A. В § 50 главы V доказано, что при числе элементов более четырех группа A простая, имеющая, следовательно, единственным нормальным делителем единичную группу.

Итак, единственный возможный ряд Jordan'a есть

$$G, \quad A, \quad I$$

с индексами

$$2, \quad \frac{1 \cdot 2 \cdot 3 \cdots n}{2};$$

таким образом мы замечаем, что группа G *не разрешимая* и теорема Abel'я доказана.

Доказанная нами теорема заключаешь как частный случай теорему, относящуюся к буквенным уравнениям.

Буквенные уравнения выше четвертой степени не решаются в радикалах.

Решение численных уравнений

§ 12

Теорема. *Разрешимая группа имеет отличный от единицы коммутативный нормальный делитель.*

Для группы простого порядка теорема, очевидно, имеет место, ибо эта группа как циклическая есть сама коммутативная. Для доказательства общей теоремы употребим способ индукции: предположим, что теорема справедлива для групп меньшого порядка.

Если задана разрешимая группа G, то эта группа имеет нормальный делитель G_1 простого индекса. Предположим, что для группы G_1 теорема справедлива, т. е. что она имеет коммутативный нормальный делитель H_1 покажем, что подобный нормальный делитель H будет иметь и заданная группа G. Если H_1 есть в тоже время нормальный делитель группы G, то теорема доказана, ибо можно положить $H = H_1$.

Если H_1 не есть нормальный делитель группы G, то преобразовывая всеми элементами G группу H_1, получим ряд сопряженных групп

$$H_1, \quad H_2, \ \ldots, \ H_k. \tag{1}$$

Все эти группы будут коммутативными, как изоморфные с H_1. Кроме того все эти группы будут нормальные делители группы G_1, ибо группа $H_2 = S^{-1}H_1S$ должна быть нормальным делителем группы $S^{-1}G_1S$, а эта последняя совпадает с G_1.

Если группы (1) имеют общее пересечение R, то группа R будет нормальным делителем G и теорема опять доказана, если только R отлично от единицы.

Остается рассмотреть лишь случай $R = I$.

Предположим, что за H_1 выбран коммутативный нормальный делитель группы G_1 *наименьшего* порядка, тогда, очевидно, общим элементом каждых двух групп H_i и H_k может быть только единица, ибо, иначе, общий делитель H_i и H_k дал бы коммутативный нормальный делитель меньшого порядка.

Возьмем произвольно элемент A из группы H_i, а также произвольный элемента B из группы H_k и рассмотрим произведение

$$A^{-1}B^{-1}AB. \tag{2}$$

Если это произведение перепишем так

$$(A^{-1}B^{-1}A)B,$$

то оно принадлежит к группе H_k, ибо $A^{-1}B^{-1}A$ как преобразование элемента B^{-1} нормального делителя H_k при помощи элемента A группы G_1 должно давать новый элемент того же нормального делителя. Подобным же образом, переписывая произведение (2) так

$$A^{-1}(B^{-1}AB),$$

замечаем, что оно заключается в группе H_i.

Итак, произведение (2) должно быть общим элементом двух групп H_i, H_k, то есть

$$A^{-1}B^{-1}AB = I,$$

или, окончательно,

$$AB = BA.$$

Мы пришли к теореме, что элементы разных групп (1) перестановочны.

Пусть A_i пробегает всю группу H_i, тогда элементы

$$A = A_1 A_2 \cdots A_i \cdots A_k$$

образуют некоторую группу H.

Докажем, что группа H будет искомым коммутативным нормальным делителем группы G.

Коммутативность группы H следует из перестановочности элементов разных групп (1) и из коммутативности каждой из этих групп в отдельности. Чтобы убедиться в том, что H нормальный делитель G, достаточно написать формулу

$$S^{-1}S = (S^{-1}A_1S)(S^{-1}A_2S)\cdots(S^{-1}A_kS).$$

§ 13

Итак, мы пришли к убеждению, что всякая разрешимая группа должна иметь отличный от единицы коммутативный нормальный делитель. Покажем, что единственное возможное предположение состоит в том, что порядок этого нормального делителя должен равняться

$$p^\omega,$$

т. е., степени простого числа p.

В самом деле, допустим, что порядок m коммутативного нормального делителя H есть

$$m = ab,$$

произведение двух взаимно простых отличных от единицы чисел a и b, тогда мы покажем, что *можно найти два другим коммутативных нормальных делителя* $\mathfrak{H}_1$ *и* $\mathfrak{H}_2$ *порядков* a *и* b.

Существование двух делителей $\mathfrak{H}_1$ и $\mathfrak{H}_2$ ведет к противоречию, а именно; если мы будем предполагать заданное уравнение примитивным[102], то оба делителя (см. § 13 главы VII) должны быть транзитивными, следовательно, степень n заданного уравнения должна делить оба порядка a и b, что невозможно.

§ 14

Итак, займемся доказательством предложения, что если разрешимая группа G имеет Abel'ев нормальный делитель H порядка $m = ab$, то она имеет подобный же делителя $\mathfrak{H}$ порядка a. Для этой цели войдем в некоторые подробности относительно абелевых групп вообще.

Пусть H будет абелева группа порядка m, а

$$S_1 = I, \quad S_2, \ \ldots, \ S_m \tag{1}$$

ее элементы, порядки которых пусть будут

$$a_1, \quad a_2, \ \ldots, \ a_m.$$

[102]Очевидно, что только такие уравнения и подлежат исследованию.

Пусть $\xi_1, \xi_2, \ldots, \xi_m$ принимают значения полной системы вычетов по модулям $a_1, a_2, \ldots, a_m$, тогда всякий элемент группы (1) может быть представлен в таком виде

$$S_1^{\xi_1} S_2^{\xi_2} \cdots S_m^{\xi_m} \tag{2}$$

и притом одинаковое число раз. Очевидно, что всякий элемент S_i группы (1) получится, полагая в (2)

$$\xi_1 = 0, \ \ldots, \ \xi_{i-1} = 0, \quad \xi_i \ \ \xi_{i+1} = 0, \ \ldots, \ \xi_m = 0.$$

Докажем теперь, что *при различных значениях показателей ξ_i каждый элемент будет повторяться одинаковое число раз.*

Рассмотрим равенство

$$S_1^{x_1} S_2^{x_2} \cdots S_m^{x_m} = I. \tag{3}$$

Положим, что мы нашли все системы целых положительных чисел $x_1, x_2, \ldots, x_m$, удовлетворяющая равенству (3). Обозначим число таких систем через M, тогда нетрудно видеть, что каждый элемент S группы может иметь M представлений в форме (2).

В самом деле, предположим, что элемент S получается при некоторой системе

$$\xi_1, \quad \xi_2, \ \ldots, \ \xi_m$$

показателей; тогда тот же элемент S получится и при систем

$$\xi_1 + x_1, \quad \xi_2 + x_2, \ \ldots, \ \xi_m + x_m, \tag{4}$$

ибо

$$S_1^{\xi_1+x_1} S_2^{\xi_2+x_2} \cdots S_m^{\xi_m+x_m} = S_1^{\xi_1} S_2^{\xi_2} \cdots S_m^{\xi_m} (S_1^{x_1} S_2^{x_2} \cdots S_m^{x_m}) = S_1^{\xi_1} S_2^{\xi_2} \cdots S_m^{\xi_m}.$$

С другой стороны, других представлений этого элемента S, не получающихся при помощи показателей (4), не существует.

В самом деле, рассмотрим какое нибудь другое представление того же элемента S

$$S_1^{\eta_1} S_2^{\eta_2} \cdots S_m^{\eta_m}.$$

Тогда получаем

$$S_1^{\eta_1} S_2^{\eta_2} \cdots S_m^{\eta_m} = S_1^{\xi_1} S_2^{\xi_2} \cdots S_m^{\xi_m}$$

или

$$S_1^{\eta_1-\xi_1} S_2^{\eta_2-\xi_2} \cdots S_m^{\eta_m-\xi_m} = I.$$

Значит, разности

$$\eta_1 - \xi_1, \quad \eta_2 - \xi_2, \ \ldots, \ \eta_m - \xi_m$$

должны представлять одну из систем чисел

$$x_1, \quad x_2, \ \ldots, \ x_m$$

и мы получаем, следовательно,

$$\eta_1 = \xi_1 + x_1, \quad \eta_2 = \xi_2 + x_2, \ \ldots, \ \eta_m = \xi_m + x_m,$$

т. е. показатели

$$\eta_1, \quad \eta_2, \ \ldots, \ \eta_m$$

выражаются по формулам (4).

Итак, мы видим, что число представлений всякого элемента S равно M.

Будем давать в формуле (2) показателям значения, пробегающие полные системы вычетов по модулям $a_1, a_2, \ldots, a_m$. Число получаемых таким образом выражений будет равно произведению $a_1 a_2 \cdots a_m$; при этом будут получаться все m элементов группы, причем каждый M раз, и мы получаем равенство

$$a_1 a_2 \cdots a_m = mM. \tag{5}$$

Равенство (5) показывает, что всякое простое число p, входящее в порядок m группы, должно входить множителем в порядок a_i, по крайней мере, одного из элементов S_i группы. Итак, $a_i = p\alpha$; тогда элемент S_i^{α} группы будет иметь порядок, равный простому числу p и мы получаем такое предложение: *всякому простому числу p, входящему в порядок группы, соответствует, по крайней мере, один элемент группы, имеющий этот порядок.*

Нетрудно видеть, что если $A, B, C, \ldots$ суть элементы абелевой группы, порядки которых суть $\alpha, \beta, \gamma, \ldots$, то произведение $ABC\cdots$ имеет порядок, равный делителю наименьшего краткого μ чисел $\alpha, \beta, \gamma, \ldots$. Такое свойство следует прямо из формулы

$$(ABC\cdots)^{\mu} = A^{\mu} B^{\mu} C^{\mu} \cdots = I.$$

§ 15

Покажем теперь, что в *абелевой группе H порядка $m = ab$, где числа a и b взаимно простые, существует ровно a элементов A, порядки которых суть делители числа a, и ровно b элементов B, порядки которых суть делители числа b.*

Совокупность элементов A образует, очевидно, некоторую подгруппу $\mathfrak{A}$, а совокупность элементов B образует подгруппу $\mathfrak{B}$. Пусть a' будет порядок подгруппы $\mathfrak{A}$, а b' порядок подгруппы $\mathfrak{B}$.

Группы $\mathfrak{A}$ и $\mathfrak{B}$ не могут иметь кроме единицы других общих элементов. Покажем, что число a' (порядок $\mathfrak{A}$) взаимно простое с b.

Пусть p одно из простых чисел, делящих a'. На оснований соображений предыдущего параграфа существует в $\mathfrak{A}$ элемент порядка p; значит, число p делит число a, а не число b.

Подобным же образом докажем, что число b' (порядок $\mathfrak{B}$) взаимно простое с a.

Рассмотрим символическое произведение

$$\mathfrak{AB},$$

обозначающее совокупность элементов вида

$$AB,$$

где A пробегает группу $\mathfrak{A}$, а B группу $\mathfrak{B}$.

Покажем, что

$$\mathfrak{A}\mathfrak{B} = H. \tag{1}$$

В самом деле, всякий элемент вида AB есть в тоже самое время элемент из H и обратно, можно показать, что всякий элемент S из H имеет вид AB. Для доказательства этого найдем два числа x и y, удовлетворяются равенству

$$ax + by = 1,$$

тогда имеем

$$S = S^{ax} \cdot S^{by}, \tag{2}$$

но очевидно, что

$$(S^{ax})^b = I, \qquad (S^{by})^a = I, \tag{3}$$

ибо $ab = m$, а $S^m = I$ при всяком элементе S любой группы порядка m.

Формула (2) убеждает в справедливости того, что надо доказать, ибо на основании (3) S^{by} есть элемент из $\mathfrak{A}$, а S^{ax} элемент из $\mathfrak{B}$.

Для довершения доказательства формулы (1) достаточно убедиться, что всякий элемент S группы H только одним способом представляется в виде AB.

Допуская возможность двух подобного вида представлений, получим

$$AB = A_1B_1,$$

или, переписывал иначе,

$$AA_1^{-1} = BB_1^{-1} = C.$$

Элемент C принадлежит к $\mathfrak{A}$, если судить по его выражению AA_1^{-1}, и принадлежит также к группе $\mathfrak{B}$, если судить по выражению BB_1^{-1}; следовательно, $C = I$, откуда $AA_1^{-1} = I$, $BB_1^{-1} = I$, или

$$A_1 = A, \qquad B_1 = B.$$

Итак, формула (1) справедлива.

