DIE GRUNDLEHREN DER MATHEMATISCHEN WISSENSCHAFTEN IN EINZELDARSTELLUNGEN

BAND XXXIII

B. L. VAN DER WAERDEN

MODERNE ALGEBRA

ERSTER TEIL

Springer-Verlag Berlin Heidelberg GmbH

DIE GRUNDLEHREN DER

MATHEMATISCHEN WISSENSCHAFTEN

IN EINZELDARSTELLUNGEN MIT BESONDERER BERÜCKSICHTIGUNG DER ANWENDUNGSGEBIETE

GEMEINSAM MIT

W. BLASCHKE
HAMBURG

M. BORN
GÖTTINGEN

C. RUNGE†
GÖTTINGEN

HERAUSGEGEBEN VON

R. COURANT
GÖTTINGEN

BAND XXXIII

MODERNE ALGEBRA I

VON

B. L. VAN DER WAERDEN

Springer-Verlag Berlin Heidelberg GmbH
1930

MODERNE ALGEBRA

VON

DR. B. L. VAN DER WAERDEN
O. PROFESSOR AN DER UNIVERSITÄT
GRONINGEN

UNTER BENUTZUNG VON VORLESUNGEN
VON
E. ARTIN UND E. NOETHER

ERSTER TEIL

Springer-Verlag Berlin Heidelberg GmbH
1930

ISBN 978-3-662-41761-4 ISBN 978-3-662-41906-9 (eBook)
DOI 10.1007/978-3-662-41906-9

Vorwort.

Das vorliegende Buch hat sich aus einer Ausarbeitung einer Vorlesung von E. ARTIN (Hamburg, Sommer 1926) entwickelt; es ist aber so vielen Umarbeitungen und Erweiterungen unterzogen und es sind so viele andere Vorlesungen und neuere Untersuchungen darin verarbeitet worden (man sehe die Einleitung), daß man die Artinsche Vorlesung nur schwer darin wird wiederfinden können.

Allen Helfern, die durch ihre kritischen Bemerkungen das Werk gefördert haben, sage ich an dieser Stelle herzlichen Dank. Vor allem muß ich aber Herrn Dr. W. WEBER in Göttingen erwähnen, dessen nie ermüdende Hilfe bei der Herstellung des Manuskriptes nicht hoch genug gewertet werden kann.

Groningen, im Sommer 1930.

B. L. VAN DER WAERDEN.

Inhaltsverzeichnis.

Seite

Einleitung 1

Erstes Kapitel.

Zahlen und Mengen.

§ 1. Mengen 4
§ 2. Abbildungen. Mächtigkeiten 6
§ 3. Die Zahlreihe 7
§ 4. Endliche und abzählbare Mengen 11
§ 5. Klasseneinteilungen 13

Zweites Kapitel.

Gruppen.

§ 6. Der Gruppenbegriff 15
§ 7. Untergruppen 23
§ 8. Isomorphismen und Automorphismen 28
§ 9. Homomorphie. Normalteiler. Faktorgruppen 32

Drittes Kapitel.

Ringe und Körper.

§ 10. Ringe 36
§ 11. Homomorphie und Isomorphie 44
§ 12. Quotientenbildung 46
§ 13. Polynomringe 49
§ 14. Ideale. Restklassenringe 53
§ 15. Teilbarkeit. Primideale 58
§ 16. Hauptidealringe 60
§ 17. Faktorzerlegung 62

Viertes Kapitel.

Ganze rationale Funktionen.

§ 18. Differentiation 67
§ 19. Nullstellen 69
§ 20. Interpolationsformeln 71
§ 21. Faktorzerlegung 73
§ 22. Irreduzibilitätskriterien 77
§ 23. Die Durchführung der Faktorzerlegung in endlichvielen Schritten . . 79
§ 24. Symmetrische Funktionen 80

Fünftes Kapitel.

Körpertheorie.

Seite
§ 25. Unterkörper. Primkörper 86
§ 26. Adjunktion 88
§ 27. Einfache Körpererweiterungen 89
§ 28. Lineare Abhängigkeit von Größen in bezug auf einen Körper 95
§ 29. Algebraische Körpererweiterungen 99
§ 30. Einheitswurzeln 104
§ 31. Galois-Felder (endliche kommutative Körper) 109
§ 32. Separable und inseparable Erweiterungen (Erweiterungen erster und zweiter Art 113
§ 33. Vollkommene und unvollkommene Körper. Wurzelkörper 118
§ 34. Einfachheit von algebraischen Erweiterungen. Der Satz vom primitiven Element 120
§ 35. Normen und Spuren 122
§ 36. Einfache transzendente Erweiterungen 125
§ 37. Die Ausführung der körpertheoretischen Operationen in endlichvielen Schritten 128

Sechstes Kapitel.

Fortsetzung der Gruppentheorie.

§ 38. Gruppen mit Operatoren 132
§ 39. Operatorisomorphismus und -homomorphismus 134
§ 40. Die beiden Isomorphiesätze 135
§ 41. Normalreihen und Kompositionsreihen 137
§ 42. Direkte Produkte 141
§ 43. Die Einfachheit der alternierenden Gruppe 144
§ 44. Transitivität und Primitivität 145

Siebentes Kapitel.

Die Theorie von Galois.

§ 45. Die Galoissche Gruppe 148
§ 46. Der Hauptsatz der Galoisschen Theorie 151
§ 47. Konjugierte Gruppen, Körper und Körperelemente 154
§ 48. Kreisteilungskörper 156
§ 49. Die Perioden der Kreisteilungsgleichung 160
§ 50. Zyklische Körper und reine Gleichungen 165
§ 51. Die Auflösung von Gleichungen durch Radikale 169
§ 52. Die allgemeine Gleichung n-ten Grades 172
§ 53. Gleichungen zweiten, dritten und vierten Grades 175
§ 54. Konstruktionen mit Zirkel und Lineal 181
§ 55. Die metazyklischen Gleichungen von Primzahlgrad 186
§ 56. Die Berechnung der Galoisschen Gruppe. Gleichungen mit symmetrischer Gruppe 188

Achtes Kapitel.

Geordnete und wohlgeordnete Mengen.

§ 57. Geordnete Mengen 192
§ 58. Das Auswahlpostulat und der Wohlordnungssatz 194
§ 59. Die transfinite Induktion 196

Neuntes Kapitel.

Unendliche Körpererweiterungen.

Seite
§ 60. Die algebraisch-abgeschlossenen Körper 198
§ 61. Rein transzendente Erweiterungen. Irreduzible Systeme 203
§ 62. Der Transzendenzgrad 206

Zehntes Kapitel.

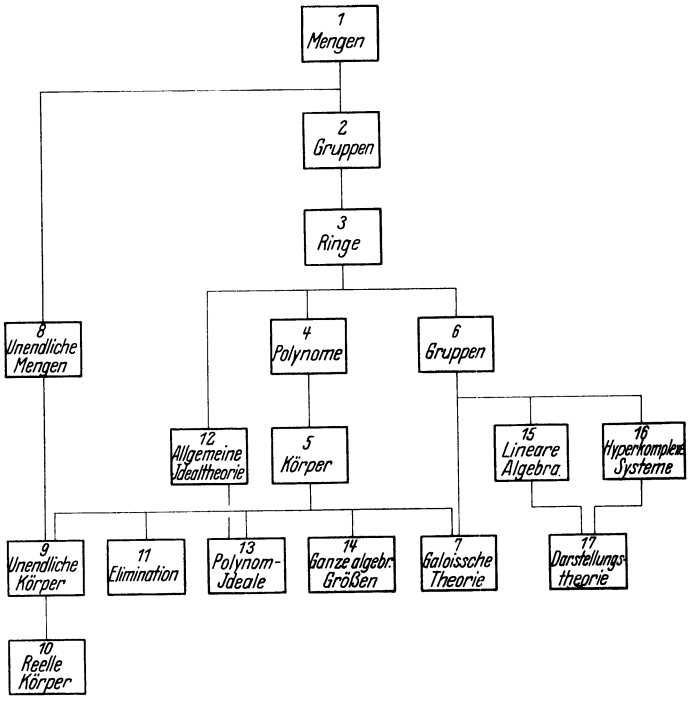
Reelle Körper.

§ 63. Angeordnete Körper 209
§ 64. Definition der reellen Zahlen 212
§ 65. Bewertete Körper. — p-adische Zahlen 218
§ 66. Nullstellen reeller Funktionen 220
§ 67. Algebraische Theorie der reellen Körper 226
§ 68. Existenzsätze für formal-reelle Körper 231
§ 69. Die Beträge der komplexen Zahlen 235
§ 70. Summen von Quadraten 236

Sachverzeichnis 239

Leitfaden.

Übersicht über die Kapitel der beiden Bände und ihre logische Abhängigkeit.



Einleitung.

Ziel des Buches. Die „abstrakte", „formale" oder „axiomatische" Richtung, der die Algebra ihren erneuten Aufschwung in der jüngsten Zeit verdankt, hat vor allem in der *Körpertheorie*, der *Idealtheorie*, der *Gruppentheorie* und der *Theorie der hyperkomplexen Zahlen* zu einer Reihe von neuartigen Begriffsbildungen, zur Einsicht in neue Zusammenhänge und zu weitreichenden Resultaten geführt. In diese ganze Begriffswelt den Leser einzuführen, soll das Hauptziel dieses Buches sein.

Stehen demnach allgemeine Begriffe und Methoden im Vordergrund, so sollen doch auch die Einzelresultate, die zum klassischen Bestand der Algebra gerechnet werden müssen, eine gehörige Berücksichtigung im Rahmen des modernen Aufbaus finden.

Einteilung. Anweisungen für die Leser. Um die allgemeinen Gesichtspunkte, welche die „abstrakte" Auffassung der Algebra beherrschen, genügend klar zu entwickeln, war es notwendig, trotzdem das Buch nicht als Anfängerlehrbuch gemeint ist, doch die ersten Grundlagen der Gruppentheorie und der elementaren Algebra von Anfang an neu darzustellen.

Angesichts der vielen in neuester Zeit erschienenen guten Darstellungen der Gruppentheorie, der klassischen Algebra und der Körpertheorie ergab sich die Möglichkeit, diese einleitenden Teile knapp (aber lückenlos) zu fassen. Eine breitere Darstellung kann der Anfänger jetzt überall finden[1].

Als weiteres Leitprinzip diente die Forderung, daß möglichst jeder

---

[1] Für die Gruppentheorie sei verwiesen auf:

Speiser, A.: Die Theorie der Gruppen von endlicher Ordnung, 2. Aufl. Berlin: Julius Springer 1927.

Für die Körpertheorie auf:

Hasse, H.: Höhere Algebra I, II. Sammlung Göschen 1926/27.

Haupt, O.: Einführung in die Algebra I, II. Leipzig 1929.

Für die klassische Algebra auf:

Perron, O.: Algebra I, II. 1927.

Für die lineare Algebra auf:

Bôcher, M.: Introduction to higher Algebra. New York 1908 (auch deutsch von H. Beck, Leipzig 1910).

Dickson, L. E.: Modern algebraic Theories, Chicago 1926 (auch deutsch von E. Bodewig, Leipzig 1929).

einzelne Teil für sich allein verständlich sein soll. Wer die allgemeine Idealtheorie oder die Theorie der hyperkomplexen Zahlen kennenlernen will, braucht nicht die Galoissche Theorie vorher zu studieren, und umgekehrt; und wer etwas über Elimination oder lineare Algebra nachschlagen will, darf nicht durch komplizierte idealtheoretische Begriffsbildungen abgeschreckt werden.

Die Einteilung ist darum so gewählt, daß die ersten drei Kapitel auf kleinstem Raum das enthalten, was für *alle* weiteren Kapitel als Vorbereitung nötig ist: die ersten Grundbegriffe über: 1. Mengen; 2. Gruppen; 3. Ringe, Ideale und Körper. Die weiteren Kapitel des I. Bandes sind hauptsächlich der Theorie der kommutativen Körper gewidmet und folgen in Einteilung und Methoden vorwiegend der grundlegenden Arbeit von STEINITZ in Crelles Journal Bd. 137 (1910)[1]. Im II. Band soll in möglichst voneinander unabhängigen Abschnitten die Theorie der Moduln, Ringe und Ideale mit Anwendungen auf Eliminationstheorie, Elementarteiler, hyperkomplexe Zahlen und Darstellungen von Gruppen zur Behandlung kommen.

Weggelassen mußten werden die Theorie der algebraischen Funktionen und die der kontinuierlichen Gruppen, weil beide für eine sachgemäße Behandlung transzendente Begriffe und Methoden benötigen würden; weiter auf Grund ihres Umfanges die Invariantentheorie. Als bekannt vorausgesetzt sind die Determinanten, die übrigens nur ganz selten und in den mehr elementaren Kapiteln überhaupt nicht benutzt werden.

Zur weiteren Orientierung sei auf das Inhaltsverzeichnis und vor allem auf den vorstehenden schematischen „Leitfaden" verwiesen, aus dem genau zu ersehen ist, wieviel von den vorangehenden Kapiteln zu jedem einzelnen Kapitel benötigt wird.

Weniger wichtige oder schwierigere Zusätze sind klein gedruckt. Die letzten drei Kapitel des I. Bandes können bei erster Lektüre übergangen werden.

Die eingestreuten Aufgaben sind meist so gewählt, daß man an ihnen erproben kann, ob man den Text verstanden hat. Sie enthalten auch Beispiele und Ergänzungen, auf die an späteren Stellen gelegentlich Bezug genommen wird. Kunstgriffe sind zu ihrer Lösung meist nicht erforderlich und sonst in eckigen Klammern angedeutet.

Quellen. Das vorliegende Buch hat sich teilweise aus Vorlesungsausarbeitungen entwickelt, und zwar wurden benutzt:

eine Vorlesung von E. ARTIN über Algebra (Hamburg, Sommersemester 1926);

ein Seminar über Idealtheorie, abgehalten von E. ARTIN, W. BLASCHKE, O. SCHREIER und dem Verfasser (Hamburg, Wintersemester 1926/27).

[1] Diese Arbeit soll demnächst in Buchform erscheinen.

eine Vorlesung vom Verfasser über allgemeine Idealtheorie (Göttingen, Wintersemester 1927/28);

zwei Vorlesungen von E. NOETHER, beide über Gruppentheorie und hyperkomplexe Zahlen (Göttingen, Wintersemester 1924/25, Wintersemester 1927/28)[1].

Wo man in diesem Buch neue Beweise oder Beweisanordnungen findet, wird man sie oft auf die erwähnten Vorlesungen und Seminare zurückzuführen haben, auch dann, wenn nicht ausdrücklich die Quelle erwähnt ist.

[1] Eine Ausarbeitung der zuletzt genannten Vorlesung von E. NOETHER ist erschienen in der Math. Zeitschrift 30 (1929) S. 641—692.

Erstes Kapitel.

Zahlen und Mengen.

Da gewisse logische und allgemein-mathematische Begriffe, insbesondere der Mengenbegriff, mit denen der angehende Mathematiker vielfach noch nicht vertraut ist, in diesem Buch Verwendung finden, soll ein kurzer Abschnitt über diese Begriffe vorangehen. Auf Grundlagenschwierigkeiten[1] soll dabei nicht eingegangen werden: wir stellen uns durchwegs auf den „naiven Standpunkt", allerdings unter Vermeidung von paradoxienerzeugenden Zirkeldefinitionen. Der Fortgeschrittene braucht sich von diesem Kapitel bloß die Bedeutung der Zeichen $\in$, $\subset$, $\supset$, $\cap$, $\vee$ und $\{..\}$ zu merken und kann alles übrige übergehen.

§ 1. Mengen.

Wir denken uns, als Ausgangspunkt aller mathematischen Betrachtung, gewisse vorstellbare Objekte, etwa Zahlzeichen, Buchstaben oder Kombinationen von solchen. Eine Eigenschaft, die jedes einzelne dieser Objekte hat oder nicht hat, definiert eine *Menge* oder *Klasse*; *Elemente der Menge* sind diejenigen Objekte, denen diese Eigenschaft zukommt. Das Zeichen

$$a \in \mathfrak{M}$$

bedeutet: a ist Element von $\mathfrak{M}$. Man sagt auch geometrisch-bildlich: a liegt in $\mathfrak{M}$. Eine Menge heißt *leer*, wenn sie keine Elemente enthält.

Wir nehmen an, daß es erlaubt ist, Folgen und Mengen von Zahlen (oder von Buchstaben usw.) selbst wieder als Objekte und Elemente von Mengen (Mengen zweiter Stufe, wie man bisweilen sagt) aufzufassen. Diese Mengen zweiter Stufe können wieder Elemente von Mengen höherer Stufe sein, usw. Wir hüten uns jedoch vor Begriffsbildungen wie „die Menge aller Mengen" u. dgl., weil diese zu Widersprüchen Anlaß geben können (und gegeben haben); vielmehr bilden wir neue Mengen nur aus einer jeweils vorher abgegrenzten Kategorie von Objekten (zu denen die neuen Mengen noch nicht gehören).

---

[1] Für diese vergleiche man A. FRAENKEL, Einführung in die Mengenlehre, 3. Aufl. (Berlin 1928).

Sind alle Elemente einer Menge $\mathfrak{N}$ zugleich Elemente von $\mathfrak{M}$, so heißt $\mathfrak{N}$ eine *Untermenge* oder *Teilmenge* von $\mathfrak{M}$, und man schreibt:

$$\mathfrak{N} \subseteq \mathfrak{M}.$$

$\mathfrak{M}$ heißt dann auch *Obermenge* oder *umfassende Menge* von $\mathfrak{N}$, in Zeichen:

$$\mathfrak{M} \supseteq \mathfrak{N}.$$

Aus $\mathfrak{A} \subseteq \mathfrak{B}$ und $\mathfrak{B} \subseteq \mathfrak{C}$ folgt $\mathfrak{A} \subseteq \mathfrak{C}$.

Die leere Menge ist in jeder Menge enthalten.

Sind zugleich alle Elemente von $\mathfrak{M}$ in $\mathfrak{N}$ enthalten und alle Elemente von $\mathfrak{N}$ in $\mathfrak{M}$, so nennt man die Mengen $\mathfrak{M}$, $\mathfrak{N}$ *gleich*:

$$\mathfrak{M} = \mathfrak{N}.$$

Gleichheit bedeutet also das gleichzeitige Bestehen der Relationen

$$\mathfrak{M} \subseteq \mathfrak{N}, \qquad \mathfrak{N} \subseteq \mathfrak{M}.$$

Oder auch: Zwei Mengen sind gleich, wenn sie dieselben Elemente enthalten.

Ist $\mathfrak{N} \subseteq \mathfrak{M}$, ohne $= \mathfrak{M}$ zu sein, so nennt man $\mathfrak{N}$ eine *echte Untermenge* von $\mathfrak{M}$, $\mathfrak{M}$ eine *echte Obermenge* von $\mathfrak{N}$ und schreibt

$$\mathfrak{N} \subset \mathfrak{M}, \qquad \mathfrak{M} \supset \mathfrak{N}.$$

$\mathfrak{N} \subset \mathfrak{M}$ heißt also, daß alle Elemente von $\mathfrak{N}$ in $\mathfrak{M}$ liegen und daß es außerdem noch mindestens ein weiteres Element in $\mathfrak{M}$ gibt, das nicht zu $\mathfrak{N}$ gehört.

Es seien nun $\mathfrak{A}$ und $\mathfrak{B}$ beliebige Mengen. Die Menge $\mathfrak{D}$, die aus allen Elementen besteht, welche sowohl zu $\mathfrak{A}$ als zu $\mathfrak{B}$ gehören, heißt der *Durchschnitt* der Mengen $\mathfrak{A}$ und $\mathfrak{B}$, geschrieben

$$\mathfrak{D} = [\mathfrak{A}, \mathfrak{B}] = \mathfrak{A} \cap \mathfrak{B}.$$

$\mathfrak{D}$ ist Untermenge sowohl von $\mathfrak{A}$ als von $\mathfrak{B}$ und jede Menge von dieser Eigenschaft ist in $\mathfrak{D}$ enthalten.

Die Menge $\mathfrak{V}$, die aus allen Elementen besteht, die zu mindestens einer der Mengen $\mathfrak{A}$, $\mathfrak{B}$ gehören, heißt die *Vereinigungsmenge* von $\mathfrak{A}$ und $\mathfrak{B}$:

$$\mathfrak{V} = \mathfrak{A} \vee \mathfrak{B}$$

$\mathfrak{V}$ umfaßt sowohl $\mathfrak{A}$ als $\mathfrak{B}$, und jede Menge, die $\mathfrak{A}$ und $\mathfrak{B}$ umfaßt, umfaßt auch $\mathfrak{V}$.

Ebenso definiert man Durchschnitt und Vereinigung einer beliebigen Menge $\sum$ von Mengen $\mathfrak{A}, \mathfrak{B}, \ldots$. Für den Durchschnitt (die Menge der Elemente, die in allen Mengen $\mathfrak{A}, \mathfrak{B}, \ldots$ der Menge $\sum$ liegen) schreibt man

$$\mathfrak{D}(\sum) = [\mathfrak{A}, \mathfrak{B}, \ldots].$$

Zwei Mengen heißen *zueinander fremd*, wenn ihr Durchschnitt leer ist, d. h. wenn die beiden Mengen keine Elemente gemein haben.

Wenn eine Menge durch Aufzählung ihrer Elemente gegeben ist, etwa: die Menge $\mathfrak{M}$ soll bestehen aus den Elementen a, b, c, so schreibt man

$$\mathfrak{M} = \{a, b, c\}.$$

Die Schreibweise findet ihre Berechtigung darin, daß nach der Definition der Gleichheit von Mengen eine Menge durch Angabe ihrer Elemente bestimmt ist. Die definierende Eigenschaft, welche die Elemente von $\mathfrak{M}$ auszeichnet, ist: mit a oder b oder c identisch zu sein.

§ 2. Abbildungen. Mächtigkeiten.

Wenn durch irgend eine Vorschrift jedem Element a einer Menge $\mathfrak{M}$ ein einziges neues Objekt $\varphi(a)$ zugeordnet wird, so nennen wir diese Zuordnung eine *Funktion* und die Menge $\mathfrak{M}$ den *Definitionsbereich* der Funktion. Die Menge $\mathfrak{N}$ aller Funktionswerte $\varphi(a)$ heißt der *Wertevorrat* der Funktion. Man nennt eine solche Zuordnung, bei welcher jedem Element von $\mathfrak{M}$ genau ein Element von $\mathfrak{N}$ zugeordnet wird und dabei alle Elemente von $\mathfrak{N}$ mindestens einmal benutzt werden, auch eine (eindeutige) *Abbildung* der Menge $\mathfrak{M}$ auf die Menge $\mathfrak{N}$. Das Element $\varphi(a)$ heißt dann das *Bild* von a, und a heißt ein *Urbild* von $\varphi(a)$. Das Bild $\varphi(a)$ ist durch a eindeutig bestimmt, aber nicht notwendig umgekehrt a durch $\varphi(a)$. Das Wort Abbildung wird im ganzen Buch nur für diese eindeutigen Abbildungen benutzt.

Tritt jedes Element von $\mathfrak{N}$ nur einmal als Bildelement auf, so heißt die Abbildung *umkehrbar eindeutig* oder *eineindeutig*. Es gibt dann eine „*inverse*" Abbildung, die jedem Element b von $\mathfrak{N}$ dasjenige Element von $\mathfrak{M}$ zuordnet, dessen Bild b ist.

Zwei Mengen, die sich eineindeutig aufeinander abbilden lassen, heißen *gleichmächtig*, in Zeichen:

$$\mathfrak{M} \sim \mathfrak{N}.$$

Von gleichmächtigen Mengen sagt man auch, daß sie „dieselbe Mächtigkeit" haben.

Beispiele. Ordnet man jeder natürlichen Zahl n die Zahl 0 oder 1 zu, je nachdem n gerade oder ungerade ist, so hat man eine Abbildung der Menge der natürlichen Zahlen auf die Menge $\{0, 1\}$. Die Abbildung ist nicht eineindeutig. Ordnet man jeder Zahl n die Zahl $2n$ zu, so hat man eine eineindeutige Abbildung der Menge aller natürlichen Zahlen auf die Menge aller geraden Zahlen. Die Menge der natürlichen Zahlen ist also mit der Menge aller geraden Zahlen gleichmächtig.

Aufgabe. Man beweise folgende drei Eigenschaften des Zeichens $\sim$:

1. $\mathfrak{A} \sim \mathfrak{A}$.
2. Aus $\mathfrak{A} \sim \mathfrak{B}$ folgt $\mathfrak{B} \sim \mathfrak{A}$.
3. Aus $\mathfrak{A} \sim \mathfrak{B}$ und $\mathfrak{B} \sim \mathfrak{C}$ folgt $\mathfrak{A} \sim \mathfrak{C}$.

Eine Menge kann sehr wohl einer echten Obermenge gleichmächtig sein. Das zeigt schon das zweite der obigen Beispiele, ebenso das folgende: Ordnet man jeder natürlichen Zahl n die Zahl $n-1$ zu, so wird die Menge der natürlichen Zahlen eineindeutig abgebildet auf eine Menge, die außer den natürlichen Zahlen auch die Null enthält. Im nächsten Paragraphen werden wir aber sehen, daß etwas Derartiges für „endliche" Mengen nicht eintreten kann.

§ 3. Die Zahlreihe.

Als bekannt wird vorausgesetzt die Menge der natürlichen Zahlen:

$$1, 2, 3, \ldots$$

sowie die folgenden Grundeigenschaften dieser Menge (*Axiome von* PEANO):

I. 1 ist eine natürliche Zahl.

II. Jede Zahl[1] a hat einen bestimmten Nachfolger a^+ in der Menge der natürlichen Zahlen.

III. Stets ist

$$a^+ \neq 1.$$

D. h. es gibt keine Zahl mit dem Nachfolger 1.

IV. Aus $a^+ = b^+$ folgt $a = b$.

D. h. zu jeder Zahl gibt es keine oder genau eine, deren Nachfolger jene Zahl ist.

V. „*Prinzip der vollständigen Induktion*": Jede Menge von natürlichen Zahlen, welche die Zahl 1 enthält und welche zu jeder Zahl a, die sie enthält, auch deren Nachfolger a^+ enthält, enthält alle natürlichen Zahlen.

Auf Eigenschaft V. beruht die Beweismethode der *vollständigen Induktion*. Wenn man eine Eigenschaft E für alle Zahlen nachweisen will, weist man sie zunächst für die Zahl 1 nach und dann für ein beliebiges n^+ unter der „Induktionsvoraussetzung", daß die Eigenschaft E für n gilt. Auf Grund von V. muß dann die Menge der Zahlen, welche die Eigenschaft E besitzen, alle Zahlen enthalten.

Mit dieser Beweismethode beweist man z. B. leicht, daß jede Zahl $\neq 1$ einen „Vorgänger" besitzt, dessen Nachfolger sie ist[2].

Summe zweier Zahlen. Auf genau eine Art läßt sich jedem Zahlenpaar x, y eine natürliche Zahl, $x + y$ genannt, so zuordnen, daß

(1) $\quad x + 1 = x^+ \quad$ für jedes x,

(2) $\quad x + y^+ = (x + y)^+ \quad$ für jedes x und jedes y.

[1] „Zahl" heißt vorläufig immer: natürliche Zahl.

[2] Für den Beweis wie für die Beweise aller noch folgenden Sätze dieses Paragraphen verweisen wir den Leser auf das Büchlein von E. LANDAU: Grundlagen der Analysis. Leipzig 1930. Kap. 1.

Auf Grund dieser Definition können wir statt a^+ fortan auch $a+1$ schreiben. Es gelten die Rechnungsregeln:

(3) $(a+b)+c=a+(b+c)$ („Assoziatives Gesetz der Addition").

(4) $a+b=b+a$ („Kommutatives Gesetz der Addition").

(5) Aus $a+b=a+c$ folgt $b=c$.

Produkt zweier Zahlen. Auf genau eine Art läßt sich jedem Zahlenpaar x, y eine natürliche Zahl, $x \cdot y$ oder xy genannt, so zuordnen, daß

(6) $x \cdot 1 = x$,

(7) $x \cdot y^+ = x \cdot y + x$ für jedes x und jedes y.

Es gelten die Rechnungsregeln:

(8) $ab \cdot c = a \cdot bc$ („Assoziatives Gesetz der Multiplikation").

(9) $a \cdot b = b \cdot a$ („Kommutatives Gesetz der Multiplikation").

(10) $a \cdot (b+c) = a \cdot b + a \cdot c$ („Distributivgesetz").

(11) Aus $ab = ac$ folgt $b = c$.

Größer und kleiner. Ist $a = b + u$, so schreibt man $a > b$, oder auch $b < a$. Man beweist nun weiter:

(12) Für je zwei Zahlen a, b gilt eine und nur eine der Relationen

$$a < b, \quad a = b, \quad a > b.$$

(13) Aus $a < b$ und $b < c$ folgt $a < c$.

(14) Aus $a < b$ folgt $a + c < b + c$.

(15) Aus $a < b$ folgt $ac < bc$.

Die [nach (5) einzige] Lösung u der Gleichung $a = b + u$ im Fall $a > b$ wird mit $a - b$ bezeichnet. Für „$a < b$ oder $a = b$" schreibt man kurz $a \leqq b$. Entsprechend wird $a \geqq b$ erklärt.

Weiter gilt der wichtige Satz:

Jede nicht leere Menge von natürlichen Zahlen enthält eine kleinste Zahl, d. h. eine solche, die kleiner ist als alle anderen Zahlen der Menge.

Auf diesem Satz beruht eine *zweite Form der vollständigen Induktion.* Man will eine Eigenschaft E für alle Zahlen als gültig nachweisen, und beweist sie zu dem Zweck für eine jede beliebige Zahl n unter der „Induktionsvoraussetzung", daß sie für alle Zahlen $< n$ bereits gilt. (Insbesondere gilt die Eigenschaft dann für $n = 1$, da es keine Zahlen < 1 gibt, also die „Induktionsvoraussetzung" hier wegfällt[1].

[1] Eine Aussage „Alle A haben die Eigenschaft B" wird immer als richtig betrachtet, wenn es überhaupt keine A gibt. Ebenso wird die Aussage „Aus E folgt F" (wo E und F Eigenschaften sind, die gewissen Objekten x zukommen können oder nicht) als richtig betrachtet, wenn es keine x mit der Eigenschaft E

Der Induktionsbeweis muß natürlich so beschaffen sein, daß er den Fall $n = 1$ mit umfaßt, sonst ist er ungenügend.) Dann muß die Eigenschaft E allen Zahlen zukommen. Sonst wäre nämlich die Menge aller Zahlen, denen die Eigenschaft E nicht zukommt, nicht leer. Ihr kleinstes Element wäre eine Zahl n, welche die Eigenschaft E nicht besitzt, während alle Zahlen $< n$ die Eigenschaft E besitzen, was nicht geht.

Neben dem „Beweis durch vollständige Induktion" in seinen beiden Formen gibt es noch die „*Definition* (oder Konstruktion) *durch vollständige Induktion*". Man will jeder natürlichen Zahl x ein neues Objekt $\varphi(x)$ zuordnen, und man gibt ein System von „rekursiven Bestimmungsrelationen" vor, die den Funktionswert $\varphi(n)$ jeweils mit den vorangehenden Werten $\varphi(m)$ $(m < n)$ verknüpfen sollen. Angenommen wird, daß diese Relationen jeweils den Wert $\varphi(n)$ eindeutig bestimmen, sobald alle $\varphi(m)$ $(m < n)$ gegeben sind und untereinander die gegebenen Relationen erfüllen[1]. Der einfachste Fall ist der, daß für $m = n^+$ der Wert $\varphi(n^+)$ durch $\varphi(n)$ ausgedrückt wird, und daß für $m = 1$ der Wert $\varphi(1)$ direkt gegeben ist. Beispiele sind die Relationen (1), (2) bzw. (6), (7), durch welche oben die Summe und das Produkt definiert wurden. Nun wird behauptet: *Unter den angegebenen Voraussetzungen gibt es eine und nur eine Funktion $\varphi(x)$, deren Werte die gegebenen Relationen erfüllen.*

Beweis: Unter einem *Abschnitt* $(1, n)$ der Zahlreihe verstehen wir die Gesamtheit der Zahlen $\leqq n$. Wir behaupten nun zunächst: Auf jedem Abschnitt $(1, n)$ gibt es eine und nur eine Funktion $\varphi_n(x)$, definiert für die Zahlen x dieses Abschnittes, die die gegebenen Relationen erfüllt. Diese Behauptung gilt nämlich für den Abschnitt $(1, 1)$, sowie für jeden Abschnitt $(1, n^+)$, sobald sie für $(1, n)$ gilt. Denn kraft der rekursiven Relationen ist der Funktionswert $\varphi(1)$ und durch die vorangehenden Werte $\varphi(m) = \varphi_n(m)$ $(m \leqq n)$ der Funktionswert $\varphi(n^+)$ eindeutig bestimmt. Also gilt die Behauptung für jeden Abschnitt $(1, n)$. So erhalten wir eine Reihe von Funktionen $\varphi_n(x)$. Jede Funktion $\varphi_n(x)$ ist definiert auf $(1, n)$, also zugleich auf jedem kleineren Abschnitt $(1, m)$; dort erfüllt sie aber auch die Bedingungsrelationen und stimmt somit dort mit der Funktion $\varphi_m(x)$ überein. Also stimmen je zwei Funktionen $\varphi_n(x)$, $\varphi_m(x)$ für alle Werte x, für die beide definiert sind, überein.

---

gibt. Das ist alles in Übereinstimmung mit der schon früher gemachten Bemerkung, daß die leere Menge in jeder Menge enthalten ist.

Die Zweckmäßigkeit dieses in der Umgangssprache vielleicht nicht so üblichen Wortgebrauchs ist z. B. daraus ersichtlich, daß nur so die Aussage „Aus E folgt F" sich ausnahmslos in „Aus nicht-F folgt nicht-E" verwandeln läßt. — Die Negation von „Aus E folgt (stets) F" heißt: Es gibt ein x, für welches E richtig und F falsch ist.

[1] Diese Annahme schließt in sich, daß $\varphi(1)$ durch die Relationen *allein* bestimmt wird; denn es gibt keine Zahlen mehr, die der 1 vorangehen.

Die gesuchte Funktion $\varphi(x)$ muß nun auf *allen* Abschnitten $(1, n)$ definiert sein und die Bedingungsrelationen erfüllen, also jeweils mit der Funktion φ_n übereinstimmen. Eine solche Funktion φ gibt es, aber auch nur eine: ihr Wert $\varphi(x)$ ist der gemeinsame Wert aller $\varphi_n(x)$, die für die Zahl x definiert sind. Damit ist der Satz bewiesen.

Wir werden von der „Konstruktion durch vollständige Induktion" sehr oft Gebrauch machen.

Aufgabe. 1. Eine Eigenschaft E gelte erstens für $n = 3$ und zweitens, wenn sie für $n \geqq 3$ gilt, auch für $n + 1$. Zu beweisen ist, daß E für alle Zahlen $\geqq 3$ gilt.

Durch Hinzunahme der Symbole $-a$ (negative ganze Zahlen) und 0 (Null) kann man die Zahlenreihe ergänzen zum Bereich der *ganzen Zahlen*. Um die Erklärung der Zeichen $+$, $\cdot$, $<$ in diesem Bereich bequemer zu gestalten, ist es zweckmäßig, die ganzen Zahlen durch Paare von natürlichen Zahlen (a, b) zu repräsentieren, und zwar repräsentiert man:

die natürliche Zahl a durch $(a + b, b)$,
die Null durch (b, b),
die negative Zahl $-a$ durch $(b, a + b)$,

wo jedesmal b eine beliebige natürliche Zahl ist.

Jede Zahl kann durch mehrere Symbole (a, b) repräsentiert werden; aber jedes Symbol (a, b) definiert eine und nur eine ganze Zahl, nämlich:

die natürliche Zahl $a - b$, falls $a > b$,
die Zahl 0, falls $a = b$,
die negative Zahl $-(b - a)$, falls $a < b$.

Man definiert nun:

$$(a, b) + (c, d) = (a + c,\ b + d),$$

$$(a, b) \cdot (c, d) = (ac + bd,\ ad + bc),$$

$$(a, b) < (c, d) \quad \text{oder} \quad (c, d) > (a, b), \quad \text{falls} \quad a + d < b + c,$$

und verifiziert mühelos: *erstens*, daß die Definitionen unabhängig sind von der Wahl der Symbole linker Hand, falls nur die durch diese Symbole dargestellten Zahlen dieselben bleiben; *zweitens*, daß die Rechengesetze (3), (4), (5), (8), (9), (10), (12), (13), (14) sowie (15) für $c > 0$ erfüllt sind; *drittens*, daß die Lösung der Gleichung $a + x = b$ im erweiterten Bereich unbeschränkt und eindeutig möglich ist (die Lösung wird wieder mit $b - a$ bezeichnet); *viertens*, daß $ab = 0$ dann und nur dann gilt, wenn $a = 0$ oder $b = 0$ ist[1].

Aufgaben. 2. Man führe die Beweise durch.

3. Dasselbe wie Aufg. 1 mit Ersetzung der Zahl 3 durch 0.

[1] Für eine etwas andere Einführung der negativen Zahlen und der Null siehe E. LANDAU: Grundlagen der Analysis, Kap. 4.

Von den elementaren Eigenschaften der ganzen Zahlen sind hier nur diejenigen erwähnt, die für das Folgende eine wichtige Rolle spielen. Für die Definition der Brüche, sowie für die Teilbarkeitseigenschaften der ganzen Zahlen siehe Kap. 3.

§ 4. Endliche und abzählbare Mengen.

Eine Menge, die mit einem Abschnitt der Zahlreihe (also mit der Menge der natürlichen Zahlen $\leqq n$) gleichmächtig ist, heißt *endlich*. Die leere Menge heißt auch endlich[1].

Einfacher ausgedrückt: Eine Menge heißt endlich, wenn ihre Elemente sich mit Nummern von 1 bis n versehen lassen, so daß verschiedene Elemente verschiedene Nummern erhalten und alle Nummern von 1 bis n benutzt werden. Die Elemente einer endlichen Menge $\mathfrak{A}$ kann man demnach mit $a_1, \ldots, a_n$ bezeichnen:

$$\mathfrak{A} = \{a_1, \ldots, a_n\}.$$

Aufgabe. 1. Man beweise durch vollständige Induktion nach n, daß jede Untermenge einer endlichen Menge $\mathfrak{A} = \{a_1, \ldots, a_n\}$ wieder endlich ist.

Jede Menge, die nicht endlich ist, heißt *unendlich*. Zum Beispiel ist die Menge aller ganzen Zahlen unendlich, wie wir gleich beweisen werden.

Der *Hauptsatz über endliche Mengen* (auch „Hauptsatz der Arithmetik" genannt) lautet so:

Eine endliche Menge kann nicht einer echten Obermenge gleichmächtig sein.

Beweis: Gesetzt, es wäre eine Abbildung einer endlichen Menge $\mathfrak{A}$ auf eine echte Obermenge $\mathfrak{O}$ gegeben. Die Elemente der Menge $\mathfrak{A}$ seien $a_1, \ldots, a_n$. Die Bildelemente seien $\varphi(a_1), \ldots, \varphi(a_n)$; unter ihnen kommen $a_1, \ldots, a_n$ wieder vor, außerdem aber mindestens noch ein weiteres Element, das wir a_{n+1} nennen.

Für $n = 1$ ist die Absurdität klar: ein einziges Element a_1 kann nicht die voneinander verschiedenen Bildelemente a_1, a_2 haben.

Die Unmöglichkeit einer Abbildung φ mit den obigen Eigenschaften sei also für den Wert $n - 1$ bewiesen; sie soll für den Wert n bewiesen werden.

Wir können annehmen, es sei $\varphi(a_n) = a_{n+1}$; denn wenn das nicht der Fall ist, also wenn etwa

$$\varphi(a_n) = a' \qquad (a' \neq a_{n+1})$$

[1] Für andere Definitionen des Begriffs der endlichen Menge, vgl. A. TARSKI: Sur les ensembles finis, Fund. Math. 6 (1925).

ist, so hat a_{n+1} ein anderes Urbild a_i:

$$\varphi(a_i) = a_{n+1},$$

und man kann statt der Abbildung φ eine andere konstruieren, die dem a_n das a_{n+1}, dem a_i das a' zuordnet und im übrigen mit φ übereinstimmt.

Jetzt wird die Untermenge $\mathfrak{A}' = \{a_1, \ldots, a_{n-1}\}$ durch die Funktion φ abgebildet auf eine Menge $\varphi(\mathfrak{A}')$, die aus $\varphi(\mathfrak{A}) = \mathfrak{D}$ entsteht durch Weglassung des Elements $\varphi(a_n) = a_{n+1}$.

$\varphi(\mathfrak{A}')$ enthält somit $a_1, \ldots, a_n$, ist also eine echte Obermenge von $\mathfrak{A}'$ und eindeutiges Bild von $\mathfrak{A}'$. Das ist nach der Induktionsvoraussetzung unmöglich.

Aus diesem Satz folgt zunächst, daß eine Menge niemals mit zwei verschiedenen Abschnitten der Zahlreihe gleichmächtig sein kann; denn dann wären diese untereinander gleichmächtig, während doch notwendig der eine der beiden eine echte Obermenge des anderen ist. Eine endliche Menge $\mathfrak{A}$ ist also einem und nur einem Abschnitt $(1, n)$ der Zahlreihe gleichmächtig. Die somit eindeutig bestimmte Zahl n heißt die *Anzahl der Elemente* der Menge $\mathfrak{A}$ und kann als Maß für die Mächtigkeit dienen.

Zweitens folgt, daß ein Abschnitt der Zahlreihe niemals der ganzen Zahlreihe gleichmächtig sein kann. Die Reihe der natürlichen Zahlen ist also unendlich. Man nennt jede Menge, die der Reihe der natürlichen Zahlen gleichmächtig ist, *abzählbar unendlich*. Die Elemente einer abzählbar unendlichen Menge lassen sich demnach so mit Nummern versehen, daß jede natürliche Zahl genau einmal als Nummer benutzt wird.

Endliche und abzählbar unendliche Mengen heißen beide *abzählbar*.

Aufgaben. 2. Man beweise, daß die Anzahl der Elemente einer Vereinigung von zwei fremden endlichen Mengen gleich der Summe der Anzahlen für die einzelnen Mengen ist. [Vollständige Induktion mit Hilfe der Rekursionsformeln (1), (2) § 3.]

3. Man beweise, daß die Anzahl der Elemente einer Vereinigung von r paarweise fremden Mengen von je s Elementen gleich rs ist. [Vollständige Induktion mit Hilfe der Rekursionsformeln (6), (7) § 3.]

4. Man beweise, daß jede Untermenge der Zahlenreihe abzählbar ist.

Daraus abzuleiten: Eine Menge ist dann und nur dann abzählbar, wenn man ihre Elemente so mit Nummern versehen kann, daß verschiedene Elemente verschiedene Nummern erhalten.

Beispiel einer nicht-abzählbaren Menge. Die Menge aller abzählbar unendlichen Folgen von natürlichen Zahlen ist nicht abzählbar. Daß sie nicht endlich ist, ist leicht einzusehen. Wäre sie abzählbar unendlich, so hätte jede Folge eine Nummer, und zu jeder

Nummer i gehörte eine Folge, die wir etwa mit

$$a_{i1}, a_{i2}, \ldots$$

bezeichnen. Man konstruiere nun die Zahlfolge

$$a_{11} + 1, \quad a_{22} + 1, \ldots$$

Diese müßte auch eine Nummer haben, etwa die Nummer j. Demnach wäre

$$a_{j1} = a_{11} + 1; \quad a_{j2} = a_{22} + 1; \text{ usw.}$$

insbesondere

$$a_{jj} = a_{jj} + 1,$$

was einen Widerspruch ergibt.

Aufgaben. 5. Man beweise, daß die Menge der ganzen Zahlen (positiven und negativen und Null) abzählbar unendlich ist. Ebenso, daß die Menge der geraden Zahlen abzählbar unendlich ist.

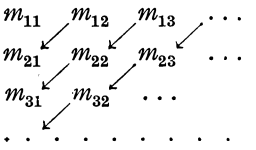
6. Man beweise, daß die Menge aller reellen Zahlen (d. h. aller unendlichen Dezimalbrüche) nicht abzählbar ist. [Die Schlußweise ist analog der im obigen Beispiel befolgten.]

7. Man beweise, daß die Mächtigkeit einer abzählbar unendlichen Menge sich nicht ändert, wenn man endlichviele oder abzählbar unendlichviele neue Elemente hinzufügt.

Die Vereinigung von abzählbar vielen abzählbaren Mengen ist wieder abzählbar.

Beweis: Die Mengen seien $\mathfrak{M}_1, \mathfrak{M}_2, \ldots$; die Elemente von $\mathfrak{M}_i$ seien $m_{i1}, m_{i2}, \ldots$.

Es gibt nur endlichviele Elemente m_{ik} mit $i + k = 2$, ebenso nur endlichviele mit $i + k = 3$, usw. Numeriert man nun erst die Elemente durch, für die $i + k = 2$ ist (etwa nach steigenden Werten von i), sodann (mit Zählen fortfahrend) die mit $i + k = 3$ usw., so bekommt schließlich jedes Element m_{ik} eine Nummer, und verschiedene bekommen verschiedene Nummern. Daraus folgt die Behauptung.



Die nebenstehende Figur erläutert die Abzählungsweise.

Aufgabe. 8. Man beweise, daß die Menge aller unkürzbaren Brüche $\frac{\pm a}{b}$ (a, b teilerfremde, natürliche Zahlen) abzählbar unendlich ist.

§ 5. Klasseneinteilungen.

Das Gleichheitszeichen genügt den folgenden Regeln:

$$a = a.$$

Aus $a = b$ folgt $b = a$.

Aus $a = b$ und $b = c$ folgt $a = c$.

Man sagt statt dessen auch: Die Relation $a = b$ ist *reflexiv, symmetrisch* und *transitiv*. Wenn nun zwischen den Elementen irgend einer Menge eine Beziehung $a \sim b$ definiert ist (so daß also für jedes Elementepaar a, b feststeht, ob $a \sim b$ ist oder nicht) und wenn diese den gleichen Axiomen genügt:

1. $a \sim a$;
2. aus $a \sim b$ folgt $b \sim a$;
3. aus $a \sim b$ und $b \sim c$ folgt $a \sim c$,

so nennt man die Relation $a \sim b$ eine *Äquivalenzrelation*. Zum Beispiel genügt die in § 2 für Mengen $\mathfrak{M}$, $\mathfrak{N}$, ... definierte Relation $\mathfrak{M} \sim \mathfrak{N}$ ($\mathfrak{M}$ gleichmächtig mit $\mathfrak{N}$) diesen Axiomen. Auch die Kongruenzrelation für Dreiecke ist eine solche Relation. Ein drittes Beispiel: Im Bereich der ganzen Zahlen nenne man zwei Zahlen äquivalent, wenn ihre Differenz durch 2 teilbar ist. Die Axiome sind offensichtlich erfüllt.

Ist nun irgend eine Äquivalenzrelation gegeben, so können wir alle die Elemente, die irgend einem Element a äquivalent sind, in eine *Klasse* $\mathfrak{K}_a$ vereinigen. Alle Elemente einer Klasse sind dann untereinander äquivalent, denn aus $a \sim b$ und $a \sim c$ folgt nach 2. und 3. $b \sim c$, und alle einem Klassenelement äquivalenten Elemente liegen in derselben Klasse, denn aus $a \sim b$ und $b \sim c$ folgt $a \sim c$. Die Klasse ist mithin gegeben durch jedes ihrer Elemente: Wenn wir statt von a von irgend einem Element b derselben Klasse ausgehen, kommen wir zur selben Klasse: $\mathfrak{K}_b = \mathfrak{K}_a$. Wir können demnach jedes b als *Repräsentanten* der Klasse wählen.

Gehen wir aber von einem Element b aus, das nicht derselben Klasse angehört (also nicht mit a äquivalent ist), so können $\mathfrak{K}_a$ und $\mathfrak{K}_b$ kein Element gemein haben; denn aus $c \sim a$ und $c \sim b$ würde ja folgen $a \sim b$, also $b \in \mathfrak{K}_a$. Die Klassen $\mathfrak{K}_a$ und $\mathfrak{K}_b$ sind also in diesem Fall fremd.

Die Klassen überdecken die gegebene Menge ganz, da jedes Element a in einer Klasse, nämlich in $\mathfrak{K}_a$ liegt. Die Menge ist also *eingeteilt in lauter zueinander fremde Klassen*. In unserem letzten Beispiel sind dies die Klasse der geraden und die der ungeraden Zahlen.

Wie wir sahen, ist $\mathfrak{K}_a = \mathfrak{K}_b$ dann und nur dann, wenn $a \sim b$ ist. Durch Einführung der Klassen statt der Elemente können wir also die Äquivalenzrelation $a \sim b$ durch eine Gleichheitsrelation $\mathfrak{K}_a = \mathfrak{K}_b$ ersetzen.

Ist umgekehrt eine Klasseneinteilung einer Menge $\mathfrak{M}$ in lauter zueinander fremde Klassen gegeben, so können wir definieren: $a \sim b$, wenn a und b derselben Klasse angehören. Die Relation $a \sim b$ genügt dann offensichtlich den Axiomen 1, 2, 3.

Zweites Kapitel.

Gruppen.

Inhalt: Erklärung der für das ganze Buch grundlegenden gruppentheoretischen Grundbegriffe: Gruppe, Untergruppe, Isomorphie, Homomorphie, Normalteiler, Faktorgruppe.

§ 6. Der Gruppenbegriff.

Definition. Eine nicht leere Menge $\mathfrak{G}$ von Elementen irgendwelcher Art (z. B. von Zahlen, von Abbildungen, von Transformationen) heißt eine *Gruppe*, wenn folgende vier Bedingungen erfüllt sind:

1. Es ist eine *Zusammensetzungsvorschrift* gegeben, welche jedem Elementepaar a, b von $\mathfrak{G}$ ein drittes Element derselben Menge zuordnet, welches meistens das *Produkt* von a und b genannt und mit ab oder $a \cdot b$ bezeichnet wird. (Das Produkt kann von der Reihenfolge der Faktoren abhängen: es braucht nicht $ab = ba$ zu sein.)

2. Das *Assoziativgesetz*: Für je drei Elemente a, b, c von $\mathfrak{G}$ gilt:

$$ab \cdot c = a \cdot bc .$$

3. Es existiert (mindestens) ein (linksseitiges) *Einselement* e in $\mathfrak{G}$ mit der Eigenschaft:

$$ea = a \text{ für alle } a \text{ von } \mathfrak{G} .$$

4. Zu jedem a von $\mathfrak{G}$ existiert (mindestens) ein (linksseitiges) *Inverses* a^{-1} in $\mathfrak{G}$, mit der Eigenschaft

$$a^{-1}a = e .$$

Eine Gruppe heißt *Abelsch*, wenn außerdem stets $ab = ba$ ist (*kommutatives Gesetz*).

Beispiele. Wenn die Elemente der Menge Zahlen sind und die Zusammensetzung die gewöhnliche Multiplikation, so muß man die Null, die ja keine Inverse hat, zunächst ausschließen. Alle rationalen Zahlen $\neq 0$ bilden nun eine Gruppe (das Einselement ist die Zahl 1); ebenso die Zahlen 1 und -1 oder die Zahl 1 allein.

Beim Gruppenbegriff kommt es aber auf die Bezeichnung nicht an: die zugrunde gelegte Zusammensetzungsvorschrift kann auch die Addition von Zahlen sein, wenn nur alle Regeln 1. bis 4. erfüllt sind. Man muß dann nur die Benennung des aus a und b zusammengesetzten Elementes als ein „Produkt" fallen lassen und statt „Produkt $a \cdot b$" in den Rechnungsregeln überall „Summe $a + b$" lesen. Das Einselement wird in diesem Fall die Zahl 0, denn es ist $0 + a = a$ für alle Zahlen a. Ebenso ist das inverse Element zu a die Zahl $-a$, denn es ist $-a + a = 0$. Das Assoziativgesetz für die Addition:

$$a + (b + c) = (a + b) + c$$

ist für Zahlen stets erfüllt. Eine Menge von Zahlen ist also dann eine Gruppe bei der Addition, wenn sie zu je zwei Zahlen a und b auch deren Summe enthält, außerdem die Null und zu jeder Zahl a auch die entgegengesetzte Zahl $-a$. Solche Zahlenmengen nennt man auch *Zahlenmoduln*. Zum Beispiel bilden alle rationalen Zahlen einen Modul, ebenso alle ganzen Zahlen, alle geraden Zahlen, schließlich die Zahl 0 für sich allein.

Ein Beispiel einer Gruppe, deren Elemente nicht Zahlen sind, bildet die Gesamtheit der Drehungen der Ebene oder des Raumes um einen festen Punkt. Zwei Drehungen A, B werden zusammengesetzt, indem man sie nacheinander ausführt. Führt man zuerst B, dann A aus, so kann dasselbe Resultat (d. h. dieselbe Endlage aller Punkte des Raumes) auch durch eine einzelne Drehung erreicht werden, die dann mit $A \cdot B$ oder AB bezeichnet wird. Eine genauere algebraische Festlegung der Drehungen und ihrer Zusammensetzung werden wir später geben (Band II); hier soll die Gruppe der Drehungen im Raum nur unter Berufung auf die geometrische Anschauung angeführt werden als ein erstes Beispiel einer Gruppe, deren Elemente nicht Zahlen sind. Zugleich bildet die räumliche Drehungsgruppe ein erstes Beispiel einer nichtabelschen Gruppe, denn es ist, wie man geometrisch sehr leicht sieht, durchaus nicht gleichgültig, ob man zuerst die Drehung A und dann B ausführt oder zuerst B und dann A. Daß das Assoziativgesetz erfüllt ist, wird sich als Spezialfall des Assoziativgesetzes für beliebige Transformationen nachher ergeben. Das Einselement der Drehungsgruppe ist die Drehung um einen Winkel 0, die jeden Punkt fest läßt. Die inverse Drehung einer gegebenen ist die entgegengesetzte Drehung, die die erste rückgängig macht.

Die Drehungsgruppe ist ein Spezialfall des allgemeineren Begriffs einer *Transformationsgruppe*. Unter einer *Transformation* oder *Permutation* einer Menge $\mathfrak{M}$ verstehen wir eine eineindeutige Abbildung der Menge $\mathfrak{M}$ auf sich, d. h. eine Zuordnung s, bei der jedem Element a von $\mathfrak{M}$ ein Bild $s(a)$ entspricht und jedes Element von $\mathfrak{M}$ das Bild genau eines a ist. Für $s(a)$ schreibt man auch sa. Die Elemente von $\mathfrak{M}$ sind die *Objekte* der Transformation s. Das Wort Transformationen wird meist bei unendlichen, das Wort Permutationen meist bei endlichen Mengen gebraucht.

Ist die Menge $\mathfrak{M}$ endlich und sind ihre Elemente mit Nummern $1, 2, \ldots, n$ versehen, so kann man jede Permutation vollständig beschreiben durch ein Schema, in dem unter jede Nummer k die Nummer $s(k)$ des Bildelementes geschrieben wird. Z. B. ist

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

diejenige Permutation der Ziffern 1, 2, 3, 4, die 1 in 2, 2 in 4, 3 in 3 und 4 in 1 überführt.

Unter dem *Produkt* st zweier Transformationen s, t wird verstanden diejenige Transformation, die entsteht, wenn man zuerst die Transformation t und dann auf die Bildelemente die Transformation s ausübt[1], d. h.:

$$st(a) = s(t(a)).$$

Z. B. ist für $s = \binom{1234}{2431}$, $t = \binom{1234}{2143}$ das Produkt $st = \binom{1234}{4213}$. Ebenso ist $ts = \binom{1234}{1342}$.

Das assoziative Gesetz:

$$(rs)t = r(st)$$

kann für Transformationen allgemein so bewiesen werden: Wendet man beide Seiten an auf ein beliebiges Objekt a, so kommt:

$$(rs)t(a) = (rs)(t(a)) = r(s(t(a)))$$
$$r(st)(a) = r(st(a)) \quad = r(s(t(a))),$$

also beide Male dasselbe.

Die *Identität* oder *identische Transformation* ist diejenige Abbildung E, die jedes Objekt auf sich selbst abbildet:

$$E(a) = a.$$

Die identische Transformation hat offenbar die charakteristische Eigenschaft eines Einselementes einer Gruppe: es gilt $Es = s$ für jede Transformation s.

Die *inverse Transformation* einer Transformation s ist diejenige Abbildung, die $s(a)$ auf a abbildet, mithin s wieder rückgängig macht. Bezeichnet man sie mit s^{-1}, so gilt demnach für jedes Objekt a:

$$s^{-1}s(a) = a$$

mithin auch

$$s^{-1}s = E.$$

Aus dem Bewiesenen folgt, daß alle Postulate 1. bis 4. für die Gesamtheit der Permutationen einer Menge $\mathfrak{M}$ erfüllt sind. Demnach bilden alle diese Permutationen eine Gruppe. Bei einer endlichen Menge $\mathfrak{M}$, von n Elementen, heißt die Gruppe ihrer Permutationen auch die *symmetrische Gruppe* $\mathfrak{S}_n$.[2]

Weiter folgt aber, daß jede Menge $\mathfrak{G}$ von Transformationen einer Menge $\mathfrak{M}$ eine Gruppe ist, sobald sie nur: a) zu je zwei Transformationen

[1] Die Reihenfolge ist Sache der Verabredung. Häufig macht man es gerade umgekehrt; st heißt dann: erst s, dann t. Zweckmäßig schreibt man dann die Transformationen rechts von den Objekten: as statt $s(a)$.

[2] Der Name ist so gewählt, weil die Funktionen von $x_1, \ldots, x_n$, die bei allen Permutationen der Gruppe invariant bleiben, die „symmetrischen Funktionen" sind.

auch deren Produkt enthält; b) zu jeder Transformation auch die inverse Transformation enthält; c) die Identität enthält. Ist die Menge nicht leer, so ist sogar die Forderung c) noch überflüssig, denn wenn s eine beliebige Transformation aus $\mathfrak{G}$ ist, so gehört nach b) auch s^{-1} und daher nach a) auch $s^{-1}s = E$ der Menge $\mathfrak{G}$ an.

Wir kehren nun zur allgemeinen Theorie der Gruppen zurück.

Für $ab \cdot c$ oder $a \cdot bc$ schreibt man kurz abc.

Aus 3. und 4. folgt:

$$a^{-1}aa^{-1} = ea^{-1} = a^{-1},$$

also, wenn man von links mit einem inversen Element von a^{-1} multipliziert:

$$eaa^{-1} = e$$

oder

$$aa^{-1} = e;$$

also ist jedes linksseitige inverse Element zugleich ein rechtsseitiges Inverses. Zugleich sieht man, daß ein Inverses von a^{-1} wieder a ist. Weiter folgt:

$$ae = aa^{-1}a = ea = a;$$

also ist das linksseitige Einselement zugleich rechtsseitiges.

Nunmehr folgt auch die *Möglichkeit der* (beiderseitigen) *Division*:

5. *Die Gleichung* $ax = b$ *besitzt eine Lösung in* $\mathfrak{G}$ *und ebenso die Gleichung* $ya = b$, *wo* a *und* b *beliebige Elemente von* $\mathfrak{G}$ *sind.*

Diese Lösungen sind nämlich $x = a^{-1}b$ und $y = ba^{-1}$, weil ja

$$a(a^{-1}b) = (aa^{-1})b = eb = b,$$

$$(ba^{-1})a = b(a^{-1}a) = be = b$$

ist.

Ebenso leicht beweist man die *Eindeutigkeit der Division*:

6. *Aus* $ax = ax'$ *und ebenso aus* $xa = x'a$ *folgt* $x = x'$.

Denn aus $ax = ax'$ folgt, indem man beide Seiten von links mit a^{-1} multipliziert, $x = x'$. Genau so beweist man den zweiten Teil der Behauptung.

Insbesondere folgt daraus die Eindeutigkeit des Einselements (als Lösung der Gleichung $xa = a$) und die Eindeutigkeit des Inversen (als Lösung der Gleichung $xa = e$). Das (einzige) Einselement wird oft mit 1 bezeichnet.

Die Möglichkeit der Division 5. ist ein Postulat, das imstande ist, die Postulate 3. und 4. zu ersetzen. Setzen wir nämlich 1., 2. und 5. voraus und suchen zunächst 3. zu beweisen. Wir wählen ein Element c aus und verstehen unter e eine Lösung der Gleichung $xc = c$. Dann ist also

$$ec = c.$$

Für beliebiges a lösen wir nun die Gleichung

$$cx = a.$$

Dann ist

$$ea = ecx = cx = a\,,$$

womit 3. bewiesen ist. 4. ist aber eine unmittelbare Folge der Lösbarkeit von $xa = e$.

Demnach können wir immer 1., 2., 5. als gleichwertige Gruppenpostulate statt 1., 2., 3., 4. benutzen.

Ist $\mathfrak{G}$ eine endliche Menge, so kann 5. auch durch 6. ersetzt werden. Man braucht also nicht die Möglichkeit der Division, sondern nur (außer den Postulaten 1. und 2.) die Eindeutigkeit derselben vorauszusetzen.

Beweis: Sei a irgend ein Element. Jedem Element x ordnen wir das Element ax zu. Diese Zuordnung ist nach 6. umkehrbar eindeutig; d. h. die Menge $\mathfrak{G}$ wird eineindeutig auf eine Untermenge, die Menge aller Produkte ax, abgebildet. Da aber $\mathfrak{G}$ nach Voraussetzung eine endliche Menge ist, so kann sie nicht auf eine echte Untermenge eineindeutig abgebildet werden. Also muß die Gesamtheit der Elemente ax mit $\mathfrak{G}$ identisch sein; d. h. jedes Element b ist in der Gestalt $b = ax$ zu schreiben, wie die erste Forderung 5. behauptet. Ebenso beweist man die Lösbarkeit von $b = xa$. Also folgt 5. aus 6.

Die Anzahl der Elemente einer endlichen Gruppe heißt die *Ordnung* der Gruppe.

Weitere Rechenregeln. Für das Inverse eines Produkts gilt die folgende Regel:

$$(ab)^{-1} = b^{-1}a^{-1}\,.$$

Denn es ist

$$(b^{-1}a^{-1})ab = b^{-1}(a^{-1}ab) = b^{-1}b = 1\,.$$

Bei *Abelschen Gruppen* ist es häufig zweckmäßig, die Verknüpfung *additiv zu schreiben*, d. h. $a + b$ statt $a \cdot b$ zu schreiben. Die Gruppe heißt dann eine *additive Gruppe* oder ein *Modul* (Verallgemeinerung der oben definierten Zahlenmoduln). Das Einselement bezeichnet man in diesem Fall mit 0, weil es, genau so wie die Null im Bereich der ganzen Zahlen, durch die Eigenschaft

$$0 + a = a$$

charakterisiert ist. Analog wird in einem Modul das inverse Element von a mit $-a$ bezeichnet.

Für $a + (-b)$ schreibt man kurz $a - b$, weil dieses Element die Lösung der Gleichung $x + b = a$ ist:

$$(a - b) + b = a + (-b + b) = a + 0 = a\,.$$

Aufgaben. 1. Die Euklidischen Bewegungen und Umlegungen des Raumes (d. h. diejenigen Transformationen, bei denen alle Entfernungen der Punktepaare ungeändert bleiben) bilden eine unendliche nichtabelsche Gruppe.

2. Man beweise, daß die Elemente e, a mit der Zusammensetzungsvorschrift

$$ee = e, \quad ea = a, \quad ae = a, \quad aa = e$$

eine (Abelsche) Gruppe bilden.

Bemerkung. Man kann die Zusammensetzung einer Gruppe darstellen durch eine „Gruppentafel", eine Tabelle mit doppeltem Eingang, in der zu je zwei Elementen das Produkt eingetragen wird. Zum Beispiel ist die Tafel für die obige Gruppe:

	e	a
e	e	a
a	a	e

3. Man stelle die Gruppentafel für die Gruppe der Permutationen von drei Ziffern auf.

Zusammengesetzte Produkte (Summen); Potenzen. In derselben Weise, wie wir für $ab \cdot c$ kurz abc geschrieben haben, wollen wir nun auch die *zusammengesetzten Produkte* von mehreren Faktoren:

$$\prod_{\nu=1}^{n} a_\nu = \prod_{1}^{n} a_\nu = a_1 a_2 \cdots a_n$$

definieren. Sind $a_1, \ldots, a_N$ gegeben, so definieren wir rekursiv (für $n < N$):

$$\begin{cases} \prod_{1}^{1} a_\nu = a_1, \\ \prod_{1}^{n+1} a_\nu = \left(\prod_{1}^{n} a_\nu\right) \cdot a_{n+1}.^1 \end{cases}$$

Insbesondere ist $\prod_{1}^{3} a_\nu$ unser altes $a_1 a_2 a_3$, ebenso $\prod_{1}^{4} = a_1 a_2 a_3 a_4 = (a_1 a_2 a_3) a_4$, usw.

Wir beweisen nun, allein mit Hilfe des Assoziativgesetzes, die Regel:

$$\prod_{\mu=1}^{m} a_\mu \cdot \prod_{\nu=1}^{n} a_{m+\nu} = \prod_{\nu=1}^{m+n} a_\nu \tag{1}$$

in Worten: *Das Produkt zweier zusammengesetzten Produkte ist gleich dem zusammengesetzten Produkt aller ihrer Faktoren in derselben Reihenfolge.* Z. B. ist:

$$(ab)(cd) = abcd$$

ein Spezialfall von (1).

---

[1] Das Symbol ν, das den variablen Index angibt, darf natürlich durch jedes andere Symbol ersetzt werden, ohne daß die Bedeutung des Produktes sich ändert.

Die Formel (1) ist klar für $n = 1$ (nach Definition des $\prod$-Zeichens). Ist sie für einen Wert n schon bewiesen, so ist für den nächsthöheren Wert $n + 1$:

$$\prod_1^m a_\mu \cdot \prod_1^{n+1} a_{m+\nu} = \prod_1^m a_\mu \left(\prod_1^n a_{m+\nu} \cdot a_{m+n+1}\right)$$

$$= \left(\prod_1^m a_\mu \cdot \prod_1^n a_{m+\nu}\right) a_{m+n+1}$$

$$= \left(\prod_1^{m+n} a_\mu\right) a_{m+n+1} = \prod_1^{m+n+1} a_\nu .$$

Damit ist (1) bewiesen.

Bemerkung. Für $\prod_1^n a_{m+\nu}$ schreibt man auch $\prod_{m+1}^{m+n} a_\nu$. Auch setzt man gelegentlich, wenn es bequem ist, $\prod_1^0 a_\nu = 1$.

Ein Produkt von n gleichen Faktoren heißt eine *Potenz*:

$$a^n = \prod_1^n a \qquad \text{(insbesondere } a^1 = a,\ a^2 = aa, \text{ usw.)}.$$

Aus dem bewiesenen Satz folgt:

$$a^n \cdot a^m = a^{n+m}. \tag{2}$$

Weiter gilt:

$$(a^m)^n = a^{mn}. \tag{3}$$

Der Beweis (durch vollständige Induktion) möge dem Leser überlassen bleiben.

Die bis jetzt bewiesenen Regeln (1), (2), (3) erforderten zu ihrem Beweis nur das Assoziativgesetz und werden daher im folgenden auf alle Arten von Bereichen angewandt, in denen Produkte definiert sind und das Assoziativgesetz gilt (wie z. B. im Bereich der natürlichen Zahlen), auch dann, wenn diese Bereiche keine Gruppen sind.

Ist die Multiplikation außerdem kommutativ (Abelsche Gruppen), so kann man weitergehend beweisen, daß der Wert eines zusammengesetzten Produktes von der Reihenfolge der Faktoren unabhängig ist, genauer: *Ist φ eine eineindeutige Abbildung des Abschnittes $(1, n)$ der Zahlenreihe auf sich, so ist*:

$$\prod_{\nu=1}^n a_{\varphi(\nu)} = \prod_1^n a_\nu .$$

Beweis. Für $n = 1$ ist die Behauptung klar; sie werde also für $n - 1$ als richtig vorausgesetzt. Es gibt ein k, das auf n abgebildet

wird: $\varphi(k) = n$. Dann ist

$$\prod_1^n a_{\varphi(\nu)} = \prod_1^{k-1} a_{\varphi(\nu)} \cdot a_{\varphi(k)} \cdot \prod_1^{n-k} a_{\varphi(k+\nu)} = \prod_1^{k-1} a_{\varphi(\nu)} \cdot \prod_1^{n-k} a_{\varphi(k+\nu)} \cdot a_{\varphi(k)}.^1$$

Definiert man nun eine Abbildung ψ des Abschnittes $(1, n-1)$ auf sich durch

$$\psi(\nu) = \varphi(\nu) \qquad (\nu < k)$$
$$\psi(\nu) = \varphi(\nu + 1) \qquad (\nu \geqq k)$$

so erhält man:

$$\prod_1^n a_{\varphi(\nu)} = \prod_1^{k-1} a_{\psi(\nu)} \prod_1^{n-k} a_{\psi(k-1+\nu)} \cdot a_n = \prod_1^{n-1} a_{\psi(\nu)} \cdot a_n,$$

also nach der Induktionsvoraussetzung

$$= \prod_1^{n-1} a_\nu \cdot a_n = \prod_1^n a_\nu.$$

Aus der bewiesenen Regel folgt, daß man bei Abelschen Gruppen berechtigt ist zu einer Schreibweise wie z. B.:

$$\prod_{1 \leqq i < k \leqq n} a_{ik},$$

oder

$$\prod_{i<k} a_{ik} \qquad (i = 1, \ldots, n; k = 1, \ldots, n),$$

welche bedeutet, daß die Menge der Indexpaare i, k mit $1 \leqq i < k \leqq n$ irgendwie durchnumeriert werden soll (wie, ist gleichgültig) und dann das Produkt gebildet wird.

In beliebigen Gruppen kann man die nullte und die negativen Potenzen eines Elementes a wie üblich definieren durch

$$a^0 = 1,$$
$$a^{-n} = (a^{-1})^n,$$

und man weist mühelos nach, daß die Regeln (2), (3) nunmehr für beliebige ganzzahlige Exponenten gelten.

In einer additiven Gruppe schreibt man statt $\prod_1^n a_\nu$ natürlich $\sum_1^n a_\nu$, und statt a^n entsprechend $n \cdot a$. In der additiven Gruppe der ganzen Zahlen ist diese Definition mit der früheren des Produktes zweier ganzen Zahlen in Übereinstimmung. Alles für Produkte Bewiesene überträgt sich jetzt auf Summen.

Die Rechnungsregel (3) hat, additiv geschrieben, die Form eines Assoziativgesetzes:

$$n \cdot m\, a = n\, m \cdot a,$$

---

[1] Im Fall $k = 1$ fällt der erste Faktor weg, im Fall $k = n$ der zweite; das stört den Beweis aber nicht.

während (2) die Form eines „Distributivgesetzes" hat:

$$m\,a + n\,a = (m + n)\,a\,.$$

Zu diesen beiden tritt nun noch ein anderes Distributivgesetz:

$$m\,(a + b) = m\,a + m\,b$$

(multiplikativ: $(ab)^m = a^m b^m$), das aber nur in Abelschen Gruppen gilt. Man beweist es wieder für positive m durch Induktion:

Für $m = 1$ ist alles klar. Angenommen, es sei $m(a+b) = ma+mb$. Dann ist

$$\begin{aligned}(m + 1)\,(a + b) &= m\,(a + b) + (a + b)\\ &= m\,a + m\,b + a + b\\ &= (m\,a + a) + (m\,b + b)\\ &= (m + 1)\,a + (m + 1)\,b\,.\end{aligned}$$

Wie man sieht, wird beim Beweis die Vertauschbarkeit von mb und a benutzt. Für $m = 0$ ist die Behauptung ebenfalls klar, während man für negative m nur die Definition der negativen Potenzen anzuwenden hat, um auf positive m zurückzukommen.

Aufgaben. 5. Man beweise für Abelsche Gruppen:

$$\prod_{\nu=1}^{n}\prod_{\mu=1}^{m} a_{\mu\nu} = \prod_{\mu=1}^{m}\prod_{\nu=1}^{n} a_{\mu\nu}\,.$$

6. Ebenso

$$\prod_{\nu=1}^{n}\prod_{\mu=1}^{\nu} a_{\mu\nu} = \prod_{\mu=1}^{n}\prod_{\nu=\mu}^{n} a_{\mu\nu}\,.$$

7. Die Ordnung der symmetrischen Gruppe $\mathfrak{S}_n$ ist $n! = \prod_{1}^{n}\nu$. [Vollst. Induktion nach n.]

§ 7. Untergruppen.

Damit eine nichtleere Untermenge $\mathfrak{g}$ einer Gruppe $\mathfrak{G}$ mit der gleichen Zusammensetzungsvorschrift für die Elemente von $\mathfrak{g}$ wie für die von $\mathfrak{G}$ wieder eine Gruppe ist, ist notwendig und hinreichend, daß sie die Forderungen 1., 2., 3., 4. erfüllt. 1. besagt, daß, wenn a und b in $\mathfrak{g}$ liegen, auch ab in $\mathfrak{g}$ liegt. Die Forderung 2. ist für $\mathfrak{g}$ von selbst erfüllt, weil sie sogar für $\mathfrak{G}$ gilt. Die Forderungen 3. und 4. besagen, daß in $\mathfrak{g}$ das Einselement liegt und daß $\mathfrak{g}$ mit a auch das inverse Element a^{-1} enthält. Davon ist wieder die Forderung des Einselements überflüssig; denn wenn a irgend ein Element von $\mathfrak{g}$ ist, so liegt in $\mathfrak{g}$ auch a^{-1}, also auch das Produkt $a\,a^{-1} = e$. Damit ist bewiesen:

Notwendig und hinreichend, damit eine nichtleere Untermenge $\mathfrak{g}$ einer gegebenen Gruppe $\mathfrak{G}$ eine Untergruppe ist, sind die folgenden Bedingungen:

1. $\mathfrak{g}$ *enthält mit je zwei Elementen* a, b *auch das Produkt* ab;
2. $\mathfrak{g}$ *enthält zu jedem Element* a *auch das inverse Element* a^{-1}.

Ist insbesondere $\mathfrak{g}$ *endlich,* so ist die zweite dieser Forderungen sogar überflüssig; denn in diesem Fall können 3. und 4. durch 6. ersetzt werden, und die Forderung 6. gilt sicher für $\mathfrak{g}$, da sie sogar für $\mathfrak{G}$ gilt.

Allgemein kann man die Bedingungen 1. und 2. in einer einzigen zusammenfassen: $\mathfrak{g}$ soll mit a und b auch ab^{-1} enthalten. Denn dann enthält $\mathfrak{g}$ mit a auch $aa^{-1} = e$, weiter $ea^{-1} = a^{-1}$, daher mit a und b auch b^{-1} und $a(b^{-1})^{-1} = ab$.

Beispiele von Untergruppen:

Jede Gruppe hat als Untergruppe die Einheitsgruppe $\mathfrak{E}$, die nur aus dem Einselement besteht.

Die Gruppe der ganzen Zahlen (mit der Addition als Verknüpfung) hat u. a. die Menge der geraden Zahlen als Untergruppe.

Die wichtigste Untergruppe der symmetrischen Gruppe $\mathfrak{S}_n$ aller Permutationen von n Objekten ist die *alternierende Gruppe* $\mathfrak{A}_n$, die aus denjenigen Permutationen besteht, welche, auf die Variablen $x_1, \ldots, x_n$ angewandt, die Funktion

$$\Delta = \prod_{i<k} (x_i - x_k) \tag{1}$$

in sich überführen. Diese Permutationen heißen *gerade,* die übrigen *ungerade.* Letztere kehren das Vorzeichen der Funktion Δ um. Jede *Transposition* (= Permutation, die zwei Ziffern vertauscht) ist eine ungerade Permutation. Das Produkt zweier geraden oder zweier ungeraden Permutationen ist gerade; das Produkt aus einer geraden und einer ungeraden Permutation ist ungerade. Aus der ersten Eigenschaft folgt, daß $\mathfrak{A}_n$ eine Gruppe ist. Da eine feste Transposition bei Multiplikation mit einer geraden Permutation eine ungerade ergibt und umgekehrt, gibt es gleich viele gerade wie ungerade Permutationen, mithin von jeder Art $\frac{n!}{2}$. (Vgl. § 6, Aufg. 7).

Um die Untergruppen der symmetrischen Gruppe $\mathfrak{S}_n$ bequem hinschreiben zu können, bedient man sich der bekannten *Zykeldarstellung* der Permutationen: Mit $(pqrs)$ bezeichnen wir eine zyklische Vertauschung, die p in q, q in r, r in s und s in p überführt und alle übrigen Objekte festläßt. Man zeigt mit Leichtigkeit, daß jede Permutation eindeutig (bis auf die Reihenfolge) als Produkt von solchen zyklischen Permutationen oder „Zyklen"

$$(ikl\ldots)(pq\ldots)\ldots$$

darstellbar ist, wobei keine zwei Zykeln ein Element gemein haben. Die Faktoren dieses Produktes sind vertauschbar. Ein Zyklus aus einem Element, etwa (1), stellt die identische Permutation dar. Es ist natürlich

$$(1\ 2\ 5\ 4) = (2\ 5\ 4\ 1) \text{ usw.}$$

Mit diesen Bezeichnungen können wir die $3! = 6$ Permutationen der Gruppe $\mathfrak{S}_3$ so darstellen:

$$(1),\ (1\ 2),\ (1\ 3),\ (2\ 3),\ (1\ 2\ 3),\ (1\ 3\ 2).$$

Die Untergruppen sind leicht alle zu bestimmen. Sie sind (außer $\mathfrak{S}_3$ selbst):

$$\begin{cases} \mathfrak{A}_3\colon (1),\ (1\ 2\ 3),\ (1\ 3\ 2); \\ \mathfrak{S}_2\colon (1),\ (1\ 2); \\ \mathfrak{S}_2'\colon (1),\ (1\ 3); \qquad \mathfrak{S}_2''\colon (1),\ (2\ 3); \\ \mathfrak{E}\colon (1). \end{cases}$$

Sind $a, b, \ldots$ irgend welche Elemente in einer Gruppe $\mathfrak{G}$, so gibt es außer $\mathfrak{G}$ möglicherweise noch andere Untergruppen, die $a, b, \ldots$ enthalten. Der Durchschnitt aller dieser ist wieder eine Gruppe $\mathfrak{A}$. Man nennt diese die von $a, b, \ldots$ *erzeugte* Gruppe. Diese enthält sicher alle Potenzprodukte wie $a^{-1}a^{-1}ba\,b^{-1}\ldots$ (von endlichvielen Faktoren, mit oder ohne Wiederholung). Diese Potenzprodukte bilden aber eine Gruppe, die $a, b, \ldots$ enthält und die also auch $\mathfrak{A}$ umfaßt. Also ist diese Gruppe mit $\mathfrak{A}$ identisch. Damit ist gezeigt:

Die von $a, b, \ldots$ erzeugte Gruppe besteht aus allen Potenzprodukten aus je endlichvielen dieser Elemente.

Insbesondere erzeugt ein einziges Element a die Gruppe aller Potenzen $a^{\pm n}$ (inklusive $a^0 = 1$). Wegen

$$a^n a^m = a^{n+m} = a^m a^n$$

ist diese Gruppe Abelsch.

Eine Gruppe, die aus den Potenzen eines einzigen Elementes besteht, nennt man *zyklisch*.

Es gibt nun zwei Möglichkeiten. *Entweder* sind alle Potenzen a^h verschieden; dann ist die zyklische Gruppe

$$\ldots,\ a^{-2},\ a^{-1},\ a^0,\ a^1,\ a^2,\ \ldots$$

unendlich. Oder es kommt einmal vor, daß

$$a^h = a^k,\ h > k$$

ist. Dann ist

$$a^{h-k} = e \qquad (h - k > 0).$$

In diesem Falle sei nun n der kleinste positive Exponent, für den $a^n = e$ ist. Dann sind die Potenzen $a^0, a^1, a^2, \ldots, a^{n-1}$ alle verschieden; denn aus

$$a^h = a^k \qquad (0 \leqq k < h < n)$$

würde folgen

$$a^{h-k} = e \qquad (0 < h - k < n),$$

entgegen der über n gemachten Voraussetzung.

Stellt man jede ganze Zahl m in der Form

$$m = q\,n + r \qquad (0 \leqq r < n)$$

dar, so ist

$$a^m = a^{q\,n+r} = a^{q\,n}\,a^r = (a^n)^q a^r = e\,a^r = a^r.$$

Also sind alle Potenzen von a schon in der Reihe $a^0, a^1, \ldots, a^{n-1}$ ver-

treten. Die zyklische Gruppe hat demnach genau n Elemente, nämlich

$$a^0,\ a^1,\ \ldots,\ a^{n-1}.$$

Die Zahl n, die Ordnung der von a erzeugten zyklischen Gruppe, heißt die *Ordnung des Elements a*. Sind alle Potenzen von a verschieden, so nennt man a ein *Element unendlicher Ordnung*.

Beispiele. Die ganzen Zahlen

$$\ldots,\ -2,\ -1,\ 0,\ 1,\ 2,\ \ldots$$

mit der Addition als Verknüpfung bilden eine unendliche zyklische Gruppe. Die oben angeschriebenen Gruppen $\mathfrak{S}_2$, $\mathfrak{A}_3$ sind zyklische Gruppen der Ordnungen 2, 3.

Aufgaben. 1. In einer Abelschen Gruppe ist das Produkt eines Elements a der Ordnung n und eines Elements b der Ordnung m, wo m und n Zahlen ohne gemeinsamen Teiler > 1 sind, ein Element der Ordnung mn.

2. Es gibt zyklische Permutationsgruppen beliebiger Ordnung.

3. Eine Untergruppe einer zyklischen Gruppe ist wieder zyklisch. Wenn die ganze Gruppe durch a und die Untergruppe durch a^m erzeugt wird, so sind die Elemente der Untergruppe die m-ten Potenzen der Elemente der ganzen Gruppe. [Man suche, falls nicht die Untergruppe $= \mathfrak{E}$ ist, das Element a^m mit kleinstem $m > 0$ und zeige, daß alle anderen Elemente Potenzen davon sind.]

4. Man beweise durch Induktion nach n, daß die $n-1$ Transpositionen (1 2), (1 3), ..., (1 n) für $n > 1$ die symmetrische Gruppe $\mathfrak{S}_n$ erzeugen.

5. Ebenso, daß die $n-2$ Dreierzyklen (1 2 3), (1 2 4), ..., (1 2 n) für $n > 2$ die alternierende Gruppe $\mathfrak{A}_n$ erzeugen.

Wenn (in Abelschen Gruppen) die Gruppenrelationen additiv geschrieben werden, so ist eine Untergruppe dadurch charakterisiert, daß sie mit a und b auch $a + b$, mit a auch $-a$ enthält. Diese beiden Forderungen kann man ersetzen durch die einzige Forderung, mit a und b auch $a - b$ zu enthalten.

Nebenklassen. Es sei a ein beliebiges Element von $\mathfrak{G}$ und $\mathfrak{g}$ sei eine Untergruppe. Dann bezeichnen wir mit $a\mathfrak{g}$ die Menge der Produkte von a mit allen Elementen von $\mathfrak{g}$. Jede solche Menge $a\mathfrak{g}$ heißt eine (linksseitige) *Nebenklasse* (auch Nebengruppe, Nebenkomplex oder Restklasse genannt) zu $\mathfrak{g}$. Liegt a in $\mathfrak{g}$, so ist offenbar $a\mathfrak{g} = \mathfrak{g}$; also ist eine der Nebenklassen von $\mathfrak{g}$ gleich $\mathfrak{g}$ selbst. (Ebenso definiert man die rechtsseitigen Nebenklassen $\mathfrak{g}a$.)

Zwei Nebenklassen $a\mathfrak{g}$, $b\mathfrak{g}$ können sehr wohl gleich sein, ohne daß $a = b$ ist. Immer dann nämlich, wenn $a^{-1}b$ in $\mathfrak{g}$ liegt, gilt

$$b\mathfrak{g} = aa^{-1}b\mathfrak{g} = a(a^{-1}b\mathfrak{g}) = a\mathfrak{g}.$$

Zwei *verschiedene* Nebenklassen haben kein Element gemeinsam. Denn wenn die Nebenklassen $a\,\mathfrak{g}$ und $b\,\mathfrak{g}$ ein Element gemein haben, etwa

$$a\,g_1 = b\,g_2\,,$$

so folgt

$$g_1\,g_2^{-1} = a^{-1}\,b\,,$$

so daß $a^{-1}b$ in $\mathfrak{g}$ liegt; nach dem Vorigen sind also $a\mathfrak{g}$ und $b\mathfrak{g}$ identisch.

Jedes Element a gehört einer Nebenklasse an, nämlich der Nebenklasse $a\mathfrak{g}$. Diese enthält ja sicher das Element $ae = a$. Nach dem eben Bewiesenen gehört das Element a auch *nur* einer Nebenklasse an. Wir können demnach jedes Element a als *Repräsentanten* der a enthaltenden Nebenklasse $a\mathfrak{g}$ ansehen.

Nach dem Vorhergehenden bilden die Nebenklassen eine *Klasseneinteilung* der Gruppe $\mathfrak{G}$. Jedes Element gehört einer und nur einer Klasse an[1].

Die Nebenklassen sind, mit Ausnahme von $\mathfrak{g}$ selbst, *keine* Gruppen; denn eine Gruppe müßte das Einselement enthalten.

Die Anzahl der verschiedenen Nebenklassen einer Untergruppe $\mathfrak{g}$ in $\mathfrak{G}$ heißt der *Index* von $\mathfrak{g}$ in $\mathfrak{G}$. Der Index kann endlich oder unendlich sein.

Ist N die (als endlich angenommene) Ordnung von $\mathfrak{G}$, n die von $\mathfrak{g}$, j der Index, so gilt die Relation

$$N = j\,n; \tag{2}$$

denn $\mathfrak{G}$ ist ja in j Klassen eingeteilt, deren jede n Elemente enthält[2].

Man kann für endliche Gruppen aus (2) den Index j berechnen:

$$j = \frac{N}{n}\,.$$

Folge. *Die Ordnung einer Untergruppe einer endlichen Gruppe ist Teiler der Ordnung der Gesamtgruppe.*

Nimmt man für die Untergruppe speziell die von einem Element c erzeugte zyklische Gruppe, so folgt:

Die Ordnung eines Elements einer endlichen Gruppe ist Teiler der Gruppenordnung.

Eine unmittelbare Folge dieses Satzes ist: *In einer Gruppe mit n Elementen gilt für jedes a die Beziehung $a^n = 1$.*

---

[1] In der Literatur findet man oft die von Galois eingeführte Schreibweise:

$$\mathfrak{G} = a_1\,\mathfrak{g} + a_2\,\mathfrak{g} + \cdots,$$

welche besagen soll, daß die Klassen $a_\nu\mathfrak{g}$ zueinander fremd sind und zusammen die Gruppe $\mathfrak{G}$ ausmachen.

[2] Die Relation gilt zwar auch, wenn N unendlich ist; nur muß man dann, um ihren Sinn zu erklären, Produkte von Kardinalzahlen einführen, was wir nicht getan haben.

Es kann vorkommen, daß alle linksseitigen Nebenklassen $a\mathfrak{g}$ zugleich rechtsseitige sind. Soll das der Fall sein, so muß diejenige linksseitige Nebenklasse, in der ein beliebig vorgegebenes Element a liegt, mit der rechtsseitigen Nebenklasse, die a enthält, identisch sein; d. h. es muß für jedes a

$$a\mathfrak{g} = \mathfrak{g}a \tag{3}$$

sein.

Man nennt eine Untergruppe $\mathfrak{g}$, welche die Eigenschaft (3) hat, d. h. welche mit jedem Element a aus $\mathfrak{G}$ vertauschbar ist, einen *Normalteiler*[1] oder eine *ausgezeichnete* oder *invariante Untergruppe* in $\mathfrak{G}$.

Aufgaben. 6. Man suche zu den Untergruppen der $\mathfrak{S}_3$ die rechts- und linksseitigen Nebenklassen. Welche von diesen Untergruppen sind Normalteiler?

7. Man zeige, daß bei einer beliebigen Untergruppe die Inversen der Elemente einer linksseitigen Nebenklasse eine rechtsseitige Nebenklasse bilden. Daraus ist weiter zu erschließen, daß der Index auch als Anzahl der rechtsseitigen Nebenklassen bestimmt werden kann.

8. Man zeige, daß jede Untergruppe vom Index 2 Normalteiler ist. Beispiel: die alternierende Gruppe in der symmetrischen von n Ziffern.

9. Eine Untergruppe einer Abelschen Gruppe ist immer Normalteiler.

10. Diejenigen Elemente einer Gruppe, die mit allen Elementen vertauschbar sind, bilden in der Gruppe einen Normalteiler (das *„Zentrum"* der Gruppe).

11. Ist $\mathfrak{G}$ eine von a erzeugte zyklische Gruppe, $\mathfrak{H}$ eine von $\mathfrak{E}$ verschiedene Untergruppe, so ist der Index m von $\mathfrak{H}$ stets endlich, und zwar gleich dem kleinsten positiven Exponenten m, so daß a^m zu $\mathfrak{H}$ gehört. Durch Angabe von m ist (bei gegebenem $\mathfrak{G}$) $\mathfrak{H}$ bestimmt. (Vgl. Aufg. 3.)

12. Der Index m von Aufg. 11 kann ein beliebiger echter Teiler der Ordnung von $\mathfrak{G}$, falls $\mathfrak{G}$ endlich, und eine ganz beliebige natürliche Zahl sein, wenn $\mathfrak{G}$ unendlich ist.

§ 8. Isomorphismen und Automorphismen.

Wir denken uns zwei Mengen $\mathfrak{M}, \overline{\mathfrak{M}}$ gegeben. In jeder dieser Mengen seien irgendwelche Relationen zwischen den Elementen definiert. Man kann sich z. B. denken, daß die Mengen $\mathfrak{M}, \overline{\mathfrak{M}}$ Gruppen sind und daß die Relationen die Gleichungen $a \cdot b = c$ sind, die vermöge der Gruppeneigenschaft bestehen. Oder man kann sich etwa denken, daß die Mengen geordnet sind und daß die Relationen $a > b$ gemeint sind.

[1] Der Name ist so zu erklären: Teiler heißt hier Untergruppe und das Wort „normal" soll die besondere Eigenschaft $a\mathfrak{g} = \mathfrak{g}a$ zum Ausdruck bringen.

Wenn es nun möglich ist, die beiden Mengen eineindeutig aufeinander abzubilden derart, daß die Relationen bei der Abbildung erhalten bleiben, d. h. wenn jedem Element a von $\mathfrak{M}$ umkehrbar eindeutig ein Element $\bar{a}$ von $\overline{\mathfrak{M}}$ zugeordnet werden kann, so daß die Relationen, die zwischen irgend welchen Elementen $a, b, \ldots$ von $\mathfrak{M}$ bestehen, auch zwischen den zugeordneten Elementen $\bar{a}, \bar{b}, \ldots$ bestehen und umgekehrt, so nennt man die beiden Mengen *isomorph* (bezüglich der fraglichen Relationen) und schreibt $\mathfrak{M} \simeq \overline{\mathfrak{M}}$. Die Zuordnung selbst heißt *Isomorphismus*.

Um die Eineindeutigkeit zum Ausdruck zu bringen, sagt man auch 1-*isomorph* und 1-*Isomorphismus*.

So kann man reden von 1-*isomorphen Gruppen*, von isomorphgeordneten oder *ähnlich-geordneten* Mengen usw. Ein 1-Isomorphismus zweier Gruppen ist also eine solche eineindeutige Abbildung $a \to \bar{a}$, bei der aus $ab = c$ folgt $\bar{a}\bar{b} = \bar{c}$ (und umgekehrt), also bei der dem Produkt ab stets das Produkt $\bar{a}\bar{b}$ zugeordnet ist.

Ebenso wie gleichmächtige Mengen für die allgemeine Mengentheorie gleichwertig sind, so sind ähnliche Mengen in der Theorie der Ordnungstypen und isomorphe Gruppen in der Gruppentheorie als nicht wesentlich verschieden zu betrachten. Man kann alle Begriffe und Sätze, die auf Grund der gegebenen Relationen einer Menge definiert und bewiesen werden können, unmittelbar auf jede 1-isomorphe Menge übertragen. Zum Beispiel ist eine Menge, in der Produktrelationen definiert sind und die einer Gruppe 1-isomorph ist, wieder eine Gruppe, und Einselement, Inverses und Untergruppen gehen bei der 1-Isomorphie wieder in Einselement, Inverses und Untergruppen über.

Wenn insbesondere die beiden Mengen $\overline{\mathfrak{M}}$, $\mathfrak{M}$ identisch sind, d. h. wenn die betrachtete Zuordnung jedem Element a ein Element $\bar{a}$ derselben Menge umkehrbar eindeutig zuordnet mit Erhaltung der Relationen, so heißt die Zuordnung ein *Automorphismus* (oder 1-*Automorphismus*).

Zum Beispiel ist, wenn $\mathfrak{M}$ die Menge der ganzen Zahlen ist und die zugrunde gelegte Relation die Anordnungsrelation $a < b$, die Zuordnung

$$a \to a + 1$$

ein 1-Automorphismus, denn die Zuordnung bildet die Menge der ganzen Zahlen eineindeutig auf sich selbst ab und aus $a < b$ folgt $a + 1 < b + 1$ und umgekehrt.

Die 1-Automorphismen einer Menge bringen gewissermaßen ihre Symmetrieeigenschaften zum Ausdruck. Denn was bedeutet eine Symmetrie z. B. einer geometrischen Figur? Sie heißt, daß die Figur bei gewissen Transformationen (Spiegelungen, Drehungen usw.) in sich übergeht, wobei gewisse Relationen (Entfernungen, Winkel, Lagebeziehun-

gen) erhalten bleiben, oder in unserer Terminologie, daß die Figur in bezug auf ihre metrischen Eigenschaften gewisse 1-Automorphismen gestattet.

Offenbar ist das Produkt zweier 1-Automorphismen (Produktbildung von Transformationen nach § 6) wieder ein 1-Automorphismus und die inverse Operation eines 1-Automorphismus wieder ein solcher. Daraus folgt nach § 6, daß die 1-Automorphismen einer beliebigen Menge (mit beliebigen Relationen zwischen ihren Elementen) eine Transformationsgruppe bilden: die *Automorphismengruppe* der Menge.

Insbesondere bilden die 1-Automorphismen einer Gruppe wieder eine Gruppe. Wir wollen einige dieser Automorphismen etwas näher betrachten.

Ist a ein festes Gruppenelement, so ist die Zuordnung, die x in

$$\bar{x} = a x a^{-1} \tag{1}$$

überführt, ein 1-Automorphismus. Denn erstens läßt sich (1) nach x eindeutig auflösen:

$$x = a^{-1} \bar{x} a;$$

also ist die Zuordnung eineindeutig. Zweitens ist

$$\bar{x}\,\bar{y} = a x a^{-1} \cdot a y a^{-1} = a (x y) a^{-1} = \overline{x y};$$

also ist die Zuordnung isomorph.

Man nennt $a x a^{-1}$ das aus x mit Hilfe von a transformierte Element und nennt die Elemente x, $a x a^{-1}$ *konjugierte Gruppenelemente.* Die von den Elementen a erzeugten Automorphismen $x \to a x a^{-1}$ heißen *innere Automorphismen* der Gruppe. Alle übrigen 1-Automorphismen (falls noch andere existieren) heißen *äußere Automorphismen.*

Bei einem inneren Automorphismus $x \to a x a^{-1}$ geht eine Untergruppe $\mathfrak{g}$ in eine Untergruppe $a \mathfrak{g} a^{-1}$ über, die man eine *zu* $\mathfrak{g}$ *konjugierte Untergruppe* nennt.

Ist eine Untergruppe $\mathfrak{g}$ mit allen ihren konjugierten identisch:

$$a \mathfrak{g} a^{-1} = \mathfrak{g} \text{ für jedes } a, \tag{2}$$

so heißt das nichts anderes, als daß die Gruppe $\mathfrak{g}$ mit jedem Element a vertauschbar ist:

$$a \mathfrak{g} = \mathfrak{g} a,$$

mithin *Normalteiler* ist (§ 7). Also:

Die gegenüber allen inneren Automorphismen invarianten Untergruppen sind die Normalteiler.

Durch diesen Satz erklärt sich die Bezeichnung „invariante Untergruppe" für die Normalteiler.

Die Forderung (2) kann durch die etwas schwächere

$$a \mathfrak{g} a^{-1} \leqq \mathfrak{g} \tag{3}$$

ersetzt werden. Denn wenn (3) für jedes a gilt, so gilt es auch für a^{-1}:

$$a^{-1}\,\mathfrak{g}\,a \subseteq \mathfrak{g},$$

$$\mathfrak{g} \subseteq a\,\mathfrak{g}\,a^{-1}; \tag{4}$$

aus (3) und (4) folgt aber (2). Also:

Eine Untergruppe ist Normalteiler, wenn sie zu jedem Element b auch alle konjugierten Elemente aba^{-1} enthält.