Получаем, очевидно, $m = a'b'$ по числу различных между собой произведений AB.

Равенство

$$ab = a'b'$$

приводить, очевидно, к двум следующим

$$a' = a, \qquad b' = b,$$

и теорема, поставленная в начале параграфа, доказана вполне.

§ 16

Пусть H есть нормальный абелевский делитель разрешимой группы G. Покажем, что, если порядок H есть $m = ab$, где a и b два отличных от единицы взаимно простых числа, то можно найти другой абелевский нормальный делитель $\mathfrak{H}$ группы G, порядок которого будет a.

Пусть группа H состоит из элементов

$$S_1, \quad S_2, \ \ldots, \ S_m.$$

Тогда возвысим эти элементы в степень b, получаем

$$S_1^b, \quad S_2^b, \ \ldots, \ S_m^b.$$

Некоторые из этих элементов (1) будут одинаковые. Покажем, что различные из них образуют искомую группу $\mathfrak{H}$.

Формула

$$\Sigma^{-1} S_1^b \Sigma = (\Sigma^{-1} S_1 \Sigma)^b = S_k^b, \tag{1}$$

где Σ произвольный элемент из G, показывает, что $\mathfrak{H}$ нормальный делитель G. Покажем, что порядок $\mathfrak{H}$ как раз равен числу a.

Очевидно, что порядок каждого из элементов (1) есть делитель числа a, ибо порядок каждого элемента S_i группы H есть делитель порядка $m = ab$ этой группы.

С другой стороны, среди элементов (1) заключается всякий элемент S_e, порядок которого есть делитель числа a. В самом деле, если $S_e^a = I$, то, подбирая числа x и y так, чтобы было $ax + by = 1$, мы получим

$$S_e = S_e^{ax} S_e^{by} = (S_e^y)^b = S_\lambda^b,$$

т. е., элемент S_e, заключается между элементами (1).

Припоминая предыдущий параграф, мы приходим к заключению, что порядок группы $\mathfrak{h}$ есть a.

§ 17

Сопоставляя последние результаты с соображениями § 13, мы приходим к заключению, что всякая примитивная разрешимая группа G должна иметь отличного от нуля абелев нормальный делитель $\mathfrak{H}$ порядка p^ω, где p простое число, а ω некоторое натуральное число.

Группа $\mathfrak{H}$ должна быть транзитивна, иначе группа G будет импримитивной. Следовательно, степень n уравнения, подлежащего изучению, должна быть делителем числа p^ω то есть

$$n = p^\mu.$$

Мы пришли таким образом к знаменитой теореме Abel'я[103]

[103] M D. Gravé. Comment on écrit les revues encyclopediques. Протоколы Киевск. Физико-Матем. Общества.

Всякое решаемое в радикалах неприводимое уравнение, степень которого делится по крайней мере на два различных простых числа, должно быть imprimитивным.

Этой теореме Galois[104] дает иную формулировку.

Для разрешимости в радикалах примитивного уравнения степени m должно быть $m = p^\nu$, где p простое число.

§ 18

Итак, пусть $\mathfrak{G}$ будет коммутативный нормальный делитель группы G, имеющий порядок p^k с возможно малым показателем k, так что всякий отличный от единицы делитель группы $\mathfrak{G}$ *не будет* уже нормальным делителем G.

Покажем, что все элементы $\mathfrak{G}$ имеют порядок p.

Допустим, что есть по крайней мере один элемент порядка p^λ, где $\lambda > 1$. Рассмотрим совокупность $\mathfrak{R}$ элементов из $\mathfrak{G}$ таких, порядки которых не выше $p^{\lambda-1}$. Совокупность $\mathfrak{R}$ будет группа отличная, очевидно, от единицы. Нетрудно убедиться, что $\mathfrak{R}$ будет нормальном делителем группы G.

В самом деле, если мы возьмем один элемент K из $\mathfrak{r}$, то очевидно, что $S^{-1}KS$ будет иметь тот же порядок, что и K, т. е. $S^{-1}KS$ будет принадлежать к той же группе $\mathfrak{R}$. Мы пришли к противоречию, ибо мы предположили, что группа $\mathfrak{G}$ не может иметь делитель подобный $\mathfrak{R}$. Итак, $\lambda = 1$.

§ 19

Чтобы рассмотреть ближе свойства группы $\mathfrak{R}$ воспользуемся ее свойством, что порядок каждого ее элемента, отличного от единицы, есть p.

Возьмем произвольный элемент A_1 порядка p группы $\mathfrak{G}$.

В группу $\mathfrak{G}$ должны входить все степени A_1, т. е.

$$I, \quad A_1, \quad A_1^2, \ \ldots, \ A_1^{p-1}. \tag{1}$$

Другими словами группа G имеет подгруппу $A_1^{x_1}$, где x_1 пробегает всю систему вычетов $0, 1, 2, \ldots, p-1$ по модулю p. Если $k = 1$, то группа (1) совпадает с G. Если же $k > 1$, тогда в группе G кроме элементов (1) должен заключаться по крайней мере еще один элемент A_2, который тоже по предыдущему параграфу имеет порядок p. В группе G будет заключаться подгруппа

$$A_1^{x_1} A_2^{x_2}, \tag{2}$$

в которой x_1 и x_2 пробегают полную систему вычетов по модулю p. Покажем, что порядок группы (2) есть p^2; для этой цели надо показать, что при двух системах показателей x_1, x_2 не могут получаться одинаковые элементы. Допустим обратное

$$A_1^{x_1} A_2^{x_2} = A_1^{x_1'} A_2^{x_2'};$$

если $x_2 = x_2'$, то, сокращая равенство на $A_2^{x_2}$, получим $A_1^{x_1} = A_1^{x_1'}$, которое дает $x_1 = x_1'$, ибо все элементы (1) различны. Если x_2 не $\equiv x_2' \pmod p$, то, обозначая

[104] E, Galois, Oevres complétes, p. 11.

$x_1 - x_1' = \xi_1$, $x_2' - x_2 = \xi_2$, получим

$$A_1^{\xi_1} = A_2^{\xi_2}; \tag{3}$$

подбирая же τ удовлетворяющее сравнению $\xi_2\tau \equiv 1 \pmod p$ и возвышая равенство (3) в степень τ, получим

$$A_2 = A_1^{\xi_1\tau},$$

что невозможно, ибо мы предположили, что элемента A_2 отличен от элементов (1).

Итак, элементы (2) все различны между собой и образуют группу порядка p^2. Если $k = 2$, то группа (2) совпадает с G.

Если же $k > 2$, тогда в группе G кроме элементов (2) должен заключаться по крайней мере еще один элемент A_3.

Составляем подгруппу

$$A_1^{x_1} A_2^{x_2} A_3^{x_3}$$

порядка p^3. Продолжая рассуждение далее, мы исчерпаем группу G порядка p^k после k-кратного повторения приведенных рассуждений.

Итак, группа G имеет элементы вида

$$A_1^{x_1} A_2^{x_2} \cdots A_k^{x_k}, \tag{4}$$

где все показатели $x_1, x_2, \ldots, x_k$ пробегают (каждый в отдельности) систему вычетов по модулю p.

Совокупность элементов $A_1, A_2, \ldots, A_k$ носит название *базиса* группы G.

§ 20

Если заданное уравнение *примитивное*, то нормальный его делитель

$$G = A_1^{x_1} A_2^{x_2} \cdots A_k^{x_k}$$

должен быть *транзитивным*.

Присоединяя к основному полю Ω функцию корней, принадлежащую, группе G, мы сведем группу заданного уравнения на группу G. Уравнение останется после такого расширения группы неприводимым; но группа его коммутативная, следовательно, уравнение окажется Abel'евым. Его степень должна равняться порядку группы G, то есть p^k. Для ясности можно указывать корни различными подстановками группы G. Каждой подстановке сопоставить корень. Можно будет поступить так, один корень x_0 взять произвольно и затем всякой подстановка $A_1^{z_1} A_2^{z_2} \cdots A_k^{z_k}$ сопоставить тот корень x_λ, в который переходить x_0 от этой подстановки.

Итак, корень, соответствующий подстановке $A_1^{z_1} A_2^{z_2} \cdots A_k^{z_k}$ можно будет обозначить одним из двух символов

$$x_{z_1, z_2, \ldots, z_k}, \qquad [z_1, z_2, \ldots, z_k].$$

Очевидно, что если за начальный корень взять тот, который указан символом

$$[0, 0, \ldots, 0],$$

то этот корень от применения подстановки $A_1^{z_1}A_2^{z_2}\cdots A_k^{z_k}$ обращается в $[z_1, z_2, \ldots, z_k]$, ибо

$$(A_0^0 A_2^0 \cdots A_k^0)(A_1^{z_1}A_2^{z_2}\cdots A_k^{z_k}) = A_1^{z_1}A_2^{z_2}\cdots A_k^{z_k}.$$

Корень $[z_1, z_2, \ldots, z_k]$ обращается через подстановку

$$A_1^{\alpha_1}A_2^{\alpha_2}\cdots A_k^{\alpha_k} \quad \text{в} \quad [z+\alpha_1, z_2+\alpha_2, \ldots, z_k+\alpha_k].$$

При заданных $\alpha_1, \alpha_2, \ldots, \alpha_k$ линейные выражения

$$z+\alpha_1, \quad z_2+\alpha_2, \ \ldots, \ z_k+\alpha_k$$

пробегают (каждое в отдельности) полную систему вычетов по модулю p, если z_i пробегает туже систему вычетов.

Подстановке корней

$$A_1^{\alpha_1}A_2^{\alpha_2}\cdots A_k^{\alpha_k} \tag{1}$$

можно дать такое толкование, которое мы будем называть *аналитическим ее представлением.*

Если мы будем рассматривать сравнения[105]

$$z_1' \equiv z_1+\alpha_1 \,(\mathrm{mod}\, p), \quad z_2' \equiv z_2+\alpha_2 \,(\mathrm{mod}\, p), \ \ldots, \ z_k' \equiv z_k+\alpha_k \,(\mathrm{mod}\, p), \tag{2}$$

то подстановке (1) соответствует переход *всякого* корня

$$[z_1, z_2, \ldots, z_k]$$

в *новый*

$$[z_1', z_2', \ldots, z_k'].$$

Итак, всякой подстановки (1) с *определенно-выбранными* показателями $\alpha_1, \alpha_2, \ldots, \alpha_k$ можно сопоставить систему сравнений (2).

Эта система сравнений (2) и есть аналитическое представление подстановки (1). Заставляя в сравнениях (2) числа $\alpha_1, \alpha_2, \ldots, \alpha_k$ пробегать полные системы вычетов по модулю p, мы получим все p^k подстановок группы G. Будем для сокращения речи называть группу G *арифметическою*[106].

Аналитическое представление подстановок

§ 21

Обобщая сказанное в предыдущем параграф мы можем высказать теорему.

Если указана некоторая, произвольно выбранная, подстановка корней, переводящая

$$[z_1, z_2, \ldots, z_k] \quad \textit{в} \quad [z_1', z_2', \ldots, z_k']$$

[105]Очевидно, что индексы ?, сравнимые по модулю ?, можно считать за равные и заменять положительными их вычетами.

[106]О. Шмидт. Об уравнениях, решаемых в радикалах, степень которых есть степень простого числа. Киев. 1913 стр. 15.

то эту подстановку можно указать сравнениями

$$(1)\qquad \left.\begin{aligned} z'_1 &\equiv \varphi_1(z_1, z_2, \ldots, z_k),\\ z'_2 &\equiv \varphi_2(z_1, z_2, \ldots, z_k),\\ &\ldots\ldots\ldots\ldots\ldots\\ z'_k &\equiv \varphi_k(z_1, z_2, \ldots, z_k), \end{aligned}\right\} \pmod p,$$

где $\varphi_1, \varphi_2, \ldots, \varphi_k$ *целые рациональные функции от* $z_1, z_2, \ldots, z_k$ *с целыми коэффициентами.*

На основании теоремы Fermat'a можно предполагать функции φ_i степени не выше $p-1$ относительно каждой из переменных z_i.

Для доказательства теоремы покажем, как найти на самом функции φ_i, если задана подстановка.