Aufgaben. 1. Abelsche Gruppen haben keine inneren Automorphismen außer dem identischen. Man zeige, daß die Gruppe

$$e,\ a,\ b,\ c$$

mit dem Einselement e und den Zusammensetzungsregeln:

$$\begin{cases} a^2 = b^2 = c^2 = e, \\ ab = ba = c, \\ bc = cb = a, \\ ca = ac = b \end{cases}$$

keine inneren Automorphismen außer dem identischen, aber fünf äußere Automorphismen hat.

2. In Permutationsgruppen kann man das transformierte Element aba^{-1} eines Elements b dadurch erhalten, daß man b als Produkt von Zyklen darstellt (§ 7) und die Ziffern in diesen Zyklen der Permutation a unterwirft. Beweis? Mit Hilfe dieses Satzes berechne man aba^{-1} für den Fall

$$b = (1\ 2)\,(3\ 4\ 5),$$
$$a = (2\ 3\ 4\ 5).$$

3. Man beweise, daß die symmetrische Gruppe $\mathfrak{S}_3$ keine äußeren, aber sechs innere Automorphismen hat.

4. Die symmetrische Gruppe $\mathfrak{S}_4$ hat außer sich selbst und der Einheitsgruppe *nur* die folgenden Normalteiler:

1) die alternierende Gruppe $\mathfrak{A}_4$,

2) die „*Klein*sche Vierergruppe" $\mathfrak{B}_4$, bestehend aus den Permutationen

$$(1),\ (1\ 2)\,(3\ 4),\ (1\ 3)\,(2\ 4),\ (1\ 4)\,(2\ 3).$$

Die letztere Gruppe ist Abelsch und isomorph zu der in Aufgabe 1 abstrakt definierten Gruppe.

5. Ist $\mathfrak{g}$ Normalteiler in $\mathfrak{G}$ und $\mathfrak{H}$ eine „Zwischengruppe":

$$\mathfrak{g} \subseteq \mathfrak{H} \subseteq \mathfrak{G},$$

so ist $\mathfrak{g}$ auch Normalteiler in $\mathfrak{H}$.

6. Alle unendlichen zyklischen Gruppen sind isomorph zur additiven Gruppe der ganzen Zahlen.

7. Die mit einem Element a vertauschbaren Elemente x in einer Gruppe $\mathfrak{G}$, die Elemente x also, für die

$$xa = ax$$

ist, bilden eine Gruppe, den *Normalisator* von a. Diese enthält die von a erzeugte zyklische Gruppe als einen Normalteiler. Die Anzahl der mit a konjugierten Elemente ist gleich dem Index des Normalisators in $\mathfrak{G}$.

8. Man kann die Elemente einer Gruppe $\mathfrak{G}$ in Klassen konjugierter Elemente einteilen. Die Anzahl der Elemente einer Klasse ist, falls $\mathfrak{G}$ endlich ist, ein Teiler der Ordnung von $\mathfrak{G}$. Die Eins, sowie jedes Zentrumselement (§ 7, Aufg. 10), bildet für sich eine Klasse.

9. Ist in einer Gruppe der Ordnung p^n, wo p Primzahl ist, a_λ die Anzahl der Klassen mit p^λ-Elementen, insbesondere a_0 die Anzahl der Zentrumselemente, so ist

$$p^n = a_0 + a_1 p + a_2 p^2 + \cdots.$$

Man zeige mit Hilfe dieser Gleichung, daß das Zentrum einer Gruppe der Ordnung p^n nicht aus dem Einselement allein bestehen kann.

§ 9. Homomorphie. Normalteiler. Faktorgruppen.

Wenn in zwei Mengen $\mathfrak{M}$, $\overline{\mathfrak{M}}$ gewisse Relationen definiert sind und wenn jedem Element a von $\mathfrak{M}$ genau ein Bildelement $\bar{a}$ in $\overline{\mathfrak{M}}$ zugeordnet ist derart, daß:

1. jedes Element $\bar{a}$ von $\overline{\mathfrak{M}}$ mindestens einmal als Bild auftritt,

2. alle Relationen zwischen Elementen von $\mathfrak{M}$ auch für die entsprechenden Elemente von $\overline{\mathfrak{M}}$ gelten,

so heißt die Zuordnung ein *Homomorphismus*[1] oder *mehrstufiger Isomorphismus*. $\overline{\mathfrak{M}}$ heißt dann ein *homomorphes Bild* von $\mathfrak{M}$ oder kurz *homomorph* zu $\mathfrak{M}$.

Man schreibt dann $\mathfrak{M} \sim \overline{\mathfrak{M}}$.

Ist die Zuordnung umkehrbar eindeutig und gilt die Homomorphieeigenschaft auch in der umgekehrten Richtung, so ist der Homomorphismus ein „einstufiger Isomorphismus" oder 1-Isomorphismus im früher erklärten Sinn.

Bei einer homomorphen Abbildung kann man die Elemente von $\mathfrak{M}$, die ein festes Bild $\bar{a}$ in $\overline{\mathfrak{M}}$ haben, zu einer Klasse $\mathfrak{a}$ vereinigen. Jedes

[1] Ein fester Sprachgebrauch für die Wörter Isomorphismus und Homomorphismus existiert nicht. SPEISER z. B. verwendet in der 1. Auflage seiner früher zitierten „Theorie der Gruppen von endlicher Ordnung" die beiden Wörter gerade umgekehrt. Die hier gewählte Bezeichnung schließt sich mehr dem Üblichen an.

Element a gehört einer und nur einer Klasse $\mathfrak{a}$ an; d. h. die Menge $\mathfrak{M}$ ist *in Klassen eingeteilt,* die den Elementen von $\overline{\mathfrak{M}}$ eineindeutig zugeordnet sind.

Beispiele: Ordnet man jedem Element einer Gruppe das Einselement zu, so entsteht eine Homomorphie der Gruppe mit der Einheitsgruppe. Ebenso entsteht eine Homomorphie, wenn man jeder Permutation einer Permutationsgruppe die Zahl $+1$ oder -1 zuordnet, je nachdem die Permutation gerade oder ungerade ist; die zugeordnete Gruppe ist die multiplikative Gruppe der Zahlen $+1$ und -1.

Ordnet man jeder ganzen Zahl m die Potenz a^m eines Elements a einer Gruppe zu, so entsteht ein Homomorphismus der additiven Gruppe der ganzen Zahlen mit der von a erzeugten zyklischen Gruppe, denn der Summe $m+n$ ist das Produkt $a^{m+n} = a^m \cdot a^n$ zugeordnet. Ist a ein Element von unendlicher Ordnung, so ist der Homomorphismus ein 1-Isomorphismus.

Wir wollen nun speziell Homomorphismen von Gruppen untersuchen.

Sind in einer Menge $\overline{\mathfrak{G}}$ *Produkte* $\bar{a}\bar{b}$ *(also Relationen der Gestalt* $\bar{a}\bar{b} = \bar{c}$*) definiert und ist eine Gruppe* $\mathfrak{G}$ *auf* $\overline{\mathfrak{G}}$ *homomorph abgebildet, so ist auch* $\overline{\mathfrak{G}}$ *eine Gruppe.* Kurz: *Das homomorphe Abbild einer Gruppe ist wieder eine Gruppe.*

Beweis: Zunächst sind je drei gegebene Elemente $\bar{a}, \bar{b}, \bar{c}$ von $\overline{\mathfrak{G}}$ stets Bilder von Elementen von $\mathfrak{G}$, also etwa von a, b, c. Aus

$$a\,b \cdot c = a \cdot b\,c$$

folgt dann

$$\bar{a}\bar{b} \cdot \bar{c} = \bar{a} \cdot \bar{b}\bar{c}.$$

Weiter folgt aus

$$a\,e = a \quad \text{für alle } a,$$

$$\bar{a}\,\bar{e} = \bar{a} \text{ für alle } \bar{a},$$

und aus

$$b\,a = e \qquad (b = a^{-1}),$$

$$\bar{b}\,\bar{a} = \bar{e}.$$

Also gibt es in $\overline{\mathfrak{G}}$ ein Einselement $\bar{e}$ und zu jedem $\bar{a}$ ein Inverses. Also ist $\overline{\mathfrak{G}}$ eine Gruppe. Zugleich ist bewiesen:

Einselement und inverses Element gehen bei einem Homomorphismus wieder in Einselement und inverses Element über.

Jetzt soll die durch eine homomorphe Abbildung $\mathfrak{G} \to \overline{\mathfrak{G}}$ gegebene Klasseneinteilung genauer studiert werden. Es wird sich dabei eine sehr wichtige eineindeutige Beziehung zwischen Homomorphismen und Normalteilern herausstellen.

Die Klasse $\mathfrak{e}$ *von* $\mathfrak{G}$, *der bei einer Homomorphie* $\mathfrak{G} \sim \overline{\mathfrak{G}}$ *das Einheitselement* $\bar{e}$ *von* $\overline{\mathfrak{G}}$ *entspricht, ist ein Normalteiler von* $\mathfrak{G}$ *und die übrigen Klassen sind die Nebenklassen dieses Normalteilers.*

Beweis: Zunächst ist $\mathfrak{e}$ eine Gruppe. Denn wenn a und b bei der Homomorphie beide in $\bar{e}$ übergehen, so geht $\overline{ab}$ über in $\bar{e}^2 = \bar{e}$; also enthält $\mathfrak{e}$ zu je zwei Elementen das Produkt. Weiter geht a^{-1} über in $\bar{e}^{-1} = \bar{e}$; also enthält $\mathfrak{e}$ auch das Inverse eines jeden Elementes.

Die Elemente einer linksseitigen Nebenklasse $a\mathfrak{e}$ gehen alle über in das Element $\bar{a}\bar{e} = \bar{a}$. Wenn umgekehrt ein Element a' in $\bar{a}$ übergeht, so bestimme man x aus

$$a x = a' .$$

Es folgt:

$$\bar{a}\bar{x} = \bar{a} ,$$

$$\bar{x} = \bar{e} .$$

Also liegt x in $\mathfrak{e}$, also a' in $a\mathfrak{e}$.

Die Klasse von $\mathfrak{G}$, die dem Element $\bar{a}$ entspricht, ist also genau die linksseitige Nebenklasse $a\mathfrak{e}$.

Genau so zeigt man aber, daß die Klasse, die $\bar{a}$ entspricht, die rechtsseitige Nebenklasse $\mathfrak{e}a$ sein muß. Also stimmen rechts- und linksseitige Nebenklassen überein:

$$a\mathfrak{e} = \mathfrak{e}a ,$$

und $\mathfrak{e}$ ist Normalteiler. Damit ist alles bewiesen.

Wir sind bis jetzt von einer gegebenen Homomorphie ausgegangen und sind zwangsläufig auf einen Normalteiler geführt worden. Nun kehren wir aber die Frage um: *Gegeben sei ein Normalteiler* $\mathfrak{g}$ *von* $\mathfrak{G}$. *Kann man eine zu* $\mathfrak{G}$ *homomorphe Gruppe* $\overline{\mathfrak{G}}$ *bilden, so daß die Nebenklassen von* $\mathfrak{g}$ *genau den Elementen von* $\overline{\mathfrak{G}}$ *entsprechen?*

Um das zu erreichen, wählen wir am einfachsten als Elemente der zu konstruierenden Gruppe $\overline{\mathfrak{G}}$ die Nebenklassen von $\mathfrak{g}$ selbst und versuchen, eine Multiplikation für sie zu definieren, so daß die Zuordnung $a \to a\mathfrak{g}$ ein Homomorphismus ist. Wir müssen demnach zu je zwei Nebenklassen $a\mathfrak{g}$, $b\mathfrak{g}$ eine dritte suchen, so daß die Produkte der Elemente von $a\mathfrak{g}$ mit denen von $b\mathfrak{g}$ sämtlich in dieser dritten Nebenklasse liegen. Diese dritte Nebenklasse muß insbesondere ab enthalten, also mit $ab\mathfrak{g}$ identisch sein. $ab\mathfrak{g}$ hat aber auch wirklich die verlangte Eigenschaft; denn jedes Produkt

$$a g_1 \cdot b g_2 \qquad (g_1, g_2 \text{ in } \mathfrak{g})$$

läßt sich als

$$a b \cdot b^{-1} g_1 b \cdot g_2 = a b g_3 \qquad (g_3 \text{ in } \mathfrak{g})$$

schreiben und gehört daher zu $ab\mathfrak{g}$.

Wir können demnach definieren: *Das Produkt zweier Nebenklassen* $a\mathfrak{g}$, $b\mathfrak{g}$ *ist die Nebenklasse* $ab\mathfrak{g}$. *Diese Nebenklasse ist von der Wahl der Repräsentanten* a, b *unabhängig; denn in ihr liegen alle Produkte je eines Elements von* $a\mathfrak{g}$ *mit einem Element von* $b\mathfrak{g}$.

Die Nebenklassen bilden mit dieser Produktdefinition eine zu $\mathfrak{G}$ homomorphe Menge, *also eine zu* $\mathfrak{G}$ *homomorphe Gruppe.* Man nennt diese die *Faktorgruppe* von $\mathfrak{G}$ nach $\mathfrak{g}$ und stellt sie durch das Symbol

$$\mathfrak{G}/\mathfrak{g}$$

dar. Die Ordnung von $\mathfrak{G}/\mathfrak{g}$ ist der Index von $\mathfrak{g}$.

Wir sehen hier die prinzipielle Wichtigkeit der Normalteiler: sie ermöglichen die Konstruktion von neuen Gruppen, die zu gegebenen Gruppen homomorph sind.

Ist eine Gruppe $\mathfrak{G}$ auf eine andere Gruppe $\overline{\mathfrak{G}}$ homomorph abgebildet, so sahen wir schon, daß den Elementen von $\overline{\mathfrak{G}}$ (umkehrbar eindeutig) die Nebenklassen eines Normalteilers $\mathfrak{e}$ in $\mathfrak{G}$ entsprechen. Diese Zuordnung ist natürlich eine Isomorphie; denn wenn $a\mathfrak{g}$, $b\mathfrak{g}$ zwei Nebenklassen sind, so ist $ab\mathfrak{g}$ ihr Produkt; die entsprechenden Elemente in $\overline{\mathfrak{G}}$ sind $\bar{a}$, $\bar{b}$, $(\overline{ab})$ und es ist in der Tat

$$(\overline{a\,b}) = \bar{a} \cdot \bar{b}$$

wegen der Homomorphie. Also haben wir:

$$\mathfrak{G}/\mathfrak{e} \simeq \overline{\mathfrak{G}},$$

und damit den *Homomorphiesatz für Gruppen*:

Jede Gruppe $\overline{\mathfrak{G}}$, *auf die* $\mathfrak{G}$ *homomorph abgebildet ist, ist isomorph einer Faktorgruppe* $\mathfrak{G}/\mathfrak{e}$; *dabei ist* $\mathfrak{e}$ *derjenige Normalteiler von* $\mathfrak{G}$, *dessen Elementen das Einselement in* $\overline{\mathfrak{G}}$ *entspricht. Umgekehrt ist* $\mathfrak{G}$ *auf jede Faktorgruppe* $\mathfrak{G}/\mathfrak{e}$ (*wo* $\mathfrak{e}$ *Normalteiler*) *homomorph abgebildet.*

Aufgaben. 1. Triviale Faktorgruppen einer jeden Gruppe $\mathfrak{G}$ sind: $\mathfrak{G}/\mathfrak{E} \simeq \mathfrak{G}$; $\mathfrak{G}/\mathfrak{G} \simeq \mathfrak{E}$.

2. Die Faktorgruppe der alternierenden Gruppe $(\mathfrak{S}_n/\mathfrak{A}_n)$ ist eine zyklische Gruppe der Ordnung 2.

3. Die Faktorgruppe $\mathfrak{S}_4/\mathfrak{B}_4$ der KLEINschen Vierergruppe (§ 8, Aufgabe 4) ist isomorph mit $\mathfrak{S}_3$.

4. Die Elemente $aba^{-1}b^{-1}$ einer Gruppe $\mathfrak{G}$ und ihre Produkte (zu je endlichvielen) bilden eine Gruppe, die man die *Kommutatorgruppe* von $\mathfrak{G}$ nennt. Diese ist Normalteiler, und ihre Faktorgruppe ist Abelsch. Jeder Normalteiler, dessen Faktorgruppe Abelsch ist, umfaßt die Kommutatorgruppe.

5. Die mit einer Untergruppe $\mathfrak{g}$ vertauschbaren Elemente bilden eine Gruppe $\mathfrak{h}$, in der $\mathfrak{g}$ Normalteiler ist. Man nennt sie den *Normalisator* von $\mathfrak{g}$. Der Index von $\mathfrak{h}$ in $\mathfrak{G}$ ist die Anzahl der mit $\mathfrak{g}$ konjugierten Untergruppen von $\mathfrak{G}$.

6. Ist $\mathfrak{G}$ zyklisch, a das erzeugende Element von $\mathfrak{G}$, $\mathfrak{g}$ eine Untergruppe vom Index m, so ist $\mathfrak{G}/\mathfrak{g}$ zyklisch von der Ordnung m. Als Repräsentanten der Nebenklassen können die Elemente $1, a, a^2, \ldots, a^{m-1}$ gewählt werden.

In einer Abelschen Gruppe ist jede Untergruppe Normalteiler (vgl. § 7, Aufgabe 9). Schreibt man die Verknüpfung als Addition, so hat man für die Untergruppen, wie schon erwähnt, auch den Namen *Moduln*. Die Nebenklassen $a + \mathfrak{M}$ (wo $\mathfrak{M}$ ein Modul ist) heißen *Restklassen*, und die Faktorgruppe $\mathfrak{G}/\mathfrak{M}$ heißt *Restklassenmodul*.

Zwei Elemente a, b liegen in einer Restklasse, wenn ihre Differenz in $\mathfrak{M}$ liegt. Man nennt zwei solche Elemente *kongruent nach dem Modul* $\mathfrak{M}$ oder: *kongruent modulo* $\mathfrak{M}$, und schreibt

$$a \equiv b \,(\mathrm{mod}\, \mathfrak{M})$$

oder kurz

$$a \equiv b \,(\mathfrak{M}) .$$

Für die im Homomorphismus zugeordneten Elemente $\bar{a}, \bar{b}$ des Restklassenmoduls gilt dann:

$$\bar{a} = \bar{b} .$$

Umgekehrt folgt aus $\bar{a} = \bar{b}$ stets $a \equiv b \,(\mathfrak{M})$.

Zum Beispiel bilden im Bereich der ganzen Zahlen die Vielfachen einer natürlichen Zahl m einen Modul, und man schreibt dementsprechend

$$a \equiv b \,(m) ,$$

wenn die Differenz $a - b$ durch m teilbar ist. Die Restklassen können durch $0, 1, 2, \ldots, m - 1$ repräsentiert werden, und der Restklassenmodul ist eine zyklische Gruppe der Ordnung m.

Aufgabe. 7. Jede zyklische Gruppe der Ordnung m ist isomorph dem Restklassenmodul nach der ganzen Zahl m.

Drittes Kapitel.

Ringe und Körper.

Inhalt: Definition der Begriffe Ring, Integritätsbereich, Körper. Allgemeine Methoden, aus Ringen andere Ringe (bzw. Körper) zu bilden. Sätze über Primfaktorzerlegung in Integritätsbereichen.

Die Begriffe dieses Kapitels werden im ganzen Buch benutzt.

§ 10. Ringe.

Die Größen, mit denen man in der Algebra und Arithmetik operiert, sind von verschiedener Natur; bald sind es die ganzen, bald die rationalen, die reellen, die komplexen, die algebraischen Zahlen;

die Polynome oder ganzen rationalen Funktionen von n Veränderlichen usw. Wir werden später noch Größen von ganz anderer Natur: hyperkomplexe Zahlen, Restklassen u. dgl., kennenlernen, mit denen man ganz oder fast ganz wie mit Zahlen rechnen kann. Es ist daher wünschenswert, alle diese Größenbereiche unter einen gemeinsamen Begriff zu bringen und die Rechengesetze in diesen Bereichen allgemein zu untersuchen.

Unter einem *System mit doppelter Komposition* versteht man eine Menge von Elementen $a, b, \ldots$, in der zu je zwei Elementen a, b eindeutig eine *Summe* $a + b$ und ein *Produkt* $a \cdot b$ definiert sind, die wieder der Menge angehören.

Ein System mit doppelter Komposition heißt ein *Ring*, wenn folgende *Rechengesetze* für alle Elemente des Systems erfüllt sind:

I. *Gesetze der Addition.*

a) *Assoziatives Gesetz*: $a + (b + c) = (a + b) + c$.

b) *Kommutatives Gesetz*: $a + b = b + a$.

c) *Lösbarkeit der Gleichung* $a + x = b$ für alle a und b.[1]

II. *Gesetz der Multiplikation.*

a) *Assoziatives Gesetz*: $a \cdot bc = ab \cdot c$.

III. *Distributivgesetze.*

a) $a \cdot (b + c) = ab + ac$.

b) $(b + c) \cdot a = ba + ca$.

Zusatz: Gilt auch für die Multiplikation das kommutative Gesetz:

II. b) $a \cdot b = b \cdot a$,

so heißt der Ring *kommutativ*. Vorläufig werden wir es hauptsächlich mit kommutativen Ringen zu tun haben.

Zu den Gesetzen der Addition. Die drei Gesetze I a, b, c zusammen besagen nichts anderes, als daß die Ringelemente bei der Addition eine Abelsche Gruppe bilden[2]. Also können wir alle früher für Abelsche Gruppen bewiesenen Sätze auf Ringe übertragen: Es gibt ein (und nur ein) *Nullelement* 0, mit der Eigenschaft:

$$a + 0 = a \text{ für alle } a.$$

Weiter existiert zu jedem Element a ein *entgegengesetztes Element* $-a$, mit der Eigenschaft

$$-a + a = 0.$$

Sodann ist die Gleichung $a + x = b$ nicht nur lösbar, sondern eindeutig lösbar; ihre einzige Lösung ist

$$x = -a + b;$$

[1] Eindeutige Lösbarkeit wird nicht verlangt, folgt aber später.

[2] Man bezeichnet diese Gruppe als die *additive Gruppe* des Ringes.

wir bezeichnen sie auch mit $b - a$. Da man vermöge

$$a - b = a + (-b)$$

jede Differenz in eine Summe verwandeln kann, so gelten in diesem Sinne auch für Differenzen dieselben Vertauschungsregeln wie für Summen, etwa

$$(a - b) - c = (a - c) - b\,,$$

usw. Schließlich ist $-(-a) = a$ und $a - a = 0$.

Zu den Assoziativgesetzen. Wie wir im Kap. 2, § 6 sahen, kann man auf Grund des Assoziativgesetzes für die Multiplikation die zusammengesetzten Produkte

$$\prod_1^n a_\nu = a_1 a_2 \cdots a_n$$

definieren und ihre Haupteigenschaft

$$\prod_1^m a_\mu \cdot \prod_{\nu=1}^n a_{m+\nu} = \prod_1^{m+n} a_\nu$$

beweisen. Ebenso kann man die Summen

$$\sum_1^n a_\nu = a_1 + a_2 + \cdots + a_n$$

definieren und ihre Haupteigenschaft

$$\sum_1^m a_\mu + \sum_{\nu=1}^n a_{m+\nu} = \sum_1^{m+n} a_\nu$$

beweisen. Vermöge Ib kann man auch in einer Summe die Glieder beliebig vertauschen, und dasselbe gilt in kommutativen Ringen auch für Produkte.

Zu den Distributivgesetzen. Sobald das Kommutativgesetz der Multiplikation gilt, ist IIIb natürlich eine Folge von IIIa.

Aus IIIa folgt durch vollständige Induktion nach n sofort:

$$a(b_1 + b_2 + \cdots + b_n) = ab_1 + ab_2 + \cdots + ab_n\,,$$

ebenso aus IIIb:

$$(a_1 + a_2 + \cdots + a_n)\, b = a_1 b + a_2 b + \cdots + a_n b\,.$$

Beide zusammen ergeben die übliche Regel für die Multiplikation von Summen:

$$\begin{aligned}(a_1 + \cdots + a_n)\,(b_1 + \cdots + b_m) &= a_1 b_1 + \cdots + a_1 b_m \\ &\quad + \cdots\cdots\cdots \\ &\quad + a_n b_1 + \cdots + a_n b_m \\ &= \sum_{i=1}^n \sum_{k=1}^m a_i b_k\,.\end{aligned}$$

Die Distributivgesetze gelten auch für die Subtraktion; z. B. ist

$$a(b - c) = ab - ac\,,$$

wie man aus

$$a(b - c) + ac = a(b - c + c) = ab$$

ersieht.

Insbesondere ist

$$a \cdot 0 = a(a - a) = a \cdot a - a \cdot a = 0\,,$$

oder: *Ein Produkt ist sicher dann Null, wenn ein Faktor es ist.*

Die Umkehrung dieses Satzes braucht, wie wir später an Beispielen sehen werden, nicht zu gelten: Es kann vorkommen, daß

$$a \cdot b = 0\,, \qquad a \neq 0\,, \qquad b \neq 0\,.$$

In diesem Fall nennt man a und b *Nullteiler*, und zwar a einen linken, b einen rechten Nullteiler. (In kommutativen Ringen fallen die beiden Begriffe zusammen.) Es ist zweckmäßig, auch die Null selbst als Nullteiler zu betrachten. a heißt also linker Nullteiler, wenn es ein $b \neq 0$ gibt, so daß $ab = 0$ ist[1].

Wenn es in einem Ring außer der Null keine Nullteiler gibt, d. h. wenn aus $ab = 0$ stets $a = 0$ oder $b = 0$ folgt, so spricht man von einem *Ring ohne Nullteiler*. Ist der Ring außerdem kommutativ, so wird er auch *Integritätsbereich* genannt.

Beispiele: Alle anfangs genannten Beispiele (Ring der ganzen Zahlen, der rationalen Zahlen usw.) sind Ringe ohne Nullteiler. Der Ring der stetigen Funktionen im Intervall $(-1, +1)$ hat Nullteiler; denn setzt man

$$f = f(x) = \max(0, x)\,,$$
$$g = g(x) = \max(0, -x)\,,$$

so ist $f \neq 0$[2], $g \neq 0$, $fg = 0$.

Aufgaben. 1. Die Zahlenpaare (a_1, a_2) (a_1, a_2 etwa rationale Zahlen) mit

$$(a_1, a_2) + (b_1, b_2) = (a_1 + b_1, a_2 + b_2)\,,$$
$$(a_1, a_2) \cdot (b_1, b_2) = (a_1 b_1, a_2 b_2)$$

bilden einen Ring mit Nullteilern.

2. Es ist erlaubt, eine Gleichung $ax = ay$ durch a zu kürzen, falls a kein linker Nullteiler ist. (Insbesondere kann man in einem Integritätsbereich durch jedes $a \neq 0$ kürzen.)

3. Man konstruiere, von einer beliebigen Abelschen Gruppe als additiver Gruppe ausgehend, einen Ring, in dem das Produkt von je zwei Elementen Null ist.

---

[1] Angenommen, daß es im Ring überhaupt Elemente $\neq 0$ gibt.

[2] $f \neq 0$ heißt: f ist eine andere Funktion als die Null. Es soll nicht heißen, daß f nirgends den Wert Null annimmt.

Einselement. Besitzt ein Ring ein links-Einselement e:

$$ex = x \text{ für alle } x,$$

und *zugleich* ein rechts-Einselement e':

$$xe' = x \text{ für alle } x,$$

so müssen beide gleich sein, wegen

$$e = ee' = e'.$$

Ebenso ist dann jedes rechts-Einselement auch gleich e, ebenso jedes links-Einselement. Man nennt dann e das Einselement schlechthin und spricht von einem *Ring mit Einselement*. Oft wird das Einselement mit 1 bezeichnet, obzwar es von der Zahl 1 zu unterscheiden ist.

Die ganzen Zahlen bilden einen Ring C mit Einselement, die geraden Zahlen einen Ring ohne Einselement. Es gibt auch Ringe, wo zwar ein oder mehrere rechts-Einselemente, aber kein links-Einselement existiert, oder umgekehrt.

Inverses Element. Ist a ein beliebiges Element eines Rings mit Einselement e, so versteht man unter einem *Linksinversen* von a ein Element $a_{(l)}^{-1}$ mit der Eigenschaft

$$a_{(l)}^{-1} a = e$$

und unter einem *Rechtsinversen* ein $a_{(r)}^{-1}$ mit der Eigenschaft

$$a a_{(r)}^{-1} = e.$$

Besitzt ein Element a sowohl Links- wie auch Rechtsinverses, so sind wiederum beide einander gleich wegen

$$a_{(l)}^{-1} = a_{(l)}^{-1} (a a_{(r)}^{-1}) = (a_{(l)}^{-1} a) a_{(r)}^{-1} = a_{(r)}^{-1}$$

und daher auch jedes Rechts- sowie jedes Linksinverse von a gleich diesem einen. Man sagt in diesem Fall: *a besitzt ein inverses Element*, und bezeichnet das inverse Element mit a^{-1}.

Potenzen und Vielfache. Wir sahen schon in Kap. II, daß man auf Grund des Assoziativgesetzes die Potenzen a^n (n eine natürliche Zahl) für jedes Ringelement a definieren kann und daß die üblichen Regeln gelten:

$$(1) \qquad \begin{cases} a^n \cdot a^m = a^{n+m}, \\ (a^n)^m = a^{nm}, \\ (ab)^n = a^n b^n, \end{cases}$$

letztere für kommutative Ringe.

Hat der Ring ein Einselement und a ein Inverses, so kann man auch die nullte und negative Potenzen einführen (Kap. 2); die Regeln (1) behalten ihre Gültigkeit.

Ebenso kann man in der additiven Gruppe die Vielfachen

$$n \cdot a \qquad (= a + a + \cdots + a, \text{ mit } n \text{ Gliedern})$$

definieren und hat:

$$(2)\qquad \begin{cases} na + ma = (n+m)a\,, \\ n \cdot ma = nm \cdot a\,, \\ n(a+b) = na + nb\,, \\ n \cdot ab = na \cdot b = a \cdot nb\,. \end{cases}$$

Setzt man wie bei Potenzen

$$(-n) \cdot a = -na\,,$$

so gelten die Regeln (2) für alle ganzzahligen n und m (positiv, negativ oder Null).

Man hüte sich davor, den Ausdruck $n \cdot a$ als ein wirkliches Produkt zweier Ringelemente aufzufassen; denn n ist im allgemeinen kein Ringelement, sondern etwas von außen Hinzukommendes: eine ganze Zahl. Hat aber der Ring ein Einselement e, so kann man na als wirkliches Produkt schreiben, nämlich:

$$na = n \cdot ea = ne \cdot a\,.$$

Aufgaben. 4. Ein linker Nullteiler besitzt kein Linksinverses, ein rechter Nullteiler kein Rechtsinverses. Insbesondere besitzt die Null weder Links- noch Rechtsinverses. Triviale Ausnahme: Der Ring besteht nur aus einem Element 0, das zugleich Einselement und sein eigenes Inverses ist („Nullring").

5. Man beweise für beliebige kommutative Ringe durch vollständige Induktion nach n den *Binomialsatz*:

$$(a+b)^n = a^n + \binom{n}{1} a^{n-1}b + \binom{n}{2} a^{n-2}b^2 + \cdots + b^n$$

wo $\binom{n}{k}$ die ganze Zahl

$$\frac{n(n-1)\cdots(n-k+1)}{1 \cdot 2 \cdots k} = \frac{n!}{(n-k)!\,k!}$$

bedeutet.

6. In einem Ring mit genau n Elementen ist für jedes a:

$$n \cdot a = 0\,.$$

[Vgl. § 7, S. 27, unten.]

7. Ist a mit b vertauschbar, d. h. ist $ab = ba$, so ist a auch mit $-b$, mit nb und mit b^{-1} vertauschbar. Ist a mit b und c vertauschbar, so auch mit $b + c$ und mit bc.

Körper. Ein Ring heißt *Körper* oder *Rationalitätsbereich*, wenn

a) er mindestens ein von Null verschiedenes Element enthält,

b) die Gleichungen

$$(3)\qquad \begin{cases} ax = b\,, \\ ya = b \end{cases}$$

für $a \neq 0$ stets lösbar sind.

Genau wie bei Gruppen (Kap. 2) beweist man aus a) und b):

c) die Existenz eines links-Einselements e. Man löse nämlich für irgend ein $a \neq 0$ die Gleichung $xa = a$ und nenne die Lösung e. Ist nun b beliebig, so löse man $ax = b$; es folgt

$$eb = eax = ax = b\,.$$

Ebenso folgt die Existenz eines rechts-Einselements, also *die Existenz eines Einselementes* überhaupt.

Weiter folgt aus c) sofort:

d) die Existenz eines Linksinversen a^{-1} zu jedem $a \neq 0$

und ebenso die eines Rechtsinversen, also *die Existenz des inversen Elements* überhaupt.

Wie bei Gruppen zeigt man weiter, daß *aus c) und d) umgekehrt b) folgt.*

Aufgabe. 8. Man führe den Beweis durch.

Ein Körper hat keine Nullteiler; denn aus $ab = 0$, $a \neq 0$ folgt durch Multiplikation mit a^{-1} sofort $b = 0$.

Die Gleichungen (3) *sind eindeutig lösbar*; denn aus der Existenz zweier Lösungen x, x' etwa der ersten Gleichung würde folgen

$$ax = ax',$$

also durch Multiplikation mit a^{-1} von links:

$$x = x'.$$

Die Lösungen von (3) lauten natürlich:

$$x = a^{-1}b\,,$$

$$y = ba^{-1}.$$

Im kommutativen Fall wird $a^{-1}b = ba^{-1}$; man schreibt dafür auch $\frac{b}{a}$.

Die von Null verschiedenen Elemente eines Körpers bilden gegenüber der Multiplikation eine Gruppe: *die multiplikative Gruppe des Körpers.*

Ein Körper vereinigt also in sich zwei Gruppen: die multiplikative und die additive. Die beiden sind durch die Distributivgesetze verknüpft.

Wir werden uns in den nächstfolgenden Kapiteln fast ausschließlich mit kommutativen Körpern beschäftigen.

Beispiele. 1. Die rationalen Zahlen, die reellen Zahlen, die komplexen Zahlen bilden kommutative Körper.

2. Einen Körper aus nur zwei Elementen 0 und 1 konstruiert man folgendermaßen: Man multipliziere die Elemente wie die Zahlen 0 und 1. Für die Addition soll die 0 das Nullelement sein:

$$0 + 0 = 0,\ 0 + 1 = 1 + 0 = 1;$$

weiter sei $1 + 1 = 0$. Die Additionsregel ist dieselbe wie die Zusammensetzungsregel einer zyklischen Gruppe mit zwei Elementen (§ 7); also gelten die Gesetze der Addition. Die Gesetze der Multiplikation

gelten, weil sie für die gewöhnlichen Zahlen 0 und 1 ja gelten. (Die Multiplikation ist kommutativ.) Das erste Distributivgesetz beweist man durch Aufzählung aller Möglichkeiten: Sobald eine Null darin vorkommt, wird es trivial; also bleibt nur zu verifizieren

$$1 \cdot (1 + 1) = 1 \cdot 1 + 1 \cdot 1 ,$$

und das führt auf $0 = 0$. Schließlich ist die Gleichung $1 \cdot x = a$ für jedes a lösbar: die Lösung lautet $x = a$.

Aufgaben. 9. Man konstruiere einen Körper mit drei Elementen. [Man diskutiere zuerst, welche Struktur die additive und die multiplikative Gruppe haben können.]

10. Ein Integritätsbereich mit endlichvielen Elementen ist ein Körper. (Vgl. den entsprechenden Gruppensatz in Kap. 2, § 6.)

Interessante Beispiele von Ringen liefern die *hyperkomplexen Zahlensysteme*, von denen wir im II. Band noch ausführlicher reden werden. Man gehe aus von einem kommutativen Ring K mit Einselement, z. B. von dem Ring der ganzen oder der rationalen Zahlen, und bilde alle möglichen Reihen $(\alpha_1, \ldots, \alpha_n)$ von n mit Nummern versehenen Elementen von K. Für diese Reihen, auch „Vektoren" genannt, wird eine Addition festgelegt durch:

$$(\alpha_1, \alpha_2, \ldots, \alpha_n) + (\beta_1, \beta_2, \ldots, \beta_n) = (\alpha_1 + \beta_1, \ldots, \alpha_n + \beta_n) .$$

Diese genügt offensichtlich allen Gesetzen der Addition. Weiter wird eine Multiplikation erklärt, zunächst nicht für zwei Vektoren, sondern für ein Element von K und einen Vektor:

$$\gamma \cdot (\alpha_1, \alpha_2, \ldots, \alpha_n) = (\gamma\,\alpha_1, \gamma\,\alpha_2, \ldots, \gamma\,\alpha_n) .$$

Diese Multiplikation ist nach beiden Richtungen hin distributiv. Sodann definiert man die „Basiselemente":

$$\begin{aligned} (1, 0, \ldots, 0) &= i_1 \\ (0, 1, \ldots, 0) &= i_2 \\ &\cdots\cdots\cdots \\ (0, 0, \ldots, 1) &= i_n \end{aligned}$$

und kann dann alle Vektoren eindeutig durch die Basiselemente ausdrücken:

$$(\alpha_1, \alpha_2, \ldots, \alpha_n) = \alpha_1 i_1 + \cdots + \alpha_n i_n .$$

Nun werde eine Multiplikation für die Größen $(\alpha_1, \ldots, \alpha_n)$ definiert, und zwar zunächst für die Basiselemente:

$$i_\lambda i_\mu = \sum_\nu c_{\lambda\mu}^\nu i_\nu$$

(wo die n^3 Koeffizienten $c_{\lambda\mu}^\nu$ Elemente von K sind); sodann für die „skalaren Vielfachen" βi_λ so, daß die Elemente β von K mit den i_λ vertauschbar sind:

$$\beta i_\lambda \cdot \gamma i_\mu = \beta\gamma i_\lambda i_\mu = \sum_\nu \beta\gamma\, c_{\lambda\mu}^\nu i_\nu$$

und schließlich für die Summen $\Sigma \alpha_\nu i_\nu$ so, wie es die Distributivgesetze nahelegen:

$$\begin{aligned} \Big(\sum_\lambda \alpha_\lambda i_\lambda\Big)\Big(\sum_\mu \beta_\mu i_\mu\Big) &= \sum_\lambda \sum_\mu \alpha_\lambda \beta_\mu i_\lambda i_\mu \\ &= \sum_\nu \Big(\sum_\lambda \sum_\mu \alpha_\lambda \beta_\mu c_{\lambda\mu}^\nu\Big) i_\nu . \end{aligned}$$

Daß bei dieser Definition die beiden Distributivgesetze tatsächlich gelten, ist leicht zu sehen. Damit nun auch das Assoziativgesetz für die Multiplikation gelte, genügt es, daß dieses Gesetz für die Basiselemente gilt (aus denen sich ja alle anderen linear zusammensetzen mit Koeffi), also daß

$$i_\lambda (i_\mu i_\nu) = (i_\lambda i_\mu) i_\nu .$$

Das ist die einzige Bedingung, welche die Koeffizienten $c_{\lambda\mu}^{\nu}$ zu erfüllen haben, damit die Größen $(\alpha_1, \ldots, \alpha_n)$ einen Ring bilden. Diese Größen nennt man, wenn ihre Multiplikation durch Wahl der $c_{\lambda\mu}^{\nu}$ festgelegt ist, *hyperkomplexe Zahlen*, ihre Gesamtheit ein *hyperkomplexes System* (englisch: a linear associative algebra).

Einen Spezialfall bildet die gewöhnliche Definition der komplexen Zahlen als Paare reeller Zahlen; hier ist $n = 2$, die Basiselemente heißen 1, i und die Multiplikation wird durch

$$1 \cdot 1 = 1, \qquad 1 \cdot i = i,$$
$$i \cdot 1 = i, \qquad i \cdot i = -1$$

festgelegt. Die Bezeichnung des ersten Basiselementes rechtfertigt sich dadurch, daß die 1 tatsächlich das Einselement des Ringes darstellt. Die Zahlen $a \cdot 1$ werden mit den reellen Zahlen a identifiziert (vgl. hierzu § 11, Schluß).

Ist K nicht der Körper der reellen, sondern der der rationalen Zahlen, so heißen die komplexen Zahlen $a \cdot 1 + b \cdot i$ auch *„Gaußsche Zahlen"*; ist K der Ring der ganzen Zahlen, so spricht man von *„ganzen Gaußschen Zahlen"*.

Aufgaben. 11. Man zeige, daß die Gaußschen Zahlen einen Körper, die ganzen Gaußschen Zahlen einen Integritätsbereich bilden.

12. Die „Quaternionen" sind hyperkomplexe Zahlen mit 4 Basiselementen $1, j, k, l$, von denen das erste Einselement sein soll, während für die übrigen die Multiplikation durch

$$jj = kk = ll = -1;$$
$$jk = l; \qquad kj = -l;$$
$$kl = j; \qquad lk = -j;$$
$$lj = k; \qquad jl = -k.$$

Zu beweisen, daß die Quaternionen einen nichtkommutativen Körper bilden, wenn als Grundbereich K etwa der Körper der rationalen Zahlen genommen wird.

[Man beweise zunächst das Assoziativgesetz, sodann die Existenz des Inversen mittels der Beziehung:

$$(a1 + bj + ck + dl)(a1 - bj - ck - dl) = a^2 + b^2 + c^2 + d^2.]$$

13. Das Assoziativgesetz ist stets erfüllt, wenn man für die i_λ die Elemente einer endlichen Gruppe nimmt. (Der so entstehende Ring heißt „Gruppenring", „Gruppenalgebra" oder „System der Gruppenzahlen".)

§ 11. Homomorphie und Isomorphie.

Es seien $\mathfrak{S}$, $\overline{\mathfrak{S}}$ Systeme mit doppelter Komposition, und es sei $\mathfrak{S}$ auf $\overline{\mathfrak{S}}$ abgebildet, so daß jedem a aus $\mathfrak{S}$ ein $\bar{a}$ aus $\overline{\mathfrak{S}}$ zugeordnet ist und jedes $\bar{a}$ aus $\overline{\mathfrak{S}}$ umgekehrt mindestens einem a aus $\mathfrak{S}$ zugeordnet ist. Die Abbildung heißt ein *Homomorphismus* (oder mehrstufiger Isomorphismus), wenn aus $a \to \bar{a}$ und $b \to \bar{b}$ immer folgt

$$a + b \to \bar{a} + \bar{b}$$

und

$$a \cdot b \to \bar{a} \cdot \bar{b}\,.$$

$\overline{\mathfrak{S}}$ heißt dann ein *homomorphes Bild* von $\mathfrak{S}$. Zeichen: $\mathfrak{S} \sim \overline{\mathfrak{S}}$.

Ist die Abbildung außerdem eineindeutig, d. h. gehört jedes $\bar{a}$ zu genau einem a, so heißt sie ein *Isomorphismus* (auch: 1-Isomorphismus oder einstufiger Isomorphismus). Zeichen: $\mathfrak{S} \cong \overline{\mathfrak{S}}$. Die Systeme $\mathfrak{S}$, $\overline{\mathfrak{S}}$ heißen dann 1-*isomorph*. Die Relation $\mathfrak{S} \cong \overline{\mathfrak{S}}$ ist reflexiv, transitiv und, da die inverse Abbildung zu einem 1-Isomorphismus wieder ein 1-Isomorphismus ist, auch symmetrisch.

Das homomorphe Bild eines Ringes ist wieder ein Ring.

Beweis: Es sei $\mathfrak{R}$ ein Ring, $\overline{\mathfrak{R}}$ ein System mit doppelter Komposition und $\mathfrak{R} \sim \overline{\mathfrak{R}}$. Wir haben zu zeigen, daß $\overline{\mathfrak{R}}$ wieder ein Ring ist. Der Beweis verläuft wie bei Gruppen (§ 9) folgendermaßen:

Sind $\bar{a}, \bar{b}, \bar{c}$ irgend drei Elemente von $\overline{\mathfrak{R}}$ und will man irgend eine Rechnungsregel beweisen, etwa $\bar{a}(\bar{b} + \bar{c}) = \bar{a}\bar{b} + \bar{a}\bar{c}$, so sucht man zu $\bar{a}, \bar{b}, \bar{c}$ drei Urbilder a, b, c. Da $\mathfrak{R}$ ein Ring ist, so ist $a(b+c) = ab + ac$, und daraus folgt wegen der Homomorphie $\bar{a}(\bar{b} + \bar{c}) = \bar{a}\bar{b} + \bar{a}\bar{c}$. Ebenso verfährt man bei allen Assoziativ-, Kommutativ- und Distributivgesetzen. Will man die Lösbarkeit der Gleichung $\bar{a} + \bar{x} = \bar{b}$ beweisen, so suche man wieder Urbilder a, b, löse $a + x = b$ und hat dann wegen der Homomorphie $\bar{a} + \bar{x} = \bar{b}$.

Dem Nullelement 0 *von* $\mathfrak{R}$ *und dem entgegengesetzten Element* $-a$ *irgendeines Elements* a *entsprechen bei einer Homomorphie wieder Nullelement und entgegengesetztes Element in* $\overline{\mathfrak{R}}$. *Hat* $\mathfrak{R}$ *ein Einselement* e, *so entspricht diesem das Einselement in* $\overline{\mathfrak{R}}$.

Beweis wie bei Gruppen:

$$\begin{array}{llllll} \text{Aus} & a + 0 = a & \text{folgt} & \bar{a} + \bar{0} = \bar{a}; \\ \text{aus} & -a + a = 0 & \text{folgt} & -a + \bar{a} = \bar{0}; \\ \text{aus} & a\,e = a & \text{folgt} & \bar{a}\,\bar{e} = \bar{a}. \end{array}$$

Ist $\mathfrak{R}$ kommutativ, so ist offenbar $\overline{\mathfrak{R}}$ es auch.

Ist $\mathfrak{R}$ ein Integritätsbereich, so braucht $\overline{\mathfrak{R}}$ es nicht zu sein, wie wir später sehen werden; auch kann $\overline{\mathfrak{R}}$ ein Integritätsbereich sein, ohne daß $\mathfrak{R}$ es ist. Ist aber die Abbildung 1-isomorph, so übertragen sich selbstverständlich alle algebraischen Eigenschaften von $\mathfrak{R}$ auf $\overline{\mathfrak{R}}$. Daraus folgt:

Das 1-*isomorphe Bild eines Integritätsbereichs bzw. eines Körpers ist wieder ein Integritätsbereich bzw. ein Körper.*

Ein an dieser Stelle fast trivial erscheinender Satz, der uns aber in der Folge wichtige Dienste erweisen wird, ist der folgende:

Es seien $\mathfrak{R}$ *und* $\mathfrak{S}'$ *zwei zueinander fremde Ringe.* $\mathfrak{S}'$ *enthalte einen zu* $\mathfrak{R}$ 1-*isomorphen Unterring* $\mathfrak{R}'$. *Dann gibt es auch einen Ring* $\mathfrak{S} \cong \mathfrak{S}'$, *der* $\mathfrak{R}$ *selbst umfaßt.*

Beweis: Wir werfen aus $\mathfrak{S}'$ die Elemente von $\mathfrak{R}'$ hinaus und ersetzen sie durch die ihnen im 1-Isomorphismus entsprechenden Elemente von $\mathfrak{R}$. Wir definieren nun die Summen und Produkte für die unersetzten und ersetzten Elemente so, daß sie genau den Summen und Produkten in $\mathfrak{S}'$ entsprechen. (Ist z. B. vor der Ersetzung $a'b' = c'$, und wird a' ersetzt durch a, während b' und c' durch die Ersetzung unberührt bleiben, so definiere man: $ab' = c'$.) In der Weise entsteht aus $\mathfrak{S}'$ ein Ring $\mathfrak{S} \cong \mathfrak{S}'$, der in der Tat $\mathfrak{R}$ umfaßt.

Aufgabe. Man beweise mit Hilfe dieses Satzes, daß man in einem hyperkomplexen System mit Einselement e (§ 10, Schluß) den Ring der Vielfachen αe (α e K) durch den Grundbereich K selbst ersetzen kann.

§ 12. Quotientenbildung.

Ist ein kommutativer Ring $\mathfrak{R}$ in einen Körper Ω eingebettet[1], so kann man in Ω aus den Elementen von $\mathfrak{R}$ Quotienten

$$\frac{a}{b} = a\,b^{-1} = b^{-1}\,a \quad (b \neq 0)^{2}$$

bilden. Für sie gelten die folgenden Rechnungsregeln:

$$(1) \qquad \begin{cases} \dfrac{a}{b} = \dfrac{c}{d} \text{ dann und nur dann, wenn } a\,d = b\,c; \\ \dfrac{a}{b} + \dfrac{c}{d} = \dfrac{a\,d + b\,c}{b\,d}; \\ \dfrac{a}{b} \cdot \dfrac{c}{d} = \dfrac{a\,c}{b\,d}. \end{cases}$$

Zum Beweise überlege man sich, daß beide Seiten jedesmal nach Multiplikation mit bd dasselbe ergeben und daß aus $bdx = bdy$ folgt $x = y$.

Man sieht also, daß die Quotienten $\frac{a}{b}$ einen kommutativen Körper P bilden, den man den *Quotientenkörper* des kommutativen Ringes $\mathfrak{R}$ nennt. Weiter ersieht man aus den Regeln (1), daß die Art, wie man Brüche vergleicht, addiert und multipliziert, bekannt ist, sobald man diese Operationen für ihre Zähler und Nenner, also für die Elemente von $\mathfrak{R}$, ausführen kann. D. h. die Struktur des Quotientenkörpers P ist durch die von $\mathfrak{R}$ völlig bestimmt, oder: *Quotientenkörper von* 1-*isomorphen Ringen sind* 1-*isomorph.* Insbesondere sind je zwei Quotienten-

[1] Ω braucht nicht kommutativ zu sein.

[2] Aus $ab = ba$ folgt nämlich $ab^{-1} = b^{-1}a$, indem man von links und von rechts mit b^{-1} multipliziert.

körper eines einzigen Ringes stets 1-isomorph, oder: *Der Quotientenkörper* P *ist durch den Ring* $\mathfrak{R}$ *bis auf Isomorphie eindeutig bestimmt, wenn es überhaupt einen Quotientenkörper zum Ring* $\mathfrak{R}$ *gibt.*

Wir fragen nun: Welche kommutativen Ringe besitzen einen Quotientenkörper? Oder, was auf dasselbe hinauskommt, welche lassen sich überhaupt in einen Körper einbetten?

Damit ein Ring $\mathfrak{R}$ in einen Körper eingebettet werden kann, ist zunächst notwendig, daß es in $\mathfrak{R}$ keine Nullteiler gibt; denn ein Körper hat keine Nullteiler. Diese Bedingung ist nun im kommutativen Fall auch hinreichend: *Jeder Integritätsbereich* $\mathfrak{R}$ *läßt sich in einen Körper einbetten.*

Beweis: Wir können von dem trivialen Fall, daß $\mathfrak{R}$ nur aus einem Nullelement besteht, absehen. Wir betrachten die Menge aller Elementpaare (a, b), wo $b \neq 0$ ist. Diesen Paaren sollen nachher Brüche $\frac{a}{b}$ zugeordnet werden.

Wir setzen $(a, b) \sim (c, d)$, wenn $ad = bc$. (Vgl. die früheren Formeln (1).) Die so definierte Relation $\sim$ ist offenbar reflexiv und symmetrisch; sie ist auch transitiv, denn aus

$$(a, b) \sim (c, d), \qquad (c, d) \sim (e, f)$$

folgt

$$ad = bc, \qquad cf = de,$$

also

$$adf = bcf = bde,$$

also wegen $d \neq 0$ und der Kommutativität von $\mathfrak{R}$:

$$af = be,$$

$$(a, b) \sim (e, f).$$

Die Relation $\sim$ hat also alle Eigenschaften einer Äquivalenzrelation; sie definiert somit nach Kap. 1, § 5 eine Klasseneinteilung für die Paare (a, b), indem äquivalente Paare zur selben Klasse gerechnet werden. Die Klasse, in der (a, b) liegt, sei durch das Symbol $\frac{a}{b}$ dargestellt. Zufolge dieser Definition ist $\frac{a}{b} = \frac{c}{d}$ dann und nur dann, wenn $(a, b) \sim (c, d)$, also wenn $ad = bc$.

Entsprechend der früheren Formel (1) *definieren* wir nun Summe und Produkt der neuen Symbole $\frac{a}{b}$ durch:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \tag{2}$$

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}. \tag{3}$$

Die Definitionen sind zulässig; denn *erstens* ist $bd \neq 0$, wenn $b \neq 0$ und $d \neq 0$, also sind $\frac{ad+bc}{bd}$ und $\frac{ac}{bd}$ erlaubte Symbole; *zweitens* sind die rechten Seiten unabhängig von der Wahl der Repräsentanten (a, b) und (c, d) der Klassen $\frac{a}{b}$ und $\frac{c}{d}$. Ersetzt man nämlich in (2) a und b durch a' und b', wo

$$ab' = ba',$$

so folgt

$$adb' = a'db,$$

$$adb' + bcb' = a'db + b'cb,$$

$$(ad + bc)b'd = (a'd + b'c)bd,$$

also

$$\frac{ad+bc}{bd} = \frac{a'd+b'c}{b'd}.$$

Ebenso:

$$ab' = ba',$$

$$acb'd = a'cbd,$$

$$\frac{ac}{bd} = \frac{a'c}{b'd}.$$

Entsprechendes gilt bei Ersetzung von (c, d) durch (c', d'), wo $cd' = dc'$ ist.

Man zeigt ohne Mühe, daß alle Körpereigenschaften erfüllt sind. Das Assoziativgesetz der Addition z. B. ergibt sich so:

$$\frac{a}{b} + \left(\frac{c}{d} + \frac{e}{f}\right) = \frac{a}{b} + \frac{cf+de}{df} = \frac{adf+bcf+bde}{bdf},$$

$$\left(\frac{a}{b} + \frac{c}{d}\right) + \frac{e}{f} = \frac{ad+bc}{bd} + \frac{e}{f} = \frac{adf+bcf+bde}{bdf},$$

und alle anderen Gesetze dementsprechend.

Der konstruierte Körper ist offenbar kommutativ. Um zu erreichen, daß er den Ring $\mathfrak{R}$ umfaßt, müssen wir gewisse Brüche mit Elementen von $\mathfrak{R}$ identifizieren. Das geschieht folgendermaßen:

Wir ordnen dem Element c alle Brüche $\frac{cb}{b}$ zu, wo $b \neq 0$ ist. Diese Brüche sind sämtlich gleich:

$$\frac{cb}{b} = \frac{cb'}{b'} \text{ wegen } (cb)b' = b(cb').$$

Jedem Element c wird also nur *ein* Bruch zugeordnet. Verschiedenen Elementen c, c' werden aber auch verschiedene Brüche zugeordnet; denn aus

$$\frac{cb}{b} = \frac{c'b'}{b'}$$

folgt

$$cbb' = bc'b'$$

oder wegen $b \neq 0$, $b' \neq 0$, da man kürzen kann:

$$c = c'.$$

Also sind den Elementen von $\mathfrak{R}$ eineindeutig gewisse Brüche zugeordnet.

Ist $c_1 + c_2 = c_3$ oder $c_1 c_2 = c_3$ in $\mathfrak{R}$, so folgt daraus für beliebige $b_1 \neq 0$, $b_2 \neq 0$ und $b_3 = b_1 b_2$:

$$\frac{c_1 b_1}{b_1} + \frac{c_2 b_2}{b_2} = \frac{c_1 b_1 b_2 + c_2 b_1 b_2}{b_1 b_2} = \frac{c_3 b_3}{b_3}$$

bzw.

$$\frac{c_1 b_1}{b_1} \cdot \frac{c_2 b_2}{b_2} = \frac{c_1 c_2 b_1 b_2}{b_1 b_2} = \frac{c_3 b_3}{b_3}.$$

Die zugeordneten Brüche $\frac{c_i b_i}{b_i}$ addieren und multiplizieren sich also genau so wie die Ringelemente c_i: sie bilden einen zu $\mathfrak{R}$ isomorphen Bereich. Demnach können wir die Brüche $\frac{c\,b}{b}$ durch die entsprechenden Elemente c ersetzen (§ 11, Schluß). Dadurch erreichen wir, daß der Körper den Ring $\mathfrak{R}$ umfaßt.

Damit ist die Existenz eines umfassenden Körpers zu jedem Integritätsbereich $\mathfrak{R}$ bewiesen.

Die Möglichkeit der Einbettung nichtkommutativer Ringe ohne Nullteiler in einen sie umfassenden Körper bildet ein ungelöstes Problem, außer in ganz speziellen Fällen.

Die Quotientenbildung ist das erste Hilfsmittel, aus Ringen andere Ringe (in casu Körper) zu bilden. Sie erzeugt z. B. aus dem Ring C der gewöhnlichen ganzen Zahlen den Körper Γ der rationalen Zahlen.

Aufgabe. Man zeige, daß jeder kommutative Ring $\mathfrak{R}$ (mit oder ohne Nullteiler) sich in einen „Quotientenring" einbetten läßt, bestehend aus allen Quotienten $\frac{a}{b}$, wo b alle Nichtnullteiler durchläuft. Allgemeiner kann man b irgendeine Menge $\mathfrak{M}$ von Nichtnullteilern durchlaufen lassen, die zu je zwei Elementen b_1, b_2 auch das Produkt $b_1 b_2$ enthält, und bekommt so einen Quotientenring $\mathfrak{R}_{\mathfrak{M}}$.

§ 13. Polynomringe.

Es sei $\mathfrak{R}$ ein Ring. Wir bilden mit einem neuen, d. h. nicht zu $\mathfrak{R}$ gehörigen Symbol x die Ausdrücke

$$f(x) = \sum a_\nu x^\nu,$$

wo über endlichviele verschiedene ganzzahlige $\nu \geqq 0$ summiert wird, und wo die „Koeffizienten" a_ν dem Ring $\mathfrak{R}$ angehören; z. B.:

$$f(x) = a_0 x^0 + a_3 x^3 + a_5 x^5.$$

Diese Ausdrücke heißen *Polynome*; das Symbol x heißt eine *Unbestimmte*. Eine Unbestimmte ist also nichts als ein Rechensymbol. Zwei Polynome heißen dann und nur dann gleich, wenn sie, abgesehen von

Gliedern mit dem Koeffizienten Null, die beliebig weggelassen oder hingeschrieben werden dürfen, genau dieselben Glieder enthalten.

Wenn man nach den gewöhnlichen Regeln der Buchstabenrechnung zwei Polynome $f(x)$, $g(x)$ addiert oder multipliziert, dabei x als vertauschbar mit den Ringelementen betrachtet ($ax = xa$) und die Glieder mit derselben Potenz von x zusammenfaßt, so kommt ein Polynom $\sum c_\nu x^\nu$ heraus. Im Falle der Addition ist

$$c_\nu = a_\nu + b_\nu \tag{1}$$

(wobei $a_\nu = 0$ oder $b_\nu = 0$ zu setzen ist, falls a_ν oder b_ν fehlt), und im Falle der Multiplikation ist

$$c_\nu = \sum_{\sigma+\tau=\nu} a_\sigma b_\tau . \tag{2}$$

Durch die Formeln (1), (2) *definieren* wir nun Summe und Produkt zweier Polynome[1] und behaupten:

Die Polynome bilden einen Ring.

Die Eigenschaften der Addition sind ohne weiteres klar, da diese ja auf die Addition der Koeffizienten a_ν, b_ν zurückgeführt ist. Das erste Distributivgesetz folgt aus

$$\sum_{\sigma+\tau=\nu} a_\sigma (b_\tau + c_\tau) = \sum_{\sigma+\tau=\nu} a_\sigma b_\tau + \sum_{\sigma+\tau=\nu} a_\sigma c_\tau ,$$

und entsprechend ergibt sich das zweite. Das Assoziativgesetz der Multiplikation ergibt sich schließlich aus

$$\sum_{\alpha+\tau=\nu} a_\alpha \Big(\sum_{\beta+\gamma=\tau} b_\beta c_\gamma \Big) = \sum_{\alpha+\beta+\gamma=\nu} a_\alpha b_\beta c_\gamma ,$$

$$\sum_{\varrho+\gamma=\nu} \Big(\sum_{\alpha+\beta=\varrho} a_\alpha b_\beta \Big) c_\gamma = \sum_{\alpha+\beta+\gamma=\nu} a_\alpha b_\beta c_\gamma .$$

Man bezeichnet den aus $\mathfrak{R}$ abgeleiteten Polynomring mit $\mathfrak{R}[x]$. Ist $\mathfrak{R}$ kommutativ, so ist $\mathfrak{R}[x]$ es auch.

---

[1] Man könnte gegen die hier gegebene Definition der Polynome noch einwenden, daß im Symbol

$$\sum_\nu a_\nu x^\nu$$

das Summenzeichen benutzt wird, noch bevor die Addition definiert ist. Um diesem Einwand zu begegnen, kann man zunächst unter einem Polynom irgend ein ganz neutrales Symbol verstehen, wie z. B.

$$(a_0, \ldots, a_\lambda, \ldots, a_n),$$

in dem gewisse Elemente von $\mathfrak{R}$ mit Indices versehen vorkommen, und dann Summe und Produkt durch (1) und (2) definieren. Führt man dann nachher für $(0, \ldots, 0, a_\nu, 0, \ldots)$ die andere Schreibweise $a_\nu x^\nu$ ein, so wird $(a_0, \ldots, a_\lambda, \ldots, a_n) = \sum_0^n a_\nu x^\nu$ nach der Summendefinition. Der Exponent und das Produkt in $a_\nu x^\nu$ sind rein symbolisch zu nehmen und bedeuten keine wirkliche Multiplikation, da die Unbestimmte x und die Potenz x^ν vielleicht gar nicht dem Polynomring $\mathfrak{R}[x]$ angehören ($\mathfrak{R}$ kann ein Ring ohne Einselement sein!) und die Multiplikation daher für diese Größen nicht definiert ist.

Der *Grad* eines von Null verschiedenen Polynoms ist die größte Zahl ν, für die $a_\nu \neq 0$ ist. Dieses a_ν heißt der *Anfangskoeffizient* oder der *höchste Koeffizient.*

Polynome vom nullten Grad haben die Form $a_0 x^0$. Diese Polynome identifizieren wir mit den Elementen a_0 des Grundrings $\mathfrak{R}$, was erlaubt ist, da sie sich genau so addieren und multiplizieren, mithin einen zum Grundring $\mathfrak{R}$ 1-isomorphes System bilden (vgl. § 11, Schluß). Der Polynomring $\mathfrak{R}[x]$ umfaßt also $\mathfrak{R}$.

Den Übergang von $\mathfrak{R}$ zu $\mathfrak{R}[x]$ nennt man auch *Adjunktion* (und zwar Ringadjunktion) *einer Unbestimmten* x.

Adjungiert man einem Ring $\mathfrak{R}$ sukzessive die Unbestimmten $x_1, \ldots, x_n$, bildet also $\mathfrak{R}[x_1][x_2]\ldots[x_n]$, so entsteht der Polynomring $\mathfrak{R}[x_1, \ldots, x_n]$, bestehend aus allen Summen

$$\sum a_{\alpha_1 \ldots \alpha_r} x_1^{\alpha_1} \ldots x_r^{\alpha_r}.$$

Schreibt man die Rechenregeln für diese Summen auf, so sieht man, daß die Unbestimmten miteinander vertauschbar sind und daher der entstehende Ring von der Reihenfolge der n Adjunktionen unabhängig ist. Man nennt $\mathfrak{R}[x_1, \ldots, x_n]$ einen *Polynomring in mehreren Unbestimmten.*

Ist insbesondere $\mathfrak{R}$ der Ring der ganzen Zahlen, so spricht man von *ganzzahligen Polynomen.*

Der Nutzen der Polynome besteht im kommutativen Fall darin, daß man für die Unbestimmten x beliebige Ringelemente (aus $\mathfrak{R}$ oder aus einem kommutativen Ring, der $\mathfrak{R}$ umfaßt) einsetzen kann, ohne daß die Gültigkeit der Relationen $f + g = h$ und $f \cdot g = k$ zerstört wird. Das ergibt sich daraus, daß wir h und k nach den gewöhnlichen Gesetzen der Buchstabenrechnung definiert haben; diese gelten ja auch, wenn x durch ein Ringelement ersetzt wird[1]. Das Ringelement, das aus $f(x)$ durch die Einsetzung $x = \alpha$ entsteht, wird mit $f(\alpha)$ bezeichnet. In dieser Bezeichnung werden die Polynome $f(x)$ als *ganze rationale Funktionen* der *„Variablen" x* aufgefaßt; dementsprechend bezeichnet man die Elemente von $\mathfrak{R}$ auch als *Konstante.* Alles Gesagte gilt natürlich auch für Polynome in mehreren Unbestimmten.

Bei den ganzzahligen Polynomen ohne konstantes Glied geht die Einsetzungsmöglichkeit noch weiter: man kann für x eine Größe irgend eines Ringes einsetzen, mag der Ring nun den der ganzen Zahlen umfassen oder nicht.

Ist $\mathfrak{R}$ ein Integritätsbereich, so ist $\mathfrak{R}[x]$ auch ein Integritätsbereich.

Beweis: Ist $f(x) \neq 0$ und $g(x) \neq 0$ und ist a_α der höchste (von Null verschiedene) Koeffizient in $f(x)$ und ebenso b_β der höchste

[1] Im nichtkommutativen Fall gilt das nicht, da wir x als vertauschbar mit den Elementen von $\mathfrak{R}$ angenommen haben. Man hüte sich vor Irrtümern!

Koeffizient in $g(x)$, so ist $a_\alpha b_\beta \neq 0$ der Koeffizient von $x^{\alpha+\beta}$ in $f(x)\cdot g(x)$; daher ist $f(x)\cdot g(x) \neq 0$. Also sind keine Nullteiler vorhanden.

Aus dem Beweis ergibt sich noch der

Zusatz: *Ist $\mathfrak{R}$ ein Integritätsbereich, so ist der Grad von $f(x)\cdot g(x)$ die Summe der Gradzahlen von $f(x)$ und $g(x)$.*

Für Polynome von n Veränderlichen ergibt sich durch vollständige Induktion unmittelbar:

Ist $\mathfrak{R}$ ein Integritätsbereich, so ist auch $\mathfrak{R}[x_1, \ldots, x_n]$ ein Integritätsbereich.

Unter dem *Grad* eines Gliedes $a_{\alpha_1 \ldots \alpha_r} x_1^{\alpha_1} \ldots x_r^{\alpha_r}$ versteht man die Summe der Exponenten $\sum \alpha_i$. Unter dem Grad eines nichtverschwindenden Polynoms versteht man den größten der Grade der von Null verschiedenen Glieder. Ein Polynom heißt *homogen* oder eine *Form*, wenn alle Glieder den gleichen Grad haben. Produkte von homogenen Polynomen sind wieder homogen, und der Grad des Produkts ist, falls $\mathfrak{R}$ ein Integritätsbereich, gleich der Summe der Gradzahlen der Faktoren.

Inhomogene Polynome lassen sich (eindeutig) als Summen von homogenen Bestandteilen verschiedenen Grades schreiben. Multipliziert man zwei solche Polynome f, g von den Gradzahlen m, n, so ist das Produkt der homogenen Bestandteile höchsten Grades, im Fall eines Integritätsbereichs $\mathfrak{R}$, eine nichtverschwindende Form vom Grade $m+n$. Alle übrigen Bestandteile von $f\cdot g$ haben niedrigeren Grad; daher ist der Grad von $f\cdot g$ wieder $m+n$. Der obige Gradsatz („Zusatz") gilt demnach auch für Polynome in beliebig vielen Unbestimmten.

Ist $\mathfrak{R}$ ein Ring mit Einselement (der wichtigste und interessanteste Fall), so enthält der Polynomring $\mathfrak{R}[x]$ insbesondere das Element $1x$, das kurz mit x bezeichnet wird. Seine Potenzen x^ν sind

$$x^\nu = (1x)^\nu = 1^\nu x^\nu = 1x^\nu$$

und das Produkt $a_\nu \cdot x^\nu$ ist:

$$(a_\nu x^0)(1x^\nu) = a_\nu x^\nu,$$

also werden die in der Definition des Polynoms $\sum a_\nu x^\nu$ vorkommenden „symbolischen" Potenzen und Produkte jetzt wirkliche Potenzen und Produkte von Polynomen.

Der Divisionsalgorithmus. Ist $\mathfrak{R}$ ein Ring mit Einselement 1, ist weiter

$$g(x) = \sum c_\nu x^\nu$$

ein Polynom, dessen höchster Koeffizient $c_n = 1$ ist, und

$$f(x) = \sum a_\nu x^\nu$$

ein beliebiges Polynom von einem Grade $m \geqq n$, so kann man den höchsten Koeffizienten a_m zum Verschwinden bringen, indem man von f ein Vielfaches von g, nämlich $a_m x^{m-n} g$, subtrahiert. Ist sodann der

Grad noch immer $\geqq n$, so kann man wieder den höchsten Koeffizienten zum Verschwinden bringen, indem man nochmals ein Vielfaches von g subtrahiert. So fortfahrend, drückt man schließlich den Grad des Restes unter n hinab und hat:

$$f - qg = r, \tag{3}$$

wo r einen kleineren Grad als g hat oder Null ist. Dieses Verfahren nennt man den *Divisionsalgorithmus*.

Ist insbesondere $\mathfrak{R}$ ein Körper und $g \neq 0$, so ist die Voraussetzung $c_n = 1$ überflüssig; denn dann kann man nötigenfalls g mit c_n^{-1} multiplizieren und so erzwingen, daß der höchste Koeffizient Eins wird.

Aufgabe. Sind $x, y, \ldots$ unendlichviele Symbole, so kann man die Gesamtheit aller $\mathfrak{R}$-Polynome in diesen Unbestimmten betrachten. Jedes Polynom darf aber nur endlichviele dieser Unbestimmten enthalten. Man beweise, daß auch der so definierte Bereich ein Ring bzw. Integritätsbereich ist, sobald $\mathfrak{R}$ einer ist.

§ 14. Ideale. Restklassenringe.

Es sei $\mathfrak{o}$ ein Ring.

Damit eine Untermenge von $\mathfrak{o}$ wieder ein Ring (*Unterring* von $\mathfrak{o}$) ist, ist notwendig und hinreichend, daß sie

1. eine Untergruppe der additiven Gruppe ist, m. a. W. zu a und b auch $a - b$ enthält[1] (*Moduleigenschaft*),

2. zu a und b auch ab enthält.

Unter den Unterringen spielen nun einige, die wir *Ideale* nennen, eine Sonderrolle, analog den Normalteilern in der Gruppentheorie.

Eine nichtleere Untermenge $\mathfrak{m}$ von $\mathfrak{o}$ heißt *Ideal* und zwar *Rechtsideal*, wenn

1. aus $a \in \mathfrak{m}$ und $b \in \mathfrak{m}$ folgt $a - b \in \mathfrak{m}$ (Moduleigenschaft),

2. aus $a \in \mathfrak{m}$, r beliebig in $\mathfrak{o}$ folgt $ar \in \mathfrak{m}$. In Worten: der Modul $\mathfrak{m}$ soll zu jedem a auch alle „*Rechtsvielfachen*“ $a \cdot r$ enthalten.

Ebenso heißt ein Modul $\mathfrak{m}$ *Linksideal*, wenn aus $a \in \mathfrak{m}$ für beliebiges r aus $\mathfrak{o}$ folgt $ra \in \mathfrak{m}$.

Schließlich heißt $\mathfrak{m}$ *zweiseitiges Ideal*, wenn $\mathfrak{m}$ sowohl Links- als auch Rechtsideal ist.

Für kommutative Ringe fallen alle drei Begriffe zusammen, und man redet von *Idealen* schlechthin. *In diesem Paragraphen wird weiterhin $\mathfrak{o}$ als kommutativer Ring vorausgesetzt.* Ideale werden immer mit kleinen deutschen Buchstaben bezeichnet.

Beispiele von Idealen:

1. Das *Nullideal*, das aus dem Nullelement allein besteht.

---

[1] Hieraus folgt schon, daß die Menge auch die Null und alle Summen $a + b$ enthält; vgl. § 7.

2. Das *Einheitsideal* $\mathfrak{o}$, das alle Größen des Ringes umfaßt.

3. Das *von einem Element a erzeugte Ideal* (a), das aus allen Ausdrücken der Gestalt

$$ra + na \qquad (r \in \mathfrak{o},\ n \text{ eine ganze Zahl})$$

besteht. Daß diese Menge stets ein Ideal ist, sieht man leicht ein: Die Differenz zweier solcher Ausdrücke hat offenbar wieder dieselbe Gestalt, und ein beliebiges Vielfaches hat die Form

$$s \cdot (ra + na) = (sr + ns) \cdot a,$$

also die Form $r'a$ oder $r'a + 0 \cdot a$.

Das Ideal (a) ist offenbar das kleinste (am wenigsten umfassende) Ideal, das a enthält; denn jedes solche Ideal muß mindestens alle Vielfachen ra und alle Summen $\pm \sum a = na$ enthalten, also auch alle Summen $ra + na$. Das Ideal (a) kann also auch definiert werden als der Durchschnitt aller Ideale, die a als Element enthalten.

Hat der Ring $\mathfrak{o}$ ein Einselement e, so kann man für $ra + na$ auch $ra + nea = (r + ne)a = r'a$ schreiben; *also besteht in diesem Falle* (a) *aus allen gewöhnlichen Vielfachen* ra. So besteht z. B. das Ideal (2) im Ring der ganzen Zahlen aus den geraden Zahlen.

Ein von einem Element a erzeugtes Ideal (a) heißt *Hauptideal*. Das Nullideal (0) ist immer Hauptideal; das Einheitsideal $\mathfrak{o}$ ist es auch, falls $\mathfrak{o}$ ein Einheitselement e besitzt, es ist dann nämlich $\mathfrak{o} = (e)$.

4. Das von mehreren Elementen $a_1, \ldots, a_n$ erzeugte Ideal kann ebenso definiert werden als Gesamtheit aller Summen der Gestalt

$$\sum r_i a_i + \sum n_j a_j$$

(bzw., wenn $\mathfrak{o}$ ein Einheitselement hat, $\sum r_i a_i$) oder als Durchschnitt aller Ideale von $\mathfrak{o}$, welche die Elemente $a_1, \ldots, a_n$ enthalten. Das Ideal wird mit $(a_1, \ldots, a_n)$ bezeichnet, und man sagt, daß $a_1, \ldots, a_n$ eine *Idealbasis* bilden.

5. Ebenso kann man das von einer unendlichen Menge $\mathfrak{M}$ erzeugte Ideal $(\mathfrak{M})$ definieren; es ist die Gesamtheit aller endlichen Summen der Gestalt

$$\sum r_i a_i + \sum n_j a_j \qquad (a_i \in \mathfrak{M},\ r_i \in \mathfrak{o},\ n_j \text{ ganze Zahlen}).$$

Restklassen. Ein Ideal $\mathfrak{m}$ in $\mathfrak{o}$ definiert, weil es Untergruppe der additiven Gruppe ist, eine Einteilung von $\mathfrak{o}$ in Nebenklassen oder *Restklassen* nach $\mathfrak{m}$. Zwei Elemente a, b heißen *kongruent nach* $\mathfrak{m}$ oder *kongruent modulo* $\mathfrak{m}$, wenn sie derselben Restklasse angehören, d. h. wenn $a - b \in \mathfrak{m}$ ist. Zeichen:

$$a \equiv b \pmod{\mathfrak{m}}$$

oder kurz

$$a \equiv b\,(\mathfrak{m}).$$

Für „a nicht kongruent b" schreibt man $a \not\equiv b$.

Ist $\mathfrak{m}$ speziell ein Hauptideal (m), so wäre statt $a \equiv b\,(\mathfrak{m})$ auch $a \equiv b\,((m))$ zu schreiben. In diesem Falle spart man indessen lieber ein Klammerpaar und schreibt einfach $a \equiv b\,(m)$.

Beispielsweise kommt man so auf die gewöhnliche Kongruenz nach einer ganzen Zahl: $a \equiv b\,(n)$ (sprich: a kongruent b modulo n) bedeutet, daß $a - b$ zu (n) gehört, d. h. ein Vielfaches von n ist.

Das Rechnen mit Kongruenzen. Eine Kongruenz $a \equiv b$ nach einem Ideal $\mathfrak{m}$ bleibt offensichtlich gültig, wenn man dasselbe Element c zu beiden Seiten addiert, oder wenn man beide Seiten mit c multipliziert. Daraus folgt weiter: Ist $a \equiv a'$ und $b \equiv b'$, so ist

$$a + b \equiv a + b' \equiv a' + b',$$
$$ab \equiv ab' \equiv a'b';$$

man darf also Kongruenzen zueinander addieren und miteinander multiplizieren.

Auch mit einer gewöhnlichen ganzen Zahl n darf man beide Seiten einer Kongruenz multiplizieren. Im Falle $n = -1$ ergibt sich insbesondere durch Kombination mit dem Vorigen, daß man Kongruenzen voneinander subtrahieren darf.

Man rechnet also mit Kongruenzen ganz wie mit Gleichungen. Nur kürzen darf man im allgemeinen nicht: im Bereich der ganzen Zahlen ist z. B.

$$15 \equiv 3\,(6);$$

aber trotzdem $3 \not\equiv 0\,(6)$ ist, kann man nicht auf $5 \equiv 1\,(6)$ schließen.

Aufgaben. 1. Man zeige, daß man im Ring der ganzen Zahlen die Restklassen nach einem Ideal (m) $(m > 0)$ durch die Zahlen $0, 1, \ldots, m-1$ repräsentieren, also mit $\mathfrak{R}_0, \mathfrak{R}_1, \ldots, \mathfrak{R}_{m-1}$ bezeichnen kann.

2. Welches Ideal erzeugen die Zahlen 10 und 13 zusammen im Ring der ganzen Zahlen?

3. Was heißt $a \equiv b\,(0)$?

4. Alle Vielfachen ra eines Elements a bilden ein Ideal $\mathfrak{o}a$. Man mache sich am Ring der geraden Zahlen klar, daß dieses Ideal nicht notwendig mit dem Hauptideal (a) übereinstimmt.

5. Man definiere auch für nichtkommutative Ringe das von einer beliebigen Menge erzeugte Rechtsideal bzw. Linksideal bzw. zweiseitige Ideal.

6. Welche Operationen mit Kongruenzen sind in nichtkommutativen Ringen erlaubt?

Die Ideale stehen in derselben Beziehung zum Begriff der Ringhomomorphie wie die Normalteiler zu dem der Gruppenhomomorphie. Gehen wir vom Homomorphiebegriff aus!

Ein Homomorphismus $\mathfrak{o} \sim \bar{\mathfrak{o}}$ zweier Ringe definiert eine Klasseneinteilung des Ringes $\mathfrak{o}$: eine Klasse $\mathfrak{K}_a$ wird gebildet von allen Elementen a, die dasselbe Bild $\bar{a}$ haben. Diese Klasseneinteilung können wir nun aber genauer charakterisieren:

Die Klasse $\mathfrak{n}$ *von* $\mathfrak{o}$, *der bei dem Homomorphismus* $\mathfrak{o} \sim \bar{\mathfrak{o}}$ *das Nullelement entspricht, ist ein Ideal in* $\mathfrak{o}$, *und die übrigen Klassen sind die Restklassen dieses Ideals.*

Beweis: Zunächst ist $\mathfrak{n}$ ein Modul. Denn wenn a und b beim Homomorphismus in Null übergehen, so geht auch $-b$ in Null über, also auch die Differenz $a - b$; mit a und b gehört also auch $a - b$ der Klasse $\mathfrak{n}$ an.

$\mathfrak{n}$ ist Ideal; denn wenn a in Null übergeht und r beliebig ist, so geht ra in $\bar{r} \cdot 0 = 0$ über, gehört also wieder zu $\mathfrak{n}$. (Im nichtkommutativen Fall ist $\mathfrak{n}$ sogar ein zweiseitiges Ideal.)

Die Elemente $a + c$ ($c \in \mathfrak{n}$) einer Restklasse nach $\mathfrak{n}$, deren Repräsentant das Element a ist, gehen über in $\bar{a} + 0$, also in $\bar{a}$, gehören also alle einer Klasse $\mathfrak{K}_a$ an. Wenn umgekehrt ein Element b in $\bar{a}$ übergeht, so geht $b - a$ in $\bar{a} - \bar{a} = 0$ über; also ist $b - a \in \mathfrak{n}$, und b liegt in derselben Restklasse wie a. Damit ist alles bewiesen.

So gehört also zu jedem Homomorphismus ein Ideal.

Wir kehren nun den Zusammenhang um: wir gehen von einem Ideal $\mathfrak{m}$ in $\mathfrak{o}$ aus und fragen, *ob es einen zu* $\mathfrak{o}$ *homomorphen Ring* $\bar{\mathfrak{o}}$ *gibt, so daß den Restklassen nach* $\mathfrak{m}$ *genau die Elemente von* $\bar{\mathfrak{o}}$ *entsprechen.*

Um einen solchen Ring zu konstruieren, verfahren wir wie in Kap. 2, § 9: wir wählen als Elemente des zu konstruierenden Rings einfach die Restklassen nach $\mathfrak{m}$, bezeichnen die Restklasse $a + \mathfrak{m}$ mit $\bar{a}$ und versuchen, eine Addition und eine Multiplikation für sie zu definieren, so daß die Zuordnung $a \to \bar{a}$ ein Homomorphismus ist. Wir müssen also zu je zwei Restklassen $\bar{a}$, $\bar{b}$ eine Summenklasse $\bar{a} + \bar{b}$ und eine Produktklasse $\bar{a} \cdot \bar{b}$ zu bestimmen versuchen, so daß alle Summen der Elemente von $\bar{a}$ mit denen von $\bar{b}$ in der Summenklasse, alle Produkte in der Produktklasse liegen.

Es sei also a irgend ein Element von $\bar{a}$, b eins von $\bar{b}$. Wir definieren versuchsweise $\bar{a} + \bar{b}$ als *die Klasse, in welcher* $a + b$ *liegt*, und $\bar{a} \cdot \bar{b}$ als *die Klasse, in welcher* $a \cdot b$ *liegt.* Ist $a' \equiv a$ irgend ein anderes Element von $\bar{a}$ und $b' \equiv b$ eins von $\bar{b}$, so ist nach dem vorigen

$$a' + b' \equiv a + b,$$
$$a' \cdot b' \equiv a \cdot b;^1$$

daher liegt $a' + b'$ in derselben Restklasse wie $a + b$, ebenso $a' \cdot b'$ in derselben wie $a \cdot b$. Unsere Definition von Summen- und Produkt-

[1] Alle Kongruenzen natürlich modulo $\mathfrak{m}$.

klasse ist also unabhängig von der Wahl der Elemente a, b innerhalb $\bar{a}$, $\bar{b}$. Diese Klassen $\bar{a}+\bar{b}$, $\bar{a}\cdot\bar{b}$ haben aber in der Tat die verlangten Eigenschaften, daß jede Summe $a'+b'$ in der Summenklasse $\bar{a}+\bar{b}$ und jedes Produkt $a'\cdot b'$ in der Produktklasse $\bar{a}\cdot\bar{b}$ liegt.

Jedem Element a entspricht eine Restklasse $\bar{a}$, und diese Zuordnung ist homomorph, da der Summe $a+b$ die Summe $\bar{a}+\bar{b}$ und dem Produkt ab ebenso $\bar{a}\bar{b}$ entspricht. Also bilden die Restklassen einen Ring (§ 11). Diesen Ring bezeichnen wir als den *Restklassenring* $\mathfrak{o}/\mathfrak{m}$ von $\mathfrak{o}$ nach dem Ideal $\mathfrak{m}$ oder von $\mathfrak{o}$ modulo $\mathfrak{m}$. Der Ring $\mathfrak{o}$ ist auf $\mathfrak{o}/\mathfrak{m}$ mittels des angegebenen Zuordnungsverfahrens homomorph abgebildet. Das Ideal $\mathfrak{m}$ spielt bei diesem Homomorphismus genau die Rolle des obigen $\mathfrak{n}$; es ist ja identisch mit der Menge aller Elemente, deren Restklasse die Nullklasse ist.

Wir sehen hier die prinzipielle Wichtigkeit der Ideale: sie ermöglichen die Konstruktion homomorpher Ringe zu einem vorgegebenen Ring. Elemente eines solchen neuen Rings sind die Restklassen nach einem Ideal: jedem Element a ist eine Restklasse $\bar{a}$ zugeordnet. Zwei Restklassen werden multipliziert oder addiert, indem man irgend zwei Repräsentanten aus diesen Restklassen multipliziert oder addiert. *Aus* $a\equiv b$ *folgt* $\bar{a}=\bar{b}$; *die Kongruenzen werden also durch Übergang zum Restklassenring in Gleichheiten verwandelt, und dem Rechnen mit Kongruenzen in* $\mathfrak{o}$ *entspricht das Rechnen mit Gleichungen in* $\mathfrak{o}/\mathfrak{m}$.

Die hier konstruierten speziellen mit $\mathfrak{o}$ homomorphen Ringe: die Restklassenringe $\mathfrak{o}/\mathfrak{m}$, erschöpfen nun im wesentlichen alle zu $\mathfrak{o}$ homomorphen Ringe. Ist nämlich $\bar{\mathfrak{o}}$ ein beliebiges homomorphes Abbild von $\mathfrak{o}$, so sahen wir, daß den Elementen von $\bar{\mathfrak{o}}$ umkehrbar eindeutig die Restklassen nach einem Ideal $\mathfrak{n}$ in $\mathfrak{o}$ entsprechen. Der Restklasse $\mathfrak{R}_a$ entspricht das Element $\bar{a}$ in $\bar{\mathfrak{o}}$. Summe und Produkt zweier Restklassen $\mathfrak{R}_a$, $\mathfrak{R}_b$ werden gegeben durch $\mathfrak{R}_{a+b}$ bzw. $\mathfrak{R}_{ab}$; ihnen entsprechen also die Elemente

$$\overline{a+b}=\bar{a}+\bar{b}$$

und

$$\overline{ab}=\bar{a}\bar{b}.$$

Also ist die Zuordnung der Restklassen zu den Elementen von $\bar{\mathfrak{o}}$ ein Isomorphismus. Damit ist bewiesen:

Jeder zu $\mathfrak{o}$ *homomorphe Ring* $\bar{\mathfrak{o}}$ *ist isomorph einem Restklassenring* $\mathfrak{o}/\mathfrak{n}$. *Dabei ist* $\mathfrak{n}$ *das Ideal derjenigen Elemente, deren Bild in* $\bar{\mathfrak{o}}$ *die Null ist. Umgekehrt ist jeder Restklassenring* $\mathfrak{o}/\mathfrak{n}$ *ein homomorphes Bild von* $\mathfrak{o}$. (*Homomorphiesatz für Ringe.*)

Beispiele zum Restklassenring. Im Ring der ganzen Zahlen kann man (vgl. Aufgabe 1) die Restklassen nach einer positiven Zahl m mit $\mathfrak{R}_0$, $\mathfrak{R}_1$, ..., $\mathfrak{R}_{m-1}$ bezeichnen, wo $\mathfrak{R}_a$ aus denjenigen Zahlen be-

steht, die bei Division durch m den Rest a lassen. Um zwei Restklassen $\mathfrak{R}_a$, $\mathfrak{R}_b$ zu addieren oder zu multiplizieren, addiere bzw. multipliziere man ihre Repräsentanten a, b und reduziere das Ergebnis auf seinen kleinsten nicht negativen Rest nach m.

Aufgaben. 7. Der Restklassenring $\mathfrak{o}/\mathfrak{m}$ kann Nullteiler haben, auch wenn $\mathfrak{o}$ keine hat. Beispiele im Ring der ganzen Zahlen?

8. Die Homomorphie $\mathfrak{o} \sim \bar{\mathfrak{o}}$ ist dann und nur dann eine 1-Isomorphie, wenn $\mathfrak{n} = (0)$ ist.

9. In einem Körper gibt es keine Ideale außer dem Nullideal und dem Einheitsideal. Beweis? Was folgt daraus für die möglichen homomorphen Abbildungen eines Körpers?

10. Bei nichtkommutativen Ringen wird ein homomorphes Abbild immer von einem *zweiseitigen* Ideal vermittelt, und jedes zweiseitige Ideal besitzt auch tatsächlich einen Restklassenring.

11. Der Ring der ganzen Gaußschen Zahlen $a + bi$ (§ 10, Schluß) ist isomorph dem Restklassenring nach dem Ideal $(x^2 + 1)$ im ganzzahligen Polynombereich der Unbestimmten x.

§ 15. Teilbarkeit. Primideale.

Es sei $\mathfrak{b}$ ein Ideal (oder allgemeiner ein Modul) im Ring $\mathfrak{o}$. Ist a Element von $\mathfrak{b}$, so kann man dafür auch schreiben $a \equiv 0(\mathfrak{b})$, und man nennt a *teilbar durch das Ideal* $\mathfrak{b}$. Sind alle Elemente eines Ideals (oder Moduls) $\mathfrak{a}$ teilbar durch $\mathfrak{b}$, so nennt man $\mathfrak{a}$ *teilbar durch* $\mathfrak{b}$; das bedeutet aber nichts anderes, als daß $\mathfrak{a}$ Untermenge von $\mathfrak{b}$ ist. Zeichen:

$$\mathfrak{a} \equiv 0(\mathfrak{b}).$$

Man nennt $\mathfrak{b}$ einen *Teiler* von $\mathfrak{a}$, $\mathfrak{a}$ ein *Vielfaches* von $\mathfrak{b}$. Also: teilen = umfassen, Vielfaches = Untermenge. Ist außerdem $\mathfrak{a} \neq \mathfrak{b}$, also $\mathfrak{a} \subset \mathfrak{b}$, so heißt $\mathfrak{b}$ ein *echter Teiler* von $\mathfrak{a}$, $\mathfrak{a}$ ein *echtes Vielfaches* von $\mathfrak{b}$.

Bei Hauptidealen in kommutativen Ringen mit Einselement bedeutet $(a) \equiv 0((b))$ nichts anderes als $a = rb$, und der idealtheoretische Teilbarkeitsbegriff geht in den gewöhnlichen über.

Von jetzt an seien wieder alle betrachteten Ringe kommutativ.

Unter einem *Primideal* in $\mathfrak{o}$ versteht man ein solches Ideal $\mathfrak{p}$, dessen Restklassenring $\mathfrak{o}/\mathfrak{p}$ ein Integritätsbereich ist, d. h. keine Nullteiler besitzt.

Bezeichnet man Restklassen nach $\mathfrak{p}$ wie früher mit Querstrichen, so soll also

aus $\bar{a}\bar{b} = 0$ *und* $\bar{a} \neq 0$ *folgen* $\bar{b} = 0$.

Oder, was auf dasselbe hinauskommt, es soll aus

$$ab \equiv 0(\mathfrak{p}),$$
$$a \not\equiv 0(\mathfrak{p})$$

folgen

$$b \equiv 0 \,(\mathfrak{p}),$$

für beliebige a und b aus $\mathfrak{o}$; in Worten: *Ein Produkt soll nur dann durch das Ideal $\mathfrak{p}$ teilbar sein, wenn ein Faktor es ist.*

Klar ist: *Das Einheitsideal ist stets prim.* Denn die Voraussetzung $a \not\equiv 0 \,(\mathfrak{o})$ ist niemals erfüllbar. — *Das Nullideal ist dann und nur dann prim, wenn der Ring $\mathfrak{o}$ selbst ein Integritätsbereich ist.* Weitere Beispiele von Primidealen sind die von den Primzahlen erzeugten Hauptideale im Ring C der ganzen Zahlen, wie wir später sehen werden.

Ein Ideal in $\mathfrak{o}$ heißt *teilerlos*, wenn es von keinem anderen Ideal in $\mathfrak{o}$ außer von $\mathfrak{o}$ selbst umfaßt wird, m. a. W., wenn es *keine echten Teiler außer dem Einheitsideal $\mathfrak{o}$ besitzt.* (Die eben genannten Prim-Hauptideale (p) in C sind z. B. teilerlos.)

Jedes von $\mathfrak{o}$ verschiedene teilerlose Ideal $\mathfrak{p}$ in einem Ring $\mathfrak{o}$ mit Einselement ist prim, und der Restklassenring $\mathfrak{o}/\mathfrak{p}$ ist ein Körper. Ist umgekehrt $\mathfrak{o}/\mathfrak{p}$ ein Körper, so ist $\mathfrak{p}$ teilerlos.

Beweis: Wir wollen im Restklassenring die Gleichung $\bar{x}\,\bar{a} = \bar{b}$ für $\bar{a} \neq 0$ lösen. Es sei also $a \not\equiv 0 \,(\mathfrak{p})$ und b beliebig. $\mathfrak{p}$ und a zusammen erzeugen ein Ideal, welches Teiler von $\mathfrak{p}$ und (weil es a enthält) sogar echter Teiler von $\mathfrak{p}$ ist, also $= \mathfrak{o}$ sein muß. Daher läßt sich das beliebige Element b von $\mathfrak{o}$ schreiben in der Form

$$b = p + ra \qquad (p \in \mathfrak{p},\ r \in \mathfrak{o}).$$

Daraus folgt vermöge der Homomorphie von $\mathfrak{o}$ zum Restklassenring:

$$\bar{b} = \bar{r}\,\bar{a},$$

womit die Gleichung $\bar{x}\,\bar{a} = \bar{b}$ gelöst ist.

Der Restklassenring ist also ein Körper. Da ein Körper keine Nullteiler hat, so ist das Ideal $\mathfrak{p}$ prim.

Ist umgekehrt $\mathfrak{o}/\mathfrak{p}$ ein Körper, $\mathfrak{a}$ ein echter Teiler von $\mathfrak{p}$, a ein Element von $\mathfrak{a}$, das nicht zu $\mathfrak{p}$ gehört, so ist die Kongruenz

$$ax \equiv b \,(\mathfrak{p})$$

für jedes b aus $\mathfrak{o}$ lösbar. Es folgt

$$ax \equiv b \,(\mathfrak{a}),$$
$$0 \equiv b \,(\mathfrak{a}),$$

also, da b jedes Element von $\mathfrak{o}$ sein kann, $\mathfrak{a} = \mathfrak{o}$.

Daß nicht umgekehrt jedes Primideal teilerlos ist, zeigt das Beispiel des Nullideals im Ring der ganzen Zahlen oder weniger trivial das Ideal (x) im ganzzahligen Polynombereich $C[x]$, welches u. a. das Ideal $(2, x)$ als echten Teiler besitzt. Beide Ideale (x) und $(2, x)$ sind, wie man leicht feststellt, Primideale.

Aufgaben. 1. Man führe den Beweis der letzten Behauptung durch.

2. Man diskutiere die Restklassenringe der Ideale (2) und (3) im Ring der ganzen Zahlen und zeige, daß diese Ideale prim sind.

3. Dasselbe für die Ideale (3) und $(1+i)$ im Ring der ganzen Gaußschen Zahlen (§ 10, Schluß). Ist das Ideal (2) hier prim?

G. G. T. und K. G. V. Das von der Vereinigung von zwei Idealen $\mathfrak{a}, \mathfrak{b}$ erzeugte Ideal $(\mathfrak{a}, \mathfrak{b})$ wird auch als der *größte gemeinsame Teiler* (G. G. T.) dieser Ideale bezeichnet, weil es ein gemeinsamer Teiler ist, den jeder gemeinsame Teiler teilt. Weiter bezeichnet man es auch als die *Summe* der beiden Ideale, weil es offenbar aus allen Summen $a+b$ besteht, wo $a \in \mathfrak{a}$, $b \in \mathfrak{b}$ ist.

In derselben Weise bezeichnet man den Durchschnitt $\mathfrak{a} \cap \mathfrak{b}$ zweier Ideale $\mathfrak{a}$, $\mathfrak{b}$ auch als deren *kleinstes gemeinsames Vielfaches* (K. G. V.), weil er ein gemeinsames Vielfaches ist und jedes andere gemeinsame Vielfache durch ihn teilbar ist.

§ 16. Hauptidealringe.

Satz. *Im Ring C der ganzen Zahlen ist jedes Ideal Hauptideal.*

Beweis: Es sei $\mathfrak{a}$ ein Ideal in C. Ist $\mathfrak{a} = (0)$, so ist man fertig. Enthält $\mathfrak{a}$ noch eine Zahl $c \neq 0$, so enthält $\mathfrak{a}$ auch die Zahl $-c$, und eine dieser beiden Zahlen ist positiv. Es sei a die kleinste positive Zahl im Ideal $\mathfrak{a}$.