Пусть заданная подстановка переводит систему индексов

$$(2)\qquad s_1 s_2 \ldots s_k$$

в систему

$$(3)\qquad \sigma_1 \sigma_2 \ldots \sigma_k,$$

причем мы будем предполагать, что *указаны правила*, по которым всякой системе чисел (2) мы можем сопоставить систему (3).

Введем в рассмотрение функцию

$$\omega(z) = z(z-1)(z-2)\cdots(z-p+1) \equiv z^p - z \pmod p.$$

Кроме того введем в рассмотрение p функций

$$\omega_0(z) = z^{p-1} - 1,$$
$$\omega_l(z) = z\,\frac{z^{p-1} - l^{p-1}}{z-l} = z(z^{p-2} + lz^{p-3} + \ldots) \qquad (l = 1, 2, \ldots, p-1).$$

Мы имеем

$$\omega_s(z) \equiv \frac{\omega(z)}{z-s} \pmod p \qquad (s = 0, 1, 2, \ldots, p-1);$$

отсюда

$$\left.\begin{aligned} \omega_s(r) &\equiv 0,\\ \omega_s(s) &\equiv -1, \end{aligned}\right\} \pmod p \qquad (s \neq r).$$

Будем искать функции φ_i в виде сумм

$$\varphi_i \equiv \sum A^{(i)}_{s_1 s_2 \ldots s_k} \omega_{s_1}(z_1)\omega_{s_2}(z_2)\cdots\omega_{s_k}(z_k),$$

где сумма распространяется на все p^k систем (2) индексов s_i.

Полагая

$$z = s_1, \quad z_2 = s_2, \ \ldots, \ z_k = s_k; \quad \varphi_i = \sigma_i,$$

получим

$$\sigma_i = A^{(i)}_{s_1 s_2 \dots s_k} \omega_{s_1}(z_1)\omega_{s_2}(z_2)\cdots\omega_{s_k}(z_k) \equiv (-1)^k A^{(i)}_{s_1 s_2 \dots s_k} \,(\mathrm{mod}\, p).$$

Получаем выражение для коэффициентов

$$A^{(i)}_{s_1 s_2 \dots s_k} = (-1)^k \sigma_i.$$

Итак, окончательно,

$$\varphi_i \equiv (-1)^k \sum \sigma_i \omega_{s_1}(z_1)\omega_{s_2}(z_2)\cdots\omega_{s_k}(z_k),$$

и возможность подбора функций φ_i доказана.

§ 22

Поясним сказанное на примере.

Пусть подстановка задана сравнениями

$$(1) \qquad \left.\begin{aligned} z_1' &\equiv z_+ z_2, \\ z_2' &\equiv z_2 + 1, \end{aligned}\right\} \,(\mathrm{mod}\, 2).$$

В этом случае каждый из знаков

$$[z_1, z_2], \quad [z_1', z_2']$$

выражает один из четырех корней

$$x_1 = [0,0], \quad x_2 = [0,1], \quad x_3 = [1,0], \quad x_4 = [1,1].$$

Из сравнений (1) видим, что

$$\begin{aligned} [0,0] &\quad \text{переходит в} \quad [0,1], \\ [0,1] &\quad \text{переходит в} \quad [1,0], \\ [1,0] &\quad \text{переходит в} \quad [1,1], \\ [1,1] &\quad \text{переходит в} \quad [0,0]; \end{aligned}$$

следовательно, подстановка аналитически выраженная сравнениями (1) есть не что иное, как цикл

$$(x_1, x_2, x_3, x_4).$$

§ 23

Теперь мы займемся нахождением аналитического вида подстановок группы в уравнения, решаемого в радикалах, на основании известного уже свойства группы G иметь нормальным делителем арифметическую группу.

§ 24

Будем для подстановки, определяемой аналитически сравнениями (1) § 21 употреблять знак

$$\begin{pmatrix} \varphi_1(z_1, z_2, \ldots) & \varphi_2(z_1, z_2, \ldots) & \ldots \\ z_1 & z_2 & \ldots \end{pmatrix},$$

или короче

$$\begin{pmatrix} \varphi(z) \\ z \end{pmatrix}.$$

В этом символе можно вместо индексов $z_1, z_2, \ldots, z_k$ подставить новую их комбинацию $z'_1, z'_2, \ldots, z'_k$, которую можно на основании теоремы § 21 указать формулами

$$z'_i = \psi_i(z_1, z_2, \ldots)$$

и мы получаем

$$\begin{pmatrix} \varphi_1(\psi_1, \psi_2, \ldots) & \varphi_2(\psi_1, \psi_2, \ldots) & \ldots \\ \psi_1(z_1, z_2, \ldots) & \psi_2(z_1, z_2, \ldots) & \ldots \end{pmatrix} = \begin{pmatrix} \varphi[\psi(z)] \\ \psi(z) \end{pmatrix}.$$

Перемножение подстановок может быть выражено формулой

$$\begin{pmatrix} \varphi(z) \\ z \end{pmatrix} \begin{pmatrix} \psi(z) \\ z \end{pmatrix} = \begin{pmatrix} \varphi[\psi(z)] \\ \psi(z) \end{pmatrix}.$$

§ 25

Пусть подстановка

$$T = \begin{pmatrix} \varphi(z) \\ z \end{pmatrix}$$

есть произвольная подстановка разрешимой группы G заданного уравнения.

Если арифметическая группа есть нормальный делитель группы G, то имеет место равенство

$$T^{-1}ST = S', \tag{1}$$

где S и S' суть элементы арифметической группы

$$S = \begin{pmatrix} z + \alpha \\ z \end{pmatrix}, \qquad S' = \begin{pmatrix} z + \alpha' \\ z \end{pmatrix}.$$

Переписывал равенство (1) в виде $ST = TS'$, получим

$$ST = \begin{pmatrix} \varphi(z + \alpha) \\ z \end{pmatrix}, \qquad TS' = \begin{pmatrix} \varphi(z) + \alpha' \\ z \end{pmatrix},$$

откуда

$$\varphi(z + \alpha) \equiv \varphi(z) + \alpha'.$$

Это сравнение является сокращенным символом для системы сравнений по модулю p

$$\begin{aligned}\varphi_1(z_1+\alpha_1, z_2+\alpha_2, \ldots) &\equiv \varphi_1(z_1, z_2, \ldots) + \alpha_1',\\ \varphi_2(z_1+\alpha_1, z_2+\alpha_2, \ldots) &\equiv \varphi_2(z_1, z_2, \ldots) + \alpha_2',\\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\end{aligned} \tag{2}$$

Применяя формулы (2) к случаю, когда, могущие быть произвольно выбранными, числа $\alpha_1, \alpha_2, \ldots, \alpha_k$ равны нулю кроме одного равного единице, получим

$$\begin{aligned}\varphi_1(z_1+1, z_2, \ldots) &\equiv \varphi_1(z_1, z_2, \ldots) + \alpha_{1,1},\\ \varphi_1(z_1, z_2+1, \ldots) &\equiv \varphi_1(z_1, z_2, \ldots) + \alpha_{1,2},\\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\end{aligned}$$

Если мы применим первую из этих формул t_1 раз, вторую t_2 раза и так далее, то получим

$$\begin{aligned}\varphi_1(z_1+t_1, z_2, \ldots) &\equiv \varphi_1(z_1, z_2, \ldots) + t_1\alpha_{1,1},\\ \varphi_1(z_1, z_2+t_2, \ldots) &\equiv \varphi_1(z_1, z_2, \ldots) + t_2\alpha_{1,2},\\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\end{aligned}$$

Применим теперь к первой формул подстановку, выражаемую второю, далее третьею и так далее; получим

$$\varphi_1(z_1+1, z_2+t_2, \ldots) \equiv \varphi_1(z_1, z_2, \ldots) + t_1\alpha_{1,1} + t_2\alpha_{1,2} + \ldots$$

Полагая $z_1 = 0$, $z_2 = 0$, ... , $z_k = 0$ и обозначая через β_1 целое число $\varphi_1(0, 0, \ldots)$, получим

$$\varphi(t_1, t_2, \ldots) \equiv \alpha_{1,1}t_1 + \alpha_{1,2}t_2 + \ldots + \alpha_{1,k}t_k + \beta_1.$$

Итак, мы видим, что функция φ_1 оказывается линейною. То же самое относится к остальным функциям и мы приходим к теореме.

Группа Galois примитивного неприводимого уравнения степени p^k решаемого алгебраически, состоит из подстановок

$$\begin{pmatrix} z_1' & z_2' & \ldots & z_k' \\ z_1 & z_2 & \ldots & z_k \end{pmatrix}$$

вида

$$\left.\begin{aligned} z_1' &\equiv \alpha_{1,1}t_1 + \alpha_{1,2}t_2 + \ldots + \alpha_{1,k}t_k + \beta_1,\\ z_2' &\equiv \alpha_{2,1}t_1 + \alpha_{2,2}t_2 + \ldots + \alpha_{2,k}t_k + \beta_2,\\ &\ldots\ldots\ldots\ldots\ldots\ldots\\ z_k' &\equiv \alpha_{k,1}t_1 + \alpha_{k,2}t_2 + \ldots + \alpha_{k,k}t_k + \beta_k, \end{aligned}\right\} \pmod p. \tag{3}$$

Для того, чтобы сравнения (3) выражали подстановку необходимо, чтобы можно было обратно выразить z_i через z_i'; для этой цели должен быть не сравним с нулем по модулю p определитель[107]

$$\sum \pm \alpha_{1,1}\alpha_{2,2}\cdots\alpha_{k,k}.$$

[107] Д. Граве. Элементарный курс теории чисел. Вт. изд. 1913. Стр. 178.

Совокупность всех подстановок вида (3) образует, очевидно, группу которая называется *общею линейной группой.*

§ 26

В предыдущем параграфе мы видели, что необходимым условием возможности решения в радикалах примитивного уравнения является линейность его группы Galois.

Не всякая однако, линейная группа будет разрешимою. Является основною задачей найти условия, при которых линейная группа будет разрешимою. Эта задача не смотря на замечательные исследования Jordan'a[108] решена в настоящее время лишь для частных случаев. Я отсылаю читателя к сочиненно моего многоуважаемого ученика О. Ю. Шмидта «Об уравнениях решаемых в радикалах, степень которых есть степень простого числа». Из этого сочинения читатель познакомится с современным положением вопроса.

Об уравнениях простой степени

§ 27

В случае $k = 1$, когда степень заданного уравнения $n = p$, т. е. равна простому числу, *линейность группы есть не только необходимое, но и достаточное условие возможности алгебраического решения уравнения.*

Это замечание принадлежишь Galois, хотя можно считать, что оно было известно Lagrange'у. В этом случае надо рассматривать только один индекс z и дело сводится к одному только сравнению

$$z' \equiv az + b \,(\mathrm{mod}\, p).$$

Будем обозначать подстановки линейной группы символом

$$[x, ax + b]. \tag{1}$$

Переменная величина x принимает значение $0, 1, 2, \ldots, n-1$ всех классов по простому модулю n. Если a не делится на n, то выражение $ax + b$ пробегает ту же систему классов.

Давая числу a $n-1$ значений

$$1, \quad 2, \quad \ldots, \quad n-1,$$

а числу b n значений

$$0, \quad 1, \quad 2, \quad \ldots, \quad n-1,$$

мы получим $n(n-1)$ подстановок.

Нетрудно видеть, что эти подстановки образуют группу. В самом деле, рассмотрим произведение

$$[x, ax + b]\ [x, a_1 x + b_1].$$

[108] C. Jordan. Traité des substitutions. Paris 1870.

Первая подстановка заменяет x на $ax+b$; следовательно, вторую подстановку можно будет представить в виде

$$[ax+b, a_1(ax+b)+b_1].$$

Отсюда совокупность двух подстановок заменяет x на

$$a_1(ax+b)+b_1.$$

Итак, получаем

$$[x, ax+b]\ [x, a_1x+b_1] = [x, a_2x+b], \tag{1}$$

где

$$\begin{aligned} a_2 &\equiv a_1a \pmod n \\ b_2 &\equiv a_1b+b_1 \pmod n. \end{aligned} \tag{2}$$

Эти равенства показывают, что *линейные подстановки образуют группу.* Мы будем называть эту группу по примеру Kronecker'a *метациклическою.*

§ 28

Частный случай линейной группы представляем, циклическая группа образуемая подстановкой $[x, x+1]$ или другой $[x, x+b]$.

Подобным же образом существует линейная группа порядка $n-1$, образуемая подстановкой $[x, ax]$, где a, по прежнему, есть число взаимно-простое с n.

§ 29

Обратимся теперь к рассмотрению делителей линейной группы.

Рассмотрим степень линейной подстановки

$$S = [x, ax+b].$$

Применяя последовательно формулу умножения § 27, мы получим

$$S^k = [x, a^kx + b(1+a+a^2+\ldots+a^{k-1})].$$

Если $a=1$, то

$$S^k = [x, x+kb].$$

Итак, мы видим, что, *если в линейную группу входит, по крайней мере, одна подстановка, у которой* $a=1$, *а* b *отлично от нуля, то группа имеет делителем циклическую группу* $[z, z+b]$, *где* $b = 0, 1, \ldots, n-1$.

Рассмотрим подстановку

$$S = [ax+b],$$

у которой a отлично от единицы.

Покажем, что *подстановка* S *будет порядка* μ, *если число* a *принадлежит показателю* μ *по модулю* n.

В самом деле, если a принадлежишь показателю μ, то

$$a^\mu - 1 \equiv 0 \,(\mathrm{mod}\, n), \tag{1}$$

и, притом, μ есть наименьшее число, при котором возможно сравнение (1).

Переписываем последнее сравнение так

$$(a-1)(1 + a + a^2 + \ldots + a^{\mu-1}) \equiv 0 \,(\mathrm{mod}\, n),$$

или

$$1 + a + a^2 + \ldots + a^{\mu-1} \equiv 0 \,(\mathrm{mod}\, n).$$

Отсюда

$$S^\mu = [x, a^\mu x + b(1 + a + \ldots + a^{\mu-1})] = [x, x] = I.$$

§ 30

Покажем теперь, что, *если a отлично от единицы, то период*

$$I, \quad S, \quad S^2, \ \ldots, \ S^\mu$$

будет интранзитивной группой.

В самом деле, в этом случае будет существовать элемент x, который оставляется без изменения подстановкой S, а следовательно, и всеми ее степенями.

Для нахождения неизменяемого элемента придется решить сравнение

$$x \equiv ax + b \,(\mathrm{mod}\, n),$$

или иначе,

$$(a-1)x + b \equiv 0 \,(\mathrm{mod}\, n).$$

Если a отлично от единицы, то последнее сравнение всегда имеет одно решение x_0, дающее единственный неизменяемый подстановкой S элемент.

§ 31

Выведем условие, при котором две линейные подстановки

$$[x, ax + b], \qquad [x, a_1 x + b_1]$$

оставляют без изменения один и тот же элемент x_0.

На основании соображений предыдущего §-а получим два условия

$$(a-1)x_0 + b \equiv 0 \,(\mathrm{mod}\, n)$$
$$(a_1 - 1)x + b_1 \equiv 0 \,(\mathrm{mod}\, n),$$

откуда получим

$$b(a_1 -) - b_1(a-1) \equiv 0 \,(\mathrm{mod}\, n).$$

§ 32

Циклическая группа

$$[x, x+b]$$

порядка n, очевидно, транзитивна.

Докажем теперь, что *всякая транзитивная линейная группа должна иметь своим делителем циклическую.*

Рассмотрим какую нибудь подстановку:

$$S = [x, ax+b]$$

линейной транзитивной группы. Пусть g будет первообразный корень числа n. Введем в рассмотрение индекс α числа a, т. е. число, удовлетворяющее сравнений

$$g^{\alpha} \equiv a \,(\mathrm{mod}\, n).$$

Для сокращения речи можем число α называть *индексом подстановки* S.

Мы имеем право предположить, что индекс α отличен от 0 и $n-1$, ибо в обоих случаях можно было бы предположить a равным единице, и следовательно, подстановка S или была бы равна единице или принадлежала бы к циклической группе.

На оснований первой формулы (2) § 27 мы замечаем. что индекс составной подстановки будет равен сумме индексов подстановок перемножаемых. Отсюда следует, что все индексы подстановок линейной группы должны быть числами, кратными наименьшему из индексов α_0, так что обозначая

$$g^{\alpha_0} \equiv a_0,$$

можем написать все подстановки линейной группы в виде:

$$S = [x, a_0^h x + b], \tag{1}$$

где числа h и b принимают известные значения.

Очевидно, что в рассматриваемую группу входить подстановка:

$$S_0 = [x, a_0 x + b_0],$$

ибо, если бы для всех подстановок рассматриваемой группы показатель h был больше единицы, то число α_0 не могло бы быть индексом одной из подстановок.

Рассмотрим подстановку

$$\Sigma = S S_0^{-h} = [x, a'x + b'].$$

Получаем

$$S = \Sigma S_0^h = [x, a'x + b']\ [x, a_0^h + b_0(1 + a_0 + \ldots + a_0^{h-1}].$$

Применяя формулы § 27, имеем

$$S = [x, a' a_0^h x + a_0^h b' + b_0(1 + a_0 + \ldots + a_0^{h-1}]. \tag{1}$$

Сравнивая (1) и (2), получим

$$a_0^h \equiv a' a_0^h \,(\mathrm{mod}\, n) \tag{3}$$

и

$$b \equiv a_0^h b' + b_0(1 + a + a_0 + \ldots + a_0^{h-1}) \,(\mathrm{mod}\, n). \tag{4}$$

Решая сравнение (3), находим $a' = 1$, следовательно,

$$\Sigma = [x, x + b']. \tag{5}$$

Мы докажем, что в рассматриваемой линейной группе будет заключаться циклическая группа, если покажем, что в формуле (5) число b' получится отличным от нуля, по крайней мире, при одной какой либо из подстановок S.

Допустим обратное, а именно, что $b' = 0$, какова бы ни была подстановка S. В этом случай сравнение (4) дает

$$b - b_0(1 + a_0 + \ldots + a_0^{h-1}) \equiv 0 \,(\mathrm{mod}\, n)$$

или иначе,

$$b(a_0 - 1) - b_0(a_0^h - 1) \equiv 0 \,(\mathrm{mod}\, n).$$

Но так как последнее сравнение есть выведенное в § 31 условие неизменяемости некоторого элемента двумя линейными подстановками, то отсюда следует, что подстановка S не меняет элемента, не изменяемого подстановкой S_0.

Меняя числа h и b, заметим, что все подстановки S рассматриваемой группы не должны изменять одного и того же элемента, не изменяемого подстановкой S_0. Этот элемента остается, следовательно, без изменения при всех подстановках группы, и значит, группа интранзитивна, что противоречить предположение.

Итак, всякая транзитивная линейная группа должна иметь делителем циклическую группу порядка n.

§ 33

Посмотрим теперь, как образуется линейная группа G, у которой индексы подстановок суть кратные одного из этих индексов α_0. Разсмотрим степени подстановки $S_0 = [x, a_0 x + b_0]$. Обозначим через μ показатель, которому принадлежим число a_0. Тогда всякая подстановка рассматриваемой группы может быть написана в таком виде

$$[x, a_0^h x + b],$$

причем число h принимает одно из следующих значений

$$0, \quad 1, \quad 2, \ \ldots, \ \mu - 1.$$

Если группа транзитивна, то в ней существует циклическая подстановка

$$[x, x + 1]$$

а, следовательно, и подстановка

$$[x, a_0^h x + b]\ [x, x + 1] = [x, a_0^h x + b + 1].$$

Мы видим отсюда, что в данной группе коэффициент b может принимать все значения

$$0, \quad 1, \quad 2, \ \ldots, \ n - 1.$$

Итак, *всякая транзитивная линейная группа может быть дана символом* $S = [x, a_0^h x + b]$, *причем* h *принимает значения*

$$0, \quad 1, \quad 2, \quad \ldots, \quad \mu - 1,$$

а b *значения*

$$0, \quad 1, \quad 2, \quad \ldots, \quad n - 1.$$

§ 34

Если a_0 есть первообразный корень числа n, то $\mu = n - 1$, и мы получаем всю метацикличесвую группу.

Покажем, что *метациклическая группа дважды траизитивна*, указав такую линейную подстановку, которая будет обращать два определенных элемента, например 0, 1, в произвольные новые i, k.

В самом деле, таковой будет подстановка

$$[x, (k - i)x + i].$$

§ 35

Покажем, что *всякая линейная группа будет разрешимою.*

Если в группе G, разобранной в § 33, $\mu = 1$, то эта группа есть циклическая порядка n и имеет нормальном делителем единицу. Покажем теперь, что если $\mu = p\mu'$, где p некоторое простое число, то линейная группа имеет нормальным делителем новую линейную группу G' порядка $n\mu'$, составленную подстановками $S' = [x, a_0^{p^h} x + b]$, где $h = 0, 1, 2, \ldots, \mu' - 1$, а $b = 0, 1, 2, \ldots, n - 1$.

Эта новая группа G' есть, очевидно, делитель группы G индекса p.

Нетрудно убедиться, что группа G' есть нормальный делитель группы G. В самом деле, придется показать, что подстановка $S^{-1}S'S$, где подстановка $S = [x, a_0^k x + b_1]$ есть одна из подстановок группы G, должна принадлежать группе G'.

На оснований формулы (2) § 27 мы получаем

$$S^{-1}S'S = [x, a_0^{-k} a_0^{p^k} a_0^k x + b_2],$$

где a_0^{-k} обозначаете корень сравнения $x a_0^k \equiv 1 \pmod p$.

Отсюда имеем окончательно $S^{-1}S'S = [x, a_0^{p^k} x + b_2]$ и, следовательно, подстановка $S^{-1}S'S$ действительно принадлежит группе G'.

Итак, группа G' есть нормальный делитель группы G с простым индексом.

Мы замечаем отсюда, что, разлагая μ на простых множители $p_1, p_2, p_3, \ldots$, мы получим ряд групп

$$(1) \qquad G, \quad G', \quad G'', \quad G''', \quad \ldots$$

порядков

$$n\mu, \quad \frac{n\mu}{p_1}, \quad \frac{n\mu}{p_1 p_2}, \quad \frac{n\mu}{p_1 p_2 p_3}, \quad \ldots.$$

Каждая из групп (1) будет нормальным делителем предыдущей. Так как индексы будут простые числа $p_1, p_2, p_3, \ldots$, то группа G будет разрешимая, что и требовалось доказать.

Полная линейная группа будет иметь Jordan'овским рядом индексов число n и все простые делители числа $n-1$.

§ 36

Покажем, что, *если линейная транзитивная группа G есть нормальный делитель группы H, то сама группа H должна быть линейною.*

Пусть S будет некоторая подстановка группы G, а T какая нибудь произвольно выбранная подстановка группы H. Тогда, по предположению, должно иметь место равенство

$$T^{-1}ST = S',$$

где S' новая подстановка линейной группы G. Пусть аналитическое выражение подстановки T будет

$$T = [x, \varphi(x)],$$

где через $\varphi(x)$ обозначена некоторая целая функция.

Возьмем за подстановку S циклическую $[x, x+1]$.

Пусть, кроме того, $S' = [x, a'x + a]$.

Тогда равенство $ST = TS'$ может быть написано так

$$[x, x+1]\ [x, \varphi(x)] = [x, \varphi(x)]\ [x, a'x + a].$$

Отсюда получаем сравнение

$$\varphi(x+1) \equiv a'\varphi(x) + a \,(\mathrm{mod}\, n)$$

Это сравнение должно иметь место при всевозможных целых значениях x. Но так как функция φ не достигает степени n, то коэффициенты при одинаковых степенях в обеих частях сравнения должны быть сравнимы по модулю n. Сравнивая коэффициенты при старшей степени, получим, очевидно,

$$a' \equiv 1 \,(\mathrm{mod}\, n),$$

откуда имеем

$$\varphi(x+1) \equiv \varphi(x) + a \,(\mathrm{mod}\, n).$$

Подставляя в это сравнение вместо x числа

$$x+1, \quad x+2, , \ \ldots, \ x+z-1$$

и складывая, получим

$$\varphi(x+z) \equiv \varphi(x) + za \,(\mathrm{mod}\, n).$$

Подставил сюда $x = 0$ и обозначая $\varphi(0) = b$, будем иметь

$$\varphi(z) \equiv az + b \,(\mathrm{mod}\, n).$$

Так как последнее сравнение справедливо при всех целых значениях z, то подстановка T равносильна подстановке

$$[x, ax + b],$$

т. е. группа H линейна.