Ist nun b irgend eine Zahl des Ideals und r der Rest, den b bei Division durch a läßt, so ist

$$b = qa + r, \qquad 0 \leqq r < a.$$

Da b und a dem Ideal angehören, tut es auch $b - qa = r$. Da $r < a$ ist, muß $r = 0$ sein; denn a war die kleinste positive Zahl des Ideals. Also folgt $b = qa$; d. h. alle Zahlen des Ideals $\mathfrak{a}$ sind Vielfache von a. Daraus folgt $\mathfrak{a} = (a)$; also ist $\mathfrak{a}$ Hauptideal.

Genau so beweist man:

Ist P ein Körper, so ist im Polynombereich $\mathsf{P}[x]$ jedes Ideal Hauptideal.

Man kann nämlich wieder $\mathfrak{a} \neq (0)$ annehmen. Für a wähle man ein Polynom kleinsten Grades im Ideal $\mathfrak{a}$. Da auch im Polynombereich ein Divisionsalgorithmus existiert, kann man jedes Polynom b des Ideals in der Gestalt

$$b = qa + r$$

annehmen; der Grad von r ist, falls $r \neq 0$, kleiner als der von a, usw.

Ein Integritätsbereich mit Einselement, in dem jedes Ideal Hauptideal ist, heißt ein *Hauptidealring*. Wie eben bewiesen, ist der Ring C der ganzen Zahlen, sowie jeder Polynomring $\mathsf{P}[x]$, ein Hauptidealring[1].

[1] Eine elementare Untersuchung über die Bedingungen, die ein Integritätsbereich zu erfüllen hat, damit jedes Ideal in ihm Hauptideal sei, gibt H. Hasse in Crelles J. f. Math. Bd. 159, S. 3—12. 1928.

In trivialer Weise ist ferner jeder Körper ein Hauptidealring. Denn wenn ein Ideal $\mathfrak{a}$ im Körper P nicht das Nullideal ist, enthält es zu einem beliebigen $a \neq 0$ auch $a^{-1}a = 1$; also ist $\mathfrak{a} = (1)$ das einzige Ideal außer dem Nullideal. (Vgl. § 14, Aufg. 9.)

In Hauptidealringen ist der G. G. T. zweier Hauptideale (a), (b) wieder ein Hauptideal (d); in diesem Fall gibt es also sogar ein Element d, das die Eigenschaften des größten gemeinsamen Teilers hat (nämlich die Eigenschaften, selbst Teiler von a und b zu sein und von jedem gemeinsamen Teiler geteilt zu werden). Außerdem aber läßt sich d, wie jedes Element des Ideals (a, b), in der Gestalt

$$d = ra + sb \tag{1}$$

darstellen. Also: *In einem Hauptidealring besitzen je zwei Elemente a, b einen größten gemeinsamen Teiler d, der sich in der Gestalt* (1) *darstellen läßt.* Das gilt insbesondere für den Ring der ganzen Zahlen und für den Ring der Polynome einer Veränderlichen mit Koeffizienten aus einem Körper. — Man schreibt oft, unter Weglassung der Klammer um d, $(a, b) = d$. Diese Relation ist also den drei Relationen

$$d = ra + sb,$$
$$a = gd,$$
$$b = hd$$

gleichwertig. Ist in diesem Sinne der G. G. T. gleich 1, so heißen a und b zueinander *teilerfremd* oder *relativprim.*

Aufgaben. 1. Die Relation $(a, b) = d$ bleibt bestehen bei Erweiterung des Ringes $\mathfrak{o}$ zu irgend einem umfassenden Ring $\bar{\mathfrak{o}}$.

2. Um den größten gemeinsamen Teiler zweier Polynome $f_0(x)$, $f_1(x)$ oder zweier ganzen Zahlen f_0, f_1 wirklich zu berechnen, kann man das Verfahren der „sukzessiven Divisionen" einschlagen:

$$f_0 = q_1 f_1 + f_2,$$
$$f_1 = q_2 f_2 + f_3,$$
$$\cdots\cdots\cdots$$
$$f_{s-1} = q_s f_s.$$

Man zeige, daß dieses Verfahren wirklich zum größten gemeinsamen Teiler führt, und gebe damit einen zweiten direkten (konstruktiven) Beweis für den obigen Satz vom größten gemeinsamen Teiler für die speziellen Ringe C und $\mathsf{P}[x]$. (Man nennt das Verfahren den „euklidischen Algorithmus".)

3. Jedes Element a der Ordnung $r \cdot s$ in einer Gruppe $\mathfrak{G}$ ist Produkt aus einem eindeutig bestimmten Element $a^{\lambda r}$ der Ordnung s und einem eindeutig bestimmten Element $a^{\mu s}$ der Ordnung r, vorausgesetzt, daß die Zahlen r und s teilerfremd sind:

$$(r, s) = 1.$$

4. Eine zyklische Gruppe der Ordnung n mit dem erzeugenden Element a hat als Erzeugende alle Potenzen a^μ, wo $(\mu, n) = 1$ ist.

Weiteres Beispiel eines Hauptidealringes. Wir betrachten den Ring der ganzen Gaußschen Zahlen $a + bi$ (§ 10, Schluß).

Aus der Produktdefinition

$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i$$

folgt, wenn man die „Norm" einer Zahl $\alpha = a + bi$ definiert durch

$$N(\alpha) = (a + bi)(a - bi) = a^2 + b^2,$$

leicht die Gleichung

$$N(\alpha\beta) = N(\alpha) \cdot N(\beta) . \tag{2}$$

Die Norm $N(\alpha)$ ist eine gewöhnliche ganze Zahl, die (als Summe zweier Quadrate) nur dann verschwindet, wenn α selbst verschwindet, und sonst positiv ist. Aus (2) folgt, daß ein Produkt $\alpha\beta$ nur dann verschwindet, wenn α oder β verschwindet; wir befinden uns also in einem Integritätsbereich.

Nach § 12 existiert ein Quotientenkörper. Ist $\alpha = a + bi \neq 0$, so ist $\alpha^{-1} = \frac{a - bi}{N(\alpha)}$; die Zahlen des Quotientenkörpers lassen sich also in der Gestalt $\frac{a}{n} + \frac{b}{n} i$ darstellen (a, b, n ganze Zahlen). Diese „gebrochenen Zahlen" bilden den „Gaußschen Zahlkörper" (§ 10, Aufg. 11). Die Normdefinition und die Gleichung (2) bleiben für die Elemente dieses Körpers wörtlich erhalten.

Um zu einem Divisionsalgorithmus zu kommen, stellen wir uns die Aufgabe, zu gegebenem α und $\beta \neq 0$ eine Zahl $\alpha - \lambda\beta$ zu finden, die eine kleinere Norm als β hat. Zunächst bestimme man eine gebrochene Zahl $\lambda' = a' + b'i$, so daß $\alpha - \lambda'\beta = 0$ ist; sodann ersetze man a' und b' durch die nächstliegenden ganzen Zahlen a und b und setze $\lambda = a + bi$, $\lambda' - \lambda = \varepsilon$. Dann folgt:

$$\alpha - \lambda\beta = \alpha - \lambda'\beta + \varepsilon\beta = \varepsilon\beta ,$$

$$N(\alpha - \lambda\beta) = N(\varepsilon)\, N(\beta) ,$$

$$N(\varepsilon) = N(\lambda' - \lambda) = (a' - a)^2 + (b' - b)^2 \leqq (\tfrac{1}{2})^2 + (\tfrac{1}{2})^2 < 1 ,$$

$$N(\alpha - \lambda\beta) < N(\beta) .$$

Damit ist ein „Divisionsalgorithmus" gefunden. Wie vorhin im Bereich der ganzen Zahlen und im Polynombereich zeigt man nun, daß jedes Ideal Hauptideal ist.

Aufgaben. 5. In derselben Weise behandle man den Ring der Zahlen $a + b\varrho$, der als hyperkomplexes System in bezug auf den Ring der ganzen Zahlen durch die Basiselemente 1, ϱ und die Rechnungsregel

$$\varrho^2 = -\varrho - 1$$

definiert wird. Ebenso die Ringe der Zahlen $a + b\sqrt{2}$; $a + b\sqrt{-2}$. Warum versagt die Methode bei $a + b\sqrt{-3}$ und $a + b\sqrt{-5}$? Ist das Ideal $(2, 1 + \sqrt{-3})$ im erstgenannten Ring Hauptideal?

§ 17. Faktorzerlegung.

Wir betrachten in diesem Paragraphen nur Integritätsbereiche mit Einselement. Zunächst wollen wir untersuchen, was wir in diesen Bereichen zweckmäßig unter Primelementen oder unzerlegbaren Elementen zu verstehen haben.

Eine gewöhnliche Primzahl im Ring der ganzen Zahlen läßt sich immer in Faktoren zerlegen, sogar auf zwei Weisen:

$$p = p \cdot 1 = (-p) \cdot (-1) .$$

Aber einer dieser Faktoren ist immer eine „Einheit", d. h. eine solche Zahl ε, deren Inverse ε^{-1} auch im Ring liegt. $+1$ und -1 sind Einheiten.

Ist allgemein ein Integritätsbereich mit Einselement gegeben, so verstehen wir unter einer *Einheit*[1] ein solches Element ε, das im Bereich ein Inverses ε^{-1} besitzt. Offensichtlich ist dann auch ε^{-1} eine Einheit.

Jedes Element a läßt, wenn ε eine Einheit ist, eine Zerlegung

$$a = a\varepsilon^{-1} \cdot \varepsilon$$

zu. Solche Zerlegungen, bei denen ein Faktor eine Einheit ist, kann man „triviale Zerlegungen" nennen.

Ein Element $p \neq 0$, das nur triviale Zerlegungen zuläßt, so daß also aus $p = ab$ folgt, daß a oder b Einheit ist, heißt ein *unzerlegbares Element* oder ein *Primelement.* (Speziell bei ganzen Zahlen auch: *Primzahl*[2]; bei Polynomen auch: *irreduzibles Polynom.*)

Man nennt bisweilen zwei Größen wie a und $b = a\varepsilon^{-1}$, die sich nur um eine Einheit als Faktor unterscheiden, „assoziierte Größen". Jede ist Teiler der anderen, und für die zugehörigen Hauptideale gilt:

$$(a) \subseteq (b), \qquad (b) \subseteq (a), \quad \text{also} \quad (b) = (a);$$

mithin erzeugen zwei assoziierte Größen dasselbe Hauptideal.

Ist c ein Teiler von a, aber nicht assoziiert zu a, also $a = cd$ und d keine Einheit, so heißt c ein *echter Teiler* von a. In diesem Fall ist a nicht zugleich Teiler von c, und das Ideal (c) ist ein echter Teiler des Ideals (a).

Ein Primelement kann jetzt auch definiert werden als ein von Null verschiedenes Element, das keine echten Teiler außer Einheiten besitzt.

Wir wollen jetzt untersuchen, wie es mit der Möglichkeit und Eindeutigkeit der Faktorzerlegung in verschiedenen Integritätsbereichen beschaffen ist, und betrachten zunächst die Hauptidealringe.

In einem Hauptidealring erzeugt ein unzerlegbares Element, das keine Einheit ist, ein teilerloses Primideal (dessen Restklassenring also ein Körper ist).

Beweis: Ist p unzerlegbar, so hat p keine echten Teiler außer Einheiten, also (da jedes Ideal Hauptideal ist) das Ideal (p) keine echten Idealteiler außer dem Einheitsideal.

---

[1] Das Wort „Einheit" wird oft als Synonym für „Einselement" gebraucht. In Untersuchungen über Faktorzerlegung aber sind die beiden Begriffe streng zu trennen, da z. B. -1 auch eine Einheit ist.

[2] Meist versteht man unter Primzahlen nur die positiven unzerlegbaren Zahlen $\neq 1$, also die Zahlen

$$2, 3, 5, 7, 11, \ldots .$$

Bemerkung. Man kann natürlich die Lösbarkeit der Gleichung $\bar{a}\bar{x} = \bar{b}$ im Restklassenring oder der Kongruenz $ax \equiv b(\mathfrak{p})$ im gegebenen Ring auch direkt aus der Tatsache erschließen, daß für $a \not\equiv 0(\mathfrak{p})$ notwendig $(a, \mathfrak{p}) = 1$ sein muß, also

$$1 = ar + \mathfrak{p}s,$$
$$b = arb + \mathfrak{p}sb$$

ist. Auf Grund dieser Bemerkung kann man auch die Lösung der genannten Kongruenz in konkreten Fällen mit Hilfe des euklidischen Algorithmus (§ 16, Aufg. 2) wirklich berechnen.

Eine unmittelbare Folgerung ist:

I. *Ist ein Produkt durch das Primelement $\mathfrak{p}$ teilbar, so muß ein Faktor es sein*; denn der Restklassenring hat keine Nullteiler.

Aufgaben. 1. Man löse die Kongruenz

$$6x \equiv 7\,(19).$$

2. Was ist das inverse Element zur Restklasse von 6 im Restklassenkörper der ganzen Zahlen modulo (19)?

Für die Theorie der Faktorzerlegung ist noch eine zweite Eigenschaft der Hauptidealringe von Wichtigkeit, nämlich:

II. *Eine Kette von Elementen $a_1, a_2, \ldots$, deren jedes folgende ein echter Teiler des vorangehenden ist, kann nur endlichviele Glieder enthalten.*

Für alle speziellen Hauptidealringe, die wir kennengelernt haben, ist dieser Satz vollkommen trivial; im Ring der ganzen Zahlen z. B. folgt das Abbrechen der Kette sofort daraus, daß die Beträge der Zahlen $a_2, a_3, \ldots$ stets abnehmen müssen; ebenso müssen im Polynomring $K[x]$ die Grade der Polynome abnehmen; im Ring der ganzen Gaußschen Zahlen die Normen, usw. Der allgemeine Beweis für Hauptidealringe verläuft so:

Die Vereinigungsmenge aller Ideale (a_ν) ist ein Ideal; denn wenn ein a zu irgend einem der Ideale (a_ν) gehört, so auch jedes ra, und wenn a und b zu den Idealen (a_μ) und (a_ν) gehören, so gehört $a - b$ zum Ideal (a_λ), wo λ der größte der Indizes μ und ν ist, mithin auch zur Vereinigung. Dieses Vereinigungsideal hat ein Basiselement d, das selbst zum Ideal gehört, also etwa durch a_n teilbar ist. Nun behaupte ich, daß a_n das letzte Element der Kette sein muß. Gäbe es nämlich noch ein weiteres a_{n+1}, echter Teiler von a_n, so hätte man

$$a_{n+1} \equiv 0\,(d) \equiv 0\,(a_n)^1;$$

also wäre a_{n+1} doch kein echter Teiler von a_n.

[1] Das ist eine kurze Schreibweise für

$$a_{n+1} \equiv 0\,(d), \quad d \equiv 0\,(a_n).$$

Auf Grund der Sätze I und II beweisen wir nun den *Satz von der eindeutigen Faktorzerlegung*:

In einem Hauptidealring läßt sich jedes Element $\neq 0$ *als Produkt von Primfaktoren darstellen, und die Darstellung ist bis auf Einheitsfaktoren eindeutig.* (Dabei wird natürlich ein einzelnes Primelement auch schon als ein Produkt mit nur einem Faktor betrachtet.)

Daß zunächst die Möglichkeit der Darstellung, so selbstverständlich sie z. B. im Ring der ganzen Zahlen ist, für allgemeinere Integritätsbereiche keineswegs zu bestehen braucht, zeigt das folgende Beispiel: Man nehme zum Bereich der ganzen Zahlen die Größen $2^{\frac{1}{2}}, 2^{\frac{1}{4}}, 2^{\frac{1}{8}}, \ldots$ hinzu (die man entweder formell durch naheliegende Rechnungsregeln einführt oder als positive reelle Zahlen annimmt) und bilde alle endlichen Summen:

$$\sum a_r 2^r,$$

wo jedes r die Gestalt $\frac{m}{2^n}$ besitzt. Diese Summen bilden einen Integritätsbereich $\mathfrak{o}$. In $\mathfrak{o}$ ist:

$$2 = 2^{\frac{1}{2}} 2^{\frac{1}{2}} = 2^{\frac{1}{2}} 2^{\frac{1}{4}} 2^{\frac{1}{4}} = \cdots;$$

also kommt man bei der Zerlegung von 2 niemals zu einem Ende, d. h. man kommt nicht zu einer Zerlegung in Primfaktoren.

Allgemein gilt folgendes: *Wenn in einem Integritätsbereich mit Einselement ein Element* $a \neq 0$ *sich nicht als Produkt von Primfaktoren darstellen läßt, so hat* a *einen echten Teiler, der wiederum nicht als Produkt von Primfaktoren darstellbar ist.* Zunächst nämlich ist unter dieser Voraussetzung a nicht prim; also besteht eine Zerlegung

$$a = b \cdot c,$$

wo b und c echte Teiler von a sind. Mindestens einer der Faktoren b und c ist nun wiederum nicht als Produkt von Primfaktoren darstellbar; denn wären beide Produkte von Primfaktoren, so wäre offenbar auch a ein Produkt von Primfaktoren. Damit ist die Behauptung bewiesen.

Durch wiederholte Anwendung folgt, daß es zu jedem nicht in Primfaktoren zerlegbaren Element eine unendliche Kette von echten Teilern gibt, wo jedes folgende Glied wieder ein echter Teiler des vorangehenden ist[1]. Da aber eine solche Kette nach Eigenschaft II in Hauptidealringen unmöglich ist, so ist die Möglichkeit der Primfaktorzerlegung bewiesen.

Wir gehen nun zum Beweis der Eindeutigkeit über.

Gesetzt, es gäbe zwei Zerlegungen eines Elements $a \neq 0$:

$$(1) \qquad a = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s.$$

[1] Eine genaue Analyse dieser Schlußweise zeigt, daß hier das „Auswahlpostulat" benutzt wurde. Vgl. dazu Kap. 8, § 58.

Wir können immer annehmen, daß a keine Einheit ist (sonst wären ja alle Faktoren links und rechts Einheiten und es wäre nichts mehr zu beweisen) und daß alle eventuellen Einheiten unter den Faktoren links und rechts schon mit dem Faktor p_1 bzw. q_1, der keine Einheit darstellen möge, vereinigt sind. Dann behaupten wir: es ist $r = s$, und die p_i stimmen mit den q_i bis auf die Reihenfolge und bis auf Einheitsfaktoren überein.

Für $r = 1$ ist die Behauptung klar; denn wegen der Unzerlegbarkeit von $a = p_1$ kann das Produkt $q_1 \cdots q_s$ auch nur einen Faktor $q_1 = p_1$ enthalten. Wir können also Induktion nach r vornehmen. Da p_1 in dem Produkt $q_1 \cdots q_s$ aufgeht, so muß p_1 nach I in einem der Faktoren q_i aufgehen. Durch Umordnung der q erreichen wir, daß p_1 in q_1 aufgeht:

$$q_1 = \varepsilon_1 p_1 . \tag{2}$$

Hierin muß ε_1 Einheit sein, da sonst q_1 nicht prim wäre. Setzt man (2) in (1) ein und kürzt durch p_1, so kommt

$$p_2 \cdots p_r = (\varepsilon_1 q_2) q_3 \cdots q_s . \tag{3}$$

Nach der Induktionsvoraussetzung müssen die Faktoren in (3) links und rechts bis auf Einheiten übereinstimmen. Da auch p_1 mit q_1 bis auf die Einheit ε_1 übereinstimmt, ist alles bewiesen.

Aus diesem Satz folgt insbesondere die bis auf Einheiten eindeutige Zerlegbarkeit der ganzen Zahlen, der Polynome einer Veränderlichen mit Koeffizienten aus einem Körper, der ganzen Gaußschen Zahlen in Primfaktoren.

Aufgaben. 3. Die ganzzahligen Polynome $f(x)$ sind modulo jeder Primzahl p eindeutig in modulo p unzerlegbare Faktoren zerlegbar.

4. Was sind die Einheiten des Gaußschen Zahlringes? Man zerlege die Zahlen 2, 3, 5 in diesem Ring in Primfaktoren.

5. Im Ring der Zahlen $a + b\sqrt{-3}$ bestehen für die Zahl 4 die beiden wesentlich verschiedenen Zerlegungen:

$$4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3}).$$

6. In einem Hauptidealring bilden diejenigen Restklassen modulo a, die aus zu a teilerfremden Elementen bestehen, bei der Multiplikation eine Gruppe.

Wir werden im nächsten Kapitel sehen, daß es auch andere als Hauptidealringe gibt, in denen der Satz von der eindeutigen Faktorzerlegung gilt. Für alle solchen Ringe beweisen wir nun den Satz:

Wenn in $\mathfrak{o}$ jedes Element eindeutig in Primelemente zerlegbar ist, so erzeugt jedes unzerlegbare Element p ein Primideal, jedes von Null verschiedene zerlegbare Element ein Nichtprimideal.

Beweis: p sei unzerlegbar. Ist nun $ab \equiv 0\,(p)$, so muß in der Faktorzerlegung von ab der Faktor p vorkommen. Diese Faktorzerlegung erhält man aber durch Zusammensetzung der Faktorzerlegungen von a und b; also muß schon in a oder b der Faktor p vorkommen, also $a \equiv 0\,(p)$ oder $b \equiv 0\,(p)$ sein.

Nun sei p zerlegbar: $p = ab$, a und b echte Teiler von p. Dann folgt $ab \equiv 0\,(p)$, $a \not\equiv 0\,(p)$, $b \not\equiv 0\,(p)$. Das Ideal (p) ist also nicht prim.

Aufgaben. 7. Man beweise für alle Ringe mit eindeutiger Faktorzerlegung, daß es für je zwei oder mehrere Elemente einen „größten gemeinsamen Teiler" und ein „kleinstes gemeinsames Vielfaches" gibt, die beide bis auf Einheitsfaktoren bestimmt sind.

Bemerkung. Für Ringe der betrachteten Art ist der G.G.T. im Elementsinn nicht immer derselbe wie der G.G.T. im Idealsinn. So haben z. B. im ganzzahligen Polynombereich einer Veränderlichen x die Elemente 2 und x keine gemeinsamen Teiler außer Einheiten; aber das Ideal $(2, x)$ ist nicht das Einheitsideal. (Daß in diesem Ring die eindeutige Faktorzerlegung besteht, wird im nächsten Kapitel bewiesen werden.)

Viertes Kapitel.

Ganze rationale Funktionen.

Inhalt: Einfache Sätze über Polynome in einer und in mehreren Veränderlichen, mit Koeffizienten aus einem kommutativen Ring $\mathfrak{o}$ oder Körper Σ.

§ 18. Differentiation.

In diesem Paragraphen sollen die Differentialquotienten ganzer rationaler Funktionen ohne Stetigkeitsbetrachtungen für beliebige Polynombereiche $\mathfrak{o}[x]$ definiert werden.

Es sei $f(x) = \sum a_i x^i$ ein Polynom in $\mathfrak{o}[x]$. Bildet man nun in einem Polynombereich $\mathfrak{o}[x, h]$ das Polynom $f(x+h) = \sum a_i (x+h)^i$ und entwickelt es nach Potenzen von h, so kommt:

$$f(x+h) = f(x) + h f_1(x) + h^2 f_2(x) + \cdots$$

oder

$$f(x+h) \equiv f(x) + h \cdot f_1(x) \pmod{h^2}.$$

Der (eindeutig bestimmte) Koeffizient $f_1(x)$ der ersten Potenz von h heißt die *Ableitung* von $f(x)$ und wird immer mit $f'(x)$ bezeichnet. Man kann $f'(x)$ offenbar auch so erhalten, daß man die Differenz $f(x+h) - f(x)$ bildet, durch den darin ganzrational enthaltenen Faktor h durchdividiert und im so entstandenen Polynom $h = 0$ setzt. Daraus folgt leicht, daß die Definition der Ableitung mit der üblichen

Definition des *Differentialquotienten* als $\lim_{h\to 0} \frac{f(x+h)-f(x)}{h}$, falls $\mathfrak{o}$ etwa der Körper der reellen Zahlen ist, in Einklang steht. Man bezeichnet daher die Ableitung auch mit $\frac{df}{dx}$ oder mit $\frac{d}{dx}f(x)$ oder aber, wenn f außer x noch andere Variablen enthält, mit $\frac{\partial f}{\partial x}$.

Es gelten die folgenden Rechnungsregeln:

(1) $$(f+g)' = f' + g' \text{ (Summenregel)}.$$

(2) $$(fg)' = f'g + fg' \text{ (Produktregel)}.$$

Beweis (1):

$$f(x+h) + g(x+h) \equiv f(x) + hf'(x) + g(x) + hg'(x) \pmod{h^2}.$$

Beweis (2):

$$f(x+h)\,g(x+h) \equiv \{f(x) + hf'(x)\}\{g(x) + hg'(x)\}$$
$$\equiv f(x)\,g(x) + h\{f'(x)\,g(x) + f(x)\,g'(x)\} \pmod{h^2}.$$

Ebenso beweist man allgemeiner:

(3) $$(f_1 + \cdots + f_n)' = f_1' + \cdots + f_n',$$

(4) $$(f_1 f_2 \cdots f_n)' = f_1' f_2 \cdots f_n + f_1 f_2' \cdots f_n + \cdots + f_1 f_2 \cdots f_n'.$$

Aus (4) folgt weiter:

(5) $$(ax^n)' = nax^{n-1}.$$

Aus (3) und (5) folgt:

(6) $$\left(\sum_0^n a_k x^k\right)' = \sum_0^n k a_k x^{k-1}.$$

Durch diese Formel hätte man auch den Differentialquotienten formal definieren können.

Aufgaben. 1. Es sei $F(z_1, \ldots, z_m)$ ein Polynom und $F_\nu = \frac{\partial F}{\partial z_\nu}$. Man beweise die Formel

$$\frac{d}{dx} F(f_1(x), \ldots, f_m(x)) = \sum_1^m F_\nu(f_1, \ldots, f_m) \frac{df_\nu}{dx}.$$

2. Man leite für homogene Polynome r-ten Grades $f(x_1, \ldots, x_n)$ aus der Gleichung

$$f(hx_1, \ldots, hx_n) = h^r f(x_1, \ldots, x_n)$$

die „Eulersche Differentialgleichung" her:

$$\sum_\nu \frac{\partial f}{\partial x_\nu} x_\nu = rf.$$

3. Man gebe eine algebraische Definition für die Ableitung einer gebrochen-rationalen Funktion $\frac{f(x)}{g(x)}$ mit Koeffizienten aus einem Körper und beweise die bekannten Rechnungsregeln für die Differentiation von Summen, Produkten und Quotienten.

§ 19. Nullstellen.

Es sei $\mathfrak{o}$ ein Integritätsbereich mit Einselement.

Ein Element α von $\mathfrak{o}$ heißt *Nullstelle* oder *Wurzel* eines Polynoms $f(x)$ aus $\mathfrak{o}[x]$, wenn $f(\alpha) = 0$ ist. Es gilt der Satz:

Ist α eine Nullstelle von $f(x)$, so ist $f(x)$ durch $x - \alpha$ teilbar.

Beweis: Division von $f(x)$ durch $x - \alpha$ ergibt:

$$f(x) = q(x) \cdot (x - \alpha) + r,$$

wo r eine Konstante ist. Einsetzung von $x = \alpha$ ergibt:

$$0 = r$$

mithin ist

$$f(x) = q(x) \cdot (x - \alpha), \qquad \text{q. e. d.}$$

Sind $\alpha_1, \ldots, \alpha_k$ verschiedene Nullstellen von $f(x)$, so ist $f(x)$ durch das Produkt $(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_k)$ teilbar.

Beweis: Für $k = 1$ wurde der Satz eben bewiesen. Ist er für den Wert $k - 1$ bewiesen, so hat man:

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_{k-1})\, g(x).$$

Einsetzung von $x = \alpha_k$ ergibt:

$$0 = (\alpha_k - \alpha_1) \cdots (\alpha_k - \alpha_{k-1})\, g(\alpha_k),$$

also, da $\mathfrak{o}$ keine Nullteiler hat und $\alpha_k \neq \alpha_1, \ldots, \alpha_k \neq \alpha_{k-1}$ ist:

$$g(\alpha_k) = 0,$$

mithin nach dem vorigen Satz:

$$g(x) = (x - \alpha_k) \cdot h(x),$$

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_{k-1})(x - \alpha_k)\, h(x), \qquad \text{q. e. d.}$$

Folgerung: *Ein von Null verschiedenes Polynom vom Grade n hat in einem Integritätsbereich höchstens n Nullstellen.*

Dieser Satz gilt auch in Integritätsbereichen ohne Einselement, da man einen solchen ja stets in einen Körper (mit Einselement) einbetten kann. Er gilt aber nicht in Ringen mit Nullteilern; beispielsweise hat im Restklassenring modulo 16 das Polynom x^2 die Nullstellen 0, 4, 8, 12, und es gibt sogar Ringe, in denen dasselbe Polynom unendlichviele Nullstellen hat (§ 10, Aufgabe 4). Ebenso wird der Satz falsch für nichtkommutative Ringe; denn im Quaternionenkörper (§ 10, Aufg. 12) hat

das Polynom $x^2 + 1$ die Nullstellen $\pm i$, $\pm j$, $\pm k$ (und noch unendlichviele andere).

Ist $f(x)$ durch $(x - \alpha)^k$, aber nicht durch $(x - \alpha)^{k+1}$ teilbar, so nennt man α eine *k-fache Nullstelle* (oder k-fache Wurzel) von $f(x)$. Es gilt:

Eine k-fache Nullstelle von $f(x)$ ist eine mindestens $(k-1)$-fache Nullstelle der Ableitung $f'(x)$.

Beweis: Aus $f(x) = (x - \alpha)^k g(x)$ folgt:

$$f'(x) = k(x - \alpha)^{k-1} g(x) + (x - \alpha)^k g'(x);$$

mithin ist $f'(x)$ durch $(x - \alpha)^{k-1}$ teilbar.

Ebenso beweist man: *Eine einfache Nullstelle von $f(x)$ ist nicht zugleich Nullstelle der Ableitung $f'(x)$.*

Wir kommen nun zu einigen Sätzen über die Nullstellen von Polynomen in mehreren Veränderlichen.

Ist ein Polynom $f(x_1, \ldots, x_n)$ von Null verschieden und stellt man für jede der Unbestimmten $x_1, \ldots, x_n$ eine unendliche Menge von speziellen Werten aus $\mathfrak{o}$ oder aus einem $\mathfrak{o}$ umfassenden Integritätsbereich zur Verfügung, so gibt es daraus mindestens ein Wertsystem $x_1 = \alpha_1, \ldots, x_n = \alpha_n$, für das $f(\alpha_1, \ldots, \alpha_n) \neq 0$ ist.

Beweis: $f(x_1, \ldots, x_n)$ hat als Polynom in x_n (mit Koeffizienten aus dem Integritätsbereich $\mathfrak{o}[x_1, \ldots, x_{n-1}]$) höchstens endlichviele Nullstellen; also gibt es in der unendlichen Menge der Werte, die für x_n zur Verfügung stehen, einen Wert α_n, so daß

$$f(x_1, \ldots, x_{n-1}, \alpha_n) \neq 0$$

ist. Diesen Ausdruck behandle man nun als Polynom in x_{n-1}; so ergibt sich ein Wert α_{n-1}, für den

$$f(x_1, \ldots, x_{n-2}, \alpha_{n-1}, \alpha_n) \neq 0$$

ist, usw.

Folgerung. *Nimmt das Polynom $f(x_1, \ldots, x_n)$ für alle speziellen Werte x_i aus einem unendlichen Integritätsbereich den Wert Null an, so verschwindet es („identisch").*

Es sei an dieser Stelle daran erinnert, daß in der Algebra das Verschwinden eines Polynoms in $x_1, \ldots, x_n$ das Verschwinden aller Koeffizienten bedeutet und nicht definiert ist durch das Verschwinden für alle Werte, die man für $x_1, \ldots, x_n$ einsetzen kann. Der eben aufgestellte Satz ist also keine Tautologie. Auch wird er gegenstandslos für endliche Integritätsbereiche[1] und ist falsch für viele Ringe mit Nullteilern.

Aufgabe. Man erweitere den letzten Satz auf ein endliches System von Polynomen $f_i(x_1, \ldots, x_n)$, von denen keines identisch verschwindet.

[1] Beispiel: Das Polynom $x^2 + x$ verschwindet für alle x aus dem Körper $C/(2)$, ohne selbst zu verschwinden.

§ 20. Interpolationsformeln.

Wir kehren zu den Polynomen in einer Veränderlichen zurück, nehmen aber nunmehr den Koeffizientenbereich als einen kommutativen *Körper* an. Nach den bewiesenen Sätzen sind zwei Polynome vom Grade $\leqq n$, deren Werte an $n+1$ Stellen übereinstimmen, einander gleich; denn ihre Differenz hat $n+1$ Nullstellen und ist höchstens vom Grade n. Es gibt also höchstens ein Polynom, welches an $n+1$ verschiedenen Stellen $\alpha_0, \ldots, \alpha_n$ vorgegebene Werte $f(\alpha_i)$ annimmt. Nun gibt es immer ein Polynom vom Grade $\leqq n$, welches an diesen Stellen die vorgegebenen Werte annimmt, nämlich das Polynom

$$(1) \qquad f(x) = \sum_{i=0}^{n} \frac{f(\alpha_i)(x-\alpha_0)\cdots(x-\alpha_{i-1})(x-\alpha_{i+1})\cdots(x-\alpha_n)}{(\alpha_i-\alpha_0)\cdots(\alpha_i-\alpha_{i-1})(\alpha_i-\alpha_{i+1})\cdots(\alpha_i-\alpha_n)}.$$

Es gibt also ein und nur ein Polynom vom Grade $\leqq n$, welches an den $n+1$ Stellen α_i vorgegebene Werte $f(\alpha_i)$ annimmt, und dieses wird durch die Formel (1) *gegeben.* Die Formel (1) heißt die *Interpolationsformel von* LAGRANGE, weil sie es gestattet, die Werte einer ganzen rationalen Funktion vom Grade n an allen Zwischenstellen zu berechnen, sobald man ihre Werte an $n+1$ Stellen kennt.

Man erhält ein Polynom mit den gewünschten Eigenschaften auch durch die *Newtonsche Interpolationsformel*

$$(2) \qquad \begin{aligned} f(x) = {} & \lambda_0 + \lambda_1(x-\alpha_0) + \lambda_2(x-\alpha_0)(x-\alpha_1) + \cdots \\ & + \lambda_n(x-\alpha_0)(x-\alpha_1)\cdots(x-\alpha_{n-1}), \end{aligned}$$

wo die Koeffizienten $\lambda_0, \ldots, \lambda_n$ sukzessiv durch Einsetzung der Werte $x=\alpha_0, \ldots, x=\alpha_n$ bestimmt werden. Es ist klar, daß man in dieser Weise für jedes λ_i eine lineare Gleichung erhält, in welcher der Koeffizient dieses λ_i den Wert

$$(\alpha_i-\alpha_0)(\alpha_i-\alpha_1)\cdots(\alpha_i-\alpha_{i-1}) \neq 0$$

hat und sonst nur λ mit kleinerem Index vorkommen.

Wird insbesondere $\alpha_0 = 0$, $\alpha_1 = 1$, $\alpha_2 = 2$, ... gewählt, so geht (2) über in

$$(3) \qquad \begin{aligned} f(x) = {} & \lambda_0 + \lambda_1 x + \lambda_2 x(x-1) + \cdots \\ & + \lambda_n x(x-1)\cdots(x-n+1). \end{aligned}$$

Ein bequemes Mittel zur Bestimmung der λ_i in diesem Fall bietet die *„Differenzenrechnung"*. Man bilde die „erste Differenz von $f(x)$":

$$\Delta f(x) = f(x+1) - f(x).$$

Aus (3) erhält man leicht:

$$\begin{aligned} \Delta f(x) = {} & \lambda_1 + 2\lambda_2 x + 3\lambda_3 x(x-1) + \cdots \\ & + n\lambda_n x(x-1)\cdots(x-n+2); \end{aligned}$$

mithin: *Die erste Differenz eines Polynoms vom Grade $n>0$ ist ein Polynom vom Grade $n-1$.*

Ebenso wird die zweite Differenz

$$\Delta^2 f(x) = \Delta\Delta f(x)$$

im Falle $n > 1$ ein Polynom $(n-2)$-ten Grades:

$$\Delta^2 f(x) = 2\lambda_2 + 2\cdot 3\lambda_3 x + 3\cdot 4\lambda_4 x(x-1) + \cdots + (n-1)\cdot n\lambda_n x(x-1)\cdots(x-n+3),$$

usw., schließlich *die n-te Differenz eine Konstante.* Es kommt uns hauptsächlich auf die konstanten Glieder der sukzessiven Differenzen an; für diese finden wir:

$$\begin{aligned}
\Delta f(x) &= \lambda_1 + \cdots,\\
\Delta^2 f(x) &= 2\lambda_2 + \cdots,\\
\Delta^3 f(x) &= 3!\lambda_3 + \cdots,\\
&\cdots\cdots\cdots\cdots\\
\Delta^n f(x) &= n!\lambda_n.
\end{aligned}$$

Setzt man $f(0) = a_0$, $f(1) = a_1, \ldots, f(n) = a_n$, so kann man die als gegeben angenommenen a_i und die daraus berechneten Differenzen in ein „Differenzenschema" anordnen:

$$\begin{array}{lllll}
a_0 & \Delta a_0 & \Delta^2 a_0 & \cdots & \Delta^n a_0\\
a_1 & \Delta a_1 & \vdots & \vdots & \\
a_2 & \vdots & \vdots & & \\
\vdots & \vdots & & & \\
\vdots & \Delta a_{n-1} & & & \\
a_n & & & &
\end{array}, \quad \text{z. B.} \quad
\begin{array}{llll}
1 & 0 & & \\
1 & & 1 & \\
2 & 1 & & 1\\
 & 3 & 2 & \\
5 & & &
\end{array}$$

Unter der Voraussetzung, daß im Körper die Division durch $n!$ erlaubt ist (vgl. später, § 25), kann man die λ_ν aus den Zahlen des Differenzenschemas berechnen:

$$(4) \qquad \left\{\begin{aligned}
\lambda_0 &= a_0,\\
\lambda_1 &= \Delta a_0,\\
\lambda_2 &= \tfrac{1}{2}\Delta^2 a_0,\\
&\cdots\cdots\cdots\\
\lambda_n &= \frac{1}{n!}\Delta^n a_0.
\end{aligned}\right.$$

Um das obige Schema nach unten fortzusetzen, hat man in der letzten Spalte immer dieselbe Größe

$$\Delta^n a_0 = n!\lambda_n$$

zu schreiben, während die Elemente der vorletzten bis ersten Spalte sich daraus sukzessiv mühelos (durch Additionen) berechnen. In der ersten Spalte treten dann die Werte von $f(x)$ für die aufeinanderfolgenden ganzen Zahlen $0, 1, 2, \ldots, n, n+1, \ldots$ auf. Versteht man nun unter einer *arithmetischen Reihe nullter Ordnung* eine Folge von

lauter gleichen Zahlen $c, c, c, \ldots$ und unter einer *arithmetischen Reihe n-ter Ordnung* eine solche Zahlenfolge, deren Differenzenfolge eine arithmetische Reihe $(n-1)$-ter Ordnung darstellt, so ist klar, daß die erste Spalte unseres Schemas die allgemeinste arithmetische Reihe n-ter Ordnung bildet. Damit ist bewiesen:

Die Werte eines Polynoms $f(x)$ vom Grade n an den Stellen $0, 1, 2, \ldots$ *bilden eine arithmetische Reihe n-ter Ordnung, und jede arithmetische Reihe n-ter Ordnung besteht aus den Werten eines Polynoms höchstens n-ten Grades an jenen Stellen.*

Aus (3) und (4) folgt noch die Formel für das allgemeine Glied a_x einer arithmetischen Reihe n-ter Ordnung:

$$
\begin{aligned}
a_x = f(x) &= a_0 + (\Delta a_0)\, x + \frac{\Delta^2 a_0}{2}\, x(x-1) + \cdots \\
&\quad + \frac{\Delta^n a_0}{n!}\, x(x-1)\cdots(x-n+1) \qquad (5) \\
&= a_0 + \binom{x}{1} \Delta a_0 + \binom{x}{2} \Delta^2 a_0 + \cdots + \binom{x}{n} \Delta^n a_0 .
\end{aligned}
$$

Die Formel (5) kann zugleich als Interpolationsformel für beliebige Zwischenstellen benutzt werden. Die häufigste Anwendung findet sie bei numerischen Tabellen, wenn die „lineare Interpolation"

$$a_x = a_0 + (\Delta a_0)\, x$$

keine hinreichend genauen Resultate gibt und man daher die durch die Tabelle dargestellte Funktion mittels eines Polynoms vom Grade n approximiert, welches an $n+1$ aufeinanderfolgenden Stellen mit den Werten der Tabelle übereinstimmt.

Aufgaben. 1. Die Teilsummen $s_m = \sum_{\nu=0}^{m-1} a_\nu$ einer arithmetischen Reihe n-ter Ordnung (wobei $s_0 = 0$ gesetzt wird) bilden eine arithmetische Reihe $(n+1)$-ter Ordnung. Daraus ist die Summenformel

$$s_m = m\, a_0 + \binom{m}{2} \Delta a_0 + \cdots + \binom{m}{n+1} \Delta^n a_0$$

herzuleiten.

2. Man gebe Formeln für die Summen $\sum_{\nu=0}^{m-1} \nu$, $\sum_{\nu=0}^{m-1} \nu^2$, $\sum_{\nu=0}^{m-1} \nu^3$.

§ 21. Faktorzerlegung.

Wir haben in § 17 schon gesehen, daß für den Polynombereich $\mathsf{K}[x]$, wo K ein kommutativer *Körper* ist, der Satz von der eindeutigen Zerlegung in Primfaktoren gilt. Wir werden jetzt den folgenden allgemeineren *Hauptsatz* beweisen:

Ist $\mathfrak{S}$ ein Integritätsbereich mit Einselement und gilt in $\mathfrak{S}$ der Satz von der eindeutigen Primfaktorzerlegung, so gilt dieser Satz auch im Polynombereich $\mathfrak{S}[x]$.

Der hier darzustellende Beweis geht auf GAUSZ zurück.

Es sei $f(x) = \sum_0^n a_i x^i$ ein von Null verschiedenes Polynom aus $\mathfrak{S}[x]$. Der größte gemeinsame Teiler d von $a_0, \ldots, a_n$ in $\mathfrak{S}$ (vgl. § 17, Aufgabe 7) heißt der *Inhalt* von $f(x)$. Klammert man d aus, so kommt

$$f(x) = d \cdot g(x),$$

wo $g(x)$ den Inhalt 1 hat. $g(x)$ und d sind bis auf Einheitsfaktoren eindeutig bestimmt. Polynome vom Inhalt 1 heißen *Einheitsformen* oder *primitive Polynome* (in bezug auf $\mathfrak{S}$).

Hilfssatz 1. *Das Produkt zweier Einheitsformen ist wieder eine Einheitsform.*

Beweis: Es seien

$$f(x) = a_0 + a_1 x + \cdots$$

und

$$g(x) = b_0 + b_1 x + \cdots$$

Einheitsformen. Gesetzt, die Koeffizienten von $f(x) \cdot g(x)$ hätten einen gemeinsamen Teiler d, der keine Einheit wäre. Ist $\mathfrak{p}$ ein Primfaktor von d, so muß $\mathfrak{p}$ in allen Koeffizienten von $f(x)g(x)$ aufgehen. Es sei a_r der erste nicht durch $\mathfrak{p}$ teilbare Koeffizient von $f(x)$ [der sicher vorhanden ist, da sonst $f(x)$ keine Einheitsform wäre] und entsprechend b_s der von $g(x)$.

Der Koeffizient von x^{r+s} in $f(x)g(x)$ sieht so aus:

$$a_r b_s + a_{r+1} b_{s-1} + a_{r+2} b_{s-2} + \cdots$$
$$+ a_{r-1} b_{s+1} + a_{r-2} b_{s+2} + \cdots.$$

Die Summe soll durch $\mathfrak{p}$ teilbar sein. Alle Glieder außer dem ersten sind durch $\mathfrak{p}$ teilbar. Also muß $a_r b_s$ durch $\mathfrak{p}$ teilbar, also a_r oder b_s durch $\mathfrak{p}$ teilbar sein, entgegen der Voraussetzung.

Es sei nun Σ der Quotientenkörper von $\mathfrak{S}$ (§ 12). Dann ist in $\Sigma[x]$ jedes Polynom eindeutig zerlegbar (§ 17). Um nun von der Zerlegung in $\Sigma[x]$ zu einer Zerlegung in $\mathfrak{S}[x]$ zu gelangen, benutzen wir folgende Tatsache: Jedes Polynom $\varphi(x)$ von $\Sigma[x]$ kann man in der Gestalt $\frac{F(x)}{b}$ ($F(x)$ in $\mathfrak{S}[x]$, b in $\mathfrak{S}$) schreiben, wo b etwa das Produkt der Nenner der Koeffizienten von $\varphi(x)$ ist. Sodann kann man $F(x)$ als Produkt „Inhalt mal Einheitsform" schreiben:

$$F(x) = a \cdot f(x),$$

$$\varphi(x) = \frac{a}{b} \cdot f(x). \tag{1}$$

Wir behaupten nun:

Hilfssatz 2. *Die in* (1) *auftretende Einheitsform $f(x)$ ist eindeutig bis auf Einheiten aus $\mathfrak{S}$ durch $\varphi(x)$ bestimmt. Umgekehrt ist $\varphi(x)$ nach* (1) *eindeutig bis auf Einheiten aus $\Sigma[x]$ durch $f(x)$ bestimmt. Läßt man*

in dieser Weise jedem $\varphi(x)$ aus $\Sigma[x]$ eine Einheitsform $f(x)$ entsprechen, so entspricht dem Produkt zweier Polynome $\varphi(x)$, $\psi(x)$ bis auf Einheiten das Produkt der zugehörigen Einheitsformen (und umgekehrt). Ist $\varphi(x)$ unzerlegbar in $\Sigma[x]$, so ist $f(x)$ unzerlegbar in $\mathfrak{S}[x]$ (und umgekehrt).

Beweis: Es seien zwei verschiedene Darstellungen eines $\varphi(x)$ gegeben:

$$\varphi(x) = \frac{a}{b} f(x) = \frac{c}{d} g(x).$$

Dann folgt:

$$adf(x) = cbg(x). \tag{2}$$

Der Inhalt der linken Seite ist ad, der der rechten Seite cb; also muß

$$ad = \varepsilon cb$$

sein, wo ε eine Einheit aus $\mathfrak{S}$ ist. Setzt man das in (2) ein und kürzt durch cb, so folgt

$$\varepsilon f(x) = g(x).$$

$f(x)$ und $g(x)$ unterscheiden sich also nur um eine Einheit aus $\mathfrak{S}$.

Für das Produkt zweier Polynome

$$\varphi(x) = \frac{a}{b} f(x),$$

$$\psi(x) = \frac{c}{d} g(x)$$

erhält man sofort:

$$\varphi(x) \cdot \psi(x) = \frac{ac}{bd} f(x) g(x),$$

und nach Hilfssatz 1 ist $f(x)g(x)$ wieder eine Einheitsform. Dem Produkt $\varphi(x) \cdot \psi(x)$ entspricht also das Produkt $f(x) \cdot g(x)$.

Ist schließlich $\varphi(x)$ unzerlegbar, so ist es auch $f(x)$; denn eine Zerlegung $f(x) = g(x)\, h(x)$ würde sofort eine Zerlegung

$$\varphi(x) = \frac{a}{b} f(x) = \frac{a}{b} g(x) \cdot h(x)$$

nach sich ziehen. Das umgekehrte wird ebenso bewiesen.

Damit ist Hilfssatz 2 bewiesen.

Vermöge des Hilfssatzes 2 überträgt sich nun die eindeutige Faktorzerlegung der Polynome $\varphi(x)$ unmittelbar auf die zugehörigen Einheitsformen. Also: *Einheitsformen lassen sich bis auf Einheiten eindeutig in Primfaktoren, die wieder Einheitsformen sind, zerlegen.*

Nun wenden wir uns der Faktorzerlegung beliebiger Polynome in $\mathfrak{S}[x]$ zu. Unzerlegbare Polynome sind notwendig entweder unzerlegbare Konstanten oder unzerlegbare Einheitsformen; denn jedes andere Polynom ist zerlegbar in Inhalt mal Einheitsform. Um also ein Polynom $f(x)$ zu zerlegen, muß man zuerst $f(x)$ in Inhalt mal Einheitsform aufspalten und dann diese beiden Bestandteile getrennt in Primfaktoren

zerlegen. Das erstere ist bis auf Einheiten eindeutig möglich nach der Voraussetzung des Hauptsatzes, das zweite ebenfalls nach dem eben Bewiesenen. Damit ist der Hauptsatz *bewiesen.*

Als wichtiges Nebenresultat des Beweises ergibt sich:

Ist ein Polynom $F(x)$ aus $\mathfrak{S}[x]$ zerlegbar in $\Sigma[x]$, so ist es schon in $\mathfrak{S}[x]$ zerlegbar.

Denn vermöge $F(x) = d \cdot f(x)$ entspricht dem Polynom $F(x)$ eine Einheitsform $f(x)$, und nach Hilfssatz 2 zieht eine Produktzerlegung von $F(x)$ in $\Sigma[x]$ eine solche von $f(x)$ in $\mathfrak{S}[x]$ nach sich; mit $f(x)$ ist aber $F(x)$ zerlegbar.

Beispielsweise ist ein jedes Polynom mit ganzen rationalen Koeffizienten, das sich rationalzahlig zerlegen läßt, schon ganzzahlig zerlegbar. Also: *Wenn ein ganzzahliges Polynom ganzzahlig unzerlegbar ist, so ist es auch rationalzahlig unzerlegbar.*

Durch vollständige Induktion erhält man aus dem Hauptsatz das weitergehende Ergebnis:

Ist $\mathfrak{S}$ ein Integritätsbereich mit Einselement und gilt in $\mathfrak{S}$ der Satz von der eindeutigen Faktorzerlegung, so gilt dieser Satz auch im Polynombereich $\mathfrak{S}[x_1, \ldots, x_n]$.

Daraus folgt u. a. die eindeutige Faktorzerlegung für die ganzzahligen Polynome (von beliebig vielen Variablen), für die Polynome mit Koeffizienten aus einem Körper usw.

Der Begriff „primitives Polynom", oben in den Gaußschen Hilfssätzen eingeführt, wird insbesondere dann verwendet, wenn es sich um Polynombereiche in mehreren Variablen handelt. Ist K ein Körper, so heißt ein Polynom f aus $\mathsf{K}[x_1, \ldots, x_n]$ *primitiv in bezug auf* $x_1, \ldots, x_{n-1}$, wenn es primitiv in bezug auf den Integritätsbereich $\mathsf{K}[x_1, \ldots, x_{n-1}]$ ist, d. h. keinen nichtkonstanten Teiler hat, der nur von $x_1, \ldots, x_{n-1}$ abhängt. Zum Beispiel ist ein Polynom dann primitiv in bezug auf $x_1, \ldots, x_{n-1}$, wenn es *„regulär in bezug auf x_n"* ist, d. h. wenn der Koeffizient der höchsten Potenz von x_n eine von Null verschiedene Konstante (unabhängig von $x_1, \ldots, x_{n-1}$) ist.

Aufgaben. 1. Einheiten in $\mathfrak{S}[x]$ sind nur die Einheiten von $\mathfrak{S}$.

2. Man beweise, daß in einer Faktorzerlegung eines homogenen Polynoms nur homogene Faktoren auftreten können.

3. Man beweise, daß die Determinante

$$\Delta = \begin{vmatrix} x_{11} & \cdots & x_{1n} \\ \vdots & & \vdots \\ \vdots & & \vdots \\ x_{n1} & \cdots & x_{nn} \end{vmatrix}$$

im Polynombereich $\mathfrak{S}[x_{11}, \ldots, x_{nn}]$ unzerlegbar ist. (Man zeichne eine Unbestimmte, etwa x_{11}, aus und zeige, daß Δ primitiv in bezug auf die übrigen ist.)

4. Man gebe eine Regel an, die es erlaubt, von jedem ganzzahligen Polynom zu entscheiden, ob es einen Faktor ersten Grades hat.

5. Man beweise die Unzerlegbarkeit des Polynoms

$$x^4 - x^2 + 1$$

im ganzzahligen Polynombereich der Unbestimmten x. Ist das Polynom im rationalzahligen Polynombereich zerlegbar? Ist es zerlegbar im Gaußschen Ring als Koeffizientenbereich?

§ 22. Irreduzibilitätskriterien.

Es sei $\mathfrak{S}$ ein Integritätsbereich mit Einselement, in dem die eindeutige Zerlegbarkeit gilt, und es sei

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n$$

ein Polynom aus $\mathfrak{S}[x]$. Der folgende Satz gibt in vielen Fällen Auskunft über die Irreduzibilität von $f(x)$.

Eisensteinscher Satz. *Wenn es ein Primelement p in $\mathfrak{S}$ gibt, so daß*

$$a_n \not\equiv 0 \,(p),$$

$$a_i \equiv 0 \,(p) \text{ für alle } i > n,$$

$$a_0 \not\equiv 0 \,(p^2)$$

ist, so ist $f(x)$ irreduzibel in $\mathfrak{S}[x]$ bis auf konstante Faktoren; m. a. W. es ist $f(x)$ irreduzibel in $\Sigma[x]$, wo Σ den Quotientenkörper von $\mathfrak{S}$ bedeutet.

Beweis: Wäre $f(x)$ zerlegbar:

$$f(x) = g(x) \cdot h(x),$$

$$g(x) = \sum_0^r b_\nu x^\nu,$$

$$h(x) = \sum_0^s c_\nu x^\nu,$$

$$r > 0, \quad s > 0, \quad r + s = n,$$

so hätte man

$$a_0 = b_0 c_0 \quad \text{und} \quad a_0 \equiv 0 \,(p).$$

Daraus folgt, daß entweder $b_0 \equiv 0\,(p)$ oder $c_0 \equiv 0\,(p)$ ist. Es sei etwa $b_0 \equiv 0\,(p)$. Dann ist $c_0 \not\equiv 0\,(p)$, weil sonst $a_0 = b_0 c_0 \equiv 0\,(p^2)$ wäre.

Nicht alle Koeffizienten von $g(x)$ sind durch p teilbar; denn sonst wäre das Produkt $f(x) = g(x) \cdot h(x)$ durch p teilbar, also alle Koeffizienten, insbesondere a_n durch p teilbar, entgegen der Voraussetzung. Es sei also b_i der erste Koeffizient von $g(x)$, der nicht durch p teilbar ist $(0 < i \leqq r < n)$. Es ist

$$a_i = b_i c_0 + b_{i-1} c_1 + \cdots + b_0 c_i,$$

$$a_i \equiv 0 \,(p),$$

$$b_{i-1} \equiv 0 \,(p),$$

$$\cdots\cdots$$

$$b_0 \equiv 0 \,(p),$$

also

$$b_i c_0 \equiv 0 \,(p),$$

$$c_0 \not\equiv 0 \,(p),$$

$$b_i \equiv 0 \,(p),$$

entgegen der Voraussetzung.

Also ist $f(x)$ bis auf konstante Faktoren irreduzibel.

Das Kriterium führt nicht immer zu einer Entscheidung; denn es gibt viele Polynome, wie $x^2 + 1$, die nicht darunter fallen und trotzdem irreduzibel sind. Doch gewinnt man aus ihm in günstigen Fällen sehr allgemeine Resultate.

Beispiel 1. $x^m - p$ (p prim) ist im ganzzahligen (und somit auch im rationalzahligen) Polynombereich irreduzibel. Also ist $\sqrt[m]{p}$ ($m > 1$, p prim) stets irrational.

Beispiel 2. $f(x) = x^{p-1} + x^{p-2} + \cdots + 1$ ist, wenn p Primzahl ist, die linke Seite einer „Kreisteilungsgleichung". Wir fragen wieder nach ganzzahliger (oder, was auf dasselbe hinauskommt, rationalzahliger) Irreduzibilität. Das EISENSTEINsche Kriterium ist nicht direkt anwendbar; aber man kann folgendermaßen schließen. Wäre $f(x)$ reduzibel, so wäre $f(x+1)$ es auch. Nun ist

$$f(x+1) = \frac{(x+1)^p - 1}{(x+1) - 1} = \frac{x^p + \binom{p}{1} x^{p-1} + \cdots + \binom{p}{p-1} x}{x}$$

$$= x^{p-1} + \binom{p}{1} x^{p-2} + \cdots + \binom{p}{p-1}.$$

Alle Koeffizienten außer dem von x^{p-1} sind durch p teilbar; denn in der Formel für die Binomialkoeffizienten

$$\binom{p}{i} = \frac{p\,(p-1)\cdots(p-i+1)}{i!}$$

ist für $i < p$ der Zähler durch p teilbar, der Nenner aber nicht. Außerdem ist das konstante Glied $\binom{p}{p-1} = p$ nicht durch p^2 teilbar. Also ist $f(x+1)$ irreduzibel, also $f(x)$ irreduzibel.

Beispiel 3. Dieselbe Transformation führt auch für $f(x) = x^2 + 1$ zur Entscheidung, da

$$f(x+1) = x^2 + 2x + 2$$

ist.

Aufgaben. 1. Man zeige die Irrationalität von $\sqrt[m]{p_1 p_2 \ldots p_r}$, wo $p_1, \ldots, p_r$ verschiedene Primzahlen sind und $m > 1$ ist.

2. Man zeige die Irreduzibilität von

$$x^2 + y^2 - 1$$

in $\mathsf{P}[x, y]$, wo P irgend ein Körper ist, in welchem $+1 \neq -1$ ist.

3. Man zeige die Irreduzibilität der Polynome

$$x^4 + 1; \quad x^6 + x^3 + 1,$$

im ganzzahligen Polynombereich.

Im Grunde beruht der EISENSTEINsche Satz darauf, daß man die Gleichung

$$f(x) = g(x) \cdot h(x)$$

in eine Kongruenz nach p^2 verwandelt:

$$f(x) \equiv g(x) \cdot h(x),$$

und diese ad absurdum führt. In sehr vielen anderen Fällen ist es ebenfalls möglich, Irreduzibilitätsbeweise dadurch zu führen, daß man die Gleichungen in Kongruenzen modulo irgend einer Größe q des Bereichs $\mathfrak{S}$ verwandelt und untersucht, ob das vorgelegte Polynom $f(x)$ modulo q zerfällt. Ist insbesondere $\mathfrak{S}$ der Bereich der ganzen Zahlen C, so gibt es im Restklassenbereich nach q nur endlichviele Polynome von gegebenem Grad; also hat man modulo q immer nur endlichviele Möglichkeiten der Zerfällung von $f(x)$ zu untersuchen. Stellt es sich heraus,

daß $f(x)$ modulo q irreduzibel ist, so war $f(x)$ auch in $C[x]$ irreduzibel, und auch im anderen Fall kann man unter Umständen Schlüsse aus der gefundenen Zerlegung mod q ziehen, wobei man sich im Falle q = Primzahl auf den Satz von der eindeutigen Primfaktorzerlegung der Polynome mod q (§ 17, Aufg. 3) stützen kann.

Beispiel 1. $\mathfrak{S} = C$; $f(x) = x^5 - x^2 + 1$. Wenn $f(x)$ mod 2 zerlegbar ist, so muß einer der Faktoren linear oder quadratisch sein. Nun gibt es mod 2 bloß zwei lineare Polynome:

$$x,\ x + 1\,,$$

und bloß ein irreduzibles quadratisches Polynom:

$$x^2 + x + 1\,.$$

Ausführung der Division lehrt, daß $x^5 - x^2 + 1$ durch alle diese Polynome nicht teilbar ist. Man sieht das auch direkt aus

$$x^5 - x^2 + 1 = x^2(x^3 - 1) + 1 \equiv x^2(x + 1)(x^2 + x + 1) + 1\,.$$

Also ist $f(x)$ irreduzibel.

Beispiel 2. $\mathfrak{S} = C$; $f(x) = x^4 + 3x^3 + 3x^2 - 5$. Modulo 2 zerfällt $f(x)$:

$$f(x) \equiv (x + 1)(x^3 + x + 1)\,.$$

Der letzte Faktor ist irreduzibel mod 2. Wenn also $f(x)$ überhaupt zerfällt, so muß es in einen Linearfaktor und einen kubischen Faktor zerfallen. Man kann nun leicht direkt zeigen, daß ein Linearfaktor nicht vorhanden ist, am bequemsten, indem man sich überlegt, daß modulo 3 die einzig in Betracht kommenden Linearfaktoren x, $x + 1$, $x - 1$ nicht in $f(x)$ aufgehen.

Literatur. Verallgemeinerungen des Eisensteinschen Kriteriums mit elementaren Beweisen findet man bei Schönemann, Th.: Crelles J. f. Math. Bd. 32, S. 93, § 61. Netto, E.: Math. Ann. Bd. 48, S. 82. Dumas, G.: Liouvilles J. de Math. (6) Bd. 2, S. 237. Ore, Ö.: Math. Z. Bd. 18, S. 278; Bd. 20, S. 267. Andere Irreduzibilitätskriterien gibt Schur, I.: Berl. Sitzungsber. 1929, S. 125 u. 370. Auch die bekannte Aufgabensammlung von Pólya und Szegö enthält derartige Sätze.

§ 23. Die Durchführung der Faktorzerlegung in endlichvielen Schritten.

Wir haben zwar die theoretische Möglichkeit eingesehen, bei gegebenem kommutativen Körper Σ jedes Polynom aus $\Sigma[x_1, \ldots, x_n]$ in Primfaktoren zu zerlegen, und in einigen Fällen auch die Mittel aufgezeigt, die Zerlegung wirklich anzugeben bzw. die Unmöglichkeit einer Zerlegung darzutun; aber eine allgemeine Methode, die Zerlegung in jedem Fall in endlichvielen Schritten durchzuführen, besitzen wir noch nicht. Eine solche Methode wollen wir wenigstens für den Fall, daß Σ der Körper der rationalen Zahlen ist, angeben.

Man kann nach § 21 jedes rationalzahlige Polynom ganzzahlig voraussetzen und seine Zerlegung im ganzzahligen Polynombereich vornehmen. Im Ring C der ganzen Zahlen selbst ist jede Primfaktorzerlegung offenbar durch endliches Ausprobieren durchführbar; außerdem gibt es dort nur endlichviele Einheiten ($+1$ und -1), also nur endlichviele mögliche Zerlegungen. Auch im Polynombereich $C[x_1, \ldots, x_n]$ gibt es nur die Einheiten $+1$, -1. Durch vollständige Induktion nach der Variablenzahl n wird nun alles auf das folgende Problem zurückgeführt:

In $\mathfrak{S}$ sei jede Faktorzerlegung in endlichvielen Schritten ausführbar; außerdem gebe es in $\mathfrak{S}$ nur endlichviele Einheiten. Gesucht wird eine Methode, jedes Polynom aus $\mathfrak{S}[x]$ in Primfaktoren zu zerlegen.

Die Lösung ist von KRONECKER gegeben worden.

Es sei $f(x)$ ein Polynom n-ten Grades in $\mathfrak{S}[x]$. Wenn $f(x)$ zerlegbar ist, so hat einer der Faktoren einen Grad $\leqq \frac{n}{2}$; ist also s die größte ganze Zahl $\leqq \frac{n}{2}$, dann haben wir zu untersuchen, ob $f(x)$ einen Faktor $g(x)$ vom Grade $\leqq s$ hat.

Wir bilden die Funktionswerte $f(a_0)$, $f(a_1)$, ..., $f(a_s)$ an $s+1$ beliebig gewählten ganzzahligen Stellen $a_0, a_1, \ldots, a_s$. Soll nun $f(x)$ durch $g(x)$ teilbar sein, so muß $f(a_0)$ durch $g(a_0)$, $f(a_1)$ durch $g(a_1)$ usw. teilbar sein. Da aber jedes $f(a_i)$ in $\mathfrak{S}$ nur endlichviele Teiler besitzt, so kommen für jedes $g(a_i)$ nur endlichviele Möglichkeiten in Betracht, die man nach Voraussetzung alle aufzufinden imstande ist. Zu jeder möglichen Kombination von Werten $g(a_0)$, $g(a_1)$, ..., $g(a_s)$ gibt es nach den Sätzen von § 20 ein und nur ein Polynom $g(x)$, welches man (etwa mit der Lagrangeschen oder bequemer mit der Newtonschen Interpolationsformel) jeweils explizite aufstellen kann. Damit hat man also endlichviele Polynome $g(x)$ gefunden, die als Teiler in Betracht kommen. Von jedem dieser Polynome $g(x)$ kann man nun durch den Divisionsalgorithmus feststellen, ob es wirklich ein Teiler von $f(x)$ ist. Ist keines der möglichen $g(x)$, abgesehen von den Einheiten, Teiler von $f(x)$, so ist $f(x)$ unzerlegbar; im anderen Fall hat man eine Zerlegung gefunden und kann auf die beiden Faktoren dasselbe Verfahren weiter anwenden, usw. Schließlich kommt man so auf die unzerlegbaren Faktoren.

Im ganzzahligen Fall ($\mathfrak{S} = C$) kann man das Verfahren oft ganz erheblich abkürzen. Zunächst läßt sich durch Zerlegung des gegebenen Polynoms modulo 2 und eventuell noch modulo 3 eine Übersicht darüber gewinnen, welche Gradzahlen die möglichen Faktorpolynome $g(x)$ haben können und welchen Restklassen die Koeffizienten modulo 2 und 3 angehören. Das schränkt die Anzahl der möglichen $g(x)$ schon erheblich ein. Sodann kann man bei Anwendung der Newtonschen Interpolationsformel beachten, daß der letzte Koeffizient λ_s ein Teiler des höchsten Koeffizienten von $f(x)$ sein muß, was wieder eine Einschränkung der Möglichkeiten bedeutet. Schließlich benutzt man oft mit Vorteil mehr als $s+1$ Stellen a_i (die man am liebsten gleich $0, \pm 1, \pm 2$ usw. wählt). Man verwendet dann zur Bestimmung der möglichen $g(a_i)$ diejenigen $f(a_i)$, welche am wenigsten Primfaktoren enthalten; die übrigen Stellen können nachher benutzt werden, um die Anzahl der Möglichkeiten noch weiter einzuschränken, indem man für jedes errechnete $g(x)$ erst prüft, ob es an den noch nicht berücksichtigten Stellen a_i Werte annimmt, die Teiler des jeweiligen $f(a_i)$ sind.

Aufgaben. 1. Man zerlege

$$f(x) = 2x^5 - x^3 + 3x^2 + 8x - 4$$

in $C[x]$.

2. Man zerlege

$$f(x, y, z) = -x^3 - y^3 - z^3 + x^2(y+z) + y^2(x+z) + z^2(x+y) - 2xyz$$

in $C[x, y, z]$.

§ 24. Symmetrische Funktionen.

Es sei $\mathfrak{o}$ ein beliebiger kommutativer Ring mit Einselement.

Ein Polynom aus $\mathfrak{o}[x_1, \ldots, x_n]$, das bei jeder beliebigen Permutation der Unbestimmten $x_1, \ldots, x_n$ in sich übergeht, heißt eine (ganze rationale) *symmetrische Funktion* der Variablen $x_1, \ldots, x_n$. Beispiele: Summe, Produkt, Potenzsumme $\sum_{\nu=1}^{n} x_\nu^r$.

Setzt man mit einer neuen Unbestimmten z

$$(1) \qquad \begin{aligned} f(z) &= (z - x_1)(z - x_2) \ldots (z - x_n) \\ &= z^n - \sigma_1 z^{n-1} + \sigma_2 z^{n-2} - \cdots + (-1)^n \sigma_n , \end{aligned}$$

so sind die Koeffizienten der Potenzen von z:

$$\begin{aligned} \sigma_1 &= x_1 + x_2 + \cdots + x_n , \\ \sigma_2 &= x_1 x_2 + x_1 x_3 + \cdots + x_2 x_3 + \cdots + x_{n-1} x_n , \\ \sigma_3 &= x_1 x_2 x_3 + x_1 x_2 x_4 + \cdots + x_{n-2} x_{n-1} x_n , \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \sigma_n &= x_1 x_2 \ldots x_n , \end{aligned}$$

offenbar symmetrische Funktionen, weil die linke Seite von (1) und somit auch die rechte bei allen Permutationen der x_i ungeändert bleibt. Man nennt $\sigma_1, \ldots, \sigma_n$ die *elementarsymmetrischen Funktionen* von $x_1, \ldots, x_n$.

Jedes Polynom $\varphi(\sigma_1, \ldots, \sigma_n)$ ergibt, wenn man die σ durch ihre Ausdrücke in den x ersetzt, eine symmetrische Funktion der $x_1, \ldots, x_n$. Und zwar ergibt ein Glied $c\sigma_1^{\mu_1} \ldots \sigma_n^{\mu_n}$ von $\varphi(\sigma_1, \ldots, \sigma_n)$ ein homogenes Polynom in den x_i vom Grade $\mu_1 + 2\mu_2 + \cdots + n\mu_n$, da jedes σ_i ein homogenes Polynom i-ten Grades ist. Wir nennen die Summe $\mu_1 + 2\mu_2 + \cdots + n\mu_n$ das *Gewicht* des Gliedes $c\sigma_1^{\mu_1} \ldots \sigma_n^{\mu_n}$ und verstehen unter dem Gewicht eines Polynoms $\varphi(\sigma_1, \ldots, \sigma_n)$ das höchste Gewicht, das unter seinen Gliedern vorkommt. Polynome $\varphi(\sigma_1, \ldots, \sigma_n)$ vom Gewicht k ergeben demnach symmetrische Polynome der x_i vom Grade $\leqq k$.

Der sogenannte *Hauptsatz über die symmetrischen Funktionen* besagt nun, daß sich diese Verhältnisse umkehren lassen:

Jede ganze rationale symmetrische Funktion vom Grade k aus $\mathfrak{o}[x_1, \ldots, x_n]$ läßt sich als Polynom $\varphi(\sigma_1, \ldots, \sigma_n)$ vom Gewicht k schreiben.

Das Wichtigste an diesem Satze ist natürlich, daß jede symmetrische Funktion sich durch $\sigma_1, \ldots, \sigma_n$ ausdrücken läßt; der Zusatz über Grad und Gewicht dient hauptsächlich dazu, den Induktionsbeweis zu erleichtern.

Dem Beweis sei eine Bemerkung vorausgeschickt:

Wenn zwei Polynome aus $\mathfrak{o}[x_1, \ldots, x_n]$ einander gleich sind und beide durch x_1 teilbar sind, so bleibt die Gleichheit der Polynome bestehen, wenn man aus allen Gliedern den Faktor x_1 heraushebt. Dies gilt unabhängig davon, ob $\mathfrak{o}$ Nullteiler hat oder nicht, einfach weil die Gleichheit zweier Polynome das völlige Übereinstimmen der Koeffizienten bedeutet.

Setzt man nun in der Identität (1) auf beiden Seiten $x_n = 0$, während die übrigen x_i den Charakter von Unbestimmten beibehalten, so kommt:

$$\begin{aligned} (z - x_1) \ldots (z - x_{n-1}) z = z^n - (\sigma_1)_0 z^{n-1} + \cdots \\ + (-1)^{n-1} (\sigma_{n-1})_0 z , \end{aligned}$$

wo $(\sigma_i)_0$ den Ausdruck bedeutet, der aus σ_i für $x_n = 0$ entsteht. Kürzt man auf Grund der obigen Bemerkung auf beiden Seiten mit z, so ergibt sich:

$$(z - x_1) \ldots (z - x_{n-1}) = z^{n-1} - (\sigma_1)_0 z^{n-2} + \cdots + (-1)^{n-1} (\sigma_{n-1})_0 .$$

Diese Gleichung besagt: Die Ausdrücke $(\sigma_1)_0, \ldots, (\sigma_{n-1})_0$ sind die elementarsymmetrischen Funktionen der ersten $n-1$ Veränderlichen.

Der *Beweis des Hauptsatzes* wird durch Induktion nach n geführt. Für $n = 1$ ist der Satz richtig; denn bei einer Veränderlichen x_1 ist jedes Polynom $f(x_1)$ symmetrisch und $\sigma_1 = x_1$, mithin $f(x_1) = f(\sigma_1)$. Der Satz sei also für Polynome in $n-1$ Variablen $(n > 1)$ bewiesen; wir zeigen ihn nunmehr für Polynome in n Variablen.

Für Polynome nullten Grades in n Variablen ist der Satz trivial. Wir können also noch annehmen, er sei für alle Polynome der Grade $< k$ in n Variablen bewiesen, und haben ihn lediglich für Polynome k-ten Grades in n Variablen zu zeigen.

Es möge nun ein symmetrisches Polynom k-ten Grades $f(x_1, \ldots, x_n)$ gegeben sein. Setzt man $x_n = 0$, so hat man nach den Induktionsvoraussetzungen

$$f(x_1, \ldots, x_{n-1}, 0) = \varphi((\sigma_1)_0, \ldots, (\sigma_{n-1})_0),$$

wo φ als Funktion der elementarsymmetrischen Funktionen von $x_1, \ldots, x_{n-1}$ ein Gewicht $\leqq k$ hat. Demnach hat auch die Funktion $\varphi(\sigma_1, \ldots, \sigma_{n-1})$ ein Gewicht $\leqq k$. Man bilde nun

$$f_1 = f(x_1, \ldots, x_{n-1}, x_n) - \varphi(\sigma_1, \ldots, \sigma_{n-1}).$$

Das Polynom $f_1(x_1, \ldots, x_n)$ ist offenbar symmetrisch. Das erste Glied der rechten Seite hat den Grad k, das zweite ein Gewicht $\leqq k$, also als Polynom in den x einen Grad $\leqq k$, und folglich hat f_1 einen Grad $\leqq k$. Außerdem verschwindet f_1 für $x_n = 0$; also haben alle Glieder den Faktor x_n. Da die Funktion f_1 symmetrisch ist, haben auch alle Glieder die Faktoren $x_1, x_2, \ldots, x_{n-1}$. Spaltet man aus allen Gliedern das Produkt $x_1 x_2 \ldots x_n = \sigma_n$ ab, so folgt

$$f_1 = \sigma_n g(x_1, \ldots, x_n),$$

wo g wieder ein symmetrisches Polynom ist und einen Grad $\leqq k - n < k$ hat. Nach Voraussetzung läßt sich daher g durch $\sigma_1, \ldots, \sigma_n$ ausdrücken:

$$g = \psi(\sigma_1, \ldots, \sigma_n),$$

wo ψ ein Polynom vom Gewichte $\leqq k - n$ ist. Daraus folgt für f die Darstellung

$$f = f_1 + \varphi(\sigma_1, \ldots, \sigma_{n-1}) = \sigma_n \psi(\sigma_1, \ldots, \sigma_n) + \varphi(\sigma_1, \ldots, \sigma_{n-1}).$$

Die rechte Seite ist ganzrational in den σ und hat höchstens das Ge-

wicht k. Das Gewicht kann nicht kleiner als k sein, da sonst f einen Grad $< k$ hätte. Also hat die rechte Seite genau das Gewicht k, womit alles bewiesen ist.

Dieser Beweis gibt zugleich ein Mittel, eine vorgelegte symmetrische Funktion wirklich rechnerisch durch die σ_i auszudrücken. Die Methode ist aber etwas umständlich; wir werden nachher eine kürzere angeben.

Aus dem Beweis folgt noch: Homogene symmetrische Funktionen können durch „isobare" Ausdrücke in den σ_i dargestellt werden, d. h. durch solche, deren Glieder alle dasselbe Gewicht haben.

Wir wollen jetzt zeigen, daß eine symmetrische Funktion sich *nur auf eine Art* durch $\sigma_1, \ldots, \sigma_n$ ganzrational ausdrücken läßt; genauer:

Sind $\varphi_1(y_1, \ldots, y_n)$ *und* $\varphi_2(y_1, \ldots, y_n)$ *zwei Polynome in den Unbestimmten* $y_1, \ldots, y_n$ *und ist*

$$\varphi_1(y_1, \ldots, y_n) \neq \varphi_2(y_1, \ldots, y_n),$$

so ist

$$\varphi_1(\sigma_1, \ldots, \sigma_n) \neq \varphi_2(\sigma_1, \ldots, \sigma_n).$$

Bildet man die Differenz $\varphi_1 - \varphi_2 = \varphi$, so sieht man, daß es genügt, zu beweisen: Aus $\varphi(y_1, \ldots, y_n) \neq 0$ folgt $\varphi(\sigma_1, \ldots, \sigma_n) \neq 0$.

Der Satz gilt für $n = 1$, da dann $\sigma_1 = x_1$ selbst eine Unbestimmte ist, mithin aus $\varphi(y_1) \neq 0$ stets $\varphi(\sigma_1) \neq 0$ folgt.

Der Satz braucht also für ein beliebiges $n > 1$ nur unter der Annahme bewiesen zu werden, daß er für jede kleinere Anzahl von Unbestimmten bereits gilt. Gesetzt, er wäre für n falsch; dann gibt es ein Polynom $\varphi(y_1, \ldots, y_n) \neq 0$ von möglichst niedrigem Grad m in bezug auf y_n, so daß $\varphi(\sigma_1, \ldots, \sigma_n) = 0$ ist. Ordnet man $\varphi(y_1, \ldots, y_n)$ nach y_n, so erhalten die beiden Relationen die Gestalt

$$\varphi_m y_n^m + \varphi_{m-1} y_n^{m-1} + \cdots + \varphi_0 \neq 0,$$

$$\varphi_m(\sigma_1, \ldots, \sigma_{n-1})\sigma_n^m + \cdots + \varphi_0(\sigma_1, \ldots, \sigma_{n-1}) = 0. \tag{2}$$

Es muß $\varphi_0(y_1, \ldots, y_{n-1}) \neq 0$ sein; denn sonst könnte man in der ersten Relation aus allen Gliedern y_n herausheben, in der zweiten Relation ebenso σ_n und würde erhalten:

$$\overline{\varphi}(y_1, \ldots, y_n) = \varphi_m y_n^{m-1} + \cdots + \varphi_1 \neq 0,$$

$$\overline{\varphi}(\sigma_1, \ldots, \sigma_n) = \varphi_m(\sigma_1, \ldots, \sigma_{n-1})\sigma_n^{m-1} + \cdots + \varphi_1(\sigma_1, \ldots, \sigma_{n-1}) = 0,$$

wo das Polynom $\overline{\varphi}$ einen Grad $< m$ hat, entgegen der Voraussetzung. Setzt man nun in (2) $x_n = 0$, so kommt:

$$\varphi_0((\sigma_1)_0, \ldots, (\sigma_{n-1})_0) = 0,$$

obgleich $\varphi_0(y_1, \ldots, y_{n-1}) \neq 0$ war, entgegen der Induktionsvoraussetzung. Wir haben also bewiesen:

Jedes symmetrische Polynom aus $\mathfrak{o}[x_1, \ldots, x_n]$ *läßt sich auf eine und nur eine Art als Polynom in* $\sigma_1, \ldots, \sigma_n$ *schreiben; das Gewicht dieses Polynoms ist gleich dem Grad des gegebenen Polynoms.*

Alle ganzrationalen Relationen zwischen symmetrischen Funktionen bleiben bestehen, wenn die x_i nicht Unbestimmte sind, sondern Größen aus $\mathfrak{o}$, etwa die Wurzeln eines in $\mathfrak{o}[z]$ vollständig zerfallenden Polynoms $f(z)$. Aus dem Bewiesenen ergibt sich also, daß jede symmetrische Funktion der Wurzeln von $f(z)$ sich durch die Koeffizienten von $f(z)$ ausdrücken läßt.

Für die praktische Durchführung der Rechnungen, die nötig sind, um eine gegebene symmetrische Funktion durch die elementarsymmetrischen Funktionen $\sigma_1, \ldots, \sigma_n$ auszudrücken, existieren verschiedene Methoden, von denen hier nur noch eine angeführt werden möge. (Weitere folgen als Übungsaufgaben.) Man ordne das gegebene symmetrische Polynom *„lexikographisch"* (wie im Lexikon), d. h. so, daß ein Glied $x_1^{\alpha_1} \ldots x_n^{\alpha_n}$ einem anderen $x_1^{\beta_1} \ldots x_n^{\beta_n}$ vorangeht, wenn die erste nichtverschwindende Differenz $\alpha_i - \beta_i$ positiv ist. Mit einem Glied $x_1^{\alpha_1} \ldots x_n^{\alpha_n}$ kommen auch alle Glieder vor, deren Exponenten eine Permutation der α_i sind; diese werden nicht alle geschrieben, sondern man schreibt $\sum x_1^{\alpha_1} \ldots x_n^{\alpha_n}$, wobei $\alpha_1 \geqq \alpha_2 \geqq \cdots \geqq \alpha_n$ angenommen werden kann. Nun sucht man zum Anfangsglied $a\, x_1^{\alpha_1} \ldots x_n^{\alpha_n}$ des gegebenen Polynoms ein Produkt von elementarsymmetrischen Funktionen, welches (ausmultipliziert und lexikographisch geordnet) dasselbe Anfangsglied $a\, x_1^{\alpha_1} \ldots x_n^{\alpha_n}$ besitzt; dieses ist leicht zu finden, nämlich:

$$a\, \sigma_1^{\alpha_1 - \alpha_2} \sigma_2^{\alpha_2 - \alpha_3} \ldots \sigma_n^{\alpha_n}.$$

Dieses Produkt subtrahiert man vom gegebenen Polynom, ordnet wieder lexikographisch, sucht das Anfangsglied usw.

Aufgaben. 1. Man zeige, daß man in dieser Weise immer zum Ziel kommt und leite daraus einen zweiten Beweis für den Hauptsatz sowie für den Eindeutigkeitssatz ab.

2. Man drücke für beliebiges n die „Potenzsummen" $\sum x_1$, $\sum x_1^2$, $\sum x_1^3$ durch die elementarsymmetrischen Funktionen aus.

3. Es sei $\sum x_1^\varrho = s_\varrho$. Man beweise die Formeln

$$s_\varrho - s_{\varrho-1}\sigma_1 + s_{\varrho-2}\sigma_2 - \cdots + (-1)^{\varrho-1} s_1 \sigma_{\varrho-1} + (-1)^\varrho \varrho\, \sigma_\varrho = 0 \quad \text{für } \varrho \leqq n,$$

$$s_\varrho - s_{\varrho-1}\sigma_1 + \cdots + (-1)^n s_{\varrho-n}\sigma_n = 0 \quad \text{für } \varrho > n$$

und drücke mit ihrer Hilfe die Potenzsummen s_1, s_2, s_3, s_4, s_5 durch die elementarsymmetrischen Funktionen aus.

4. Setzt man, dem Hauptsatz entsprechend:

$$s_\varrho = \sum a_{\lambda_1, \ldots, \lambda_n} \sigma_1^{\lambda_1} \sigma_2^{\lambda_2} \ldots \sigma_n^{\lambda_n}$$

(Summation über alle λ_i mit $\lambda_1 + 2\lambda_2 + 3\lambda_3 + \cdots = \varrho$), so erhält man aus Aufgabe 3 für die $a_{\lambda_1, \ldots, \lambda_n}$ die Rekursionsformeln:

$$a_{\lambda_1, \ldots, \lambda_n} = a_{\lambda_1 - 1, \lambda_2, \ldots, \lambda_n} - a_{\lambda_1, \lambda_2 - 1, \ldots, \lambda_n} + \cdots [+ (-1)^{\varrho-1} \varrho],$$

wo das Glied in eckiger Klammer nur dann (und zwar als einziges)

auftritt, wenn $\lambda_\varrho = 1$ ist und alle übrigen $\lambda_i = 0$ sind, und wo alle a mit einem negativen Index gleich Null zu setzen sind. Man zeige, daß die Lösung dieser rekursiven Beziehung lautet:

$$a_{\lambda_1, \ldots, \lambda_n} = (-1)^{\lambda_2 + \lambda_4 + \lambda_6 + \cdots} \frac{\varrho \cdot (\lambda_1 + \lambda_2 + \cdots + \lambda_n - 1)!}{\lambda_1! \lambda_2! \cdots \lambda_n!}.$$

5. Es sei gesetzt

$$(k_1, \ldots, k_h) = \sum x_1^{k_1} x_2^{k_2} \cdots x_h^{k_h}$$

mit Summation über alle *verschiedenen* permutierten Glieder, die entstehen, wenn man statt $1, 2, \ldots, h$ eine andere Indexfolge nimmt. Zu beweisen:

$$\begin{aligned}(k_1, \ldots, k_h) \cdot (m) &= c_1(k_1 + m, k_2, \ldots, k_h) \\ &+ c_2(k_1, k_2 + m, \ldots, k_h) + \cdots \\ &+ c_h(k_1, k_2, \ldots, k_h + m) + c_0(k_1, \ldots, k_h, m),\end{aligned}$$

wobei die Koeffizienten $c_i (i = 1, \ldots, h)$ bzw. c_0 angeben, wie viele der ganzen Zahlen im danebenstehenden Symbol gleich $k_i + m$ bzw. gleich m sind.

6. Man löse die in Aufg. 5 gefundene Formel nach $(k_1, \ldots, k_h, m)$ auf und leite daraus ein Rechenverfahren ab, mit dessen Hilfe beliebige symmetrische Funktionen durch die Potenzsummen (m) ausgedrückt werden können (vorausgesetzt, daß im zugrundegelegten Ring die Division durch beliebige von Null verschiedene ganze Zahlen erlaubt ist).

Eine wichtige symmetrische Funktion ist das Quadrat des Differenzenprodukts:

$$D = \prod_{i<k} (x_i - x_k)^2.$$

Der Ausdruck von D als Polynom in $a_1 = -\sigma_1$, $a_2 = \sigma_2, \ldots, a_n = (-1)^n \sigma_n$ heißt die *Diskriminante* des Polynoms $f(z) = z^n + a_1 z^{n-1} + \cdots + a_n$; das Verschwinden der Diskriminante für spezielle $a_1, \ldots, a_n$ gibt an, daß $f(z)$ einen mehrfachen Linearfaktor enthält.

Durch Anwendung der oben erklärten allgemeinen Methode findet man für die Diskriminanten

von $x^2 + a_1 x + a_2$:

$$D = a_1^2 - 4 a_2,$$

von $x^3 + a_1 x^2 + a_2 x + a_3$:

$$D = a_1^2 a_2^2 - 4 a_2^3 - 4 a_1^3 a_3 - 27 a_3^2 + 18 a_1 a_2 a_3.$$

Aufgabe. 7. Die Diskriminante bleibt bei der Ersetzung aller x_i durch $x_i + h$ invariant. Daraus ist die Differentialbedingung

$$\Omega D = n \frac{\partial D}{\partial a_1} + (n-1) a_1 \frac{\partial D}{\partial a_2} + \cdots + a_{n-1} \frac{\partial D}{\partial a_n} = 0$$

abzuleiten.

Fünftes Kapitel.

Körpertheorie.

Ziel dieses Kapitels ist, über die Struktur der kommutativen Körper, über ihre einfachsten Unterkörper und Erweiterungskörper eine erste Übersicht zu gewinnen. Indessen gelten einige der folgenden Untersuchungen (§§ 25, 26, 28) auch für nichtkommutative Körper.

§ 25. Unterkörper. Primkörper.

Σ sei ein Körper.

Wenn eine Untermenge Δ von Σ wieder ein Körper ist, so heißt sie *Unterkörper* von Σ. Dazu ist notwendig und hinreichend, daß Δ erstens ein Unterring ist (d. h. mit a und b auch $a - b$ und $a \cdot b$ enthält), zweitens das Einselement und zu jedem $a \neq 0$ auch das Inverse a^{-1} enthält. Statt dessen kann man auch verlangen, daß Δ ein von Null verschiedenes Element mit a und b auch $a - b$ und ab^{-1} enthält.

Klar ist:

Der Durchschnitt beliebig vieler Unterkörper von Σ ist wieder ein Unterkörper von Σ.

Ein *Primkörper* ist ein Körper, der keinen echten Unterkörper enthält.

In jedem Körper Σ gibt es einen und nur einen Primkörper.

Beweis: Der Durchschnitt *aller* Unterkörper von Σ ist ein Körper, der offenbar keinen echten Unterkörper mehr hat.

Gäbe es zwei verschiedene Primkörper, so wäre ihr Durchschnitt wieder Unterkörper von beiden, also mit beiden identisch; die beiden wären also doch nicht verschieden.

Typen von Primkörpern. Π sei der in Σ enthaltene Primkörper. Er enthält die Null und die Einheit e, also auch alle ganzzahligen Vielfachen $n \cdot e = \pm \Sigma e$.

Die Addition und Multiplikation dieser Elemente ne geschieht nach den Regeln:

$$ne + me = (n + m)e,$$

$$ne \cdot me = nm \cdot e^2 = nm \cdot e.$$

Die ganzzahligen Vielfachen ne bilden also einen kommutativen Ring $\mathfrak{P}$. Weiter ist durch $n \to ne$ eine homomorphe Abbildung des Ringes C der ganzen Zahlen auf den Ring $\mathfrak{P}$ gegeben. Nach dem Homomorphiesatz (§ 14) ist daher $\mathfrak{P}$ isomorph einem Restklassenring $C/\mathfrak{p}$, wo $\mathfrak{p}$ das Ideal derjenigen ganzen Zahlen n ist, denen die Null zugeordnet wird, also für die $ne = 0$ gilt. (In vielen bekannten Körpern ist $ne = 0$ nur für $n = 0$ möglich, also $\mathfrak{p}$ das Nullideal. Dagegen gilt z. B. im Körper $C/(p)$ der Restklassen nach einer Primzahl p die Gleichung $pe = 0$.)

Da $\mathfrak{P}$ keine Nullteiler hat, kann $C/\mathfrak{p}$ auch keine haben; also muß $\mathfrak{p}$ ein Primideal sein. Weiter kann $\mathfrak{p}$ nicht das Einheitsideal sein; denn sonst wäre schon $1 \cdot e = 0$. Es gibt also zwei Möglichkeiten:

1. $\mathfrak{p} = (p)$, wo p eine Primzahl ist. p ist dann die kleinste positive Zahl mit der Eigenschaft $pe = 0$. Es folgt

$$\mathfrak{P} \cong C/(p).$$

$C/(p)$ ist ein Körper; also ist auch der Ring $\mathfrak{P}$ ein Körper, stellt somit den gesuchten Primkörper dar. *In diesem Fall ist also der Primkörper Π isomorph dem Restklassenring nach einer Primzahl im Ring der ganzen Zahlen: mit den Elementen $n \cdot e$ wird gerechnet wie mit den Restklassen der Zahlen n mod p.*

2. $\mathfrak{p} = (0)$. Die Homomorphie $C \to \mathfrak{P}$ wird eine 1-Isomorphie. Die Vielfachen ne sind in diesem Falle alle verschieden: aus $ne = 0$ folgt $n = 0$. In diesem Falle ist der Ring $\mathfrak{P}$ noch kein Körper; denn der Ring der ganzen Zahlen ist keiner. Der Primkörper Π muß nicht nur die Elemente von $\mathfrak{P}$, sondern auch deren Quotienten enthalten. Nun wissen wir aus § 12, daß die isomorphen Integritätsbereiche $\mathfrak{P}, C$ auch isomorphe Quotientenkörper haben müssen, mithin ist in diesem Falle *der Primkörper Π isomorph dem Körper Γ der rationalen Zahlen.*

Demnach ist allgemein die Struktur des in Σ enthaltenen Primkörpers völlig bestimmt durch Angabe der Zahl p oder 0, welche das Ideal $\mathfrak{p}$ erzeugt. ($\mathfrak{p}$ besteht, wie gesagt, aus den Zahlen n mit der Eigenschaft $ne = 0$.) Die Zahl p bzw. 0 heißt die *Charakteristik* des Körpers Σ oder des Primkörpers Π. Der Primkörper Π ist stets kommutativ.

Alle gewöhnlichen Zahl- und Funktionenkörper, welche den Körper der rationalen Zahlen umfassen, haben die Charakteristik Null.

Die Definition der Charakteristik führt sofort zu folgendem Satz:

Es sei $a \neq 0$ ein Element von Σ, und k sei die Charakteristik von Σ. Dann folgt aus $na = ma$ stets $n \equiv m\,(k)$ und umgekehrt.

Beweis: Multipliziert man die Gleichung $na = ma$ mit a^{-1}, so folgt $ne = me$ und daraus nach Definition der Charakteristik $n \equiv m\,(k)$. Der Schluß ist umkehrbar.

Ebenso beweist man, daß aus $na = nb$ und $n \not\equiv 0\,(k)$ folgt $a = b$.

Eine wichtige Rechnungsregel sei noch hergeleitet:

In kommutativen Körpern der Charakteristik p ist

$$(a + b)^p = a^p + b^p,$$

$$(a - b)^p = a^p - b^p.$$

Beweis: Es gilt der Binomialsatz (§ 10, Aufg. 5):

$$(a + b)^p = a^p + \binom{p}{1} a^{p-1} b + \cdots + \binom{p}{p-1} a\, b^{p-1} + b^p.$$

Nun ist aber für $0 < i < p$:

$$\binom{p}{i} = \frac{p(p-1)\ldots(p-i+1)}{1 \cdot 2 \cdots i} \equiv 0\,(p),$$

weil der Zähler den Faktor p enthält, der sich nicht wegkürzen kann. Also bleiben nur die Glieder a^p und b^p stehen:

$$(a + b)^p = a^p + b^p.$$

Setzt man hier $a + b = a'$, so kommt

$$a'^p = (a' - b)^p + b^p,$$

$$(a' - b)^p = a'^p - b^p,$$

womit beide Behauptungen bewiesen sind.

Aufgaben. 1. Man beweise für Charakteristik p durch Induktion nach f:

$$(a + b)^{p^f} = a^{p^f} + b^{p^f},$$

$$(a - b)^{p^f} = a^{p^f} - b^{p^f}.$$

2. Ebenso:

$$(a_1 + a_2 + \cdots + a_n)^p = a_1^p + a_2^p + \cdots + a_n^p.$$

3. Man wende Aufg. 2 auf eine Summe $1 + 1 + \cdots + 1$ modulo p an.

4. Man beweise für Charakteristik p:

$$(a - b)^{p-1} = \sum_{j=0}^{p-1} a^j b^{p-1-j}.$$

5. Welche Charakteristik haben die Restklassenringe der Primideale $(1 + i)$, (3), $(2 + i)$ im Ring der ganzen Gaußschen Zahlen? (§ 15, Aufg. 3.)

§ 26. Adjunktion.

Ist Δ ein Unterkörper von Ω, so heißt Ω ein *Erweiterungskörper* oder *Oberkörper* von Δ. Unser Ziel ist, eine Übersicht über alle möglichen Erweiterungen eines vorgegebenen Körpers Δ zu erhalten. Damit würde zugleich eine Übersicht über alle überhaupt möglichen Körper gewonnen sein, da ja jeder Körper als Erweiterung des darin enthaltenen Primkörpers aufgefaßt werden kann. Allerdings ist das gesteckte Ziel nur im kommutativen Fall in den wichtigsten Teilen als erreicht zu betrachten.

Zunächst sei Ω ein vorgelegter Erweiterungskörper von Δ, und $\mathfrak{S}$ sei eine beliebige Menge von Elementen aus Ω. Es gibt Körper, die Δ und $\mathfrak{S}$ umfassen; denn Ω ist ein solcher. Der Durchschnitt aller Körper, die Δ und $\mathfrak{S}$ umfassen, ist selbst ein Körper, der Δ und $\mathfrak{S}$ umfaßt, und wird mit $\Delta(\mathfrak{S})$ bezeichnet. Er ist der kleinste Körper, der Δ und $\mathfrak{S}$ umfaßt. Wir sagen, daß $\Delta(\mathfrak{S})$ aus Δ durch *Adjunktion* (und zwar Körperadjunktion) der Menge $\mathfrak{S}$ hervorgeht. Es ist

$$\Delta \subseteq \Delta(\mathfrak{S}) \subseteq \Omega,$$

und die beiden Extremfälle sind: $\Delta(\mathfrak{S}) = \Delta$, $\Delta(\mathfrak{S}) = \Omega$.

Zu $\Delta(\mathfrak{S})$ gehören alle Elemente von Δ und alle von $\mathfrak{S}$, also auch alle die Elemente, die durch Addition, Subtraktion, Multiplikation und Division aus Elementen von Δ und $\mathfrak{S}$ hervorgehen. Diese Elemente

zusammen bilden aber schon einen Körper, der folglich mit $\Delta(\mathfrak{S})$ identisch sein muß. Mithin: $\Delta(\mathfrak{S})$ *besteht aus allen rationalen Verbindungen der Elemente von* $\mathfrak{S}$ *mit denen von* Δ. Im kommutativen Fall lassen sich diese Verbindungen einfach schreiben als Quotienten ganzer rationaler Funktionen der Elemente von $\mathfrak{S}$ mit Koeffizienten aus Δ.