§ 37

Нетрудно видеть, что метацикличеекая группа может быть получена от комбинирования двух основных подстановок,

$$S = [x, x + 1], \qquad T = [x, gx],$$

где g один из первообразных корней числа n.

Подобным же образом всякий делитель полной линейной группы может быть образован подстановками S, $T^{\alpha-0} = [x, g^{\alpha_0}x]$. Так например, подстановки S, $T^2 = [x, g^2x]$ образуют линейную группу порядка $\dfrac{n(n-1)}{2}$, аналитическое выражение которой будет иметь вид $[x, ax+b]$, причем b проходит все значения $0, 1, 2, \ldots, n-1$, а a распространяется только на квадратичные вычеты числа n.

L. Kronecker называет эту группу *полуметациклической*.

Если n число простое, то подстановка S состоит из одного цикла

$$(0, 1, 2, \ldots, n - 1),$$

обнимающего нечетное число элементов, и, следовательно, эта подстановка принадлежит знакопеременной группе.

Что же касается подстановки T, то она оставляет элемент 0 без перемены; остальные же $n - 1$ элементов она перемещает по циклу

$$(1, g, g^2, \ldots, g^{n-2}).$$

Так как этот цикл обнимает четное число элементов, то подстановка T не принадлежит знакопеременной группе, но T^2, а, следовательно, и вся полуметациклическая группа входит в состав знакопеременной группы. Итак, мы видим, что метациклическая группа не представляет из себя делителя знакопеременной группы. Общий же наибольший делитель метациклической группы и знакопеременной есть полуметациклическая группа.

§ 38

Из соображений предшествовавших параграфов следует теорема.

Всякое неприводимое уравнение простой степени, имеющее линейную группу решается в радикалах.

Для доказательства этой теоремы надо принять во внимание теорему § 25, показывающую, что группа всякого разрешимого уравнения линейная и обратно, если степень n уравнения есть простое число, то в § 35 мы видели, что линейная группа будет разрешимою.

§ 39

Необходимыми и достаточным условием решимости в радикалах неприводимого уравнения простой степени является свойство всех корней выражаться рационально через произвольные два.

Необходимость теоремы доказывается так. Если уравнение решается в радикалах, то его группа линейная. Мы видели в § 30, что линейная подстановка, если она не приводится к тождественной, может оставить без изменения только один корень; поэтому в линейной группе только одна тождественная подстановка оставляет без перемены два корня. В самом деле, сравнение $x \equiv ax + b \,(\mathrm{mod}\, n)$ может иметь два решения только в случае $a \equiv 1$, $b \equiv 0 \,(\mathrm{mod}\, n)$.

Итак, если группа уравнения линейная, то присоединение к основному полю Ω двух корней должно сводить группу уравнения на единицу. Тогда в полученном поле должны заключаться все остальные корни, которые, следовательно, и будут выражаться рационально через два присоединенных.

Обращаемся теперь к предложений обратному.

Пусть корни неприводимого уравнения простой степени выражаются рационально через два из них

$$x_k = \mathfrak{D}(x_0, x_1). \tag{1}$$

К соотношению (1) между корнями можно, очевидно, применить любую подстановку группы G заданного уравнения. Если эта подстановка не меняет двух корней x_0, x_1, то она, очевидно, не должна менять и всякий другой корень x_k, т. е. она должна быть тождественною.

Группа G уравнения не содержит отличной от единицы подстановки, не меняющей двух корней.

Очевидно, что возможен только один из двух случаев: 1) подстановка S группы G состоит из одного *цикла*, 2) подстановка S оставляет без перемены *одну* букву и, кроме того, относительно остальных $n-1$ букв она заключает *циклы с одинаковым числом букв*. В самом деле, если допустить в S существование двух циклов C и C_1 порядков k и k_1, причем $1 < k < k_1$, то

$$S^k = C_1^k \cdots$$

будет подстановкой группы G, *оставляющей без перемены* k букв цикла C, и *нетождественною*, ибо буквы цикла C_1 будут перемещаться.

Итак, подстановки группы G состоят из *тождественной* подстановки, подстановок S, из которых каждая состоит из одного цикла и подстановок Σ, не меняющих одной буквы.

Пусть число подстановок S будет ν. Пусть в группе G будут существовать подстановки Σ_0, не меняющие x_0, Σ_1, не меняющие x_1, …, Σ_{n-1}, не меняющие x_{n-1}.

Если группа G *транзитивная*, то можно показать, что, если обозначить через μ число подстановок Σ_0, то такое же число μ будет подстановок Σ_1, подстановок Σ_2 и т. д. В самом деле, если группа G транзитивная, то в ней существует подстановка

T переводящая x_0 в x_1, тогда всякая подстановка $T^{-1}\Sigma_0 T$ будет принадлежать к числу Σ_1 и обратно $T\Sigma_1 T^{-1}$ к числу Σ_0. Обозначая через m порядок группы G мы получим

$$m = \mu n + \nu + 1. \tag{2}$$

Подстановки Σ_0 вместе с тождественною образуют подгруппу G_1, не меняющую x_0. Разлагаем группу G на сопряженные системы по подгруппе G_1

$$G = G_1 + G_1T_1 + G_1T_2 + \ldots + G_1T_{n-1},$$

где T_i переводит x_0 в x_i.

Мы получаем

$$m = n(\mu + 1). \tag{3}$$

Сопоставляя (2) и (3), имеем

$$\nu = n - 1.$$

Итак, существует только $n-1$ и *не более* циклических подстановок S, которые образуют вместе с единицей, очевидно, *циклическую* группу

$$\mathfrak{G} = (I, S, S^2, \ldots, S^{n-1}).$$

Подстановка $T^{-1}ST$ состоит также из одного цикла, а потому, будучи элементом группы G, должна входит в состав G.

Итак, группа $\mathfrak{G}$ есть нормальный делитель группы G, но $\mathfrak{G}$, будучи циклическою, представляет из себя частный случай линейной, следовательно, группа G будет также линейная, и заданное уравнение решается в радикалах.

Точка зрения Lagrange'a

§ 40

Lagrange дал простой и замечательный пример функции принадлежащей к метациклической группе; подобные функции мы будем называть метациклическими.

Не трудно видеть, что, если мы обозначим

$$S_a = [z, az], \qquad \Sigma_b = [z, z + b]$$
$$4pt]a = 1,\ 2,\ \ldots,\ n-1, b = 0,\ 1,\ 2,\ \ldots,\ n-1,$$

то метациклическая группа будет состоять из подстановок вида

$$S_a\Sigma_b.$$

Приступим теперь к изложению соображений Lagrange'a.

§ 41

Пусть g первообразный корень простого числа n.

Возьмем резольвенту

$$\psi_k = x_0 + \varepsilon^{g^h} x_1 + \varepsilon^{2g^h} x_2 + \ldots + \varepsilon^{(n-1)g^h} x_{n-1}.$$

Функции

$$\varphi_1 = \psi_1^n, \quad \varphi_2 = \psi_2^n, \ \ldots, \ \varphi_{n-1} = \psi_{n-1}^n$$

будут, как мы уже видели в главе XVIII, функциями циклическими, то есть не меняющимися от циклических подстановок Σ_b.

Посмотрим, что произойдет с функцией φ_h от какой нибудь подстановки S_a. Обозначим через φ'_h то выражение, которое получится после подстановки; будем иметь

$$\varphi'_h = (x_0 + \varepsilon^{g^h} x_a + \varepsilon^{2g^h} x_{2a} + \ldots + \varepsilon^{(n-1)g^h} x_{(n-1)a})^n.$$

Обозначим через a_1 корень сравнения $a_1 a \equiv 1 \,(\mathrm{mod}\, \mathrm{n})$, тогда не трудно написать выражение φ'_h в таком виде, чтобы индексы i у букв x_i шли в натуральном возрастающем порядке:

$$\varphi'_h = (x_0 + \varepsilon^{a_1 g^h} x_{aa1} + \varepsilon^{2a_1 g^h} x_{2aa_1} + \ldots + \varepsilon^{(n-1)a_1 g^h} x_{(n-1)aa_1})^n =$$
$$= (x_0 + \varepsilon^{a_1 g^h} x_1 + \varepsilon^{2a_1 g^h} x_2 + \ldots + \varepsilon^{(n-1)a_1 g^h} x_{n-1})^n.$$

Полагал

$$a_1 \equiv g^\alpha \,(\mathrm{mod}\, n),$$

получим

$$\varphi'_h = (x_0 + \varepsilon^{g^{h+\alpha}} x_1 + \varepsilon^{2g^{h+\alpha}} x_2 + \ldots + \varepsilon^{(n-1)g^{h+\alpha}} x_{n-1})^n = \varphi_{h+\alpha}.$$

Итак, подстановка S_a производит циклическую подстановку $[z, z+\alpha]$ между функциями

$$\varphi_1, \quad \varphi_2, \quad \varphi_3, \ \ldots, \ \varphi_{n-1}. \tag{1}$$

Отсюда мы замечаем. что всякая циклическая функция от функции (1) будет метациклическою, ибо она не меняется от подстановок S_a, Σ_b. Особенное значение имеет функция

$$\omega = (\varphi_1 + \alpha\varphi_2 + \alpha^2\varphi_3 + \ldots + \alpha^{n-2}\varphi_{n-1})^{n-1}, \tag{2}$$

где α первообразный корень $n-1$ степени из 1.

§ 42

В случае $n = 5$ имеем $\alpha = i$, $g = 2$

$$\omega = (\varphi_1 + i\varphi_2 - \varphi_3 - i\varphi_4)^4,$$

где

$$\varphi_1 = (x_0 + \varepsilon^2 x_1 + \varepsilon^4 x_2 + \varepsilon x_3 + \varepsilon^3 x_4)^5,$$
$$\varphi_2 = (x_0 + \varepsilon^4 x_1 + \varepsilon^3 x_2 + \varepsilon^2 x_3 + \varepsilon x_4)^5,$$
$$\varphi_3 = (x_0 + \varepsilon^3 x_1 + \varepsilon x_2 + \varepsilon^4 x_3 + \varepsilon^2 x_4)^5,$$
$$\varphi_4 = (x_0 + \varepsilon x_1 + \varepsilon^2 x_2 + \varepsilon^3 x_3 + \varepsilon^4 x_4)^5,$$

где ε первообразный корень пятой степени из единицы.

§ 43

На основании соображений главы XV метациклическая функция (2) § 41 должна быть корнем уравнения степени $\nu = 1 \cdot 2 \cdots (n-2)$, ибо число $1 \cdot 2 \cdots (n-2)$ есть индекс метациклической группы, имеющей порядок $n(n-1)$ по отношению ко всей симметрической группе. Пусть уравнение степени ν, которому удовлетворяет метациклическая функция будет

$$\Phi(x) = 0. \tag{1}$$

Уравнение (1) я буду называть *уравнением Lagrange'a*. Для $n = 5$ уравнение Lagrange'а будет шестой степени, ибо $\nu = 1 \cdot 2 \cdot 3 = 6$.

§ 44

Теорема. *Необходимым и достаточным условием разрешимости в радикалах неприводимого уравнения простой степени является существование у уравнения Lagrange'a простого рационального корня.*

В самом деле, если уравнение решается в радикалах, то его группа будет линейная. Но линейная группа есть делитель метациклической, следовательно, метациклическая функция не меняется от подстановок группы уравнения, следовательно, эта функция принадлежит к основному полю уравнения Lagrange'а, то есть уравнение Lagrange'а имеет рациональный корень.

Обратно, если все корни уравнения Lagrange'а *различны* между собой, то один из них принадлежит точно к метациклической группе; если этот корень ω равен рациональному числу a, то соотношение

$$\omega(x_0, x_1, \ldots, x_{n-1}) = a$$

между корнями заданного уравнения *нарушается* при всякой подстановке, не входящей в *метациклическую* группу. Следовательно, группа G заданного уравнения должна быть делителем метациклической.

Итак, мы видим, что группа G линейная, но кроме того нам задана неприводимость уравнения, следовательно, уравнение решается в радикалах, и теорема доказана.

§ 45

Формула (2) на основании известных нам из главы XVIII свойств резольвент Lagrange'а дает возможность, когда задано рациональное[109] выражение ω вычислить в радикалах величины $\varphi_1, \varphi_2, \varphi_3 \ldots, \varphi_{n-1}$, а далее по формулам

$$\varphi_1 = (x_0 + \varepsilon^g x_1 + \varepsilon^{2g} x_2 + \ldots)^n,$$
$$\varphi_2 = (x_0 + \varepsilon^{g^2} x_1 + \varepsilon^{2g^2} x_2 + \ldots)^n,$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots,$$

[109]Надо помнить, что при составлении уравнения Lagrange'а мы присоединили корни ε и α из единицы

получить окончательные радикальные выражения для корней $x_0, x_1, \ldots, x_{n-1}$ заданного уравнения.