Ist $\mathfrak{S}$ eine endliche Menge: $\mathfrak{S} = \{u_1, \ldots, u_n\}$, so schreibt man für $\Delta(\mathfrak{S})$ auch $\Delta(u_1, \ldots, u_n)$. Man spricht dann auch von Adjunktion der Elemente $u_1, \ldots, u_n$ zu Δ. Die runden Klammern bedeuten demnach immer Körperadjunktion, während eckige Klammern, z. B. $\Delta[x]$, die Ringadjunktion (Bildung aller *ganzen* rationalen Verbindungen) bezeichnen.

In dem rationalen Ausdruck eines Elements von $\Delta(\mathfrak{S})$ durch Elemente von Δ und von $\mathfrak{S}$ kommen auf jeden Fall nur endlichviele Elemente von $\mathfrak{S}$ vor. Jedes Element des Körpers $\Delta(\mathfrak{S})$ liegt also schon in einem Körper $\Delta(\mathfrak{T})$, wo $\mathfrak{T}$ eine endliche Untermenge von $\mathfrak{S}$ ist. *Demnach ist* $\Delta(\mathfrak{S})$ *die Vereinigungsmenge aller Körper* $\Delta(\mathfrak{T})$, *wo* $\mathfrak{T}$ *jeweils eine endliche Untermenge von* $\mathfrak{S}$ *ist.* Die Adjunktion einer beliebigen Menge ist damit zurückgeführt auf Adjunktionen endlicher Mengen und Bildung einer Vereinigungsmenge.

Ist $\mathfrak{S}$ die Vereinigungsmenge von $\mathfrak{S}_1$ und $\mathfrak{S}_2$, so ist offenbar

$$\Delta(\mathfrak{S}) = \Delta(\mathfrak{S}_1)(\mathfrak{S}_2).$$

Denn $\Delta(\mathfrak{S}_1)(\mathfrak{S}_2)$ umfaßt $\Delta(\mathfrak{S}_1)$ und $\mathfrak{S}_2$, folglich Δ, $\mathfrak{S}_1$ und $\mathfrak{S}_2$, folglich Δ und $\mathfrak{S}$, also $\Delta(\mathfrak{S})$, und umgekehrt umfaßt $\Delta(\mathfrak{S})$ sicher Δ, $\mathfrak{S}_1$ und $\mathfrak{S}_2$, also $\Delta(\mathfrak{S}_1)$ und $\mathfrak{S}_2$, also $\Delta(\mathfrak{S}_1)(\mathfrak{S}_2)$.

Die Adjunktion einer endlichen Menge ist demnach zurückführbar auf endlichviele sukzessive Adjunktionen eines einzigen Elementes. Erweiterungen durch Adjunktion eines einzigen Elements nennt man *einfache Körpererweiterungen.* Solche wollen wir im nächsten Paragraphen studieren, und zwar im kommutativen Fall.

§ 27. Einfache Körpererweiterungen.

Alle in diesem Paragraphen zu betrachtenden Körper sollen kommutativ sein. Es sei wieder $\Delta \subseteq \Omega$, und Θ sei ein beliebiges Element von Ω; wir untersuchen den einfachen Erweiterungskörper $\Delta(\Theta)$.

Dieser Körper umfaßt zunächst den Ring $\mathfrak{S}$ aller Polynome $\sum a_k \Theta^k$ ($a_k \in \Delta$). Wir vergleichen $\mathfrak{S}$ mit dem Polynombereich $\Delta[x]$ einer Unbestimmten x.

Durch die Abbildung $f(x) \to f(\Theta)$, genauer:

$$\sum a_k x^k \to \sum a_k \Theta^k$$

ist $\Delta[x]$ homomorph auf $\mathfrak{S}$ abgebildet[1]. Nach dem Homomorphiesatz

[1] Im nichtkommutativen Fall ist dies falsch, weil die Variable x immer als mit dem Koeffizienten a_k vertauschbar angenommen wurde, die Größe Θ es aber nicht zu sein braucht. Nur wenn speziell Θ mit allen Elementen von Δ vertauschbar ist, gelten alle Betrachtungen dieses Paragraphen.

ist also $\mathfrak{S}$ isomorph einem Restklassenring:

$$\mathfrak{S} \cong \Delta[x]/\mathfrak{p},$$

wo $\mathfrak{p}$ das Ideal derjenigen Polynome $f(x)$ ist, welche die Nullstelle Θ besitzen, d. h. für welche $f(\Theta) = 0$ ist.

Da $\mathfrak{S}$ keine Nullteiler hat, so muß auch $\Delta[x]/\mathfrak{p}$ nullteilerfrei, mithin das Ideal $\mathfrak{p}$ prim sein. Weiter kann $\mathfrak{p}$ nicht das Einheitsideal sein, da dem Einheitselement e bei der Homomorphie nicht die Null, sondern e selbst zugeordnet wird. Da in $\Delta[x]$ jedes Ideal Hauptideal ist, so bleiben nur zwei Möglichkeiten:

1. $\mathfrak{p} = (\varphi(x))$, wo $\varphi(x)$ ein in $\Delta[x]$ unzerlegbares Polynom ist[1]. $\varphi(x)$ ist ein Polynom niedrigsten Grades mit der Eigenschaft $\varphi(\Theta) = 0$. Es folgt:

$$\mathfrak{S} \cong \Delta[x]/(\varphi(x)).$$

Der Restklassenring rechts ist ein Körper (§ 17); also ist auch der Ring $\mathfrak{S}$ ein Körper. Demnach ist $\mathfrak{S}$ der gesuchte einfache Erweiterungskörper $\Delta(\Theta)$.

2. $\mathfrak{p} = (0)$. Der Homomorphismus $\Delta[x] \sim \mathfrak{S}$ wird zu einem Isomorphismus. Es gibt außer der Null kein Polynom $f(x)$ mit der Eigenschaft $f(\Theta) = 0$, und mit den Ausdrücken $f(\Theta)$ wird gerechnet, als ob Θ eine Unbestimmte x wäre. Der Ring $\mathfrak{S} \cong \Delta[x]$ ist in diesem Fall noch kein Körper; aber aus der 1-Isomorphie dieser Ringe folgt eine Isomorphie ihrer Quotientenkörper: *Der Körper* $\Delta(\Theta)$, *Quotientenkörper von* $\mathfrak{S}$, *ist* 1*-isomorph dem Körper der rationalen Funktionen einer Unbestimmten* x.

Im ersten Fall, wo Θ einer algebraischen Gleichung $\varphi(\Theta) = 0$ in Δ genügt, heißt Θ *algebraisch in bezug auf* Δ und der Körper $\Delta(\Theta)$ eine *einfache algebraische Erweiterung* von Δ; im zweiten Fall, wo aus $f(\Theta) = 0$ folgt $f(x) = 0$, heißt Θ *transzendent in bezug auf* Δ und der Körper $\Delta(\Theta)$ eine *einfache transzendente Erweiterung* von Δ. Mit einer Transzendenten wird nach dem Obigen gerechnet wie mit einer Unbestimmten: es ist $\Delta(\Theta) \cong \Delta(x)$. Im algebraischen Fall dagegen gilt nach dem Obigen:

$$\Delta(\Theta) = \mathfrak{S} \cong \Delta[x]/(\varphi(x)),$$

wo $\varphi(x)$ das (unzerlegbare) Polynom niedrigsten Grades mit der Nullstelle Θ ist.

Aus der letzten Relation ergeben sich im algebraischen Fall folgende Tatsachen:

a) Jede rationale Funktion von Θ ist auch als Polynom $\sum a_k \Theta^k$ zu schreiben. (Denn $\mathfrak{S}$ war definiert als die Gesamtheit dieser Polynome.)

b) Mit diesen Polynomen wird gerechnet wie mit Restklassen modulo $\varphi(x)$ im Polynombereich $\Delta[x]$.

[1] Für „Unzerlegbar in $\Delta[x]$" sagt man gelegentlich auch weniger exakt: „Unzerlegbar im Körper Δ". Besser wäre vielleicht: „Unzerlegbar über dem Körper Δ".

c) Eine Gleichung

$$f(\Theta) = 0$$

läßt sich in eine Kongruenz

$$f(x) \equiv 0(\varphi(x))$$

verwandeln und umgekehrt.

d) Da jedes Polynom $f(x)$ modulo $\varphi(x)$ auf ein Polynom vom Grade $< n$ reduzierbar ist, wo n der Grad von $\varphi(x)$ ist, so lassen sich alle Größen von $\Delta(\Theta)$ in der Gestalt $\beta = \sum_{k=0}^{n-1} a_k \Theta^k$ schreiben.

e) Da Θ keiner Gleichung von niedrigerem als n-tem Grade genügt, so ist die Darstellung

$$\beta = \sum_{k=0}^{n-1} a_k \Theta^k$$

der Elemente von $\Delta(\Theta)$ eindeutig.

Die irreduzible Gleichung $\varphi(x) = 0$, deren Lösung oder *Wurzel* Θ ist, heißt die *definierende Gleichung* des Körpers $\Delta(\Theta)$. Der Grad des Polynoms $\varphi(x)$ heißt der *Grad* der algebraischen Größe Θ in bezug auf Δ.

Der Grad ist gleich 1, wenn Θ eine Lösung einer *linearen* Gleichung in Δ ist, also selbst dem Körper Δ angehört. Man kann dann $\varphi(x) = x - \Theta$ wählen. Der obige Satz c) ergibt somit von neuem die schon in § 19 bewiesene Tatsache:

Jedes Polynom $f(x)$ mit der Nullstelle Θ ist durch $x - \Theta$ teilbar.

Aufgaben. 1. Man beweise für den Fall einer einfachen algebraischen Erweiterung die Irreduzibilität des Minimalpolynoms $\varphi(x)$ sowie die Tatsachen a) bis e) direkt, d. h. ohne Benutzung des Homomorphiesatzes und der Körpereigenschaft von $\Delta[x]/(\varphi(x))$. [Reihenfolge der Behauptungen: Irreduzibilität, c), b), a), d), e). Bei a) benutze man c).]

2. Man zeige weiter, daß $\varphi(x)$ bis auf konstante Faktoren das einzige in $\Delta[x]$ irreduzible Polynom mit der Nullstelle Θ ist.

3. Was sind der Grad des erzeugenden Elements und die definierende Gleichung

a) des Körpers der komplexen in bezug auf den der reellen Zahlen;

b) des Körpers $\Gamma(\sqrt[5]{3})$ in bezug auf den Körper Γ der rationalen Zahlen;

c) des Körpers $\Gamma\left(e^{\frac{2\pi i}{5}}\right)$ in bezug auf den Körper Γ der rationalen Zahlen;

d) des Körpers $C[i]/(7)$ in bezug auf den darin enthaltenen Primkörper? ($C[i]$ ist der Ring der ganzen Gaußschen Zahlen.)

4. Es sei Γ ein kommutativer Grundkörper, z eine Unbestimmte, $\Sigma = \Gamma(z)$, $\Delta = \Gamma\left(\frac{z^3}{z+1}\right)$. Man zeige, daß Σ eine einfache algebraische

Erweiterung von Δ ist. Welches ist die in Δ irreduzible Gleichung, der das Element z genügt?

Zwei Erweiterungen Σ, Σ' eines Körpers Δ heißen *äquivalent* (in bezug auf Δ), wenn es einen 1-Isomorphismus $\Sigma \cong \Sigma'$ gibt, der jedes Element von Δ in sich selbst überführt (fest läßt).

Je zwei einfache transzendente Erweiterungen eines Körpers Δ sind äquivalent.

Denn vermöge $\frac{f(x)}{g(x)} \to \frac{f(\Theta)}{g(\Theta)}$ ist jede einfache transzendente Erweiterung $\Delta(\Theta)$ äquivalent dem Körper der rationalen Funktionen der Unbestimmten x.

Je zwei einfache algebraische Erweiterungen $\Delta(\alpha)$, $\Delta(\beta)$ sind äquivalent, sobald α und β Nullstellen desselben in $\Delta[x]$ irreduziblen Polynoms $\varphi(x)$ sind, und zwar gibt es dann eine solche 1-Isomorphie, welche die Elemente von Δ fest läßt und α in β überführt.

Beweis: Die Elemente von $\Delta(\alpha)$ haben die Gestalt $\sum_0^{n-1} a_k \alpha^k$ und die von $\Delta(\beta)$ die Gestalt $\sum_0^{n-1} a_k \beta^k$. Mit diesen Elementen wird beide Male gerechnet wie mit Polynomen modulo $\varphi(x)$. Die Zuordnung

$$\sum a_k \alpha^k \to \sum a_k \beta^k$$

ist also eine Isomorphie von der gesuchten Art.

Ein in Δ irreduzibles Polynom $\varphi(x)$ braucht in einem Erweiterungskörper Ω nicht irreduzibel zu bleiben. Hat es in Ω eine Nullstelle Θ, so spaltet es mindestens einen Linearfaktor $x - \Theta$ ab. Möglicherweise zerfällt es in Ω noch weiter in lineare und nichtlineare Faktoren:

$$\varphi(x) = (x - \Theta)(x - \Theta_2) \ldots (x - \Theta_j)\, \varphi_1(x) \ldots \varphi_k(x).$$

Nach dem oben Bewiesenen sind in diesem Fall die Körper $\Delta(\Theta)$, $\Delta(\Theta_2)$, $\ldots$, $\Delta(\Theta_j)$ alle äquivalent, und bei den Isomorphismen

$$\Delta(\Theta) \cong \Delta(\Theta_2) \cong \cdots \cong \Delta(\Theta_j)$$

geht Θ in $\Theta_2, \ldots, \Theta_j$ über.

Äquivalente Erweiterungen [wie $\Delta(\Theta)$, $\Delta(\Theta_2)$, $\ldots$, $\Delta(\Theta_j)$], die einem gemeinsamen Oberkörper Ω angehören, nennt man untereinander *konjugiert* (in bezug auf Δ), und die Größen $\Theta, \Theta_2, \ldots$, die bei den betreffenden 1-Isomorphismen ineinander übergehen, heißen *konjugierte Größen*[1]. Aus dem Bewiesenen folgt: *Alle Nullstellen in Ω eines in $\Delta[x]$ irreduziblen Polynoms $\varphi(x)$ sind untereinander konjugiert in bezug auf Δ.* Umgekehrt sind konjugierte Größen, wenn sie algebraisch sind, stets Nullstellen desselben irreduziblen Polynoms $\varphi(x)$; denn aus $\varphi(\Theta_1) = 0$ folgt, wenn Θ_1 durch eine 1-Isomorphie in Θ_2 übergeht, vermöge ebendieser Isomorphie $\varphi(\Theta_2) = 0$.

[1] Die Bezeichnung wird hauptsächlich auf algebraische Größen Θ angewandt. Transzendente Größen desselben Körpers sind *stets* untereinander konjugiert (s. o.).

Die Existenz der einfachen Erweiterungen. Bis jetzt war immer Ω ein vorgegebener Oberkörper, und es wurde die Struktur der einfachen Erweiterungen $\Delta(\Theta)$ innerhalb Ω studiert. Jetzt aber soll das Problem anders gestellt werden: Gegeben sei ein Körper Δ; gesucht ist eine Erweiterung $\Delta(\Theta)$, wobei von Θ außerdem verlangt wird, entweder daß Θ transzendent oder daß Θ Nullstelle eines vorgegebenen in $\Delta[x]$ irreduziblen Polynoms sein soll.

Soll Θ transzendent sein, so ist die Lösung leicht: Man nehme für Θ eine Unbestimmte:

$$\Theta = x,$$

bilde den Polynombereich $\Delta[x]$ und dessen Quotientenkörper $\Delta(x)$, den „Körper der rationalen Funktionen der Unbestimmten x". Wie wir sahen, ist $\Delta(x)$ bis auf äquivalente Erweiterungen die einzige einfache transzendente Erweiterung; mithin:

Es gibt eine und bis auf äquivalente Erweiterungen nur eine einfache transzendente Erweiterung $\Delta(\Theta)$ eines vorgegebenen Körpers Δ.

Soll zweitens Θ algebraisch sein, und zwar Nullstelle des in $\Delta[x]$ irreduziblen Polynoms $\varphi(x)$, so können wir zunächst annehmen, daß φ nicht linear ist, da sonst $\Delta(\Theta) = \Delta$ genommen werden kann.

Der gesuchte Körper $\Delta(\Theta)$ muß nach dem Vorigen isomorph dem Körper der Restklassen

$$\Sigma' = \Delta[x]/(\varphi(x))$$

sein. Nun ist jedem Polynom f aus $\Delta[x]$ eine Restklasse $\bar{f}$ in Σ' zugeordnet und die Abbildung ist homomorph. Insbesondere entspricht jeder Konstanten a aus Δ eine Restklasse $\bar{a}$ und diese Abbildung von Δ ist nicht nur homomorph, sondern sogar 1-isomorph, da die Null die einzige Konstante ist, die $\equiv 0 \bmod \varphi(x)$ ist. Also können wir nach § 11, Schluß im Körper Σ' die Restklassen $\bar{a}$ durch die ihnen entsprechenden Elemente a von Δ ersetzen; dadurch geht Σ' über in einen Körper Σ, der Δ umfaßt und $\cong \Sigma'$ ist.

Dem Polynom x ist eine Restklasse zugeordnet, welche Θ heißen möge. Wir können also in Σ den Körper $\Delta(\Theta)$ bilden. (Übrigens ist $\Sigma = \Delta(\Theta)$, wie leicht zu sehen.) Aus

$$\varphi(x) = \sum_0^n a_k x^k \equiv 0 \,(\varphi(x))$$

folgt vermöge der Isomorphie

$$\sum_0^n \bar{a}_k \Theta^k = 0 \quad (\text{in } \Sigma')$$

und daraus, wenn die $\bar{a}_k$ durch die a_k ersetzt werden:

$$\varphi(\Theta) = \sum_0^n a_k \Theta^k = 0.$$

Also ist Θ Nullstelle von $\varphi(x)$.

Damit ist bewiesen:

Zu einem vorgegebenen Körper Δ gibt es eine (und bis auf äquivalente Erweiterungen nur eine) einfache algebraische Erweiterung $\Delta(\Theta)$ von der Beschaffenheit, daß Θ einer vorgegebenen in $\Delta[x]$ irreduziblen Gleichung $\varphi(x) = 0$ genügt.

Der beim Beweis benutzte Prozeß der *„symbolischen Adjunktion"* mit Hilfe des Restklassenringes und des Symbols Θ steht in einem gewissen Gegensatz zur unsymbolischen Adjunktion, die möglich ist, wenn man von vornherein über einen umfassenden Körper Ω verfügt, in dem eine Größe Θ mit den verlangten Eigenschaften schon vorhanden ist (vgl. den Anfang dieses Paragraphen). Ist Δ z. B. der Körper der rationalen Zahlen, so kann man die unsymbolische Adjunktion einer algebraischen Zahl, d. h. einer Wurzel einer algebraischen Gleichung, dadurch erreichen, daß man von dem auf transzendentem Wege konstruierten Körper der komplexen Zahlen Ω ausgeht, in dem nach dem „Fundamentalsatz der Algebra" jede Gleichung mit rationalen Zahlenkoeffizienten tatsächlich lösbar ist. Die obige symbolische Adjunktion vermeidet diesen transzendenten Umweg, indem sie direkt die algebraische Zahl als Symbol einer Restklasse einführt und Rechnungsregeln für sie definiert. Dabei werden keine Größenrelationen ($>$, $<$) oder Realitätseigenschaften eingeführt. Trotzdem entsteht auf dem symbolischen und auf dem unsymbolisch-transzendenten Wege stets (algebraisch gesprochen) derselbe Körper $\Delta(\Theta)$; denn nach dem zu Anfang Bewiesenen sind alle möglichen Erweiterungen $\Delta(\Theta)$, deren Θ derselben irreduziblen Gleichung genügen, äquivalent. Sowohl die symbolische wie die unsymbolische Adjunktion fallen nämlich unter den allgemeinen Adjunktionsbegriff des § 26; der einzige Unterschied ist, daß der umfassende Körper Ω oder Σ, der zur Adjunktion erforderlich ist, im einen Fall schon vorher bekannt ist, im anderen Fall ad hoc konstruiert wird.

Genaueres über das Verhältnis von Größenbeziehungen zu algebraischen Relationen findet sich in Kap. 10.

Aufgaben. 5. Das Polynom $x^4 + 1$ ist im Körper Γ der rationalen Zahlen irreduzibel (§ 22, Aufg. 3). Man adjungiere eine Nullstelle Θ und zerlege das Polynom im erweiterten Körper $\Gamma(\Theta)$ in Primfaktoren.

6. Es sei Π der Primkörper der Charakteristik p, x eine Unbestimmte, $\Delta = \Pi(x)$. Man adjungiere an Δ eine Nullstelle $\zeta = x^{\frac{1}{p}}$ des irreduziblen Polynoms $z^p - x$ und zerlege das Polynom $z^p - x$ im erweiterten Körper $\Pi(\zeta)$.

7. Aus dem Primkörper der Charakteristik 2 konstruiere man durch Adjunktion einer Nullstelle einer irreduziblen quadratischen Gleichung einen Körper mit 4 Elementen.

§ 28. Lineare Abhängigkeit von Größen in bezug auf einen Körper.

Es sei $\mathfrak{G}$ ein Ring, der einen Körper Δ umfaßt[1], wobei das Einselement von Δ zugleich Einselement von $\mathfrak{G}$ sein soll.

In den nachfolgenden Anwendungen ist $\mathfrak{G}$ meist ein Erweiterungskörper von Δ; aber die Begriffe werden absichtlich etwas allgemeiner gehalten, da sie später auch auf hyperkomplexe Zahlen anwendbar sein sollen[2].

Griechische Buchstaben $\alpha, \beta, \ldots$ bezeichnen die Elemente des Grundkörpers Δ, lateinische $u, v, \ldots$ die des Erweiterungsrings $\mathfrak{G}$.

Ein Element v heißt von $u_1, \ldots, u_n$ *linear-abhängig* (in bezug auf Δ), wenn

$$v = \alpha_1 u_1 + \cdots + \alpha_n u_n$$

ist.

Die Elemente $u_1, \ldots, u_n$ heißen *untereinander linear-abhängig*, falls eine Relation

$$\alpha_1 u_1 + \cdots + \alpha_n u_n = 0 \tag{1}$$

besteht, ohne daß alle α_i verschwinden. Ist etwa $\alpha_1 \neq 0$, so ist u_1 linear-abhängig von $u_2, \ldots, u_n$; denn man kann die Gleichung (1) mit α_1^{-1} multiplizieren und nach u_1 auflösen.

Besteht keine Gleichung von der Form (1), ohne daß

$$\alpha_1 = \cdots = \alpha_n = 0$$

ist, so heißen $u_1, \ldots, u_n$ *linear-unabhängig*. So sind z. B., wenn β ein algebraisches Element n-ten Grades in bezug auf Δ ist, die Potenzen

$$1, \beta, \beta^2, \ldots, \beta^{n-1}$$

linear-unabhängig; denn β genügt keiner Gleichung

$$\alpha_0 + \alpha_1 \beta + \cdots + \alpha_{n-1} \beta^{n-1} = 0$$

von niedrigerem als n-tem Grad.

Klar ist:

Satz 1. *Hängen $v_1, \ldots, v_s$ von $u_1, \ldots, u_r$ (linear) ab und ebenso w von $v_1, \ldots, v_s$, so hängt w auch von $u_1, \ldots, u_r$ ab.*

Satz 2. *Sind $u_1, \ldots, u_{s-1}$ linear-unabhängig, aber $u_1, \ldots, u_s$ linear-abhängig, so ist u_s linear abhängig von $u_1, \ldots, u_{s-1}$.*

Beweis: In der Gleichung

$$\sum \alpha_\nu u_\nu = 0$$

muß $\alpha_s \neq 0$ sein.

---

[1] Δ und $\mathfrak{G}$ brauchen nicht kommutativ zu sein.

[2] Die Sätze dieses Paragraphen gelten sogar dann noch, wenn $\mathfrak{G}$ kein Ring, sondern nur ein Δ-Modul (eine Abelsche Gruppe mit Δ als Operatorenbereich; vgl. Kap. 6) ist. Das Einselement von Δ muß dann zugleich Einheitsoperator sein.

Satz 3. *In jeder endlichen Menge* $\{u_1, \ldots, u_s\}$ *von Größen, die nicht alle Null sind, gibt es ein linear-unabhängiges Teilsystem* $\{u_{i_1}, \ldots, u_{i_r}\}$, *von dem die übrigen* u_j *linear abhängen.*

Beweis: Man suche aus der Menge $\{u_1, \ldots, u_s\}$ ein Teilsystem von möglichst vielen linear-unabhängigen Größen. Von diesen muß nun nach Satz 2 jedes weitere u linear abhängen.

Man nennt zwei Systeme $\{u_1, \ldots, u_r\}$ und $\{v_1, \ldots, v_s\}$ (linear-) *äquivalent,* wenn jedes u_i linear von den v_j und jedes v_j linear von den u_i abhängt. Die Äquivalenzrelation ist offenbar reflexiv und symmetrisch und nach Satz 1 auch transitiv. Man kann jetzt Satz 3 auch so formulieren: *Jede endliche Menge ist einem linear-unabhängigen Teilsystem äquivalent.*

Zur Gewinnung von Aussagen über Anzahlgleichheit äquivalenter irreduzibler Systeme und dgl. bedient man sich zweckmäßig des folgenden, von STEINITZ herrührenden *Austauschsatzes*:

Satz 4. *Sind* $v_1, \ldots, v_s$ *untereinander linear-unabhängig und alle linear-abhängig von* $u_1, \ldots, u_r$, *so gibt es in* $\{u_1, \ldots, u_r\}$ *ein Teilsystem* $\{u_{i_1}, \ldots, u_{i_s}\}$ *von genau s Elementen, welches man gegen das System* $\{v_1, \ldots, v_s\}$ *austauschen kann, so daß das durch diesen Austausch aus* $\{u_1, \ldots, u_r\}$ *entstehende System dem ursprünglichen System* $\{u_1, \ldots, u_r\}$ *äquivalent ist.*

Beweis: Für $s = 0$ ist die Behauptung trivial; denn dann gibt es keine v_i, und es wird gar nichts ausgetauscht. Die Behauptung sei also für $\{v_1, \ldots, v_{s-1}\}$ schon bewiesen, und es sei etwa $\{v_1, \ldots, v_{s-1}\}$ gegen $\{u_{i_1}, \ldots, u_{i_{s-1}}\}$ austauschbar. v_s hängt vom System $\{u_1, \ldots, u_r\}$ also auch vom neuen (durch Austausch der u_{i_ν} gegen die v_ν entstehenden) System linear ab. Aber v_s hängt nicht von $v_1, \ldots, v_{s-1}$ allein linear ab (da $v_1, \ldots, v_s$ linear-unabhängig sein sollten). Also kommt im linearen Ausdruck für v_s ein u_i, das wir u_{i_s} nennen können, wirklich vor:

$$v_s = \alpha_1 v_1 + \cdots + \alpha_{s-1} v_{s-1} + \alpha_s u_{i_s} + \cdots; \quad \alpha_s \neq 0.$$

Multipliziert man diese Gleichung mit α_s^{-1} und löst nach u_{i_s} auf, so folgt, daß umgekehrt u_{i_s} von den übrigen nicht ausgetauschten u_j und den v_ν (inklusive v_s) abhängt. Tauscht man noch u_{i_s} gegen v_s aus, so hängen alle u_i von den nichtausgetauschten u_j und den v_ν ab (und umgekehrt), q. e. d.

Aus Satz 4 folgt insbesondere:

$$s \leqq r. \tag{2}$$

Eine weitere Folgerung ist:

Satz 5. *Sind* $\{u_1, \ldots, u_r\}$ *und* $\{v_1, \ldots, v_s\}$ *zwei untereinander äquivalente, einzeln linear-unabhängige Systeme, so muß* $r = s$ *sein.*

Beweis: Nach dem Obigen ist sowohl $r \leqq s$ wie $r \geqq s$.

Wenn alle Größen des Bereichs $\mathfrak{G}$ von endlichvielen $u_1, \ldots, u_n$ in bezug auf Δ linear abhängen, so heißt der Bereich $\mathfrak{G}$ *endlich in bezug*

auf Δ (*endlicher Erweiterungsring* bzw. *-körper* von Δ). Infolge von Satz 3 können wir aus den $u_1, \ldots, u_n$ ein äquivalentes linear-unabhängiges Teilsystem, etwa $\{u_1, \ldots, u_r\}$, auswählen. Ein solches linear unabhängiges System $\{u_1, \ldots, u_r\}$, von dem alle Elemente von $\mathfrak{G}$ linear abhängen, heißt eine *Basis*, genauer Δ-Basis (auch „Minimalbasis" oder „linear-unabhängige Basis"; speziell, wenn $\mathfrak{G}$ ein Körper ist: „Körperbasis") des Systems $\mathfrak{G}$ in bezug auf Δ.[1] Wählen wir statt $\{u_1, \ldots, u_r\}$ eine andere Basis $\{v_1, \ldots, v_s\}$, so muß (nach Satz 5) $r = s$ sein; *also ist die Anzahl r der Basiselemente eindeutig bestimmt.* Man nennt sie den *Grad* oder *linearen Rang* der endlichen Erweiterung $\mathfrak{G}$ *in bezug auf* Δ.

Beispielsweise ist eine einfache Körpererweiterung $\Delta(\Theta)$, erzeugt von einem algebraischen Element n-ten Grades Θ, stets endlich und vom Grade n; denn die Größen $1, \Theta, \Theta^2, \ldots, \Theta^{n-1}$ bilden eine Basis.

Auf Grund der linearen Unabhängigkeit der Elemente $u_1, \ldots, u_r$ einer Basis ist die Darstellung eines beliebigen Elements u von $\mathfrak{G}$:

$$u = a_1 u_1 + \cdots + a_r u_r,$$

stets *eindeutig*; denn aus

$$a_1 u_1 + \cdots + a_r u_r = b_1 u_1 + \cdots + b_r u_r$$

folgt

$$\Sigma (a_i - b_i) u_i = 0, \quad \text{also} \quad a_i - b_i = 0.$$

Satz 6. *Ist* $\mathfrak{G}$ *endlich in bezug auf* Δ, *so ist jedes Teilsystem* $\mathfrak{H}$[2] *von* $\mathfrak{G}$ *wieder endlich, und jede Basis* $\{v_1, \ldots, v_s\}$ *von* $\mathfrak{H}$ *kann zu einer Basis von* $\mathfrak{G}$ *ergänzt werden.*

Beweis: Nach Satz 4 gibt es in $\mathfrak{H}$ höchstens r linear-unabhängige Elemente. Es sei $\{v_1, \ldots, v_s\}$ ein System von möglichst vielen solchen linear-unabhängigen Größen. Dann muß offenbar jede weitere Größe aus $\mathfrak{H}$ von $v_1, \ldots, v_s$ abhängen; also bilden $v_1, \ldots, v_s$ eine Basis. Es sei nun weiter $\{u_1, \ldots, u_r\}$ ein das System $\{v_1, \ldots, v_s\}$ umfassendes System von möglichst vielen linear-unabhängigen Größen in $\mathfrak{G}$; dann sieht man in derselben Weise, daß $u_1, \ldots, u_r$ eine Basis für $\mathfrak{G}$ bilden.

Satz 7. *Ist* $\mathfrak{G}$ *endlich vom Grade r in bezug auf* Δ, *so bilden je r unabhängige Elemente* $v_1, \ldots, v_r$ *von* $\mathfrak{G}$ *eine Basis für* $\mathfrak{G}$.

Beweis: Mehr als r unabhängige Elemente gibt es in $\mathfrak{G}$ nicht; also muß jedes weitere Element linear von $v_1, \ldots, v_r$ abhängen.

Spezialfall: Hat $\mathfrak{G}$ den Grad 1, so bildet jedes von Null verschiedene Element eine Basis für $\mathfrak{G}$. Da $\mathfrak{G}$ den Körper Δ umfaßt, bildet z. B. das Einheitselement e von Δ schon eine Basis; jedes Element von $\mathfrak{G}$ hat also die Form $\alpha e = \alpha$, und mithin ist $\mathfrak{G} = \Delta$. Der Schluß ist umkehrbar; mithin:

[1] Der Begriff der Δ-Basis ist zu unterscheiden von dem der Idealbasis (§ 14). Beide sind Spezialfälle des allgemeinen Begriffs einer Modulbasis (Basis eines Moduls in bezug auf einen Operatorenbereich).

[2] D. h. jeder Unterring oder Untermodul oder überhaupt jede Untermenge.

Der Grad eines Δ umfassenden Bereichs $\mathfrak{G}$ ist dann und nur dann 1, *wenn* $\mathfrak{G} = \Delta$ *ist.*

Aufgaben. 1. Ein hyperkomplexes System in bezug auf einen kommutativen Körper, definiert mittels eines Systems von n Symbolen $i_1, \ldots, i_n$ (§ 10, S. 43), hat in bezug auf den Körper den Grad n. Jede Basis $\{v_1, \ldots, v_n\}$ kann an Stelle von $\{s_1, \ldots, s_n\}$ zur Definition des hyperkomplexen Systems benutzt werden.

Wir wenden jetzt den Gradbegriff insbesondere auf Körper an. Den Grad eines endlichen Erweiterungskörpers Σ in bezug auf Δ bezeichnen wir mit (Σ/Δ). Wenn der Grad die Werte 2, 3, 4, ... hat, spricht man von quadratischen, kubischen, biquadratischen, ... Erweiterungskörpern.

Satz 8. *Sind Δ, Σ und Ω Körper und ist Σ endlich in bezug auf Δ und Ω endlich in bezug auf Σ, so ist Ω endlich in bezug auf Δ, und es gilt die Gradrelation:*

$$(\Omega/\Delta) = (\Omega/\Sigma) \cdot (\Sigma/\Delta) . \tag{3}$$

Beweis: Es sei $\{x_1, \ldots, x_n\}$ eine Basis von Σ in bezug auf Δ und $\{y_1, \ldots, y_m\}$ eine Basis von Ω in bezug auf Σ. Dann ist jedes Element von Ω darstellbar in der Gestalt

$$\begin{aligned} \omega &= \sum_i \sigma_i y_i && (\sigma_i \in \Sigma) \\ &= \sum_i \Big(\sum_k \delta_{ik} x_k\Big) y_i && (\delta_{ik} \in \Delta) \\ &= \sum_i \sum_k \delta_{ik} (x_k y_i) . \end{aligned}$$

Jedes Element von Ω hängt also von den nm Größen $x_k y_i$ linear ab. Diese Größen sind untereinander in bezug auf Δ linear-unabhängig; denn aus

$$\sum_i \sum_k d_{ik} x_k y_i = 0 \qquad (d_{ik} \in \Delta)$$

folgt wegen der linearen Unabhängigkeit der y in bezug auf Σ:

$$\sum_k d_{ik} x_k = 0 ,$$

also wegen der Unabhängigkeit der x in bezug auf Δ:

$$d_{ik} = 0 .$$

Also ist nm der Grad von Ω in bezug auf Δ, q. e. d.

Folgerungen aus (3).

a) Ist $\Delta \subseteq \Sigma \subseteq \Omega$ und $(\Omega/\Delta) = (\Sigma/\Delta)$, so ist $\Omega = \Sigma$. Aus (3) folgt dann nämlich $(\Omega/\Sigma) = 1$. — Ebenso:

b) Ist $\Delta \subseteq \Sigma \subseteq \Omega$ und $(\Omega/\Sigma) = (\Omega/\Delta)$, so ist $\Sigma = \Delta$.

Aufgaben. 2. Welchen Grad hat der Körper $\Gamma(i, \sqrt{2})$ in bezug auf den Körper Γ der rationalen Zahlen?

3. Alle Elemente eines endlichen kommutativen Erweiterungskörpers

Ω eines kommutativen Körpers Δ sind algebraisch in bezug auf Δ, und ihre Grade sind Teiler des Körpergrades (Ω/Δ).

4. Aus wie vielen Elementen besteht ein Körper von der Charakteristik p, der in bezug auf den darin enthaltenen Primkörper den Grad n hat?

§ 29. Algebraische Körpererweiterungen.

In diesem Paragraphen sollen die Begriffe und Methoden der beiden vorangehenden miteinander verbunden werden. Wir beschäftigen uns also mit kommutativen Erweiterungskörpern eines kommutativen Körpers Δ.

Ein solcher Erweiterungskörper Σ heißt *algebraisch über* Δ, wenn jedes Element von Σ algebraisch über Δ ist.

Satz. *Jede endliche Erweiterung Σ von Δ ist algebraisch und läßt sich aus Δ durch Adjunktion endlichvieler algebraischer Elemente gewinnen.*

Beweis: Ist n der Grad der endlichen Erweiterung Σ und $\alpha \in \Sigma$, so gibt es unter den Potenzen $1, \alpha, \alpha^2, \ldots, \alpha^n$ eines Elements α höchstens n linear-unabhängige. Es muß also eine Relation $\sum_0^n c_k \alpha^k = 0$ bestehen, d. h. α ist algebraisch; demnach ist der Körper Σ algebraisch. Als Erzeugende der Erweiterung Σ (d. h. als adjungierte Menge) kann man eine Körperbasis von Σ wählen.

Infolge dieses Satzes kann man statt „endliche Erweiterung" auch „endliche algebraische Erweiterung" sagen.

Umkehrung. *Jede Erweiterung eines Körpers Δ, die durch Adjunktion endlichvieler algebraischer Größen zu Δ entsteht, ist endlich (und folglich algebraisch).*

Beweis: Adjunktion einer algebraischen Größe Θ vom Grade n ergibt eine endliche Erweiterung mit der Basis $1, \Theta, \ldots, \Theta^{n-1}$. Sukzessive Bildung endlicher Erweiterungen ergibt nach Satz 8, § 28 stets wieder eine endliche Erweiterung.

Folgerung. *Summe, Differenz, Produkt und Quotient algebraischer Größen sind wieder algebraische Größen.*

Satz. *Ist α algebraisch in bezug auf Σ und Σ algebraisch in bezug auf Δ, so ist α algebraisch in bezug auf Δ.*

Beweis: In der algebraischen Gleichung für α mit Koeffizienten aus Σ können nur endlichviele Elemente $\beta, \gamma, \ldots$ von Σ als Koeffizienten vorkommen. Der Körper $\Sigma' = \Delta(\beta, \gamma, \ldots)$ ist endlich in bezug auf Δ, und der Körper $\Sigma'(\alpha)$ ist wieder endlich in bezug auf Σ'; also ist $\Sigma'(\alpha)$ auch endlich in bezug auf Δ, also α algebraisch in bezug auf Δ.

Zerfällungskörper. Unter den endlichen algebraischen Erweiterungen sind besonders wichtig die *„Zerfällungskörper"* eines Polynoms $f(x)$, die durch *„Adjunktion aller Wurzeln einer Gleichung $f(x) = 0$"*

entstehen. Darunter versteht man solche Körper $\Delta(\alpha_1, \ldots, \alpha_n)$, in denen das Polynom $f(x)$ aus $\Delta[x]$ vollständig in Linearfaktoren zerfällt:

$$f(x) = (x - \alpha_1) \ldots (x - \alpha_n),$$[1]

und die durch Adjunktion der Wurzeln α_i dieser Linearfaktoren zu Δ entstehen. Über diese Körper gelten die folgenden Sätze:

Zu jedem Polynom $f(x)$ aus $\Delta[x]$ gibt es einen Zerfällungskörper.

Beweis: In $\Delta[x]$ möge $f(x)$ folgendermaßen in unzerlegbare Faktoren zerfallen:

$$f(x) = \varphi_1(x)\,\varphi_2(x) \ldots \varphi_r(x).$$

Wir adjungieren nun zunächst eine Nullstelle α_1 des irreduziblen Polynoms $\varphi_1(x)$ und erhalten dadurch einen Körper $\Delta(\alpha_1)$, in dem $\varphi_1(x)$, also auch $f(x)$, einen Linearfaktor $x - \alpha_1$ abspaltet.

Gesetzt nun, man habe schon einen Körper $\Delta_k = \Delta(\alpha_1, \ldots, \alpha_k)$ $(k < n)$ konstruiert, in dem das Polynom $f(x)$ die (gleichen oder verschiedenen) Faktoren $x - \alpha_1, \ldots, x - \alpha_k$ abspaltet. In dem Körper Δ_k möge $f(x)$ folgendermaßen zerfallen:

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_k) \cdot \psi_{k+1}(x) \cdots \psi_l(x).$$

Wir adjungieren nun zu Δ_k eine Nullstelle α_{k+1} von $\psi_{k+1}(x)$. Im so erweiterten Körper $\Delta_k(\alpha_{k+1}) = \Delta(\alpha_1, \ldots, \alpha_{k+1})$ spaltet $f(x)$ die Faktoren $x - \alpha_1, \ldots, x - \alpha_{k+1}$ ab. Vielleicht spaltet sogar $f(x)$ nach der Adjunktion noch mehr als diese $k+1$ Linearfaktoren ab, aber das schadet nichts.

In dieser Art schrittweise weitergehend, findet man schließlich den gesuchten Körper $\Delta_n = \Delta(\alpha_1, \ldots, \alpha_n)$. —

Wir werden nun weiter zeigen, daß der Zerfällungskörper eines gegebenen Polynoms $f(x)$ bis auf äquivalente Erweiterungen eindeutig bestimmt ist. Dazu benötigen wir den Begriff der *Fortsetzung eines Isomorphismus.*

Es sei $\Delta \subseteqq \Sigma$ und $\bar{\Delta} \subseteqq \bar{\Sigma}$, und es sei ein 1-Isomorphismus $\Delta \cong \bar{\Delta}$ gegeben. Ein 1-Isomorphismus $\Sigma \cong \bar{\Sigma}$ heißt nun eine *Fortsetzung* des gegebenen 1-Isomorphismus $\Delta \cong \bar{\Delta}$, wenn jede Größe a von Δ, die beim alten Isomorphismus $\Delta \cong \bar{\Delta}$ das Bild $\bar{a}$ hat, beim neuen Isomorphismus $\Sigma \cong \bar{\Sigma}$ dasselbe Bild $\bar{a}$ aus $\bar{\Delta}$ hat.

Alle Sätze über Fortsetzungen von Isomorphismen bei algebraischen Erweiterungen beruhen auf dem folgenden:

Geht bei einem 1-Isomorphismus $\Delta \cong \bar{\Delta}$ ein irreduzibles Polynom $\varphi(x)$ aus $\Delta[x]$ in das (natürlich ebenfalls irreduzible) Polynom $\bar{\varphi}(x)$ aus $\bar{\Delta}[x]$ über, ist weiter α eine Nullstelle von $\varphi(x)$ in einem Erweiterungskörper von Δ

[1] Den höchsten Koeffizienten von $f(x)$ wollen wir hier und im folgenden gleich 1 annehmen, was offenbar nichts ausmacht.

und $\bar{\alpha}$ eine Nullstelle von $\bar{\varphi}(x)$ in einem Erweiterungskörper von $\bar{\Delta}$, so läßt sich der gegebene 1*-Isomorphismus $\Delta \cong \bar{\Delta}$ zu einem* 1*-Isomorphismus $\Delta(\alpha) \cong \bar{\Delta}(\bar{\alpha})$, der α in $\bar{\alpha}$ überführt, fortsetzen.*

Beweis: Die Elemente von $\Delta(\alpha)$ haben die Gestalt $\sum c_k \alpha^k (c_k \in \Delta)$, und mit ihnen wird gerechnet wie mit Polynomen modulo $\varphi(x)$. Ebenso haben die Elemente von $\bar{\Delta}(\bar{\alpha})$ die Gestalt $\sum \bar{c}_k \bar{\alpha}^k (\bar{c}_k \in \bar{\Delta})$, und mit ihnen wird gerechnet wie mit Polynomen modulo $\bar{\varphi}(x)$, also genau so, nur mit Querstrichen. Also ist die Zuordnung

$$\sum c_k \alpha^k \rightarrow \sum \bar{c}_k \bar{\alpha}^k$$

(wobei die $\bar{c}_k$ die entsprechenden Elemente zu den c_k im Isomorphismus $\Delta \cong \bar{\Delta}$ sind) ein Isomorphismus, der die verlangten Eigenschaften besitzt.

Ist speziell $\Delta = \bar{\Delta}$ und bildet der gegebene Isomorphismus jedes Element von Δ auf sich ab, so erhält man den früheren Satz zurück, daß alle Erweiterungen $\Delta(\alpha), \Delta(\bar{\alpha}), \ldots$, die durch Adjunktion je einer Wurzel derselben irreduziblen Gleichung entstehen, äquivalent sind und daß jede Wurzel durch die betreffenden 1-Isomorphismen in jede andere übergeführt werden kann.

Ein entsprechender Satz gilt nun bei Adjunktion aller Wurzeln eines Polynoms statt einer einzigen:

Geht bei einem 1*-Isomorphismus $\Delta \cong \bar{\Delta}$ ein beliebiges Polynom $f(x)$ aus $\Delta[x]$ in ein Polynom $\bar{f}(x)$ aus $\bar{\Delta}[x]$ über, so läßt sich der* 1*-Isomorphismus zu einem* 1*-Isomorphismus eines beliebigen Zerfällungskörpers $\Delta(\alpha_1, \ldots, \alpha_n)$ von $f(x)$ mit einem beliebigen Zerfällungskörper $\bar{\Delta}(\bar{\alpha}_1, \ldots, \bar{\alpha}_n)$ von $\bar{f}(x)$ fortsetzen, wobei $\alpha_1, \ldots, \alpha_n$ in einer gewissen Reihenfolge in $\bar{\alpha}_1, \ldots, \bar{\alpha}_n$ übergehen.*

Beweis: Gesetzt, man habe (eventuell nach Abänderung der Reihenfolge der Wurzeln) den 1-Isomorphismus $\Delta \cong \bar{\Delta}$ schon fortgesetzt zu einem 1-Isomorphismus $\Delta(\alpha_1, \ldots, \alpha_k) \cong \bar{\Delta}(\bar{\alpha}_1, \ldots, \bar{\alpha}_k)$, wobei jedes α_i in $\bar{\alpha}_i$ übergeht. (Für $k = 0$ ist das tatsächlich der Fall.) In $\Delta(\alpha_1, \ldots, \alpha_k)$ möge $f(x)$ so zerfallen:

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_k) \cdot \varphi_{k+1}(x) \cdots \varphi_h(x).$$

Entsprechend zerfällt dann, vermöge des 1-Isomorphismus, $\bar{f}(x)$ in $\bar{\Delta}(\bar{\alpha}_1, \ldots, \bar{\alpha}_k)$ folgendermaßen:

$$\bar{f}(x) = (x - \bar{\alpha}_1) \cdots (x - \bar{\alpha}_k) \cdot \bar{\varphi}_{k+1}(x) \cdots \bar{\varphi}_h(x).$$

In $\Delta(\alpha_1, \ldots, \alpha_n)$ bzw. $\bar{\Delta}(\bar{\alpha}_1, \ldots, \bar{\alpha}_n)$ zerlegen sich die Faktoren φ_ν und $\bar{\varphi}_\nu$ weiter in $(x - \alpha_{k+1}) \cdots (x - \alpha_n)$ bzw. $(x - \bar{\alpha}_{k+1}) \cdots (x - \bar{\alpha}_n)$. Die $\alpha_{k+1}, \ldots, \alpha_n$ und $\bar{\alpha}_{k+1}, \ldots, \bar{\alpha}_n$ mögen so umgeordnet werden, daß α_{k+1} Wurzel von $\varphi_{k+1}(x)$ und $\bar{\alpha}_{k+1}$ Wurzel von $\bar{\varphi}_{k+1}(x)$ wird. Nach dem

vorigen Satz läßt sich dann der 1-Isomorphismus

$$\Delta(\alpha_1, \ldots, \alpha_k) \cong \overline{\Delta}(\bar{\alpha}_1, \ldots, \bar{\alpha}_k)$$

zu einem ebensolchen

$$\Delta(\alpha_1, \ldots, \alpha_{k+1}) \cong \overline{\Delta}(\bar{\alpha}_1, \ldots, \bar{\alpha}_{k+1})$$

fortsetzen, wobei α_{k+1} in $\bar{\alpha}_{k+1}$ übergeht.

In dieser Weise Schritt für Schritt von $k = 0$ aus weitergehend, kommt man schließlich zum gesuchten 1-Isomorphismus

$$\Delta(\alpha_1, \ldots, \alpha_n) \cong \overline{\Delta}(\bar{\alpha}_1, \ldots, \bar{\alpha}_n),$$

wobei laut Konstruktion jedes α_i in $\bar{\alpha}_i$ übergeht. —

Ist jetzt insbesondere $\Delta = \overline{\Delta}$ und läßt der gegebene 1-Isomorphismus $\Delta \cong \Delta$ jedes Element von Δ fest, so wird $\bar{f} = f$, und der erweiterte 1-Isomorphismus

$$\Delta(\alpha_1, \ldots, \alpha_n) \cong \Delta(\bar{\alpha}_1', \ldots, \bar{\alpha}_n)$$

läßt ebenfalls alle Elemente von Δ fest, d. h. die beiden Zerfällungskörper von $f(x)$ sind *äquivalent. Mithin ist der Zerfällungskörper eines Polynoms $f(x)$ bis auf äquivalente Erweiterungen eindeutig bestimmt.*

Daraus folgt, daß alle algebraischen Eigenschaften der Wurzeln unabhängig von der Art der Konstruktion des Zerfällungskörpers sind. Zum Beispiel: Ob man ein Polynom zerfällt im Körper der komplexen Zahlen oder mittels symbolischer Adjunktion, man wird „im wesentlichen", d. h. bis auf Äquivalenz, stets dasselbe finden.

Insbesondere hat jede Wurzel oder Nullstelle von $f(x)$ eine bestimmte *Vielfachheit*, in der sie bei der Zerlegung

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$$

vorkommt.

Vielfache Wurzeln sind dann und nur dann vorhanden, wenn $f(x)$ und $f'(x)$ über dem Zerfällungskörper einen gemeinsamen Teiler haben, der keine Konstante ist (§ 19). Der größte gemeinsame Teiler von $f(x)$ und $f'(x)$ über irgend einem Erweiterungskörper ist aber derselbe wie der größte gemeinsame Teiler im Grundbereich $\Delta[x]$ (§ 16, Aufg. 1). Demnach kann man durch Bildung des größten gemeinsamen Teilers von $f(x)$ und $f'(x)$ in $\Delta[x]$ schon erkennen, ob $f(x)$ in seinem Zerfällungskörper vielfache Nullstellen besitzt.

Zwei Zerfällungskörper eines und desselben Polynoms, die in einem gemeinsamen Umfassungskörper Ω enthalten sind, sind nicht nur äquivalent, sondern sogar *gleich*. Denn wenn in Ω zwei Zerlegungen

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_n),$$
$$f(x) = (x - \bar{\alpha}_1) \cdots (x - \bar{\alpha}_n)$$

stattfinden, so stimmen nach dem Satz von der eindeutigen Faktorzerlegung in $\Omega[x]$ die Faktoren bis auf die Reihenfolge überein.

Galoissche Erweiterungskörper. Ein Körper Σ heißt *Galoissch* oder *normal* über Δ, wenn er erstens algebraisch in bezug auf Δ ist und zweitens jedes in $\Delta[x]$ irreduzible Polynom $g(x)$, das in Σ *eine* Nullstelle α hat, in $\Sigma[x]$ ganz in Linearfaktoren zerfällt[1].

Unsere früher konstruierten Zerfällungskörper sind Galoissch nach folgendem Satz:

Ein Körper, der aus Δ durch Adjunktion aller Nullstellen eines oder mehrerer oder sogar unendlichvieler Polynome aus $\Delta[x]$ entsteht, ist Galoissch.

Zunächst können wir den Fall unendlichvieler Polynome auf den endlichvieler zurückführen; denn jedes Element α des Körpers hängt doch nur von den Wurzeln endlichvieler unserer Polynome ab, und wir können uns für die Zerfällung des irreduziblen Polynoms, welches α zur Nullstelle hat, ganz auf den von diesen endlichvielen Wurzeln erzeugten Körper beschränken.

Sodann können wir den Fall endlichvieler Polynome auf den eines einzigen zurückführen, indem wir sie alle miteinander multiplizieren und die Nullstellen des Produkts adjungieren; das sind ja dieselben Größen wie die Nullstellen aller Faktoren zusammengenommen.

Es sei also $\Sigma = \Delta(\alpha_1, \ldots, \alpha_n)$, wo die α_ν die Wurzeln eines Polynoms $f(x)$ sind, und das irreduzible Polynom $g(x)$ aus $\Delta[x]$ habe eine Nullstelle β in Σ. Wenn $g(x)$ in Σ nicht ganz zerfällt, können wir Σ durch Adjunktion einer weiteren Nullstelle β' von $g(x)$ zu einem Körper $\Sigma(\beta')$ erweitern; dann ist, da β und β' konjugiert sind,

$$\Delta(\beta) \cong \Delta(\beta').$$

Bei dieser Isomorphie gehen die Größen von Δ und somit auch die Koeffizienten des Polynoms $f(x)$ in sich über. Adjungieren wir nun links und rechts alle Nullstellen von $f(x)$, so läßt sich die Isomorphie fortsetzen:

$$\Delta(\beta, \alpha_1, \ldots, \alpha_n) \cong \Delta(\beta', \alpha_1, \ldots, \alpha_n),$$

wobei die α_i wieder in die α_j, vielleicht in anderer Reihenfolge, übergehen. Nun ist β eine rationale Funktion von $\alpha_1, \ldots, \alpha_n$ mit Koeffizienten aus Δ:

$$\beta = r(\alpha_1, \ldots, \alpha_n),$$

---

[1] Man kann die Definition auch so fassen: *Eine algebraische Erweiterung Σ ist Galoissch, wenn Σ zugleich mit einer Größe α auch alle zu α konjugierten Größen (irgend eines umfassenden Körpers) enthält.* Die zu α konjugierten Größen eines beliebigen umfassenden Körpers sind nämlich nichts anderes als die Wurzeln desselben irreduziblen Polynoms $g(x)$, dessen Nullstelle α ist, und der Umfassungskörper kann immer so gewählt werden, daß in ihm $g(x)$ ganz zerfällt. Diese Definition ist aber hier vermieden worden, da sie auf die Gesamtheit aller umfassenden Körper Bezug nimmt, was (abgesehen von der mengentheoretischen Bedenklichkeit dieser Gesamtheit, die sich wohl beseitigen ließe) weniger schön erscheint, da es sich in Wirklichkeit um eine Eigenschaft von Σ und Δ allein handelt.

und diese rationale Beziehung bleibt bei jedem Isomorphismus erhalten. Mithin ist auch β' eine rationale Funktion von $\alpha_1, \ldots, \alpha_n$, gehört also ebenfalls dem Körper Σ an, entgegen unserer Annahme.

Umkehrung. *Ein Galoisscher Körper Σ über Δ entsteht durch Adjunktion aller Nullstellen einer Menge von Polynomen und, wenn er endlich ist, sogar durch Adjunktion aller Nullstellen eines einzigen Polynoms.*

Beweis: Der Körper Σ entstehe durch Adjunktion einer Menge $\mathfrak{M}$ von algebraischen Größen. (Im allgemeinen Fall kann man etwa $\mathfrak{M} = \Sigma$ wählen; im endlichen Fall ist $\mathfrak{M}$ endlich.) Jedes Element von $\mathfrak{M}$ genügt einer algebraischen Gleichung $f(x) = 0$ mit Koeffizienten aus Δ, die in Σ ganz zerfällt. Die Adjunktion aller Nullstellen aller dieser Polynome $f(x)$ (bzw., wenn es nur endlichviele sind, aller Nullstellen ihres Produktes) ergibt mindestens so viel wie die Adjunktion von $\mathfrak{M}$ allein, d. h. sie ergibt den ganzen Körper Σ, q. e. d.

Eine irreduzible Gleichung $f(x) = 0$ heißt *Galoissch*, wenn der durch Adjunktion *einer* Wurzel entstehende Körper schon Galoissch ist, d. h. wenn in ihm $f(x)$ völlig zerfällt.

Die Termini „Galoissche Körper" und „Galoissche Gleichungen" erklären sich folgendermaßen: In der früheren Theorie spielten die Hauptrolle die „Galoisschen Resolventen" einer Gleichung. Eine *Galoissche Resolvente* einer Gleichung $f(x) = 0$ ist eine irreduzible Gleichung $g(x) = 0$ mit der Eigenschaft, daß die Adjunktion einer Wurzel dieser Gleichung schon den vollständigen Zerfällungskörper des Polynoms $f(x)$ ergibt. (Die Existenz solcher Resolventen werden wir später beweisen.) Der durch eine Galoissche Resolvente definierte Körper wurde nun als Galoisscher Körper bezeichnet und eine Gleichung, die ihre eigene Galoissche Resolvente darstellt, als Galoissche oder normale Gleichung.

Aufgaben. 1. Ist $\Delta \leqq \Sigma \leqq \Omega$ und Ω Galoissch über Δ, so ist Ω Galoissch über Σ.

2. Man konstruiere den Wurzelkörper von $x^3 - 2$ in bezug auf den rationalen Grundkörper Γ. Man zeige: Ist α eine Wurzel, so ist $\Gamma(\alpha)$ nicht Galoissch.

3. Ist $f(x)$ im Körper K irreduzibel, so zerfällt $f(x)$ in einem Galoisschen Erweiterungskörper in lauter Faktoren gleichen Grades, die in bezug auf K konjugiert sind.

4. Jeder in bezug auf Δ quadratische Körper ist Galoissch in bezug auf Δ.

§ 30. Einheitswurzeln.

Wir haben im vorangehenden die allgemeinen Grundlagen der Körpertheorie dargestellt. Bevor wir die allgemeine Theorie weiter entwickeln, wenden wir die erhaltenen Sätze auf einige ganz spezielle Gleichungen und spezielle Körper an.

Es sei Π ein Primkörper und h eine natürliche Zahl, die nicht kongruent Null ist nach der Charakteristik von Π. (Ist die Charakteristik Null, so darf h demnach eine beliebige natürliche Zahl sein.) Unter einer *h-ten Einheitswurzel* verstehen wir eine Nullstelle des Polynoms

$$f(x) = x^h - 1$$

in irgend einem kommutativen Erweiterungskörper.

Die h-ten Einheitswurzeln in einem Körper bilden bei der Multiplikation eine Abelsche Gruppe.

Denn wenn $\alpha^h = 1$ und $\beta^h = 1$, so ist auch $\left(\frac{\alpha}{\beta}\right)^h = 1$, woraus die Gruppeneigenschaft folgt. Daß die Gruppe Abelsch ist, ist klar.

Die Ordnung eines Gruppenelements α ist Teiler von h, da $\alpha^h = 1$ sein muß.

Der Zerfällungskörper Σ von $f(x)$ heißt der *Körper der h-ten Einheitswurzeln über dem Primkörper* Π. Das Polynom $f(x)$ zerfällt in lauter *verschiedene* Linearfaktoren; denn die Ableitung

$$f'(x) = hx^{h-1}$$

verschwindet, da h nicht durch die Charakteristik teilbar ist, nur für $x = 0$, hat also keine Nullstelle mit $f(x)$ gemein. *Es gibt also in* Σ *genau* h *h-te Einheitswurzeln.*

Wir zerlegen nun h in Primfaktoren:

$$h = \prod_{i=1}^{m} q_i^{\nu_i}.$$

In der Gruppe der h-ten Einheitswurzeln gibt es höchstens $\frac{h}{q_i}$ Elemente a, für die $a^{\frac{h}{q_i}} = 1$ ist; denn das Polynom $x^{\frac{h}{q_i}} - 1$ hat höchstens $\frac{h}{q_i}$ Nullstellen. Also gibt es in der Gruppe ein a_i mit

$$a_i^{h:q_i} \neq 1.$$

Das Gruppenelement

$$b_i = a_i^{h:q_i^{\nu_i}}$$

hat die Ordnung $q_i^{\nu_i}$. Denn seine $q_i^{\nu_i}$-te Potenz ist 1, seine Ordnung also ein Teiler von $q_i^{\nu_i}$; aber seine $q_i^{\nu_i - 1}$-te Potenz ist von 1 verschieden, seine Ordnung also kein echter Teiler von $q_i^{\nu_i}$. Das Produkt

$$\zeta = \prod_{1}^{m} b_i$$

hat nun, als Produkt von Elementen der teilerfremden Ordnungen $q_1^{\nu_1}, \ldots, q_m^{\nu_m}$, genau die Ordnung

$$\prod_{1}^{m} q_i^{\nu_i} = h$$

(§ 7, Aufg. 1). Eine solche Einheitswurzel, deren Ordnung genau h ist, nennen wir eine *primitive h-te Einheitswurzel.*

Die Potenzen $1, \zeta, \zeta^2, \ldots, \zeta^{h-1}$ einer primitiven Einheitswurzel sind alle verschieden; da aber die Gruppe im ganzen nur h Elemente hat, so sind alle ihre Elemente Potenzen von ζ. Mithin:

Die Gruppe der h-ten Einheitswurzeln ist zyklisch und wird von jeder primitiven Einheitswurzel ζ erzeugt.

Die Anzahl der primitiven h-ten Einheitswurzeln ist nun leicht zu bestimmen. Wir geben sie zunächst mit $\varphi(h)$ an. *$\varphi(h)$ ist die Anzahl der Elemente der Ordnung h in einer zyklischen Gruppe der Ordnung h.*[1] Ist zunächst h eine Primzahlpotenz, $h = q^\nu$, so sind alle q^ν Potenzen von ζ, mit Ausnahme der $q^{\nu-1}$ Potenzen von ζ^q, Elemente h-ter Ordnung; mithin ist

$$\varphi(q^\nu) = q^\nu - q^{\nu-1} = q^{\nu-1}(q-1) = q^\nu\left(1 - \frac{1}{q}\right). \tag{1}$$

Ist zweitens h in zwei teilerfremde Faktoren zerlegt: $h = rs$, so ist jedes Element h-ter Ordnung eindeutig als Produkt eines Elements r-ter Ordnung und eines Elements s-ter Ordnung darstellbar (§ 16, Aufg. 3) und umgekehrt jedes solche Produkt ein Element h-ter Ordnung. Die Elemente r-ter Ordnung gehören der von ζ^s erzeugten zyklischen Gruppe r-ter Ordnung an; ihre Anzahl ist demnach $\varphi(r)$. Ebenso ist die Anzahl der Elemente s-ter Ordnung $\varphi(s)$; für die Anzahl der Produkte hat man demnach

$$\varphi(h) = \varphi(r)\,\varphi(s).$$

Aus dieser Formel folgt durch wiederholte Anwendung, wenn wie bisher

$$h = \prod_1^m q_i^{\nu_i}$$

die Zerlegung von h in teilerfremde Primzahlpotenzen ist:

$$\varphi(h) = \varphi(q_1^{\nu_1} q_2^{\nu_2} \ldots q_m^{\nu_m}) = \varphi(q_1^{\nu_1})\,\varphi(q_2^{\nu_2}) \ldots \varphi(q_m^{\nu_m}),$$

also nach (1):

$$\begin{aligned}\varphi(h) &= q_1^{\nu_1-1}(q_1-1)\,q_2^{\nu_2-1}(q_2-1) \ldots q_m^{\nu_m-1}(q_m-1)\\ &= h\left(1-\frac{1}{q_1}\right)\left(1-\frac{1}{q_2}\right)\cdots\left(1-\frac{1}{q_m}\right).\end{aligned}$$

Mithin:

Die Anzahl der primitiven h-ten Einheitswurzeln ist

$$\varphi(h) = h\prod_1^m\left(1-\frac{1}{q_i}\right).$$

---

[1] Nach § 16, Aufg. 4 ist $\varphi(h)$ zugleich die Anzahl der zu h teilerfremden natürlichen Zahlen $\leqq h$. Man nennt $\varphi(h)$ die *Eulersche φ-Funktion.*

Wir setzen $n = \varphi(h)$. Die primitiven h-ten Einheitswurzeln seien $\zeta_1, \ldots, \zeta_n$. Sie sind die Nullstellen des Polynoms

$$(x - \zeta_1)(x - \zeta_2) \ldots (x - \zeta_n) = \Phi_h(x).$$

Es ist

$$x^h - 1 = \prod_{d|h} \Phi_d(x), \tag{2}$$

wo d die positiven Teiler von h durchläuft[1]; denn jede h-te Einheitswurzel ist primitive d-te Einheitswurzel für einen und nur einen positiven Teiler d von h, und daher kommt jeder Linearfaktor von $x^h - 1$ in einem und nur einem der Polynome $\Phi_d(x)$ vor.

Die Formel (2) bestimmt $\Phi_h(x)$ eindeutig. Denn aus ihr folgt zunächst

$$\Phi_1(x) = x - 1,$$

und wenn Φ_d für alle positiven $d < h$ bekannt ist, so bestimmt sich Φ_h durch Division aus (2).

Da diese Divisionen sich nach dem Algorithmus im ganzzahligen Polynombereich der Variablen x ausführen lassen, so folgt:

Jedes $\Phi_h(x)$ ist ein ganzzahliges Polynom und unabhängig von der Charakteristik des Körpers Π (solange nur h nicht durch sie teilbar ist).

Die Polynome $\Phi_h(x)$ heißen, aus einem später zu erwähnenden Grunde, *Kreisteilungspolynome.* Man kann für sie explizite rationale Formeln angeben mit Hilfe der *„Möbiusschen Funktion"* $\mu(n)$, die folgendermaßen definiert wird:

$$\mu(n) = \begin{cases} 0, \text{ wenn } p_i^2 | n \text{ für ein } p_i, \\ (-1)^\lambda, \text{ wenn } n = p_1 p_2 \ldots p_\lambda \text{ (also } n \text{ „quadratfrei"}), \\ 1, \text{ wenn } n = 1 \text{ ist} \end{cases}$$

($p_1, \ldots, p_\lambda$ sind die verschiedenen Primfaktoren der Zahl n). Die Möbiussche Funktion hat die wichtige Eigenschaft:

$$\sum_{d|h} \mu(d) = \begin{cases} 1 \text{ für } h = 1, \\ 0 \text{ für } h > 1, \end{cases}$$

die man etwa beweist, indem man $h = q_1^{\nu_1} \ldots q_m^{\nu_m}$ setzt, das Produkt $\prod_1^m (1 - z_i)$ entwickelt und dann alle z_i gleich 1 setzt. Die Glieder

$$(-1)^\lambda z_{i_1} z_{i_2} \ldots z_{i_\lambda}$$

dieses Produktes entsprechen nämlich genau den quadratfreien Teilern $d = q_{i_1} q_{i_2} \ldots q_{i_\lambda}$ von h, und es ist

$$(-1)^\lambda = \mu(d).$$

---

[1] $a|b$ (sprich: a teilt b) bedeutet: a ist Teiler von b.

Setzt man also alle $z_i = 1$, so kommt für $m > 0$ (d. h. $h > 1$):

$$0 = \prod_1^m (1 - 1) = \sum_{d|h} \mu(d),$$

während für $h = 1$ offenbar $\sum_{d|h} \mu(d) = 1$ ist.

Nunmehr behaupten wir:

Die Kreisteilungspolynome werden gegeben durch

$$\Phi_h(x) = \prod_{d|h} (x^d - 1)^{\mu\left(\frac{h}{d}\right)}. \tag{3}$$

Zum Beweis genügt es, zu zeigen, daß die Funktionen rechter Hand die Gleichung (2) befriedigen, also daß:

$$x^h - 1 = \prod_{d|h} \prod_{d'|d} (x^{d'} - 1)^{\mu\left(\frac{d}{d'}\right)}$$

ist. Die Exponenten eines festen $x^{d'} - 1$ sind die Zahlen $\mu\left(\frac{d}{d'}\right)$, wo d Teiler von h und Vielfaches von d' ist, d. h. es sind alle $\mu(\lambda)$, wo λ Teiler von $\frac{h}{d'}$ ist. Die Summe dieser Exponenten ist im allgemeinen gleich Null; nur im Falle $\frac{h}{d'} = 1$ hat sie den Wert 1. Demnach bleibt rechts aus dem ganzen Doppelprodukt nur der eine Faktor $x^h - 1$ stehen, und zwar mit dem Exponenten 1. Die Gleichung (2) wird also durch die Funktionen (3) befriedigt.

Beispiele:

$$\begin{aligned} \Phi_{12}(x) &= (x^{12} - 1)^{+1} (x^6 - 1)^{-1} (x^4 - 1)^{-1} (x^2 - 1)^{+1} \\ &= (x^6 + 1)^{+1} (x^2 + 1)^{-1} = x^4 - x^2 + 1; \\ \Phi_{q^\nu}(x) &= (x^{q^\nu} - 1)\,(x^{q^{\nu-1}} - 1)^{-1} \\ &= 1 + x^{q^{\nu-1}} + x^{2q^{\nu-1}} + \cdots + x^{(q-1)q^{\nu-1}} \end{aligned}$$

für jede Primzahl q.

Das Polynom $\Phi_h(x)$ kann sehr wohl reduzibel sein; so ist z. B. für die Charakteristik 11

$$\Phi_{12}(x) = x^4 - x^2 + 1 = (x^2 - 5x + 1)\,(x^2 + 5x + 1).$$

Wir werden aber später (§ 48) sehen, daß im Primkörper der Charakteristik Null das Polynom $\Phi_h(x)$ irreduzibel, mithin alle primitiven h-ten Einheitswurzeln konjugiert sind. In § 22 haben wir auf Grund des Eisensteinschen Satzes schon erkannt, daß dies für alle Primzahlen h der Fall ist; für $\Phi_8 = x^4 + 1$ und $\Phi_{12} = x^4 - x^2 + 1$ war es der Inhalt von Aufg. 3, § 22 und Aufg. 5, § 21.

Ein oft benutzter Satz ist der folgende:

Ist ζ eine h-te Einheitswurzel, so ist

$$1 + \zeta + \zeta^2 + \cdots + \zeta^{h-1} = \begin{cases} h\ (\zeta = 1) \\ 0\ (\zeta \neq 1) \end{cases}.$$

Der Beweis ergibt sich unmittelbar aus der Summenformel der geometrischen Reihe: Für $\zeta \neq 1$ erhält man

$$\frac{1-\zeta^h}{1-\zeta} = 0.$$

Aufgaben. 1. Der Körper der h-ten Einheitswurzeln ist für ungerades h zugleich Körper der $2h$-ten Einheitswurzeln.

2. Die Körper der dritten und vierten Einheitswurzeln über dem Körper der rationalen Zahlen sind quadratisch. Man drücke diese Einheitswurzeln durch Quadratwurzeln aus.

3. Der Körper der achten Einheitswurzeln ist quadratisch in bezug auf den Gaußschen Zahlkörper $\Gamma(i)$. Man drücke eine primitive achte Einheitswurzel mit Hilfe einer Quadratwurzel aus einem Element von $\Gamma(i)$ aus.

4. Im Falle der Charakteristik p sind die $(p^\lambda h)$-ten Einheitswurzeln zugleich h-te Einheitswurzeln. (Das rechtfertigt die zu Anfang gemachte Beschränkung $h \not\equiv 0 (p)$.)

5. Die „*Kreisteilungsgleichung*" $\Phi_h(x) = 0$ ist stets Galoissch.

§ 31. Galois-Felder (endliche kommutative Körper).

Wir haben in den Primkörpern der Charakteristik p schon kommutative Körper mit endlichvielen Elementen kennengelernt. Die endlichen kommutativen Körper heißen nach ihrem Entdecker GALOIS auch *Galois-Felder*. Wir untersuchen zunächst ihre allgemeinen Eigenschaften.

Es sei Δ ein Galois-Feld und q die Anzahl seiner Elemente.

Die Charakteristik von Δ kann nicht Null sein; denn sonst würde der in Δ liegende Primkörper Π schon unendlich viele Elemente haben. Es sei p die Charakteristik. Der Primkörper Π ist dann 1-isomorph dem Restklassenring modulo p und hat p Elemente.

Da es in Δ überhaupt nur endlichviele Elemente gibt, so gibt es auch in Δ ein größtes System von linear-unabhängigen Elementen $\alpha_1, \ldots, \alpha_n$ in bezug auf Π. n ist der Körpergrad (Δ/Π), und jedes Element von Δ hat die Gestalt

$$c_1\alpha_1 + \cdots + c_n\alpha_n \tag{1}$$

mit eindeutig bestimmten Koeffizienten c_i aus Π.

Für jeden Koeffizienten c_i sind p Werte möglich; es gibt also genau p^n Ausdrücke von der Gestalt (1). Da diese die sämtlichen Körperelemente darstellen, so folgt

$$q = p^n.$$

Damit ist bewiesen: *Die Anzahl der Elemente eines Galois-Feldes ist eine Potenz der Charakteristik p; der Exponent gibt den Körpergrad (Δ/Π) an.*

Jeder Körper ist nach Weglassung des Nullelements eine multiplikative Gruppe. Im Fall des Galois-Feldes ist die Gruppe Abelsch

und ihre Ordnung $q-1$. Die Ordnung eines beliebigen Elements α muß ein Teiler von $q-1$ sein; daraus folgt:

$$\alpha^{q-1}=1, \qquad \text{für jedes } \alpha \neq 0.$$

Die hieraus folgende Gleichung

$$\alpha^q-\alpha=0$$

gilt auch für $\alpha=0$. Alle Körperelemente sind also Nullstellen der Funktion x^q-x. Sind $\alpha_1, \ldots, \alpha_q$ die Körperelemente, so muß x^q-x teilbar sein durch

$$\prod_1^q (x-\alpha_i).$$

Wegen der Gradzahlen ist also

$$x^q-x=\prod_1^q (x-\alpha_i).$$

Δ entsteht demnach aus Π durch Adjunktion aller Nullstellen einer einzigen Funktion x^q-x. Durch diese Angabe ist aber Δ bis auf 1-Isomorphie eindeutig bestimmt (§ 29); also:

Bei gegebenem p und n sind alle kommutativen Körper mit p^n Elementen 1-isomorph.

Wir wollen nun zeigen, daß es zu jedem $n>0$ und jedem p auch wirklich einen Körper mit $q=p^n$ Elementen gibt.

Man gehe vom Primkörper Π der Charakteristik p aus und bilde über Π einen Körper, in dem x^q-x vollständig in Linearfaktoren zerfällt. In diesem Körper betrachte man die Menge der Nullstellen von x^q-x. Diese Menge ist ein Körper; denn aus $x^{p^n}=x$ und $y^{p^n}=y$ folgt nach § 25, Aufg. 1:

$$(x-y)^{p^n}=x^{p^n}-y^{p^n},$$

und im Falle $y\neq 0$:

$$\left(\frac{x}{y}\right)^{p^n}=\frac{x^{p^n}}{y^{p^n}},$$

wonach Differenz und Quotient zweier Nullstellen wieder Nullstellen sind.

Das Polynom x^q-x hat lauter einfache Nullstellen; denn seine Ableitung ist wegen $q\equiv 0\,(p)$

$$q\,x^{q-1}-1=-1,$$

und -1 wird nie Null. Die Menge seiner Nullstellen ist also ein Körper mit q Elementen.

Damit ist bewiesen:

Zu jeder Primzahlpotenz $q=p^n\,(n>0)$ gibt es ein und bis auf Isomorphie nur ein Galois-Feld mit genau q Elementen. Die Elemente sind die Nullstellen von x^q-x.

Das Galois-Feld mit genau p^n Elementen sei im folgenden mit $GF(p^n)$ bezeichnet.

Wir setzen $q - 1 = h$ und bemerken, daß alle von Null verschiedenen Elemente des Galois-Feldes Nullstellen von $x^h - 1$, also h-te Einheitswurzeln sind. Da h zu p teilerfremd ist, so gilt für diese Einheitswurzeln alles im vorigen Paragraphen Gesagte:

Alle von Null verschiedenen Körperelemente sind Potenzen einer einzigen primitiven h-ten Einheitswurzel. Oder: *Die multiplikative Gruppe des Galois-Feldes ist zyklisch.*

Durch diese Theoreme ist die Struktur der endlichen kommutativen Körper vollständig aufgedeckt.

Es ist ein leichtes, sämtliche Unterkörper von $GF(p^n)$ zu bestimmen. Jeder Unterkörper hat einen Grad m, der Teiler von n ist, und besteht somit aus p^m Elementen, die dadurch gekennzeichnet sind, daß sie Nullstellen von $x^{p^m} - x$ sein müssen. Zu jedem positiven Teiler m von n gibt es aber auch wirklich einen solchen Unterkörper; denn wenn m Teiler von n ist, so ist $p^m - 1$ Teiler von $p^n - 1 = (p^m - 1)(p^{n-m} + p^{n-2m} + \cdots + p^m + 1)$, mithin $x^{p^m-1} - 1$ Teiler von $x^{p^n-1} - 1$, also $x^{p^m} - x$ Teiler von $x^{p^n} - x$. Da das letztere Polynom in $GF(p^n)$ vollständig zerfällt, muß das erstere es auch tun, und seine Nullstellen bilden einen $GF(p^m)$. Damit ist bewiesen: *Zu jedem Teiler $m > 0$ von n gibt es einen und nur einen Unterkörper m-ten Grades $GF(p^m)$ in $GF(p^n)$. Ein Element $\alpha \neq 0$ gehört dem Unterkörper an, wenn es der Gleichung $\alpha^{p^m-1} = 1$ genügt, also wenn seine Ordnung (in der multiplikativen Gruppe) Teiler von $p^m - 1$ ist.*

Im nächsten Paragraphen werden wir den folgenden Satz brauchen:

Ein Galois-Feld der Charakteristik p enthält zu jedem Element a genau eine p-te Wurzel $a^{\frac{1}{p}}$.

Beweis: Zu jedem Element x existiert im Körper eine p-te Potenz x^p. Verschiedene Elemente haben verschiedene p-te Potenzen wegen

$$x^p - y^p = (x - y)^p.$$

Also gibt es im Körper genau so viele p-te Potenzen wie Elemente. Alle Elemente sind also p-te Potenzen.

Wir wollen schließlich noch die 1-Automorphismen des Körpers $\Sigma = GF(p^m)$ bestimmen.

Zunächst ist $\alpha \to \alpha^p$ ein Automorphismus. Denn einerseits ist die Zuordnung nach dem vorigen Satz umkehrbar eindeutig, und andrerseits ist

$$(\alpha + \beta)^p = \alpha^p + \beta^p,$$
$$(\alpha\beta)^p = \alpha^p \beta^p.$$

Die Potenzen dieses Automorphismus führen α über in $\alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^m} = \alpha$. Damit haben wir m Automorphismen gefunden.

Daß es nicht mehr als m 1-Automorphismen geben kann, werden wir im § 32 sehen. Die oben bestimmten m 1-Automorphismen $\alpha \to \alpha^{p^\nu}$ sind also die *einzigen*.

Die für $GF(p^n)$ gültigen Sätze ergeben, für $n = 1$ spezialisiert und auf den Restklassenring $C/(p)$ angewandt, bekannte Sätze der elementaren Zahlentheorie, nämlich:

1. Eine Kongruenz nach p hat höchstens so viel Wurzeln mod p, als ihr Grad beträgt.

2. Der Fermatsche Satz

$$a^{p-1} \equiv 1 \,(p) \quad \text{für} \quad a \not\equiv 0 \,(p)$$

ist ein Spezialfall des für $GF(p^n)$ gültigen Satzes:

$$a^{p^n-1} = 1 \quad \text{für} \quad a \neq 0 .$$

3. Es gibt eine „Primitivzahl ζ modulo p", so daß jede zu p teilerfremde Zahl b einer Potenz von ζ mod p kongruent ist. (Oder: Die Gruppe der Restklassen mod p mit Ausschluß der Nullklasse ist zyklisch.)

4. Das Produkt aller von Null verschiedenen Elemente $a_1, a_2, \ldots, a_h$ eines $GF(p^n)$ ist -1 wegen

$$x^h - 1 = \prod_1^h (x - a_\nu) .$$

Für $n = 1$ ergibt das den „Wilsonschen Satz":

$$(p-1)! \equiv -1 \,(p) .$$

Aufgaben. 1. Ist α in $GF(p^n)$ eine Nullstelle des in $\Pi[x]$ irreduziblen Polynoms $f(x)$ vom Grad m, so sind die sämtlichen Nullstellen (die zu α konjugierten Größen) gegeben durch

$$\alpha^p, \alpha^{p^2}, \ldots, \alpha^{p^m} = \alpha .$$

2. Ist r teilerfremd zu $p^n - 1$, so ist jedes Element von $GF(p^n)$ eine r-te Potenz. Ist r Teiler von $p^n - 1$, so sind die und nur die Elemente α von $GF(p^n)$ r-te Potenzen, die der Gleichung

$$\alpha^{\frac{p^n-1}{r}} = 1$$

genügen. Zahlentheoretische Spezialisierung („r-te Potenzreste")! Wie lautet die Regel für beliebiges $r = s \cdot t$, wo s Teiler von $p^n - 1$, t teilerfremd zu $p^n - 1$ ist?

3. Wenn ein Primideal $\mathfrak{p}$ in einem kommutativen Ring $\mathfrak{o}$ nur endlichviele Restklassen besitzt, so ist $\mathfrak{o}/\mathfrak{p}$ ein Galois-Feld.

4. Man untersuche insbesondere die Restklassenringe nach den Primidealen $(1+i)$, (3), $(2+i)$, (7) im Ring der ganzen Gaußschen Zahlen.

5. Man gebe die in Π ($p = 3$) irreduzible Gleichung für eine primitive achte Einheitswurzel in $GF(9)$ an, ebenso die in Π ($p = 2$) irreduzible Gleichung für eine primitive siebente Einheitswurzel in $GF(8)$.

6. Es gibt zu jedem p und m ganzzahlige Polynome $f(x)$ m-ten Grades, die mod p irreduzibel sind. Alle diese sind (mod p) Teiler von $x^{p^m} - x$.

§ 32. Separable und inseparable Erweiterungen (Erweiterungen erster und zweiter Art).

Δ sei wieder ein kommutativer Körper.

Wir fragen: Kann ein in $\Delta[x]$ irreduzibles Polynom in einem Erweiterungskörper mehrfache Nullstellen haben?

Damit $f(x)$ mehrfache Nullstellen besitzt, müssen $f(x)$ und $f'(x)$ einen nicht konstanten Faktor gemein haben, der sich nach **§ 16** schon in $\Delta[x]$ berechnen läßt. Ist $f(x)$ irreduzibel, so kann $f(x)$ mit einem Polynom niedrigeren Grades keinen nicht konstanten Faktor gemein haben; es muß also $f'(x) = 0$ sein.

Wir setzen

$$f(x) = \sum_0^n a_\nu x^\nu,$$

$$f'(x) = \sum_1^n \nu a_\nu x^{\nu-1}.$$

Soll $f'(x) = 0$ sein, so muß jeder Koeffizient verschwinden:

$$\nu a_\nu = 0 \qquad (\nu = 1, 2, \ldots).$$

Im Fall der Charakteristik Null folgt daraus $a_\nu = 0$ für alle $\nu \neq 0$. Ein nicht konstantes Polynom kann also keine mehrfache Nullstelle haben. — Im Fall der Charakteristik p ist $\nu a_\nu = 0$ auch für $a_\nu \neq 0$ möglich; dann muß aber

$$\nu \equiv 0 \,(p)$$

sein. Damit $f(x)$ eine mehrfache Nullstelle hat, müssen also alle Glieder verschwinden mit Ausnahme der Glieder $a_\nu x^\nu$ mit $\nu \equiv 0 \,(p)$; mithin hat $f(x)$ die Gestalt

$$f(x) = a_0 + a_p x^p + a_{2p} x^{2p} + \cdots.$$

Umgekehrt: wenn $f(x)$ diese Gestalt hat, so ist $f'(x) = 0$. Wir können in diesem Fall schreiben:

$$f(x) = \varphi(x^p).$$

Damit ist bewiesen: *Für Charakteristik Null hat ein in $\Delta[x]$ irreduzibles Polynom $f(x)$ nur einfache Nullstellen; für Charakteristik p hat $f(x)$ (wofern es nicht konstant ist) dann und nur dann vielfache Nullstellen, wenn $f(x)$ sich als Funktion von x^p schreiben läßt.*

Im letzteren Fall kann es sein, daß $\varphi(x)$ seinerseits Funktion von x^p ist. Dann ist $f(x)$ Funktion von x^{p^2}. Es sei $f(x)$ Funktion von x^{p^e}:

$$f(x) = \psi(x^{p^e}),$$

aber nicht Funktion von $x^{p^{e+1}}$. Dann ist $\psi(y)$ natürlich irreduzibel. Weiterhin ist $\psi'(y) \neq 0$; sonst wäre nämlich $\psi(y) = \chi(y^p)$, also $f(x) = \chi(x^{p^{e+1}})$, entgegen der Voraussetzung. — Also hat $\psi(y)$ lauter einfache Nullstellen.

Wir zerlegen $\psi(y)$ in einem Erweiterungskörper in Linearfaktoren:

$$\psi(y) = \prod_1^{n_0}(y - \beta_i).^1$$

Daraus folgt:

$$f(x) = \prod_1^{n_0}(x^{p^e} - \beta_i).$$

Es sei α_i eine Nullstelle von $x^{p^e} - \beta_i$. Dann ist

$$\alpha_i^{p^e} = \beta_i,$$
$$x^{p^e} - \beta_i = x^{p^e} - \alpha_i^{p^e} = (x - \alpha_i)^{p^e}.$$

Also ist α_i eine p^e-fache Nullstelle von $x^{p^e} - \beta_i$, und es ist

$$f(x) = \prod_1^{n_0}(x - \alpha_i)^{p^e}.$$

Alle Nullstellen von $f(x)$ haben also die gleiche Vielfachheit p^e.

Der Grad n_0 des Polynoms ψ heißt der *reduzierte Grad* von $f(x)$ (oder von α_i). e heißt der *Exponent* von $f(x)$ (oder von α_i) in bezug auf Δ. Zwischen dem Grad, dem reduzierten Grad und dem Exponenten besteht die Beziehung

$$n = n_0 p^e.$$

n_0 ist zugleich die Anzahl der verschiedenen Nullstellen von $f(x)$.

Ist Θ Nullstelle eines in $\Delta[x]$ irreduziblen Polynoms mit lauter getrennten (einfachen) Nullstellen, so heißt Θ *separabel* oder *von erster Art*[2] in bezug auf Δ. Auch das irreduzible Polynom $f(x)$, dessen Nullstellen alle separabel sind, heißt *separabel*. Im entgegengesetzten Fall heißen das algebraische Element Θ und das irreduzible Polynom $f(x)$ *inseparabel* oder *von zweiter Art*. Schließlich heißt ein algebraischer Oberkörper Σ, dessen Elemente sämtlich separabel in bezug auf Δ sind, *separabel* in bezug auf Δ und jeder andere algebraische Oberkörper *inseparabel*.

Im Fall der Charakteristik Null ist nach dem Vorigen jedes irreduzible Polynom (mithin auch jeder algebraische Erweiterungskörper) separabel; im Fall der Charakteristik p nur die Polynome mit dem Exponenten $e = 0$ (und mithin dem reduzierten Grad $n_0 = n$). Im Fall der Charakteristik p ist ein irreduzibles nichtkonstantes $\varphi(x)$ dann und nur dann inseparabel, wenn es sich als Polynom in x^p schreiben läßt.

---

[1] Ohne Beschränkung der Allgemeinheit kann der höchste Koeffizient von $\psi(y)$ gleich 1 gesetzt werden. n_0 ist der Grad von $\psi(y)$.

[2] Der Ausdruck „von erster Art" stammt von Steinitz. Ich schlage das Wort „separabel" vor, das in mehr suggestiver Weise zum Ausdruck bringen soll, daß alle Nullstellen von $f(x)$ getrennt liegen.

Wir werden später noch sehen, daß die meisten wichtigen und interessanten Körpererweiterungen separabel sind, und daß es ausgedehnte Klassen von Körpern gibt, die keiner inseparablen Erweiterungen fähig sind (sogenannte „vollkommene Körper"). Aus diesem Grunde sind im folgenden alle Untersuchungen, die sich insbesondere mit inseparablen Erweiterungen beschäftigen, mit kleinen Typen gedruckt.

Wir betrachten nun den algebraischen Körper $\Sigma = \Delta(\Theta)$. Während der Grad n der definierenden Gleichung $f(x) = 0$ zugleich den Körpergrad (Σ/Δ) angibt, gibt der reduzierte Grad n_0 zugleich die *Anzahl der Isomorphismen* des Körpers Σ an, in folgendem präzisierten Sinne: Wir betrachten nur solche Isomorphismen $\Sigma \cong \Sigma'$, welche alle Elemente des Unterkörpers Δ fest lassen, mithin Σ in äquivalente Körper Σ' überführen (*„relative Isomorphismen von Σ in bezug auf Δ"*), und weiter nur solche, bei denen der Bildkörper Σ' mit Σ zusammen innerhalb eines passend gewählten Oberkörpers Ω liegt. Es gilt nämlich der Satz:

Bei passender Wahl des Oberkörpers Ω hat $\Sigma = \Delta(\Theta)$ genau n_0 relative Isomorphismen, und bei keiner Wahl von Ω hat Σ mehr als n_0 solche Isomorphismen.

Beweis: Jeder relative Isomorphismus muß Θ in eine konjugierte Größe Θ' in Ω (Wurzel derselben irreduziblen Gleichung $f(x) = 0$) überführen. Wählt man nun Ω so, daß $f(x)$ in Ω ganz in Linearfaktoren zerfällt, so hat Θ tatsächlich n_0 Konjugierte $\Theta, \Theta', \ldots$, und die Körper $\Delta(\Theta), \Delta(\Theta'), \ldots$ sind in der Tat konjugiert oder äquivalent. Wie man aber auch Ω wählt, niemals hat Θ mehr als n_0 Konjugierte. Man beachte nun, daß ein relativer Isomorphismus $\Delta(\Theta) \cong \Delta(\Theta')$ vollständig durch die Angabe $\Theta \to \Theta'$ bestimmt ist. Soll nämlich Θ in Θ' übergehen und jede Größe aus Δ fest bleiben, so muß

$$\sum a_k \Theta^k \qquad (a_k \in \Delta)$$

in

$$\sum a_k \Theta'^k$$

übergehen, und das bestimmt den Isomorphismus. —

Ist speziell Θ separabel, so ist $n_0 = n$, mithin die Anzahl der relativen Isomorphismen gleich dem Körpergrad.

Wenn wir im folgenden von den (relativen) Isomorphismen von $\Sigma = \Delta(\Theta)$, von den Konjugierten zu Θ oder von den konjugierten Körpern zu Σ (in bezug auf Δ) reden, meinen wir immer die Isomorphismen bzw. Konjugierten in einem passend gewählten Körper Ω, für den wir immer wie oben den Zerfällungskörper von $f(x)$, d. h. den kleinsten in bezug auf Δ Galoisschen Körper, der Σ umfaßt, wählen können.

Wenn man einen festen Oberkörper zur Verfügung hat, in dem *jede* Gleichung $f(x) = 0$ ganz in Linearfaktoren zerfällt (wie es z. B. im Körper der komplexen Zahlen der Fall ist), so kann man für Ω ein für allemal diesen festen Oberkörper wählen und den Zusatz „in Ω" bei

Aussagen über Isomorphismen immer weglassen. So wird es z. B. in der Theorie der Zahlkörper immer getan. Daß man sich auch bei abstrakten Körpern immer ein solches Ω verschaffen kann, wird sich in § 60 zeigen.

Aufgaben. 1. Ist Π ein Körper von der Charakteristik p und x eine Unbestimmte, so ist die Gleichung $z^p - x = 0$ in $\Pi(x)[z]$ irreduzibel und der durch diese Gleichung definierte Körper $\Pi\left(x^{\frac{1}{p}}\right)$ inseparabel über $\Pi(x)$.

2. Man konstruiere die relativen Isomorphismen in bezug auf den rationalen Grundkörper Γ:

a) des Körpers der fünften Einheitswurzeln,

b) des Körpers $\Gamma(\sqrt[3]{2})$.

3. Wenn $\Theta^{p^e} = \gamma$ in Δ liegt, aber $\Theta^{p^{e-1}}$ nicht, so ist das Polynom $x^{p^e} - \gamma$ in $\Delta[x]$ irreduzibel.

Eine Verallgemeinerung des obigen Satzes ist der folgende:

Wenn ein Oberkörper Σ aus Δ entsteht durch sukzessive Adjunktion von m algebraischen Größen $\alpha_1, \ldots, \alpha_m$ und wenn jedes α_i Wurzel einer in $\Delta(\alpha_1, \ldots, \alpha_{i-1})$ irreduziblen Gleichung vom reduzierten Grad n_i' ist, so hat Σ in einem passenden Oberkörper Ω genau $\prod_1^m n_i'$ relative Isomorphismen in bezug auf Δ, und in keinem Oberkörper gibt es mehr als $\prod_1^m n_i'$ solche Isomorphismen von Σ.

Beweis: Der Satz wurde für $m = 1$ eben bewiesen. Er möge also für $\Sigma_1 = \Delta(\alpha_1, \ldots, \alpha_{m-1})$ schon als richtig erkannt sein: es gebe in einem passenden Ω_1 genau $\prod_1^{m-1} n_i'$ relative Isomorphismen von Σ_1 und niemals mehr. Einer dieser $\prod_1^{m-1} n_i'$ Isomorphismen sei $\Sigma_1 \to \overline{\Sigma}_1$. Wir behaupten nun, daß dieser Isomorphismus sich in passendem Ω auf genau n_m' Weisen zu einem Isomorphismus $\Sigma = \Sigma_1(\alpha_m) \cong \overline{\Sigma} = \overline{\Sigma}_1(\bar{\alpha}_m)$ fortsetzen läßt und niemals auf mehr als n_m' Arten.

α_m genügt in Σ_1 einer Gleichung $f_1(x) = 0$ mit genau n_m' verschiedenen Wurzeln. Durch die Isomorphie $\Sigma_1 \to \overline{\Sigma}_1$ möge $f_1(x)$ in $\bar{f}_1(x)$ übergehen. Dann hat $\bar{f}_1(x)$ in einem passenden Erweiterungskörper wieder n_m' verschiedene Wurzeln und niemals mehr. Eine dieser Wurzeln sei $\bar{\alpha}_m$. Nach Wahl von $\bar{\alpha}_m$ läßt sich der Isomorphismus $\Sigma_1 \cong \overline{\Sigma}_1$ in einer und nur einer Weise zu einem Isomorphismus $\Sigma_1(\alpha_m) \cong \overline{\Sigma}_1(\bar{\alpha}_m)$ mit $\alpha_m \to \bar{\alpha}_m$ fortsetzen; diese Fortsetzung ist nämlich gegeben durch die Formel

$$\sum c_k \alpha_m^k \to \sum \bar{c}_k \bar{\alpha}_m^k .$$

Da man die Wahl von $\bar{\alpha}_m$ auf n_m' Arten treffen kann, so gibt es n_m' solche Fortsetzungen zu jedem gewählten Isomorphismus $\Sigma_1 \to \overline{\Sigma}_1$. Da man diesen Isomorphismus seinerseits auf $\prod_1^{m-1} n_i'$ Arten wählen kann, so gibt es im ganzen (in einem solchen Oberkörper Ω, in dem alle in Betracht kommenden Gleichungen vollständig zerfallen)

$$\prod_1^{m-1} n_i' \cdot n_m' = \prod_1^m n_i'$$

relative Isomorphismen für Σ und niemals mehr, q. e. d.

Ist n_i der volle (nichtreduzierte) Grad von α_i in bezug auf $\Delta(\alpha_1, \ldots, \alpha_{i-1})$, so ist n_i zugleich der Körpergrad von $\Delta(\alpha_1, \ldots, \alpha_i)$ in bezug auf $\Delta(\alpha_1, \ldots, \alpha_{i-1})$; mithin ist der Körpergrad (Σ/Δ) gleich $\prod_1^m n_i$. Vergleichen wir diese Anzahl mit der Isomorphismenzahl $\prod_1^m n_i'$, so folgt:

Die Anzahl der relativen Isomorphismen eines endlichen Erweiterungskörpers $\Sigma = \Delta(\alpha_1, \ldots, \alpha_m)$ in bezug auf Δ (in einem passenden Erweiterungskörper Ω) ist dann und nur dann gleich dem Körpergrad (Σ/Δ), wenn jedes α_i separabel in bezug auf das zugehörige $\Delta(\alpha_1, \ldots, \alpha_{i-1})$ ist. Ist dagegen auch nur ein α_i inseparabel, so ist die Isomorphismenzahl kleiner als der Körpergrad.

Aus diesem Satz fließen sofort eine Anzahl wichtige Folgerungen. Der Satz besagt zunächst, daß die Eigenschaft, daß jedes α_i separabel in bezug auf den Körper der vorangehenden ist, eine Eigenschaft des Körpers Σ darstellt, unabhängig von der Wahl der Erzeugenden α_i. Da man jede beliebige Größe β des Körpers als erste Erzeugende wählen kann, so folgt sofort, daß jede Größe β des Körpers Σ separabel ist, sobald alle α_i es im angegebenen Sinne sind. Mithin:

Adjungiert man zu Δ sukzessiv die Größen $\alpha_1, \ldots, \alpha_n$ und ist jedes α_i separabel in bezug auf den Körper der vorangehenden, so ist der entstehende Körper

$$\Sigma = \Delta(\alpha_1, \ldots, \alpha_n)$$

separabel über Δ.