§ 46

Мы теперь приходим к концу нашего изложения. Поставив себе целью простое и строгое изложение основных принципов теории алгебраического решения уравнений, положенных в основу гениальными исследованиями Lagrange'a, Gauss'a, Abel'я и Galois, мы должны предупредить читателя, что задача не исчерпывается изложенною теорией.

Теперь только лишь следовало бы приступить к настоящей задаче решения уравнений в радикалах, которая разбивается на две: дать удобные для практики приемы узнать относительно всякого заданного уравнения, решается ли оно в радикалах, и если решается, то написать само радикальное выражение и подробно его наследовать, подобно тому, например, как мы это делали в §§ 8, 9 главы III для кубических уравнений.

Abel поставил задачу найти способ, по которому можно было бы найти все уравнения, решаемые в радикалах. Abel оставил, однако, лишь короткие указания без доказательств. Kronecker решил поставленную Abel'ем задачу, причем он ищет не сами уравнения, а радикальные выражения их корней. Для простой степени n Kronecker указывал выражение, составляемое из элементов поля и повторным извлечением радикалов, и которое обладает двойным свойством: 1) что всякий корень неприводимого разрешимого уравнения n-ой степени из поля Ω заключается в этом выражении, 2) это выражение само удовлетворяешь уравнению n-ой степени.

Формулы Kronecker'a доказаны H. Weber'ом[110]. Для уравнений степени p^k задача решена вполне лишь в немногих частных случаях.

[110]H. Weber. Lehrbuch der Algebra 1898 Bd. I Achtzehnter Abschnitt.

Глава XX

Об уравнениях пятой степени

Знакопеременная группа подстановок пяти элементов

§ 1

Уравнения пятой степени заслуживают особенного внимания, потому что, с одной стороны, они принадлежат к числу не решаемых в радикалах в общем случае; с другой стороны, они обладают свойствами, сближающими их с уравнениями низших степеней. Эти свойства состоят в их связи с группами многогранников (см. стр. 173).

Симметрическая группа для уравнения четвертой степени имеет порядок $24 = 1 \cdot 2 \cdot 3 \cdot 4$ и изоморфна с группой *октаэдра*. *Знакопеременная* группа для тех же уравнений имеет порядок 12 и изоморфна с группой *тетраэдра*.

Для уравнений *пятой степени* оказывается замечательный факт, что их знакопеременная группа, имеющая порядок $60 = \frac{1}{2} \cdot 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5$, изоморфна с группой *икосаэдра*.

Для лиц, желающих ближе изучить связь уравнений 5-ой степени с икосаэдром, можно рекомендовать книгу проф. Klein'a «Vorlesungen über das Ikosaeder und die Auflösung der Gleichungen vom fünften Grade» (1884).

Для наглядного пояснения изоморфизма групп подстановок с группами многогранников мною сделаны модели, находящаяся в Механическом Кабинете Университета Св. Владимира. Эти модели представляют из себя тетраэдр, октаэдр и икосаэдр, на углах граней которых написаны подстановки таким образом, что умножение подстановок производится простым поворотом фигуры.

§ 2

Рассмотрим все перемещения пяти элементов $1, 2, 3, 4, 5$:

12345	21345	31245	41235	51234
12354	21354	31254	41253	51243
12435	21435	31425	41325	51324
12453	21453	31452	41352	51342
12534	21534	31524	41523	51423
12543	21543	31542	41532	51432
13245	23145	32145	42135	52134

13254	23154	32154	42153	52143
13425	23415	32415	42315	52314
13452	23451	32451	42351	52341
13524	23514	32514	42513	52413
13542	23541	32541	42531	52431
14235	24135	34125	43125	53124
14253	24153	34152	43152	53142
14325	24315	34215	43215	53214
14352	24351	34251	43251	53241
14523	24513	34512	43512	53412
14532	24531	34521	43521	53421
15234	25134	35124	45123	54123
15243	25143	35142	45132	54132
15324	25314	35214	45213	54213
15342	25341	35241	45231	54231
15423	25413	35412	45312	54312
15432	25431	35421	45321	54321

Этим перемещениям соответствуют подстановки

I	(12)	(132)	(1432)	(15432)
(45)	(12)(45)	(132)(45)	(14532)	(1532)
(34)	(12)(34)	(1342)	(142)	(1542)
(345)	(12)(345)	(13452)	(1452)	(152)
(354)	(12)(354)	(13542)	(142)(35)	(15342)
(35)	(12)(35)	(1352)	(14352)	(152)(34)
(23)	(123)	(13)	(143)	(1543)
(23)(45)	(123)(45)	(13)(45)	(1453)	(153)
(234)	(1234)	(134)	(14)	(154)
(2345)	(12345)	(1345)	(145)	(15)
(2354)	(12354)	(1354)	(14)(35)	(1534)
(235)	(1235)	(135)	(1435)	(15)(34)
(243)	(1243)	(13)(24)	(1423)	(15423)
(2453)	(12453)	(13)(245)	(14523)	(1523)
(24)	(124)	(1324)	(14)(23)	(154)(23)
(245)	(1245)	(13245)	(145)(23)	(15)(23)
(24)(35)	(124)(35)	(13524)	(14)(235)	(15234)
(2435)	(12435)	(135)(24)	(14235)	(15)(234)
(2543)	(12543)	(13)(254)	(14253)	(153)(24)
(253)	(1253)	(13)(25)	(143)(25)	(15243)
(254)	(1254)	(13254)	(14)(253)	(15324)
(25)	(125)	(1325)	(14325)	(15)(243)
(2534)	(12534)	(134)(25)	(14)(25)	(1524)
(25)(34)	(125)(34)	(13425)	(1425)	(15)(24)

Знакопеременную группу будут составлять подстановки четного числа транспозиций. Расположим эти подстановки по периодам. Сначала напишем периоды для пятизначных циклов, они обнимают 24 подстановки:

$$\begin{array}{llll} S_1 = (12345), & S_1^2 = (13524), & S_1^3 = (14253), & S_1^4 = (15432), \\ S_2 = (12354), & S_2^2 = (13425), & S_2^3 = (15243), & S_2^4 = (14532), \\ S_3 = (12453), & S_3^2 = (14325), & S_3^3 = (15234), & S_3^4 = (13542), \\ S_4 = (12435), & S_4^2 = (14523), & S_4^3 = (13254), & S_4^4 = (15342), \\ S_5 = (12543), & S_5^2 = (15324), & S_5^3 = (24235), & S_5^4 = (13452), \\ S_6 = (12534), & S_6^2 = (15423), & S_6^3 = (13245), & S_6^4 = (14352). \end{array}$$

Далее мы имеем 20 тройных циклов, которые можно расположить в 10 периодов:

$$\begin{array}{llll} T_1 = (123), & T_1^2 = (132), & T_6 = (145), & T_6^2 = (154), \\ T_2 = (124), & T_2^2 = (142), & T_7 = (234), & T_7^2 = (243), \\ T_3 = (125), & T_3^2 = (152), & T_8 = (235), & T_8^2 = (253), \\ T_4 = (134), & T_4^2 = (143), & T_9 = (245), & T_9^2 = (254), \\ T_5 = (135), & T_5^2 = (153), & T_{10} = (345), & T_{10}^2 = (354). \end{array}$$

Далее следуют 15 пар транспозиций:

$$\begin{array}{lll} U_1 = (12)(34), & U_6 = (13)(45), & U_{11} = (15)(24), \\ U_2 = (12)(35), & U_7 = (14)(23), & U_{12} = (15)(34), \\ U_3 = (12)(45), & U_8 = (14)(25), & U_{13} = (23)(45), \\ U_4 = (13)(24), & U_9 = (14)(35), & U_{14} = (24)(35), \\ U_5 = (13)(25), & U_{10} = (15)(23), & U_{15} = (25)(34). \end{array}$$

Все S удовлетворяют уравнение $S^5 = I$, все T — уравнению $T^3 = I$ и все U — уравнению $U^2 = I$.

Единичная подстановка вместе с S, U, T образует знакопеременную группу порядка $1 + 24 + 15 + 20 = 60$.

§ 3

Покажем, что знакопеременная группа 5 элементов изоморфна с группой вращения икосаэдра.

Икосаэдр имеет 12 вершин. Соединяя противоположные вершины прямыми, получим 6 осей вращения. Около каждой из вершин икосаэдра сходятся 5 граней. Следовательно, около осей, проведенных через противоположный вершины, можно сделать пять различных вращений, на $\dfrac{360}{5} = 72$ градуса каждое. После пятикратного повторения такого вращения фигура примет первоначальное положение. Эти 6 осей пятикратных вращений соответствуют 6-ти периодам подстановок S.

Можно вращать икосаэдр около прямой, соединяющей центры противоположных граней. Граней икосаэдр имеет двадцать, следовательно, будет десять таких осей вращения. После трех поворотов около этих осей, на $\dfrac{360}{3} = 120$ градусов

каждый, фигура приметь первоначальное положение. Эти оси вращения соответствуют десяти периодам тройных циклов T.

И, наконец, подстановки U соответствуют вращениям на $\frac{360}{2} = 180$ градусов около прямых, соединяющих середины противоположных ребер. Ребер икосаэдр имеет 30, следовательно, получается 15 осей вращения.

Метациклическая функция

§ 4

В предыдущей главе мы указали способ, при помощи которого Lagrange привел решение общего уравнения пятой степени к резольвенте шестой степени.

Lagrange пользовался побочной иррациональностью

$$x_0 + \varepsilon x_1 + \varepsilon^2 x_2 + \varepsilon^3 x_3 + \varepsilon^4 x_4,$$

где ε корень пятой степени из единицы.

Мы знаем уже из общей теории, что той же цели можно достигнуть при помощи натуральных иррациональностей.

Рассмотрим метациклическую группу (см. глава XIX) для случая $n = 5$. Порядок этой группы будет $n(n-1) = 5 \cdot 4 = 20$. Полуметациклическая группа имеет порядок 10.

Для общего уравнения 5-ой степени метациклическая функция удовлетворяет, очевидно, уравнению $\frac{1 \cdot 2 \cdot 3 \cdot 4 \cdot 5}{20} = 6$-ой степени.

Полуметациклическая функция будет удовлетворять уравнений 12-ой степени, которое от присоединения корня квадратного из дискриминанта разложится на два множителя 6-ой степени.

Равенство

$$(z, bz)\ (z, z + a) = (z, bz + a)$$

показывает, что метациклическую группу можно получить при помощи формулы

$$T^\tau S^\sigma,$$

если[111] $T = (z, 2z)$, $S = (z, z + 1)$, причем τ пробегает полную систему вычетов по модулю 4, а σ по модулю 5.

Полуметациклическую группу получим, полагая

$$T_0^{\tau_0} S^\sigma,$$

где $T_0 = T^2 = (z, 4z)$, а $\tau_0 = 0, 1$.

Обозначая индексы пяти корней

$$0,\quad 1,\quad 2,\quad 3,\quad 4,$$

мы заметим, что *пять следующих пар индексов*

(1) $$(0,1),\quad (1,2),\quad (2,3),\quad (3,4),\quad (4,0)$$

[111] Число 2 есть первообразный корень числа 5.

после применения к ним подстановки T дают следующие пары

$$(0,2),\quad (2,4),\quad (4,1),\quad (1,3),\quad (3,0) \tag{2}$$

Пары (1) и (2) исчерпывают все 10 возможных пар составленных из 5-ти предметов.

Покажем, что от применения к парам (1) подстановок полуметациклической группы эти пары остаются теми же самыми только меняется их порядок.

В самом деле, от применения подстановки S получаем пары

$$(1,2),\quad (2,3),\quad (3,4),\quad (4,0),\quad (0,1),$$

а применяя T_0 приходим к парам

$$(0,4),\quad (4,3),\quad (3,2),\quad (2,1),\quad (1,0).$$

Очевидно, что будет полуметациклическою всякая симметрическая функция от пяти произведений корней

$$x_0x_1,\quad x_1x_2,\quad x_2x_3,\quad x_3x_4,\quad x_4x_0.$$

Самою простою из таких функций является сумма

$$u = x_0x_1 + x_1x_2 + x_2x_3 + x_3x_4 + x_4x_0;$$

применяя подстановку T, получаем

$$u_1 = x_0x_2 + x_2x_4 + x_4x_1 + x_1x_3 + x_3x_0.$$

Функция u' принадлежит также к полуметациклической группе.

Пусть заданное уравнение пятой степени имеет вид

$$ax^5 + bx^4 + cx^3 + dx^2 + ex + f = 0. \tag{3}$$

Будем иметь

$$u + u' = \frac{c}{a}.$$

Функция

$$y = u - u' \tag{4}$$

есть также метацикдическая, ее квадрат y^2 будет полною метациклическою функцией и будет корнем уравнения 6-ой степени.

Будем рассматривать *полуметациклическую функцию* y, она удовлетворяет также уравнению 6-ой степени, если присоединить к основному полю $\sqrt{\Delta}$, где Δ — дискриминант уравнения (3). После этого присоединения группой уравнения будет знакопеременная A.

Если мы обозначим через M — полуметациклическую группу, то простая проверка убедить нас в том, что разложение группы A на сопряженные системы по подгрупп M будет иметь вид

$$\begin{aligned} A &= M + M(1,2)(34) + MT(0,1) + MT(0,2) + MT(0,3) + MT(0,4) = \\ &= M + M(1,2)(3,4) + M(0,1,2,4,3) + M(0,2,4,3,1) + \\ &\quad + M(0,3,1,2,4) + M(0,4,3,1,2). \end{aligned}$$

Сопряженные значения функций u и u' будут

$$
\begin{aligned}
u &= x_0x_1 + x_1x_2 + x_2x_3 + x_3x_4 + x_4x_0,\\
u_1 &= x_0x_2 + x_2x_1 + x_1x_4 + x_4x_3 + x_3x_0,\\
u_2 &= x_1x_2 + x_2x_4 + x_4x_0 + x_0x_3 + x_3x_1,\\
u_3 &= x_2x_0 + x_0x_4 + x_4x_1 + x_1x_3 + x_3x_2,\\
u_4 &= x_3x_2 + x_2x_4 + x_4x_1 + x_1x_0 + x_0x_3,\\
u_5 &= x_4x_2 + x_2x_0 + x_0x_1 + x_1x_3 + x_3x_4,
\end{aligned}
\tag{5}
$$

подобным образом,

$$
\begin{aligned}
u' &= x_0x_2 + x_2x_4 + x_4x_1 + x_1x_3 + x_3x_0,\\
u'_1 &= x_0x_1 + x_1x_3 + x_3x_2 + x_2x_4 + x_4x_0,\\
u'_2 &= x_1x_4 + x_4x_3 + x_3x_2 + x_2x_0 + x_0x_1,\\
u'_3 &= x_2x_4 + x_4x_3 + x_3x_0 + x_0x_1 + x_1x_2,\\
u'_4 &= x_3x_4 + x_4x_0 + x_0x_2 + x_2x_1 + x_1x_3,\\
u'_5 &= x_4x_0 + x_0x_3 + x_3x_2 + x_2x_1 + x_1x_4.
\end{aligned}
\tag{6}
$$

Резольвента Cayley

§ 5

Все относящаяся к нахождению уравнения шестой степени, которому удовлетворяет функцию

$$u = y - y',$$

выкладки для самого общего буквенного уравнения пятой степени (3) § 4 были выполнены Cayley в его знаменитом мемуаре «On a new auxiliary equation in the theorie of equations of the fifth order» Papers V. IV p. 309 № 268. Главным результатом этого мемуара является блестящая, мастерски проведенная до конца, выкладка длинного вычисления, устрашавшего всех предшествовавших авторов.

Мы выведешь резольвенту Cayley, не следуя буквенно методе указанного мемуара.

Величины y, y_1, y_2, y_3, y_4, y_5 будут корнями уравнения 6-ой степени, коэффициенты которого будут рационально выражаться через величины

$$a,\quad b,\quad c,\quad d,\quad e,\quad f,\quad \sqrt{\Delta}.$$

Так как y меняет знак с изменением знака

$$
\begin{aligned}
\sqrt{\Delta} = (x_0 - x_1)(x_0 - x_2)(x_0 - x_3)(x_0 - x_4)(x_1 - x_2)(x_1 - x_3)\cdot\\
\cdot(x_1 - x_4)(x_2 - x_3)(x_2 - x_4)(x_3 - x_4),
\end{aligned}
$$

то искомое уравнение 6-ой степени будет иметь вид

$$y^6 + A_2y^4 + A_4y^2 + A_6 - \sqrt{\Delta}(A_1y^5 + A_3y^3 + A_5y) = 0.$$

Коэффициенты

$$A_2, \quad A_4, \quad A_6, \quad \sqrt{\Delta}A_1, \quad \sqrt{\Delta}A_3, \quad \sqrt{\Delta}A_5,$$

должны быть целыми функциями от корней x_i, кроме того три последних коэффициенты должны делиться на $\sqrt{\Delta}$, следовательно, коэффициенты A_2, A_4, A_6, A_1, A_3, A_5 суть целые симметричесния функции от корней x_i.

Корни y_i суть целые функции второй степени от x_i, следовательно, величины

$$A_1\sqrt{\Delta}, \quad A_2, \quad A_3\sqrt{\Delta}, \quad A_4, \quad A_5\sqrt{\Delta}, \quad A_6$$

имеют степени относительно x_i

$$2, \quad 4, \quad 6, \quad 8, \quad 10, \quad 12.$$

Но $\sqrt{\Delta}$ есть функция 10-ой степени относительно x_i и мы получаем

$$A_1 = 0, \quad A_2 = 0,$$

а коэффициент A_5 есть число.

Итак, искомое уравнение имеет вид

$$y^6 + A_2y^4 + A_4y^2 + A_6 - k\sqrt{\Delta}y = 0, \tag{1}$$

где A_2, A_4, A_6 выражаются рационально через коэффициенты a, b, c, d, e, f уравнения 5-ой степени, а k есть число независимое от этих коэффициентов и, следовательно, общее для всех уравнений пятой степени.

§ 6

Начнем с вычисления коэффициента k и покажем, что должно быть $k = 32$.

Проще всего применим вывод уравнения (1) § 5 к самому простому уравнений 5-ой степени

$$x^5 - 1 = 0. \tag{1}$$

Мы имеем $x^5 - 1 = (X - 1)X_5$. По формуле для дискриминанта Δ_0 уравнения $X_5 = 0$, данной в § 35 главы XIII, мы имеем

$$\Delta_0 = 5^3.$$

Тогда дискриминант Δ уравнения (1) будет выражаться так

$$\Delta = (1 - x_1)^2(1 - x_2)^2(1 - x_3)^2(1 - x_4)^2\Delta_0,$$

где x_1, x_2, x_3, x_4 корни X_5.

Мы получаем

$$\Delta = [X_5(1)]^2\Delta_0 = 5^5.$$

Очевидно, что этот результат можно получить сразу, как результант функции $x^5 - 1$ и ее производной $5x^4$

$$\Delta = 5 \cdot 1^4 \cdot 5x_1^4 \cdot 5x_2^4 \cdot 5x_3^2 \cdot 5x_4^4 = 5^5.$$

Резольвента Cayley должна иметь вид

$$y^6 + A_2y^4 + A_4y^2 + A_6 - k5^{\frac{5}{2}}y = 0. \tag{2}$$

Теперь составим эту резольвенту по ее определению.

Пусть корни уравнения (1) будут

$$x_0 = 1, \quad x_1 = e^{\alpha}, \quad x_2 = e^{2\alpha}, \quad x_3 = e^{3\alpha}, \quad x_4 = e^{4\alpha}, \quad \text{где} \quad \alpha = \frac{2\pi i}{5}.$$

После простой выкладки получим по формулам (5) и (6) § 4

$$y = 0, \ y_1 = 2e^{\alpha}\cdot\mathfrak{A}, \ y_1 = 2e^{\alpha}\cdot\mathfrak{A}, \ y_2 = 2e^{2\alpha}\cdot\mathfrak{A}, \ y_3 = 2e^{3\alpha}\cdot\mathfrak{A}, \ y_4 = 2e^{4\alpha}\cdot\mathfrak{A}, \ y_5 = 2e^{5\alpha}\cdot\mathfrak{A},$$

где $\mathfrak{A} = -(1 - e^{\alpha})(1 - e^{2\alpha})$..

Получаем для y такое уравнение

$$y[y^5 - 2^5\mathfrak{A}^5] = 0. \tag{3}$$

Сравнивая (2) и (3), получим

$$A_2 = 0, \quad A_4 = 0, \quad A_6 = 0,$$

$$k5^{\frac{5}{2}} = 32\mathfrak{A}^5.$$

Но мы имеем (см. § 22 главы XIII)

$$(1 - e^{\alpha})(1 - e^{2\alpha})(1 - e^{3\alpha})(1 - e^{4\alpha}) = 5,$$

откуда

$$[(1 - e^{\alpha})(1 - e^{2\alpha})]^2 = 5e^{3\alpha};$$

далее, возвышая в 5-ую степень,

$$\mathfrak{A}^{10} = 5^5,$$

и, следовательно, $k = 32$, что и требовалось показать.

§ 7

Обращаясь к вычислений других коэффициентов резольвенты Cayley, заметим, что упрощение, которым Cayley пользуется, состоит в том, что коэффициенты A_2, A_4, A_6, а также и дискриминант Δ суть то, что мы назвали в § 29 главы IX функциями критическими, ибо они суть функции разностей корней, значить, для вычисления таких функций применим простой способ, приведенный в § 30 главы IX.

В самом деле,

$$\begin{gathered}(x_0 - x_4)(x_1 - x_4) + (x_1 - x_4)(x_2 - x_4) + (x_2 - x_4)(x_3 - x_4) = \\ = x_0x_1 + x_1x_2 + x_2x_3 - x_4(x_0 + 2x_1 + 2x_2 + x_3) + x_4^2 \\ (x_1 - x_4)(x_3 - x_4) + (x_3 - x_4)(x_0 - x_4) + (x_0 - x_4)(x_2 - x_4) = \\ = x_0x_2 + x_0x_3 + x_1x_3 - x_4(x_1 + 2x_3 + 2x_0 + x_2) = x_4^2.\end{gathered}$$

Вычитая второе тождество из первого, получим во второй части $y = u - u'$, следовательно, будем иметь

$$y = [(x_0 - x_4)(x_1 - x_4) + (x_1 - x_4)(x_2 - x_4) + (x_2 - x_4)(x_3 - x_4)] -$$
$$-[(x_1 - x_4)(x_3 - x_4) + (x_3 - x_4)(x_0 - x_4) + (x_0 - x_4)(x_2 - x_4)].$$

Итак, мы можем вычислять искомые коэффициенты как функции критические, т. е. удовлетворяющие дифференциальному уравнению

$$5a\,\frac{\partial\varphi}{\partial b} + 4b\,\frac{\partial\varphi}{\partial c} + 3c\,\frac{\partial\varphi}{\partial d} + 2d\,\frac{\partial\varphi}{\partial e} + e\,\frac{\partial\varphi}{\partial f} = 0. \tag{1}$$

На оснований теорем § 28 главы IX мы замечаем, что коэффициент A_2 должен иметь степень 2 и вес 4 относительно отношений

$$\frac{b}{a},\quad \frac{c}{a},\quad \frac{d}{a},\quad \frac{e}{a},\quad \frac{f}{a}, \tag{2}$$

веса которых суть

$$1,\quad 2,\quad 3,\quad 4,\quad 5$$

мы будем умножением на известную степень a писать коэффициенты A_2, A_4, A_6 в целом виде. Так как A_6 шестой степени относительно дробей (2), то, умножая всю резольвенту Cayley на a^6, перепишем ее так:

$$a^6y^6 + \mathfrak{A}a^4y^4 + \mathfrak{B}a^2y^2 - 32a^2\sqrt{\Delta'}y + \mathfrak{C} = 0,$$

где коэффициенты

$$\mathfrak{A},\quad \mathfrak{B},\quad \mathfrak{C} \tag{3}$$

однородные функции от a, b, c, d, e, f степеней

$$2,\quad 4,\quad 6.$$

Полагая веса коэффициентов a, b, c, d, e, f равными $0, 1, 2, 3, 4, 5$, получим для весов коэффициентов (3) значения

$$4,\quad 8,\quad 14.$$

Таким образом, мы найдем сразу буквенное выражение функций $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$ с неопределенными коэффициентами. Дифференциальное уравнение (2) поможет вычислить эти коэффициенты с точностью до постоянного множителя. Чтобы определить далее этот множитель, достаточно будет указать один из коэффициентов.