Insbesondere: *Summe, Differenz, Produkt und Quotient separabler Größen sind separabel.*

Weiter: *Ist β separabel in bezug auf Σ und Σ separabel in bezug auf Δ, so ist β separabel in bezug auf Δ.* Denn β genügt einer Gleichung mit endlichvielen Koeffizienten $\alpha_1, \ldots, \alpha_m$ aus Σ, ist also separabel in bezug auf $\Delta(\alpha_1, \ldots, \alpha_m)$. Daher ist auch

$$\Delta(\alpha_1, \ldots, \alpha_m, \beta)$$

separabel.

Schließlich haben wir: *Die Anzahl der relativen Isomorphismen eines separablen endlichen Erweiterungskörpers Σ von Δ ist gleich dem Körpergrad (Σ/Δ).*

Da nach dem Vorigen alle rationalen Operationen, ausgeübt auf separable Elemente, wieder separable Elemente ergeben, so bilden in einem beliebigen Oberkörper Ω von Δ die separablen Größen für sich einen Körper Ω_0. Man kann Ω_0 auch beschreiben als die größte separable Erweiterung von Δ, die in Ω liegt.

Ist Ω algebraisch in bezug auf Δ, aber nicht notwendig separabel, so liegt von jedem Element α von Ω die p^e-te Potenz in Ω_0, wenn e der Exponent des betreffenden Elements ist. Aus den Betrachtungen zu Anfang dieses Paragraphen folgt nämlich unmittelbar, daß α^{p^e} einer Gleichung mit lauter verschiedenen Wurzeln genügt. Also:

Ω entsteht aus Ω_0 durch Ausziehung von lauter p^e-ten Wurzeln.

Ist Ω insbesondere endlich in bezug auf Δ, so sind die Exponenten e natürlich beschränkt. Der größte unter ihnen, der wieder mit e bezeichnet werden soll, heißt der *Exponent* von Ω. Der Grad von Ω_0 heißt der *reduzierte Grad* von Ω.

Man kann natürlich die Ausziehung der p^e-ten Wurzeln auch durch sukzessive Ausziehung von p-ten Wurzeln erreichen. Bei Ausziehung einer p-ten Wurzel, die nicht schon im Körper vorhanden war (also bei Adjunktion einer Wurzel einer irreduziblen Gleichung $z^p - \beta = 0$), multipliziert sich der Körpergrad mit p. Also wird schließlich, wenn man insgesamt f mal eine p-te Wurzel ausgezogen hat,

$$(\Omega/\Delta) = (\Omega_0/\Delta) \cdot p^f$$

oder

$$\text{Grad} = \text{reduzierter Grad} \cdot p^f,$$

wie bei einfachen inseparablen Erweiterungen.

Mit p^e-ten Wurzeln rechnet es sich besonders einfach. Ist α eine p^e-te Wurzel aus β, so ist, wie wir schon sahen,

$$x^{p^e} - \beta = x^{p^e} - \alpha^{p^e} = (x - \alpha)^{p^e};$$

also ist eine p^e-te Wurzel aus β in jedem Körper, in dem sie überhaupt existiert, *eindeutig bestimmt*. Weiter ist

$$\sqrt[p^e]{\alpha + \beta} = \sqrt[p^e]{\alpha} + \sqrt[p^e]{\beta},$$
$$\sqrt[p^e]{\alpha\,\beta} = \sqrt[p^e]{\alpha} \cdot \sqrt[p^e]{\beta},$$

wie man durch Erhebung in die p^e-te Potenz sieht.

Aufgabe. 4. Sind für eine endliche inseparable Erweiterung e und f wie oben definiert, so ist $e \leqq f$. Bei einer einfachen Erweiterung ist $e = f$. Man gebe ein Beispiel für $e < f$. [Adjunktion der p-ten Wurzeln aus zwei oder mehr Unbestimmten.]

§ 33. Vollkommene und unvollkommene Körper. Wurzelkörper.

Alle in diesem Paragraphen vorkommenden Körper sollen kommutativ sein.

Ein Körper Δ heißt *vollkommen*, wenn jedes in $\Delta[x]$ irreduzible Polynom $f(x)$ separabel ist. Jeder andere Körper heißt *unvollkommen*.

Wann ein Körper vollkommen ist, kommt in den folgenden beiden Sätzen zum Ausdruck:

I. *Körper von der Charakteristik Null sind immer vollkommen.*

Beweis: Siehe § 32.

II. *Ein Körper von der Charakteristik p ist dann und nur dann vollkommen, wenn es zu jedem Element im Körper eine p-te Wurzel gibt.*

Beweis: Wenn es zu jedem Element eine p-te Wurzel im Körper gibt, so ist jedes Polynom $f(x)$, das nur Potenzen von x^p enthält, eine p-te Potenz, wegen:

$$f(x) = \sum_k a_k (x^p)^k = \Big\{ \sum_k \sqrt[p]{a_k}\, x^k \Big\}^p;$$

d. h. jedes irreduzible Polynom ist in diesem Fall separabel, mithin der Körper vollkommen.

Andrerseits: Gibt es ein Element α im Körper, das keine p-te Potenz ist, so ist das Polynom

$$f(x) = x^p - \alpha$$

irreduzibel und nicht separabel, mithin der Körper unvollkommen.

Aus diesem Satz II und einem Satz von § 31 folgt unmittelbar:

Alle Galois-Felder sind vollkommen.

In einem algebraisch-abgeschlossenen Körper (Definition siehe § 60) ist jedes irreduzible Polynom linear; mithin:

Alle algebraisch-abgeschlossenen Körper sind vollkommen.

Aus der Definition des vollkommenen Körpers folgen unmittelbar die beiden Sätze:

Jede algebraische Erweiterung eines vollkommenen Körpers ist in bezug auf diesen separabel.

Zu einem unvollkommenen Körper gibt es inseparable Erweiterungen. Diese inseparablen Erweiterungen erhält man nämlich, indem man irgend eine Nullstelle einer Primfunktion zweiter Art adjungiert.

Die beim Beweis von II gemachte Bemerkung, daß in einem vollkommenen Körper von der Charakteristik p jedes Polynom $f(x)$, das nur von x^p abhängt, eine p-te Potenz ist, gilt kraft ihres Beweises auch für Polynome in mehreren Veränderlichen $f(x, y, z, \ldots)$, die zugleich Polynome in $x^p, y^p, z^p, \ldots$ sind. Auch dies ist eine oft verwendete Eigenschaft der vollkommenen Körper von der Charakteristik p.

Wurzelkörper. Es sei Δ irgend ein Körper von der Charakteristik p. Ordnet man jedem Element x von Δ seine p-te Potenz x^p zu, so entsteht eine Zuordnung von Δ zu einer Untermenge, die wir Δ^p nennen. Im Falle eines vollkommenen Δ ist, wie wir sahen, $\Delta^p = \Delta$. Auf jeden Fall ist aber die Zuordnung eineindeutig; denn wegen

$$a^p - b^p = (a - b)^p$$

zieht $a^p = b^p$ notwendig $a = b$ nach sich. Weiter ist die Zuordnung ein *Isomorphismus* wegen

$$a^p + b^p = (a + b)^p,$$
$$a^p \cdot b^p = (a \cdot b)^p.$$

Also ist Δ^p ein mit Δ isomorpher Körper.

In genau derselben Weise kann man nun umgekehrt aus einem Körper Δ einen isomorphen Erweiterungskörper $\Delta^{\frac{1}{p}}$ konstruieren, von dem Δ eine p-te Potenz ist. Man hat nur alle p-ten Wurzeln $a^{\frac{1}{p}}$ der Elemente von Δ zu adjungieren, soweit sie nicht in Δ liegen, und diese den Rechnungsregeln

$$a^{\frac{1}{p}} + b^{\frac{1}{p}} = (a + b)^{\frac{1}{p}},$$
$$a^{\frac{1}{p}} \cdot b^{\frac{1}{p}} = (a \cdot b)^{\frac{1}{p}}$$

zu unterwerfen. Die Körpereigenschaften für $\Delta^{\frac{1}{p}}$ sind mit Hilfe der Isomorphie $a \to a^{\frac{1}{p}}$ mühelos zu beweisen, was dem Leser überlassen bleiben möge. Auch ist $\Delta^{\frac{1}{p}}$ bis auf äquivalente Erweiterungen eindeutig durch Δ bestimmt.

Ist Δ vollkommen, so ist natürlich $\Delta^{\frac{1}{p}} = \Delta$ und umgekehrt.

Man nennt $\Delta^{\frac{1}{p}}$ den *Wurzelkörper* von Δ. Konstruiert man zu $\Delta^{\frac{1}{p}}$ wieder den Wurzelkörper usw., so entsteht eine Reihe von Körpern

$$\Delta, \Delta^{\frac{1}{p}}, \Delta^{\frac{1}{p^2}}, \ldots,$$

deren Vereinigung offenbar ein vollkommener Körper ist, und zwar der kleinste vollkommene Körper, der Δ umfaßt.

Aufgaben. 1. Man führe die Beweise durch.

2. Jede algebraische Erweiterung eines vollkommenen Körpers ist vollkommen.

3. Jede endliche algebraische Erweiterung eines unvollkommenen Körpers ist unvollkommen.

4. Man konstruiere den Wurzelkörper zu $\Pi(x)$, wo Π ein vollkommener Körper der Charakteristik p und x eine Unbestimmte ist; ebenso den kleinsten umfassenden vollkommenen Körper.

§ 34. Einfachheit von algebraischen Erweiterungen. Der Satz vom primitiven Element.

Wir wollen untersuchen, in welchen Fällen eine kommutative endliche Erweiterung Σ eines (kommutativen) Körpers Δ einfach ist, d. h. durch Adjunktion eines einzigen erzeugenden oder „*primitiven*" Elements entsteht. Auf diese Frage gibt der folgende *Satz vom primitiven Element* in einer weiten Klasse von Fällen Antwort. Er lautet:

Es sei $\Delta(\alpha_1, \ldots, \alpha_h)$ *ein endlicher algebraischer Erweiterungskörper von* Δ *und* $\alpha_2, \ldots, \alpha_h$ *separable Elemente*[1]. *Dann ist* $\Delta(\alpha_1, \ldots, \alpha_h)$ *eine einfache Erweiterung*:

$$\Delta(\alpha_1, \ldots, \alpha_h) = \Delta(\Theta).$$

Beweis: Wir beweisen den Satz zunächst für zwei Elemente α, β, von denen zumindest β separabel sein soll. Es sei $f(x) = 0$ die irreduzible Gleichung für α, $g(x) = 0$ die für β. Wir gehen in einen Körper, in dem $f(x)$ und $g(x)$ vollständig zerfallen. Die verschiedenen Nullstellen von $f(x)$ seien $\alpha_1, \ldots, \alpha_r$; die von $g(x)$ seien $\beta_1, \ldots, \beta_s$; es sei etwa $\alpha_1 = \alpha$, $\beta_1 = \beta$.

Wir können voraussetzen, daß Δ unendlichviele Elemente hat; denn andernfalls hat auch $\Delta(\alpha, \beta)$ nur endlichviele, und für endliche Körper ist die Existenz eines primitiven Elements (sogar einer primitiven Einheitswurzel, von der alle Körperelemente außer der Null Potenzen sind) bereits in § 31 bewiesen.

Für $k \neq 1$ ist $\beta_k \neq \beta_1$, also hat die Gleichung

$$\alpha_i + x\beta_k = \alpha_1 + x\beta_1$$

für jedes i und jedes $k \neq 1$ höchstens eine Wurzel x in Δ. Wählt man nun c verschieden von den Wurzeln aller dieser linearen Gleichungen, so ist für jedes i und $k \neq 1$:

$$\alpha_i + c\beta_k \neq \alpha_1 + c\beta_1.$$

Wir setzen

$$\Theta = \alpha_1 + c\beta_1 = \alpha + c\beta.$$

Dann ist Θ Element von $\Delta(\alpha, \beta)$. Ich behaupte, daß Θ schon die Eigenschaft des gesuchten primitiven Elementes hat: $\Delta(\alpha, \beta) = \Delta(\Theta)$.

Das Element β genügt den Gleichungen

$$g(\beta) = 0,$$
$$f(\Theta - c\beta) = f(\alpha) = 0,$$

deren Koeffizienten in $\Delta(\Theta)$ liegen. Die Polynome $g(x)$, $f(\Theta - cx)$ haben auch nur die Wurzel β gemein; denn für die weiteren Wurzeln $\beta_k (k \neq 1)$ der ersten Gleichung ist

$$\Theta - c\beta_k \neq \alpha_i \qquad (i = 1, \ldots, r),$$

also

$$f(\Theta - c\beta_k) \neq 0.$$

---

[1] Ob auch α_1 und damit der ganze Körper separabel ist, ist gleichgültig.

β ist eine einfache Wurzel von $g(x)$; demnach haben $g(x)$ und $f(\Theta - cx)$ nur einen Linearfaktor $x - \beta$ gemein. Die Koeffizienten dieses größten gemeinsamen Teilers müssen schon in $\Delta(\Theta)$ liegen; β liegt also in $\Delta(\Theta)$. Aus $\alpha = \Theta - c\beta$ folgt dasselbe für α, mithin ist in der Tat $\Delta(\alpha, \beta) = \Delta(\Theta)$.

Damit ist unser Satz für $h = 2$ bewiesen. Ist er für $h - 1$ ($\geqq 2$) schon bewiesen, so hat man

$$\Delta(\alpha_1, \ldots, \alpha_{h-1}) = \Delta(\eta),$$

also

$$\Delta(\alpha_1, \ldots, \alpha_h) = \Delta(\eta, \alpha_h) = \Delta(\Theta),$$

nach dem schon bewiesenen Teil des Satzes; mithin folgt der Satz für h.

Folgerung: *Jede separable endliche Erweiterung ist einfach.*

Dieser Satz vereinfacht die Untersuchung der endlichen separablen Erweiterungen oft sehr, da wir Struktur und Isomorphismen dieser Erweiterungen vermöge der übersichtlichen Basisdarstellung

$$\sum_0^{n-1} a_k \Theta^k$$

leicht beherrschen. Zum Beispiel ergibt sich jetzt ein neuer Beweis für die in § 32 (kleine Typen) mittels sukzessiver Fortsetzung von Isomorphismen bewiesene Tatsache, daß *eine endliche separable Erweiterung Σ von Δ so viele Isomorphismen relativ zu Δ besitzt, wie der Grad (Σ/Δ) angibt.* Denn für einfache separable Erweiterungen wurde diese Behauptung schon vorher in § 32 bewiesen, und jede endliche separable Erweiterung ist, wie wir jetzt wissen, eine einfache[1].

Im Falle der Charakteristik Null ist jede endliche Erweiterung separabel, also einfach. Wir können aber auch im Falle der Charakteristik p genau angeben, wann eine endliche Erweiterung einfach ist:

Eine endliche Erweiterung Σ eines Körpers Δ von der Charakteristik p ist dann und nur dann einfach, wenn

$$n = n_0 p^e \tag{1}$$

ist, wo n der Grad, n_0 der reduzierte Grad und e der Exponent der Erweiterung ist.

Beweis: Zunächst eine Vorbemerkung. Ist $\Sigma = \Delta(\alpha_1, \ldots, \alpha_r)$, so ist der Exponent von Σ gleich dem Maximum e der Exponenten von $\alpha_1, \ldots, \alpha_r$. Denn zunächst ist der Exponent von Σ sicher $\geqq e$. Da aber alle Elemente von Σ sich rational durch $\alpha_1, \ldots, \alpha_r$ (mit Koeffizienten aus Δ) ausdrücken, so lassen sich wegen der Potenzierungsregel die p^e-ten Potenzen der Elemente von Σ rational durch $\alpha_1^{p^e}, \ldots, \alpha_r^{p^e}$ ausdrücken; diese p^e-ten Potenzen sind mithin separable Elemente, und der Exponent von Σ ist genau e. Die separablen Elemente von Σ bilden nach § 32 wieder einen separablen Erweiterungskörper Σ_0 in Σ.

[1] Der frühere (längere) Beweis mittels sukzessiver Fortsetzung war lehrreicher; denn aus ihm ließ sich die ganze Theorie der inseparablen Erweiterungen entwickeln. Demjenigen Leser aber, der sich hauptsächlich für separable Erweiterungen interessiert, die ja auch die wichtigsten und häufigsten sind, sei der obige Beweisgang mittels des Satzes vom primitiven Element empfohlen.

Nun sei Σ einfach: $\Sigma = \Delta(\Theta)$. Dann ist $\Theta^{p^e} \in \Sigma_0$. Setzt man also wieder $(\Sigma/\Sigma_0) = p^f$, so ist $f \leqq e$ und (wie immer) $e \leqq f$, mithin $e = f$; daraus und aus $n = n_0 p^f$ folgt die Relation (1).

Umgekehrt sei (1) erfüllt. Σ_0 ist eine endliche separable Erweiterung, also einfach:

$$\Sigma_0 = \Delta(\alpha).$$

Ich suche mir ein Element β von Σ, das genau den Exponenten e hat. Dann ist

$$\beta^{p^e} = \mu_0 \in \Sigma_0$$

und $x^{p^e} - \mu_0$ ist irreduzibel in Σ_0, da sonst schon $\beta^{p^{e-1}}$ in Σ_0 liegen müßte (§ 32, Aufg. 3). $\Sigma_0(\beta)$ hat also den Grad p^e in bezug auf Σ_0, also den Grad $n = n_0 p^e$ in bezug auf Δ. Da auch Σ den Grad n in bezug auf Δ hat, so folgt $\Sigma_0(\beta) = \Sigma$ oder $\Sigma = \Delta(\alpha, \beta)$. Da α separabel ist, so ergibt sich aus dem Satz vom primitiven Element, daß Σ einfach ist, q. e. d.

Aufgaben. 1. Sind x und y Unbestimmte, so ist die Erweiterung $\Delta\left(x^{\frac{1}{p}}, y^{\frac{1}{p}}\right)$ von $\Delta(x, y)$ nicht mehr einfach.

2. Für Charakteristik $\neq 2$ gilt immer

$$\Delta(\sqrt{x}, \sqrt{y}) = \Delta(x, y, \sqrt{x} + \sqrt{y}),$$

dagegen nicht für Charakteristik 2.

§ 35. Normen und Spuren.

Es sei wieder Σ ein endlicher kommutativer Erweiterungskörper von Δ. Die relativen Isomorphismen von Σ, die Σ in seine konjugierten Körper überführen, führen jedes Element η von Σ auch in zu η konjugierten Elemente über. Nehmen wir der Einfachheit halber Σ als eine einfache Erweiterung an: $\Sigma = \Delta(\Theta)$, so ist

$$\eta = \psi(\Theta) = a_0 + a_1\Theta + \cdots + a_{n-1}\Theta^{n-1}$$

und wir erhalten bei Ausführung der Isomorphismen, indem wir Θ durch seine konjugierten Größen ersetzen:

$$\eta_\nu = \psi(\Theta_\nu) = a_0 + a_1\Theta_\nu + \cdots + a_{n-1}\Theta_\nu^{n-1}.$$

Dabei sind die konjugierten Größen Θ_ν numeriert von 1 bis n und jede so oft gezählt, als sie vorkommt bei der Linearfaktorzerlegung des in $\Delta[t]$ irreduziblen Polynoms $\varphi(t)$, dessen Wurzel Θ ist. Bei separablem Θ wird demnach jeder Isomorphismus einmal, bei inseparablem Θ mehrmals gezählt.

Das Polynom

$$G(z) = \prod_1^n (z - \eta_\nu) = \prod_1^n (z - \psi(\Theta_\nu))$$

ist symmetrisch in $\Theta_1, \ldots, \Theta_n$ und seine Koeffizienten sind daher ganzrational durch die elementarsymmetrischen Funktionen, d. h. durch die Koeffizienten von $\varphi(t)$ ausdrückbar. $G(z)$ hat als Nullstellen nur η und dessen konjugierten Größen. Ist $g(z)$ das (irreduzible) Polynom kleinsten Grades in $\Delta[z]$ mit der Nullstelle η und dem höchsten Koeffizienten 1,

so muß $G(z)$ einer Potenz von $g(z)$ gleich sein, denn wenn $G(z)$ noch andere irreduzible Faktoren hätte, so hätte $G(z)$ auch Nullstellen, die nicht mit η konjugiert wären. Mithin ist

$$G(z) = g(z)^r; \tag{1}$$

$$r = \frac{n}{\text{Grad von } g(z)} = \frac{(\Sigma/\Delta)}{(\Delta(\eta)/\Delta)} = (\Sigma/\Delta(\eta)).$$

Setzt man

$$G(z) = z^n - b_1 z^{n-1} + \cdots + (-1)^n b_n,$$

so sind die Koeffizienten b_λ die elementarsymmetrischen Funktionen der η_ν. Besondere Namen hat man für den ersten und den letzten Koeffizienten:

$$b_1 = \sum_1^n \eta_\nu = S(\eta) = \text{Spur von } \eta,$$

$$b_n = \prod_1^n \eta_\nu = N(\eta) = \text{Norm von } \eta.$$

Offenbar ist

$$S(\alpha + \beta) = S(\alpha) + S(\beta),$$
$$N(\alpha\beta) = N(\alpha) \cdot N(\beta).$$

Die Norm und Spur hängen nicht nur von η und vom Grundkörper Δ ab, sondern auch vom Oberkörper Σ. Wenn man das zum Ausdruck bringen will, schreibt man N_Σ und S_Σ statt N und S. Ist T ein Erweiterungskörper von Σ vom Relativgrad $(\mathsf{T}/\Sigma) = s$, so wird:

$$G_\mathsf{T}(z) = g(z)^{rs} = G_\Sigma(z)^s$$

und daher

$$S_\mathsf{T}(\eta) = s \cdot S_\Sigma(\eta),$$
$$N_\mathsf{T}(z) = (N_\Sigma(z))^s.$$

Für $G(z) = \prod_1^n (z - \eta_\nu)$ kann man nunmehr auch schreiben

$$G(z) = N(z - \eta),$$

indem man die Normenbezeichnung in naheliegender Weise auf solche Ausdrücke ausdehnt, die außer Größen von Σ auch noch Unbestimmte enthalten. Bei der Berechnung der symmetrischen Funktion

$$G(z) = N(z - \eta) = \prod_1^n (z - \psi(\Theta_\nu))$$

zeigt sich, daß $N(z - \eta)$ eine homogene Form vom Grade n in $z, a_0, \ldots, a_{n-1}$ wird. Um das zum Ausdruck zu bringen, ist es angemessen, die a vorher durch Unbestimmte u zu ersetzen, mithin statt η die Größe

$$\eta_u = u_0 + u_1\Theta + \cdots + u_{n-1}\Theta^{n-1}$$

zu betrachten. Nach vollendeter Berechnung von $G(z, u) = N(z - \eta_u)$ kann man dann immer die Unbestimmten u durch die a ersetzen.

Das Polynom $N(z-\eta_u)$ ist nun zu charakterisieren als das (natürlich irreduzible) Polynom kleinsten Grades in $\Delta(u)[z]$ mit Anfangskoeffizienten 1, das η_u als Nullstelle hat. Gäbe es nämlich ein irreduzibles Polynom kleineren Grades mit Anfangskoeffizienten 1 und der Nullstelle η_u, so müßte zunächst dieses Polynom ein Teiler von $N(z-\eta_u)$ sein, also nach § 21 auch ganzrational in den u, und es würde sich bei der Spezialisierung: $u_1 = 1$, übrige $u_\nu = 0$ ergeben, daß auch Θ einer Gleichung in Δ vom Grad $m < n$ genügte, was nicht geht.

Einen anderen Ausdruck für das Polynom $N(z-\eta_u)$ bzw. $N(z-\eta)$ erhält man folgendermaßen. Man wähle irgend eine Körperbasis $(\omega_1, \ldots, \omega_n)$ von Σ (am bequemsten wieder die Basis $(1, \Theta, \Theta^2, \ldots, \Theta^{n-1})$) und drücke alle Produkte $\eta_u \omega_\lambda$ durch diese Basis aus:

$$\eta_u \omega_\lambda = \sum_1^n c_{\lambda\mu}(u)\, \omega_\mu .$$

Aus diesen linearen Gleichungen eliminiert man die ω_μ, die ja nicht Null sind, und erhält:

$$D(\eta_u) = \begin{vmatrix} \eta_u - c_{11}(u) & -c_{12}(u) \cdots \\ -c_{21}(u) & \eta_u - c_{22}(u) \cdots \\ \cdots & \cdots \end{vmatrix} = 0 .$$

Da die c_{ik} Linearformen der u_ν sind, ist $D(z)$ ein Polynom in z und den u vom Grade n, mit Anfangskoeffizienten 1 und der Nullstelle η_u. Daraus folgt nach dem Vorigen:

$$D(z) = N(z-\eta_u) .$$

Ersetzt man nachher die u durch Koeffizienten a_ν aus Δ, so erhält man einen Determinantenausdruck für $N(z-\eta)$:

$$\eta \omega_\lambda = \sum c_{\lambda\mu} \omega_\mu ,$$

$$N(z-\eta) = \begin{vmatrix} z - c_{11} & -c_{12} \cdots \\ -c_{21} & z - c_{22} \cdots \\ \cdots & \cdots \end{vmatrix} . \tag{2}$$

Daraus sind die Koeffizienten $b_1, \ldots, b_n$ von $N(z-\eta)$ abzulesen. Z. B. ist

$$S(\eta) = \sum_\nu c_{\nu\nu} , \qquad N(\eta) = |c_{\lambda\mu}| .$$

Aufgaben. 1. Man beweise direkt die Unabhängigkeit der Determinante (2) von der Wahl der Basis $(\omega_1, \ldots, \omega_n)$.

2. Für nicht-einfache Erweiterungen kann man entweder die Formel (1) oder (2) als Definition von $N(z-\eta)$ benutzen (letzteres eindeutig nach Aufg. 1). Man beweise die Übereinstimmung der beiden Definitionen.

§ 36. Einfache transzendente Erweiterungen.

Jede einfache transzendente Erweiterung eines (kommutativen) Körpers Δ ist, wie wir wissen, äquivalent dem Quotientenkörper $\Delta(x)$ des Polynombereichs $\Delta[x]$. Wir studieren daher diesen Quotientenkörper

$$\Omega = \Delta(x).$$

Elemente von Ω sind rationale Funktionen

$$\eta = \frac{f(x)}{g(x)},$$

die in unverkürzbarer Gestalt (f und g teilerfremd) angenommen werden können. Der größte der beiden Grade von $f(x)$ und $g(x)$ heißt der *Grad* der Funktion η.

Satz. *Jedes nichtkonstante η vom Grade n ist transzendent in bezug auf Δ, und $\Delta(x)$ ist algebraisch vom Grade n in bezug auf $\Delta(\eta)$.*

Beweis: Die Darstellung $\eta = \frac{f(x)}{g(x)}$ sei unverkürzbar. Dann genügt x der Gleichung

$$g(x) \cdot \eta - f(x) = 0$$

mit Koeffizienten aus $\Delta(\eta)$. Diese Koeffizienten können nicht alle Null sein. Wären sie es nämlich und wäre a_k ein nichtverschwindender Koeffizient in $g(x)$, b_k der Koeffizient derselben Potenz von x in $f(x)$, so hätte man

$$a_k \eta - b_k = 0,$$

mithin $\eta = \frac{b_k}{a_k} = \text{konst.}$, entgegen der Voraussetzung. Also ist x algebraisch in bezug auf $\Delta(\eta)$.

Wäre nun η algebraisch in bezug auf Δ, so wäre auch x algebraisch in bezug auf Δ, was nicht der Fall ist. Mithin ist η transzendent.

x ist Nullstelle des Polynoms in $\Delta(\eta)[z]$

$$g(z)\eta - f(z)$$

vom Grade n. Dieses Polynom ist irreduzibel in $\Delta(\eta)[z]$. Denn sonst wäre es nach § 21 auch in $\Delta[\eta, z]$ reduzibel; da es linear in η ist, müßte ein Faktor von η unabhängig sein und nur von z abhängen; einen solchen Faktor kann es aber nicht geben, da $g(z)$ und $f(z)$ teilerfremd sind.

Mithin ist x algebraisch vom Grade n in bezug auf $\Delta(\eta)$. Daraus folgt die Behauptung $(\Delta(x)/\Delta(\eta)) = n$.

Wir merken uns für später noch, daß das Polynom

$$g(z)\eta - f(z)$$

keinen von z allein abhängigen (in $\Delta[z]$ liegenden) Faktor hat. Dieser Tatbestand bleibt erhalten, wenn man η durch seinen Wert $\frac{f(x)}{g(x)}$ er-

setzt und mit dem Nenner $g(x)$ aufmultipliziert; mithin hat das Polynom in $\Delta[x, z]$

$$g(z)f(x) - f(z)g(x)$$

keinen von z allein abhängigen Faktor.

Aus dem bewiesenen Satz fließen drei *Folgerungen.*

1. Der Grad einer Funktion $\eta = \frac{f(x)}{g(x)}$ hängt nur von den Körpern $\Delta(\eta)$ und $\Delta(x)$, nicht von der speziellen Wahl der Erzeugenden x des letzteren Körpers ab.

2. Dann und nur dann ist $\Delta(\eta) = \Delta(x)$, wenn η vom Grade 1, also gebrochen-linear ist. Das heißt: *Körpererzeugende sind neben x alle gebrochenen linearen Funktionen von x und nur diese.*

3. Ein Automorphismus von $\Delta(x)$, der die Elemente von Δ fest läßt, muß x wieder in eine Körpererzeugende überführen. Führt man umgekehrt x in eine andere Körpererzeugende $\bar{x} = \frac{ax + b}{cx + d}$ und jedes $\varphi(x)$ in $\varphi(\bar{x})$ über, so entsteht ein Automorphismus, bei dem die Elemente von Δ fest bleiben. Also:

Alle relativen Automorphismen von $\Delta(x)$ in bezug auf Δ sind die gebrochen-linearen Substitutionen

$$\bar{x} = \frac{ax + b}{cx + d}, \qquad ad - bc \neq 0.$$

Wichtig für gewisse geometrische Untersuchungen ist der folgende Satz von Lüroth: *Jeder Zwischenkörper Σ mit $\Delta \subset \Sigma \subseteq \Delta(x)$ ist eine einfache transzendente Erweiterung: $\Sigma = \Delta(\Theta)$.*

Beweis: Das Element x muß algebraisch in bezug auf Σ sein; denn wenn η irgend ein nicht in Δ gelegenes Element von Σ ist, so ist x, wie gezeigt, algebraisch in bezug auf $\Delta(\eta)$, also um so mehr in bezug auf Σ. Das im Polynombereich $\Sigma[z]$ irreduzible Polynom mit dem höchsten Koeffizienten 1 und der Nullstelle x sei

$$f_0(z) = z^n + a_1 z^{n-1} + \cdots + a_n. \tag{1}$$

Wir wollen den Bau dieses $f_0(z)$ bestimmen.

Die a_i sind rationale Funktionen von x. Durch Multiplikation mit dem Hauptnenner kann man sie ganzrational machen und außerdem erreichen, daß man ein in bezug auf x primitives Polynom (vgl. § 21) erhält:

$$f(x, z) = b_0(x)z^n + b_1(x)z^{n-1} + \cdots + b_n(x).$$

Der Grad dieses irreduziblen Polynoms in x sei m, der Grad in z ist n.

Die Koeffizienten $a_i = \frac{b_i}{b_0}$ von (1) können nicht sämtlich von x unabhängig sein, da sonst x algebraisch in bezug auf Δ wäre, es muß also einer unter ihnen, etwa

$$\Theta = a_i = \frac{b_i(x)}{b_0(x)}$$

oder, unverkürzbar geschrieben,

$$\Theta = \frac{g(x)}{h(x)}$$

von x wirklich abhängen. Die Grade von $g(x)$ und $h(x)$ sind $\leqq m$. Das (nichtverschwindende) Polynom

$$g(z) - \Theta h(z) = g(z) - \frac{g(x)}{h(x)} h(z)$$

hat die Nullstelle $z = x$, ist also in $\Sigma[z]$ durch $f_0(z)$ teilbar. Geht man nach § 21 von diesen in x rationalen Polynomen zu ganzrationalen und in x primitiven Polynomen über, so bleibt diese Teilbarkeit bestehen, und man erhält

$$h(x)\, g(z) - g(x)\, h(z) = q(x, z)\, f(x, z).$$

In x hat die linke Seite einen Grad $\leqq m$. Auf der rechten hat aber f schon den Grad m; also folgt, daß der Grad auf der linken Seite genau m ist und daß $q(x, z)$ nicht von x abhängt. Einen von z allein abhängigen Faktor hat aber die linke Seite nicht (siehe oben); also ist $q(x, z)$ eine Konstante:

$$h(x)\, g(z) - g(x)\, h(z) = q \cdot f(x, z).$$

Damit ist, da es auf die Konstante q nicht ankommt, der Bau von $f(x, z)$ bestimmt. Der Grad von $f(x, z)$ in x ist m; also ist (aus Symmetriegründen) der Grad in z auch m, mithin $m = n$. Mindestens eine der Gradzahlen von $g(x)$ und $h(x)$ muß den Höchstwert m wirklich erreichen; also hat auch Θ als Funktion von x genau den Grad m.

Demnach ist einerseits

$$(\Delta(x)/\Delta(\Theta)) = m,$$

andrerseits

$$(\Delta(x)/\Sigma) = m,$$

mithin, da Σ ja $\Delta(\Theta)$ umfaßt:

$$(\Sigma/\Delta(\Theta)) = 1,$$

$$\Sigma = \Delta(\Theta), \qquad \text{q. e. d.}$$

Der Lürothsche Satz hat die folgende Bedeutung für die Geometrie:

Eine ebene (irreduzible) algebraische Kurve $F(\xi, \eta) = 0$ heißt *rational*, wenn ihre Punkte bis auf endlichviele dargestellt werden können durch rationale Parametergleichungen:

$$\xi = f(t),$$
$$\eta = g(t).$$

Es kann nun vorkommen, daß jeder Kurvenpunkt (vielleicht mit endlichvielen Ausnahmen) zu mehreren Werten von t gehört. (Beispiel:

$$\xi = t^2,$$
$$\eta = t^2 + 1;$$

zu t und $-t$ gehört der gleiche Punkt.) Zufolge des Lürothschen Satzes kann man das aber immer durch geschickte Parameterwahl vermeiden. Es sei nämlich Δ ein Körper, der die Koeffizienten der Funktionen f, g enthält, und t zunächst eine Unbestimmte. $\Sigma = \Delta(f, g)$ ist ein Unterkörper von $\Delta(t)$. Ist t' ein primitives Element von Σ, so ist etwa

$$f(t) = f_1(t') \qquad \text{(rational)},$$
$$g(t) = g_1(t') \qquad \text{(rational)},$$
$$t' = \varphi(f, g) = \varphi(\xi, \eta),$$

und man verifiziert leicht, daß die neue Parameterdarstellung

$$\xi = f_1(t'),$$
$$\eta = g_1(t')$$

die gleiche Kurve darstellt, während der Nenner der Funktion $\varphi(x, y)$ nur in endlichvielen Punkten der Kurve verschwindet, so daß zu allen Kurvenpunkten (bis auf endlichviele) nur *ein* t'-Wert gehört.

Aufgabe. Ist der Körper $\Delta(x)$ Galoissch in bezug auf den Unterkörper $\Delta(\eta)$, so zerfällt das Polynom (1) in ihm in Linearfaktoren. Alle diese Linearfaktoren gehen durch gebrochen-lineare Transformationen von x aus einem unter ihnen, etwa aus $z - x$ hervor. Diese linearen Transformationen bilden eine endliche Gruppe, lassen die Funktion $\eta = \frac{g(x)}{h(x)}$ invariant und sind dadurch gekennzeichnet.

§ 37. Die Ausführung der körpertheoretischen Operationen in endlichvielen Schritten.

Wir haben in diesem Kapitel verschiedene Existenzbeweise von Körpern geführt: Existenz des rationalen Funktionenkörpers $\Delta(x, y, \ldots)$, der einfachen algebraischen Erweiterungen $\Delta(\Theta)$ (wo Θ einer vorgegebenen irreduziblen Gleichung genügt), Existenz des Zerfällungskörpers $\Delta(\alpha_1, \ldots, \alpha_n)$ eines Polynoms $f(x)$. Es fragt sich nun, ob sich alle diese Körper auch explizit rechnerisch konstruieren lassen.

Wir nennen einen Körper Δ *„explizit gegeben"*, wenn die Elemente von Δ eindeutig durch wohlunterscheidbare Symbole dargestellt sind, mit denen man die Addition, die Multiplikation, die Subtraktion und die Division in endlichvielen Rechenoperationen ausführen kann.

Wir zeigen nun zunächst:

Wenn der kommutative Körper Δ explizit gegeben ist, so ist auch jede einfache transzendente Erweiterung $\Delta(t)$ sowie jede einfache algebraische Erweiterung $\Delta(\Theta)$, deren definierende Gleichung $\varphi = 0$, die natürlich irreduzibel sein muß, bekannt ist, explizit gegeben.

Beweis. Die Elemente von $\Delta(t)$ sind Quotienten $\frac{f(t)}{g(t)}$, $g(t) \neq 0$, deren Rechnungsregeln im § 12 schon aufgestellt wurden. Um Eindeu-

tigkeit der Darstellung zu erzwingen, kann man noch verlangen, daß f und g teilerfremd sind und der Anfangskoeffizient von $g(t)$ gleich Eins ist. Bei gegebenem f und g läßt sich die Auffindung des größten gemeinsamen Teilers und damit auch die Reduktion auf die teilerfremde Form mittels des euklidischen Algorithmus (§ 16, Aufg. 2) tatsächlich explizit ausführen.

Im Fall $\Delta(\Theta)$ lassen sich die Körperelemente eindeutig durch Ausdrücke $a_0 + a_1\Theta + \cdots + a_{n-1}\Theta^{n-1}$ darstellen, und mit diesen Ausdrücken wird gerechnet wie mit Polynomen, nur daß zum Schluß immer das Ergebnis auf den kleinsten Rest modulo φ reduziert wird (§ 27). Wie man die Division zweier solcher Ausdrücke auszuführen hat, wurde im § 17 schon angegeben (Lösung der Gleichung $\bar{a}\,\bar{x} = \bar{b}$ im Restklassenring nach einem Primelement).

Wenn man versucht, in ähnlicher Weise mit den Methoden des § 29 den Zerfällungskörper eines Polynoms $f(x)$ zu konstruieren, so stößt man auf das Problem der Faktorzerlegung eines Polynoms in einem gegebenen oder schon konstruierten Körper. Man hat kein allgemeines Mittel, für jeden explizit-bekannten Körper K die Primfaktorzerlegung der Polynome aus $\mathsf{K}[z]$ in endlichvielen Schritten auszuführen, und es gibt Gründe für die Annahme, daß eine solche allgemeine Methode überhaupt unmöglich ist[1]. Wohl aber haben wir gesehen, daß es für besondere Körper (Körper der rationalen Zahlen, der Gaußschen Zahlen, der rationalzahligen rationalen Funktionen von n Unbestimmten, der Restklassen modulo p, usw.) solche Methoden der Primfaktorzerlegung gibt. Wir werden nun zeigen:

1. *Wenn im Körper Δ die Zerlegung der Polynome einer Unbestimmten in endlichvielen Schritten ausführbar ist, so auch die der Polynome in n Unbestimmten.*

2. *Wenn im Körper Δ die Zerlegung der Polynome (in einer oder mehreren Unbestimmten) in endlichvielen Schritten ausführbar ist, so gilt dasselbe für jede einfache transzendente Erweiterung $\Delta(t)$ und für jede separable einfache algebraische Erweiterung $\Delta(\Theta)$, deren definierende Gleichung $\varphi(\Theta) = 0$ bekannt ist.*

Der Beweis von 1. beruht auf einem Kunstgriff von KRONECKER. Ist das Polynom $f(x_1, \ldots, x_n)$ gegeben, so wähle man eine Zahl m größer als der Grad des Polynoms und mache die Substitution

$$x_\nu = t^{m^{\nu-1}}.$$

Dabei geht ein Glied $a_\varrho x_1^{\varrho_1} x_2^{\varrho_2} \ldots x_n^{\varrho_n}$ über in $a_\varrho t^{\varrho_1 + \varrho_2 m + \cdots + \varrho_n m^{n-1}}$, also verschiedene Potenzprodukte der x in verschiedene Potenzen von t (denn es läßt sich jede ganze Zahl nur in höchstens einer Weise in

[1] Siehe B. L. VAN DER WAERDEN: Eine Bemerkung über die Unzerlegbarkeit von Polynomen. Math. Ann. Bd. 102, S. 738. 1930.

der Gestalt $\varrho_1 + \varrho_2 m + \cdots + \varrho_n m^{n-1}$ mit $0 \leqq \varrho_\nu < m$ schreiben). Wenn nun das vorgelegte Polynom $f(x_1, \ldots)$ sich zerlegen läßt:

$$f = g_1 g_2,$$

so gilt die Zerlegung auch nach der obigen Substitution; sie möge dann in

$$f^*(t) = g_1^*(t)\, g_2^*(t)$$

übergehen. Man kann dann aus den Polynomen g_1^*, g_2^* die ursprünglichen g_1, g_2 zurückgewinnen, da ja jedem Glied in g_ν^* nur ein Glied in g_ν entsprechen kann. Also zerlege man $f^*(t)$ in *allen möglichen* Weisen in zwei Faktoren (das geht, wenn man die Zerlegung in Primfaktoren kennt) und untersuche jedesmal, welche Polynome g_1, g_2 zu den gefundenen Faktoren g_1^*, g_2^* gehören können. Jedesmal kann man dann nachprüfen, ob mit diesen g_1, g_2 die Gleichung

$$f = g_1 g_2$$

stimmt. Tut sie das nie, so ist f unzerlegbar; tut sie es, so untersuche man g_1 und g_2 in derselben Weise wie vorhin f, bis man nach höchstens m Schritten die vollständige Zerlegung von f in Primfaktoren gefunden hat.

Der *Beweis von* 2. ist ganz einfach in dem Fall einer transzendenten Erweiterung $\Delta(t)$. Ein jedes Polynom $f(t, z)$ in $\Delta(t)[z]$ ist durch Multiplikation mit einem Polynom in t allein ganzrational in t zu machen, und nach § 21 entspricht dann jeder in t rationalen Zerlegung von $f(t, z)$ eine ganzrationale Zerlegung und umgekehrt. Damit ist alles auf die Polynomzerlegung in $\Delta[t, z]$ zurückgeführt.

Im Fall einer algebraischen Erweiterung $\Delta(\Theta)$, wo Θ einer separablen irreduziblen Gleichung $\varphi(\Theta) = 0$ genügt, ist die Sache nicht so einfach. Es sei ein Polynom $f(\Theta, z)$ in $\Delta(\Theta)[z]$ vorgelegt. Man bilde mit einer Unbestimmten u das Polynom $f(\Theta, z - u\Theta)$, bilde dessen Norm $F(z, u)$ nach § 35 und zerlege $F(z, u)$ in $\Delta[z, u]$ in unzerlegbare Faktoren:

$$N f(\Theta, z - u\Theta) = F(z, u) = F_1(z, u) \cdot F_2(z, u) \cdots F_r(z, u).$$

Schließlich bilde man den größten gemeinsamen Teiler von $f(\Theta, z - u\Theta)$ und jedem $F_\nu(z, u)$ in $\Delta(\Theta)[z, u]$. Wir werden beweisen, daß diese Teiler für $u = 0$ gerade die irreduziblen Faktoren von $f(\Theta, z)$ ergeben.

Es sei also

$$f(\Theta, z) = f_1(\Theta, z) \cdot f_2(\Theta, z) \cdots f_k(\Theta, z)$$

die Zerlegung von f in irreduzible Faktoren in $\Delta(\Theta)[z]$. Dann folgt

$$f(\Theta, z - u\Theta) = f_1(\Theta, z - u\Theta) \cdots f_k(\Theta, z - u\Theta)$$
$$F(z, u) = N f(\Theta, z - u\Theta) = N f_1(\Theta, z - u\Theta) \cdots N f_k(\Theta, z - u\Theta).$$

Die Polynome $f(\Theta, z - u\Theta)$ und $Nf_1(\Theta, z - u\Theta)$ haben in $\Delta(\Theta)[z, u]$ den Faktor $f_1(\Theta, z - u\Theta)$ gemein. Die restlichen Faktoren

$$\frac{f(\Theta, z - u\Theta)}{f_1(\Theta, z - u\Theta)} = f_2(\Theta, z - u\Theta) \cdots f_k(\Theta, z - u\Theta)$$

und

$$\frac{Nf_1(\Theta, z - u\Theta)}{f_1(\Theta, z - u\Theta)} = \Pi' f_1(\Theta_\nu, z - u\Theta_\nu),$$

(wo der Strich am Produktzeichen bedeutet, daß über alle konjugierten Θ_ν außer Θ selbst das Produkt gebildet wird) haben keinen Faktor gemein, denn hätten sie etwa den irreduziblen Faktor $f_2(\Theta, z - u\Theta)$ gemein, so hätte man:

$$\Pi' f_1(\Theta_\nu, z - u\Theta_\nu) = g(\Theta, z, u) f_2(\Theta, z - u\Theta)$$

und der Vergleich der Glieder höchsten Grades in z und u links und rechts würde ergeben:

$$\Pi'(z - u\Theta_\nu)^{m_1} = h(\Theta, z, u) \cdot (z - u\Theta)^{m_2},$$

was ein Unsinn ist, denn keiner der Linearfaktoren $z - u\Theta_\nu$ enthält den Linearfaktor $z - u\Theta$.

Demnach ist $f_1(\Theta, z - u\Theta)$ in der Tat der größte gemeinsame Teiler von $f(\Theta, z - u\Theta)$ und $Nf_1(\Theta, z - u\Theta)$, also von $f(\Theta, z - u\Theta)$ und einem in bezug auf Δ rationalen Faktor von $F(z, u)$.

Wenn nun ein Körper Δ sukzessiv erweitert wird durch Adjunktion von (transzendenten oder separablen algebraischen) Größen $\Theta_1, \Theta_2, \ldots, \Theta_h$, so kann man zufolge der obigen Sätze die Faktorzerlegung von Polynomen im Körper $\Delta(\Theta_1, \Theta_2, \ldots, \Theta_h)$ schrittweise auf die von Polynomen in Δ zurückführen.

Damit sind nun die Hilfsmittel gegeben, die nötig sind, um in den wichtigsten Fällen die Existenzbeweise dieses Kapitels konstruktiv zu verfolgen, z. B.: die Konstruktion des Zerfällungskörpers eines Polynoms $f(x)$, die des zugehörigen Galoisschen Körpers zu einem Körper $\Delta(\Theta_1, \ldots, \Theta_h)$, die des primitiven Elementes Θ, sowie die der Isomorphismen des Körpers $\Delta(\Theta_1, \ldots, \Theta_h) = \Delta(\Theta)$ im zugehörigen Galoisschen Körper.

Sechstes Kapitel.

Fortsetzung der Gruppentheorie.

Inhalt. In den §§ 38 bis 39 wird eine Erweiterung des Gruppenbegriffs besprochen. §§ 40 bis 42 enthalten wichtige allgemeine Sätze über Normalteiler und „Kompositionsreihen", während §§ 43 bis 44 speziellere Sätze über Permutationsgruppen enthalten, die nur in der Theorie von GALOIS nachher gebraucht werden.

§ 38. Gruppen mit Operatoren.

In diesem Paragraphen soll der Gruppenbegriff erweitert werden, wodurch alle folgenden Untersuchungen eine größere Allgemeinheit erhalten, die für spätere Anwendungen (Kap. 5 bis 17) nötig ist. Derjenige Leser, der sich im Augenblick nur für die Galoissche Theorie interessiert, kann diesen und den nächsten Paragraphen ruhig übergehen; er möge bei den folgenden Paragraphen an (etwa endliche) Gruppen im bisher betrachteten Sinn denken.

Es sei gegeben: *erstens* eine Gruppe (im gewöhnlichen Sinn) $\mathfrak{G}$, mit Elementen $a, b, \ldots$; *zweitens* eine Menge Ω von neuen Symbolen $\eta, \Theta, \ldots$, die wir *Operatoren* nennen. Zu jedem Θ und jedem a sei ein Produkt Θa („der Operator Θ angewandt auf das Gruppenelement a") definiert; dieses Produkt gehöre wieder der Gruppe $\mathfrak{G}$ an. Weiter wird angenommen, daß jeder einzelne Operator Θ „distributiv" ist, d. h. daß

$$\Theta(ab) = \Theta a \cdot \Theta b \tag{1}$$

ist. Anders ausgedrückt: Die „Multiplikation" mit dem Operator Θ soll ein Homomorphismus sein, der die Gruppe $\mathfrak{G}$ auf eine Untergruppe (möglicherweise auf $\mathfrak{G}$ selbst) abbildet[1]. Sind alle diese Bedingungen erfüllt, so nennt man $\mathfrak{G}$ eine *Gruppe mit Operatoren*, Ω den *Operatorenbereich*.

Eine *zulässige Untergruppe* von $\mathfrak{G}$ (in bezug auf den Operatorenbereich Ω) soll eine solche Untergruppe $\mathfrak{H}$ sein, die wieder die Operatoren von Ω gestattet; das heißt: wenn a zu $\mathfrak{H}$ gehört, so soll auch jedes Θa zu $\mathfrak{H}$ gehören. Ist die zulässige Untergruppe zugleich Normalteiler, so spricht man von einem zulässigen Normalteiler.

Beispiele. 1. Die Operatoren seien die inneren Automorphismen von $\mathfrak{G}$:

$$\Theta a = c\,a\,c^{-1}.$$

Zulässig sind diejenigen Untergruppen, die mit jedem a auch jedes cac^{-1} enthalten, d. h. die Normalteiler.

2. Die Operatoren seien die sämtlichen A = Automorphismen von $\mathfrak{G}$. Zulässig sind diejenigen Untergruppen, die bei jedem A = Automorphismus in sich übergehen; man nennt sie *charakteristische Untergruppen*.

3. $\mathfrak{G}$ sei ein Ring, aufgefaßt als Gruppe gegenüber der Addition. Der Operatorenbereich Ω sei derselbe Ring; das Produkt Θa sei einfach das Ringprodukt. Alsdann ist (1) das gewöhnliche Distributivgesetz:

$$r(a + b) = r\,a + r\,b.$$

Zulässige Untergruppen sind die *Linksideale*, d. h. diejenigen Untergruppen, die mit jedem a auch alle ra enthalten.

[1] Daraus folgt, daß bei der „Multiplikation" mit Θ das Einselement in das Einselement, Inverses in Inverses übergeht.

4. Es kann unter Umständen von Vorteil sein, die Operatoren Θ rechts von den Gruppenelementen zu schreiben, also $a\Theta$ statt Θa zu schreiben. Dann lautet (1):

$$(a\,b)\,\Theta = a\,\Theta \cdot b\,\Theta .$$

Faßt man z. B. die Elemente eines (als Gruppe mit dem Verknüpfungsgesetz der Addition gedachten) Rings als derartige Rechtsoperatoren auf, wobei $a\Theta$ wiederum das Ringprodukt sein soll, so erhält man als zulässige Untergruppen die *Rechtsideale.*

5. Schließlich kann man einen Teil der Operatoren links, einen anderen Teil rechts schreiben. Nimmt man z. B. zu einem Ring als Operatoren sowohl die als Linksmultiplikatoren betrachteten Elemente des Ringes als auch dieselben Elemente als Rechtsmultiplikatoren, so erhält man als zulässige Untergruppen die *zweiseitigen Ideale.*

6. Als *Modul* bezeichnet man, wie gesagt, jede additiv geschriebene Abelsche Gruppe. Auch ein Modul kann einen Operatorenbereich haben; dieser heißt hier auch *Multiplikatorenbereich.* Es gilt dann

$$\Theta\,(a + b) = \Theta\,a + \Theta\,b .$$

Meist nimmt man an, der Multiplikatorenbereich sei ein *Ring* und es sei

$$(2) \qquad \begin{cases} (\eta + \Theta)\,a = \eta\,a + \Theta\,a , \\ (\eta\Theta)\,a = \eta\,(\Theta\,a) \end{cases}$$

(bzw., wenn die Multiplikatoren rechts geschrieben werden, $a(\eta\Theta) = (a\eta)\Theta$). Es folgt dann $(\eta - \Theta)\,a = \eta a - \Theta a$ und $0 \cdot a = 0$ (die erste Null ist das Nullelement des Ringes, die zweite das Nullelement des Moduls). Ist $\mathfrak{o}$ der Ring, so spricht man von $\mathfrak{o}$-*Moduln* oder *Moduln in bezug auf den Ring* $\mathfrak{o}$. Wenn der Ring ein Einselement ε hat, so nimmt man sehr oft an, das Einselement sei zugleich „Einheitsoperator"; d. h. es sei $\varepsilon \cdot a = a$ für alle a aus $\mathfrak{G}$.

7. Jeder Modul gestattet als Operatoren die gewöhnlichen ganzen Zahlen n im Sinne einer gewöhnlichen Multiplikation; denn es ist

$$n\,(a + b) = n\,a + n\,b .$$

Alle Untermoduln sind dabei zulässig.

8. Die Gesamtheit aller Homomorphismen einer Abelschen Gruppe (eines Moduls) in sich (d. h. aller homomorphen Abbildungen auf sich selbst oder auf echte Teilmengen) ist ein Operatorenbereich, der als Ring aufgefaßt werden kann, wenn man die Summe und das Produkt zweier Homomorphismen durch die Formeln (2) (in denen das Pluszeichen rechts die Verknüpfung der Gruppenelemente andeutet) definiert. Dieser Ring heißt der *Automorphismenring*[1] der Abelschen Gruppe.

[1] Mit „Automorphismen" sind also in diesem Fall nicht nur 1-Automorphismen gemeint, sondern alle homomorphen Abbildungen auf Teilmengen.

Aus diesen Beispielen ist ersichtlich, wie weit das Anwendungsgebiet der Gruppen mit Operatoren reicht. Hinsichtlich weiterer Beispiele siehe das Kapitel „Lineare Algebra" (Band II).

Aufgaben. 1. Der Durchschnitt zweier zulässiger Untergruppen ist wieder eine zulässige Untergruppe. Das Entsprechende gilt für zulässige Normalteiler.

2. Das Produkt aus einer zulässigen Untergruppe $\mathfrak{A}$ und einem zulässigen Normalteiler $\mathfrak{N}$, d. h. die Menge aller Produkte $a \cdot b$, wo a zu $\mathfrak{A}$ und b zu $\mathfrak{N}$ gehört, ist wieder eine zulässige Untergruppe, und zwar die kleinste, welche $\mathfrak{A}$ und $\mathfrak{N}$ umfaßt.

Bemerkung: Bei Moduln, wo automatisch jede Untergruppe Normalteiler ist und wo man natürlich Summe statt Produkt sagt, ergibt die letzte Aufgabe den Satz: Die Summe oder das Erzeugnis zweier zulässiger Untermoduln $\mathfrak{A}$ und $\mathfrak{N}$ ist wieder ein zulässiger Untermodul. Man bezeichnet diese Modulsumme mit $(\mathfrak{A}, \mathfrak{N})$, wie bei den Idealen (§ 15).

§ 39. Operatorisomorphismus und -homomorphismus.

Sind $\mathfrak{G}$ und $\overline{\mathfrak{G}}$ Gruppen mit demselben Operatorenbereich Ω und ist eine Abbildung von $\mathfrak{G}$ auf eine Untermenge von $\overline{\mathfrak{G}}$ gegeben, wobei jedem a ein $\bar{a}$ entspricht und wobei einem Produkt ab das Produkt $\bar{a}\bar{b}$ und einem Θa das zugehörige $\Theta \bar{a}$ entspricht, so heißt die Abbildung ein *Operatorhomomorphismus*. Ist die Bildmenge die ganze Gruppe $\overline{\mathfrak{G}}$, d. h. gehört jedes Element von $\overline{\mathfrak{G}}$ zu mindestens einem Element von $\mathfrak{G}$, so hat man eine homomorphe Abbildung von $\mathfrak{G}$ *auf* $\overline{\mathfrak{G}}$, im allgemeinen Falle dagegen eine homomorphe Abbildung von $\mathfrak{G}$ *in* $\overline{\mathfrak{G}}$. Entspricht jedem $\bar{a}$ genau ein a, so hat man einen 1-*Operatorisomorphismus*.

Zeichen: $\mathfrak{G} \sim \overline{\mathfrak{G}}$ für Operatorhomomorphismus, $\mathfrak{G} \cong \overline{\mathfrak{G}}$ für 1-Operatorisomorphismus.

Ist $\mathfrak{N}$ ein zulässiger Normalteiler von $\mathfrak{G}$, so gehen die Elemente an einer Nebenklasse $\bar{a} = a\mathfrak{N}$ bei Anwendung des Operators Θ in $\Theta a \cdot \Theta n$, also in Elemente der Nebenklasse $\Theta a \cdot \mathfrak{N}$ über. Diese Nebenklasse $\overline{\Theta a}$ nennen wir das Produkt des Operators Θ mit der Nebenklasse $\bar{a}$. *Dadurch wird die Faktorgruppe $\mathfrak{G}/\mathfrak{N}$ zu einer Gruppe mit demselben Operatorenbereich Ω, und zwar ist die Zuordnung $a \to \bar{a}$ ein Operatorhomomorphismus.*

Gehen wir umgekehrt von einem Operatorhomomorphismus aus, so erhalten wir wie in § 9 den *Homomorphiesatz*:

Ist $\mathfrak{G} \sim \overline{\mathfrak{G}}$, so ist die Menge $\mathfrak{N}$ der Elemente von $\mathfrak{G}$, denen das Einheitselement von $\overline{\mathfrak{G}}$ entspricht, ein zulässiger Normalteiler in $\mathfrak{G}$, und den

Nebenklassen von $\mathfrak{N}$ *entsprechen ein-eindeutig und operatorisomorph die Elemente von* $\overline{\mathfrak{G}}$:

$$\mathfrak{G}/\mathfrak{N} \simeq \overline{\mathfrak{G}}\,.$$

Daß $\mathfrak{N}$ ein Normalteiler ist, wissen wir schon aus § 9. Daß $\mathfrak{N}$ zulässig ist, ist klar; denn wenn a auf das Einselement $\bar{e}$ abgebildet wird, wird Θa auf $\Theta\bar{e} = \bar{e}$ abgebildet, d. h. mit a gehört auch Θa zu $\mathfrak{N}$. Daß die Zuordnung der Nebenklassen zu den Elementen von $\overline{\mathfrak{G}}$ ein-eindeutig ist, wissen wir schon; daß sie ein Operatorisomorphismus ist, folgt daraus, daß die gegebene Zuordnung $\mathfrak{G} \to \overline{\mathfrak{G}}$ ein Operatorhomomorphismus war.

Bei additiv geschriebenen Gruppen mit Operatorenbereich $\mathfrak{o}$ ($\mathfrak{o}$-Moduln, speziell Ideale in $\mathfrak{o}$) heißt der Operatorhomomorphismus auch *Modulhomomorphismus*. Man beachte, daß bei einem solchen wieder Θa in $\Theta\bar{a}$ übergeht, also daß Θ untransformiert bleibt; das ist der Unterschied zwischen dem Modulhomomorphismus und dem Ringhomomorphismus, bei dem ab in $\bar{a}\bar{b}$ übergeht. Nehmen wir ein Beispiel: Zwei Linksideale aus einem Ring $\mathfrak{o}$ können als $\mathfrak{o}$-Moduln aufgefaßt werden; ein Operatorhomomorphismus ordnet dann jedem a ein $\bar{a}$ und dem Produkt ra das Produkt $r\bar{a}$ zu (für r aus $\mathfrak{o}$). Sie können aber auch als Ringe aufgefaßt werden; ein Ringhomomorphismus ordnet dem Produkt ra (r im Ideal) nicht $r\bar{a}$, sondern $\bar{r}\bar{a}$ zu.

Wo immer im folgenden von „Gruppen" schlechthin die Rede ist, sind auch Gruppen mit Operatoren einbegriffen. Mit „Untergruppen" und „Normalteiler" sind dann stillschweigend immer zulässige Untergruppen und Normalteiler, mit „Iso-" und „Homomorphismen" immer Operatoriso- und -homomorphismen gemeint. Benutzt werden in den beiden nächsten Paragraphen ausschließlich der Homomorphiesatz und die Tatsachen, daß der Durchschnitt zweier (zulässigen) Untergruppen wieder eine solche, das Produkt aus einem Normalteiler und einer Untergruppe wieder eine (zulässige) Untergruppe ist.

Aufgaben. 1. Die Ideale (1) und (2) im Ring der ganzen Zahlen sind modulisomorph, aber nicht ringisomorph.

2. Im Ring der Zahlenpaare (a_1, a_2) (§ 10, Aufg. 1) sind die durch $(1, 0)$ und $(0, 1)$ erzeugten Ideale ringisomorph, aber nicht operatorisomorph.

§ 40. Die beiden Isomorphiesätze.

Beim Homomorphismus $\mathfrak{G} \sim \overline{\mathfrak{G}} = \mathfrak{G}/\mathfrak{N}$ wird jede Untergruppe $\mathfrak{H}$ von $\mathfrak{G}$ auf eine Untergruppe $\overline{\mathfrak{H}}$ von $\overline{\mathfrak{G}}$ homomorph abgebildet. Geht man nun von $\overline{\mathfrak{H}}$ wieder zurück und sucht in $\mathfrak{G}$ die Gesamtheit $\mathfrak{K}$ derjenigen Elemente, deren Bildelemente (oder Nebenklassen) zu $\overline{\mathfrak{H}}$ ge-

hören, so kann $\mathfrak{K}$ unter Umständen mehr Elemente als die von $\mathfrak{H}$ umfassen. Denn $\mathfrak{K}$ enthält neben jedem a aus $\mathfrak{H}$ auch alle Elemente der Nebenklasse $a\mathfrak{N}$. Bezeichnet man mit $\mathfrak{H}\mathfrak{N}$ die Gruppe, die besteht aus allen Produkten ab von einem a aus $\mathfrak{H}$ mit einem b aus $\mathfrak{N}$ (vgl. Aufg. 2, § 38), so folgt $\mathfrak{K} = \mathfrak{H}\mathfrak{N}$ und weiter $\overline{\mathfrak{H}} = \mathfrak{H}\mathfrak{N}/\mathfrak{N}$. Andererseits ist $\mathfrak{H}$ auf $\overline{\mathfrak{H}}$ homomorph abgebildet, also $\overline{\mathfrak{H}}$ isomorph der Faktorgruppe von $\mathfrak{H}$ nach einem Normalteiler von $\mathfrak{H}$, der aus denjenigen Elementen von $\mathfrak{H}$ besteht, denen das Einheitselement entspricht, d. h. aus denjenigen Elementen von $\mathfrak{H}$, die zugleich zu $\mathfrak{N}$ gehören. Daraus ergibt sich der *erste Isomorphiesatz*:

Ist $\mathfrak{N}$ Normalteiler in $\mathfrak{G}$ und ist $\mathfrak{H}$ Untergruppe von $\mathfrak{G}$, so ist der Durchschnitt $\mathfrak{H} \cap \mathfrak{N}$ Normalteiler in $\mathfrak{H}$, und es ist

$$\mathfrak{H}\mathfrak{N}/\mathfrak{N} \cong \mathfrak{H}/(\mathfrak{H} \cap \mathfrak{N}).^1$$

Dann und nur dann wird die Gesamtheit der Elemente, die auf $\overline{\mathfrak{H}}$ abgebildet werden, wieder genau $\mathfrak{H}$ sein, wenn $\mathfrak{H}$ zu jedem a auch die ganze Nebenklasse $a\mathfrak{N}$ enthält, d. h. wenn

$$\mathfrak{H} > \mathfrak{N}.^2$$

Diesen Gruppen $\mathfrak{H} > \mathfrak{N}$ entsprechen mithin ein-eindeutig gewisse Gruppen $\overline{\mathfrak{H}} = \mathfrak{H}/\mathfrak{N}$ in $\overline{\mathfrak{G}}$. Auch ergibt *jede* Untergruppe $\overline{\mathfrak{H}}$ von $\overline{\mathfrak{G}}$ eine Untergruppe $\mathfrak{H} > \mathfrak{N}$, bestehend aus allen Elementen aller in $\overline{\mathfrak{H}}$ vorkommenden Nebenklassen von $\mathfrak{N}$. Schließlich entsprechen den Rechts- und Linksnebenklassen von $\overline{\mathfrak{H}}$ in $\overline{\mathfrak{G}}$ die Rechts- bzw. Linksnebenklassen von $\mathfrak{H}$ in $\mathfrak{G}$. Ist also $\overline{\mathfrak{H}}$ Normalteiler in $\overline{\mathfrak{G}}$, so ist auch $\mathfrak{H}$ Normalteiler in $\mathfrak{G}$ und umgekehrt. Dieses ergibt sich auf anderem Wege auch beim Beweis des *zweiten Isomorphiesatzes*:

Ist $\overline{\mathfrak{G}} = \mathfrak{G}/\mathfrak{N}$, $\overline{\mathfrak{H}}$ Normalteiler in $\overline{\mathfrak{G}}$, so ist die zugehörige Untergruppe $\mathfrak{H}$ Normalteiler in $\mathfrak{G}$, und es ist

$$\mathfrak{G}/\mathfrak{H} \cong \overline{\mathfrak{G}}/\overline{\mathfrak{H}}. \tag{1}$$

Beweis: Es ist $\mathfrak{G} \sim \overline{\mathfrak{G}}$ und $\overline{\mathfrak{G}} \sim \overline{\mathfrak{G}}/\overline{\mathfrak{H}}$, also $\mathfrak{G} \sim \overline{\mathfrak{G}}/\overline{\mathfrak{H}}$, also $\overline{\mathfrak{G}}/\overline{\mathfrak{H}}$ isomorph der Faktorgruppe von $\mathfrak{G}$ nach dem Normalteiler, der aus denjenigen Elementen von $\mathfrak{G}$ besteht, denen beim Homomorphismus $\mathfrak{G} \sim \overline{\mathfrak{G}}/\overline{\mathfrak{H}}$ das Einheitselement, d. h. beim ersten Homomorphismus $\mathfrak{G} \sim \overline{\mathfrak{G}}$ ein Element von $\overline{\mathfrak{H}}$ zugeordnet wird. Dieser Normalteiler ist $\mathfrak{H}$, q. e. d.

Die 1-Isomorphie (1) läßt sich auch so schreiben:

$$\mathfrak{G}/\mathfrak{H} \cong (\mathfrak{G}/\mathfrak{N})/(\mathfrak{H}/\mathfrak{N}).$$

---

[1] Bei Moduln hat man natürlich $(\mathfrak{H}, \mathfrak{N})$ statt $\mathfrak{H}\mathfrak{N}$ zu schreiben.

[2] In diesem Kapitel verwenden wir einfachheitshalber für „ist enthalten in" und „umfaßt" die Zeichen $<$ und $>$ (statt $\leq$ und $\geq$).

Aufgaben. 1. Man zeige mit Hilfe des ersten Isomorphiesatzes, daß die Faktorgruppe der symmetrischen Gruppe $\mathfrak{S}_4$ nach der Vierergruppe $\mathfrak{B}_4$ (§ 8, Aufg. 4) isomorph der symmetrischen Gruppe $\mathfrak{S}_3$ ist.

2. Ebenso, daß in jeder Permutationsgruppe, die nicht aus lauter geraden Permutationen besteht, die geraden Permutationen einen Normalteiler vom Index 2 bilden.

3. Ebenso, daß die Faktorgruppe der euklidischen Bewegungsgruppe nach dem Normalteiler der Translationen isomorph der Gruppe der Drehungen um einen Punkt ist.

§ 41. Normalreihen und Kompositionsreihen.

Eine Gruppe $\mathfrak{G}$ heißt *einfach*, wenn sie außer sich selbst und der Einheitsgruppe keinen Normalteiler besitzt.

Beispiele: Die Gruppen von Primzahlordnung sind einfach, weil die Ordnung einer Untergruppe ein Teiler der Ordnung der Gesamtgruppe sein müßte, so daß außer dieser und der Einheitsgruppe überhaupt keine Untergruppe, also auch kein Normalteiler existiert. Es wird später gezeigt werden, daß auch die alternierende Gruppe $\mathfrak{A}_n$ für $n \neq 4$ einfach ist (§ 43); weiter jeder eingliedrige Modul in bezug auf einen Körper als Multiplikatorenbereich, usw.

Eine endliche Reihe von Untergruppen einer Gruppe $\mathfrak{G}$:

$$\{\mathfrak{G} = \mathfrak{G}_0 \supset \mathfrak{G}_1 \supset \cdots \supset \mathfrak{G}_l = \mathfrak{E}\}, \tag{1}$$

heißt *Normalreihe*, wenn für $\nu = 1, \ldots, l$ jedes $\mathfrak{G}_\nu$ Normalteiler in $\mathfrak{G}_{\nu-1}$ ist. Die Zahl l heißt die *Länge* der Normalreihe; die Faktorgruppen $\mathfrak{G}_{\nu-1}/\mathfrak{G}_\nu$ heißen die *Faktoren* der Normalreihe. Zu beachten: Die Länge ist nicht die Anzahl der Glieder der Reihe (1), sondern die Anzahl der Faktoren $\mathfrak{G}_{\nu-1}/\mathfrak{G}_\nu$.

Eine zweite Normalreihe

$$\{\mathfrak{G} \supset \mathfrak{H}_1 \supset \cdots \supset \mathfrak{H}_m = \mathfrak{E}\} \tag{2}$$

heißt eine *Verfeinerung* der ersten, wenn alle $\mathfrak{G}_i$ aus (1) auch in (2) auftreten. Zum Beispiel ist für die Gruppe $\mathfrak{S}_4$ (§ 6) die Reihe

$$\{\mathfrak{S}_4 \supset \mathfrak{A}_4 \supset \mathfrak{B}_4 \supset \mathfrak{E}\}$$

(vgl. § 8, Aufg. 4) eine Verfeinerung von

$$\{\mathfrak{S}_4 \supset \mathfrak{B}_4 \supset \mathfrak{E}\}.$$

In einer Normalreihe kann ein Glied beliebig oft wiederholt werden: $\mathfrak{G}_i = \mathfrak{G}_{i+1} = \cdots = \mathfrak{G}_k$. Kommt das *nicht* vor, so spricht man von einer Reihe *ohne Wiederholungen*. Eine Reihe ohne Wiederholungen, die sich ohne Wiederholungen nicht mehr verfeinern läßt, heißt eine *Kompositionsreihe*. Zum Beispiel ist in der symmetrischen Gruppe $\mathfrak{S}_3$ die Reihe

$$\{\mathfrak{S}_3 \supset \mathfrak{A}_3 \supset \mathfrak{E}\}$$

eine Kompositionsreihe, ebenso in $\mathfrak{S}_4$ die Reihe

$$\{\mathfrak{S}_4 > \mathfrak{A}_4 > \mathfrak{B}_4 > \{1, (1\,2)(3\,4)\} > \mathfrak{E}\}.$$

In beiden Fällen schließt man die Unmöglichkeit einer weiteren Verfeinerung daraus, daß die Indizes der aufeinanderfolgenden Normalteiler in den jeweils vorangehenden sämtlich Primzahlen sind. Es gibt aber andere Gruppen, in denen jede Normalreihe sich weiter verfeinern läßt; solche Gruppen besitzen also keine Kompositionsreihe. Ein Beispiel bildet jede unendliche zyklische Gruppe; denn wenn in einer solchen eine Normalreihe ohne Wiederholungen

$$\{\mathfrak{G} > \mathfrak{G}_1 > \cdots > \mathfrak{G}_{l-1} > \mathfrak{E}\}$$

gegeben ist und $\mathfrak{G}_{l-1}$ etwa den Index m hat, also $\mathfrak{G}_{l-1} = \{a^m\}$ ist, so gibt es zwischen $\mathfrak{G}_{l-1}$ und $\mathfrak{E}$ immer noch eine Untergruppe $\{a^{2m}\}$ vom Index $2\,m$.

Eine Normalreihe ist dann und nur dann Kompositionsreihe, wenn sich zwischen je zwei aufeinanderfolgende Glieder $\mathfrak{G}_{\nu-1}$ und $\mathfrak{G}_\nu$ kein von diesen verschiedener Normalteiler von $\mathfrak{G}_{\nu-1}$ mehr einschieben läßt oder, was nach § 40 auf dasselbe hinauskommt, wenn $\mathfrak{G}_{\nu-1}/\mathfrak{G}_\nu$ einfach ist. Die einfachen Faktoren $\mathfrak{G}_{\nu-1}/\mathfrak{G}_\nu$ einer Kompositionsreihe heißen *Kompositionsfaktoren*. In den beiden oben angeführten Kompositionsreihen sind alle Kompositionsfaktoren zyklische Gruppen der Ordnungen 2, 3; resp. 2, 3, 2, 2.

Zwei Normalreihen heißen *isomorph*, wenn alle Faktoren $\mathfrak{G}_{\nu-1}/\mathfrak{G}_\nu$ der einen Reihe in irgend einer Reihenfolge den Faktoren der zweiten Reihe 1-isomorph sind. Zum Beispiel sind in einer zyklischen Gruppe $\{a\}$ von der Ordnung 6 die beiden Reihen

$$\{\{a\}, \{a^2\}, \mathfrak{E}\},$$
$$\{\{a\}, \{a^3\}, \mathfrak{E}\}$$

isomorph; denn die Faktoren der ersten Reihe sind zyklisch von den Ordnungen 2, 3, die der zweiten Reihe zyklisch von den Ordnungen 3, 2. — Für die Isomorphie von Normalreihen werden wir im folgenden der Bequemlichkeit halber ebenfalls das Zeichen $\cong$ verwenden.

Endigt eine Kette von Normalteilern

$$\{\mathfrak{G} > \mathfrak{G}_1 > \cdots\}$$

mit irgend einem Normalteiler $\mathfrak{A}$ von $\mathfrak{G}$, der nicht gleich $\mathfrak{E}$ zu sein braucht, so spricht man von einer *Normalreihe von* $\mathfrak{G}$ *nach* $\mathfrak{A}$; einer solchen entspricht eine Normalreihe

$$\{\mathfrak{G}/\mathfrak{A} > \mathfrak{G}_1/\mathfrak{A} > \cdots > \mathfrak{A}/\mathfrak{A} = \mathfrak{E}\}$$

der Faktorgruppe $\mathfrak{G}/\mathfrak{A}$, und umgekehrt. Die Faktoren der zweiten Reihe sind nach dem zweiten Isomorphiesatz isomorph denen der ersten.

Sind zwei Normalreihen

$$\{\mathfrak{G} \supset \mathfrak{G}_1 \supset \cdots \supset \mathfrak{G}_r = \mathfrak{E}\}$$

und

$$\{\mathfrak{G} \supset \mathfrak{H}_1 \supset \cdots \supset \mathfrak{H}_r = \mathfrak{E}\}$$

isomorph, so kann man zu jeder Verfeinerung der ersten eine dazu isomorphe Verfeinerung der zweiten finden. Denn jeder Faktor $\mathfrak{G}_{\nu-1}/\mathfrak{G}_\nu$ ist isomorph einem ganz bestimmten Faktor $\mathfrak{H}_{\mu-1}/\mathfrak{H}_\mu$; somit entspricht jeder Normalreihe für $\mathfrak{G}_{\nu-1}/\mathfrak{G}_\nu$ eine isomorphe Normalreihe für $\mathfrak{H}_{\mu-1}/\mathfrak{H}_\mu$ und daher auch jeder Normalreihe von $\mathfrak{G}_{\nu-1}$ nach $\mathfrak{G}_\nu$ eine isomorphe Reihe von $\mathfrak{H}_{\mu-1}$ nach $\mathfrak{H}_\mu$.

Wir können nun den folgenden, von O. SCHREIER herrührenden *Hauptsatz über Normalreihen* beweisen: *Zwei beliebige Normalreihen einer beliebigen Gruppe* $\mathfrak{G}$:

$$\{\mathfrak{G} \supset \mathfrak{G}_1 \supset \mathfrak{G}_2 \supset \cdots \supset \mathfrak{G}_r = \mathfrak{E}\},$$
$$\{\mathfrak{G} \supset \mathfrak{H}_1 \supset \mathfrak{H}_2 \supset \cdots \supset \mathfrak{H}_s = \mathfrak{E}\}$$

besitzen isomorphe Verfeinerungen:

$$\{\mathfrak{G} \supset \cdots \supset \mathfrak{G}_1 \supset \cdots \supset \mathfrak{G}_2 \supset \cdots \supset \mathfrak{E}\} \simeq \{\mathfrak{G} \supset \cdots \supset \mathfrak{H}_1 \supset \cdots \supset \mathfrak{H}_2 \supset \cdots \supset \mathfrak{E}\}.$$

Beweis. Für $r = 1$ oder $s = 1$ ist der Satz klar; denn dann lautet eine der Reihen $\{\mathfrak{G} \supset \mathfrak{E}\}$, und die andere ist ganz von selbst eine Verfeinerung davon.

Wir beweisen den Satz zunächst für $s = 2$ durch vollständige Induktion nach r, sodann für beliebige s durch vollständige Induktion nach s.

Für $s = 2$ lautet die zweite Reihe

$$\{\mathfrak{G} \supset \mathfrak{H} \supset \mathfrak{E}\}.$$

Wir setzen $\mathfrak{D} = \mathfrak{G}_1 \cap \mathfrak{H}$ und $\mathfrak{P} = \mathfrak{G}_1 \cdot \mathfrak{H}$; dann sind $\mathfrak{P}$ und $\mathfrak{D}$ Normalteiler in $\mathfrak{G}$. Nach der Induktionsvoraussetzung besitzen nun die Reihen von den Längen $r - 1$ und 2

$$\{\mathfrak{G}_1 \supset \mathfrak{G}_2 \supset \cdots \supset \mathfrak{G}_r = \mathfrak{E}\} \quad \text{und} \quad \{\mathfrak{G}_1 \supset \mathfrak{D} \supset \mathfrak{E}\}$$

isomorphe Verfeinerungen

$$\{\mathfrak{G}_1 \supset \cdots \supset \mathfrak{G}_2 \supset \cdots \supset \mathfrak{E}\} \simeq \{\mathfrak{G}_1 \supset \cdots \supset \mathfrak{D} \supset \cdots \supset \mathfrak{E}\}. \tag{3}$$

Auf Grund des ersten Isomorphiesatzes ist weiter

$$\mathfrak{P}/\mathfrak{H} \simeq \mathfrak{G}_1/\mathfrak{D} \quad \text{und} \quad \mathfrak{P}/\mathfrak{G}_1 \simeq \mathfrak{H}/\mathfrak{D},$$

mithin

$$\{\mathfrak{P} \supset \mathfrak{G}_1 \supset \mathfrak{D} \supset \mathfrak{E}\} \simeq \{\mathfrak{P} \supset \mathfrak{H} \supset \mathfrak{D} \supset \mathfrak{E}\}. \tag{4}$$

Die rechte Seite von (3) ergibt eine Verfeinerung der linken Seite von (4), zu der man eine isomorphe Verfeinerung der rechten Seite finden kann:

$$\{\mathfrak{P} \supset \mathfrak{G}_1 \supset \cdots \supset \mathfrak{D} \supset \cdots \supset \mathfrak{E}\} \cong \{\mathfrak{P} \supset \cdots \supset \mathfrak{H} \supset \mathfrak{D} \supset \cdots \supset \mathfrak{E}\}. \tag{5}$$

Aus (3) und (5) folgt:

$$\{\mathfrak{G} \supset \mathfrak{P} \supset \mathfrak{G}_1 \supset \cdots \supset \mathfrak{G}_2 \supset \cdots \supset \mathfrak{E}\} \cong \{\mathfrak{G} \supset \mathfrak{P} \supset \cdots \supset \mathfrak{H} \supset \mathfrak{D} \supset \cdot \cdot \supset \mathfrak{E}\},$$

womit der Satz im Falle $s = 2$ bewiesen ist.

Für beliebige s können wir nach dem eben Bewiesenen die erste Reihe $\{\mathfrak{G} \supset \mathfrak{G}_1 \supset \cdots\}$ so verfeinern, daß sie einer Verfeinerung von $\{\mathfrak{G} \supset \mathfrak{H}_1 \supset \mathfrak{E}\}$ isomorph wird:

$$\{\mathfrak{G} \supset \cdots \supset \mathfrak{G}_1 \supset \cdots \supset \mathfrak{G}_2 \supset \cdots \supset \mathfrak{E}\} \cong \{\mathfrak{G} \supset \cdots \supset \mathfrak{H}_1 \supset \cdots \supset \mathfrak{E}\}. \tag{6}$$

Die rechts als Teilstück vorkommende Reihe $\{\mathfrak{H}_1 \supset \cdots \supset \mathfrak{E}\}$ und die Reihe $\{\mathfrak{H}_1 \supset \mathfrak{H}_2 \supset \cdots \supset \mathfrak{H}_s = \mathfrak{E}\}$ besitzen nach der Induktionsvoraussetzung isomorphe Verfeinerungen:

$$\{\mathfrak{H}_1 \supset \cdots \supset \mathfrak{E}\} \cong \{\mathfrak{H}_1 \supset \cdots \supset \mathfrak{H}_2 \supset \cdots \supset \mathfrak{E}\}. \tag{7}$$

Die linke Seite von (7) ergibt eine Verfeinerung der rechten Seite von (6), zu der man eine isomorphe Verfeinerung der linken Seite von (6) finden kann. Also:

$$\begin{aligned} &\{\mathfrak{G} \supset \cdots \supset \mathfrak{G}_1 \supset \cdots \supset \mathfrak{G}_2 \supset \cdots \supset \mathfrak{E}\} \\ &\cong \{\mathfrak{G} \supset \cdots \supset \mathfrak{H}_1 \supset \cdots \supset \mathfrak{E}\} \\ [\text{nach (7)}] \quad &\cong \{\mathfrak{G} \supset \cdots \supset \mathfrak{H}_1 \supset \cdots \supset \mathfrak{H}_2 \supset \cdots \supset \mathfrak{E}\}. \end{aligned}$$

Damit ist der Satz allgemein bewiesen.

Streicht man aus zwei isomorphen Reihen alle Wiederholungen weg, so bleiben sie isomorph. Man kann also die im Hauptsatz gemeinten Verfeinerungen immer als solche ohne Wiederholungen annehmen.

Aus dem Hauptsatz über Normalreihen ergeben sich für Gruppen, die eine Kompositionsreihe besitzen, unmittelbar die folgenden beiden Sätze.

1. Satz von JORDAN und HÖLDER: *Je zwei Kompositionsreihen einer und derselben Gruppe $\mathfrak{G}$ sind isomorph.*

Denn diese Reihen sind mit ihren wiederholungsfreien Verfeinerungen identisch.

2. *Besitzt $\mathfrak{G}$ eine Kompositionsreihe, so läßt sich jede Normalreihe von $\mathfrak{G}$ zu einer Kompositionsreihe verfeinern; insbesondere gibt es also durch jeden Normalteiler eine Kompositionsreihe*[1].

[1] Einen anderen Beweis dieser beiden Sätze findet man z. B. bei E. NOETHER Abstrakter Aufbau der Idealtheorie in algebraischen Zahl- und Funktionenkörpern, Math. Ann. Bd. 96, § 10, S. 57. 1926.

Eine Gruppe heißt *auflösbar*, wenn sie eine Normalreihe besitzt, in der alle Faktoren Abelsch sind. (Beispiele: die Gruppen $\mathfrak{S}_3$ und $\mathfrak{S}_4$, siehe oben.)

Aus dem Hauptsatz folgt, daß bei einer auflösbaren Gruppe jede Normalreihe sich zu einer solchen mit Abelschen Faktoren verfeinern läßt. Hat die Gruppe insbesondere eine Kompositionsreihe, so sind alle Kompositionsfaktoren einfache Abelsche Gruppen, d. h. im Fall der gewöhnlichen endlichen Gruppen: zyklische Gruppen von Primzahlordnung. (Vgl. die nachstehende Aufg. 3.)

Aufgaben. 1. Jede endliche Gruppe besitzt eine Kompositionsreihe.

2. Man bilde alle Kompositionsreihen einer zyklischen Gruppe der Ordnung 20.

3. Eine Abelsche Gruppe (ohne Operatoren) ist nur dann einfach, wenn sie zyklisch von Primzahlordnung ist.

4. Eine Gruppe der Ordnung p^n ist nur dann einfach, wenn $n = 1$ ist [vgl. § 8, Aufg. 8].

5. Jede Gruppe der Ordnung p^n ist auflösbar. [Man bilde eine Kompositionsreihe und wende Aufg. 4 an.]

§ 42. Direkte Produkte.

Die Gruppe $\mathfrak{G}$ heißt *direktes Produkt* der Untergruppen $\mathfrak{A}$ und $\mathfrak{B}$, wenn folgende Bedingungen erfüllt sind:

I. 1. $\mathfrak{A}$ und $\mathfrak{B}$ sind Normalteiler in $\mathfrak{G}$;

2. $\mathfrak{G} = \mathfrak{A} \cdot \mathfrak{B}$;

3. $\mathfrak{A} \cap \mathfrak{B} = \mathfrak{E}$.

Äquivalent damit ist:

II. 1. Jedes Element von $\mathfrak{G}$ ist als Produkt

$$g = a\,b\,, \qquad a \in \mathfrak{A}\,, \qquad b \in \mathfrak{B} \tag{1}$$

darstellbar;

2. die Faktoren a und b sind durch g eindeutig bestimmt;

3. jedes Element von $\mathfrak{A}$ ist mit jedem von $\mathfrak{B}$ vertauschbar.

Aus I *folgt* II. Nämlich II 1 folgt aus I 2. II 2 folgt so: Ist $g = a_1 b_1 = a_2 b_2$, so wird $a_2^{-1} a_1 = b_2 b_1^{-1}$; dieses Element $a_2^{-1} a_1$ muß sowohl zu $\mathfrak{A}$ als auch zu $\mathfrak{B}$ gehören, mithin nach I 3 gleich dem Einheitselement sein; daraus folgt

$$a_1 = a_2\,, \qquad b_1 = b_2\,,$$

also die Eindeutigkeit. II 3 folgt daraus, daß $a\,b\,a^{-1} b^{-1}$ wegen I 1 sowohl zu $\mathfrak{A}$ als auch zu $\mathfrak{B}$ gehört, mithin wegen I 3 das Einheitselement ist.

Aus II *folgt* I. Die Normalteilereigenschaft von $\mathfrak{A}$ folgt so:

$$g\,\mathfrak{A}\,g^{-1} = a\,b\,\mathfrak{A}\,b^{-1}\,a^{-1} = a\,\mathfrak{A}\,a^{-1} = \mathfrak{A} \qquad \text{[wegen II 3]}.$$

I 2 folgt aus II 1. Schließlich ergibt sich I 3 folgendermaßen: Ist c ein Element von $\mathfrak{A} \cap \mathfrak{B}$, so ist c auf zwei Arten als Produkt eines Elements von $\mathfrak{A}$ und eines Elements von $\mathfrak{B}$ darzustellen:

$$c = c \cdot 1 = 1 \cdot c .$$

Wegen der Eindeutigkeit [II 3] muß $c = 1$ sein. Damit ist I 3 bewiesen.

Das Produkt $\mathfrak{A}\mathfrak{B}$ wird, wenn es direkt ist, auch mit $\mathfrak{A} \times \mathfrak{B}$ bezeichnet. Bei additiven Gruppen (Moduln) schreibt man $(\mathfrak{A}, \mathfrak{B})$ für die Summe, $\mathfrak{A} + \mathfrak{B}$ für die direkte Summe.

Kennt man die Struktur von $\mathfrak{A}$ und von $\mathfrak{B}$, so ist auch die Struktur von $\mathfrak{G}$ bekannt; denn je zwei Elemente $g_1 = a_1 b_1$ und $g_2 = a_2 b_2$ werden multipliziert, indem man ihre Faktoren multipliziert:

$$g_1 g_2 = a_1 a_2 \cdot b_1 b_2 .$$

Ein *direktes Produkt mehrerer Gruppen:* $\mathfrak{A}_1 \times \mathfrak{A}_2 \times \cdots \times \mathfrak{A}_r$, kann durch vollständige Induktion definiert werden:

$$\mathfrak{A}_1 \times \mathfrak{A}_2 \times \cdots \times \mathfrak{A}_r = (\mathfrak{A}_1 \times \cdots \times \mathfrak{A}_{r-1}) \times \mathfrak{A}_r .$$

Ein Produkt von n Gruppen ist also direkt, wenn das Produkt eines jeden Faktors $\mathfrak{A}_\nu$ mit dem Produkt der vorangehenden Faktoren $\mathfrak{A}_1, \ldots, \mathfrak{A}_{\nu-1}$ direkt ist. Deutet man das mittels Definition I, so kommt:

I_n. *Eine Gruppe $\mathfrak{G}$ ist das direkte Produkt der Untergruppen $\mathfrak{A}_1, \ldots, \mathfrak{A}_n$, wenn*

1. *alle $\mathfrak{A}_\nu$ Normalteiler in $\mathfrak{G}$ sind;*
2. $\mathfrak{A}_1 \ldots \mathfrak{A}_n = \mathfrak{G}$;
3. $(\mathfrak{A}_1 \ldots \mathfrak{A}_{\nu-1}) \cap \mathfrak{A}_\nu = \mathfrak{E}$.

Verwendet man aber II, so erhält man:

II_n. *Eine Gruppe $\mathfrak{G}$ ist das direkte Produkt der Untergruppen $\mathfrak{A}_1, \ldots, \mathfrak{A}_n$, wenn jedes Element von $\mathfrak{G}$ eindeutig als Produkt*

$$g = a_1 a_2 \ldots a_n \qquad (a_\nu \in \mathfrak{A}_\nu)$$

darstellbar und jedes Element von $\mathfrak{A}_\nu$ mit jedem von $\mathfrak{A}_\mu (\mu \neq \nu)$ vertauschbar ist.

Aus dieser Fassung erhellt, daß die Faktoren $\mathfrak{A}_1, \ldots, \mathfrak{A}_n$ für die Definition gleichberechtigt und im Produkt vertauschbar sind. Es ist also nicht nur $\mathfrak{A}_n$, sondern jedes $\mathfrak{A}_\nu$ zum Produkt der übrigen „fremd“:

$$(\mathfrak{A}_1 \ldots \mathfrak{A}_{\nu-1} \mathfrak{A}_{\nu+1} \ldots \mathfrak{A}_n) \cap \mathfrak{A}_\nu = \mathfrak{E} .$$

Bezeichnet man dieses Produkt der übrigen Faktoren mit $\mathfrak{B}_\nu$, so hat man

$$\mathfrak{G} = \mathfrak{A}_\nu \times \mathfrak{B}_\nu .$$

Nach dem ersten Isomorphiesatz ist

$$\mathfrak{G}/\mathfrak{A}_\nu \simeq \mathfrak{B}_\nu ; \qquad \mathfrak{G}/\mathfrak{B}_\nu \simeq \mathfrak{A}_\nu .$$

Die Gruppen

$$(2)\qquad \begin{cases} \mathfrak{G} &= \mathfrak{A}_1 \times \mathfrak{A}_2 \times \cdots \times \mathfrak{A}_n, \\ \mathfrak{G}_1 &= \mathfrak{A}_1 \times \mathfrak{A}_2 \times \cdots \times \mathfrak{A}_{n-1}, \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ \mathfrak{G}_{n-1} &= \mathfrak{A}_1, \\ \mathfrak{G}_n &= \mathfrak{E} \end{cases}$$

bilden eine Normalreihe von $\mathfrak{G}$ mit den Faktoren $\mathfrak{G}_{\nu-1}/\mathfrak{G}_\nu \cong \mathfrak{A}_{n-\nu+1}$. Besitzen die Gruppen $\mathfrak{A}_\nu$ Kompositionsreihen, so besitzt auch $\mathfrak{G}$ eine Kompositionsreihe (Verfeinerung der obigen Normalreihe (2)), deren Länge die Summe der Längen der einzelnen Faktoren ist.

Sehr leicht ist der folgende Satz zu beweisen:

Ist $\mathfrak{G} = \mathfrak{A} \times \mathfrak{B}$, $\mathfrak{G}'$ *eine Untergruppe von* $\mathfrak{G}$ *und* $\mathfrak{G}' \supset \mathfrak{A}$, *so ist* $\mathfrak{G}' = \mathfrak{A} \times \mathfrak{B}'$, *wo* $\mathfrak{B}'$ *den Durchschnitt von* $\mathfrak{G}'$ *und* $\mathfrak{B}$ *darstellt.*

Beweis: Für jedes Element von $\mathfrak{G}$ gilt eine Darstellung $g = a \cdot b$. Diese Darstellung besteht insbesondere für die Elemente von $\mathfrak{G}'$. Die dabei auftretenden Faktoren b sind in $\mathfrak{B}$ und auch in $\mathfrak{G}'$ enthalten (da sowohl g wie a in $\mathfrak{G}'$ liegt); mithin gehören die b zum Durchschnitt $\mathfrak{G}' \cap \mathfrak{B}$. Andererseits kann man für a und b beliebige Elemente von $\mathfrak{A}$ bzw. $\mathfrak{G}' \cap \mathfrak{B}$ wählen und erhält immer ein Produkt $g = a \cdot b$ aus $\mathfrak{G}'$. Daher ist $\mathfrak{G}' = \mathfrak{A} \times (\mathfrak{G}' \cap \mathfrak{B})$, q. e. d.

Aufgaben. 1. Eine zyklische Gruppe $\{a\}$ der Ordnung $n = r \cdot s$ mit $(r, s) = 1$ ist das direkte Produkt ihrer Untergruppen $\{a^r\}$, $\{a^s\}$ der Ordnungen s und r.

2. Eine endliche zyklische Gruppe ist das direkte Produkt ihrer Untergruppen von den höchstmöglichen Primzahlpotenzordnungen.

Eine Gruppe $\mathfrak{G}$ heißt *vollständig reduzibel,* wenn sie ein direktes Produkt von einfachen Gruppen ist. In diesem Fall ist die zugehörige Normalreihe (2) schon eine Kompositionsreihe. Nach dem Jordan-Hölderschen Satz sind die Kompositionsfaktoren $\mathfrak{G}_{\nu-1}/\mathfrak{G}_\nu \cong \mathfrak{A}_{n-\nu+1}$ bis auf Isomorphie und bis auf die Reihenfolge eindeutig bestimmt.

Satz. *In einer vollständig reduziblen Gruppe* $\mathfrak{G}$ *ist jeder Normalteiler direkter Faktor; d. h. zu jedem Normalteiler* $\mathfrak{H}$ *gibt es eine Zerlegung* $\mathfrak{G} = \mathfrak{H} \times \mathfrak{B}$.

Beweis: Aus $\mathfrak{G} = \mathfrak{A}_1 \times \mathfrak{A}_2 \times \cdots \times \mathfrak{A}_n$ folgt

$$(3)\qquad \mathfrak{G} = \mathfrak{H} \cdot \mathfrak{G} = \mathfrak{H} \cdot \mathfrak{A}_1 \cdot \mathfrak{A}_2 \cdot \cdots \mathfrak{A}_n.$$

Mit jedem der Faktoren $\mathfrak{A}_1, \ldots, \mathfrak{A}_n$ kann man nun hierin eine Operation vornehmen, die darin besteht, daß man den betreffenden Faktor entweder wegstreicht oder das vor ihm stehende Zeichen $\cdot$ in das Zeichen $\times$ für direktes Produkt verwandelt. Nämlich der Durchschnitt des jeweils betrachteten $\mathfrak{A}_k$ mit dem vorangehenden Produkt

$\Pi = \mathfrak{H} \cdot \mathfrak{A}_1 \cdots \mathfrak{A}_{k-1}$ ist Normalteiler in $\mathfrak{A}_k$, also entweder $= \mathfrak{A}_k$ oder $= \mathfrak{E}$. Im ersten Fall: $\Pi \cap \mathfrak{A}_k = \mathfrak{A}_k$, ist $\mathfrak{A}_k \subset \Pi$, also der Faktor $\mathfrak{A}_k$ im Produkt $\Pi\, \mathfrak{A}_k$ überflüssig. Im anderen Fall ist das Produkt $\Pi \cdot \mathfrak{A}_k$ direkt: $\Pi \cdot \mathfrak{A}_k = \Pi \times \mathfrak{A}_k$.

Nach dem eben Bewiesenen erhält das Produkt (3) nach Streichung aller überflüssigen $\mathfrak{A}$ die Form eines direkten Produktes:

$$\mathfrak{G} = \mathfrak{H} \times \mathfrak{A}_{i_1} \times \mathfrak{A}_{i_2} \times \cdots \times \mathfrak{A}_{i_r}.$$

Daraus folgt die Behauptung.

§ 43. Die Einfachheit der alternierenden Gruppe.