Это можно сделать проще всего следующим образом.

Положим $x_2 = 0$, $x_3 = 0$, $x_4 = 0$. Тогда будем иметь $\Delta = 0$. Уравнение 5-ой степени принимает вид

$$ax^5 + bx^4 + cx^3 = 0,$$

и, значить, $d = 0$, $e = 0$, $f = 0$.

Получаем,

$$\begin{aligned} u &= x_0x_1, & u' &= 0,\\ u_1 &= 0, & u_1' &= x_0x_1,\\ u_2 &= 0, & u_2' &= x_0x_1,\\ u_3 &= 0, & u_3' &= x_0x_1,\\ u_4 &= x_0x_1, & u_4' &= 0,\\ u_5 &= x_0x_1, & u_5' &= 0. \end{aligned}$$

Принимая во внимание, что $x_0x_1 = \dfrac{c}{a}$, получим

$$y = y_4 = y_5 = -y_1 = -y_2 = -y_3 = \frac{c}{a}.$$

Резольвента Cayley принимает вид

$$(a^2y^2 - c^2)^3 = 0.$$

Итак, мы видим, что в общем случае

$$\begin{aligned} \mathfrak{A} &= -3c^2 + \ldots\\ \mathfrak{B} &= 3c^4 + \ldots\\ \mathfrak{C} &= -c^6 + \ldots \end{aligned}$$

§ 8

Обращаемся теперь к вычислению $\mathfrak{A}$, $\mathfrak{B}$, $\mathfrak{C}$.

Функция $\mathfrak{A}$ второй степени и четвертого веса, следовательно, ее буквенное выражение должно быть

$$Aae + Bdb + Cc^2, \tag{1}$$

причем мы знаем уже, что $C = -3$.

Подставляя выражение (1) в дифференциальное уравнение, получим тождество

$$(5B + 2A)ad + (8C + 3B)cb = 0 = 0;$$

Приравнивая нулю коэффициенты, получим

$$5B + 2A = 0, \quad 8C + 3B = 0,$$

откуда

$$A = -20, \quad B = 8, \quad C = -3.$$

Итак,

$$\mathfrak{A} = -20ae + 8db - 3c^2. \tag{2}$$

Если заданное уравнение 5-й степени написано так

$$ax^5 + 5bx^4 + 10cx^3 + 10dx^2 + 5ex + f = 0, \tag{3}$$

где к коэффитцентам приписаны множителями биномиальные коэффициенты, то такую форму (3) уравнения 5-й степени Cayley называет Standart form. В отличие от этого он называет denumerate form обычную форму писания уравнения 5-ой степени

$$ax^5 + bx^4 + cx^3 + dx^2 + ex + f = 0.$$

Для Standart form мы получим, очевидно,

$$\mathfrak{A} = 100(-ae + 4db - 3c^2). \tag{4}$$

Формы (2) и (4) можно указать при помощи такой таблички

d.f.	s.f. 100	a	b	c	d	e	f
−20	−1	1	0	0	0	1	0
+8	+4	0	1	0	1	0	0
−3	−3	0	0	2	0	0	0

В этой табличке в левых двух колоннах написаны коэффициенты для обеих форм, в шести следующих колоннах, соответствующих буквенному выражений члена, написаны показатели над соответственной буквой.

Подобным же образом мы можем вычислить без особенного затруднения величины $\mathfrak{B}$, $\mathfrak{C}$ и Δ.

Для $\mathfrak{B}$ получаем

d.f.	s.f. 2000	a	b	c	d	e	f
−400	−2	2	0	0	1	0	1
+240	+3	2	0	0	0	2	0
+240	+6	1	1	1	0	0	1
−112	−14	1	1	0	1	1	0
−8	−2	1	0	2	0	1	0
+16	+8	1	0	1	2	0	0
−64	−4	0	3	0	0	0	1
+16	+10	0	2	1	0	1	0
+16	+20	0	2	0	2	0	0
−16	−40	0	1	2	1	0	0
+3	+15	0	0	3	0	0	0

Для $\mathfrak{C}$ получаем

d.f.	s.f. 40000	a	b	c	d	e	f	d.f.	s.f. 40000	a	b	c	d	e	f
+4000	+1	3	0	1	0	0	2	+224	+35	1	2	1	0	2	0
−1600	−2	3	0	0	1	1	1	−128	−40	1	2	0	2	1	0
+320	+1	3	0	0	0	3	0	+48	+6	1	1	3	0	0	1
−1600	−1	2	2	0	0	0	2	−112	−70	1	1	2	1	1	0
−640	−4	2	1	1	0	1	1	+64	+80	1	1	1	3	0	0
+640	+8	2	1	0	2	0	1	+28	+35	1	0	4	0	1	0

−64	−2	2	1	0	1	2	0	−16	−40	1	0	3	2	0	0
−80	−2	2	0	2	1	0	1	−64	−25	0	4	0	0	2	0
−176	−11	2	0	2	0	2	0	+64	+100	0	3	1	1	1	0
+224	+28	2	0	1	2	1	0	−16	−50	0	2	3	0	1	0
−64	−16	2	0	0	4	0	0	−16	−100	0	2	2	2	0	0
+384	+6	1	3	0	0	1	1	+8	+100	0	1	4	1	0	0
−192	−12	1	2	1	1	0	1	−1	−25	0	0	6	0	0	0

Для дискриминанта Δ получаем

d.f.	s.f. 3125	a	b	c	d	e	f	d.f.	s.f. 3125	a	b	c	d	e	f
+3125	+1	4	0	0	0	0	4	+24	+960	1	2	0	3	1	1
−2500	−20	3	1	0	0	1	3	−6	−600	1	2	0	2	3	0
−3750	−120	3	0	1	1	0	3	−630	−10080	1	1	3	1	0	2
+2000	+160	3	0	1	0	2	2	+24	+960	1	1	3	2	0	1
+2050	+360	3	0	0	2	1	2	+356	+28480	1	1	2	2	1	1
−1600	−640	3	0	0	1	3	1	−80	−16000	1	1	2	1	3	0
+256	+256	3	0	0	0	5	0	−72	−11520	1	1	1	4	0	1
+2000	+160	2	2	0	1	0	3	+18	+7200	1	1	1	3	2	0
−50	−10	2	2	0	0	2	2	+108	+3456	1	0	5	0	0	2
+2250	+360	2	1	2	0	0	3	−72	−11520	1	0	4	1	1	1
−2050	−1640	3	1	1	1	1	2	+16	+6400	1	0	4	0	3	0
+160	+320	2	1	1	0	3	1	+16	+5120	1	0	3	3	0	1
−900	−1440	2	1	0	3	0	2	−4	−3200	1	0	3	2	2	0
+1020	+4080	2	1	0	2	2	1	+256	+256	0	5	0	0	0	3
−192	−1920	2	1	0	1	4	0	−192	−41920	0	4	1	0	1	2
−900	−1440	2	0	3	0	1	2	−128	−2560	0	4	0	2	0	2
+825	+2640	2	0	2	2	0	2	+144	+7200	0	4	0	1	2	1
+560	+4480	2	0	2	1	2	1	−27	−3375	0	4	0	0	4	0
−128	−2560	2	0	2	0	4	0	+144	+5760	0	3	2	1	0	2
−630	−10080	2	0	1	3	1	1	−6	−600	0	3	2	0	2	1
+144	+5760	2	0	1	2	3	0	−80	−16000	0	3	1	2	1	1
+108	+3456	2	0	0	5	0	1	+18	+9000	0	3	1	1	3	0
−27	−2160	2	0	0	4	2	0	+16	+6400	0	3	0	4	0	1
−1600	−640	1	3	1	0	0	3	−4	−4000	0	3	0	3	2	0
+160	+320	1	3	0	1	1	2	−27	−2160	0	2	4	0	0	2
−36	−180	1	3	0	0	3	1	+18	+7200	0	2	3	1	1	1
+1020	+4080	1	2	2	0	1	2	−4	−400	0	2	3	0	3	0
+560	+4480	1	2	1	2	0	2	−4	−3200	0	2	2	3	0	1
−746	−14920	1	2	1	1	2	1	+1	+2000	0	2	2	2	2	0
+144	+7200	1	2	1	0	4	0								

§ 9

Вычисление $\mathfrak{C}$ и Δ приводит к довольно большим выкладкам, а потому заслу-

живает внимания остроумный способ рассуждения, придуманный Cayley.

Он полагает один из корней равным нулю

$$x_4 = 0,$$

тогда четыре других корня x_0, x_1, x_2, x_3 удовлетворяют уравнению четвертой степени

$$ax^4 + bx^3 + cx^2 + dx + e = 0, \tag{1}$$

причем $f = 0$.

Пусть искомый дискриминант раскладывается следующим образом по степеням f

$$\Delta = A + f \cdot B + f^2 \cdot C + \ldots, \tag{2}$$

где A, B, C суть целые функций от коэффициентов уравнения четвертой степени (1).

Обозначая операцию

$$5a\,\frac{\partial\varphi}{\partial b} + 4b\,\frac{\partial\varphi}{\partial c} + 3c\,\frac{\partial\varphi}{\partial d} + 2d\,\frac{\partial\varphi}{\partial e}$$

через

$$\nabla\varphi,$$

мы замечаем, что дискриминант, как критическая функция, должен удовлетворять дифференциальному уравнению

$$\nabla\varphi + e\,\frac{\partial\varphi}{\partial f} = 0. \tag{3}$$

Подставляя выражение (2) в уравнение (3), должны придти к тождеству

$$\nabla A + f\nabla B + f^2\nabla C + \ldots + eB + 2feC + \ldots = 0,$$

откуда, приравнивая нулю коэффициенты при разных степенях f, получаем ряд равенств

$$eB = -\nabla A, \quad 2eC = -\nabla B, \ \ldots \tag{4}$$

Мы видим, что, если у нас известна функция A, то по формулам (4) мы найдем последовательно B, C, ...

Обозначая через Δ_0 дискриминант уравнения четвертой степени (1), получим

$$\Delta = \Delta_0(x_0 - x_4)^2(x_1 - x_4)^2(x_2 - x_4)^2(x_3 - x_4)^2,$$

полагая $x_4 = 0$, получим

$$A = \Delta_0 x_0^2 x_1^2 x_3^2 = \Delta_0 e^2.$$

Итак, метод Cayley состоит в том, что дискриминант уравнения 5-ой степени выводится из дискриминанта уравнения 4-ой степени. По идее он аналогичен методу Cauchy, изложенному в § 27 главы IX.

Подобным же образом ложно вычислить коэффициент $\mathfrak{B}$ в случае $f = 0$ и далее дополнить его членами, заключающими f, что и проделал Cayley.

Группа резольвенты

§ 10

Рассмотрим резольвенту Cayley 6-ой степени, корни которой суть

$$v = (u - u')^2, \qquad v_1 = (u_1 - u'_1)^2, \quad v_2 = (u_2 - u'_2)^2,$$
$$v_3 = (u_3 - u'_3)^2, \quad v_4 = (u_4 - u'_4)^2, \quad v_5 = (u_5 - u'_5)^2.$$

Корень v принадлежит к полной метациклической группе $\mathfrak{M}$, все сопряженные группы

$$S^{-1}\mathfrak{M}S$$

в случае буквенных уравнений не могут иметь общий делитель, отличный от единицы, ибо, иначе, этот делитель, отличаясь от знакопеременной группы, должен был бы быть нормальным делителем симметрической, что невозможно.

Итак, резольвента 6-ой степени есть полная резольвента, следовательно, группа этой резольвенты должна совпадать с группой заданного уравнения, то есть, иметь порядок $120 = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5$.

Кроме того, в общем случай резольвента есть уравнение неприводимое, сдедовательно, группа резольвенты должна быть транзитивною.

Симметрическая группа перестановок шести букв имеет порядок $1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 = 6 \cdot 120$.

Мы приходим к заключению, что симметрическая группа шести перемещаемых элементов должна иметь транзитивный делитель индекса 6. Этот делитель есть та группа, о которой сказано в § 41 главы V.

Index nominum

Index rerum