In § 41 haben wir gesehen, daß die symmetrischen Gruppen $\mathfrak{S}_3$, $\mathfrak{S}_4$ auflösbar sind. Im Gegensatz dazu sind alle weiteren symmetrischen Gruppen $\mathfrak{S}_n (n > 4)$ nicht auflösbar. Sie haben zwar immer einen Normalteiler vom Index 2, nämlich die alternierende Gruppe $\mathfrak{A}_n$; aber die Kompositionsreihe geht von $\mathfrak{A}_n$ gleich auf $\mathfrak{E}$, nach dem folgenden

Satz. *Die alternierende Gruppe* $\mathfrak{A}_n (n > 4)$ *ist einfach.*

Wir brauchen einen

Hilfssatz. *Wenn ein Normalteiler* $\mathfrak{N}$ *der Gruppe* $\mathfrak{A}_n$ $(n > 2)$ *einen Dreierzyklus enthält, so ist* $\mathfrak{N} = \mathfrak{A}_n$.

Beweis des Hilfssatzes: $\mathfrak{N}$ enthalte etwa den Zyklus (1 2 3). Dann muß $\mathfrak{N}$ auch das Quadrat (2 1 3), sowie alle Transformierten

$$\sigma \cdot (2\ 1\ 3) \cdot \sigma^{-1} \qquad (\sigma \in \mathfrak{A}_n)$$

enthalten. Wählt man $\sigma = (1\ 2)\ (3\ k)$, wo $k > 3$ ist, so wird

$$\sigma \cdot (2\ 1\ 3) \cdot \sigma^{-1} = (1\ 2\ k);$$

also enthält $\mathfrak{N}$ alle Zyklen von der Gestalt (1 2 k). Diese erzeugen aber die Gruppe $\mathfrak{A}_n$ (§ 7, Aufg. 5); also muß $\mathfrak{N} = \mathfrak{A}_n$ sein.

Beweis des Satzes: Es sei $\mathfrak{N}$ ein von $\mathfrak{E}$ verschiedener Normalteiler in $\mathfrak{A}_n$. Wir wollen zeigen, daß $\mathfrak{N} = \mathfrak{A}_n$ ist.

Wir wählen eine Permutation τ in $\mathfrak{N}$, die, ohne $= 1$ zu sein, möglichst viele Ziffern fest läßt. Dann läßt sich zunächst feststellen:

1. τ kann nicht aus Zyklen von verschiedener Länge bestehen; denn wäre etwa

$$\tau = (a_1 \ldots a_n)\ (b_1 \ldots b_m) \ldots \qquad (n > m),$$

so wäre τ^m eine Permutation, die außer den gegenüber τ invarianten Ziffern auch noch $b_1, \ldots, b_m$ fest ließe, aber a_1 in $a_m (\neq a_1)$ überführte. Diese Permutation würde also mehr Ziffern fest lassen als τ, ohne $= 1$ zu sein.

2. τ kann nicht mehr als 4 Ziffern verrücken. Andernfalls nämlich könnte man setzen:

$$\tau = (1\ 2 \ldots) \ldots (\ldots k) \qquad (k > 4).$$

Dann besteht *entweder* τ aus lauter Zweierzyklen, also aus mindestens 3 solchen; in diesem Fall stehen die beiden Ziffern 3, 4 in einem Zyklus nebeneinander. *Oder* τ besteht aus Zyklen von mindestens 3 Ziffern; dann stehen die Ziffern $k-2$, $k-1$ im letzten Zyklus nebeneinander. Auf jeden Fall gibt es also zwei von 1, 2, k verschiedene Ziffern i, j, die in einem Zyklus nebeneinander stehen. Wir bilden die Permutation

$$\tau' = (1\,2\,k)\,\tau\,(1\,2\,k)^{-1} = (2\,k\,\ldots)\ldots(\ldots 1).$$

Diese ist von τ verschieden, da sie 2 in k überführt, was τ sicher nicht tut. Sie führt, ebenso wie τ, die Ziffer i in j über und muß auch in $\mathfrak{N}$ liegen. Also wird

$$\tau^{-1}\tau'$$

von 1 verschieden sein, in $\mathfrak{N}$ liegen und die Ziffer i fest lassen, also eine Ziffer mehr fest lassen als τ, entgegen der Minimalvoraussetzung.

3. Da τ eine gerade Permutation ist, kommen nur mehr die beiden folgenden Typen in Betracht:

$$\tau = (1\,2\,3),$$
$$\tau = (1\,2)\,(3\,4).$$

Der erste Fall führt auf Grund des Hilfssatzes direkt zu $\mathfrak{N} = \mathfrak{A}_n$. Der zweite ist für $n = 4$ möglich und führt dann auf die Kleinsche Vierergruppe; für $n > 4$ aber ist der Fall ausgeschlossen, denn dann enthält $\mathfrak{N}$ zugleich mit τ auch die Permutationen

$$\tau' = (3\,4\,5)\,\tau\,(3\,4\,5)^{-1} = (1\,2)\,(4\,5),$$
$$\tau\tau' = (3\,4\,5),$$

und die letztere läßt mehr Elemente fest als τ. Damit ist die Behauptung bewiesen.

Aufgabe. Man beweise, daß für $n \neq 4$ die alternierende Gruppe $\mathfrak{A}_n$ der einzige Normalteiler der symmetrischen Gruppe $\mathfrak{S}_n$ außer ihr selbst und $\mathfrak{E}$ ist.

§ 44. Transitivität und Primitivität.

Eine Gruppe von Permutationen einer Menge $\mathfrak{M}$ heißt *transitiv über* $\mathfrak{M}$, wenn es in $\mathfrak{M}$ ein Element a gibt, das durch die Permutationen der Gruppe in alle Elemente x von $\mathfrak{M}$ übergeführt wird, so daß es also zu jedem x eine Operation σ der Gruppe mit $\sigma a = x$ gibt.

Ist diese Bedingung erfüllt, so gibt es auch zu je zwei Elementen x, y eine Operation τ der Gruppe, die x in y überführt. Denn aus

$$\varrho\, a = x, \qquad \sigma\, a = y$$

folgt

$$(\sigma\,\varrho^{-1})\,x = \sigma\, a = y.$$

Es ist also für die Frage nach der Transitivität gleichgültig, von welchem Element a man ausgeht.

Ist die Gruppe $\mathfrak{G}$ nicht transitiv über $\mathfrak{M}$ (*intransitive Gruppe*), so zerfällt die Menge $\mathfrak{M}$ in *„Transitivitätsgebiete"*, d. h. Teilmengen, die durch die Gruppe in sich transformiert werden und über welchen die Gruppe transitiv ist. Zu dieser Einteilung in Teilmengen gelangt man nach folgendem Prinzip: Zwei Elemente a, b von $\mathfrak{M}$ sollen dann und nur dann in dieselbe Teilmenge aufgenommen werden, wenn es in $\mathfrak{G}$ eine Operation σ gibt, die a in b überführt.

Diese Eigenschaft ist 1. reflexiv, 2. symmetrisch und 3. transitiv; denn es gilt:

1. $\sigma a = a$ für $\sigma = 1$.
2. Aus $\sigma a = b$ folgt $\sigma^{-1} b = a$.
3. Aus $\sigma a = b$, $\tau b = c$ folgt $(\tau\sigma) a = c$.

Also ist dadurch tatsächlich eine Klasseneinteilung der Menge $\mathfrak{M}$ definiert.

Ist eine Gruppe $\mathfrak{G}$ transitiv über $\mathfrak{M}$ und ist $\mathfrak{G}_a$ die Untergruppe derjenigen Elemente von $\mathfrak{G}$, welche das Element a von $\mathfrak{M}$ fest lassen, so führt jede linksseitige Nebenklasse $\tau\mathfrak{G}_a$ von $\mathfrak{G}_a$ das Element a in das einzige Element τa über. Den linksseitigen Nebenklassen entsprechen in dieser Weise eineindeutig die Elemente von $\mathfrak{M}$, wie auf Grund der Transitivität von $\mathfrak{G}$ unmittelbar einzusehen ist. Die Anzahl der Nebenklassen (der Index von $\mathfrak{G}_a$) ist also gleich der Anzahl der Elemente von $\mathfrak{M}$. Die Gruppe derjenigen Elemente von $\mathfrak{G}$, die τa invariant lassen, ist durch

$$\mathfrak{G}_{\tau a} = \tau\, \mathfrak{G}_a \tau^{-1}$$

gegeben.

Eine transitive Gruppe von Permutationen einer Menge $\mathfrak{M}$ heißt *imprimitiv*, wenn es möglich ist, $\mathfrak{M}$ in mindestens zwei fremde Teilmengen $\mathfrak{M}_1, \mathfrak{M}_2, \ldots$ zu zerlegen, die nicht alle aus nur einem Element bestehen, derart, daß die Transformationen der Gruppe jede Menge $\mathfrak{M}_\mu$ in eine Menge $\mathfrak{M}_\nu$ überführen. Die Mengen $\mathfrak{M}_1, \mathfrak{M}_2, \ldots$ heißen dann *Imprimitivitätsgebiete*. Ist eine solche Zerlegung

$$\mathfrak{M} = \{\mathfrak{M}_1, \mathfrak{M}_2, \ldots\}$$

unmöglich, so heißt die Gruppe *primitiv*.

Beispiele. Die Kleinsche Vierergruppe ist imprimitiv, mit den Teilmengen

$$\{1, 2\},\ \{3, 4\}$$

als Imprimitivitätsgebieten. (Es sind übrigens noch zwei andere Zerlegungen in Imprimitivitätsgebiete möglich.) Dagegen ist die volle Permutationsgruppe (und ebenso die alternierende Gruppe) von n Dingen stets primitiv; denn bei jeder Zerlegung der Menge $\mathfrak{M}$ in Teilmengen, etwa:

$$\mathfrak{M} = \{\{1, 2, \ldots, k\},\ \{\ldots\},\ \ldots\} \qquad (1 < k < n),$$

gibt es eine Permutation, die $\{1, 2, \ldots, k\}$ in $\{1, 2, \ldots, k-1, k+1\}$ überführt, also in eine Menge, die weder zu $\{1, 2, \ldots, k\}$ fremd noch damit identisch ist.

Bei einer Zerlegung $\mathfrak{M} = \{\mathfrak{M}_1, \ldots, \mathfrak{M}_r\}$ von der obigen Eigenschaft, wobei also die Gruppe $\mathfrak{G}$ die Mengen $\mathfrak{M}_\nu$ untereinander permutiert, gibt es für jedes ν eine zur Gruppe gehörige Permutation, welche $\mathfrak{M}_1$ in $\mathfrak{M}_\nu$ überführt. Man braucht nämlich nur auf Grund der Transitivität eine Permutation zu suchen, welche ein beliebig gewähltes Element von $\mathfrak{M}_1$ in ein Element von $\mathfrak{M}_\nu$ überführt; diese Permutation kann dann $\mathfrak{M}_1$ nur in $\mathfrak{M}_\nu$ überführen. Daraus folgt insbesondere, daß die Mengen $\mathfrak{M}_1, \mathfrak{M}_2, \ldots$ alle aus gleich vielen Elementen bestehen.

Für beliebige transitive Permutationsgruppen $\mathfrak{G}$ einer Menge $\mathfrak{M}$ gilt der folgende Satz:

Es sei $\mathfrak{g}$ *die Untergruppe aus denjenigen Elementen von* $\mathfrak{G}$, *welche ein Element* a *von* $\mathfrak{M}$ *invariant lassen. Wenn die Gruppe* $\mathfrak{G}$ *imprimitiv ist, so existiert eine von* $\mathfrak{g}$ *und* $\mathfrak{G}$ *verschiedene Gruppe* $\mathfrak{h}$ *mit*

$$\mathfrak{g} < \mathfrak{h} < \mathfrak{G},$$

und umgekehrt, wenn eine solche Zwischengruppe $\mathfrak{h}$ *existiert, so ist* $\mathfrak{G}$ *imprimitiv. Die Gruppe* $\mathfrak{h}$ *läßt ein Imprimitivitätsgebiet* $\mathfrak{M}_1$ *invariant, und die linksseitigen Nebenklassen von* $\mathfrak{h}$ *führen* $\mathfrak{M}_1$ *in die einzelnen Gebiete* $\mathfrak{M}_\nu$ *über.*

Beweis. Es sei zunächst $\mathfrak{G}$ imprimitiv und $\mathfrak{M} = \{\mathfrak{M}_1, \mathfrak{M}_2, \ldots\}$ eine Zerlegung in Imprimitivitätsgebiete. $\mathfrak{M}_1$ enthalte das Element a. Es sei $\mathfrak{h}$ die Untergruppe derjenigen Elemente von $\mathfrak{G}$, die $\mathfrak{M}_1$ invariant lassen. Nach der obigen Bemerkung enthält $\mathfrak{h}$ alle die Permutationen von $\mathfrak{G}$, welche a in sich selbst oder in ein anderes Element von $\mathfrak{M}_1$ überführen; daraus folgt $\mathfrak{g} < \mathfrak{h}$ und $\mathfrak{h} \neq \mathfrak{g}$. Es gibt aber in $\mathfrak{G}$ auch Permutationen, welche $\mathfrak{M}_1$ etwa in $\mathfrak{M}_2$ überführen; daher ist $\mathfrak{h} \neq \mathfrak{G}$. Ferner: Wenn τ das System $\mathfrak{M}_1$ in $\mathfrak{M}_\nu$ überführt, so führt die ganze Nebenklasse $\tau\mathfrak{h}$ ebenfalls $\mathfrak{M}_1$ in $\mathfrak{M}_\nu$ über.

Es sei nun umgekehrt eine von $\mathfrak{g}$ und $\mathfrak{G}$ verschiedene Gruppe $\mathfrak{h}$ mit

$$\mathfrak{g} < \mathfrak{h} < \mathfrak{G}$$

gegeben. $\mathfrak{G}$ zerfällt ganz in Nebenklassen $\tau\mathfrak{h}$, und jede von diesen zerfällt wieder in Nebenklassen $\sigma\mathfrak{g}$. Die letzteren Nebenklassen führen a je in ein weiteres Element σa über; faßt man sie also zu Nebenklassen $\tau\mathfrak{h}$ zusammen, so werden auch die Elemente σa zu mindestens zwei paarweise fremden Mengen $\mathfrak{M}_1, \mathfrak{M}_2, \ldots$ zusammengefaßt, von denen jede aus mindestens zwei Elementen besteht. Die $\mathfrak{M}_\nu$ sind also definiert durch

$$\mathfrak{M}_\nu = \tau\mathfrak{h}a. \tag{1}$$

Jede weitere Substitution σ führt $\mathfrak{M}_\nu = \tau\mathfrak{h}a$ in $\sigma\tau\mathfrak{h}a$, also wieder in eine Menge von derselben Art über, womit die Imprimitivität der

Gruppe bewiesen ist. Bezeichnet man etwa mit $\mathfrak{M}_1$ die aus (1) für $\tau = 1$ entstehende Menge, so läßt $\mathfrak{h}$ (wegen $\mathfrak{h}\mathfrak{M}_1 = \mathfrak{h}\mathfrak{h}a = \mathfrak{h}a = \mathfrak{M}_1$ das Imprimitivitätsgebiet $\mathfrak{M}_1$ fest, und die Nebenklassen $\tau\mathfrak{h}$ führen $\mathfrak{M}_1$ (wegen $\tau\mathfrak{h}\mathfrak{M}_1 = \tau\mathfrak{h}\mathfrak{h}a = \tau\mathfrak{h}a$) in die übrigen Imprimitivitätsgebiete $\mathfrak{M}_\nu$ über.

Aufgaben. 1. Ist die Anzahl der Elemente der Menge $\mathfrak{M}$ eine Primzahl, so ist jede transitive Gruppe primitiv.

2. Die oben definierte Gruppe $\mathfrak{h}$ ist über $\mathfrak{M}_1$ transitiv.

3. Die Menge $\mathfrak{M}$ sei in 3 Imprimitivitätsgebiete zu je 2 Elementen zerlegt; die Ordnung der Gruppe $\mathfrak{G}$ sei 12. Was ist

a) der Index von $\mathfrak{h}$ in $\mathfrak{G}$,

b) der Index von $\mathfrak{g}$ in $\mathfrak{h}$,

c) die Ordnung von $\mathfrak{g}$?

4. Die Ordnung einer transitiven Gruppe aus Permutationen endlichvieler Objekte ist durch die Anzahl dieser Objekte teilbar.

Bemerkung. Die Anzahl der permutierten Objekte nennt man auch den *Grad* der Permutationsgruppe.

Siebentes Kapitel.

Die Theorie von GALOIS.

Die Theorie von GALOIS beschäftigt sich mit den endlichen separablen Erweiterungen eines kommutativen Körpers K und insbesondere mit deren 1-Isomorphismen und 1-Automorphismen. Sie stellt eine Beziehung her zwischen den Erweiterungskörpern von K, welche in einem gegebenen Galoisschen Körper enthalten sind, und den Untergruppen einer gewissen endlichen Gruppe. Durch diese Theorie finden verschiedene Fragen über die Auflösung algebraischer Gleichungen eine Lösung.

Alle in diesem Kapitel vorkommenden Körper sind kommutativ.

§ 45. Die Galoissche Gruppe.

Ist der Grundkörper K gegeben, so wird nach § 34 jeder endliche separable Erweiterungskörper Σ von einem „primitiven Element" Θ erzeugt: $\Sigma = \mathsf{K}(\Theta)$. Nach § 32 besitzt Σ in einem passenden Erweiterungskörper Ω so viele „relative", d. h. K elementweise festlassende Isomorphismen, wie der Grad n von Σ in bezug auf K beträgt. Für diesen Erweiterungskörper Ω kann man wählen den Zerfällungskörper des irreduziblen Polynoms $f(x)$, dessen Nullstelle Θ ist. Dieser Zerfällungskörper ist der kleinste in bezug auf K Galoissche Körper, der Σ umfaßt, oder, wie wir auch sagen werden, *der zu Σ gehörige Galoissche Körper*. Die relativen Isomorphismen von $\mathsf{K}(\Theta)$ können dadurch ge-

kennzeichnet werden, daß sie die Größe Θ in ihre konjugierten Größen $\Theta_1, \ldots, \Theta_n$ in Ω überführen[1]. Jedes Körperelement $\varphi(\Theta) = \sum a_\lambda \Theta^\lambda$ $(a_\lambda \in \mathsf{K})$ geht dann in $\varphi(\Theta_\nu) = \sum a_\lambda \Theta_\nu^\lambda$ über, und man kann daher, statt vom Isomorphismus zu reden, auch reden von der *Substitution* $\Theta \to \Theta_\nu$.

Zu beachten ist aber, daß die Größen Θ und Θ_ν nur *Hilfsmittel* sind, die Isomorphismen bequem darzustellen, und daß der *Begriff* eines Isomorphismus gänzlich unabhängig von der speziellen Wahl eines Θ ist. Man kann durchaus auch von mehr als einer Körpererzeugenden ausgehend die Isomorphismen konstruieren, wie wir nachher noch sehen werden.

Ist Σ selbst ein Galoisscher Körper, so fallen alle konjugierten Körper $\mathsf{K}(\Theta_\nu)$ mit Σ zusammen.

Denn erstens sind alle Θ_ν in diesem Fall in $\mathsf{K}(\Theta)$ enthalten. Aber die $\mathsf{K}(\Theta_\nu)$ sind zu $\mathsf{K}(\Theta)$ äquivalent, also selbst Galoissch; also ist auch umgekehrt Θ in jedem $\mathsf{K}(\Theta_\nu)$ enthalten.

Umgekehrt: *Ist Σ mit allen konjugierten Körpern $\mathsf{K}(\Theta_\nu)$ identisch, so ist Σ Galoissch.*

Denn unter dieser Voraussetzung ist Σ gleich dem Zerfällungskörper $\mathsf{K}(\Theta_1, \ldots, \Theta_n)$ von $f(x)$, also Galoissch.

Wir nehmen hinfort an, $\Sigma = \mathsf{K}(\Theta)$ sei ein Galoisscher Körper. Unter dieser Voraussetzung werden die Isomorphismen, die Σ in seine konjugierten Körper $\mathsf{K}(\Theta_\nu)$ überführen, *Automorphismen* von Σ. Diese Automorphismen von Σ (die K elementweise festlassen) bilden offensichtlich eine Gruppe von n Elementen, die man *die Galoissche Gruppe von Σ nach K oder in bezug auf K* nennt. Diese Gruppe spielt in unseren weiteren Betrachtungen die Hauptrolle. Wir bezeichnen sie mit $\mathfrak{G}$. Wir konstatieren noch einmal ausdrücklich: *Die Ordnung der Galoisschen Gruppe ist gleich dem Körpergrad $n = (\Sigma|\mathsf{K})$.*

Wenn man, wie es bisweilen geschieht, auch bei nicht-Galoisschen endlichen separablen Erweiterungskörpern Σ' von der Galoisschen Gruppe redet, so ist damit die Gruppe des zugehörigen Galoisschen Körpers $\Sigma \geqq \Sigma'$ gemeint.

Um die Automorphismen zu finden, braucht man keineswegs zuerst ein primitives Element Θ für den Körper Σ zu suchen. Man kann auch Σ durch mehrere sukzessive Adjunktionen erzeugen, etwa in der Gestalt $\Sigma = \mathsf{K}(\alpha_1, \ldots, \alpha_m)$, und dann zuerst die 1-Isomorphismen von $\mathsf{K}(\alpha_1)$ aufsuchen, die α_1 in seine konjugierten Größen überführen; sodann diese 1-Isomorphismen fortsetzen zu den 1-Isomorphismen von $\mathsf{K}(\alpha_1, \alpha_2)$, usw.

Ein wichtiger Spezialfall ist der, daß die $\alpha_1, \ldots, \alpha_m$ die Wurzeln einer Gleichung $f(x) = 0$ sind[2]. Unter der *Galoisschen Gruppe der Glei-*

[1] Unter den $\Theta_1, \ldots, \Theta_n$ kommt natürlich Θ selbst vor.

[2] $f(x)$ soll ein Polynom ohne mehrfache Linearfaktoren sein.

chung $f(x) = 0$ versteht man die Galoissche Gruppe des Zerfällungskörpers $\mathsf{K}(\alpha_1, \ldots, \alpha_m)$ dieser Gleichung. Jeder relative Automorphismus führt das System der Wurzeln in sich selbst über; d. h. jeder Automorphismus permutiert die Wurzeln. Ist diese Permutation bekannt, so ist auch der Automorphismus bekannt; denn wenn etwa $\alpha_1, \ldots, \alpha_m$ der Reihe nach in $\alpha_1', \ldots, \alpha_m'$ übergeführt werden, so muß jedes Element von $\mathsf{K}(\alpha_1, \ldots, \alpha_m)$, als rationale Funktion $\varphi(\alpha_1, \ldots, \alpha_m)$, in die entsprechende Funktion $\varphi(\alpha_1', \ldots, \alpha_m')$ übergehen. *Also läßt sich die Galoissche Gruppe einer Gleichung auch als eine Gruppe von Permutationen der Wurzeln auffassen.* Diese Permutationsgruppe ist immer gemeint, wenn von der Gruppe der Gleichung die Rede ist.

Es sei Δ ein „Zwischenkörper": $\mathsf{K} \subseteq \Delta \subseteq \Sigma$. Nach einem Satz von § 29 läßt sich jeder (relative) Isomorphismus von Δ, welcher Δ in einen konjugierten Körper Δ' innerhalb Σ überführt, fortsetzen zu einem Isomorphismus von Σ, also zu einem Element der Galoisschen Gruppe. Daraus folgt:

Zwei Zwischenkörper Δ, Δ' sind dann und nur dann konjugiert in bezug auf K, *wenn sie durch eine Substitution der Galoisschen Gruppe ineinander übergeführt werden können.*

Setzt man $\Delta = \mathsf{K}(\alpha)$, so folgt ebenso:

Zwei Elemente α, α' von Σ sind dann und nur dann konjugiert in bezug auf K, *wenn sie durch eine Substitution der Galoisschen Gruppe von Σ ineinander übergeführt werden können.*

Die Anzahl der verschiedenen Konjugierten einer Größe α in Σ ist gleich dem Grad der irreduziblen Gleichung für α. Ist diese Anzahl gleich 1, so ist α Wurzel einer linearen Gleichung, also in K enthalten. Daraus folgt:

Wenn ein Element α von Σ alle Substitutionen der Galoisschen Gruppe von Σ „gestattet", d. h. bei allen diesen Substitutionen in sich übergeht, so gehört α dem Grundkörper K *an.*

Aus allen diesen Sätzen ersieht man schon die große Bedeutung, die die Automorphismengruppe für das Studium der Eigenschaften des Körpers hat. Diese Sätze wurden der Bequemlichkeit halber für endliche Erweiterungskörper ausgesprochen, sind aber durch „transfinite Induktion" (Kap. 8) unschwer auf unendliche Erweiterungen zu übertragen. Sie gelten sogar noch für inseparable Erweiterungen, wenn man nur den Körpergrad durch den reduzierten Körpergrad ersetzt und die Behauptung des letzten Satzes abändert in: „so gehört eine Potenz α^{p^r}, wo p die Charakteristik ist, dem Grundkörper K an". Dagegen gilt der im nächsten Paragraphen aufzustellende „Hauptsatz der Galoisschen Theorie" nur für endliche, separable Erweiterungen.

Man nennt den Erweiterungskörper Σ über K *Abelsch*, wenn die Galoissche Gruppe Abelsch; *zyklisch*, wenn die Gruppe zyklisch ist, usw. Ebenso heißt eine Gleichung *Abelsch, zyklisch, primitiv*, wenn

ihre Galoissche Gruppe Abelsch, zyklisch oder (als Permutationsgruppe der Wurzeln) primitiv ist.

Ein besonders einfaches *Beispiel* für die Galoissche Gruppe liefern die Galois-Felder $GF(p^m)$ (§ 31), wenn man den darin enthaltenen Primkörper Π als Grundkörper betrachtet. Der in § 31 betrachtete 1-Automorphismus $s(\alpha \to \alpha^p)$ und dessen Potenzen $s^2, s^3, \ldots, s^m = 1$ lassen alle Elemente von Π fest und gehören daher zur Galoisschen Gruppe; da aber der Körpergrad auch m ist, bilden sie die ganze Gruppe. Diese ist also zyklisch von der Ordnung m.

Aufgaben. 1. Jede rationale Funktion der Wurzeln einer Gleichung, die bei den Permutationen der Galoisschen Gruppe in sich übergeht, gehört dem Grundkörper an, und umgekehrt.

2. Die Galoissche Gruppe einer doppelwurzelfreien Gleichung $f(x) = 0$ ist transitiv (§ 44) dann und nur dann, wenn die Gleichung im Grundkörper irreduzibel ist.

3. Welche Möglichkeiten für die Gruppe einer irreduziblen Gleichung 3. Grades gibt es?

4. Die Gruppe einer Gleichung besteht dann und nur dann aus lauter geraden Permutationen, wenn die Quadratwurzel aus der Diskriminante im Grundkörper enthalten ist.

5. Man stelle die Galoisschen Gruppen der Gleichungen

$$x^3 - 2 = 0,$$
$$x^3 + 2x + 1 = 0,$$
$$x^4 - 5x^2 + 6 = 0$$

auf; ebenso die der „Kreisteilungsgleichungen"

$$x^4 + x^2 + 1 = 0,$$
$$x^4 + 1 = 0$$

(alles in bezug auf den rationalen Grundkörper).

§ 46. Der Hauptsatz der Galoisschen Theorie.

Der „Hauptsatz" lautet:

1. *Zu jedem Zwischenkörper* Δ, $\mathsf{K} \leqq \Delta \leqq \Sigma$, *gehört eine Untergruppe* $\mathfrak{g}$ *der Galoisschen Gruppe* $\mathfrak{G}$, *nämlich die Gesamtheit derjenigen Automorphismen von* Σ, *die alle Elemente von* Δ *festlassen.* 2. Δ *ist durch* $\mathfrak{g}$ *eindeutig bestimmt;* Δ *ist nämlich die Gesamtheit derjenigen Elemente von* Σ, *welche die Substitutionen von* $\mathfrak{g}$ *„gestatten", d. h. bei ihnen invariant bleiben.* 3. *Zu jeder Untergruppe* $\mathfrak{g}$ *von* $\mathfrak{G}$ *kann man einen Körper* Δ *finden, der zu* $\mathfrak{g}$ *in der erwähnten Beziehung steht.* 4. *Die Ordnung von* $\mathfrak{g}$ *ist gleich dem Grad von* Σ *in bezug auf* Δ; *der Index von* $\mathfrak{g}$ *in* $\mathfrak{G}$ *ist gleich dem Grad von* Δ *in bezug auf* K.

Beweis: Die Gesamtheit der Automorphismen von Σ, welche alle Elemente von Δ festlassen, ist die Galoissche Gruppe von Σ nach Δ, hat also jedenfalls die Gruppeneigenschaft. Damit ist die Behauptung 1. bewiesen, während 2. folgt aus dem letzten Satz von § 45, angewandt auf Σ als Oberkörper und Δ als Grundkörper. Etwas schwieriger ist die Behauptung 3.

Es sei wieder $\Sigma = \mathsf{K}(\Theta)$ und es sei $\mathfrak{g}$ eine gegebene Untergruppe von $\mathfrak{G}$. Wir bezeichnen mit Δ die Gesamtheit der Elemente von Σ, die bei den Substitutionen σ von $\mathfrak{g}$ in sich übergehen. Dieses Δ ist offenbar ein Körper; denn wenn α und β bei den Substitutionen σ festbleiben, so gilt dasselbe für $\alpha + \beta$, $\alpha - \beta$, $\alpha \cdot \beta$ und im Falle $\beta \neq 0$ für $\alpha : \beta$. Weiter gilt $\mathsf{K} \subseteq \Delta \subseteq \Sigma$. Die Galoissche Gruppe von Σ in bezug auf Δ umfaßt die Gruppe $\mathfrak{g}$, da die Substitutionen von $\mathfrak{g}$ sicher die Eigenschaft haben, die Elemente von Δ fest zu lassen. Würde die Galoissche Gruppe von Σ nach Δ mehr Elemente als die von $\mathfrak{g}$ allein enthalten, so wäre auch der Grad (Σ/Δ) größer als die Ordnung von $\mathfrak{g}$. Dieser Grad (Σ/Δ) ist gleich dem Grad von Θ in bezug auf Δ, da ja $\Sigma = \Delta(\Theta)$ ist. Sind nun $\sigma_1, \ldots, \sigma_h$ die Substitutionen von $\mathfrak{g}$, so ist Θ eine Wurzel der Gleichung h-ten Grades

$$(1) \qquad (x - \sigma_1\Theta)(x - \sigma_2\Theta) \ldots (x - \sigma_h\Theta) = 0,$$

deren Koeffizienten bei der Gruppe $\mathfrak{g}$ invariant bleiben, also zu Δ gehören. Daher ist der Grad von Θ in bezug auf Δ nicht größer als die Ordnung h von $\mathfrak{g}$.

Es bleibt also nur die Möglichkeit übrig, daß $\mathfrak{g}$ genau die Galoissche Gruppe von Σ nach Δ ist. Damit ist 3. bewiesen. (Nebenbei folgt noch die Irreduzibilität von (1) in $\Delta[x]$.)

Ist schließlich n die Ordnung von $\mathfrak{G}$, h wiederum die von $\mathfrak{g}$, j der Index, so ist

$$n = (\Sigma/\mathsf{K}), \quad h = (\Sigma/\Delta), \quad n = h \cdot j,$$
$$(\Sigma/\mathsf{K}) = (\Sigma/\Delta) \cdot (\Delta/\mathsf{K}),$$

mithin

$$(\Delta/\mathsf{K}) = j.$$

Damit ist auch 4. bewiesen.

Nach dem nunmehr bewiesenen Hauptsatz ist die Beziehung zwischen den Untergruppen $\mathfrak{g}$ und den Zwischenkörpern Δ eine umkehrbar eindeutige. Es entsteht die Frage: Wie findet man $\mathfrak{g}$, wenn man Δ hat, oder Δ, wenn man $\mathfrak{g}$ hat?

Das erstere ist leicht. Wir nehmen an, wir hätten die zu Θ konjugierten Größen $\Theta_1, \ldots, \Theta_n$, ausgedrückt durch Θ, schon gefunden; dann haben wir auch die Automorphismen $\Theta \to \Theta_\nu$, welche die Gruppe $\mathfrak{G}$ ausmachen. Ist nun ein Unterkörper $\Delta = \mathsf{K}(\beta_1, \ldots, \beta_k)$ gegeben, wo $\beta_1, \ldots, \beta_k$ bekannte Ausdrücke in Θ sind, so besteht $\mathfrak{g}$ einfach aus denjenigen Substitutionen von $\mathfrak{G}$, welche $\beta_1, \ldots, \beta_k$ invariant

lassen; denn diese lassen auch alle rationalen Funktionen von $\beta_1, \ldots, \beta_k$ invariant.

Ist umgekehrt $\mathfrak{g}$ gegeben, so bilde man das zugehörige Produkt

$$(x - \sigma_1\Theta)\,(x - \sigma_2\Theta) \ldots (x - \sigma_h\Theta)\,.$$

Die Koeffizienten dieses Polynoms müssen, dem Beweis des Hauptsatzes zufolge, in Δ liegen und sogar Δ erzeugen; denn sie erzeugen einen Körper, in bezug auf den das Element Θ, als Wurzel der Gleichung (1), schon den Grad h hat und der daher kein echter Unterkörper von Δ sein kann. Die Erzeugenden von Δ sind also einfach die elementarsymmetrischen Funktionen von $\sigma_1\Theta, \ldots, \sigma_h\Theta$.

Eine andere Methode besteht darin, daß man sich eine Größe $\chi(\Theta)$ zu verschaffen sucht, die bei den Substitutionen von $\mathfrak{g}$ invariant bleibt, aber keine weiteren Substitutionen von $\mathfrak{G}$ gestattet. Die Größe $\chi(\Theta)$ wird dann dem Körper Δ, aber keinem echten Unterkörper von Δ angehören, mithin Δ erzeugen. Daß es eine solche Größe stets gibt, folgt z. B. aus dem Satz vom primitiven Element (§ 34).

Durch den Hauptsatz der Galoisschen Theorie erhält man, wenn man einmal die Galoissche Gruppe kennt, eine vollständige Übersicht über alle Zwischenkörper von K und Σ. Ihre Anzahl ist offenbar endlich; denn eine endliche Gruppe hat nur endlichviele Untergruppen. Auch wie die verschiedenen Körper ineinander geschachtelt sind, ist aus den Gruppen zu erkennen; denn es gilt der Satz:

Ist Δ_1 Unterkörper von Δ_2, so ist die zu Δ_1 gehörige Gruppe $\mathfrak{g}_1$ Obergruppe der zu Δ_2 gehörigen Gruppe $\mathfrak{g}_2$, und umgekehrt.

Beweis: Es sei erstens $\Delta_1 \subseteq \Delta_2$. Dann wird jede Substitution, die alle Elemente von Δ_2 festläßt, auch alle Elemente von Δ_1 festlassen.

Es sei zweitens $\mathfrak{g}_1 \supseteq \mathfrak{g}_2$. Dann wird jedes Körperelement, das alle Substitutionen von $\mathfrak{g}_1$ gestattet, auch alle Substitutionen von $\mathfrak{g}_2$ gestatten.

Wir wollen zum Schluß noch die Frage stellen: Was geschieht mit der Galoisschen Gruppe von $\mathsf{K}(\Theta)$ in bezug auf K, wenn man den Grundkörper K zu einem Körper Λ und dementsprechend auch den Oberkörper $\mathsf{K}(\Theta)$ zu $\Lambda(\Theta)$ erweitert? (Wir setzen natürlich voraus, daß $\Lambda(\Theta)$ einen Sinn hat, d. h. daß Λ und Θ in einem gemeinsamen Oberkörper Ω enthalten sind).

Die Substitutionen $\Theta \to \Theta_\nu$, die nach der Erweiterung Automorphismen von $\Lambda(\Theta)$ ergeben, ergeben auch Isomorphismen von $\mathsf{K}(\Theta)$, mithin, da $\mathsf{K}(\Theta)$ Galoissch ist, Automorphismen von $\mathsf{K}(\Theta)$. *Daher ist die Substitutionsgruppe nach der Erweiterung des Grundkörpers eine Untergruppe der ursprünglichen.* Daß die Untergruppe eine echte sein kann, sieht man sofort, wenn man Λ speziell als Zwischenkörper von K und $\mathsf{K}(\Theta)$ wählt. Die Untergruppe kann aber auch mit der ursprünglichen zu-

sammenfallen; dann sagt man, daß die Erweiterung des Grundkörpers die Gruppe von $\mathsf{K}(\Theta)$ *nicht reduziert.*

Aufgaben. 1. Zum Durchschnitt zweier Untergruppen der Galoisschen Gruppe $\mathfrak{G}$ gehört der Vereinigungskörper der zu diesen Untergruppen gehörigen Körper, und zur Vereinigungsgruppe gehört der Durchschnittskörper[1].

2. Ist der Körper Σ in bezug auf K zyklisch vom Grade n, so gibt es zu jedem Teiler d von n genau einen Zwischenkörper Δ vom Grade d, und zwei solche Zwischenkörper sind dann und nur dann ineinander enthalten, wenn der Grad des einen durch den des anderen teilbar ist. [Vgl. § 7, Aufg. 11 und 12.]

3. Mit Hilfe der Galoisschen Theorie bestimme man von neuem die Unterkörper der $GF(p^n)$ (§ 31).

4. Es sei $\mathsf{K} \subseteq \Delta$, und Θ eine separable algebraische Größe über K in irgend einem Erweiterungskörper. Man zeige, daß die Gruppe von $\mathsf{K}(\Theta)$ nach K dann und nur dann gleich der von $\Delta(\Theta)$ nach Δ ist, wenn $\mathsf{K}(\Theta) \cap \Delta = \mathsf{K}$ ist.

5. Mit Hilfe des Satzes von § 44 zeige man:

Der Körper $\mathsf{K}(\alpha_1)$, der durch Adjunktion einer Wurzel einer irreduziblen algebraischen Gleichung entsteht, besitzt dann und nur dann einen Unterkörper Δ, so daß

$$\mathsf{K} \subset \Delta \subset \mathsf{K}(\alpha_1),$$

wenn die Galoissche Gruppe der Gleichung, als Permutationsgruppe der Wurzeln aufgefaßt, imprimitiv ist. Insbesondere kann dann Δ so bestimmt werden, daß der Körpergrad (Δ/K) gleich der Anzahl der Imprimitivitätsgebiete ist und die Gleichung in Δ in irreduzible Faktoren zerfällt, die den Imprimitivitätsgebieten entsprechen.

6. Man zeige, daß der Hauptsatz auch für inseparable Erweiterungen (Charakteristik p) gilt mit folgenden Modifikationen. Behauptung 2 wird: Die Gesamtheit der Elemente von Σ, welche die Substitutionen von $\mathfrak{g}$ gestatten, ist der „Wurzelkörper von Δ in Σ", d. h. die Gesamtheit der Elemente von Σ, von denen eine p^t-te Potenz zu Δ gehört. Behauptung 3 wird: Zu jeder Untergruppe von $\mathfrak{g}$ kann man genau einen Körper Δ finden, der gegenüber der Operation des Ausziehens der p-ten Wurzel invariant ist und die Substitutionen von $\mathfrak{g}$ und nur diese gestattet. Behauptung 4 gilt für die reduzierten Grade.

§ 47. Konjugierte Gruppen, Körper und Körperelemente.

Es sei wieder $\mathfrak{G}$ die Galoissche Gruppe von Σ nach K, und es sei β ein Element von Σ. Die Untergruppe $\mathfrak{g}$, die zum Zwischenkörper $\mathsf{K}(\beta)$

[1] Die Vereinigungsgruppe zweier Untergruppen bedeutet die durch die Vereinigungsmenge erzeugte Gruppe. Entsprechend definiert man den Begriff Vereinigungskörper.

gehört, besteht aus den Substitutionen, die β invariant lassen. Die übrigen Substitutionen von $\mathfrak{G}$ transformieren β in die dazu konjugierten Größen, und jede konjugierte Größe kann so erhalten werden (§ 45). Wir behaupten nun weiter:

Die Substitutionen von $\mathfrak{G}$, die β in ein vorgegebenes konjugiertes Element transformieren, bilden eine Nebenklasse $\tau\mathfrak{g}$ von $\mathfrak{g}$, und jede Nebenklasse transformiert β in ein einziges konjugiertes Element.

Beweis: Sind ϱ und τ Substitutionen, die β in dasselbe konjugierte Element überführen:

$$\varrho(\beta) = \tau(\beta),$$

so folgt

$$\tau^{-1}\varrho(\beta) = \tau^{-1}\tau(\beta) = \beta;$$

also ist $\tau^{-1}\varrho = \sigma$ ein Element von $\mathfrak{g}$, und es folgt $\varrho = \tau\sigma$; mithin liegen ϱ und τ in derselben Nebenklasse $\tau\mathfrak{g}$. Liegen umgekehrt ϱ und τ in derselben Nebenklasse, also beide in $\tau\mathfrak{g}$, so ist $\varrho = \tau\sigma$, wobei σ in $\mathfrak{g}$ liegt; mithin ist

$$\varrho(\beta) = \tau\sigma(\beta) = \tau(\sigma(\beta)) = \tau(\beta).$$

Aus diesem Satz folgt von neuem, daß der Grad von β (= Anzahl der Konjugierten) gleich dem Index von $\mathfrak{g}$ (= Anzahl der Nebenklassen) ist.

Ein Automorphismus τ, der β in $\tau\beta$ überführt, führt $\mathsf{K}(\beta)$ in den konjugierten Körper $\mathsf{K}(\tau\beta)$ über. Wir behaupten: *Der Körper $\mathsf{K}(\tau\beta)$ gehört zur Untergruppe $\tau\mathfrak{g}\tau^{-1}$.*

Denn die zu $\mathsf{K}(\tau\beta)$ gehörige Untergruppe besteht aus den Substitutionen σ', welche $\tau\beta$ invariant lassen, für die also gilt

$$\sigma'\tau\beta = \tau\beta$$

oder

$$\tau^{-1}\sigma'\tau\beta = \beta$$

oder

$$\tau^{-1}\sigma'\tau = \sigma \qquad \text{in } \mathfrak{g}$$

oder

$$\sigma' = \tau\sigma\tau^{-1},$$

d. h. es ist genau die Gruppe $\tau\mathfrak{g}\tau^{-1}$.

Zu konjugierten Körpern gehören demnach konjugierte Gruppen.

Nach § 45 ist ein Körper Δ über K dann und nur dann Galoissch, wenn er mit allen seinen konjugierten Körpern identisch ist. Daraus folgt nunmehr:

Ein Körper Δ, $\mathsf{K} \subseteq \Delta \subseteq \Sigma$, ist dann und nur dann Galoissch, wenn die zugehörige Gruppe $\mathfrak{g}$ mit allen ihren Konjugierten $\tau\mathfrak{g}\tau^{-1}$ in $\mathfrak{G}$ identisch, d. h. Normalteiler in $\mathfrak{G}$ ist.

Wenn nun Δ Galoissch ist, so drängt sich die Frage auf: Welches ist die Gruppe von Δ in bezug auf K?

Jeder Automorphismus aus $\mathfrak{G}$ transformiert Δ in sich selbst und bewirkt also einen Automorphismus der gesuchten Gruppe von Δ

über K. Dem Produkt zweier Automorphismen aus $\mathfrak{G}$ entspricht dabei wieder das Produkt der entsprechenden Automorphismen von Δ, also ist $\mathfrak{G}$ auf die Gruppe von Δ homomorph abgebildet. Die Elemente aus $\mathfrak{G}$, denen die Einheitssubstitution von Δ entspricht, sind gerade die von $\mathfrak{g}$; daraus folgt nach dem Homomorphiesatz (§ 9), daß die gesuchte Gruppe 1-isomorph zur Faktorgruppe $\mathfrak{G}/\mathfrak{g}$ ist. Mithin:

Die Galoissche Gruppe von Δ in bezug auf K ist isomorph zur Faktorgruppe $\mathfrak{G}/\mathfrak{g}$.

Aufgaben. 1. Alle Unterkörper eines Abelschen Körpers sind Galoissch und selbst wieder Abelsch. Alle Unterkörper eines zyklischen Körpers sind wieder zyklisch.

2. Ist $\mathsf{K} \subseteq \Delta \subseteq \Sigma$, und Λ der zu Δ gehörige kleinste Galoissche Körper in bezug auf K, so ist die zu Λ gehörige Gruppe der Durchschnitt der zu Δ gehörigen Gruppe mit ihren konjugierten Gruppen.

3. Welches sind die Unterkörper des Körpers $\Gamma(\varrho, \sqrt[3]{2})$, wo Γ der rationale Grundkörper, $\varrho = \frac{1-\sqrt{-3}}{2}$ eine primitive dritte Einheitswurzel ist? Welches sind die Körpergrade? Welche Unterkörper sind konjugiert, welche normal?

4. Dieselben Fragen für den Körper $\Gamma(\sqrt{2}, \sqrt{5})$.

§ 48. Kreisteilungskörper.

Es sei Γ der Körper der rationalen Zahlen, also der Primkörper von der Charakteristik Null. Die Gleichung, die genau die primitiven h-ten Einheitswurzeln, jede einmal gezählt, zu Wurzeln hat:

$$\Phi_h(x) = 0 \tag{1}$$

(vgl. § 30), heißt in diesem Falle die *Kreisteilungsgleichung*, und der Körper der h-ten Einheitswurzeln heißt *Kreisteilungskörper* oder *Kreiskörper*. Das hat folgenden Grund: Die komplexe Zahl

$$\zeta = e^{\frac{2\pi i}{h}} = \cos\frac{2\pi}{h} + i \sin\frac{2\pi}{h}$$

ist eine primitive h-te Einheitswurzel; aus ihr bestimmt sich $\cos\frac{2\pi}{h}$ nach der Gleichung

$$2\cos\frac{2\pi}{h} = \zeta + \zeta^{-1},$$

und die Kenntnis dieses Cosinus gestattet die Konstruktion des regelmäßigen h-Ecks, also die Teilung des Kreises in h gleiche Bogen.

Die folgende Theorie der Kreiskörper gilt natürlich unabhängig davon, ob man die primitive Einheitswurzel ζ als komplexe Zahl deutet oder als bloßes Symbol auffaßt.

Es handelt sich zunächst darum, zu zeigen, daß die Gleichung (1) in Γ irreduzibel ist.

Die irreduzible Gleichung, der eine beliebig gewählte primitive Einheitswurzel ζ genügt, sei $f(x) = 0$. Das Polynom $f(x)$ ist Teiler von $x^h - 1$; zu zeigen ist $f(x) = \Phi_h(x)$.

Es sei nun p eine Primzahl, die in h nicht aufgeht. Dann ist mit ζ auch ζ^p eine primitive h-te Einheitswurzel und genügt einer irreduziblen Gleichung $g(x) = 0$. Wir normieren f und g so, daß der Koeffizient der höchsten vorkommenden Potenz von x gleich 1 wird, und wollen nun zunächst zeigen: $f(x) = g(x)$.

Wären $f(x)$ und $g(x)$ verschieden, so wäre $x^h - 1$ teilbar durch beide, also durch das Produkt $f(x) \cdot g(x)$. Die rationale Polynomzerlegung

$$x^h - 1 = f(x) \cdot g(x) \cdot h(x)$$

kann nach dem Gaußschen Satz (§ 21) ganzzahlig angenommen werden. Weiter hat man

$$f(\zeta) = 0, \qquad g(\zeta^p) = 0;$$

also haben $f(x)$ und $g(x^p)$ eine Wurzel gemein, also einen rationalen Faktor gemein, der wieder ganz-rational angenommen werden kann.

Alle Gleichungen zwischen ganzzahligen Polynomen gelten auch modulo p. Also haben $f(x)$ und $g(x^p)$ auch modulo p einen Faktor gemein. Nun ist aber modulo p:

$$g(x^p) \equiv \{g(x)\}^p;$$

denn wenn man die Potenzierung rechts wirklich ausführt, wobei $g(x)$ als algebraische Summe von Potenzprodukten ohne Koeffizienten gedacht werden mag (indem man etwa $2x_1^2 x_2$ als $x_1^2 x_2 + x_1^2 x_2$ ausschreibt), so bleiben nur die p-ten Potenzen stehen, und diese bilden $g(x^p)$. Demnach haben $f(x)$ und $\{g(x)\}^p \pmod p$ mindestens einen mod p irreduziblen Faktor $\varphi(x)$ gemein. Wenn aber $g(x)^p$ mod p durch $\varphi(x)$ teilbar ist, so muß auch $g(x)$ selbst (mod p) den Faktor $\varphi(x)$ enthalten, da ja für Polynome mit Koeffizienten aus dem Körper $C/(p)$ nach § 17 der Satz von der eindeutigen Faktorzerlegung gilt. Schließlich ist $x^h - 1$ durch das Produkt $f(x) \cdot g(x)$ teilbar, also modulo p durch das Quadrat des Faktors $\varphi(x)$. Somit hätte $x^h - 1$ modulo p mit seiner Ableitung einen Faktor gemein. Die Ableitung $h x^{h-1}$ aber verschwindet (wegen $h \not\equiv 0 (p)$) nicht; überdies hat sie als Faktoren nur Potenzen von x, die nicht in $x^h - 1$ aufgehen. Wir sind damit auf einen Widerspruch gestoßen.

Also ist in der Tat $f(x) = g(x)$ und ζ^p Nullstelle von $f(x)$.

Wir wollen nun weiter zeigen: Alle primitiven Einheitswurzeln sind Nullstellen von $f(x)$. Es sei ζ^ν eine primitive Einheitswurzel und

$$\nu = p_1 \dots p_n,$$

wo die p_i gleiche oder verschiedene Primfaktoren, aber sicher zu h teilerfremd sind.

Da ζ der Gleichung $f(x) = 0$ genügt, so muß nach dem eben Bewiesenen auch ζ^{p_1} es tun. Wiederholung des Schlusses für die Primzahl p_2 lehrt, daß auch $\zeta^{p_1 p_2}$ es tut. So weiterschließend, finden wir (vollständige Induktion!), daß ζ^{ν} der Gleichung $f(x) = 0$ genügt.

Alle Nullstellen von $\Phi_h(x)$ genügen also der Gleichung $f(x) = 0$; da $f(x)$ irreduzibel war, so folgt

$$\Phi_h(x) = f(x).$$

Damit ist die *Irreduzibilität der Kreisteilungsgleichung* bewiesen[1].

Auf Grund dieser einen Tatsache können wir die Galoissche Gruppe des Kreisteilungskörpers $\Gamma(\zeta)$ mühelos konstruieren.

Zunächst ist der Körpergrad gleich dem Grad von $\Phi_h(x)$, also gleich $\varphi(h)$ (vgl. § 30). Ein Automorphismus von $\Gamma(\zeta)$ wird dadurch gegeben, daß ζ in eine andere Nullstelle von $\Phi_h(x)$ übergeht. Nullstellen von $\Phi_h(x)$ sind alle Potenzen ζ^{λ}, wo λ zu h teilerfremd ist. Es sei σ_λ der Automorphismus, der ζ in ζ^{λ} überführt. Dann und nur dann ist

$$\sigma_\lambda = \sigma_\mu,$$

wenn

$$\zeta^{\lambda} = \zeta^{\mu}$$

oder

$$\lambda \equiv \mu \ (h)$$

ist. Weiter ist:

$$\sigma_\lambda \sigma_\mu(\zeta) = \sigma_\lambda(\zeta^{\mu}) = \{\sigma_\lambda(\zeta)\}^{\mu} = \zeta^{\lambda\mu},$$

also

$$\sigma_\lambda \sigma_\mu = \sigma_{\lambda\mu}.$$

Die Automorphismengruppe von $\Gamma(\zeta)$ ist demnach isomorph zur Gruppe der zu h teilerfremden Restklassen mod h. (Vgl. § 17, Aufg. 6.)

Die Gruppe ist insbesondere Abelsch. Folglich sind alle Untergruppen Normalteiler und alle Unterkörper Galoissch und Abelsch.

Beispiel: die 12-ten Einheitswurzeln. Die zu 12 relativ-primen Restklassen werden repräsentiert durch

$$1, 5, 7, 11.$$

Die Automorphismen können demnach mit $\sigma_1, \sigma_5, \sigma_7, \sigma_{11}$ bezeichnet werden, wobei ζ durch den Automorphismus σ_λ in ζ^{λ} übergeführt wird. Die Multiplikationstafel lautet:

σ_1	σ_5	σ_7	σ_{11}
σ_5	σ_1	σ_{11}	σ_7
σ_7	σ_{11}	σ_1	σ_5
σ_{11}	σ_7	σ_5	σ_1

[1] Für andere einfache Beweise siehe z. B. E. LANDAU und unmittelbar darauffolgend I. SCHUR in der Math. Zeitschr. Bd. 29. 1929.

Jedes Element hat die Ordnung 2. Außer der Gruppe selbst und der Einheitsgruppe gibt es also genau drei Untergruppen:

$$1. \quad \{\sigma_1, \sigma_5\},$$
$$2. \quad \{\sigma_1, \sigma_7\},$$
$$3. \quad \{\sigma_1, \sigma_{11}\}.$$

Zu diesen drei Gruppen gehören quadratische Körper, erzeugt durch Quadratwurzeln. Um diese zu finden, überlegen wir uns folgendes:

Die vierten Einheitswurzeln i, $-i$ sind auch zwölfte Einheitswurzeln, liegen also im Körper. Also ist $\Gamma(i)$ ein quadratischer Unterkörper.

Ebenso liegen die dritten Einheitswurzeln im Körper. Da

$$\varrho = -\tfrac{1}{2} + \tfrac{1}{2}\sqrt{-3}$$

eine dritte Einheitswurzel ist, so ist $\Gamma(\sqrt{-3})$ ein quadratischer Unterkörper.

Aus den beiden Quadratwurzeln i und $\sqrt{-3}$ erhält man durch Multiplikation $\sqrt{3}$. Also ist $\Gamma(\sqrt{3})$ der dritte Unterkörper.

Wir fragen nun, welche Untergruppen zu diesen drei Körpern gehören.

Wegen $\sigma_5 \zeta^3 = \zeta^{15} = \zeta^3$ gestattet $i = \zeta^3$ den Automorphismus σ_5. Also gehört $\Gamma(i)$ zur Gruppe $\{\sigma_1, \sigma_5\}$.

Wegen $\sigma_7 \zeta^4 = \zeta^{28} = \zeta^4$ gestattet $\varrho = \zeta^4$ den Automorphismus σ^7. Somit gehört $\Gamma(\sqrt{-3})$ zur Gruppe $\{\sigma_1, \sigma_7\}$.

Der übrigbleibende Körper $\Gamma(\sqrt{3})$ muß zur Gruppe $\{\sigma_1, \sigma_{11}\}$ gehören.

Je zwei der drei Unterkörper erzeugen den ganzen. Also muß sich die Einheitswurzel ζ durch zwei Quadratwurzeln ausdrücken lassen. In der Tat ist:

$$\zeta = \zeta^{-3}\zeta^4 = i^{-1}\varrho = -i\,\frac{-1+\sqrt{-3}}{2} = \frac{i-\sqrt{3}}{2}.$$

Wie man für Kreisteilungskörper mit Primzahlexponenten die Unterkörper explizit bestimmen und den Kreiskörper selbst aus diesen Unterkörpern durch sukzessive Adjunktionen aufbauen kann, werden wir im nächsten Paragraphen sehen.

Aufgaben. 1. Die Größe $\zeta + \zeta^{-1}$ erzeugt für $h > 2$ stets einen Unterkörper vom Grad $\frac{1}{2}\varphi(h)$.

2. Man bestimme Gruppe und Unterkörper des Körpers der 5-ten Einheitswurzeln, und drücke diese durch Quadratwurzeln aus. Ebenso für die 8-ten Einheitswurzeln.

3. Man bestimme die Gruppe und die Unterkörper des Körpers der 7-ten Einheitswurzeln. Was ist die definierende Gleichung des Körpers $\Gamma(\zeta + \zeta^{-1})$?

§ 49. Die Perioden der Kreisteilungsgleichung.

Der Exponent h der betrachteten Einheitswurzeln sei jetzt eine Primzahl q. Die Kreisteilungsgleichung lautet in diesem Fall

$$\Phi_q(x) = \frac{x^q - 1}{x - 1} = x^{q-1} + x^{q-2} + \cdots + x + 1 = 0.$$

Sie hat den Grad $n = q - 1$.

Es sei ζ eine primitive q-te Einheitswurzel.

Die Gruppe der zu q teilerfremden Restklassen ist zyklisch (§ 31), besteht demnach aus den n Restklassen

$$1,\ g,\ g^2,\ \ldots,\ g^{n-1},$$

wo g eine „Primitivzahl mod q" oder eine primitive Wurzel der Kongruenz $g^n \equiv 1\,(q)$ ist. *Die Galoissche Gruppe ist demnach auch zyklisch* und wird erzeugt von demjenigen Automorphismus σ, der ζ in ζ^g überführt. Die primitiven Einheitswurzeln lassen sich folgendermaßen darstellen:

$$\zeta,\ \zeta^g,\ \zeta^{g^2},\ \ldots,\ \zeta^{g^{n-1}},\quad \text{wo } \zeta^{g^n} = \zeta.$$

Wir setzen

$$\zeta^{g^\nu} = \zeta_\nu,$$

wobei mit den Zahlen ν modulo n gerechnet werden kann wegen

$$\zeta^{g^{\nu+n}} = \zeta^{g^\nu}.$$

Es ist

$$\sigma(\zeta_i) = \sigma(\zeta^{g^i}) = \{\sigma(\zeta)\}^{g^i} = (\zeta^g)^{g^i} = \zeta^{g^{i+1}} = \zeta_{i+1}.$$

Der Automorphismus σ erhöht also jeden Index um 1. Die ν-fache Wiederholung von σ ergibt

$$\sigma^\nu(\zeta_i) = \zeta_{i+\nu}.$$

Die $\zeta_i (i = 0, 1, \ldots, n-1)$ bilden eine Körperbasis. Um das zu erkennen, haben wir bloß zu zeigen, daß sie linear-unabhängig sind. In der Tat, die ζ_i stimmen bis auf die Reihenfolge mit den $\zeta, \ldots, \zeta^{q-1}$ überein; eine lineare Relation zwischen ihnen würde also bedeuten:

$$a_1\zeta + \cdots + a_{q-1}\zeta^{q-1} = 0,$$

oder nach Heraushebung eines Faktors ζ:

$$a_1 + a_2\zeta + \cdots + a_{q-1}\zeta^{q-2} = 0.$$

Daraus folgt, da ζ keiner Gleichung vom Grade $\leqq q - 2$ genügen kann:

$$a_1 = a_2 = \cdots = a_{q-1} = 0;$$

die ζ_i sind also linear-unabhängig.

Die Unterkörper des Kreisteilungskörpers ergeben sich sofort aus den Untergruppen der zyklischen Gruppe (vgl. § 7, Aufg. 11 und 12):

Ist

$$e f = n$$

eine Zerlegung von n in zwei positive Faktoren, so existiert eine Untergruppe $\mathfrak{g}$ *der Ordnung f, bestehend aus den Elementen*

$$\sigma^e,\ \sigma^{2e},\ \ldots,\ \sigma^{(f-1)e},\ \sigma^{fe},$$

wobei σ^{fe} *das Einselement ist. Diese Untergruppen sind die einzigen.*

Wir suchen nun die Elemente α, die σ^e (also auch die Untergruppe $\mathfrak{g}$) gestatten. Ist

$$\alpha = a_0\zeta_0 + \cdots + a_{n-1}\zeta_{n-1}, \tag{1}$$

so ist

$$\sigma^e(\alpha) = a_0\zeta_e + a_1\zeta_{e+1} + \cdots + a_{n-1}\zeta_{e+n-1}.$$

Soll dies gleich α sein, so muß sein

$$\begin{aligned} a_0 &= a_e, \\ &\cdots\cdots \\ a_\nu &= a_{e+\nu}, \\ &\cdots\cdots \\ a_{n-1} &= a_{e+n-1}, \end{aligned}$$

womit den Indizes modulo n gerechnet werden muß. Es folgt

$$a_\nu = a_{\nu+e} = a_{\nu+2e} = \cdots;$$

also kann man in (1) die Glieder zu Gruppen

$$a_\nu(\zeta_\nu + \zeta_{\nu+e} + \cdots)$$

zusammenfassen. Wir setzen deshalb

$$\eta_\nu = \zeta_\nu + \zeta_{\nu+e} + \zeta_{\nu+2e} + \cdots + \zeta_{\nu+(f-1)e} \qquad (\nu = 0, \ldots, e-1) \tag{2}$$

und schreiben für (1):

$$\alpha = a_0\eta_0 + a_1\eta_1 + \cdots + a_{e-1}\eta_{e-1}.$$

Daraus liest man ab, daß die η_i eine Basis für den zu $\mathfrak{g}$ gehörigen Unterkörper bilden.

Es ist

$$\begin{aligned} \sigma(\eta_0) &= \eta_1, \\ &\cdots\cdots \\ \sigma^\nu(\eta_0) &= \eta_\nu; \end{aligned}$$

also sind $\eta_0, \eta_1, \ldots$ konjugiert und das Polynom

$$(x - \eta_0)(x - \eta_1)\ldots(x - \eta_{e-1}) \tag{3}$$

irreduzibel.

Da der Körper $\Gamma(\eta_0)$, wie jeder Unterkörper, Galoissch ist, so zerfällt in ihm das Polynom (3) vollständig; daraus folgt

$$\Gamma(\eta_0) = \Gamma(\eta_0, \ldots, \eta_{e-1});$$

der betrachtete Unterkörper wird also schon von η_0 erzeugt.

Die durch (2) definierten Größen $\eta_0, \ldots, \eta_{e-1}$ heißen nach Gausz die *f-gliedrigen Perioden* des Kreiskörpers.

Gausz hat eine Formel angegeben, die es gestattet, ein Produkt $\eta_i \eta_k$ bequem zu berechnen. Er führt die neue Bezeichnung

$$\begin{aligned}\eta^{(r)} &= \zeta^r + \zeta^{r g^e} + \cdots + \zeta^{r g^{(f-1)e}} \\ &= \sum_{\nu \bmod f} \zeta^{r g^{\nu e}}\end{aligned}$$

ein (wo die Bezeichnung „ν mod f" bedeutet, daß ν ein Repräsentantensystem der Restklassen nach f durchläuft). $\eta^{(r)}$ ist also für $r \not\equiv 0 \pmod q$ dasjenige η_ν, in welchem ein Glied ζ^r vorkommt. Man bemerkt, daß

$$\eta^{(r g^e)} = \eta^{(r)}$$

und

$$\eta^{(0)} = 1 + \cdots + 1 = f$$

ist. Multiplikation zweier $\eta^{(r)}$ ergibt nun:

$$\eta^{(r)} \eta^{(s)} = \sum_{\nu \bmod f} \left(\sum_{\mu \bmod f} \zeta^{r g^{\nu e} + s g^{\mu e}} \right)$$

oder mit $\mu = \mu' + \nu$

$$\begin{aligned}\eta^{(r)} \eta^{(s)} &= \sum_{\nu \bmod f} \left(\sum_{\mu' \bmod f} \zeta^{r g^{\nu e} + s g^{(\mu' + \nu) e}} \right) \\ &= \sum_{\mu' \bmod f} \left(\sum_{\nu \bmod f} \zeta^{(r + s g^{\mu' e}) g^{\nu e}} \right).\end{aligned}$$

Die in der Klammer stehende Größe ist $\eta^{(r + s g^{\mu' e})}$; mithin folgt, wenn wieder μ statt μ' geschrieben wird:

$$\eta^{(r)} \eta^{(s)} = \sum_{\mu \bmod f} \eta^{(r + s g^{\mu e})} \qquad \text{(Formel von Gausz).}$$

Die Indizes der η in dieser Summe stimmen mit den Exponenten überein, die man erhält, wenn man das erste Glied von $\eta^{(r)}$ mit allen Gliedern von $\eta^{(s)}$ multipliziert.

Aus

$$\zeta + \zeta^2 + \cdots + \zeta^{q-1} = -1$$

folgt noch

$$\eta_0 + \eta_1 + \cdots + \eta_{e-1} = -1,$$

mithin

$$\eta^{(0)} = f = -f(\eta_0 + \cdots + \eta_{e-1}).$$

Damit kann man jedes in der Gaußschen Formel rechts auftretende $\eta^{(0)}$ wegschaffen. Beachtet man, daß die übrigen $\eta^{(j)}$ bis auf die Reihenfolge

mit den Größen $\eta_0, \ldots, \eta_{e-1}$ übereinstimmen, so erhält man also für jedes Produkt $\eta_i \eta_k$ eine Darstellung als Summe von ganzzahligen Vielfachen der η_j.

Beispiel: $q = 17$. Die Zahl 3 ist eine Primitivwurzel; denn die Potenzen von 3 sind modulo 17 die folgenden:

Indizes (Exponenten):	0	1	2	3	4	5	6	7	8	9	10	11
Numeri (Potenzen):	1	3	−8	−7	−4	5	−2	−6	−1	−3	8	7
Indizes (Exponenten):	12	13	14	15	16							
Numeri (Potenzen):	4	−5	2	6	1							

Wir berechnen zunächst die 8-*gliedrigen Perioden* ($e = 2$, $f = 8$):

$$\eta_0 = \zeta + \zeta^{-8} + \zeta^{-4} + \zeta^{-2} + \zeta^{-1} + \zeta^{8} + \zeta^{4} + \zeta^{2},$$
$$\eta_1 = \zeta^{3} + \zeta^{-7} + \zeta^{5} + \zeta^{-6} + \zeta^{-3} + \zeta^{7} + \zeta^{-5} + \zeta^{6}.$$

Es ist $\eta_0 + \eta_1 = -1$ und nach der Gaußschen Formel (wegen $\eta_0 = \eta^{(1)}$, $\eta_1 = \eta^{(3)}$):

$$\eta_0 \eta_1 = \eta^{(4)} + \eta^{(-6)} + \eta^{(6)} + \eta^{(-5)} + \eta^{(-2)} + \eta^{(8)} + \eta^{(-4)} + \eta^{(7)}.$$

Nun ist $\eta^{(r)}$ immer dasjenige η_ν, in dem ζ^r vorkommt. Also ist

$$\eta^{(4)} = \eta^{(-2)} = \eta^{(8)} = \eta^{(-4)} = \eta_0,$$

und

$$\eta^{(-6)} = \eta^{(6)} = \eta^{(-5)} = \eta^{(7)} = \eta_1,$$

mithin

$$\eta_0 \eta_1 = 4\eta_0 + 4\eta_1 = -4.$$

Also sind η_0 und η_1 die Wurzeln der Gleichung

$$y^2 + y - 4 = 0, \tag{4}$$

deren Lösung lautet:

$$y = -\frac{1}{2} \pm \frac{1}{2}\sqrt{17}.$$

Die 4-*gliedrigen Perioden* ($e = 4$, $f = 4$) sind:

$$\xi_0 = \zeta + \zeta^{-4} + \zeta^{-1} + \zeta^{4},$$
$$\xi_1 = \zeta^{3} + \zeta^{5} + \zeta^{-3} + \zeta^{-5},$$
$$\xi_2 = \zeta^{-8} + \zeta^{-2} + \zeta^{8} + \zeta^{2},$$
$$\xi_3 = \zeta^{-7} + \zeta^{-6} + \zeta^{7} + \zeta^{6}.$$

Es ist

$$\xi_0 + \xi_2 = \eta_0,$$
$$\xi_1 + \xi_3 = \eta_1.$$

Um für ξ_0 und ξ_2 eine Gleichung zu finden, berechnen wir

$$\xi_0 \xi_2 = \xi^{(-7)} + \xi^{(-1)} + \xi^{(-8)} + \xi^{(3)}$$
$$= \xi_3 + \xi_0 + \xi_2 + \xi_1$$
$$= -1.$$

Also genügen ξ_0 und ξ_2 der Gleichung

$$x^2 - \eta_0 x - 1 = 0. \tag{5}$$

Ebenso genügen ξ_1 und ξ_3 der Gleichung

$$x^2 - \eta_1 x - 1 = 0. \tag{6}$$

Diese Gleichungen bringen zum Ausdruck, was wir von vornherein wußten, daß $\Gamma(\xi_0)$ quadratisch in bezug auf $\Gamma(\eta_0)$ ist.

Zwei 2-*gliedrige Perioden* sind

$$\lambda^{(1)} = \zeta + \zeta^{-1},$$
$$\lambda^{(4)} = \zeta^4 + \zeta^{-4}.$$

Addition und Multiplikation ergeben:

$$\lambda^{(1)} + \lambda^{(4)} = \xi_0,$$
$$\lambda^{(1)}\lambda^{(4)} = \zeta^5 + \zeta^{-3} + \zeta^3 + \zeta^{-5} = \xi_1.$$

Also genügen $\lambda^{(1)}$ und $\lambda^{(4)}$ der Gleichung

$$\Lambda^2 - \xi_0 \Lambda + \xi_1 = 0. \tag{7}$$

Schließlich genügt ζ selbst der Gleichung

$$\zeta + \zeta^{-1} = \lambda^{(1)}$$

oder

$$\zeta^2 - \lambda^{(1)}\zeta + 1 = 0.$$

Damit sind die 17-ten Einheitswurzeln durch quadratische Gleichungen ausgerechnet.

Deutet man insbesondere die 17-ten Einheitswurzeln als Zahlen, so kann man setzen:

$$\zeta = e^{\frac{2\pi i}{17}},$$

$$\lambda^{(1)} = \zeta + \zeta^{-1} = 2\cos\frac{2\pi}{17}.$$

Die Gleichung (4) hat eine positive und eine negative Wurzel; da nun

$$\eta_0 = (\zeta + \zeta^{-1}) + (\zeta^8 + \zeta^{-8}) + (\zeta^4 + \zeta^{-4}) + (\zeta^2 + \zeta^{-2})$$
$$= 2\left(\cos\frac{2\pi}{17} + \cos\frac{16\pi}{17} + \cos\frac{8\pi}{17} + \cos\frac{4\pi}{17}\right) > 2\left(\frac{1}{2} - 1 + 0 + \frac{1}{2}\right) = 0$$

ist, so ist η_0 die positive Wurzel:

$$\eta_0 = -\frac{1}{2} + \frac{1}{2}\sqrt{17}.$$

Ebenso haben (5) und (6) je eine positive und eine negative Wurzel; da

$$\xi_0 = 2\left(\cos\frac{2\pi}{17} + \cos\frac{8\pi}{17}\right) > 0,$$

$$\xi_3 = 2\left(\cos\frac{14\pi}{17} + \cos\frac{12\pi}{17}\right) < 0$$

ist, so sind ξ_0 und ξ_1 die positiven Wurzeln von (5) und (6). Schließlich ist

$$\lambda^{(1)} = 2\cos\frac{2\pi}{17} > 2\cos\frac{8\pi}{17} = \lambda^{(4)}$$

die größere der beiden (positiven) Wurzeln von (7). Mit Hilfe dieser Formeln läßt sich die *Konstruktion des regulären 17-Ecks* mit Zirkel und Lineal ausführen (vgl. § 54).

Aufgaben. 1. Man führe die Konstruktion des 17-Ecks wirklich aus.

2. Man beweise für die $\frac{p-1}{2}$-gliedrigen Perioden η_0 und η_1 allgemein die Relationen:

$$\eta_0 + \eta_1 = -1$$

$$\eta_0\eta_1 = \frac{1+p}{4} \text{ für } p \equiv -1\,(4),$$

$$\eta_0\eta_1 = \frac{1-p}{4} \text{ für } p \equiv 1\,(4),$$

und leite daraus eine quadratische Gleichung für η_0 her.

3. Das η_0 von Aufg. 2 ist die „Gaußsche Summe“:

$$\eta_0 = \sum_{s=1}^{\frac{p-1}{2}} \zeta^{s^2}.$$

§ 50. Zyklische Körper und reine Gleichungen.

Es sei K ein Grundkörper, der die n-ten Einheitswurzeln enthält und in welchem das n-fache des Einselementes nicht die Null ist (d. h. n nicht teilbar durch die Charakteristik). Dann behaupten wir: *Die Gruppe einer „reinen“ Gleichung*

$$x^n - a = 0 \qquad (a \neq 0)$$

in bezug auf K *ist zyklisch.*

Beweis: Ist Θ eine Wurzel der Gleichung, so sind $\zeta\Theta, \zeta^2\Theta, \ldots, \zeta^{n-1}\Theta$ (wo ζ eine primitive n-te Einheitswurzel bedeutet) die übrigen[1]. Daher erzeugt Θ schon den Körper der Wurzeln, und jede Substitution der Galoisschen Gruppe hat die Gestalt

$$\Theta \to \zeta^\nu\Theta.$$

Die Zusammensetzung zweier Substitutionen $\Theta \to \zeta^\nu\Theta$ und $\Theta \to \zeta^\mu\Theta$ ergibt $\Theta \to \zeta^{\mu+\nu}\Theta$. Es entspricht also jeder Substitution eine bestimmte Einheitswurzel ζ^ν, und dem Produkt der Substitutionen das Produkt der Einheitswurzeln. Also ist die Galoissche Gruppe isomorph einer Untergruppe der Gruppe der n-ten Einheitswurzeln. Da die

[1] Offensichtlich sind die Wurzeln alle verschieden, mithin die Gleichung separabel.

letztere Gruppe zyklisch ist, ist auch jede ihrer Untergruppen und damit auch die Galoissche Gruppe zyklisch.

Ist speziell die Gleichung $x^n - a = 0$ irreduzibel, so sind alle Wurzeln $\zeta^\nu \Theta$, zu Θ konjugiert und daher die Galoissche Gruppe isomorph der vollen Gruppe der n-ten Einheitswurzeln. Ihre Ordnung ist in diesem Falle n.

Wir wollen nun umgekehrt zeigen, daß jeder zyklische Körper n-ten Grades über K durch Wurzeln reiner Gleichungen $x^n - a = 0$ erzeugt werden kann.

Es sei also $\Sigma = \mathsf{K}(\Theta)$ ein zyklischer Körper vom Grade n, σ die erzeugende Substitution der Galoisschen Gruppe, also $\sigma^n = 1$. Wir nehmen wieder an, daß der Grundkörper K die n-ten Einheitswurzeln enthält.

Ist ζ eine solche n-te Einheitswurzel, so bilden wir die „*Lagrangesche Resolvente*“:

$$(1) \qquad (\zeta, \Theta) = \Theta_0 + \zeta \Theta_1 + \cdots + \zeta^{n-1} \Theta_{n-1},$$

wo

$$\Theta_\nu = \sigma^\nu \Theta$$

gesetzt ist.

Bei der Substitution σ werden die Θ_ν zyklisch vertauscht:

$$\sigma \Theta_\nu = \Theta_{\nu+1} \qquad (\Theta_n = \Theta_0),$$

und die Resolvente (ζ, Θ) geht über in

$$\begin{aligned} \sigma(\zeta, \Theta) &= \Theta_1 + \zeta \Theta_2 + \cdots + \zeta^{n-2} \Theta_{n-1} + \zeta^{n-1} \Theta_0 \\ &= \zeta^{-1} (\Theta_0 + \zeta \Theta_1 + \zeta^2 \Theta_2 + \cdots + \zeta^{n-1} \Theta_{n-1}) \\ &= \zeta^{-1} (\zeta, \Theta). \end{aligned}$$

Daher bleibt die n-te Potenz $(\zeta, \Theta)^n$ bei der Substitution σ ungeändert; d. h. $(\zeta, \Theta)^n$ gehört dem Grundkörper K an.

Wir können $(\zeta, \Theta)^n$ rein formal aus (1) durch Potenzieren erhalten und finden einen Ausdruck von der Gestalt

$$(2) \qquad (\zeta, \Theta)^n = P_0 + \zeta P_1 + \cdots + \zeta^{n-1} P_{n-1},$$

wo die P_ν Polynome n-ten Grades in den Θ sind, welche nicht davon abhängen, welche Einheitswurzel ζ zugrunde gelegt wurde.

Multiplizieren wir (1) mit ζ^{-r} und summieren über alle ζ, so erhalten wir (unter Beachtung des letzten Satzes von § 30):

$$(3) \qquad \sum_\zeta \zeta^{-r} (\zeta, \Theta) = n \Theta_r.$$

Da nach Annahme die Zahl n nicht durch die Charakteristik des Körpers teilbar ist, läßt sich aus (3) die Größe Θ_r ausrechnen, sobald die (ζ, Θ) bekannt sind. Wegen (2) sind aber die (ζ, Θ) durch Ausziehung je einer n-ten Wurzel aus einer Größe des Grundkörpers K

zu erhalten. (Es ist nicht a priori ersichtlich, *welche* der n-ten Wurzeln die Größe (ζ, Θ) darstellt; es genügt aber, irgend eine zu adjungieren und sie hinterher eventuell mit einer Potenz von ζ zu multiplizieren.) Daraus erhalten wir das gesuchte Resultat:

Jeder zyklische Körper n-ten Grades läßt sich, wenn die n-ten Einheitswurzeln schon im Grundkörper liegen und n nicht durch die Charakteristik teilbar ist, durch Adjunktion von n-ten Wurzeln erzeugen.

Oft ist die Bemerkung nützlich, daß auch $(\zeta, \Theta) \cdot (\zeta^{-1}, \Theta)$ sich bei der Substitution σ nicht ändert, weil der erste Faktor dabei mit ζ^{-1}, der zweite mit ζ multipliziert wird. Demnach gehört auch

$$(\zeta, \Theta) \cdot (\zeta^{-1}, \Theta)$$

dem Grundkörper an. Von je zwei solchen „konjugierten" Resolventen braucht man daher nur eine zu adjungieren.

Schließlich gehört auch

$$(1, \Theta) = \Theta_0 + \Theta_1 + \cdots + \Theta_{n-1},$$

wie sofort ersichtlich, zu K.

Entsteht unser Körper Σ durch Adjunktion der Wurzeln $\xi_1, \ldots, \xi_m$ einer Gleichung $f(x) = 0$, so bewirkt σ eine Permutation dieser Wurzeln, also auch eine Permutation ihrer Nummern $1, 2, \ldots, m$, die, in Zyklen zerlegt, etwa so aussehen möge:

$$(1\,2 \ldots j)\,(j+1 \ldots l) \ldots$$

Die übrigen Permutationen der Galoisschen Gruppe sind die Potenzen der angeschriebenen und führen die Nummer 1 in $1, 2, 3, \ldots, j$ über. Nehmen wir nun an, daß die Gleichung $f(x) = 0$ irreduzibel ist, so sind alle Wurzeln konjugiert; mithin muß die Wurzel ξ_1 in alle anderen Wurzeln übergeführt werden können, d. h. der eine Zykel $(1\ 2 \ldots j)$ schon alle Wurzeln umfassen. Da die erzeugende Permutation des Zykels die Ordnung n haben muß, muß $j = n$ sein. Der Grad m der Gleichung ist also ebenfalls gleich n, also gleich dem Körpergrad; daher muß die Adjunktion einer Wurzel schon den ganzen Körper erzeugen. Numerieren wir die Wurzeln nun mit $0, 1, \ldots, n-1$ statt mit $1, 2, \ldots, n$, so können wir unsere Körpererzeugende $\Theta = \Theta_0$ gleich ξ_0 wählen; bei geeigneter Numerierung der übrigen Wurzeln wird dann automatisch $\Theta_1 = \sigma\Theta = \sigma\xi_0 = \xi_1$, $\Theta_2 = \sigma\Theta_1 = \sigma\xi_1 = \xi_2$, usw. *Für die Θ_ν in* (1) *können wir daher die Wurzeln von $f(x)$ in passender Numerierung wählen.*

Enthält der Grundkörper K nicht die n-ten Einheitswurzeln, so haben wir, um die obige Auflösungsmethode mittels n-ter Wurzeln anwenden zu können, zunächst die n-ten Einheitswurzeln ζ an K zu adjungieren. Bei dieser Adjunktion bleibt die Galoissche Gruppe zyklisch, da eine Untergruppe einer zyklischen Gruppe stets zyklisch ist.

Wir wollen nun noch einiges über die *Irreduzibilität der reinen Gleichungen vom Primzahlgrad p* beweisen.

Enthält zunächst wieder der Grundkörper K die p-ten Einheitswurzeln, so ist nach dem zu Anfang dieses Paragraphen Bewiesenen die Gruppe eine Untergruppe einer zyklischen Gruppe der Ordnung p und daher entweder die volle Gruppe oder die Einheitsgruppe. Im ersten Fall sind alle Wurzeln konjugiert, daher die Gleichung irreduzibel. Im zweiten Fall sind alle Wurzeln gegenüber den Substitutionen der Galoisschen Gruppe invariant; mithin zerfällt die Gleichung schon im Körper K in Linearfaktoren. Also: *Das Polynom $x^p - a$ zerfällt entweder ganz, oder es ist irreduzibel.*

Enthält K die Einheitswurzeln nicht, so läßt sich nicht so viel behaupten. Es gilt aber der Satz:

Entweder ist $x^p - a$ irreduzibel, oder a ist in K eine p-te Potenz, so daß in K eine Zerlegung

$$x^p - a = x^p - \beta^p = (x - \beta)(x^{p-1} + \beta x^{p-2} + \cdots + \beta^{p-1})$$

besteht.

Beweis: Nehmen wir an, $x^p - a$ sei reduzibel:

$$x^p - a = \varphi(x) \cdot \psi(x).$$

In seinem Zerfällungskörper zerfällt $x^p - a$ in folgender Weise:

$$x^p - a = \prod_{\nu=0}^{p-1} (x - \zeta^\nu \Theta) \qquad (\Theta^p = a).$$

Daher muß der eine Faktor $\varphi(x)$ ein Produkt von gewissen Faktoren $x - \zeta^\nu \Theta$ sein, und das von x unabhängige Glied b von $\varphi(x)$ muß die Form $\zeta' \Theta^\mu$ haben, wo ζ' eine p-te Einheitswurzel ist:

$$b = \zeta' \Theta^\mu,$$
$$b^p = \Theta^{p\mu} = a^\mu.$$

Wegen $0 < \mu < p$ ist $(\mu, p) = 1$, daher mit passenden ganzen rationalen Zahlen ϱ und σ:

$$\varrho\mu + \sigma p = 1,$$
$$a = a^{\varrho\mu} a^{\sigma p} = b^{\varrho p} a^{\sigma p};$$

a ist also eine p-te Potenz.

Interessante Sätze über die Reduzibilität der reinen Gleichungen enthalten die Arbeiten von A. CAPELLI: Sulla riducibilità dell'equazioni algebriche, Rendiconti Napoli 1898, und G. DARBI: Sulla riducibilità dell'equazioni algebriche, Annali di Mat. (4) 4 (1926).

Aufgabe. 1. Wenn nicht vorausgesetzt wird, daß der Grundkörper K die n-ten Einheitswurzeln enthält, so ist die Gruppe der reinen Gleichung $x^n - a = 0$ isomorph einer Gruppe von linearen Substitutionen modulo n:

$$x' \equiv cx + b.$$

[Der zugehörige Galoissche Körper ist $K(\Theta, \zeta)$ und für jede Substitution σ der Gruppe ist

$$\sigma\zeta = \zeta^c,$$
$$\sigma\Theta = \zeta^b\Theta].$$

§ 51. Die Auflösung von Gleichungen durch Radikale.

Bekanntlich lassen sich die Wurzeln einer Gleichung zweiten, dritten oder vierten Grades aus den Koeffizienten durch rationale Operationen und Wurzelzeichen $\sqrt{}$, $\sqrt[3]{}$, ... („Radikale") berechnen (vgl. § 53). Wir fragen nun, welche Gleichungen die Eigenschaft haben, daß ihre Wurzeln sich aus Größen eines Grundkörpers K durch rationale Operationen und Radikale ausdrücken lassen. Dabei können wir uns natürlich auf irreduzible Gleichungen mit Koeffizienten aus K beschränken. Die Aufgabe besteht darin, durch sukzessive Adjunktionen von Größen $\sqrt[n]{a}$ (wo a jeweils dem schon konstruierten Körper angehört) einen Körper über K zu konstruieren, der eine oder alle Wurzeln der vorgelegten Gleichung enthält.

Die Fragestellung ist aber in einem Punkt noch ungenau. Das Wurzelzeichen $\sqrt[n]{}$ ist in einem Körper im allgemeinen eine mehrdeutige Funktion, und es fragt sich, welche Wurzel jeweils mit $\sqrt[n]{a}$ gemeint ist. Wenn man z. B. eine primitive sechste Einheitswurzel durch Radikale ausdrückt, indem man sie einfach durch $\sqrt[6]{1}$ oder gar durch $\sqrt[12]{1}$ darstellt, wird man das als eine unbefriedigende Lösung anzusehen haben, während die Lösung $\zeta = \frac{1}{2} \pm \frac{1}{2}\sqrt{-3}$ viel befriedigender ist, weil der Ausdruck $\frac{1}{2} \pm \frac{1}{2}\sqrt{-3}$ bei *jeder* Wahl des Wertes von $\sqrt{-3}$ (d. h. einer Lösung der Gleichung $x^2 + 3 = 0$) die beiden primitiven sechsten Einheitswurzeln darstellt.

Die schärfste Forderung, die man in dieser Hinsicht stellen kann, ist die, daß man erstens *alle* Lösungen der fraglichen Gleichung durch Ausdrücke der Gestalt

$$\sqrt[n]{\dots\sqrt[m]{\dots} + \sqrt[r]{\dots} + \dots + \dots} \tag{1}$$

(oder ähnlich) darstellen soll und daß zweitens diese Ausdrücke auch bei *jeder* Wahl der in ihnen vorkommenden Radikale Lösungen der Gleichung darstellen sollen. (Dabei ist natürlich, wenn ein Radikal $\sqrt[m]{a}$ im Ausdruck (1) mehrmals vorkommt, dem stets derselbe Wert beizulegen.)

Nehmen wir an, die erste Forderung sei erfüllt. Dann wird die zweite auch erfüllt sein, sobald man dafür sorgen kann, daß bei der sukzessiven Adjunktion der Radikale $\sqrt[n]{a}$ im Augenblick einer solchen Adjunktion die jeweilige Gleichung $x^n - a = 0$ stets *irreduzibel* ist.

Denn dann werden alle möglichen Wahlen der $\sqrt[n]{a}$ stets konjugierte Größen ergeben, welche sich also durch Isomorphismen ineinander überführen lassen; wenn also bei einer Wertbestimmung dieser Radikale der Ausdruck (1) eine Wurzel der fraglichen Gleichung darstellt, so muß er bei jeder Wertbestimmung eine Wurzel der fraglichen Gleichung darstellen, da jeder Isomorphismus stets die Nullstellen eines Polynoms aus $\mathsf{K}[x]$ wieder in ebensolche Nullstellen überführt.

Nach diesen Vorbemerkungen sind wir imstande, den Hauptsatz über die durch Radikale lösbaren Gleichungen zu formulieren:

1. *Wenn auch nur eine Wurzel einer in* K *irreduziblen Gleichung* $f(x) = 0$ *sich durch einen Ausdruck* (1) *darstellen läßt und wenn die Wurzelexponenten nicht durch die Charakteristik des Körpers* K *teilbar sind*[1], *so ist die Gruppe dieser Gleichung auflösbar (d. h. ihre Kompositionsfaktoren sind zyklisch von Primzahlordnung). 2. Wenn umgekehrt die Gruppe der Gleichung auflösbar ist, so lassen sich alle Wurzeln durch Ausdrücke* (1) *darstellen, und zwar so, daß bei den sukzessiven Adjunktionen der* $\sqrt[n]{a}$ *die Exponenten Primzahlen und die Gleichungen* $x^n - a = 0$ *jeweils irreduzibel sind, vorausgesetzt, daß die Charakteristik des Körpers* K *Null oder größer als die größte Primzahl ist, die unter den Ordnungen der Kompositionsfaktoren vorkommt*[2].

Der Satz besagt also im wesentlichen, daß die Auflösbarkeit der Gruppe für die Auflösbarkeit der Gleichung durch Radikale entscheidend ist. Der Begriff der Auflösbarkeit durch Radikale ist im ersten Teil des Satzes möglichst schwach, im zweiten Teil aber möglichst stark gefaßt, so daß der Satz möglichst viel aussagt.

Beweis: 1. Zunächst kann man alle Wurzelexponenten in (1) zu Primzahlen machen vermöge

$$\sqrt[rs]{a} = \sqrt[r]{\sqrt[s]{a}}\,.$$

Sodann adjungieren wir zu K alle p_1-ten, p_2-ten usw. Einheitswurzeln, wo $p_1, p_2, \ldots$ die als Wurzelexponenten in (1) auftretenden Primzahlen sind. Das kommt also auf eine Reihe von aufeinander folgenden zyklischen Galoisschen Körpererweiterungen hinaus, die wir noch in Erweiterungen von Primzahlgrad zerlegt denken können. Sind aber diese Einheitswurzeln einmal vorhanden, so ist auch die Adjunktion eines $\sqrt[p]{a}$ nach § 50 entweder überhaupt keine Erweiterung oder eine zyklische Galoissche Erweiterung vom Grade p. Wir adjungieren nun, sobald wir ein $\sqrt[p]{a}$ adjungiert haben, nacheinander

[1] Diese Annahme hat den Zweck, das Auftreten inseparabler Erweiterungen zu verhüten. Man könnte sich von ihr befreien; doch interessiert uns das hier nicht.

[2] Wenn man außer Radikalen von der beschriebenen Art auch noch Einheitswurzeln in der Auflösungsformel zuläßt, so läßt sich die letztere Bedingung ersetzen durch die schwächere: unter den Ordnungen der Kompositionsfaktoren soll die Charakteristik nicht vorkommen.

auch alle p-ten Wurzeln aus den zu a konjugierten Größen; das sind entweder gar keine oder zyklische Erweiterungen von Primzahlgrad, und durch sie erreichen wir, daß unsere Körper hernach immer Galoissch in bezug auf K bleiben. So kommen wir schließlich durch eine Reihe von zyklischen Adjunktionen:

$$\mathsf{K} \subset \Lambda_1 \subset \Lambda_2 \subset \cdots \subset \Lambda_\omega , \tag{2}$$

zu einem Galoisschen Körper $\Lambda_\omega = \Omega$, der den Ausdruck (1), eine Wurzel von $f(x)$, enthält. Da der Körper Ω Galoissch ist, enthält er alle Wurzeln von $f(x)$, d. h. er enthält den Zerfällungskörper Σ von $f(x)$.

Es sei $\mathfrak{G}$ die Galoissche Gruppe von Ω nach K. Dann entspricht der Körperkette (2) eine Kette von Untergruppen von $\mathfrak{G}$:

$$\mathfrak{G} \supset \mathfrak{G}_1 \supset \mathfrak{G}_2 \supset \cdots \supset \mathfrak{G}_\omega = \mathfrak{E} , \tag{3}$$

und jede dieser Gruppen ist Normalteiler in der vorangehenden, wobei die Faktorgruppe zyklisch von Primzahlordnung ist. Das heißt, die Gruppe $\mathfrak{G}$ ist auflösbar und (3) eine Kompositionsreihe.

Zum Körper Σ gehört eine Untergruppe $\mathfrak{H}$, Normalteiler von $\mathfrak{G}$, und nach § 41 können wir auch durch $\mathfrak{H}$ eine Kompositionsreihe legen, welche dann bis auf Isomorphie dieselben Kompositionsfaktoren hat, eventuell in anderer Reihenfolge:

$$\mathfrak{G} \supset \mathfrak{H}_1 \supset \mathfrak{H}_2 \supset \cdots \supset \mathfrak{H} \supset \cdots \supset \mathfrak{E} , \tag{4}$$

Die Galoissche Gruppe von Σ nach K ist die Gruppe $\mathfrak{G}/\mathfrak{H}$; für sie haben wir jetzt die Kompositionsreihe

$$\mathfrak{G}/\mathfrak{H} \supset \mathfrak{H}_1/\mathfrak{H} \supset \mathfrak{H}_2/\mathfrak{H} \supset \cdots \supset \mathfrak{H}/\mathfrak{H} = \mathfrak{E} ,$$

deren Faktoren nach dem zweiten Isomorphiesatz (§ 40) zu den entsprechenden Faktoren von (4) 1-isomorph, also wieder zyklisch von Primzahlordnung sind. Damit ist die Behauptung 1 bewiesen.

Zu Behauptung 2 beweisen wir zunächst den

Hilfssatz. *Die q-ten Einheitswurzeln (q prim) sind durch „irreduzible Radikale" (d. h. Wurzeln irreduzibler Gleichungen $x^p - a = 0$) ausdrückbar, vorausgesetzt, daß die Charakteristik von K Null oder größer als q ist.*

Da die Behauptung für $q = 2$ trivial ist (die zweiten Einheitswurzeln ± 1 sind ja rational), können wir sie für alle Primzahlen unterhalb q als bewiesen annehmen. Der Körper der q-ten Einheitswurzeln ist zyklisch vom Grade $q - 1$, und wenn wir $q - 1$ in Primfaktoren zerlegen: $q - 1 = p_1^{\varrho_1} \ldots p_r^{\varrho_r}$, so können wir diesen Körper durch eine Folge zyklischer Erweiterungen von den Graden p_ν aufbauen. Adjungieren wir nun vorher die p_1-ten, ..., p_r-ten Einheitswurzeln, die nach der Induktionsvoraussetzung ja durch Radikale ausdrückbar sind, so können wir auf die zyklischen Erweiterungen der Grade p_ν den Satz von § 50 anwenden, der die Darstellbarkeit der sukzessiven Körpererzeugenden durch Radikale lehrt. Die betreffenden Gleichungen $x^{p_\nu} - a = 0$ müssen irreduzibel sein, da sonst die Körpergrade nicht gleich den p_ν sein könnten.

Nunmehr können wir die Behauptung 2 beweisen. Es sei Σ der Zerfällungskörper von $f(x)$, und $\mathfrak{G} \supset \mathfrak{G}_1 \supset \cdots \supset \mathfrak{G}_l = \mathfrak{E}$ sei eine Kompositionsreihe für die Galoissche Gruppe von Σ in bezug auf K. Zu dieser Reihe von Gruppen gehört eine Reihe von Körpern:

$$\mathsf{K} \subset \Lambda_1 \subset \cdots \subset \Lambda_l = \Sigma,$$

deren jeder Galoissch und zyklisch in bezug auf den vorangehenden ist. Sind $q_1, q_2, \ldots$ die in der Reihe vorkommenden Relativgrade, so adjungieren wir an K zunächst die q_1-ten, q_2-ten usw. Einheitswurzeln, was nach dem Hilfssatz durch irreduzible Radikale möglich ist. Sodann lassen sich nach dem Satz von § 50 die Erzeugenden von $\Lambda_1, \Lambda_2, \ldots, \Lambda_l$ durch Radikale ausdrücken, wobei die betreffenden Gleichungen $x^{q_\nu} - a = 0$ jedesmal entweder irreduzibel sind oder ganz zerfallen (§ 50, Schluß); im letzteren Fall ist die Adjunktion des betreffenden Radikals überflüssig. Damit ist 2. bewiesen.

Daß die Behauptung 2 wirklich falsch wird, wenn einer der Grade q_ν gleich der Charakteristik p des Körpers wird, zeigt das folgende Beispiel: Die „allgemeine Gleichung 2. Grades" $x^2 + ux + v$ (u, v Unbestimmte, die dem Primkörper der Charakteristik 2 adjungiert werden) ist irreduzibel und separabel und bleibt irreduzibel bei Adjunktion sämtlicher Einheitswurzeln. Adjunktion einer Wurzel einer irreduziblen reinen Gleichung von ungeradem Grade kann die Gleichung nicht zum Zerfall bringen, da jene einen Körper ungeraden Grades erzeugt. Adjunktion einer Quadratwurzel kann aber die Gleichung ebensowenig zum Zerfall bringen, weil dabei der reduzierte Körpergrad sich nicht ändert. Die Gleichung ist also in keiner Weise durch Radikale lösbar.

Anwendung. Die symmetrischen Permutationsgruppen von 2, 3 oder 4 Ziffern (und ihre Untergruppen) sind auflösbar; daraus erklärt sich die Möglichkeit der Auflösungsformeln der Gleichungen 2., 3. und 4. Grades (Ausführung in § 53). Die symmetrischen Gruppen von 5 und mehr Ziffern sind aber nicht mehr auflösbar (§ 43), und wir werden sogleich sehen, daß es Gleichungen von jedem Grade gibt, deren Gruppe wirklich die symmetrische ist; daher gibt es keine allgemeine Auflösungsformel für die Gleichungen 5. Grades oder höherer Grade. Nur gewisse spezielle von diesen Gleichungen (wie die Kreisteilungsgleichungen) können durch Radikale gelöst werden.

Solche Körper oder Gleichungen, deren Gruppe auflösbar ist, heißen *metazyklisch*. Bisweilen nennt man auch die Gruppe metazyklisch (statt auflösbar).

§ 52. Die allgemeine Gleichung n-ten Grades.

Unter der *allgemeinen Gleichung n-ten Grades* versteht man die Gleichung

$$(1) \qquad z^n - u_1 z^{n-1} + u_2 z^{n-2} - + \cdots + (-1)^n u_n = 0,$$

mit *unbestimmten* Koeffizienten $u_1, \ldots, u_n$, die dem Grundkörper K adjungiert werden. Sind ihre Wurzeln $v_1, \ldots, v_n$, so ist

$$\begin{cases} u_1 = v_1 + \cdots + v_n, \\ u_2 = v_1v_2 + v_1v_3 + \cdots + v_{n-1}v_n, \\ \cdots\cdots\cdots\cdots\cdots \\ u_n = v_1v_2 \ldots v_n. \end{cases}$$

Wir vergleichen die allgemeine Gleichung (1) mit einer anderen Gleichung, deren *Wurzeln* Unbestimmte $x_1, \ldots, x_n$ sind und deren Koeffizienten daher die elementarsymmetrischen Funktionen dieser Unbestimmten sind:

$$(2) \qquad \begin{aligned} &z^n - \sigma_1 z^{n-1} + \sigma_2 z^{n-2} - + \cdots + (-1)^n \sigma_n \\ &= (z - x_1)(z - x_2) \ldots (z - x_n) = 0; \end{aligned}$$

$$\begin{cases} \sigma_1 = x_1 + \cdots + x_n, \\ \sigma_2 = x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n, \\ \cdots\cdots\cdots\cdots\cdots \\ \sigma_n = x_1x_2 \ldots x_n. \end{cases}$$

Die Gleichung (2) ist separabel und hat als Galoissche Gruppe in bezug auf den Körper $\mathsf{K}(\sigma_1, \ldots, \sigma_n)$ die symmetrische Gruppe aller Permutationen der x_ν; denn jede solche Permutation stellt einen 1-Automorphismus des Körpers $\mathsf{K}(x_1, \ldots, x_n)$ dar, der die symmetrischen Funktionen $\sigma_1, \ldots, \sigma_n$ und somit auch alle Elemente des Körpers $\mathsf{K}(\sigma_1, \ldots, \sigma_n)$ invariant läßt. Jede Funktion der $x_1, \ldots, x_n$, die bei den Permutationen der Gruppe invariant bleibt, gehört also dem Körper $\mathsf{K}(\sigma_1, \ldots, \sigma_n)$ an; d. h. *jede symmetrische Funktion der x_ν ist rational durch $\sigma_1, \ldots, \sigma_n$ ausdrückbar.* Damit haben wir einen Teil des „Hauptsatzes über symmetrische Funktionen" von § 24 mit Hilfe der Galoisschen Theorie neu bewiesen.

Auch den „Eindeutigkeitssatz" von § 24, d. h. die Tatsache, daß *keine Relation $f(\sigma_1, \ldots, \sigma_n) = 0$ bestehen kann, wenn nicht das Polynom f selber identisch verschwindet,* erhalten wir mühelos wieder. Denn gesetzt, es wäre

$$f(\sigma_1, \ldots, \sigma_n) = f(\sum x_i, \sum x_ix_k, \ldots, x_1x_2 \ldots x_n) = 0,$$

so würde diese Relation bestehen bleiben bei Substitution der Größen v_i für die Unbestimmten x_i. Wir hätten also

$$f(\sum v_i, \sum v_iv_k, \ldots, v_1v_2 \ldots v_n) = 0$$

oder $f(u_1, \ldots, u_n) = 0$; also würde f identisch verschwinden.

Aus dem Eindeutigkeitssatz folgt, daß die Zuordnung

$$f(u_1, \ldots, u_n) \to f(\sigma_1, \ldots, \sigma_n)$$

nicht nur ein Homomorphismus, sondern ein 1-Isomorphismus der Ringe $\mathsf{K}[u_1, \ldots, u_n]$ und $\mathsf{K}[\sigma_1, \ldots, \sigma_n]$ ist. Sie läßt sich zu einem Isomorphismus der Quotientenkörper $\mathsf{K}(u_1, \ldots, u_n)$ und $\mathsf{K}(\sigma_1, \ldots, \sigma_n)$ und nach § 29 weiter zu einem Isomorphismus der Nullstellenkörper $\mathsf{K}(v_1, \ldots, v_n)$ und $\mathsf{K}(x_1, \ldots, x_n)$ erweitern. Die v_i gehen in die x_k in irgend einer Reihenfolge über; da die x_k aber permutierbar sind, können wir auch jedes v_i in x_i übergehen lassen. Damit ist bewiesen:

Es gibt einen Isomorphismus

$$\mathsf{K}(v_1, \ldots, v_n) \cong \mathsf{K}(x_1, \ldots, x_n),$$

der jedes v_i in x_i, jedes u_i in σ_i überführt.

Vermöge dieses Isomorphismus können alle Sätze über die Gleichung (2) unmittelbar auf (1) übertragen werden. Insbesondere erhält man:

Die allgemeine Gleichung (1) *ist separabel und hat als Galoissche Gruppe in bezug auf ihren Koeffizientenkörper $\mathsf{K}(u_1, \ldots, u_n)$ die symmetrische. Der Grad ihres Zerfällungskörpers ist $n!$.*

Wir setzen

$$\mathsf{K}(u_1, \ldots, u_n) = \Delta,$$
$$\mathsf{K}(v_1, \ldots, v_n) = \Sigma$$

und bezeichnen die symmetrische Gruppe mit $\mathfrak{S}_n$. Sie besitzt immer eine Untergruppe vom Index 2: die alternierende Gruppe $\mathfrak{A}_n$. Der zugehörige Zwischenkörper Λ hat den Grad 2 und wird von jeder Funktion der v_i erzeugt, welche $\mathfrak{A}_n$, nicht aber $\mathfrak{S}_n$ gestattet. Eine solche Funktion ist das *Differenzenprodukt*

$$\prod_{i<k}(v_i - v_k) = \sqrt{D},$$

dessen Quadrat die *Diskriminante* der Gleichung (1)

$$D = \prod_{i<k}(v_i - v_k)^2$$

ist. Die Diskriminante ist eine symmetrische Funktion, also ein Polynom in den u_i. Den Körper Λ erhalten wir also in der Form

$$\Lambda = \Delta(\sqrt{D}).$$

Für $n > 4$ ist die Gruppe $\mathfrak{A}_n$ einfach (§ 43), daher

$$\mathfrak{S}_n \supset \mathfrak{A}_n \supset \mathfrak{E} \tag{3}$$

eine Kompositionsreihe. Die Gruppe $\mathfrak{S}_n$ ist also für $n > 4$ nicht auflösbar, und daraus folgt nach § 51 der berühmte Satz von ABEL:

Die allgemeine Gleichung n-ten Grades ist für $n > 4$ nicht durch Radikale lösbar.

Für $n = 2$ und $n = 3$ sind in (3) die Kompositionsfaktoren zyklisch. Für $n = 2$ ist sogar $\mathfrak{A}_n = \mathfrak{E}$; für $n = 3$ haben die Faktoren die Ord-

nungen 2 und 3. Für $n = 4$ hat man die Kompositionsreihe

$$\mathfrak{S}_n \supset \mathfrak{A}_n \supset \mathfrak{B}_4 \supset \mathfrak{Z}_2 \supset \mathfrak{E},$$

wo $\mathfrak{B}_4$ die „Kleinsche Vierergruppe"

$$\{1, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$$

und $\mathfrak{Z}_2$ irgend eine ihrer Untergruppen der Ordnung 2 ist. Die Ordnungen der Kompositionsfaktoren sind

$$2, 3, 2, 2.$$

Auf diesen Tatsachen beruhen die Auflösungsformeln der Gleichungen 2., 3. und 4. Grades, die wir im nächsten Paragraphen behandeln werden.

§ 53. Gleichungen zweiten, dritten und vierten Grades.

Die Auflösung der allgemeinen *Gleichung 2. Grades*

$$x^2 + px + q = 0$$

muß nach der allgemeinen Theorie durch eine Quadratwurzel geschehen können; für diese kann man wählen (vgl. den Schluß des vorigen Paragraphen) das Differenzenprodukt der Wurzeln x_1, x_2:

$$x_1 - x_2 = \sqrt{D}; \quad D = p^2 - 4q.$$

Hieraus und aus

$$x_1 + x_2 = -p$$

erhält man die bekannten Auflösungsformeln

$$x_1 = \frac{-p + \sqrt{D}}{2}, \qquad x_2 = \frac{-p - \sqrt{D}}{2}.$$

Voraussetzung ist dabei nur, daß die Charakteristik des Grundkörpers nicht 2 ist.

Die allgemeine *Gleichung 3. Grades*

$$z^3 + a_1 z^2 + a_2 z + a_3 = 0$$

läßt sich zunächst durch die Substitution

$$z = x - \tfrac{1}{3} a_1$$

auf die Gestalt

$$x^3 + px + q = 0$$

bringen[1]. (Entsprechend der allgemeinen Auflösungstheorie des vorigen Paragraphen setzen wir voraus, daß die Charakteristik des Grundkörpers von 2 und 3 verschieden sei.)

[1] Nur zur Vereinfachung der Formeln. Aus dem Beweis ist ebenso leicht zu entnehmen, wie die Ausführungsformeln für die ursprüngliche Gleichung

$$z^3 + a_1 z^2 + a_2 z + a_3 = 0$$

lauten.

Gemäß der Kompositionsreihe

$$\mathfrak{S}_3 > \mathfrak{A}_3 > \mathfrak{E}$$

adjungieren wir zunächst das Differenzenprodukt der Wurzeln:

$$(x_1 - x_2)(x_1 - x_3)(x_2 - x_3) = \sqrt{D} = \sqrt{-4p^3 - 27q^2}$$

(vgl. § 24, Schluß, wo wir $a_1 = 0$, $a_2 = -p$, $a_3 = -q$ zu setzen haben). Durch diese Adjunktion entsteht ein Körper $\Delta(\sqrt{D})$, in bezug auf den die Gleichung die Gruppe $\mathfrak{A}_3$ hat, also eine zyklische Gruppe 3. Ordnung. Der allgemeinen Theorie von § 50 entsprechend adjungieren wir zunächst die dritten Einheitswurzeln:

$$(1) \qquad \varrho = -\tfrac{1}{2} + \tfrac{1}{2}\sqrt{-3}, \qquad \varrho^2 = -\tfrac{1}{2} - \tfrac{1}{2}\sqrt{-3}$$

und betrachten dann die Lagrangesche Resolventen:

$$\begin{aligned}(1, x_1) &= x_1 + x_2 + x_3 = 0,\\ (\varrho, x_1) &= x_1 + \varrho x_2 + \varrho^2 x_3,\\ (\varrho^2, x_1) &= x_1 + \varrho^2 x_2 + \varrho x_3.\end{aligned}$$

Die dritte Potenz einer jeden dieser Größen muß sich rational durch $\sqrt{-3}$ und $\sqrt{D}$ ausdrücken. Die Rechnung ergibt:

$$\begin{aligned}(\varrho, x_1)^3 = {} & x_1^3 + x_2^3 + x_3^3\\ & + 3\varrho x_1^2 x_2 + 3\varrho x_2^2 x_3 + 3\varrho x_3^2 x_1\\ & + 3\varrho^2 x_1 x_2^2 + 3\varrho^2 x_2 x_3^2 + 3\varrho^2 x_3 x_1^2\\ & + 6 x_1 x_2 x_3,\end{aligned}$$

und entsprechend ergibt sich $(\varrho^2, x_1)^3$ durch Vertauschung von ϱ und ϱ^2. Setzen wir hierin (1) ein und beachten

$$\begin{aligned}\sqrt{D} &= (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)\\ &= x_1^2 x_2 + x_2^2 x_3 + x_3^2 x_1 - x_1 x_2^2 - x_2 x_3^2 - x_3 x_1^2,\end{aligned}$$

so folgt:

$$(\varrho, x_1)^3 = \sum x_1^3 - \tfrac{3}{2}\sum x_1^2 x_2 + 6 x_1 x_2 x_3 + \tfrac{3}{2}\sqrt{-3}\,\sqrt{D}.$$

(Die Bedeutung der Summenzeichen ist dieselbe wie bei den symmetrischen Funktionen, § 24.) Die hier auftretenden symmetrischen Funktionen lassen sich nach § 24 leicht durch die elementarsymmetrischen Funktionen $\sigma_1, \sigma_2, \sigma_3$ und damit durch die Koeffizienten unserer Gleichung ausdrücken. Es ist

$$\begin{aligned}\sigma_1^3 &= \sum x_1^3 + 3\sum x_1^2 x_2 + 6 x_1 x_2 x_3 &&= 0 \text{ wegen } \sigma_1 = 0,\\ -\tfrac{9}{2}\sigma_1\sigma_2 &= -\tfrac{9}{2}\sum x_1^2 x_2 - \tfrac{27}{2} x_1 x_2 x_3 &&= 0 \text{ wegen } \sigma_1 = 0,\\ \tfrac{27}{2}\sigma_3 &= \tfrac{27}{2} x_1 x_2 x_3 &&= -\tfrac{27}{2} q\\ \hline & \sum x_1^3 - \tfrac{3}{2}\sum x_1^2 x_2 + 6 x_1 x_2 x_3 &&= -\tfrac{27}{2} q;\end{aligned}$$

daher

$$(\varrho, x_1)^3 = -\frac{27}{2}q + \frac{3}{2}\sqrt{-3}\sqrt{D}$$

und ebenso

$$(\varrho^2, x_1)^3 = -\frac{27}{2}q - \frac{3}{2}\sqrt{-3}\sqrt{D}\,.$$

Die beiden kubischen Irrationalitäten (ϱ, x_1) und (ϱ^2, x_1) sind nicht unabhängig; sondern es ist (vgl. § 50)

$$\begin{aligned}(\varrho, x_1)\cdot(\varrho^2, x_1) &= x_1^2 + x_2^2 + x_3^2 + (\varrho + \varrho^2)x_1x_2 + (\varrho + \varrho^2)x_1x_3 + (\varrho + \varrho^2)x_2x_3\\ &= x_1^2 + x_2^2 + x_3^2 - x_1x_2 - x_1x_3 - x_2x_3\\ &= \sigma_1^2 - 3\sigma_2 = -3p\,.\end{aligned}$$

Man hat also die Kubikwurzeln

$$(2)\quad (\varrho, x_1) = \sqrt[3]{-\frac{27}{2}q + \frac{3}{2}\sqrt{-3D}}\,, \qquad (\varrho^2, x_1) = \sqrt[3]{-\frac{27}{2}q - \frac{3}{2}\sqrt{-3D}}$$

so zu bestimmen, daß ihr Produkt

$$(3)\qquad (\varrho, x_1)\cdot(\varrho^2, x_1) = -3p$$

wird.

Die Wurzeln x_1, x_2, x_3 bestimmen sich nun mit Hilfe von Gleichung (3), § 50 folgendermaßen:

$$(4)\qquad \begin{cases} 3\cdot x_1 = \sum\limits_{\zeta}(\zeta, x_1) = (\varrho, x_1) + (\varrho^2, x_1),\\ 3\cdot x_2 = \sum\limits_{\zeta}\zeta^{-1}(\zeta, x_1) = \varrho^2(\varrho, x_1) + \varrho(\varrho^2, x_1),\\ 3\cdot x_3 = \sum\limits_{\zeta}\zeta^{-2}(\zeta, x_1) = \varrho(\varrho, x_1) + \varrho^2(\varrho^2, x_1). \end{cases}$$

Die Formeln (2), (3), (4) sind die „*Auflösungsformeln von* CARDANO". Sie gelten kraft ihrer Herleitung nicht nur für die „allgemeine", sondern auch für jede spezielle kubische Gleichung.

Realitätsfragen. Ist der Grundkörper, dem die Koeffizienten p, q angehören, ein reeller Zahlkörper, so sind zwei Fälle möglich:

a) Die Gleichung hat eine reelle und zwei konjugiert-komplexe Wurzeln. Dann ist offenbar $(x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$ rein imaginär, mithin $D < 0$. Die Größen $\pm\sqrt{-3D}$ sind reell, und man kann in (2) für (ϱ, x_1) eine reelle dritte Wurzel wählen. Wegen (3) wird dann auch (ϱ^2, x_1) reell, und die Formel (4) liefert $3x_1$ als Summe zweier reeller Kubikwurzeln, während x_2 und x_3 durch (4) als konjugiert-komplexe Größen dargestellt werden.

b) Die Gleichung hat drei reelle Wurzeln. Jetzt ist $\sqrt{D}$ reell, mithin $D \geqq 0$. Im Falle $D = 0$ (zwei Wurzeln gleich) geht alles wie bisher; im Falle $D > 0$ aber werden die Größen unter dem Kubikwurzelzeichen in (2) imaginär, und man erhält mithin die drei (reellen) Ausdrücke (4) als Summen *imaginärer* Kubikwurzeln, d. h. nicht in reeller Form.

Dieser Fall ist der sogenannte „*Casus irreducibilis*" der kubischen Gleichung. Wir zeigen, daß *es in diesem Fall tatsächlich unmöglich ist, die Gleichung*

$$x^3 + px + q = 0$$

durch reelle Radikale aufzulösen, es sei denn, daß die Gleichung schon im Grundkörper K *zerfällt.*

Die Gleichung $x^3 + px + q = 0$ sei also irreduzibel in K und habe drei reelle Wurzeln x_1, x_2, x_3. Wir adjungieren zunächst $\sqrt{D}$. Dadurch zerfällt die Gleichung nicht (denn der höchstens quadratische Körper $\mathsf{K}(\sqrt{D})$ kann keine Wurzel einer irreduziblen kubischen Gleichung enthalten), und ihre Gruppe wird jetzt $\mathfrak{A}_3$. Wenn es nun möglich ist, die Gleichung durch eine Reihe von Adjunktionen reeller Radikale, deren Wurzelexponenten natürlich als Primzahlen angenommen werden können, zum Zerfall zu bringen, so gibt es unter diesen Adjunktionen eine „kritische" Adjunktion $\sqrt[h]{a}$ (h prim), welche gerade den Zerfall bewirkt, während vor der Adjunktion der $\sqrt[h]{a}$, etwa im Körper Λ, die Gleichung noch irreduzibel war. Nach § 50 ist entweder $x^h - a$ irreduzibel in Λ, oder a ist eine h-te Potenz einer Zahl aus Λ. Der letzte Fall scheidet aus, da dann die reelle h-te Wurzel aus a schon in Λ enthalten wäre, also ihre Adjunktion keinen Zerfall bewirken könnte. Also ist $x^h - a$ irreduzibel und der Grad des Körpers $\Lambda(\sqrt[h]{a})$ genau h. In $\Lambda(\sqrt[h]{a})$ ist nach Voraussetzung eine Wurzel der in Λ noch irreduziblen Gleichung $x^3 + px + q = 0$ enthalten; mithin ist h durch 3 teilbar, also $h = 3$, und etwa $\Lambda(\sqrt[3]{a}) = \Lambda(x_1)$. Der Zerfällungskörper $\Lambda(x_1, x_2, x_3)$ hat in bezug auf Λ ebenfalls den Grad 3; mithin ist auch $\Lambda(\sqrt[3]{a}) = \Lambda(x_1, x_2, x_3)$. Der nunmehr als Galoissch erkannte Körper $\Lambda(\sqrt[3]{a})$ muß neben $\sqrt[3]{a}$ auch die konjugierten Größen $\varrho\sqrt[3]{a}$ und $\varrho^2\sqrt[3]{a}$ enthalten, also auch die Einheitswurzeln ϱ und ϱ^2. Damit sind wir auf einen Widerspruch gestoßen; denn der Körper $\Lambda(\sqrt[3]{a})$ ist reell und die Zahl ϱ nicht.

Die allgemeine *Gleichung* 4. *Grades*

$$z^4 + a_1 z^3 + a_2 z^2 + a_3 z + a_4 = 0$$

kann wieder durch die Substitution

$$z = x - \tfrac{1}{4} a_1$$

in

$$x^4 + px^2 + qx + r = 0$$

transformiert werden. Zu der Kompositionsreihe

$$\mathfrak{S}_4 > \mathfrak{A}_4 > \mathfrak{B}_4 > \mathfrak{Z}_2 > \mathfrak{E}$$

gehört eine Reihe von Körpern

$$\mathsf{K} < \mathsf{K}(\sqrt{D}) < \Lambda < \Lambda_1 < \Sigma .$$

Die Charakteristik von K sei wieder $\neq 2$ und $\neq 3$. Die explizite Bestimmung von D ist, wie wir sehen werden, nicht nötig. Der Körper Λ wird aus $\mathsf{K}(\sqrt{D})$ erzeugt durch eine Größe, welche die Substitutionen von $\mathfrak{B}_4$, aber nicht die von $\mathfrak{A}_4$ gestattet; eine solche ist

$$\Theta_1 = (x_1 + x_2)(x_3 + x_4) .$$

Diese Größe gestattet, nebenbei bemerkt, außer den Substitutionen von $\mathfrak{B}_4$ noch die folgenden:

$$(1\ 2),\ (3\ 4),\ (1\ 3\ 2\ 4),\ (1\ 4\ 2\ 3)$$

(die zusammen mit $\mathfrak{B}_4$ eine Gruppe der Ordnung 8 bilden). Sie hat in bezug auf K drei verschiedene Konjugierte, in die sie durch die Substitutionen von $\mathfrak{S}_4$ übergeführt wird, nämlich:

$$\Theta_1 = (x_1 + x_2)(x_3 + x_4),$$
$$\Theta_2 = (x_1 + x_3)(x_2 + x_4),$$
$$\Theta_3 = (x_1 + x_4)(x_2 + x_3).$$

Diese Größen sind Wurzeln einer Gleichung dritten Grades

$$\Theta^3 - b_1\Theta^2 + b_2\Theta - b_3 = 0, \tag{5}$$

worin die b_i die elementarsymmetrischen Funktionen von Θ_1, Θ_2, Θ_3 sind:

$$\begin{aligned} b_1 &= \Theta_1 + \Theta_2 + \Theta_3 = 2\sum x_1x_2 = 2p, \\ b_2 &= \sum\Theta_1\Theta_2 \quad\quad = \sum x_1^2x_2^2 + 3\sum x_1^2x_2x_3 + 6x_1x_2x_3x_4, \\ b_3 &= \Theta_1\Theta_2\Theta_3 \quad\quad = \sum x_1^3x_2^2x_3 + 2\sum x_1^3x_2x_3x_4 \\ &\qquad\qquad + 2\sum x_1^2x_2^2x_3^2 + 4\sum x_1^2x_2^2x_3x_4. \end{aligned}$$

b_2 und b_3 können durch die elementarsymmetrischen Funktionen σ_1, σ_2, σ_3, σ_4 der x_i ausgedrückt werden. Es ist (Methode des § 24):

$$\begin{aligned} \sigma_2^2 &= \sum x_1^2x_2^2 + 2\sum x_1^2x_2x_3 + 6x_1x_2x_3x_4 = p^2, \\ \sigma_1\sigma_3 &= \quad\quad \sum x_1^2x_2x_3 + 4x_1x_2x_3x_4 = 0, \\ -4\sigma_4 &= \quad\quad\quad\quad - 4x_1x_2x_3x_4 = -4r \\ \hline b_2 &= \sum x_1^2x_2^2 + 3\sum x_1^2x_2x_3 + 6x_1x_2x_3x_4 = p^2 - 4r; \end{aligned}$$

$$\begin{aligned} \sigma_1\sigma_2\sigma_3 &= \sum x_1^3x_2^2x_3 + 3\sum x_1^3x_2x_3x_4 + 3\sum x_1^2x_2^2x_3^2 + 8\sum x_1^2x_2^2x_3x_4 = 0, \\ -\sigma_1^2\sigma_4 &= \quad\quad -\sum x_1^3x_2x_3x_4 \quad\quad\quad\quad - 2\sum x_1^2x_2^2x_3x_4 = 0, \\ -\sigma_3^2 &= \quad\quad\quad\quad\quad\quad - \sum x_1^2x_2^2x_3^2 - 2\sum x_1^2x_2^2x_3x_4 = -q^2 \\ \hline b_3 &= \sum x_1^3x_2^2x_3 + 2\sum x_1^3x_2x_3x_4 + 2\sum x_1^2x_2^2x_3^2 + 4\sum x_1^2x_2^2x_3x_4 = -q^2. \end{aligned}$$

Damit wird die Gleichung (5) zu:

$$\Theta^3 - 2p\Theta^2 + (p^2 - 4r)\Theta + q^2 = 0. \tag{6}$$

Diese Gleichung heißt die *kubische Resolvente* der Gleichung 4. Grades; ihre Wurzeln Θ_1, Θ_2, Θ_3 können nach CARDANO durch Radikale ausgedrückt werden. Jedes einzelne Θ gestattet eine Gruppe von 8 Permutationen; alle drei gestatten aber nur $\mathfrak{B}_4$, und daher ist

$$\mathsf{K}(\Theta_1, \Theta_2, \Theta_3) = \Lambda.$$

Der Körper Λ_1 entsteht aus Λ durch Adjunktion einer Größe, die nicht alle vier Substitutionen von $\mathfrak{B}_4$, sondern nur (etwa) das Einselement und die Substitution (1 2) (3 4) gestattet. Eine solche ist $x_1 + x_2$. Man hat

$$(x_1 + x_2)(x_3 + x_4) = \Theta_1 \quad \text{und} \quad (x_1 + x_2) + (x_3 + x_4) = 0,$$

daher etwa

$$x_1 + x_2 = \sqrt{-\Theta_1}; \quad x_3 + x_4 = -\sqrt{-\Theta_1}.$$

Ebenso hat man

$$x_1 + x_3 = \sqrt{-\Theta_2}; \quad x_2 + x_4 = -\sqrt{-\Theta_2};$$
$$x_1 + x_4 = \sqrt{-\Theta_3}; \quad x_2 + x_3 = -\sqrt{-\Theta_3}.$$

Diese drei Irrationalitäten sind aber nicht unabhängig; sondern es ist

$$\begin{aligned}\sqrt{-\Theta_1}\cdot\sqrt{-\Theta_2}\cdot\sqrt{-\Theta_3} &= (x_1+x_2)(x_1+x_3)(x_1+x_4)\\ &= x_1^3 + x_1^2(x_2+x_3+x_4) + x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4\\ &= x_1^2(x_1+x_2+x_3+x_4) + \sum x_1x_2x_3\\ &= \sum x_1x_2x_3\\ &= -q.\end{aligned}$$

Zwei quadratische Irrationalitäten braucht man gerade, um von $\mathfrak{V}_4$ zu $\mathfrak{E}$ hinunter- oder von A zu Σ hinaufzusteigen; denn $\mathfrak{V}_4$ hat die Ordnung 4 und besitzt eine Untergruppe von der Ordnung 2. Und tatsächlich lassen sich durch die drei Größen Θ (die schon von zweien unter ihnen abhängen) die x_i rational bestimmen; denn es ist offenbar

$$\begin{cases} 2x_1 = \sqrt{-\Theta_1} + \sqrt{-\Theta_2} + \sqrt{-\Theta_3},\\ 2x_2 = \sqrt{-\Theta_1} - \sqrt{-\Theta_2} - \sqrt{-\Theta_3},\\ 2x_3 = -\sqrt{-\Theta_1} + \sqrt{-\Theta_2} - \sqrt{-\Theta_3},\\ 2x_4 = -\sqrt{-\Theta_1} - \sqrt{-\Theta_2} + \sqrt{-\Theta_3}. \end{cases}$$

Das sind die Auflösungsformeln der allgemeinen Gleichung 4. Grades. Sie gelten kraft ihrer Herleitung auch für jede spezielle Gleichung 4. Grades.

Bemerkung: Wegen

$$\begin{aligned}\Theta_1 - \Theta_2 &= -(x_1-x_4)(x_2-x_3),\\ \Theta_1 - \Theta_3 &= -(x_1-x_3)(x_2-x_4),\\ \Theta_2 - \Theta_3 &= -(x_1-x_2)(x_3-x_4)\end{aligned}$$

ist die Diskriminante der kubischen Resolvente gleich der Diskriminante der ursprünglichen Gleichung. Das gibt ein einfaches Mittel, die Diskriminante der Gleichung 4. Grades zu berechnen, da wir die der kubischen Gleichung schon kennen; man findet:

$$D = 16p^4r - 4p^3q^2 - 128p^2r^2 + 144pq^2r - 27q^4 + 256r^3.$$

Aufgaben. 1. Die Gruppe der kubischen Resolvente einer bestimmten Gleichung 4. Grades ist die Faktorgruppe der Gruppe der Ausgangsgleichung nach ihrem Durchschnitt mit der Vierergruppe $\mathfrak{V}_4$.

2. Man bestimme die Gruppe der Gleichung

$$x^4 + x^2 + x + 1 = 0.$$

[Vgl. Aufg. 4 § 45 und Aufg. 1 § 53.]

§ 54. Konstruktionen mit Zirkel und Lineal.

Wir wollen die Frage untersuchen: *Wann ist ein geometrisches Konstruktionsproblem lösbar mit Zirkel und Lineal?*

Gegeben seien einige elementargeometrische Gebilde (Punkte, Gerade oder Kreise). Die Aufgabe laute, daraus andere zu konstruieren, welche gewissen Bedingungen genügen.

Wir denken uns zu den gegebenen Gebilden noch ein kartesisches Koordinatensystem hinzugegeben. Alle gegebenen Gebilde kann man dann durch Zahlen (Koordinaten) repräsentieren, und das gleiche gilt für die zu konstruierenden Gebilde. Wenn es gelingt, die letzteren Zahlen (als Strecken) zu konstruieren, so ist die Aufgabe gelöst. Alles ist demnach auf die Konstruktion von Strecken aus gegebenen Strecken zurückgeführt. Es seien $a, b, \ldots$ die gegebenen Strecken, x eine gesuchte.

Wir können nun zunächst eine *hinreichende* Bedingung für die Konstruierbarkeit angeben:

Immer dann, wenn eine Lösung x des Problems reell ist und sich mittels rationaler Operationen und (nicht notwendig reeller) Quadratwurzeln aus den gegebenen Strecken $a, b, \ldots$ berechnen läßt, ist die Strecke x mit Zirkel und Lineal konstruierbar.

Am bequemsten ist dieser Satz so zu beweisen, daß man alle komplexen Zahlen $p + iq$, die in der Berechnung von x vorkommen, in bekannter Weise[1] durch Punkte in einer Ebene mit rechtwinkligen Koordinaten p, q darstellt und alle vorzunehmenden Rechenoperationen durch geometrische Konstruktionen in dieser Ebene ersetzt. Wie das ausgeführt wird, ist hinreichend bekannt: Die Addition ist die Vektoraddition, die Subtraktion die dazu inverse Operation. Bei der Multiplikation addieren sich die Argumentenwinkel und multiplizieren sich die Beträge; daher hat man, wenn φ_1, φ_2 die Argumente und r_1, r_2 die Beträge der zu multiplizierenden Zahlen sind, die entsprechenden Größen φ, r für das Produkt mit Hilfe der Gleichungen

$$\varphi = \varphi_1 + \varphi_2 \quad \text{und} \quad r = r_1 r_2 \quad \text{oder} \quad 1 : r_1 = r_2 : r$$

zu konstruieren. Die inverse Operation ist wieder die Division. Um schließlich eine Quadratwurzel aus einer Zahl mit dem Betrag r und

[1] Wir setzen für den Augenblick die komplexen Zahlen, deren genaue Bedeutung im Rahmen der abstrakten Algebra wir erst im Kap. 10 behandeln werden, als bekannt voraus.

dem Argument φ zu berechnen, hat man r_1, φ_1 aus

$$\varphi = 2\varphi_1 \quad \text{oder} \quad \varphi_1 = \tfrac{1}{2}\varphi$$

und

$$r = r_1^2 \quad \text{oder} \quad 1 : r_1 = r_1 : r$$

zu konstruieren. Damit ist alles auf bekannte Konstruktionen mit Zirkel und Lineal zurückgeführt[1].

Von dem eben bewiesenen Satz gilt nun aber auch die Umkehrung:

Wenn eine Strecke x sich mit Lineal und Zirkel aus gegebenen Strecken $a, b, \ldots$ konstruieren läßt, so läßt sich x mittels rationaler Operationen und Quadratwurzeln durch $a, b, \ldots$ ausdrücken.

Um dies zu beweisen, sehen wir uns genauer die Operationen an, die bei der Konstruktion verwendet werden dürfen. Es sind dies: Annahme eines beliebigen Punktes (innerhalb eines vorgegebenen Gebiets); Konstruktion einer Geraden durch zwei Punkte, eines Kreises aus Mittelpunkt und Radius, endlich eines Schnittpunkts zweier Geraden, einer Geraden und eines Kreises, oder zweier Kreise.

Alle diese Operationen lassen sich nun mit Hilfe unseres Koordinatensystems algebraisch verfolgen. Annahme eines beliebigen Punktes bedeutet Hinzunahme zweier unbestimmt gelassener Zahlen (der Koordinaten des Punktes) oder, was algebraisch auf dasselbe hinauskommt, Adjunktion zweier Unbestimmten. Alle übrigen Konstruktionen führen auf rationale Operationen, mit Ausnahme der letzten beiden (Schnitt von Kreisen mit Geraden oder mit Kreisen), die auf quadratische Gleichungen, also auf Quadratwurzeln führen.

Also läßt sich x durch $a, b, \ldots$ nebst einigen adjungierten Unbestimmten $u, v, \ldots$ und Quadratwurzeln mittels rationaler Operationen darstellen. Das Ergebnis muß von den Unbestimmten $u, v, \ldots$ unabhängig sein, weil sonst das geometrische Problem unendlich viele Lösungen hätte. Setzt man nun für $u, v, \ldots$ solche rationale Zahlen ein, daß alle vorkommenden rationalen Funktionen sinnvoll bleiben (Quadratwurzeln bleiben immer sinnvoll, wenn man Realität nicht verlangt), so kann x sich nicht geändert haben; also läßt sich x mittels rationaler Operationen und Quadratwurzeln durch $a, b, \ldots$ allein ausdrücken, q. e. d.

Man hat noch zu beachten, daß es bei einem geometrischen Problem nicht darauf ankommt, für jede *spezielle* Wahl der gegebenen Punkte eine Konstruktion zu finden, sondern daß eine *allgemeine* Konstruktion gefordert wird, die (innerhalb gewisser Schranken) immer die Lösung ergibt. Algebraisch kommt das darauf hinaus, daß eine und dieselbe Formel (sie darf Quadratwurzeln enthalten) für alle Werte von $a, b, \ldots$

[1] Einen anderen Beweis erhält man, wenn man alle vorkommenden Zahlen in Real- und Imaginärteil spaltet und nach § 66 die komplexen Quadratwurzeln auf reelle zurückführt, welche dann in bekannter Weise konstruierbar sind.

innerhalb gewisser Schranken eine sinnvolle Lösung x ergibt, welche den Gleichungen des geometrischen Problems genügt. Oder, wie wir auch sagen können, die Gleichungen, durch die x bestimmt wird, und die Quadratwurzeln usw., durch die wir die Gleichungen lösen, müssen sinnvoll bleiben, wenn die gegebenen Elemente $a, b, \ldots$ durch *Unbestimmte* ersetzt werden. Wenn also z. B. gefragt wird, ob die Dreiteilung des Winkels mit Lineal und Zirkel ausführbar ist (ein Problem, welches vermöge der Beziehung

$$\cos 3\varphi = 4\cos^3\varphi - 3\cos\varphi$$

auf die Auflösung der Gleichung

$$4x^3 - 3x = \alpha \qquad (\alpha = \cos 3\varphi) \tag{1}$$

zurückgeführt werden kann), so ist nicht die Frage gemeint, ob für jeden speziellen Wert von α eine Lösung der Gleichung (1) mit Hilfe von Quadratwurzeln gefunden werden kann; sondern es ist gefragt, ob eine allgemeine Lösungsformel der Gleichung (1) existiert; eine Lösungsformel also, die bei unbestimmtem α sinnvoll bleibt.

Wir haben das geometrische Problem der Konstruierbarkeit mit Zirkel und Lineal jetzt auf das folgende algebraische Problem zurückgeführt: Wann läßt eine Größe x sich mittels rationaler Operationen und Quadratwurzeln durch gegebene Größen $a, b, \ldots$ ausdrücken?

Diese Frage ist nicht schwer zu beantworten. $\mathfrak{R}$ sei der Körper der rationalen Funktionen der gegebenen Größen $a, b, \ldots$. Soll sich dann x mittels rationaler Operationen und Quadratwurzeln durch $a, b, \ldots$ ausdrücken lassen, so muß x jedenfalls einem Körper angehören, der aus $\mathfrak{R}$ durch sukzessive Adjunktion endlichvieler Quadratwurzeln, also durch endlichviele Erweiterungen vom Grade 2 entsteht. Adjungiert man nach jeder Quadratwurzel auch noch die Quadratwurzeln aus den konjugierten Körperelementen, so sind nach wie vor alle Erweiterungen quadratisch, und es entsteht somit ein Galoisscher Erweiterungskörper vom Grade 2^m, in dem x liegt. Also:

Damit die Strecke x mit Zirkel und Lineal konstruierbar ist, ist notwendig, daß die Zahl x einem Galoisschen Erweiterungskörper vom Grade 2^m von $\mathfrak{R}$ angehört.

Diese Bedingung ist aber auch hinreichend. Denn die Galoissche Gruppe eines Körpers vom Grade 2^m ist eine Gruppe der Ordnung 2^m, also, wie jede Gruppe von Primzahlpotenzordnung, eine *auflösbare* Gruppe (§ 41, Aufg. 5). Es gibt also eine Kompositionsreihe, deren Kompositionsfaktoren die Ordnung 2 haben, und ihr entspricht nach dem Hauptsatz der Galoisschen Theorie eine Kette von Körpern, in der jeder folgende in bezug auf den vorigen den Grad 2 hat. Eine Erweiterung vom Grade 2 läßt sich aber immer durch Adjunktion einer

Quadratwurzel erzielen; demnach läßt sich die Größe x durch Quadratwurzeln ausdrücken, woraus die Behauptung folgt.

Wir wenden diese allgemeinen Sätze gleich auf einige klassische Probleme an.

Das Delische Problem der *Kubusverdoppelung* führt auf die kubische Gleichung

$$x^3 = 2,$$

die nach dem Eisensteinschen Kriterium irreduzibel ist, so daß jede Wurzel einen Erweiterungskörper vom Grade 3 erzeugt. Ein solcher aber kann niemals Unterkörper eines Körpers vom Grade 2^m sein. *Also ist die Kubusverdoppelung nicht mit Zirkel und Lineal ausführbar.*

Das Problem der *Trisektion des Winkels* führt, wie wir schon sahen, auf die Gleichung

$$4x^3 - 3x - \alpha = 0,$$

wo α eine Unbestimmte ist. Die Irreduzibilität dieser Gleichung im Rationalitätsbereich von α ist leicht nachzuweisen: Hätte die linke Seite einen in α rationalen Faktor, so hätte sie auch einen in α ganzrationalen Faktor; aber ein lineares Polynom in α, dessen Koeffizienten keinen gemeinsamen Teiler haben, ist offenbar irreduzibel. Daraus schließt man wie vorhin, daß die Trisektion des Winkels nicht mit Zirkel und Lineal ausführbar ist.

Eine algebraisch bequemere Form für die Gleichung der Winkeltrisektion erhält man, wenn man zum Rationalitätsbereich von $\alpha = \cos 3\varphi$ noch die Größe

$$i \sin 3\varphi = \sqrt{-(1 - \cos^2 3\varphi)}$$

adjungiert und die Gleichung für

$$y = \cos\varphi + i \sin\varphi$$

sucht. Sie lautet

$$(\cos\varphi + i \sin\varphi)^3 = \cos 3\varphi + i \sin 3\varphi,$$

kurz

$$y^3 = \beta.$$

Auch aus der geometrischen Deutung der komplexen Zahlen geht leicht hervor, daß die Trisektion des Winkels 3φ auf diese reine Gleichung zurückgeführt werden kann.

Die Größen x und y lassen sich mit Hilfe von Quadratwurzeln durcheinander ausdrücken.

Die *Quadratur des Kreises* führt auf die Konstruktion der Zahl π. Ihre Unmöglichkeit wird nachgewiesen sein, wenn gezeigt ist, daß π überhaupt keiner algebraischen Gleichung genügt, m. a. W. transzendent ist; denn dann kann π nicht in einem endlichen Erweiterungskörper

des Körpers der rationalen Zahlen liegen. Hinsichtlich dieses Beweises, der nicht in die Algebra gehört, siehe etwa das Buch von G. HESSENBERG, Transzendenz von e und π.

Die *Konstruktion der regulären Polygone* mit gegebenem Umkreis führt im Falle des h-Ecks auf die Größe

$$2\cos\frac{2\pi}{h} = \zeta + \zeta^{-1},$$

wo ζ die primitive h-te Einheitswurzel $e^{\frac{2\pi i}{h}}$ bedeutet. Da diese Größe nur bei den Substitutionen $\zeta \to \zeta$ und $\zeta \to \zeta^{-1}$ der Galoisschen Gruppe des Kreisteilungskörpers in sich übergeht, also einen reellen Unterkörper vom Grade $\frac{\varphi(h)}{2}$ erzeugt, so erhalten wir als Bedingung für ihre Konstruierbarkeit, daß $\frac{\varphi(h)}{2}$, also auch $\varphi(h)$, eine Potenz von 2 sein soll. Nun ist für $h = 2^\nu q_1^{\nu_1} \dots q_r^{\nu_r}$ (q_i ungerade Primzahlen)

$$\varphi(h) = 2^{\nu-1} q_1^{\nu_1-1} \cdots q_r^{\nu_r-1}(q_1 - 1) \cdots (q_r - 1). \tag{2}$$

(Im Fall $\nu = 0$ fällt der erste Faktor $2^{\nu-1}$ aus.) Die Bedingung besteht also darin, daß die ungeraden Primfaktoren nur in der ersten Potenz in h aufgehen dürfen ($\nu_i = 1$) und außerdem für jede in h aufgehende ungerade Primzahl q_i die Zahl $q_i - 1$ eine Zweierpotenz sein soll; d. h. jedes q_i muß die Form

$$q_i = 2^k + 1$$

haben. Welche sind die Primzahlen von dieser Gestalt?

k kann nicht durch eine ungerade Zahl $\mu > 2$ teilbar sein; denn aus

$$k = \mu\nu, \qquad \mu \not\equiv 0 \pmod 2, \qquad \mu > 2$$

würde folgen, daß $(2^\nu)^\mu + 1$ teilbar durch $2^\nu + 1$, also nicht prim wäre.

Also muß $k = 2^\lambda$ und

$$q_i = 2^{2^\lambda} + 1$$

sein. Die Werte $\lambda = 0, 1, 2, 3, 4$ geben in der Tat Primzahlen q_i, nämlich

$$3, 5, 17, 257, 65537.$$

Für $\lambda = 5$ und einige größere λ (wie weit, ist unbekannt) ist $2^{2^\lambda} + 1$ aber nicht mehr prim; beispielsweise hat $2^{2^5} + 1$ den Teiler 641.

Jedes h-Eck, wo h außer Zweierpotenzen nur die genannten Primzahlen 3, 5, 17, . . in höchstens erster Potenz enthält, ist demnach konstruierbar (GAUSZ). Das Beispiel des 17-Ecks haben wir in § 49 behandelt. Bekannt sind die Konstruktionen des 3-, 4-, 5-, 6-, 8- und 10-Ecks. Die regulären 7- und 9-Ecke sind schon nicht mehr konstruierbar, da sie auf kubische Unterkörper in Kreisteilungskörpern sechsten Grades führen.

Aufgabe. Man zeige, daß die kubische Gleichung

$$x^3 + p x + b$$

im Casus irreducibilis durch eine Substitution $x = \beta x'$ stets auf die Gestalt der Trisektionsgleichung (1) zu bringen ist und leite daraus für diese kubische Gleichung eine Lösungsformel mit trigonometrischen Funktionen ab.

§ 55. Die metazyklischen Gleichungen von Primzahlgrad.

Zu einer irreduziblen Gleichung vom Primzahlgrad q gehört eine transitive Permutationsgruppe vom „Grade" q, d. h. eine transitive Gruppe $\mathfrak{G}$ von Permutationen von q Dingen $1, 2, \ldots, q$. Wir wollen diese Gruppen und ihre Normalteiler untersuchen, und insbesondere sehen, welche Struktur die Gruppe haben kann, wenn sie metazyklisch sein soll.

In § 44 wurde schon bemerkt, daß die Untergruppe $\mathfrak{G}_1$, welche die Ziffer 1 fest läßt, den Index q hat; daraus folgt, daß die Ordnung von $\mathfrak{G}$ durch den Grad q teilbar sein muß. (Für diesen Schluß braucht q noch keine Primzahl zu sein.)

Ist $\mathfrak{H}$ ein Normalteiler von $\mathfrak{G}$, so gibt es zwei Möglichkeiten:

Entweder $\mathfrak{H}$ ist transitiv. Dann ist die Ordnung von $\mathfrak{H}$ wieder durch q teilbar.

Oder $\mathfrak{H}$ ist intransitiv. Ist dann etwa $\{1, 2, \ldots, k\}$ ein Transitivitätsgebiet von $\mathfrak{H}$, und σ eine Substitution aus $\mathfrak{G}$, welche die Ziffer 1 in eine andere, nicht zum Transitivitätsgebiet gehörige Ziffer i überführt, so wird $\sigma\{1, 2, \ldots, k\}$ ein Transitivitätsgebiet von $\sigma\mathfrak{H}\sigma^{-1}$ sein. Da aber $\mathfrak{H}$ Normalteiler ist, ist $\sigma\mathfrak{H}\sigma^{-1} = \mathfrak{H}$; also ist $\sigma\{1, 2, \ldots, k\}$ wieder ein Transitivitätsgebiet von $\mathfrak{H}$, welches zudem aus genau k Ziffern besteht und die Ziffer i enthält. Da i beliebig war, bestehen alle Transitivitätsgebiete aus gleich vielen, nämlich k Ziffern; somit ist k ein (echter) Teiler von q.

Ist nun, wie zu Anfang vorausgesetzt, q eine Primzahl, so kommt nur $k = 1$ in Frage; in diesem Fall läßt aber $\mathfrak{H}$ alle Ziffern $1, 2, \ldots, q$ fest. Also:

Ein Normalteiler $\mathfrak{H}$ einer transitiven Permutationsgruppe vom Primzahlgrad q ist entweder transitiv oder gleich $\mathfrak{E}$.

Wir beweisen nun den Satz:

Eine transitive metazyklische Gruppe $\mathfrak{G}$ vom Primzahlgrad q läßt sich bei passender Numerierung der Permutationsobjekte $1, 2, \ldots, q$ stets als Gruppe von linearen Substitutionen modulo q schreiben:

$$\tau(z) \equiv a z + b \pmod q \quad (a \not\equiv 0 (q);\ z = 1, 2, \ldots, q),$$

und in der Gruppe kommen stets alle Substitutionen mit $a = 1$:

$$\sigma(z) \equiv z + b \qquad (b = 1, \ldots, q),$$

vor.

Beweis. Die Ordnung der Gruppe $\mathfrak{G}$ ist durch q teilbar. Ist sie gleich q, so ist die Gruppe zyklisch (denn die Ordnung eines beliebigen von der Einheit verschiedenen Elements σ kann, als Teiler von q, nur gleich q sein, und dann erzeugt σ schon die ganze Gruppe). Die erzeugende Permutation σ muß aus einem einzigen, alle Ziffern $1, 2, \ldots, q$ enthaltenden Zyklus bestehen; denn sonst wäre die Gruppe nicht transitiv. Bei passender Numerierung ist daher

$$\sigma = (1\,2 \ldots q),$$

mithin

$$\sigma(z) \equiv z + 1 \pmod q,$$

$$\sigma^b(z) \equiv z + b \pmod q \qquad (b = 1, \ldots, q).$$

In diesem Fall ist der Satz also bewiesen. Wir können also eine Induktion nach der Ordnung der Gruppe $\mathfrak{G}$ vornehmen und voraussetzen, diese Ordnung sei eine zusammengesetzte Zahl $q \cdot j$ und der Satz sei (bei festem q) für alle Gruppen kleinerer Ordnung richtig.

Wegen der Auflösbarkeit von $\mathfrak{G}$ gibt es einen von $\mathfrak{E}$ verschiedenen auflösbaren Normalteiler $\mathfrak{H}$ von Primzahlindex. Auf Grund des vorangehenden Satzes ist dieser Normalteiler $\mathfrak{H}$ transitiv und daher nach der Induktionsvoraussetzung eine Gruppe von linearen Substitutionen modulo q, welche die Gruppe der Substitutionen $z \to z + b$ umfaßt.

Die Substitutionen $z \to z + b$ sind, wie man leicht sieht, für $b \not\equiv 0$ stets q-gliedrige Zyklen. Sie sind in der Gruppe $\mathfrak{H}$ die einzigen; denn jede andere Substitution $z \to az + b$ läßt ein Element z fest, das aus

$$az + b \equiv z,$$
$$(a - 1)z \equiv -b$$

bestimmt werden kann.

Ist nun σ die Substitution

$$\sigma(z) \equiv z + 1$$

und τ eine beliebige Substitution aus $\mathfrak{G}$, so ist $\tau\sigma\tau^{-1}$ wieder ein q-gliedriger Zyklus und wieder in $\mathfrak{H}$ enthalten, also wieder von der Form

$$\tau\sigma\tau^{-1}(z) \equiv z + a.$$

Es sei nun $\tau^{-1}(z) = \zeta$, also $z = \tau(\zeta)$,

$$\tau\sigma(\zeta) \equiv \tau(\zeta) + a,$$
$$\tau(\zeta + 1) \equiv \tau(\zeta) + a.$$

Hieraus folgt durch Induktion nach ν:

$$\tau(\zeta + \nu) \equiv \tau(\zeta) + \nu a,$$

insbesondere für $\zeta = 0$, wenn $\tau(0) = b$ gesetzt wird:

$$\tau(\nu) \equiv \nu a + b.$$

Also ist τ eine lineare Substitution modulo q. Und da die Substitutionen $\sigma(z) \equiv z + b$ schon sämtlich in $\mathfrak{H}$ enthalten sind, sind sie auch in $\mathfrak{G}$ enthalten. Damit ist der Satz bewiesen.

Umgekehrt: *Jede Gruppe $\mathfrak{G}$ von linearen Substitutionen modulo q, die die Substitutionen*

$$\sigma(z) \equiv z + b$$

sämtlich enthält, ist auflösbar.

Beweis. Die eben genannten Substitutionen σ bilden einen Normalteiler $\mathfrak{N}$ in $\mathfrak{G}$; denn mit σ ist auch jedes $\tau\sigma\tau^{-1}$ ein q-gliedriger Zyklus bzw. die Identität. In jeder Nebenklasse $\mathfrak{N}\tau$, wo τ die Substitution

$$\tau(z) \equiv az + b$$

darstellt, kommt auch die Substitution $\sigma^{-1}\tau$ vor:

$$\sigma^{-1}\tau(z) \equiv az.$$

Die Zusammensetzung zweier Nebenklassen geschieht demnach am bequemsten so, daß man einfach die Substitutionen $\tau'(z) \equiv az$ zusammensetzt. Das geschieht aber einfach durch Multiplikation der Koeffizienten a (die demnach eine multiplikative Gruppe modulo q bilden). Also bilden die Nebenklassen nach $\mathfrak{N}$ eine Abelsche Gruppe: $\mathfrak{G}/\mathfrak{N}$ ist Abelsch. Da auch $\mathfrak{N}$ Abelsch ist, ist $\mathfrak{G}$ auflösbar.

Folgerungen. Eine von der Identität verschiedene lineare Substitution

$$\sigma(z) \equiv az + b$$

läßt höchstens ein Element z fest; denn die Kongruenz

$$(a - 1)\, z \equiv -b \pmod{q}$$

hat höchstens eine Lösung, es sei denn, daß $a \equiv 1$ und $b \equiv 0$ ist. Das heißt, *die einzige Untergruppe, die zwei Ziffern i, k fest läßt, ist die Einheitsgruppe.*

Die bei unseren Beweisen benutzten Überlegungen geben uns zugleich das Mittel, alle Normalteiler der linearen Gruppe $\mathfrak{G}$ aufzustellen. Es zeigte sich ja, daß jeder Normalteiler (außer $\mathfrak{E}$) den Normalteiler $\mathfrak{N}$ umfassen muß und daß in jeder Nebenklasse nach $\mathfrak{N}$ eine Substitution $\tau(z) \equiv az$ vorhanden ist. Es genügt also, in der multiplikativen Gruppe der vorkommenden a (mod q) alle Untergruppen zu bestimmen. Nun ist die Gruppe *aller* Restklassen $\not\equiv 0$ (mod q) zyklisch, und jede Untergruppe ebenfalls. Hat die gegebene Gruppe von Restklassen die Ordnung j, so gehört also zu jedem Teiler von j eine Untergruppe.

Sind die Permutationsobjekte die Wurzeln einer Gleichung und ist $\mathfrak{G}$ die Galoissche Gruppe der Gleichung, so lassen sich unsere Gruppensätze sofort körpertheoretisch deuten. Wir erhalten:

Die Gruppe einer irreduziblen metazyklischen Gleichung vom Primzahlgrad q über dem Körper K läßt sich bei passender Numerierung der Wurzeln stets als Gruppe von linearen Substitutionen der Nummern mod q auffassen. Der Grad des Zerfällungskörpers $\mathsf{K}(\alpha_1, \ldots, \alpha_q)$ ist $q \cdot j$, wo $j \mid q - 1$. Es gibt einen Galoisschen Zwischenkörper vom Grade j, in dem alle anderen Galoisschen Zwischenkörper enthalten sind. Zu jedem Teiler von j gehört ein Galoisscher Zwischenkörper. Der Zwischenkörper $\mathsf{K}(\alpha_i, \alpha_k)$, der von zwei Wurzeln α_i, α_k erzeugt wird, ist notwendig schon mit dem ganzen Körper $\mathsf{K}(\alpha_1, \ldots, \alpha_q)$ identisch.

Aufgaben. 1. Eine metazyklische irreduzible Gleichung vom Primzahlgrad $q \neq 2$ über einem reellen Zahlkörper K hat entweder nur eine reelle Wurzel, oder alle ihre Wurzeln sind reell.

2. Eine irreduzible Gleichung 5. Grades mit genau 3 reellen Wurzeln ist nicht durch Radikale auflösbar.

3. Mit Hilfe von 2. ist zu beweisen, daß die Gleichung

$$x^5 - 4x + 2 = 0$$

nicht durch Radikale lösbar ist. [Zur Bestimmung der Anzahl der reellen Wurzeln kann man Sätze aus Kap. 10, z. B. den Satz von WEIERSTRASZ und den von ROLLE heranziehen.]

§ 56. Die Berechnung der Galoisschen Gruppe. Gleichungen mit symmetrischer Gruppe.

Eine Methode, mit der man (wenigstens in Theorie) die Galoissche Gruppe einer Gleichung $f(x) = 0$ in bezug auf einen Körper Δ wirklich aufstellen kann, ist die folgende.

Die Wurzeln der Gleichung seien $\alpha_1, \ldots, \alpha_n$. Man bilde mit Hilfe der Unbestimmten $u_1, \ldots, u_n$ den Ausdruck

$$\Theta = u_1 \alpha_1 + \cdots + u_n \alpha_n,$$

übe auf ihn alle Permutationen s_u der Unbestimmten u aus, und bilde das Produkt

$$F(z, u) = \prod_s (z - s_u \Theta).$$

Dieses Produkt ist offensichtlich eine symmetrische Funktion der Wurzeln und kann daher nach § 24 durch die Koeffizienten von $f(x)$

ausgedrückt werden. Nun zerlege man $F(z, u)$ in irreduzible Faktoren in $\Delta[u, z]$:

$$F(z, u) = F_1(z, u) F_2(z, u) \dots F_r(z, u).$$

Die Permutationen s_u, die irgend einen der Faktoren, etwa F_1, in sich überführen, bilden eine Gruppe $\mathfrak{g}$. Nun behaupten wir, *daß* $\mathfrak{g}$ *genau die Galoissche Gruppe der gegebenen Gleichung ist.*

Beweis. Nach Adjunktion aller Wurzeln zerfällt F und daher auch F_1 in Linearfaktoren $z - \Sigma u_\lambda \alpha_\nu$, mit den Wurzeln α_ν in irgendeiner Anordnung als Koeffizienten. Wir numerieren nun die Wurzeln so, daß F_1 den Faktor $z - (u_1\alpha_1 + \cdots + u_n\alpha_n)$ enthält. Im folgenden bezeichne immer s_u irgend eine Permutation der u_α und s_α dieselbe Permutation der α. Dann läßt offenbar das Produkt $s_u s_\alpha$ den Ausdruck $\Theta = u_1\alpha_1 + \cdots + u_n\alpha_n$ invariant, d. h. es ist

$$s_u s_\alpha \Theta = \Theta$$
$$s_\alpha \Theta = s_u^{-1} \Theta .$$

Wenn s_u zur Gruppe $\mathfrak{g}$ gehört, d. h. F_1 invariant läßt, so transformiert s_u jeden Linearfaktor von F_1, insbesondere den Faktor $z - \Theta$, wieder in einen Linearfaktor von F_1. Wenn umgekehrt eine Permutation s_u den Faktor $z - \Theta$ in einen anderen Linearfaktor von F_1 transformiert, so transformiert sie F_1 in ein in $\Delta[u, z]$ irreduzibles Polynom, Teiler von $F(z, u)$, also wieder in eins der Polynome F_j, aber in ein solches, das mit F_1 einen Linearfaktor gemein hat, also notwendigerweise in F_1 selbst; mithin gehört dann s_u zu $\mathfrak{g}$. Also besteht $\mathfrak{g}$ aus den Permutationen der u, welche $z - \Theta$ wieder in einen Linearfaktor von F_1 transformieren.

Die Permutationen s_α der Galoisschen Gruppe von $f(x)$ sind solche Permutationen der α, welche die Größe

$$\Theta = u_1\alpha_1 + \cdots + u_n\alpha_n$$

in ihre konjugierten Größen überführen, für die also $s_\alpha\Theta$ derselben irreduziblen Gleichung wie Θ genügt, d. h. es sind die Permutationen s_α, die den Linearfaktor $z - \Theta$ in die anderen Linearfaktoren von F_1 überführen. Wegen $s_\alpha\Theta = s_u^{-1}\Theta$ führt dann auch s_u^{-1} den Linearfaktor $z - \Theta$ wieder in einen Linearfaktor von F_1 über, d. h. s_u^{-1} und damit auch s_u gehört zu $\mathfrak{g}$. Und umgekehrt. Also besteht die Galoissche Gruppe aus genau denselben Permutationen wie die Gruppe $\mathfrak{g}$, nur auf die α statt auf die u angewandt.

Diese Methode zur Bestimmung der Galoisschen Gruppe ist nicht so sehr praktisch von Interesse als wegen einer theoretischen Folgerung, die so lautet:

Es sei $\mathfrak{R}$ *ein Integritätsbereich mit Einselement, in dem der Satz von der eindeutigen Primfaktorzerlegung gilt. Es sei* $\mathfrak{p}$ *ein Primideal in* $\mathfrak{R}$,

$\overline{\mathfrak{R}} = \mathfrak{R}/\mathfrak{p}$ *der Restklassenring. Die Quotientenkörper von* $\mathfrak{R}$ *und* $\overline{\mathfrak{R}}$ *seien* Δ *und* $\overline{\Delta}$. *Es sei* $f(x) = x^n + \cdots$ *ein Polynom aus* $\mathfrak{R}[x]$, $\overline{f}(x)$ *das ihm in der Homomorphie* $\mathfrak{R} \to \overline{\mathfrak{R}}$ *zugeordnete Polynom, beide als doppelwurzelfrei vorausgesetzt. Dann ist die Galoissche Gruppe* $\overline{\mathfrak{g}}$ *der Gleichung* $\overline{f} = 0$ *in bezug auf* $\overline{\Delta}$ *(als Permutationsgruppe der passend angeordneten Wurzeln) eine Untergruppe der Galoisschen Gruppe* $\mathfrak{g}$ *von* $f = 0$.

Beweis. Die Zerlegung von

$$F(z, u) = \prod_s (z - s_u \Theta)$$

in irreduzible Faktoren $F_1 F_2 \ldots F_k$ in $\Delta[z, u]$ kann nach § 21 ganzrational in $\mathfrak{R}[z, u]$ geschehen und überträgt sich dann vermöge des Homomorphismus auf $\overline{\mathfrak{R}}[z, u]$:

$$\overline{F}(z, u) = \overline{F}_1 \overline{F}_2 \ldots \overline{F}_k .$$

Die Faktoren $\overline{F}_1, \ldots$ können eventuell noch weiter zerlegbar sein. Die Permutationen von $\mathfrak{g}$ führen F_1 und daher auch $\overline{F}_1$ in sich, die übrigen Permutationen der u führen $\overline{F}_1$ in $\overline{F}_2, \ldots, \overline{F}_k$ über. Die Permutationen von $\overline{\mathfrak{g}}$ führen einen irreduziblen Faktor von $\overline{F}_1$ in sich über, also können sie $\overline{F}_1$ nicht in $\overline{F}_2, \ldots, \overline{F}_k$ überführen, sondern müssen $\overline{F}_1$ in $\overline{F}_1$ überführen, d. h. $\overline{\mathfrak{g}}$ ist Untergruppe von $\mathfrak{g}$.

Der Satz wird oft angewandt zur Bestimmung der Gruppe $\mathfrak{g}$. Insbesondere wählt man das Ideal $\mathfrak{p}$ oft so, daß das Polynom $f(x)$ mod $\mathfrak{p}$ zerfällt, weil dann die Galoissche Gruppe $\overline{\mathfrak{g}}$ von $\overline{f}$ leichter zu bestimmen ist. Es sei z. B. $\mathfrak{R}$ der Ring der ganzen Zahlen und $\mathfrak{p} = (p)$, wo p eine Primzahl. Modulo p zerfalle $f(x)$ folgendermaßen:

$$f(x) \equiv \varphi_1(x)\, \varphi_2(x) \ldots \varphi_k(x) \quad (p) .$$

Es folgt

$$\overline{f} = \overline{\varphi}_1 \overline{\varphi}_2 \ldots \overline{\varphi}_h .$$

Die Galoissche Gruppe $\overline{\mathfrak{g}}$ von $\overline{f}(x)$ ist immer zyklisch, da die Automorphismengruppe eines Galoisfeldes stets zyklisch ist (§ 31). Die erzeugende Permutation s von $\overline{\mathfrak{g}}$ sei, in Zyklen zerlegt:

$$(1\,2 \ldots j)\ (j+1 \ldots) \ldots$$

Da die Transitivitätsgebiete der Gruppe $\overline{\mathfrak{g}}$ genau den irreduziblen Faktoren von $\overline{f}$ entsprechen, so müssen die in den Zyklen $(1\,2 \ldots j)$, $(\ldots)$, $\ldots$ vorkommenden Nummern genau die Wurzeln von $\overline{\varphi}_1$, von $\overline{\varphi}_2$, $\ldots$ angeben. Sobald man also die Grade j, k, $\ldots$ von φ_1, φ_2, $\ldots$ kennt, ist der Typus der Substitution s bekannt: s besteht dann aus einem j-gliedrigen, einem k-gliedrigen Zyklus, usw. Da nun nach dem obigen Satz bei passender Anordnung der Wurzeln $\overline{\mathfrak{g}}$ eine Untergruppe von $\mathfrak{g}$ ist, so *muß* $\mathfrak{g}$ *eine Permutation vom gleichen Typus enthalten.*

Wenn also z. B. eine ganzzahlige Gleichung 5-ten Grades modulo irgend einer Primzahl in einen irreduziblen Faktor 2-ten und einen 3-ten Grades zerfällt, so enthält die Galoissche Gruppe eine Permutation vom Typus (12) (345).

Beispiel. Vorgelegt sei die ganzzahlige Gleichung

$$x^5 - x - 1 = 0 .$$

Modulo 2 ist die linke Seite zerlegbar in

$$(x^2 + x + 1)(x^3 + x^2 + 1)$$

und modulo 3 ist sie irreduzibel, denn hätte sie einen linearen oder quadratischen Faktor, so müßte sie mit $x^9 - x$ einen Faktor gemein haben (§ 31, Aufg. 6), also entweder mit $x^5 - x$ oder mit $x^5 + x$ einen Faktor gemein haben, was offensichtlich nicht der Fall ist. Also enthält ihre Gruppe einen Fünferzyklus und ein Produkt $(ik)(l\,m\,n)$. Die dritte Potenz der letzteren Permutation ist (ik); diese, transformiert mit (12345) und dessen Potenzen, ergibt eine Kette von Transpositionen (ik), (kp), (pq), (qr), (ri), die zusammen die symmetrische Gruppe erzeugen. Also ist die Gruppe $\mathfrak{g}$ die *symmetrische.*

Man kann die erwähnten Tatsachen benutzen zur Konstruktion von Gleichungen beliebigen Grades, deren Gruppe die symmetrische ist, auf Grund des folgenden Satzes: *Eine transitive Permutationsgruppe von n Objekten, die einen Zweierzyklus und einen* $(n-1)$*-Zyklus enthält, ist die symmetrische Gruppe.*

Beweis. Es sei $(1\,2\,\ldots\,n-1)$ der $(n-1)$-Zyklus. Der Zweierzyklus (ij) kann vermöge der Transitivität in (kn) transformiert werden, wo k eine der Ziffern von 1 bis $(n-1)$ ist. Transformation von (kn) mit $(1\,2\,\ldots\,n-1)$ und dessen Potenzen ergibt alle Zyklen $(1\,n)$, $(2\,n)$, $\ldots$, $(n-1\,n)$, und diese erzeugen zusammen die symmetrische Gruppe.

Um auf Grund dieses Satzes eine Gleichung n-ten Grades $(n > 3)$ zu konstruieren, deren Gruppe die symmetrische ist, wähle man zunächst ein mod 2 irreduzibles Polynom n-ten Grades, f_1, sodann ein Polynom f_2, das in einen mod 3 irreduziblen Faktor $(n-1)$-ten Grades und einen Linearfaktor zerfällt, und schließlich ein Polynom f_3 vom Grade n, das sich mod 5 zerlegt in einen quadratischen Faktor und einen oder zwei Faktoren ungeraden Grades (alle irreduzibel mod 5). Das geht alles, weil es modulo jeder Primzahl irreduzible Polynome jeden Grades gibt (§ 31, Aufg. 6). Schließlich wähle man f so, daß

$$f \equiv f_1 \pmod 2$$
$$f \equiv f_2 \pmod 3$$
$$f \equiv f_3 \pmod 5$$

ist, was immer möglich ist. Es genügt zum Beispiel,

$$f = -15 f_1 + 10 f_2 + 6 f_3$$

zu wählen. Die Galoissche Gruppe ist dann transitiv (weil das Polynom mod 2 irreduzibel ist), enthält einen Zyklus vom Typus $(12 \ldots n-1)$, und enthält einen Zweierzyklus multipliziert mit Zyklen ungerader Ordnung. Erhebt man dieses Produkt in eine passende ungerade Potenz, so erhält man einen reinen Zweierzyklus und schließt nach dem obigen Satz, daß die Galoissche Gruppe die symmetrische ist.

Die angegebene Konstruktionsmethode ist natürlich lange nicht die einzige. Man kann z. B., um die Irreduzibilität der Gleichung und damit die Transitivität der Gruppe zu erzwingen, auch den Eisensteinschen Satz (§ 22) benutzen. Für Gleichungen ungeraden Grades $n > 3$ kann man noch einfacher verfahren, indem man Sorge trägt, daß die Gleichung mod 2 in Faktoren der Grade $(n-1)$ und 1, mod 3 aber in Faktoren der Grade $(n-2)$ und 2 zerfällt. Die Irreduzibilität ist dann automatisch gewährleistet. Für alle geraden Gradzahlen > 6 erreicht man dasselbe, indem man modulo 2 wie vorhin, modulo 3 aber in Faktoren der Grade 2, 3 und $n-5$ zerfallen läßt. Andere Kriterien und Methoden um Gleichungen der verlangten Art zu bilden findet man bei PH. FURTWÄNGLER, Math. Ann. Bd. 85, S. 34—40. Ob es Gleichungen mit rationalen Koeffizienten gibt, deren Gruppe eine beliebig vorgegebene Permutationsgruppe ist, ist im allgemeinen ein ungelöstes Problem; vgl. dazu E. NOETHER, Gleichungen mit vorgeschriebener Gruppe. Math. Ann. Bd. 78, S. 221.

Aufgaben. 1. Was ist (in bezug auf den rationalen Zahlkörper) die Gruppe der Gleichung

$$x^4 + 2x^2 + x + 3 = 0?$$

2. Man konstruiere eine Gleichung 6-ten Grades, deren Gruppe die symmetrische ist.

Achtes Kapitel.

Geordnete und wohlgeordnete Mengen.

Das Kapitel enthält diejenigen allgemeinen Sätze über Ordnung und insbesondere Wohlordnung von beliebigen Mengen, die in der Theorie der unendlichen Körpererweiterungen (Kap. 9 und 10) Verwendung finden.

§ 57. Geordnete Mengen.

Eine Menge heißt *geordnet*, wenn für ihre Elemente durch irgend eine Festsetzung eine Relation $a < b$ definiert ist derart, daß

1. für je zwei Elemente a, b entweder $a < b$ oder $b < a$ oder $a = b$ ist,
2. die Relationen $a < b$, $b < a$, $a = b$ sich gegenseitig ausschließen,
3. aus $a < b$ und $b < c$ folgt $a < c$.

Die Relation $a < b$ braucht keine wirkliche Größenbeziehung zu sein (wie es bei der Relation $a < b$ im Bereich der ganzen Zahlen der Fall war), sondern sie kann irgendwie definiert sein; nur muß für irgend zwei Elemente a, b feststehen, ob $a < b$ oder nicht. Zum Beispiel ist eine Menge geordnet, wenn man ihre Elemente in irgend einer Reihenfolge anschreibt und $a < b$ nennt, sobald a früher als b angeschrieben wird.

Aus der Relation $a < b$ definiert man einige abgeleitete Relationen:

$a > b$ soll heißen $b < a$;

$a \leqq b$ soll heißen: entweder $a = b$ oder $a < b$;

$a \geqq b$ soll heißen: entweder $a = b$ oder $a > b$.

Demzufolge ist $a \leqq b$ gleichbedeutend mit der Negation von $a > b$, ebenso $a \geqq b$ mit der Negation von $a < b$.

Ist $a < b$, so nennt man *a früher als b*, *b später als a*, und man sagt, daß a dem b *vorangeht*.

Es kann vorkommen, daß eine Menge ein „erstes Element" hat, welches allen anderen vorangeht. Beispiel: die 1 in der Reihe der natürlichen Zahlen (mit der gewöhnlichen Größenrelation $a < b$ als Ordnungsrelation). In der Menge aller (positiven und negativen) ganzen Zahlen gibt es aber kein erstes Element.

Wenn eine Menge geordnet ist, so ist durch dieselbe Relation $a < b$ auch jede ihrer Untermengen geordnet.

Eine geordnete Menge heißt *wohlgeordnet*, falls jede nichtleere Untermenge (insbesondere die Menge selbst) ein erstes Element besitzt.

Beispiele:

1. Jede geordnete endliche Menge ist wohlgeordnet (vgl. Aufg. 1, unten).

2. Die Reihe der natürlichen Zahlen $1, 2, 3, \ldots$ ist wohlgeordnet; denn in jeder nicht leeren Menge von natürlichen Zahlen gibt es ein erstes Element.

3. Die Menge aller ganzen Zahlen $\ldots, -2, -1, 0, 1, 2, \ldots$ in „natürlicher" Anordnung ist nicht wohlgeordnet; denn sie besitzt kein erstes Element. Man kann sie aber wohlordnen, indem man sie anders anordnet, etwa so:

$$0, 1, -1, 2, -2, \ldots$$

oder so:

$$1, 2, 3, \ldots; \quad 0, -1, -2, -3, \ldots,$$

wo alle positiven Zahlen allen übrigen vorangehen und die Zahlen im übrigen nach dem Betrag geordnet werden.

Aufgaben. 1. Man beweise, daß es in jeder geordneten nicht leeren endlichen Menge ein erstes Element gibt.

2. Für die Menge der Paare natürlicher Zahlen (a, b) definiere man eine Ordnungsrelation folgendermaßen: Es sei $(a, b) < (a', b')$, wenn entweder $a < a'$ oder $a = a'$, $b < b'$. Man beweise, daß dadurch eine Wohlordnung definiert ist.

3. In einer wohlgeordneten Menge hat jedes Element a (mit Ausnahme des eventuell vorhandenen letzten Elements der Menge) einen „unmittelbaren Nachfolger" $b > a$, so daß es kein Element x zwischen b und a (d. h. mit $b > x > a$) mehr gibt. Das ist zu beweisen. Hat auch jedes Element mit Ausnahme des ersten einen unmittelbaren Vorgänger?

§ 58. Das Auswahlpostulat und der Wohlordnungssatz.

ZERMELO hat zuerst bemerkt, daß vielen mathematischen Untersuchungen eine Annahme zugrunde liegt, die er als erster ausdrücklich formuliert und *Auswahlpostulat* genannt hat. Sie lautet:

Ist eine Menge von nichtleeren Mengen gegeben, so gibt es eine „Auswahlfunktion", d. h. eine Funktion, die jeder dieser Mengen eins ihrer Elemente zuordnet.

Man bemerke, daß jede einzelne Menge als nichtleer vorausgesetzt wurde, daß man also aus jeder dieser Mengen stets ein Element auswählen kann. Das Postulat besagt nur, daß man aus allen diesen Mengen gleichzeitig durch eine einzige Zuordnung eine Auswahl vornehmen kann.

Wir werden im folgenden immer, wo wir es nötig haben, die Richtigkeit des Auswahlpostulats annehmen.

Die wichtigste Konsequenz des Auswahlpostulats ist der *Zermelosche Wohlordnungssatz*:

Jede Menge $\mathfrak{M}$ kann wohlgeordnet werden.

ZERMELO hat für diesen Satz zwei Beweise gegeben[1]; wir geben hier den zweiten wieder.

Um kurz anzudeuten, worauf der Beweis beruht, denken wir uns die Wohlordnung schon ausgeführt. Jedes Element a bestimmt dann einen „*Abschnitt*" $\mathfrak{A}(a)$ (bestehend aus den Elementen $< a$) und einen „*Rest*" $\mathfrak{R}(a)$ (bestehend aus den Elementen $\geqq a$). Der Beweis geht nun darauf aus, zunächst die Menge dieser Restmengen $\mathfrak{R}(a)$ zu konstruieren, und zwar wird es so eingerichtet, daß a gerade dasjenige Element ist, das in $\mathfrak{R}(a)$ ausgezeichnet wird, wenn man vermöge des Auswahlprinzips in allen Untermengen von $\mathfrak{M}$ ein Element auszeichnet. Die Menge, die aus $\mathfrak{R}(a)$ durch Weglassung von a entsteht, ist wieder ein Rest (nämlich der Rest des auf a folgenden Elements). Ebenso ist der Durchschnitt beliebig vieler Reste wieder ein Rest. Die gegebene Menge $\mathfrak{M}$ selbst ist auch Rest. Schließlich ist, wenn $\mathfrak{R}(a)$ und $\mathfrak{R}(b)$ verschiedene Reste sind, entweder $\mathfrak{R}(a) \subset \mathfrak{R}(b)$ oder $\mathfrak{R}(a) \supset \mathfrak{R}(b)$ (je nachdem $a > b$ oder $a < b$ ist). Eine Menge von Untermengen mit diesen Eigenschaften soll nun zuerst konstruiert werden.

Die Untermengen von $\mathfrak{M}$ werden im folgenden mit $\mathfrak{A}, \mathfrak{B}, \ldots$ bezeichnet.

Man ordne zunächst, entsprechend dem Auswahlpostulat, jeder nichtleeren Untermenge $\mathfrak{A}$ von $\mathfrak{M}$ ein „ausgezeichnetes Element" a zu. Mit $\mathfrak{A}'$ bezeichnen wir die Menge, die aus $\mathfrak{A}$ durch Weglassung von a entsteht. Die Strichelung soll in diesem Beweis durchweg dieselbe Bedeutung haben.

Eine Menge K von Untermengen von $\mathfrak{M}$ heißt eine *Θ-Kette*, wenn sie folgende Eigenschaften hat:

1. $\mathfrak{M}$ selbst gehört zu K.

[1] Math. Ann. Bd. 59 (1904), S. 514; Math. Ann. Bd. 65 (1908), S. 107.

2. Wenn $\mathfrak{A}$ zu K gehört und nicht leer ist, so gehört auch $\mathfrak{A}'$ zu K.

3. Wenn die Elemente $\mathfrak{A}, \mathfrak{B}, \ldots$ einer Menge $\mathsf{A} = \{\mathfrak{A}, \mathfrak{B}, \ldots\}$ alle zu K gehören, so gehört auch der Durchschnitt $\mathfrak{D}(\mathsf{A})$ zu K.

Zunächst gibt es eine Θ-Kette, nämlich die Menge aller Untermengen von $\mathfrak{M}$. Weiter ist der Durchschnitt mehrerer Θ-Ketten offenbar selbst eine Θ-Kette. Daher ist der Durchschnitt Δ aller Θ-Ketten wieder eine Θ-Kette. Δ ist offenbar eine minimale Θ-Kette; d. h. eine echte Untermenge von Δ ist keine Θ-Kette mehr.

Wir betrachten insbesondere solche Mengen $\mathfrak{A}$ der Kette Δ, die die Eigenschaft haben, daß alle übrigen Mengen der Kette entweder Obermengen oder Untermengen von $\mathfrak{A}$ sind. Nachher wird sich zeigen, daß diese Eigenschaft allen $\mathfrak{A}$ der Kette zukommt; jetzt aber stellen wir nur fest, daß $\mathfrak{M}$ die Eigenschaft hat. Die echten Obermengen von $\mathfrak{A}$ innerhalb der Kette bezeichnen wir mit $\mathfrak{O}_{\mathfrak{A}}$, die echten Untermengen mit $\mathfrak{U}_{\mathfrak{A}}$. Ist ein $\mathfrak{U}_{\mathfrak{A}}$ sogar Untermenge von $\mathfrak{A}'$, so bezeichnen wir es mit $\mathfrak{V}_{\mathfrak{A}}$.

Nun bilden (für ein festes $\mathfrak{A}$) die $\mathfrak{O}_{\mathfrak{A}}$ zusammen mit $\mathfrak{A}$ und den $\mathfrak{V}_{\mathfrak{A}}$ wieder eine Θ-Kette; denn:

a) $\mathfrak{M}$ ist entweder ein $\mathfrak{O}_{\mathfrak{A}}$ oder gleich $\mathfrak{A}$.

b) Jedes $(\mathfrak{O}_{\mathfrak{A}})'$, abgeleitet aus einem $\mathfrak{O}_{\mathfrak{A}}$, ist entweder selbst ein $\mathfrak{O}_{\mathfrak{A}}$ oder gleich $\mathfrak{A}$. Denn wäre es das nicht, so müßte es (als Element von Δ) eine Untermenge von $\mathfrak{A}$ sein, sogar eine echte. Es gäbe also in $\mathfrak{A}$ ein Element, das nicht zu $(\mathfrak{O}_{\mathfrak{A}})'$ gehörte. Außerdem gibt es noch ein Element in $\mathfrak{O}_{\mathfrak{A}}$, das nicht zu $\mathfrak{A}$ gehört, also erst recht nicht zu der Untermenge $(\mathfrak{O}_{\mathfrak{A}})'$ gehören würde. Es gäbe also zwei verschiedene Elemente in $\mathfrak{O}_{\mathfrak{A}}$, die nicht zu $(\mathfrak{O}_{\mathfrak{A}})'$ gehörten, entgegen der Definition von $(\mathfrak{O}_{\mathfrak{A}})'$.

c) $\mathfrak{A}'$ sowie jedes $\mathfrak{V}_{\mathfrak{A}}$ gehört wieder zu Δ und ist jedesmal Untermenge von $\mathfrak{A}'$, also ein $\mathfrak{V}_{\mathfrak{A}}$.

d) Jeder Durchschnitt mehrerer $\mathfrak{O}_{\mathfrak{A}}$, eventuell mit $\mathfrak{A}$, ist wieder Obermenge von $\mathfrak{A}$ und gehört zu Δ, ist also wieder ein $\mathfrak{O}_{\mathfrak{A}}$ oder $\mathfrak{A}$.

e) Jeder Durchschnitt mehrerer $(\mathfrak{V}_{\mathfrak{A}})'$ eventuell mit einigen $\mathfrak{O}_{\mathfrak{A}}$ oder $\mathfrak{A}$, ist Untermenge von $\mathfrak{A}'$ und gehört zu Δ, ist also wieder ein $\mathfrak{V}_{\mathfrak{A}}$.

Damit sind die Ketteneigenschaften nachgewiesen.

Da aber Δ eine minimale Θ-Kette war, so erschöpfen die $\mathfrak{O}_{\mathfrak{A}}$, $\mathfrak{A}$ und die $\mathfrak{V}_{\mathfrak{A}}$ zusammen die ganze Kette Δ. Mithin ist jedes $\mathfrak{U}_{\mathfrak{A}}$, da es weder $\mathfrak{A}$ noch ein $\mathfrak{O}_{\mathfrak{A}}$ sein kann, ein $\mathfrak{V}_{\mathfrak{A}}$.

Daraus folgt, daß auch $\mathfrak{A}'$ dieselbe Eigenschaft hat, die von $\mathfrak{A}$ vorausgesetzt wurde, d. h. daß alle anderen Elemente von Δ entweder Obermengen oder Untermengen von $\mathfrak{A}'$ sind.

Ist nun weiter $\mathfrak{D}$ ein Durchschnitt mehrerer Mengen $\mathfrak{A}, \mathfrak{B}, \ldots$ von der soeben für $\mathfrak{A}$ vorausgesetzten Beschaffenheit und ist $\mathfrak{X}$ eine andere Menge aus der Kette Δ, so sind nur zwei Fälle möglich: Entweder umfaßt $\mathfrak{X}$ eine der Mengen $\mathfrak{A}, \mathfrak{B}, \ldots$ und damit auch $\mathfrak{D}$, oder $\mathfrak{X}$ ist in allen $\mathfrak{A}, \mathfrak{B}, \ldots$ und damit auch in $\mathfrak{D}$ als Untermenge enthalten. Also hat auch $\mathfrak{D}$ die genannte Beschaffenheit.

Da endlich $\mathfrak{M}$ selbst die von $\mathfrak{A}$ vorausgesetzte Beschaffenheit hat, so bilden die so beschaffenen Elemente von Δ wieder eine Θ-Kette. Da Δ minimal ist, muß diese Θ-Kette mit Δ selbst übereinstimmen. Also haben alle Mengen von Δ die früher genannte Beschaffenheit, und für zwei beliebige Mengen $\mathfrak{A}, \mathfrak{B}$ aus Δ ist entweder $\mathfrak{A} \subseteq \mathfrak{B}$ oder $\mathfrak{B} \subseteq \mathfrak{A}$.

Jetzt sei $\mathfrak{P}$ eine beliebige nicht leere Untermenge von $\mathfrak{M}$ und $\mathfrak{P}_0$ der Durchschnitt aller derjenigen Mengen aus Δ, welche $\mathfrak{P}$ umfassen (zu denen jedenfalls die Menge $\mathfrak{M}$ gehört). Dann gehört auch $\mathfrak{P}_0$ der Kette Δ an. Das ausgezeichnete Element p_0 von $\mathfrak{P}_0$ muß ein Element von $\mathfrak{P}$ sein, weil sonst $\mathfrak{P}_0'$ (die aus $\mathfrak{P}_0$ durch Weglassung von p_0 entstehende Menge) alle Elemente von $\mathfrak{P}$ enthielte, der Kette Δ angehörte und doch nur ein Teil von $\mathfrak{P}_0$ wäre. Jede andere $\mathfrak{P}$ umfassende Menge $\mathfrak{P}_1$

aus Δ muß $\mathfrak{P}_0$ umfassen: $\mathfrak{P}_0$ ist echte Untermenge von jedem $\mathfrak{P}_1$. Daraus folgt nach dem früher Bewiesenen, daß $\mathfrak{P}_0$ sogar Untermenge der Menge $\mathfrak{P}_1'$ ist, die aus $\mathfrak{P}_1$ durch Weglassung des ausgezeichneten Elementes p_1 von $\mathfrak{P}_1$ entsteht. Also liegt p_1 nicht in $\mathfrak{P}_0$, also sicher nicht in $\mathfrak{P}$. *Es gibt also nur eine Menge* $\mathfrak{P}_0$ *in* Δ, *welche* $\mathfrak{P}$ *umfaßt und deren ausgezeichnetes Element in* $\mathfrak{P}$ *liegt.*

Wählt man hier $\mathfrak{P} = \{a\}$, wo a irgend ein Element von $\mathfrak{M}$ ist, so ergibt sich, daß jedem Element a von $\mathfrak{M}$ eine einzige Menge von Δ entspricht, in welcher a ausgezeichnetes Element ist. Wir nennen diese Menge $\mathfrak{R}(a)$.

Wählt man sodann $\mathfrak{P} = \{a, b\}$ $(a \neq b)$, so ist das ausgezeichnete Element von $\mathfrak{P}_0$ entweder a oder b; d. h. es ist entweder $\mathfrak{P}_0 = \mathfrak{R}(a)$ oder $\mathfrak{P}_0 = \mathfrak{R}(b)$. Niemals gilt aber beides gleichzeitig; denn dann müßte das ausgezeichnete Element sowohl a wie b sein. Der Fall $\mathfrak{R}(a) = \mathfrak{R}(b)$ ist demnach ausgeschlossen, und es bleiben nur die beiden Möglichkeiten $\mathfrak{R}(a) \subset \mathfrak{R}(b)$ und $\mathfrak{R}(b) \subset \mathfrak{R}(a)$. Im ersten Fall schreiben wir $b < a$, im zweiten Fall demnach $a < b$.

Von den drei Möglichkeiten

$$a < b, \qquad a = b, \qquad b < a$$

tritt nach dem eben Bewiesenen immer eine und nur eine ein. Das transitive Gesetz gilt auch; denn aus

$$\mathfrak{R}(c) \subset \mathfrak{R}(b), \qquad \mathfrak{R}(b) \subset \mathfrak{R}(a)$$

folgt

$$\mathfrak{R}(c) \subset \mathfrak{R}(a).$$

Die Relation $a < b$ definiert also eine *Ordnung von* $\mathfrak{M}$.

Um zu zeigen, daß eine Wohlordnung vorliegt, betrachte man eine nicht leere Untermenge $\mathfrak{P}$ von $\mathfrak{M}$ und die zugehörige Menge $\mathfrak{P}_0$ aus Δ, deren ausgezeichnetes Element p_0 in $\mathfrak{P}$ liegt. Ist p irgend ein Element von $\mathfrak{P}$, so ist, weil $\mathfrak{R}(p)$ als Durchschnitt aller p umfassenden Mengen von Δ definiert war, und weil $\mathfrak{P}_0$ eine solche Menge von Δ ist:

$$\mathfrak{R}(p) \leqq \mathfrak{P}_0 = \mathfrak{R}(p_0),$$

also

$$p_0 \leqq p.$$

Also ist p_0 das erste Element von $\mathfrak{P}$, womit alles bewiesen ist.

Die Wichtigkeit der Wohlordnung beruht auf der Möglichkeit, die Methode der vollständigen Induktion, die uns von den abzählbaren Mengen her bekannt ist, auf beliebige wohlgeordnete Mengen auszudehnen. Das soll im nächsten Paragraphen geschehen.

§ 59. Die transfinite Induktion.

Der Beweis durch transfinite Induktion. Um eine Eigenschaft E für alle Elemente einer wohlgeordneten Menge zu beweisen, kann man so verfahren: Man weist nach, daß die Eigenschaft E einem Element zukommt, sobald sie allen vorangehenden Elementen zukommt (also insbesondere, daß sie dem ersten Element der Menge zukommt). Dann muß die Eigenschaft E überhaupt allen Elementen zukommen. Denn gesetzt, es gäbe Elemente, die die Eigenschaft E nicht hätten, so müßte es auch ein erstes Element e geben, welches die Eigenschaft E nicht hätte. Alle vorangehenden Elemente hätten dann aber die Eigenschaft E, also e auch, was einen Widerspruch ergibt.

Die Konstruktion durch transfinite Induktion. Gesetzt, man will den Elementen x einer wohlgeordneten Menge $\mathfrak{M}$ irgend welche neuen Objekte $\varphi(x)$ zuordnen, und man gibt, um diese zu bestimmen, eine Relation vor, eine „rekursive Bestimmungsrelation", die immer den Funktionswert $\varphi(a)$ mit den Werten $\varphi(b)$ $(b < a)$ verknüpfen soll. Angenommen wird, daß die Relation jeweils $\varphi(a)$ eindeutig bestimmt, sobald alle Werte $\varphi(b)$ $(b < a)$ gegeben sind und untereinander allemal die gegebene Relation erfüllen. Statt einer Relation kann auch ein System von Relationen gegeben sein.

Satz. *Unter den angegebenen Voraussetzungen gibt es eine und nur eine Funktion $\varphi(x)$, deren Werte die gegebene Relation erfüllen.*

Zunächst werde die Eindeutigkeit bewiesen. Gesetzt, es gäbe zwei verschiedene Funktionen $\varphi(x)$, $\overline{\varphi}(x)$, welche die Bestimmungsrelationen erfüllen. Dann muß es ein erstes a geben, für welches $\varphi(a) \neq \overline{\varphi}(a)$ ist. Für alle $b < a$ ist $\varphi(b) = \overline{\varphi}(b)$. Vermöge der Voraussetzung, daß die Relationen den Wert $\varphi(a)$ eindeutig bestimmen sollen, sobald alle $\varphi(b)$ gegeben sind, ist aber doch $\varphi(a) = \overline{\varphi}(a)$, entgegen der Annahme.

Um nun die Existenz zu beweisen, betrachten wir die Abschnitte $\mathfrak{A}$ der Menge $\mathfrak{M}$. (Ein Abschnitt $\mathfrak{A}$ ist wieder die Menge der Elemente, die einem Element a vorangehen.) Diese bilden (mit der Relation $\mathfrak{A} \subset \mathfrak{B}$ als Ordnungsrelation) eine wohlgeordnete Menge; denn jedem Element a entspricht umkehrbar eindeutig ein Abschnitt $\mathfrak{A}$, und aus $b < a$ folgt $\mathfrak{B} \subset \mathfrak{A}$. Nehmen wir als letzten Abschnitt noch die Menge $\mathfrak{M}$ selbst hinzu, so bleibt die Menge wohlgeordnet.

Wir wollen nun durch Induktion nach $\mathfrak{A}$ beweisen, daß es auf jeder der Mengen $\mathfrak{A}$ eine Funktion $\varphi(x) = \varphi_{\mathfrak{A}}(x)$ gibt (definiert für alle x in $\mathfrak{A}$), welche den gegebenen Relationen genügt. Diese Existenz sei also für alle Abschnitte, die einem gegebenen Abschnitt $\mathfrak{A}$ vorangehen, bewiesen. Nun gibt es zwei Fälle:

1. $\mathfrak{A}$ hat ein letztes Element a. Auf der Menge $\mathfrak{A}'$, die aus $\mathfrak{A}$ durch Weglassung von a entsteht, ist eine Funktion $\varphi(x)$ definiert, da $\mathfrak{A}'$ ein früherer Abschnitt als $\mathfrak{A}$ ist. Durch die Gesamtheit der Werte $\varphi(b)$ $(b < a)$ ist aber vermöge der Relationen ein Wert $\varphi(a)$ definiert. Nimmt man diesen hinzu, so ist die Funktion φ für alle Elemente von $\mathfrak{A}$ erklärt und genügt ausnahmslos den Relationen.

2. $\mathfrak{A}$ hat kein letztes Element. Jedes Element a von $\mathfrak{A}$ gehört also schon einem früheren Abschnitt $\mathfrak{B}$ an. Auf jedem früheren Abschnitt $\mathfrak{B}$ ist eine Funktion $\varphi_{\mathfrak{B}}$ definiert. Wir wollen definieren:

$$\varphi(a) = \varphi_{\mathfrak{B}}(a),$$

müssen dann aber zuerst nachweisen, daß die Funktionen $\varphi_{\mathfrak{B}}$, $\varphi_{\mathfrak{C}}$, ..., die zu verschiedenen Abschnitten gehören, auf jedem gemeinsamen Punkt dieser Abschnitte übereinstimmen. Es seien also $\mathfrak{B}$ und $\mathfrak{C}$ verschiedene Abschnitte, und es sei etwa $\mathfrak{B} \subset \mathfrak{C}$. Dann sind $\varphi_{\mathfrak{B}}$ und $\varphi_{\mathfrak{C}}$

beide auf $\mathfrak{B}$ definiert und genügen dort beide den gegebenen Relationen; also stimmen sie (nach dem Eindeutigkeitssatz, der schon bewiesen wurde) überein. Damit erhält also die Definition $\varphi(a) = \varphi_{\mathfrak{B}}(a)$ einen eindeutigen Sinn. Daß die so konstruierte Funktion φ den Relationen genügt, ist klar; denn alle Funktionen $\varphi_{\mathfrak{B}}$ tun es ja.

Sowohl im Fall 1 wie im Fall 2 gibt es demnach eine Funktion φ auf $\mathfrak{A}$ mit den angegebenen Eigenschaften, und damit ist die Existenz der Funktion φ auf jedem Abschnitt bewiesen. Nimmt man für diesen Abschnitt insbesondere die Menge $\mathfrak{M}$ selbst, so folgt die Behauptung.

Neuntes Kapitel.

Unendliche Körpererweiterungen.

Jeder beliebige kommutative Körper entsteht aus seinem Primkörper durch eine endliche oder unendliche Körpererweiterung. In den Kapiteln 5 und 7 haben wir die endlichen Körpererweiterungen studiert; in diesem Kapitel sollen die unendlichen Körpererweiterungen behandelt werden, und zwar zunächst die algebraischen, sodann die transzendenten.

Alle betrachteten Körper sind kommutativ.

§ 60. Die algebraisch-abgeschlossenen Körper.

Unter den algebraischen Erweiterungen eines vorgelegten Körpers spielen naturgemäß eine wichtige Rolle die *maximalen* algebraischen Erweiterungen, d. h. die, welche sich nicht mehr algebraisch erweitern lassen. Daß solche existieren, wird in diesem Paragraphen bewiesen werden.

Damit Ω ein solcher maximaler algebraischer Erweiterungskörper ist, ist eine notwendige Bedingung die, daß jedes Polynom in $\Omega[x]$ vollständig in Linearfaktoren zerfällt (sonst könnte man nämlich nach § 27 den Körper Ω noch erweitern durch Adjunktion einer Nullstelle einer nichtlinearen Primfunktion). Diese Bedingung reicht aber auch hin. Denn wenn jedes Polynom in $\Omega[x]$ in Linearfaktoren zerfällt, so muß, falls Ω' ein algebraischer Erweiterungskörper ist, jedes Element von Ω' einer Gleichung in Ω genügen, also (indem man die linke Seite in lineare Faktoren zerlegt) auch einer linearen Gleichung in Ω genügen, also schon in Ω liegen; mithin ist $\Omega' = \Omega$, und Ω ist maximal.

Wir definieren deshalb:

Ein Körper Ω heißt algebraisch-abgeschlossen, wenn in $\Omega[x]$ jedes Polynom in Linearfaktoren zerfällt.

Zum Beispiel ist der Körper der komplexen Zahlen ein solcher Körper; denn der „Fundamentalsatz der Algebra" (vgl. später, § 67) lehrt geradezu, daß jedes Polynom in diesem Körper vollständig zer-

fällt. Auch der Körper aller komplexen algebraischen Zahlen (Zahlen, die einer Gleichung mit rationalen Koeffizienten genügen) ist ein solcher; denn die komplexen Wurzeln einer Gleichung mit algebraischen Koeffizienten sind nicht nur algebraisch in bezug auf den Körper der algebraischen Zahlen, sondern sogar algebraisch in bezug auf den Körper der rationalen Zahlen, also selbst algebraische Zahlen.

Wir werden in diesem Paragraphen lernen, zu jedem Körper P einen algebraisch-abgeschlossenen Erweiterungskörper auf rein algebraischem Wege zu konstruieren. Es gilt der folgende

Hauptsatz: *Zu jedem Körper* P *gibt es einen algebraisch-abgeschlossenen algebraischen Erweiterungskörper* Ω. *Und zwar ist dieser Körper bis auf äquivalente Erweiterungen eindeutig bestimmt: Je zwei algebraisch-abgeschlossene algebraische Erweiterungen* Ω, Ω' *von* P *sind äquivalent.*

Dem Beweis dieses Satzes müssen einige Hilfssätze vorausgeschickt werden:

Hilfssatz 1. *Es sei* Ω *ein algebraischer Erweiterungskörper von* P. *Hinreichend, damit* Ω *algebraisch-abgeschlossen sei, ist die Bedingung, daß alle Polynome aus* $\mathsf{P}[x]$ *in* $\Omega[x]$ *in Linearfaktoren zerfallen.*

Beweis: Es sei $f(x)$ ein Polynom aus $\Omega[x]$. Wenn es nicht in Linearfaktoren zerfiele, so könnte man eine Nullstelle α adjungieren und käme zu einem echten Oberkörper Ω'. α ist algebraisch in bezug auf Ω und Ω algebraisch in bezug auf P, also α algebraisch in bezug auf P. Daher ist α Nullstelle eines Polynoms $g(x)$ in $\mathsf{P}[x]$. Dieses zerfällt aber in $\Omega[x]$ in Linearfaktoren. Also ist α Nullstelle eines Linearfaktors in $\Omega[x]$, liegt also in Ω, entgegen der Voraussetzung.

Hilfssatz 2. *Ist ein Körper* P *wohlgeordnet, so läßt sich der Polynombereich* $\mathsf{P}[x]$ *in einer eindeutig bestimmbaren Weise wohlordnen.* P *ist in dieser Wohlordnung ein Abschnitt.*

Beweis: Wir definieren eine Anordnung der Polynome $f(x)$ aus $\mathsf{P}[x]$ folgendermaßen: Es sei $f(x) < g(x)$ in den folgenden Fällen:

1. Grad von $f(x) <$ Grad von $g(x)$;

2. Grad von $f(x) =$ Grad von $g(x) = n$; etwa $f(x) = a_0 x^n + \cdots + a_n$, $g(x) = b_0 x^n + \cdots + b_n$; außerdem für einen Index k:

$$\begin{cases} a_i = b_i & \text{für} \quad i < k; \\ a_k < b_k & \text{in der Wohlordnung von } \mathsf{P}. \end{cases}$$

Dabei wird dem Polynom 0 ausnahmsweise der Grad 0 zugeschrieben. Daß so eine Anordnung erhalten wird, ist klar. Daß es eine Wohlordnung ist, zeigt man folgendermaßen: In jeder nichtleeren Menge von Polynomen liegt die nichtleere Untermenge der Polynome niedrigsten Grades; dieser Grad sei n. Darin liegt die nichtleere Untermenge der Polynome, deren a_0 in der Wohlordnung von P möglichst früh kommt; darin die Untermenge mit möglichst frühem a_1 usw. Die schließlich

erhaltene Untermenge mit möglichst frühem a_n kann nur aus einem Polynom bestehen (da $a_0, \ldots, a_n$ durch die sukzessiven Minimalforderungen eindeutig bestimmt werden), und dieses Polynom ist das erste Element der gegebenen Menge.

Hilfssatz 3. *Ist ein Körper* P *wohlgeordnet und sind außerdem ein Polynom* $f(x)$ *vom Grad* n *und* n *Symbole* $\alpha_1, \ldots, \alpha_n$ *vorgegeben, so läßt sich ein Körper* $\mathsf{P}(\alpha_1, \ldots, \alpha_n)$, *in dem* $f(x)$ *vollständig in Linearfaktoren* $\prod_1^n (x - \alpha_i)$ *zerfällt, eindeutig konstruieren und wohlordnen.* P *ist in dieser Wohlordnung ein Abschnitt.*

Beweis: Wir wollen die Wurzeln $\alpha_1, \ldots, \alpha_n$ sukzessive adjungieren, wodurch aus $\mathsf{P} = \mathsf{P}_0$ sukzessive die Körper $\mathsf{P}_1, \ldots, \mathsf{P}_n$ entstehen mögen. Nehmen wir an, daß $\mathsf{P}_{i-1} = \mathsf{P}(\alpha_1, \ldots, \alpha_{i-1})$ schon konstruiert und wohlgeordnet ist und daß P ein Abschnitt von P_{i-1} ist, so wird P_i folgendermaßen konstruiert:

Zunächst werde nach Hilfssatz 2 der Polynombereich $\mathsf{P}_{i-1}[x]$ wohlgeordnet. f zerfällt in diesem Bereich in irreduzible Faktoren, unter denen zunächst $x - \alpha_1, \ldots, x - \alpha_{i-1}$ vorkommen; von den übrigen Faktoren sei $f_i(x)$ der in der Wohlordnung dieses Bereiches erste. Mit α_i als Symbol für eine Wurzel von $f_i(x)$ definieren wir nun nach § 27 den Körper $\mathsf{P}_i = \mathsf{P}_{i-1}(\alpha_i)$ als Gesamtheit aller Summen

$$\sum_0^{h-1} c_\lambda \alpha_i^\lambda,$$

wo h der Grad von $f_i(x)$ ist. Sollte $f_i(x)$ linear sein, so ist natürlich $\mathsf{P}_i = \mathsf{P}_{i-1}$ zu setzen; α_i ist dann kein neues Symbol, sondern die Nullstelle von $f_i(x)$ in P_i. Der Körper wird wohlgeordnet durch die folgende Festsetzung: Jedem Körperelement $\sum_0^{h-1} c_\lambda \alpha_i^\lambda$ wird ein Polynom $\sum_0^{h-1} c_\lambda x^\lambda$ zugeordnet, und die Körperelemente werden genau so angeordnet wie die ihnen entsprechenden Polynome.

Offenbar ist dann P_{i-1} ein Abschnitt von P_i, also auch P ein Abschnitt von P_i.

Damit sind $\mathsf{P}_1, \ldots, \mathsf{P}_n$ konstruiert und wohlgeordnet. P_n ist der gesuchte eindeutig definierte Körper $\mathsf{P}(\alpha_1, \ldots, \alpha_n)$.

Hilfssatz 4. *Wenn in einer geordneten Menge von Körpern jeder frühere Körper Unterkörper eines jeden späteren ist, so ist ihre Vereinigungsmenge wieder ein Körper.*

Beweis. Zu je zwei Elementen α, β der Vereinigung gibt es zwei Körper $\Sigma_\alpha, \Sigma_\beta$, welche α bzw. β enthalten und von denen einer den anderen umfaßt. In diesem umfassenden Körper sind $\alpha + \beta$ und $\alpha \cdot \beta$ definiert, und diese Definitionen stimmen für alle Körper der Menge, welche α und β umfassen, überein, da ja von zwei solchen Körpern

immer einer ein Unterkörper des anderen ist. Um nun z. B. das Assoziativgesetz

$$\alpha\beta \cdot \gamma = \alpha \cdot \beta\gamma$$

zu beweisen, suche man aus den Körpern Σ_α, Σ_β, Σ_γ wieder den umfassendsten (spätesten); in ihm sind α, β und γ enthalten und in ihm gilt auch das Assoziativgesetz. In derselben Weise werden alle Rechnungsregeln bewiesen.

Der Beweis des Hauptsatzes zerfällt in zwei Teile: die Konstruktion von Ω und den Eindeutigkeitsbeweis.

Die Konstruktion von Ω. Hilfssatz 1 zeigt, daß man, um einen algebraisch-abgeschlossenen Erweiterungskörper Ω von P zu konstruieren, bloß einen solchen über P algebraischen Körper zu konstruieren hat, in welchem alle Polynome von $\mathsf{P}[x]$ vollständig zerfallen.

Man denke sich den Körper P und demnach auch den Polynombereich $\mathsf{P}[x]$ wohlgeordnet. Jedem Polynom $f(x)$ seien so viele neue Symbole $\alpha_1, \ldots, \alpha_n$ zugeordnet, wie der Grad des Polynoms beträgt.

Jedem Polynom $f(x)$ sollen nunmehr zwei wohlgeordnete Körper P_f, Σ_f zugeordnet werden, und zwar werden diese definiert durch die folgenden rekursiven Relationen:

1. P_f ist die Vereinigungsmenge von P und allen Σ_g mit $g < f$.

2. Die Wohlordnung von P_f ist so beschaffen, daß P, sowie alle Σ_g mit $g < f$, Abschnitte von P_f sind.

3. Σ_f entsteht aus P_f durch Adjunktion aller Wurzeln von f mit Hilfe der Symbole $\alpha_1, \ldots, \alpha_n$ nach der Konstruktion von Hilfssatz 3.

Zu beweisen ist, daß durch diese Forderungen in der Tat zwei wohlgeordnete Körper P_f, Σ_f eindeutig bestimmt werden, sobald alle früheren P_g, Σ_g gegeben sind und den Forderungen genügen.

Wenn 3. erfüllt ist, so ist zunächst P_f Abschnitt von Σ_f. Daraus und aus 2. folgt, daß P und jedes $\Sigma_g (g < f)$ Abschnitte von Σ_f sind. Nimmt man an, daß die Forderungen für alle früheren Indizes als f bereits erfüllt sind, so ist also

$$\begin{cases} \mathsf{P} \text{ Abschnitt von } \Sigma_h \text{ für } h < f, \\ \Sigma_g \text{ Abschnitt von } \Sigma_h \text{ für } g < h < f. \end{cases}$$

Daraus folgt nun, daß die Körper P und $\Sigma_h (h < f)$ eine Menge von der in Hilfssatz **4** geforderten Art bilden. Also ist die Vereinigungsmenge wieder ein Körper, den wir der Forderung 1 entsprechend P_f zu nennen haben. Die Wohlordnung von P_f ist aber durch die Forderung 2 eindeutig bestimmt. Denn je zwei Elemente a, b von P_f liegen schon in einem der Körper P oder Σ_g und haben darin eine Reihenfolge: $a < b$ oder $a > b$, die in der Wohlordnung von P_f beibehalten werden muß. Diese Reihenfolge ist dieselbe in allen Körpern P oder Σ_g, welche sowohl a wie b umfassen; denn alle diese Körper sind ja Abschnitte von-

einander. Also ist eine Ordnung in der Tat definiert. Daß es eine Wohlordnung ist, ist auch klar; denn jede nichtleere Menge $\mathfrak{M}$ in P_f enthält mindestens ein Element aus P oder aus einem Σ_g, also auch ein erstes Element aus P oder dem betreffenden Σ_g. Dieses ist dann zugleich das erste Element von $\mathfrak{M}$.

Also ist der Körper P_f samt seiner Wohlordnung durch 1., 2. eindeutig bestimmt. Da Σ_f durch 3. eindeutig bestimmt wird, so sind die P_f und Σ_f konstruiert.

In Σ_f zerfällt wegen 3. das Polynom $f(x)$ völlig in Linearfaktoren. Weiter zeigt man durch transfinite Induktion, daß Σ_f algebraisch in bezug auf P ist. Angenommen nämlich, alle $\Sigma_g (g < f)$ seien schon algebraisch. Dann ist auch ihre Vereinigungsmenge mit P, also P_f algebraisch. Weiter ist Σ_f nach 3. algebraisch in bezug auf P_f, also algebraisch in bezug auf P.

Bildet man nun die Vereinigung Ω aller Σ_f, so ist sie nach Hilfssatz 4 ein Körper; dieser Körper ist algebraisch in bezug auf P, und in ihm zerfallen alle Polynome f (weil jedes f schon in Σ_f zerfällt). Also ist der Körper Ω algebraisch-abgeschlossen (Hilfssatz 1).

Die Eindeutigkeit von Ω. Es seien Ω und Ω' zwei Körper, beide algebraisch-abgeschlossen und algebraisch in bezug auf P. Wir wollen ihre Äquivalenz beweisen. Zu diesem Zweck werden sie beide als wohlgeordnet vorausgesetzt. Wir wollen zu jedem Abschnitt $\mathfrak{A}$ von Ω (wobei Ω selbst auch zu den Abschnitten gerechnet wird) einen Abschnitt $\mathfrak{A}'$ von Ω' und einen 1-Isomorphismus

$$\mathsf{P}(\mathfrak{A}) \cong \mathsf{P}(\mathfrak{A}')$$

konstruieren. Dieser soll den folgenden rekursiven Bedingungen genügen:

1. Der 1-Isomorphismus $\mathsf{P}(\mathfrak{A}) \cong \mathsf{P}(\mathfrak{A}')$ soll P elementweise festlassen.

2. Der 1-Isomorphismus $\mathsf{P}(\mathfrak{A}) \cong \mathsf{P}(\mathfrak{A}')$ soll für $\mathfrak{B} < \mathfrak{A}$ eine Fortsetzung von $\mathsf{P}(\mathfrak{B}) \cong \mathsf{P}(\mathfrak{B}')$ sein.

3. Wenn $\mathfrak{A}$ ein letztes Element a hat, also $\mathfrak{A} = \mathfrak{B} \vee \{a\}$ ist, und wenn a eine Wurzel des in $\mathsf{P}(\mathfrak{B})$ irreduziblen Polynoms $f(x)$ ist, so soll a' die in der Wohlordnung von Ω erste Wurzel des vermöge $\mathsf{P}(\mathfrak{B}) \cong \mathsf{P}(\mathfrak{B}')$ zugeordneten Polynoms $f'(x)$ sein.

Zu zeigen ist, daß durch diese drei Forderungen in der Tat ein und nur ein 1-Isomorphismus $\mathsf{P}(\mathfrak{A}) \cong \mathsf{P}(\mathfrak{A}')$ bestimmt wird, falls dasselbe schon für alle früheren Abschnitte $\mathfrak{B} < \mathfrak{A}$ der Fall ist. Wir haben da zwei Fälle zu unterscheiden.

Erster Fall: $\mathfrak{A}$ hat kein letztes Element. Dann gehört jedes Element a schon einem früheren Abschnitt $\mathfrak{B}$ an; daher ist $\mathfrak{A}$ die Vereinigung der Abschnitte $\mathfrak{B}$, also $\mathsf{P}(\mathfrak{A})$ die Vereinigung der Körper $\mathsf{P}(\mathfrak{B})$ mit $\mathfrak{B} < \mathfrak{A}$. Da jeder der 1-Isomorphismen $\mathsf{P}(\mathfrak{B}) \cong \mathsf{P}(\mathfrak{B}')$ Fortsetzung aller früheren

ist, so ist jedem Element α in allen diesen 1-Isomorphismen nur ein α' zugeordnet. Es gibt demnach eine und nur eine Zuordnung $\mathsf{P}(\mathfrak{A}) \to \mathsf{P}(\mathfrak{A}')$, welche alle früheren 1-Isomorphismen $\mathsf{P}(\mathfrak{B}) \to \mathsf{P}(\mathfrak{B}')$ umfaßt, nämlich die Zuordnung $\alpha \to \alpha'$. Diese ist offenbar ein 1-Isomorphismus und genügt den Bedingungen 1, 2.

Zweiter Fall: $\mathfrak{A}$ hat ein letztes Element a; es ist also $\mathfrak{A} = \mathfrak{B} \vee \{a\}$. Durch die Bedingung 3 ist das dem a zugeordnete Element a' eindeutig festgelegt. Da a' in bezug auf $\mathsf{P}(\mathfrak{B}')$ (im Sinne des 1-Isomorphismus) „derselben" irreduziblen Gleichung genügt wie a in bezug auf $\mathsf{P}(\mathfrak{B})$, so läßt sich der 1-Isomorphismus $\mathsf{P}(\mathfrak{B}) \to \mathsf{P}(\mathfrak{B}')$ bzw., wenn $\mathfrak{B}$ leer ist, der identische Isomorphismus $\mathsf{P} \to \mathsf{P}$ fortsetzen zu einem 1-Isomorphismus $\mathsf{P}(\mathfrak{B}, a) \to \mathsf{P}(\mathfrak{B}', a')$, wobei a in a' übergeht (§ 27). Und zwar ist dieser Isomorphismus durch jene Bedingung eindeutig bestimmt; denn jede rationale Funktion $\varphi(a)$ mit Koeffizienten aus $\mathfrak{B}$ muß notwendig übergehen in ein $\varphi'(a')$ mit entsprechenden Koeffizienten aus $\mathfrak{B}'$. Daß der so konstruierte Isomorphismus $\mathsf{P}(\mathfrak{A}) \to \mathsf{P}(\mathfrak{A}')$ den Bedingungen 1 und 2 genügt, ist klar.

Damit ist die Konstruktion der Isomorphismen $\mathsf{P}(\mathfrak{A}) \to \mathsf{P}(\mathfrak{A}')$ geleistet. Bezeichnet Ω'' die Vereinigung aller $\mathsf{P}(\mathfrak{A}')$, so existiert also ein 1-Isomorphismus $\mathsf{P}(\Omega) \to \Omega''$ oder $\Omega \to \Omega''$, der P elementweise fest läßt. Da Ω algebraisch-abgeschlossen ist, so muß Ω'' es auch sein, und daher ist notwendig Ω'' schon das ganze Ω'. Daraus folgt die behauptete Äquivalenz von Ω und Ω'.

Die Bedeutung der algebraisch-abgeschlossenen Erweiterungskörper eines gegebenen Körpers liegt darin, daß sie bis auf äquivalente Erweiterungen alle überhaupt möglichen algebraischen Erweiterungen umfassen. Genauer:

Ist Ω ein algebraisch-abgeschlossener algebraischer Erweiterungskörper von P und Σ irgendein algebraischer Erweiterungskörper von P, so gibt es innerhalb Ω einen zu Σ äquivalenten Erweiterungskörper Σ_0.

Beweis. Man erweitere Σ zu einem algebraisch-abgeschlossenen algebraischen Erweiterungskörper Ω'. Dieser ist auch algebraisch in bezug auf P, also mit Ω äquivalent. Bei einem 1-Isomorphismus, der Ω' in Ω überführt und P elementweise fest läßt, geht insbesondere Σ über in einen äquivalenten Unterkörper Σ_0 von Ω.

Aufgabe. Man beweise die Existenz und Eindeutigkeit eines Erweiterungskörpers von P, der durch Adjunktion aller Nullstellen einer vorgegebenen Menge von Polynomen aus $\mathsf{P}[x]$ entsteht.

§ 61. Rein transzendente Erweiterungen. Irreduzible Systeme.

Die Frage nach der Struktur aller (kommutativen) Erweiterungskörper eines vorgelegten (kommutativen) Körpers P ist durch die obigen Betrachtungen für die *algebraischen Erweiterungen* weitgehend gelöst.

Alle algebraischen Erweiterungen ergaben sich einerseits als Vereinigungsmengen endlicher Erweiterungen (§ 26), deren Struktur schon früher (Kap. 5 und 7) aufgedeckt wurde — andererseits als Unterkörper eines (im wesentlichen einzigen) universellen algebraischen Erweiterungskörpers: des algebraisch-abgeschlossenen Erweiterungskörpers (§ 60).

In diesem und dem nächsten Paragraphen sollen nun auch die nicht algebraischen oder *transzendenten* Erweiterungen in die Untersuchung einbezogen werden, und zwar ergibt sich eine vollständige Übersicht über diese Erweiterungen dadurch, daß man sie zerlegt in eine *„rein transzendente"* Erweiterung, die auf die Adjunktion unabhängiger Unbestimmten hinauskommt, und eine darauffolgende algebraische Erweiterung.

Um dazu zu kommen, müssen wir einige neue Begriffe einführen.

Es sei Ω ein Erweiterungskörper eines festen Körpers P. Ein Element a von Ω heißt (*algebraisch-*)*abhängig* von einer Menge $\mathfrak{M}$ (in bezug auf den Grundkörper P), falls es algebraisch in bezug auf den Körper $\mathsf{P}(\mathfrak{M})$ ist, also einer Gleichung genügt, deren Koeffizienten nicht sämtlich verschwinden und rationale Funktionen der Elemente von $\mathfrak{M}$ mit Koeffizienten aus P sind[1]. In diesem Fall kann man die Gleichung durch Multiplikation mit dem Hauptnenner ganz-rational in den Elementen von $\mathfrak{M}$ machen. Da in der Gleichung nur endlichviele Elemente $m_1, \ldots, m_n$ von $\mathfrak{M}$ vorkommen, so hängt a schon von einer endlichen Untermenge von $\mathfrak{M}$ ab. Wählt man diese Untermenge minimal, d. h. so, daß kein Element mehr weggelassen werden kann (eventuell leer), so muß in der zugehörigen Gleichung $f(a, m_1, \ldots, m_n) = 0$ jedes m_i wirklich vorkommen, d. h. eine Potenz von m_i muß mit einem nichtverschwindenden Koeffizienten versehen sein. Also ist dann auch umgekehrt jedes m_i algebraisch von a und den übrigen m_j abhängig. Die Relation der algebraischen Abhängigkeit hat demnach die folgenden Eigenschaften:

1. a ist abhängig von sich selbst, d. h. von der Menge $\{a\}$.

2. Ist a abhängig von $\mathfrak{M}$, so hängt es auch von jeder Obermenge von $\mathfrak{M}$ ab.

3. Ist a abhängig von $\mathfrak{M}$, so ist a schon von einer endlichen Untermenge $\{m_1, \ldots, m_n\}$ von $\mathfrak{M}$ (die auch leer sein kann) abhängig.

4. Wählt man diese Untermenge minimal, so ist jedes m_i von a und den übrigen m_j abhängig.

Weiter gilt:

5. Ist a abhängig von $\mathfrak{M}$ und jedes Element von $\mathfrak{M}$ abhängig von $\mathfrak{N}$, so ist a abhängig von $\mathfrak{N}$.

---

[1] Ein Element a hängt von der leeren Menge algebraisch ab, wenn a algebraisch in bezug auf P ist.

Das sieht man so ein: Ist a algebraisch in bezug auf $\mathsf{P}(\mathfrak{M})$ und $\mathfrak{M}$ algebraisch in bezug auf $\mathsf{P}(\mathfrak{N})$, so sind nach § 29 auch $\mathsf{P}(\mathfrak{M})$ und weiterhin a algebraisch in bezug auf $\mathsf{P}(\mathfrak{N})$.

Eine Menge $\mathfrak{N}$ heißt (*algebraisch*) *abhängig* von einer Menge $\mathfrak{M}$, wenn alle Elemente von $\mathfrak{N}$ es sind. Ist $\mathfrak{N}$ abhängig von $\mathfrak{M}$ und $\mathfrak{M}$ abhängig von $\mathfrak{L}$, so ist auch $\mathfrak{N}$ abhängig von $\mathfrak{L}$ (Folge von 5).

Sind zwei Mengen $\mathfrak{M}$ und $\mathfrak{N}$ gegenseitig voneinander abhängig, so heißen sie *äquivalent* (in bezug auf P). Die Äquivalenzrelation ist offenbar reflexiv, symmetrisch und transitiv.

Eine Menge $\mathfrak{M}$ heißt *irreduzibel* (in bezug auf P), wenn kein Element von $\mathfrak{M}$ algebraisch von den übrigen abhängt. Man sagt in diesem Fall auch, die Menge $\mathfrak{M}$ „bestehe aus lauter algebraisch-unabhängigen Elementen" oder „aus lauter unabhängigen Transzendenten".

Ein irreduzibles System — so kann man auch sagen — ist von keiner echten Teilmenge abhängig. (Eine leere Menge ist immer irreduzibel.)

Ist $\mathfrak{M}$ irreduzibel, so kann eine Relation zwischen endlichvielen verschiedenen Elementen von $\mathfrak{M}$

$$f(m_1, \ldots, m_r) = 0,$$

(wo f ein Polynom mit Koeffizienten aus P ist) nur dann bestehen, wenn f identisch verschwindet:

$$f(x_1, \ldots, x_r) = 0 \qquad \text{(für unbestimmte } x_i\text{)}.$$

Bildet man nun einen Polynombereich $\mathsf{P}[\mathfrak{X}]$ in so vielen Unbestimmten x_i, wie es Elemente in $\mathfrak{M}$ gibt (endlich oder unendlich vielen), und ordnet man jedem Polynom $f(x_1, \ldots, x_r)$ das Körperelement $f(m_1, \ldots, m_r)$ zu, so entsteht offenbar ein Homomorphismus des Polynombereichs mit der Menge $\mathsf{P}[\mathfrak{M}]$ der Körperelemente $f(m_1, \ldots, m_r)$. Dabei gehen aber, falls $\mathfrak{M}$ irreduzibel ist, verschiedene Polynome in verschiedene Körperelemente über; man hat also in diesem Fall einen 1-Isomorphismus:

$$\mathsf{P}[\mathfrak{X}] \cong \mathsf{P}[\mathfrak{M}].$$

Bildet man auf beiden Seiten den Quotientenkörper, nämlich links rein formal den Körper der rationalen Funktionen der Unbestimmten x_i und rechts den Quotientenkörper $\mathsf{P}(\mathfrak{M})$ in Ω, so sind nach § 12 auch diese Quotientenkörper 1-isomorph. Damit ist bewiesen:

Der Körper $\mathsf{P}(\mathfrak{M})$, der durch Adjunktion eines irreduziblen Systems $\mathfrak{M}$ an P entsteht, ist isomorph dem Körper der rationalen Funktionen einer mit $\mathfrak{M}$ gleichmächtigen Menge $\mathfrak{X}$ von Unbestimmten x_i, d. h. dem Quotientenkörper des Polynombereichs $\mathsf{P}[\mathfrak{X}]$.

Man nennt jeden Körper $\mathsf{P}(\mathfrak{M})$, der durch Adjunktion eines irreduziblen Systems $\mathfrak{M}$ an P entsteht, eine *rein transzendente Erweiterung* von P. Die Struktur der rein transzendenten Erweiterungen ist durch den vorigen Satz vollkommen bestimmt: jede solche ist isomorph dem

Quotientenkörper eines Polynombereichs. Die Struktur hängt demnach nur von der Mächtigkeit des irreduziblen Systems $\mathfrak{M}$ ab: diese Mächtigkeit ist der im nächsten Paragraphen zu behandelnde *Transzendenzgrad*.

§ 62. Der Transzendenzgrad.

Die zu Beginn des vorigen Paragraphen erwähnte Aufspaltung einer jeden Körpererweiterung in eine rein transzendente und eine algebraische wird durch den folgenden Satz ermöglicht:

Es sei Ω eine Erweiterung von P. Dann ist jede Untermenge $\mathfrak{M}$ von Ω einem in ihr gelegenen irreduziblen System $\mathfrak{M}'$ äquivalent.

Beweis. Der Beweis stützt sich ausschließlich auf die Eigenschaften 1 bis 5 des vorigen Paragraphen.

$\mathfrak{M}$ sei wohlgeordnet. Die Untermenge $\mathfrak{M}'$ werde folgendermaßen definiert: Ein Element a von $\mathfrak{M}$ gehört zu $\mathfrak{M}'$, falls a von dem ihm vorangehenden Abschnitt $\mathfrak{A}$ nicht abhängt (also transzendent in bezug auf $\mathsf{P}(\mathfrak{A})$ ist). Von $\mathfrak{M}'$ gilt nun folgendes:

1. $\mathfrak{M}'$ ist irreduzibel. Denn hinge ein Element, etwa a_1, von anderen Elementen $a_2, \ldots, a_k$ ab, so könnte man die Menge $\{a_2, \ldots, a_k\}$ minimal wählen, und jedes der a_i hinge dann von den übrigen ab. Insbesondere würde das in der Wohlordnung letzte a_i von den ihm vorangehenden übrigen abhängen. Dann könnte aber (nach Definition von $\mathfrak{M}'$) dieses letzte a_i nicht zu $\mathfrak{M}'$ gehören.

2. $\mathfrak{M}$ hängt von $\mathfrak{M}'$ ab. Denn sonst würde es in $\mathfrak{M}$ ein frühestes Element a geben, das von $\mathfrak{M}'$ nicht abhängt. a gehört nicht zu $\mathfrak{M}'$, hängt also von dem vorangehenden Abschnitt $\mathfrak{A}$ ab, der seinerseits (da a das erste nicht von $\mathfrak{M}'$ abhängige Element war) von $\mathfrak{M}'$ abhängt. Demnach hängt a doch von $\mathfrak{M}'$ ab, entgegen der Voraussetzung.

Zusatz. *Ist $\mathfrak{M} \leqq \mathfrak{N}$, so läßt sich jedes zu $\mathfrak{M}$ äquivalente irreduzible Teilsystem $\mathfrak{M}'$ von $\mathfrak{M}$ zu einem mit $\mathfrak{N}$ äquivalenten irreduziblen Teilsystem von $\mathfrak{N}$ erweitern.*

Beweis: Man wähle die Wohlordnung von $\mathfrak{N}$ so, daß die Elemente von $\mathfrak{M}'$ vorangehen, und konstruiere $\mathfrak{N}'$ aus $\mathfrak{N}$ wie vorhin $\mathfrak{M}'$ aus $\mathfrak{M}$. Offenbar umfaßt dann $\mathfrak{N}'$ insbesondere die Elemente von $\mathfrak{M}'$.

Dem obigen Satz zufolge ist jeder Erweiterungskörper Ω von P aufzufassen als eine algebraische Erweiterung von $\mathsf{P}(\mathfrak{S})$, wo $\mathfrak{S}$ ein irreduzibles System und daher $\mathsf{P}(\mathfrak{S})$ eine transzendente Erweiterung von P ist. Das heißt also, man erhält Ω aus P durch eine rein transzendente und eine nachfolgende rein algebraische Erweiterung.

Das durch die vorigen Sätze konstruierte irreduzible System $\mathfrak{M}'$ ist natürlich nicht eindeutig bestimmt; wohl aber ist seine Mächtigkeit (also auch der Typ der rein transzendenten Erweiterung $\mathsf{P}(\mathfrak{M}')$) eindeutig bestimmt. Es gilt nämlich der Satz:

Zwei äquivalente irreduzible Systeme $\mathfrak{M}$, $\mathfrak{N}$ sind gleichmächtig.

Wir beweisen diesen von STEINITZ herrührenden Satz hier nur für den Fall, daß mindestens eins der beiden Systeme, etwa $\mathfrak{M}$, endlich sei. Dieser Fall ist für die Anwendungen der wichtigste. Für einen allgemeinen Beweis siehe die Steinitzsche Originalarbeit in Crelles Journal Bd. 137, oder auch O. HAUPT: Einführung in die Algebra II, Kap. 23, 6.

Die endliche Menge $\mathfrak{M}$ möge aus den Elementen $x_1, \ldots, x_n$ bestehen. Jedes Element von $\mathfrak{N}$ hängt von $x_1, \ldots, x_n$ ab; aber nicht jedes hängt von $x_2, \ldots, x_n$ allein ab, da sonst $\mathfrak{N}$ von $x_2, \ldots, x_n$, also auch $\mathfrak{M}$ von $x_2, \ldots, x_n$, insbesondere x_1 von $x_2, \ldots, x_n$ abhängen würde, entgegen der Irreduzibilität von $\mathfrak{M}$. Es sei y_1 ein Element von $\mathfrak{N}$, das von $x_2, \ldots, x_n$ nicht abhängt. Dann ist das System $y_1, x_2, \ldots, x_n$ irreduzibel. In der Gleichung

$$f(y_1, x_1, \ldots, x_n) = 0\,,$$

die ausdrückt, daß y_1 von $\mathfrak{M}$ abhängt, kommt demnach x_1 wirklich vor. Also hängt x_1 von $y_1, x_2, \ldots, x_n$ ab. Daraus folgt die Äquivalenz der beiden irreduziblen Systeme $x_1, \ldots, x_n$ und $y_1, x_2, \ldots, x_n$.

Mit dem System $y_1, x_2, \ldots, x_n$ kann man nun ebenso verfahren wie zuvor mit $x_1, \ldots, x_n$: man kann x_2 gegen ein Element y_2 von $\mathfrak{N}$ austauschen und erhält ein äquivalentes irreduzibles System $y_1, y_2, x_3, \ldots, x_n$. So fortfahrend, kommt man zu einem mit $\mathfrak{M}$, also auch mit $\mathfrak{N}$, äquivalenten irreduziblen System $y_1, \ldots, y_n$. Dieses muß $\mathfrak{N}$ ganz erschöpfen, da sonst $\mathfrak{N}$ nicht irreduzibel wäre. Also hat $\mathfrak{N}$ genau n Elemente, womit die Gleichmächtigkeit von $\mathfrak{M}$ und $\mathfrak{N}$ bewiesen ist.

Ein ganz ähnlicher Austauschbeweis wurde schon früher in § 28 geführt. Tatsächlich gelten für die dort betrachtete lineare Abhängigkeit dieselben Regeln 1 bis 5, die für die algebraische Abhängigkeit in § 61 aufgestellt wurden; man kann also alle Beweise wörtlich übertragen.

Die nunmehr eindeutig bestimmte Mächtigkeit eines mit Ω äquivalenten irreduziblen Systems $\mathfrak{M}'$ heißt der *Transzendenzgrad* des Körpers Ω (in bezug auf P).

Satz. *Eine Erweiterung, die sich aus zwei sukzessiven Erweiterungen von den (endlichen) Transzendenzgraden s und t zusammensetzt, hat den Transzendenzgrad $s + t$.* [1]

Beweis: Es sei $\mathsf{P} \subseteq \Sigma \subseteq \Omega$. Es sei $\mathfrak{S}$ ein in bezug auf P irreduzibles und mit Σ äquivalentes System in Σ und $\mathfrak{T}$ ein in bezug auf Σ irreduzibles und mit Ω äquivalentes System in Ω. Dann hat $\mathfrak{S}$ die Mächtigkeit s, $\mathfrak{T}$ die Mächtigkeit t, und $\mathfrak{S}$ ist zu $\mathfrak{T}$ fremd, also hat die Vereinigung $\mathfrak{S} \vee \mathfrak{T}$ die Mächtigkeit $s + t$. Wenn wir beweisen können, daß $\mathfrak{S} \vee \mathfrak{T}$ in bezug auf P irreduzibel und mit Ω äquivalent ist, so sind wir fertig.

[1] Der Satz gilt zwar auch für unendliche Transzendenzgrade, erfordert dann aber den Begriff der Addition von unendlichen Mächtigkeiten, den wir nicht erklärt haben.

Ω ist algebraisch in bezug auf $\Sigma(\mathfrak{T})$ und Σ algebraisch in bezug auf $\mathsf{P}(\mathfrak{S})$, also Ω algebraisch in bezug auf $\mathsf{P}(\mathfrak{S}, \mathfrak{T})$, also äquivalent mit $\mathfrak{S} \vee \mathfrak{T}$.

Bestünde eine algebraische Relation zwischen endlichvielen Elementen von $\mathfrak{S} \vee \mathfrak{T}$ mit Koeffizienten aus P, so könnten darin zunächst die Elemente von $\mathfrak{T}$ nicht wirklich vorkommen; denn sonst bestünde eine Relation zwischen diesen mit Koeffizienten aus Σ, was der Irreduzibilität von $\mathfrak{T}$ widerstreitet. Also bestünde eine Relation zwischen den Elementen von $\mathfrak{S}$ allein, was wiederum der Irreduzibilität von $\mathfrak{S}$ widerspricht. $\mathfrak{S} \vee \mathfrak{T}$ ist also irreduzibel in bezug auf P, womit alles bewiesen ist.

Zehntes Kapitel.

Reelle Körper.

Beim Studium der algebraischen Zahlkörper spielen außer den algebraischen Eigenschaften ihrer Zahlen gewisse unalgebraische Eigenschaften: *absolute Beträge* $|a|$, *Realität, Positivsein*, eine Rolle. Daß diese Eigenschaften sich nicht mit Hilfe der algebraischen Operationen $+$ und $\cdot$ eindeutig definieren lassen, zeigt sich an folgendem Beispiel.

Es sei w eine reelle, also iw eine rein imaginäre Wurzel der Gleichung $x^4 = 2$. Bei der Isomorphie

$$\Gamma(w) \cong \Gamma(iw)$$

bleiben alle algebraischen Eigenschaften erhalten; aber diese Isomorphie führt die reelle Zahl w in die rein imaginäre iw, die positive Zahl $w^2 = \sqrt{2}$ in die negative $(iw)^2 = -\sqrt{2}$ über, während die Zahl $1 + \sqrt{2}$ vom Betrag > 1 in die Zahl $1 - \sqrt{2}$ vom Betrag < 1 übergeht.

Im Verlauf der Untersuchung wird sich aber zeigen, daß an diesen nichtalgebraischen Eigenschaften trotzdem etwas Algebraisches haftet, daß man nämlich im Körper der algebraischen Zahlen (d. h. in dem zu Γ gehörigen algebraisch-abgeschlossenen Erweiterungskörper) zwar nicht *einen*, wohl aber eine ganze Schar von Unterkörpern, deren jeder dem Körper der reellen algebraischen Zahlen algebraisch-äquivalent ist, durch algebraische Eigenschaften auszeichnen kann. Bei einer bestimmten Wahl eines solchen Körpers, dessen Elemente dann als „reell" bezeichnet werden können, lassen sich auch die Beträge und das Positivsein algebraisch definieren. Für jeden endlichen algebraischen Zahlkörper werden dann die Definitionen der Beträge, der Realität usw. *endlich-vieldeutig*.

Bevor wir aber an diese algebraische Theorie herangehen, erörtern wir zunächst die in der Analysis übliche (transzendente) Einführung der reellen und komplexen Zahlen, nicht so sehr, weil es logisch notwendig

wäre, das vorwegzunehmen, als weil die Problemstellung der rein algebraischen Theorie klarer wird, wenn man einmal weiß, was reelle und komplexe Zahlen überhaupt sind, und weil wir zugleich die prinzipiell wichtigen Begriffe der Anordnung und der Bewertung dabei besprechen können. Wir beschränken uns dabei wieder auf kommutative Körper.

§ 63. Angeordnete Körper.

In diesem Paragraphen sollen eine erste nichtalgebraische Eigenschaft: das „Positivsein", und die darauf beruhende „Anordnung" axiomatisch untersucht werden.

Ein (kommutativer) Körper K *heiße „angeordnet", wenn für seine Elemente die Eigenschaft, positiv* (>0) *zu sein, gemäß den folgenden Forderungen definiert ist:*

1. *Für jedes Element* a *aus* K *gilt genau eine der Beziehungen*

$$a = 0, \quad a > 0, \quad -a > 0.$$

2. *Ist* $a > 0$ *und* $b > 0$, *so ist* $a + b > 0$ *und* $ab > 0$.

Ist $-a > 0$, so sagen wir: a ist *negativ*.

Definieren wir in einem angeordneten Körper allgemein eine Größenbeziehung durch die Festsetzung

$$a > b, \text{ in Worten: } a \text{ größer als } b,$$
$$(\text{oder } b < a, \text{ in Worten: } b \text{ kleiner als } a),$$
$$\text{wenn } a - b > 0,$$

so zeigt man mühelos, daß die mengentheoretischen Ordnungsaxiome (§ 57) erfüllt sind. Für je zwei Elemente a, b ist nämlich entweder $a < b$ oder $a = b$ oder $a > b$. Aus $a > b$ und $b > c$ folgt $a - b > 0$ und $b - c > 0$, also auch $a - c = (a - b) + (b - c) > 0$, mithin $a > c$. Weiter hat man wie im § 3 die Regel, daß aus $a > b$ folgt $a + c > b + c$ und im Falle $c > 0$ auch $ac > bc$. Schließlich folgt, wenn a und b positiv sind, aus $a > b$ stets $a^{-1} < b^{-1}$ (und umgekehrt), da

$$ab\,(b^{-1} - a^{-1}) = a - b$$

ist.

Verstehen wir in einem angeordneten Körper unter dem *Betrag* $|a|$ eines Elements a das nicht-negative unter den Elementen a, $-a$, so gelten für das Rechnen mit Beträgen die Regeln

$$|ab| = |a| \cdot |b|,$$
$$|a + b| \leqq |a| + |b|.$$

Die erstere verifiziert man ohne jede Mühe für die vier möglichen Fälle

$$a \geqq 0, \quad b \geqq 0;$$
$$a \geqq 0, \quad b < 0;$$
$$a < 0, \quad b \geqq 0;$$
$$a < 0, \quad b < 0.$$

Die zweite Regel gilt offenbar mit dem Gleichheitszeichen im Fall $a \geqq 0$, $b \geqq 0$, da dann beide Seiten gleich der nicht-negativen Zahl $a + b$ sind, und ebenso im Fall $a < 0$, $b < 0$, wo beide Seiten gleich der nicht-negativen Zahl $-(a + b)$ sind. Es bleiben von unseren vier Fällen noch die beiden mittleren übrig; es genügt, den einen: $a \geqq 0$, $b < 0$, zu betrachten. Es ist dann

$$\begin{aligned} a + b < \ a \ < a - b &= |a| + |b|, \\ -a - b \leqq -b \leqq a - b &= |a| + |b|, \end{aligned}$$

also

$$|a + b| \leqq |a| + |b|.$$

Man hat auch

$$a^2 = (-a)^2 = |a|^2 \geqq 0,$$

mit dem Gleichzeichen nur für $a = 0$. Daraus folgt weiter, daß eine Summe von Quadraten stets $\geqq 0$ ist, und zwar $= 0$ nur dann, wenn alle Summanden einzeln verschwinden.

Insbesondere ist das Einselement $1 = 1^2$ stets positiv, ebenso jede Summe $n \cdot 1 = 1 + 1 + \cdots + 1$. Daher kann auch nie $p \cdot 1 = 0$ sein, wenn p eine Primzahl ist. Also: *Die Charakteristik eines angeordneten Körpers ist Null.*

Hilfssatz. *Ist* K *der Quotientenkörper des Ringes* $\mathfrak{R}$ *und ist* $\mathfrak{R}$ *angeordnet, so kann* K *auf eine und nur eine Weise so angeordnet werden, daß die Anordnung von* $\mathfrak{R}$ *erhalten bleibt.*

Es sei nämlich K in der gewünschten Weise angeordnet. Ein beliebiges Element von K hat die Gestalt $a = \frac{b}{c}$ (b und c in $\mathfrak{R}$ und $c \neq 0$). Aus

$$\frac{b}{c} > 0 \text{ bzw. } = 0 \text{ bzw. } < 0$$

folgt durch Multiplikation mit c^2 sofort

$$bc > 0 \text{ bzw. } = 0 \text{ bzw. } < 0.$$

Also ist die etwaige Anordnung von K durch die von $\mathfrak{R}$ eindeutig bestimmt. Umgekehrt erkennt man leicht, daß durch die Festsetzung

$$\frac{b}{c} > 0, \text{ wenn } bc > 0,$$

tatsächlich eine Anordnung von K definiert ist, bei der die Anordnung von $\mathfrak{R}$ erhalten bleibt.

Insbesondere läßt sich also der Körper Γ der rationalen Zahlen nur in einer Weise anordnen, da der Ring C der ganzen Zahlen offenbar nur der natürlichen Anordnung fähig ist. Es ist also $\frac{m}{n} > 0$, sobald $m \cdot n$ eine natürliche Zahl ist.

Zwei angeordnete Körper heißen *ähnlich-isomorph*, wenn es einen Isomorphismus der beiden Körper gibt, der positive Elemente stets wieder in positive überführt.

Ein Körper heißt *archimedisch angeordnet*[1], wenn es in einer gegebenen Anordnung zu jedem Körperelement a eine „natürliche Zahl" $n > a$ gibt. Es gibt dann auch zu jedem a eine Zahl $-n < a$ und zu jedem positiven a einen Bruch $\frac{1}{n} < a$. Z. B. ist der rationale Zahlkörper Γ archimedisch angeordnet. Ist ein Körper nicht-archimedisch angeordnet, so gibt es „unendlich große" Elemente, die größer als jede rationale Zahl, und „unendlich kleine" Elemente, die kleiner als jede positive rationale Zahl, aber größer als Null sind.

Literatur über nicht-archimedisch angeordnete Körper.

Artin, E. u. O. Schreier: Algebraische Konstruktion reeller Körper. Abh. Math. Sem. Hamburg. Bd. 5, S. 83—115. 1926.

Baer, R.: Über nicht-archimedisch geordnete Körper. Sitzungsber. Heidelb. Ak. 8. Abhandlung, 1927.

Aufgaben. 1. Man nenne ein Polynom $f(t)$ mit rationalen Koeffizienten positiv, wenn der Koeffizient der höchsten vorkommenden Potenz der Unbestimmten t positiv ist. Man zeige, daß damit eine Anordnung des Polynomrings $\Gamma[t]$ und daher auch des Quotientenkörpers $\Gamma(t)$ definiert ist und daß die letztere Anordnung nicht-archimedisch ist (t ist „unendlich groß").

2. Es sei

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_n,$$

wo die a_i einem angeordneten Körper K entnommen sind. Es sei M das größte der Elemente 1 und $|a_1| + \cdots + |a_n|$. Man zeige, daß

$$f(s) > 0 \text{ für } s > \mathsf{M}$$
$$(-1)^n f(s) > 0 \text{ für } s < -\mathsf{M}$$

ist. Wenn also $f(x)$ Nullstellen in K besitzt, so liegen diese im Bereich $-\mathsf{M} \leqq s \leqq \mathsf{M}$.

3. Unter den Bezeichnungen von Aufg. 2 sei $R > 0$, $-S$ die Summe der negativen unter den Größen $a_1, \frac{a_2}{R}, \frac{a_3}{R^2}, \ldots, \frac{a_n}{R^{n-1}}$; es sei M_R die größte der Zahlen R und S. Dann ist für $s > \mathsf{M}_R$ stets $f(s) > 0$. (Für $R = 1$ erhält man eine Verschärfung der oberen Grenze M von Aufg. 2.)

4. Es sei wieder $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$, alle $a_\nu \geqq -c$, $c \geqq 0$. Man zeige, daß $f(s) > 0$ für $s \geqq 1 + c$. [Man benutze die Ungleichung $s^m \geqq c\,(s^{m-1} + s^{m-2} + \cdots + 1)$.] Durch Ersetzung von x durch $-x$ bestimme man in derselben Weise eine Schranke $-1 - c'$, so daß $(-1)^n f(s) > 0$ für $s < -1 - c'$. Sind außer dem Anfangskoeffizienten 1

[1] Das „Archimedische Axiom" in der Geometrie lautet nämlich so: Man kann jede gegebene Strecke PQ („Einheitsstrecke") von einem gegebenen Punkt P („Nullpunkt") stets so oft in der Richtung PR abtragen, daß man über jeden gegebenen Punkt R hinauskommt.

auch noch $a_1, \ldots, a_r$ positiv, so läßt sich die Schranke $1 + c$ auch durch $1 + \frac{c}{1+a_1+\cdots+a_r}$ ersetzen.

5. Für $a > b > 0$ ist $a^n > b^n > 0$ (n eine natürliche Zahl). Das Polynom $x^n - c$ hat in jedem angeordneten Körper K höchstens eine positive Nullstelle $\sqrt[n]{c}$. Für ungerades n hat es überhaupt höchstens eine Nullstelle; für gerades n höchstens zwei, die dann entgegengesetzt sind. Existieren $\sqrt[n]{c}$ und $\sqrt[n]{d}$ beide und ist $0 < c < d$, so ist $\sqrt[n]{c} < \sqrt[n]{d}$.

§ 64. Definition der reellen Zahlen.

Es sei K ein angeordneter Körper und $\mathfrak{M}$ eine nichtleere Menge von Elementen aus K. Wenn alle Elemente von $\mathfrak{M}$ kleiner oder gleich einer festen Größe s aus K sind, so heißt s eine *obere Schranke* von $\mathfrak{M}$, und $\mathfrak{M}$ heißt *nach oben beschränkt*. Wenn es eine kleinste obere Schranke gibt, so heißt diese *die obere Grenze* der Menge $\mathfrak{M}$.

Sind alle Elemente von $\mathfrak{M}$ größer oder gleich einer festen Größe s' aus K, so heißt s' eine *untere Schranke* von $\mathfrak{M}$, und $\mathfrak{M}$ heißt *nach unten beschränkt*.

Im rationalen Zahlkörper Γ besitzt nicht jede nach oben beschränkte Menge $\mathfrak{M}$ eine obere Grenze. Beispiel: $\mathfrak{M}$ sei die Menge der positiven Zahlen, deren Quadrat kleiner als 3 ist. Eine obere Schranke von $\mathfrak{M}$ ist jede positive rationale Zahl, deren Quadrat größer als 3 ist. Eine Zahl von Γ, deren Quadrat gleich 3 ist, gibt es nicht, da $x^2 - 3$ in Γ irreduzibel ist. Ist r eine positive rationale Zahl und $r^2 > 3$, so ist

$$r' = \frac{r + 3r^{-1}}{2}$$

eine kleinere positive Zahl, deren Quadrat auch noch > 3 ist; denn es ist

$$r' = \frac{r + 3r^{-1}}{2} > \frac{r}{2} > 0,$$

$$r' = \frac{r + 3r^{-1}}{2} < \frac{r + r^2 r^{-1}}{2} = r,$$

$$r'^2 = \left(\frac{r + 3r^{-1}}{2}\right)^2 = \left(\frac{r - 3r^{-1}}{2}\right)^2 + 3 \geqq 3, \quad \text{also} \quad > 3.$$

Also gibt es zu jeder oberen Schranke r in Γ eine kleinere obere Schranke r', und somit existiert keine obere Grenze.

Wir wollen nun versuchen, zu jedem archimedisch angeordneten Körper K einen angeordneten Erweiterungskörper Ω zu finden, in welchem jede nach oben beschränkte nichtleere Menge auch eine obere Grenze besitzt. Ist speziell K der Körper der rationalen Zahlen, so wird Ω der wohlbekannte Körper der „reellen Zahlen" werden. Von den verschiedenen aus der Grundlegung der Analysis bekannten Konstruktionen des Körpers Ω bringen wir hier die Cantorsche Konstruktion durch „Fundamentalfolgen".

Eine unendliche Folge von Elementen $a_1, a_2, \ldots$ aus einem angeordneten Körper K heißt eine *Fundamentalfolge* $\{a_\nu\}$, wenn es zu jeder positiven Größe ε von K eine natürliche Zahl $n = n(\varepsilon)$ gibt, so daß

$$|a_p - a_q| < \varepsilon \quad \text{für} \quad p > n,\ q > n. \tag{1}$$

Aus (1) folgt für $q = n + 1$:

$$|a_p| \leqq |a_q| + |a_p - a_q| < |a_{n+1}| + \varepsilon = \mathsf{M} \quad \text{für} \quad p > n.$$

Also ist jede Fundamentalfolge nach oben und unten beschränkt.

Summen und Produkte von Fundamentalfolgen werden definiert durch

$$c_n = a_n + b_n; \qquad d_n = a_n b_n.$$

Daß die Summe und das Produkt wieder Fundamentalfolgen sind, sieht man so: Zu jedem ε gibt es ein n_1 mit

$$|a_p - a_q| < \tfrac{1}{2}\varepsilon \quad \text{für} \quad p > n_1,\ q > n_1$$

und ein n_2 mit

$$|b_p - b_q| < \tfrac{1}{2}\varepsilon \quad \text{für} \quad p > n_2,\ q > n_2.$$

Ist nun n die größte der Zahlen n_1 und n_2, so folgt

$$|(a_p + b_p) - (a_q + b_q)| < \varepsilon \quad \text{für} \quad p > n,\ q > n.$$

Ebenso gibt es ein M_1 und ein M_2 mit

$$|a_p| < \mathsf{M}_1 \quad \text{für} \quad p > n_1,$$
$$|b_p| < \mathsf{M}_2 \quad \text{für} \quad p > n_2$$

und weiter zu jedem ε ein $n' \geqq n_2$ und ein $n'' \geqq n_1$ mit

$$|a_p - a_q| < \frac{\varepsilon}{2\,\mathsf{M}_2} \quad \text{für} \quad p > n',\ q > n',$$

$$|b_p - b_q| < \frac{\varepsilon}{2\,\mathsf{M}_1} \quad \text{für} \quad p > n'',\ q > n''.$$

Daraus folgt durch Multiplikation mit $|b_p|$ bzw. $|a_q|$

$$|a_p b_p - a_q b_p| < \frac{\varepsilon}{2} \quad \text{für} \quad p > n',\ q > n',$$

$$|a_q b_p - a_q b_q| < \frac{\varepsilon}{2} \quad \text{für} \quad p > n'',\ q > n'',$$

also, wenn n die größte der Zahlen n' und n'' ist,

$$|a_p b_p - a_q b_q| < \varepsilon \quad \text{für} \quad p > n,\ q > n.$$

Die Addition und Multiplikation von Fundamentalfolgen erfüllen offensichtlich alle Postulate für einen Ring; es gilt also: *Die Fundamentalfolgen bilden einen Ring* $\mathfrak{o}$.

Eine Fundamentalfolge $\{a_p\}$, die „zu 0 konvergiert", d. h. bei der es zu jedem ε ein n gibt mit

$$|a_p| < \varepsilon \quad \text{für} \quad p > n,$$

heißt eine *Nullfolge*. Wir zeigen nun:

Die Nullfolgen bilden ein Ideal $\mathfrak{n}$ *im Ring* $\mathfrak{o}$.

Beweis. Wenn $\{a_\nu\}$ und $\{b_\nu\}$ Nullfolgen sind, so gibt es zu jedem ε ein n_1 und ein n_2 mit

$$|a_\nu| < \tfrac{1}{2}\varepsilon \qquad \text{für} \quad \nu > n_1,$$
$$|b_\nu| < \tfrac{1}{2}\varepsilon \qquad \text{für} \quad \nu > n_2,$$

also, wenn wieder n die größte der Zahlen n_1, n_2 ist,

$$|a_\nu - b_\nu| < \varepsilon \qquad \text{für} \quad \nu > n;$$

mithin ist auch $\{a_\nu - b_\nu\}$ eine Nullfolge. Ist weiter $\{a_\nu\}$ eine Nullfolge und $\{c_\nu\}$ eine beliebige Fundamentalfolge, so bestimme man ein n' und ein M so, daß

$$|c_\nu| < \mathsf{M} \qquad \text{für} \quad \nu > n',$$

und zu jedem ε ein $n = n(\varepsilon) \geqq n'$, so daß

$$|a_\nu| < \frac{\varepsilon}{\mathsf{M}} \qquad \text{für} \quad \nu > n.$$

Dann folgt

$$|a_\nu c_\nu| < \varepsilon \qquad \text{für} \quad \nu > n;$$

mithin ist auch $\{a_\nu c_\nu\}$ eine Nullfolge.

Der Restklassenring $\mathfrak{o}/\mathfrak{n}$ heiße Ω. Wir zeigen, daß *Ω ein Körper ist*, d. h. daß in $\mathfrak{o}$ die Kongruenz

$$a x \equiv 1 \,(\mathfrak{n}) \tag{2}$$

für $a \not\equiv 0\,(\mathfrak{n})$ eine Lösung besitzt. Dabei bedeutet 1 das Einselement von $\mathfrak{o}$, d. h. die Fundamentalfolge $\{1, 1, \ldots\}$.

Es muß ein n und ein $\eta > 0$ geben mit

$$|a_\varrho| \geqq \eta \qquad \text{für} \quad \varrho > n.$$

Denn wenn es für alle n und alle $\eta > 0$ noch

$$|a_\varrho| < \eta \qquad (\varrho > n),$$

geben würde, so würde man n bei gegebenem η auch so groß wählen können, daß für $\nu > n$, $\varrho > n$

$$|a_\nu - a_\varrho| < \eta$$

wäre, und daraus würde folgen

$$|a_\nu| < 2\eta$$

für alle $\nu > n$, d. h. die Folge $\{a_\nu\}$ wäre eine Nullfolge, entgegen der Voraussetzung.

Die Fundamentalfolge $\{a_\nu\}$ bleibt in derselben Restklasse modulo $\mathfrak{n}$, wenn wir $a_1, \ldots, a_n$ durch η ersetzen. Bezeichnet man diese n neuen Elemente η wieder mit $a_1, \ldots, a_n$, so ist für *alle* ν

$$|a_\nu| \geqq \eta, \quad \text{insbesondere} \quad a_\nu \neq 0.$$

Nun ist $\{a_\nu^{-1}\}$ eine Fundamentalfolge. Denn zu jedem ε gibt es ein n, so daß

$$|a_\varrho - a_\nu| < \varepsilon\eta^2 \qquad \text{für} \quad \nu > n, \ \varrho > n.$$

Wäre nun $|a_p^{-1} - a_q^{-1}| \geqq \varepsilon$ für ein $p > n$ und ein $q > n$, so würde durch Multiplikation mit $|a_p| \geqq \eta$ und $|a_q| \geqq \eta$ folgen

$$|a_q - a_p| = |a_p a_q (a_p^{-1} - a_q^{-1})| \geqq \varepsilon \eta^2,$$

was nicht zutrifft. Also ist

$$|a_p^{-1} - a_q^{-1}| < \varepsilon \qquad \text{für} \quad p > n, \; q > n.$$

Die Fundamentalfolge $\{a_p^{-1}\}$ löst offenbar die Kongruenz (2).

Der Körper Ω enthält insbesondere diejenigen Restklassen mod $\mathfrak{n}$, die durch Fundamentalfolgen von der Gestalt

$$\{a, a, a, \ldots\}$$

dargestellt werden. Diese bilden einen zu K isomorphen Unterring K' von Ω; denn jedem a von K entspricht eine solche Restklasse, verschiedenen a entsprechen verschiedene Restklassen, der Summe entspricht die Summe, und dem Produkt entspricht das Produkt. Identifizieren wir nun die Elemente von K' mit denen von K, so wird Ω ein Erweiterungskörper von K.

Eine Fundamentalfolge $\{a_p\}$ heißt *positiv*, wenn es ein $\varepsilon > 0$ in K und ein n gibt, derart, daß

$$a_p > \varepsilon \qquad \text{für} \quad p > n$$

ist. Die Summe und das Produkt zweier positiver Fundamentalfolgen sind offenbar wieder positiv. Auch die Summe einer positiven Folge $\{a_p\}$ und einer Nullfolge $\{b_p\}$ ist stets positiv; das zeigt man, indem man ein n so groß wählt, daß

$$a_p > \varepsilon \qquad \text{für} \quad p > n,$$
$$|b_p| < \tfrac{1}{2}\varepsilon \qquad \text{für} \quad p > n$$

ist, und daraus schließt, daß $a_p + b_p > \frac{1}{2}\varepsilon$ ist für $p > n$. Mithin sind alle Folgen einer Restklasse modulo $\mathfrak{n}$ positiv, sobald eine einzige es ist. In diesem Fall heißt die Restklasse selbst *positiv*. Eine Restklasse k heißt *negativ*, wenn $-k$ positiv ist.

Ist weder $\{a_p\}$ noch $\{-a_p\}$ positiv, so gibt es zu jedem $\varepsilon > 0$ und jedem n ein $r > n$ und ein $s > n$, so daß

$$a_r \leqq \varepsilon \quad \text{und} \quad -a_s \leqq \varepsilon.$$

Wählt man nun n so groß, daß für $p > n$, $q > n$

$$|a_p - a_q| < \varepsilon$$

ist, so folgert man, indem man zuerst $q = r$ und p beliebig $> n$ nimmt,

$$a_p = (a_p - a_q) + a_r < \varepsilon + \varepsilon = 2\varepsilon$$

und, indem man sodann $q = s$ und p beliebig $> n$ nimmt,

$$-a_p = (a_q - a_p) - a_s < \varepsilon + \varepsilon = 2\varepsilon,$$

mithin

$$|a_p| < 2\varepsilon \qquad \text{für} \quad p > n.$$

Daher ist $\{a_p\}$ eine Nullfolge.

Also ist stets entweder $\{a_\nu\}$ positiv oder $\{-a_\nu\}$ positiv oder $\{a_\nu\}$ eine Nullfolge. Daher ist jede Restklasse mod $\mathfrak{n}$ entweder positiv oder negativ oder Null. Da Summe und Produkt positiver Restklassen wieder positiv sind, so schließt man:

Ω ist ein angeordneter Körper.

Man sieht unmittelbar, daß die Anordnung von K in Ω erhalten bleibt.

Definiert eine Folge $\{a_\nu\}$ ein Element α und eine Folge $\{b_\nu\}$ ein Element β von Ω, so folgt aus

$$a_\nu \geqq b_\nu \qquad \text{für} \quad \nu > n$$

stets $\alpha \geqq \beta$. Wäre nämlich $\alpha < \beta$, also $\beta - \alpha > 0$, so würde es zu der Fundamentalfolge $\{b_\nu - a_\nu\}$ ein ε und ein m geben, so daß

$$b_\nu - a_\nu > \varepsilon > 0 \qquad \text{für} \quad \nu > m$$

wäre. Wählt man hier $\nu = m + n$, so kommt man in Widerspruch zur Voraussetzung $a_\nu \geqq b_\nu$.

Aus der Beschränktheit einer jeden Fundamentalfolge nach oben folgt, daß es zu jedem Element ω von Ω ein größeres Element s von K gibt. Ist K *archimedisch* angeordnet, so gibt es zu s wiederum eine größere natürliche Zahl n; mithin gibt es zu jedem ω auch ein $n > \omega$, d. h. *Ω ist archimedisch angeordnet.*

Nunmehr wollen wir für den archimedisch angeordneten Körper Ω den *Satz von der oberen Grenze* beweisen:

Jede nach oben beschränkte nichtleere Menge $\mathfrak{M} \subset \Omega$ hat in Ω eine obere Grenze.

Beweis. Es sei s eine obere Schranke von $\mathfrak{M}$, M eine ganze Zahl $> s$ (also ebenfalls eine obere Schranke), μ ein beliebiges Element von $\mathfrak{M}$ und m eine ganze Zahl $> -\mu$. Dann ist

$$-m < \mu < M.$$

Für jede natürliche Zahl ν bilden wir nun die endlichvielen Brüche $k \cdot 2^{-\nu}$ (k eine ganze Zahl), die „zwischen" $-m$ und M liegen:

$$-m \leqq k \cdot 2^{-\nu} \leqq M.$$

Wir suchen den kleinsten derjenigen unter diesen Brüchen, die noch obere Schranken der Menge $\mathfrak{M}$ bilden. Einen solchen gibt es, weil M selbst diese Eigenschaft hat.

Diese kleinste obere Schranke bezeichnen wir mit a_ν. Dann ist $a_\nu - 2^{-\nu}$ keine obere Schranke mehr; mithin ist für jedes $\varrho > \nu$

$$a_\nu - 2^{-\nu} < a_\varrho \leqq a_\nu. \tag{4}$$

Daraus folgt

$$|a_\nu - a_\varrho| < 2^{-\nu},$$

mithin

$$|a_\nu - a_\varrho| < 2^{-n} \qquad \text{für} \quad \nu > n, \ \varrho > n. \tag{5}$$

Bei gegebenem ε kann man nun stets eine natürliche Zahl $h > \varepsilon^{-1}$ und weiter ein $2^n > h > \varepsilon^{-1}$ finden. Dann ist $2^{-n} < \varepsilon$. Mithin besagt (5), daß $\{a_p\}$ eine Fundamentalfolge ist, die somit ein Element ω von Ω definiert. Aus (4) folgt weiter, daß

$$a_p - 2^{-p} \leqq \omega \leqq a_p$$

ist.

ω ist eine obere Schranke von $\mathfrak{M}$; d. h. alle Elemente μ von $\mathfrak{M}$ sind $\leqq \omega$. Wäre nämlich $\mu > \omega$, so könnte man eine Zahl $2^p > (\mu - \omega)^{-1}$ finden; dann wäre also $2^{-p} < \mu - \omega$. Addiert man dazu $a_p - 2^{-p} \leqq \omega$, so folgt $a_p < \mu$, was nicht geht, da a_p eine obere Schranke von $\mathfrak{M}$ ist.

ω ist die kleinste obere Schranke von $\mathfrak{M}$. Wäre nämlich σ eine kleinere, so könnte man wieder eine Zahl p mit $2^{-p} < \omega - \sigma$ finden. Da $a_p - 2^{-p}$ keine obere Schranke von $\mathfrak{M}$ ist, so gibt es ein μ in $\mathfrak{M}$ mit $a_p - 2^{-p} < \mu$. Daraus folgt

$$a_p - 2^{-p} < \sigma$$

und durch Addition zum vorigen

$$a_p < \omega,$$

was nicht zutrifft. Also ist ω die obere Grenze von $\mathfrak{M}$.

Die obige Konstruktion ergibt demnach zu jedem angeordneten Körper K einen eindeutig bestimmten angeordneten Erweiterungskörper Ω, in dem, wenn K archimedisch ist, der Satz von der oberen Grenze gilt. Ist K speziell der Körper der rationalen Zahlen, so ist Ω der Körper der *reellen Zahlen*. Eine reelle Zahl ist also in dieser Theorie definiert als eine Restklasse modulo $\mathfrak{n}$ im Bereich der Fundamentalfolgen aus rationalen Zahlen.

Wir können zeigen, daß der Körper Ω selbst sich nicht mehr durch Hinzunahme von Fundamentalfolgen erweitern läßt, sondern daß jede Fundamentalfolge $\{a_p\}$ aus Ω zu einer Folge $\{a\}$ aus lauter gleichen Elementen von Ω kongruent ist modulo dem Ideal der Nullfolgen aus Ω.

Ist $\{\alpha_p\} \equiv \{\alpha\}$ modulo diesem Ideal, d. h. ist $\{\alpha_p - \alpha\}$ eine Nullfolge, so sagt man, die Folge $\{\alpha_p\}$ *konvergiere zum Limes* α, geschrieben

$$\lim_{p \to \infty} \alpha_p = \alpha, \qquad \text{kurz} \quad \lim \alpha_p = \alpha.$$

Wir haben also zu zeigen, daß jede Fundamentalfolge $\{\alpha_p\}$ in Ω einen Limes besitzt (*Konvergenzsatz von* CAUCHY). Zu dem Zweck wählen wir zu jedem α_p ein approximierendes a_p aus K mit der Eigenschaft

$$|a_p - \alpha_p| < 2^{-p}.$$

Das geht, weil α_p selbst durch eine Fundamentalfolge $\{a_{p1}, a_{p2}, \ldots\}$ aus K definiert war, deren Elemente für hinreichend hohen Index sich um beliebig wenig von ihrem Limes α_p unterscheiden. Man zeigt dann mühelos, daß diese a_p eine Fundamentalfolge in K bilden, die also ein Element ω von Ω definiert, und daß $|\alpha_p - \omega| < \varepsilon$ ist für alle $p > n(\varepsilon)$.

Aufgaben. 1. Man zeige die folgenden Eigenschaften des Limesbegriffs:

a) Sind $\{\alpha_n\}$ und $\{\beta_n\}$ konvergente Folgen, so ist

$$\lim(\alpha_n \pm \beta_n) = \lim \alpha_n \pm \lim \beta_n,$$
$$\lim \alpha_n \beta_n = \lim \alpha_n \cdot \lim \beta_n.$$

b) Ist $\lim \beta_n \neq 0$ und alle $\beta_n \neq 0$, so ist

$$\lim(\beta_n^{-1}) = (\lim \beta_n)^{-1}.$$

c) Eine Teilfolge einer konvergenten Folge ist konvergent zum selben Limes.

2. Die (bis auf äquivalente Erweiterungen) einzige Art, einen archimedisch angeordneten Körper zu einem ebensolchen zu erweitern, in dem der Cauchysche Konvergenzsatz gilt, ist die obige Konstruktion mittels der Fundamentalfolgen.

3. Jeder archimedisch angeordnete Körper ist ähnlich-isomorph einem Unterkörper des Körpers der reellen Zahlen.

4. Jede reelle Zahl s ist als unendlicher Dezimalbruch

$$s = a_0 + \sum_{\nu=1}^{\infty} a_\nu 10^{-\nu} \text{ (d. h. } s = \lim_{n\to\infty}(a_0 + \sum_{\nu=1}^{n} a_\nu 10^{-\nu})) \quad (0 \leqq a_\nu < 10)$$

darstellbar.

§ 65. Bewertete Körper. — p-adische Zahlen.

Die im vorigen Paragraphen angegebene Konstruktion des Körpers Ω zu einem gegebenen Körper K benutzt[1] nicht ganz die Anordnung des Körpers K, sondern nur die Anordnung der absoluten Beträge $|a|$ der Körperelemente a. Es liegt daher nahe, zu versuchen, diese Konstruktion auch auf andere als nur angeordnete Körper auszudehnen, für welche eine Funktion $\varphi(a)$ mit den Eigenschaften des absoluten Betrages $|a|$ existiert.

Ein Körper K heißt *bewertet*, wenn für die Elemente a von K eine Funktion $\varphi(a)$ definiert ist mit folgenden Eigenschaften:

1. $\varphi(a)$ ist ein Element eines festen archimedisch angeordneten Körpers P.
2. $\varphi(a) > 0$ für $a \neq 0$; $\varphi(0) = 0$.
3. $\varphi(a) \cdot \varphi(b) = \varphi(ab)$.
4. $\varphi(a + b) \leqq \varphi(a) + \varphi(b)$.

Aus 2. und 3. folgt sofort:

$$\varphi(1) = 1, \quad \varphi(-1) = 1, \quad \varphi(a) = \varphi(-a).$$

Aus 4. folgt

$$\varphi(c) - \varphi(a) \leqq \varphi(c - a),$$

ebenso

$$\varphi(a) - \varphi(c) \leqq \varphi(c - a),$$

mithin schließlich

$$|\varphi(c) - \varphi(a)| \leqq \varphi(c - a).$$

---

[1] Im Gegensatz zu anderen Verfahren, z. B. zu der Dedekindschen Schnittkonstruktion.

Nach Aufgabe 3, § 64 kann man für P immer den Körper der reellen Zahlen nehmen, was wir im folgenden tun werden.

Die Eigenschaften 1 bis 4 sind erfüllt, wenn K selbst archimedisch angeordnet ist und $\varphi(a) = |a|$ gesetzt wird.

Aber auch für nicht-angeordnete Körper kann man Funktionen $\varphi(a)$ mit den obigen Eigenschaften konstruieren. Außer der „trivialen" Bewertung: $\varphi(a) = 1$ für $a \neq 0$, $\varphi(0) = 0$, die für jeden Körper gilt, hat man z. B. für den Körper der komplexen Zahlen die Bewertung

$$\varphi(a + bi) = |a + bi| = \sqrt{a^2 + b^2}$$

(siehe später § 69).

Weiter gibt es für gewisse Körper, wie z. B. für den der rationalen Zahlen, andere Bewertungen, die nichts mit dem absoluten Betrag zu tun haben und trotzdem die Eigenschaften 1 bis 4 besitzen. Ist p eine feste Primzahl und schreibt man jede rationale Zahl $a \neq 0$ in der Form

$$a = r\,p^n,$$

wo r ein Bruch ist, der weder im Zähler noch im Nenner den Faktor p hat, und n eine ganze Zahl bedeutet, so kann man setzen

$$\varphi(a) = p^{-n};\ \varphi(0) = 0.$$

Diese Funktion genügt, wie leicht ersichtlich, den Bedingungen 1 bis 4. Sie heißt die *p-adische Bewertung* des Körpers Γ. Bei dieser Bewertung ist die Folge p, p^2, p^3, ... eine Nullfolge.

Zu jedem bewerteten Körper K kann man nun genau nach dem Verfahren von § 64 einen bewerteten Erweiterungskörper Ω konstruieren, für den der Cauchysche Konvergenzsatz gilt. Einen solchen Körper nennt man „*perfekt*". Die Beweise sind wörtlich die gleichen wie in § 64. Die Bewertung von Ω wird so definiert: Ist α durch die Fundamentalfolge $\{a_\nu\}$ definiert, also $\alpha = \lim a_\nu$, so setze man

$$\varphi(\alpha) = \lim \varphi(a_\nu).$$

Daß die $\varphi(a_\nu)$ tatsächlich eine Fundamentalfolge in P bilden, folgt aus

$$|\varphi(a_\mu) - \varphi(a_\nu)| \leqq \varphi(a_\mu - a_\nu).$$

Aus dem p-adisch bewerteten Körper der rationalen Zahlen erhält man so den perfekten *Körper der p-adischen Zahlen* Ω_p von Hensel. Die Körper Ω_2, Ω_3, Ω_5, Ω_7, Ω_{11}, ... sind alle verschieden, d. h. nicht isomorph.

Ist $\{r_1, r_2, \ldots\}$ eine p-adische Fundamentalfolge aus rationalen Zahlen und setzt man

$$r_\nu = \frac{a_\nu}{b_\nu}\,p^{m_\nu}\ (a_\nu \text{ und } b_\nu \text{ relativprim zu } p),$$

so kann man eine neue Folge $\{s_\nu\} = \{x_\nu\,p^{m_\nu}\}$ (x_ν eine natürliche Zahl) bestimmen aus der Bedingung

$$\varphi(r_\nu - s_\nu) \leqq p^{-\nu}.$$

Dazu hat man nämlich nur $x_\nu = 1$ zu setzen für $\nu < m_\nu$, während man für $\nu \geqq m_\nu$ die Kongruenz

$$b_\nu x_\nu \equiv a_\nu \pmod{p^{\nu - m_\nu}}$$

zu lösen hat. Die Folge $\{s_\nu\}$ hat dann denselben p-adischen Limes wie $\{r_\nu\}$.

Entwickelt man die Zahlen s_ν nach aufsteigenden Potenzen von p mit Koeffizienten von 0 bis $p - 1$ und versteht man für festes ganzzahliges n unter s'_ν den Anfang der Entwicklung, abgebrochen bei den Gliedern mit p^n, so daß also

$$s'_\nu \equiv s_\nu \pmod{p^{n+1}}$$

ist, so ist leicht zu sehen, daß fast alle s_ν (d. h. alle bis auf endlichviele) denselben Anfang s'_ν haben. Diesen gemeinsamen Anfang nennen wir t_n und setzen

$$t_n = \sum_{\lambda=-m}^{n} a_\lambda p^\lambda.$$

Jedes t_n stellt zugleich den Anfang von $t_{n+1}, t_{n+2}, \ldots$ dar. Die Folge $\{t_1, t_2, \ldots\}$ hat nun wieder denselben p-adischen Limes wie $\{s_1, s_2, \ldots\}$; für diesen Limes können wir also schreiben

$$\lim t_n = \sum_{\lambda=-m}^{\infty} a_\lambda p^\lambda.$$

So lassen sich alle p-adischen Zahlen (eindeutig) als Potenzreihen nach aufsteigenden Potenzen von p schreiben, und umgekehrt stellt jede solche Potenzreihe, da sie in Ω_p automatisch konvergiert, eine p-adische Zahl dar.

Aufgaben. 1. Man führe die Beweise ausführlich durch.

2. Man schreibe -1 und $\frac{1}{2}$ als 3-adische Potenzreihen.

3. Eine Gleichung $f(x) = 0$, wo f ein ganzzahliges Polynom ist, ist im Körper Ω_p dann und nur dann lösbar, wenn die Kongruenz

$$f(x) \equiv 0 \pmod{p^n}$$

für jede natürliche Zahl n eine rationale Lösung besitzt.

4. Sind die Gleichungen

$$x^2 = -1,$$
$$x^2 = 3,$$
$$x^2 = 7$$

im Körper Ω_3 lösbar?

Literatur zu den p-adischen Zahlen.

Hensel, K.: Math. Z. Bd. 2, S. 433. 1918.
Kürschak, J.: J. Math. Bd. 142, S. 211—253. 1912.
Ostrowski, A.: Acta Mathematica Bd. 41, S. 271—284. 1918.

§ 66. Nullstellen reeller Funktionen.

Es sei P der Körper der reellen Zahlen. Wir betrachten nun reellwertige Funktionen $f(x)$ der reellen Veränderlichen x. Eine solche Funktion heißt *stetig* für $x = a$, wenn es zu jedem $\varepsilon > 0$ ein $\delta > 0$ gibt, so daß

$$|f(a+h) - f(a)| < \varepsilon \qquad \text{für} \quad |h| < \delta.$$

Man beweist leicht, daß Summen und Produkte stetiger Funktionen wieder stetige Funktionen sind (vgl. den entsprechenden Nachweis für Fundamentalfolgen in § 64). Da die Konstanten und die Funktion $f(x) = x$ überall stetige Funktionen sind, so stellen alle Polynome in x überall stetige Funktionen von x dar.

Der *Weierstraßsche Nullstellensatz für stetige Funktionen* lautet:

Eine für $a \leqq x \leqq b$ stetige Funktion $f(x)$, für die $f(a) < 0$ und $f(b) > 0$ ist, hat zwischen a und b eine Nullstelle.

Beweis. Es sei c die obere Grenze aller x zwischen a und b, für die $f(x) < 0$ ist. Dann gibt es drei Möglichkeiten:

1. $f(c) > 0$. Dann ist zunächst $c > a$ und es gibt ein $\delta > 0$, so daß für $0 < h < \delta$

$$|f(c-h) - f(c)| < f(c),$$
$$f(c) - f(c-h) < f(c),$$
$$f(c-h) > 0,$$
$$f(x) > 0 \qquad (c - \delta < x \leqq c).$$

Also ist $c - \delta$ eine obere Schranke für die x mit $f(x) < 0$. Aber c war die kleinste obere Schranke. Der Fall ist also unmöglich.

2. $f(c) < 0$. Dann ist $c < b$ und es gibt ein $\delta > 0$, so daß für $0 < h < \delta$, z. B für $h = \frac{1}{2}\delta$,

$$f(c+h) - f(c) < -f(c),$$
$$f(c+h) < 0.$$

Daher ist c keine obere Schranke aller x mit $f(x) < 0$. Dieser Fall ist also ebenfalls unmöglich.

3. $f(c) = 0$ ist der einzig übrigbleibende Fall. Also hat $f(x)$ die Nullstelle c.

Der Weierstraßsche Nullstellensatz für Polynome ist das Fundament aller Sätze über die reellen Wurzeln algebraischer Gleichungen. Wir werden ihn später auf andere Körper als den der reellen Zahlen, nämlich auf die sogenannten „reell-abgeschlossenen Körper" ausdehnen. Alle weiteren Sätze dieses Paragraphen beruhen ausschließlich auf dem Weierstraßschen Nullstellensatz für Polynome und gelten dementsprechend auch für die späteren allgemeineren Körper.

Folgerungen. 1. *Das Polynom $x^n - d$ hat für $d > 0$ und jedes natürliche n immer eine, sogar eine positive Nullstelle.*

Denn für $x = 0$ ist $x^n - d < 0$, und für große x $\left(\text{z. B. } x > 1 + \frac{d}{n}\right)$ ist $x^n - d > 0$.

Aus $a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \cdots + b^{n-1})$ folgt weiter, daß für $a > b > 0$ auch $a^n > b^n$ ist, mithin kann es auch nur eine positive Wurzel der Gleichung $x^n = d$ geben. Diese wird mit $\sqrt[n]{d}$, für $n = 2$ kurz mit $\sqrt{d}$ („Quadratwurzel") bezeichnet. Ferner setzt man $\sqrt[n]{0} = 0$. Aus $a > b \geqq 0$ folgt nunmehr $\sqrt[n]{a} > \sqrt[n]{b}$, denn wenn $\sqrt[n]{a} \leqq \sqrt[n]{b}$ wäre, so würde $a \leqq b$ folgen.

2. *Jedes Polynom ungeraden Grades hat in* P *eine Nullstelle.*

Denn nach Aufg. 2, § 63, gibt es ein M so, daß $f(\mathsf{M}) > 0$ und $f(-\mathsf{M}) < 0$ ist.

Adjungiert man zum Körper der reellen Zahlen P eine Wurzel i des in P irreduziblen Polynoms $x^2 + 1$, so erhält man den *Körper der komplexen Zahlen* $\Omega = \mathsf{P}(i)$.

Wenn von „Zahlen" die Rede ist, sind im folgenden immer komplexe (und insbesondere reelle) Zahlen gemeint. *Algebraische Zahlen* sind solche

Zahlen, die in bezug auf den rationalen Zahlkörper Γ algebraisch sind. Es ist nun klar, was man unter algebraischen Zahlkörpern, reellen Zahlkörpern usw. zu verstehen hat. Die algebraischen Zahlen bilden den Sätzen von § 29 zufolge einen Körper A; in ihm sind alle algebraischen Zahlkörper enthalten.

Wir beweisen nun:

Im Körper der komplexen Zahlen ist die Gleichung $x^2 = a + bi$ (a, b *reell*) *stets lösbar; d. h. jede Zahl des Körpers besitzt im Körper eine „Quadratwurzel".*

Beweis. Eine Zahl $x = c + di$ (c, d reell) hat dann und nur dann die verlangte Eigenschaft, wenn

$$(c + di)^2 = a + bi$$

ist, d. h. wenn die Bedingungen

$$c^2 - d^2 = a, \qquad 2cd = b$$

erfüllt sind. Aus diesen Gleichungen folgt weiter: $(c^2 + d^2)^2 = a^2 + b^2$, also $c^2 + d^2 = \sqrt{a^2 + b^2}$. Daraus und aus der ersten Bedingung bestimmt man c^2 und d^2:

$$c^2 = \frac{a + \sqrt{a^2 + b^2}}{2},$$

$$d^2 = \frac{-a + \sqrt{a^2 + b^2}}{2}.$$

Die rechts stehenden Größen sind tatsächlich $\geqq 0$. Also kann man aus ihnen c und d bis auf die Vorzeichen bestimmen. Multiplikation ergibt

$$4c^2d^2 = -a^2 + (a^2 + b^2) = b^2;$$

mithin kann man die Vorzeichen von c und d auch so bestimmen, daß die letzte Bedingung

$$2cd = b$$

erfüllt ist.

Aus dem Bewiesenen folgt, daß man im Körper der komplexen Zahlen jede quadratische Gleichung

$$x^2 + px + q = 0$$

lösen kann, indem man sie auf die Form

$$\left(x + \frac{p}{2}\right)^2 = \frac{p^2}{4} - q$$

bringt. Die Lösung lautet also

$$x = -\frac{p}{2} \pm w,$$

wenn w irgend eine Lösung der Gleichung $w^2 = \frac{p^2}{4} - q$ bedeutet. Daß man im Körper Ω nicht nur quadratische, sondern beliebige Gleichungen

lösen kann, mit anderen Worten, daß Ω algebraisch-abgeschlossen ist, wird sich im § 67 zeigen.

Wir wenden uns nun zur *Berechnung der reellen Wurzeln eines Polynoms* $f(x)$. Unter Berechnung ist, entsprechend der Definition der reellen Zahlen, beliebig genaue Approximation durch rationale Zahlen zu verstehen.

Wir haben in § 63 (Aufg. 2) schon gesehen, wie man die reellen Wurzeln von $f(x)$ in Schranken einschließen kann: Ist

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$$

und ist M die größte der Zahlen 1 und $|a_1| + \cdots + |a_n|$, so liegen alle Wurzeln zwischen $-\mathsf{M}$ und $+\mathsf{M}$. (Der Wert von $f(x)$ ist >0 für $x > \mathsf{M}$ und hat das Vorzeichen von $(-1)^n$ für $x < -\mathsf{M}$.) Man kann M durch eine (eventuell größere) rationale Zahl ersetzen, diese wieder M nennen und dann das Intervall $-\mathsf{M} \leqq x \leqq \mathsf{M}$ durch rationale Zwischenpunkte in beliebig kleine Teile zerlegen. In welchen dieser Teile die Wurzeln liegen, kann man feststellen, sobald man ein Mittel hat, zu entscheiden, wie viele Wurzeln zwischen zwei gegebenen Grenzen liegen. Durch weitere Unterteilung der Intervalle, in denen Wurzeln liegen, kann man dann die reellen Wurzeln beliebig genau approximieren.

Das Mittel, zu entscheiden, wie viele Wurzeln zwischen zwei gegebenen Grenzen liegen oder auch wie viele Wurzeln es überhaupt gibt, liefert das

Theorem von STURM. *Man bestimme die Polynome* $X_1, X_2, \ldots, X_r$, *von einem gegebenen Polynom* $X = f(x)$ *ausgehend, folgendermaßen*:

$$(1)\qquad \begin{aligned} &X_1 = f'(x) && \text{(Differentiation)},\\ &\left.\begin{aligned} X &= Q_1 X_1 - X_2,\\ X_1 &= Q_2 X_2 - X_3,\\ &\cdots\cdots\cdots\\ X_{r-1} &= Q_r X_r \end{aligned}\right\} && \text{(euklidischer Algorithmus)}. \end{aligned}$$

Für jede reelle Zahl a, *die keine Nullstelle von* $f(x)$ *ist, sei* $w(a)$ *die Anzahl der Vorzeichenwechsel*[1] *in der Zahlenfolge*

$$X(a),\ X_1(a),\ \ldots,\ X_r(a),$$

in der man alle Nullen weggelassen hat. Sind dann b *und* c *irgendwelche Zahlen mit* $b < c$, *für die* $f(x)$ *nicht verschwindet, so hat die Anzahl der verschiedenen Nullstellen im Intervall* $b \leqq x \leqq c$ (*mehrfache Nullstellen nur einmal gezählt*!) *den Wert*

$$w(b) - w(c).$$

[1] Unter dem *Vorzeichen* einer Zahl c verstehen wir das Symbol $+$, $-$ oder 0, je nachdem c positiv, negativ oder Null ist. Ein *Wechsel* in einer nur die Zeichen $+$ und $-$ in beliebiger Anzahl aufweisenden Vorzeichenfolge liegt vor, sobald einem $+$ ein $-$ oder einem $-$ ein $+$ folgt. Sind auch Nullen vorhanden, so hat man diese bei der Zählung der Wechsel einfach wegzulassen.

Die Reihe der Polynome $X, X_1, \ldots, X_r$ heißt die *Sturmsche Kette* von $f(x)$. Das Theorem besagt also, daß die Anzahl der Nullstellen zwischen b und c gegeben wird durch die Anzahl der Vorzeichenwechsel, die beim Übergang von b nach c verloren gehen.

Beweis. Das letzte Polynom X_r der Kette ist offenbar der G. G. T. von $X = f(x)$ und $X_1 = f'(x)$. Denkt man sich alle Polynome der Kette durch $c \cdot X_r$ dividiert, wo c eine Konstante ist, so hat man $f(x)$ von mehrfachen Linearfaktoren befreit, ohne die Anzahl der Vorzeichenwechsel an einer Nichtnullstelle a zu beeinflussen; denn die Vorzeichen der Kettenglieder sind bei der Division entweder alle ungeändert geblieben oder alle umgekehrt worden. Wir können also beim Beweis diese Division vorher ausgeführt denken; das letzte Glied der Kette ist dann eine von Null verschiedene Konstante. Das zweite Glied der Kette wird nun im allgemeinen nicht mehr die Ableitung des ersten sein; vielmehr führt, wenn etwa d eine l-fache Nullstelle von $f(x)$, also etwa

$$X = f(x) = (x - d)^l g(x), \qquad g(d) \neq 0,$$
$$X_1 = f'(x) = l(x - d)^{l-1} g(x) + (x - d)^l g'(x)$$

ist, die Weghebung des Faktors $(x - d)^{l-1}$ auf zwei Polynome von der Gestalt

$$\overline{X} = (x - d) g(x),$$
$$\overline{X}_1 = l \cdot g(x) + (x - d) g'(x),$$

aus denen für die anderen Nullstellen $d', d'', \ldots$ noch weitere Faktoren herauszuheben sind. Wir bezeichnen die so modifizierten Polynome der Sturmschen Kette wieder mit $X = X_0, X_1, \ldots, X_r$.

Unter dieser Annahme werden an keiner Stelle a zwei aufeinanderfolgende Glieder der Kette gleich Null. Denn wären etwa $X_k(a)$ und $X_{k+1}(a)$ gleichzeitig Null, so würde man aus den Gleichungen (1) schließen, daß auch $X_{k+2}(a), \ldots, X_r(a)$ gleich Null wären, während doch $X_r = \text{konst.} \neq 0$ ist.

Die Nullstellen der Polynome der Sturmschen Kette teilen das Intervall $b \leqq x \leqq c$ in Teilintervalle. Innerhalb eines solchen Teilintervalls wird weder X noch irgend ein X_k Null, und daraus folgt nach dem Weierstraßschen Nullstellensatz, daß im Innern eines solchen Intervalls alle Polynome der Sturmschen Kette ihre Vorzeichen beibehalten, mithin die Zahl $w(a)$ konstant bleibt. Wir haben also nur noch zu untersuchen, wie sich die Zahl $w(a)$ an einer Stelle d ändert, an der ein Polynom der Kette verschwindet.

Es sei zunächst d eine Nullstelle von X_k $(0 < k < r)$. Auf Grund der Gleichung

$$X_{k-1} = Q_k X_k - X_{k+1}$$

haben die Zahlen $X_{k-1}(d)$ und $X_{k+1}(d)$ notwendig entgegengesetzte Vorzeichen. Auch in den beiden angrenzenden Teilintervallen haben

also X_{k-1} und X_{k+1} entgegengesetzte Vorzeichen. Welches Vorzeichen nun X_k hat (+, − oder 0), ist für die Anzahl der Vorzeichenwechsel zwischen X_{k-1} und X_{k+1} ganz gleichgültig: es gibt immer genau einen Wechsel. Also ändert die Zahl $w(a)$ sich beim Durchgang durch die Stelle d überhaupt nicht.

Sodann sei d eine Nullstelle von $f(x)$, also nach der zu Anfang gemachten Bemerkung etwa

$$X = (x-d)\,g(x), \qquad g(d) \neq 0,$$
$$X_1 = l \cdot g(x) + (x-d)\,g'(x),$$

wo l eine natürliche Zahl ist. Das Vorzeichen von X_1 an der Stelle d und daher auch in den beiden angrenzenden Intervallen ist gleich dem von $g(d)$, während das von X an jeder einzelnen Stelle gleich dem von $(x-d)\,g(d)$ ist. Also hat man für $a < d$ einen Vorzeichenwechsel zwischen $X(a)$ und $X_1(a)$, dagegen für $a > d$ keinen Wechsel mehr. Alle etwaigen übrigen Wechsel in der Sturmschen Kette bleiben, wie schon gezeigt, beim Durchgang durch die Stelle d erhalten. Also nimmt die Zahl $w(a)$ beim Durchgang durch die Stelle d um Eins ab. Damit ist das Sturmsche Theorem bewiesen.

Will man das Sturmsche Theorem dazu benutzen, die Gesamtzahl der verschiedenen reellen Nullstellen von $f(x)$ zu bestimmen, so hat man für die Schranke b einen so kleinen und für die Schranke c einen so großen Wert zu nehmen, daß es für $x < b$ und für $x > c$ keine Nullstelle mehr gibt. Es genügt z. B., $b = -\mathsf{M}$ und $c = \mathsf{M}$ zu wählen. Noch bequemer ist es aber, b und c so zu wählen, daß alle Polynome der Sturmschen Kette für $x < b$ und $x > c$ keine Nullstellen mehr haben. Ihre Vorzeichen werden dann durch die Vorzeichen ihrer Anfangskoeffizienten bestimmt: $a_0 x^m + a_1 x^{m-1} + \cdots$ hat für sehr große x das Vorzeichen von a_0 und für sehr kleine (negative) x das von $(-1)^m a_0$. Um die Frage, wie groß b und c sein müssen, braucht man sich bei dieser Methode nicht zu kümmern: man braucht nur die Anfangskoeffizienten a_0 und Grade m der Sturmschen Polynome zu berechnen.

Aufgaben. 1. Man bestimme die Anzahl der reellen Nullstellen des Polynoms

$$x^3 - 5x^2 + 8x - 8.$$

Zwischen welchen aufeinanderfolgenden ganzen Zahlen liegen diese Nullstellen?

2. Sind die letzten beiden Polynome X_{r-1}, X_r der Sturmschen Kette vom Grade 1, 0, so kann man die Konstante X_r (oder deren Vorzeichen, auf das es allein ankommt) auch berechnen, indem man die Nullstelle von X_{r-1} in $-X_{r-2}$ einsetzt.

3. Ist man bei der Berechnung der Sturmschen Kette auf ein X_k gestoßen, welches nirgends sein Vorzeichen wechselt (etwa eine Summe

von Quadraten), so kann man die Kette mit diesem X_k abbrechen. Ebenso kann man stets aus einem X_k einen überall positiven Faktor weglassen und mit dem in dieser Weise modifizierten X_k die Rechnung fortsetzen.

4. Das beim Beweis des Sturmschen Satzes benutzte Polynom X_1 (ein Teiler von $f'(x)$) wechselt zwischen zwei aufeinanderfolgenden Nullstellen von $f(x)$ sicher sein Vorzeichen. Beweis? Daher hat $f'(x)$ zwischen je zwei Nullstellen von $f(x)$ mindestens eine Nullstelle (*Satz von* ROLLE).

5. Aus dem Satz von ROLLE ist der *Mittelwertsatz der Differentialrechnung* herzuleiten, der besagt, daß für $a < b$

$$\frac{f(b)-f(a)}{b-a} = f'(c)$$

ist für ein passendes c mit $a < c < b$. [Man setze

$$f(x) - f(a) - \frac{f(b)-f(a)}{b-a}(x-a) = \varphi(x).]$$

6. In einem Intervall $a \leqq x \leqq b$, wo $f'(x) > 0$ ist, ist $f(x)$ eine zunehmende Funktion von x; ebenso, wenn $f'(x) < 0$ ist, eine abnehmende.

7. Ein Polynom $f(x)$ hat in jedem Intervall $a \leqq x \leqq b$ einen größten und einen kleinsten Wert, und zwar wird er entweder in einer Nullstelle von $f'(x)$ oder in einem der Endpunkte a oder b angenommen.

§ 67. Algebraische Theorie der reellen Körper.

Die angeordneten Körper, insbesondere die reellen Zahlkörper, haben die Eigenschaft, daß in ihnen eine Summe von Quadraten nur dann verschwindet, wenn die einzelnen Summanden verschwinden. Oder, was damit gleichbedeutend ist: -1 ist nicht als Quadratsumme darstellbar[1]. Der Körper der komplexen Zahlen hat diese Eigenschaft nicht; denn in ihm ist -1 sogar ein Quadrat. Es wird sich nun zeigen, daß diese Eigenschaft für die reellen algebraischen Zahlkörper und ihre konjugierten Körper (im Körper aller algebraischen Zahlen) charakteristisch ist und auch zu einer algebraischen Konstruktion des Körpers der reellen algebraischen Zahlen samt den konjugierten Körpern verwendet werden kann. Wir definieren[2]:

Ein Körper heißt formal-reell, wenn in ihm -1 nicht als Quadratsumme darstellbar ist.

---

[1] Ist in irgend einem Körper das Element -1 als Summe Σa_ν^2 darstellbar, so ist $1^2 + \Sigma a_\nu^2 = 0$; somit ist 0 eine Summe von Quadraten mit nicht sämtlich verschwindenden Basen. Ist umgekehrt eine Summe $\Sigma b_\nu^2 = 0$ gegeben, wo ein $b_\lambda \neq 0$ ist, so kann man dieses b_λ leicht zu Eins machen, indem man die Summe durch b_λ^2 dividiert; schafft man die Eins auf die andere Seite, so erhält man $-1 = \Sigma a_\nu^2$.

[2] Vgl. E. ARTIN und O. SCHREIER: Algebraische Konstruktion reeller Körper. Abh. Math. Sem. Hamburg, Bd. 5, S. 83—115. 1926.

Ein formal-reeller Körper hat stets die Charakteristik Null; denn in einem Körper der Charakteristik p ist -1 Summe von $p-1$ Summanden 1^2. — Ein Unterkörper eines formal-reellen Körpers ist offenbar wieder formal-reell.

Ein Körper P *heißt reell-abgeschlossen*[1]*, wenn zwar* P *formal-reell, dagegen keine echte algebraische Erweiterung von* P *formal-reell ist.*

Satz 1. *Jeder reell-abgeschlossene Körper kann auf eine und nur eine Weise angeordnet werden.*

Sei P reell-abgeschlossen. Dann wollen wir zeigen:

Ist a ein von 0 verschiedenes Element aus P, so ist a entweder selbst Quadrat, oder es ist $-a$ Quadrat, und diese Fälle schließen einander aus. Quadratsummen von Elementen aus P sind selbst Quadrate.

Hieraus wird Satz 1 unmittelbar folgen; denn durch die Festsetzung $a > 0$, wenn a Quadrat und von 0 verschieden ist, wird dann offenbar eine Anordnung des Körpers P definiert sein, und sie ist die einzig mögliche, da ja Quadrate in jeder Anordnung $\geqq 0$ ausfallen müssen.

Ist γ nicht Quadrat eines Elements aus P, so ist, wenn $\sqrt{\gamma}$ eine Wurzel des Polynoms $x^2 - \gamma$ bedeutet, $\mathsf{P}(\sqrt{\gamma})$ eine echte algebraische Erweiterung von P, also nicht formal-reell. Demnach gilt eine Gleichung

$$-1 = \sum_{\nu=1}^{n} (\alpha_\nu \sqrt{\gamma} + \beta_\nu)^2$$

oder

$$-1 = \gamma \sum_{\nu=1}^{n} \alpha_\nu^2 + \sum_{\nu=1}^{n} \beta_\nu^2 + 2\sqrt{\gamma} \sum_{\nu=1}^{n} \alpha_\nu \beta_\nu ,$$

wobei die α_ν, β_ν zu P gehören. Hierin muß der letzte Term verschwinden, da sonst $\sqrt{\gamma}$ entgegen der Annahme in P läge. Dagegen kann das erste Glied nicht verschwinden, da andernfalls P nicht formal-reell wäre. Daraus schließen wir zunächst, daß γ in P nicht als Quadratsumme darstellbar ist; denn sonst erhielten wir auch für -1 eine Darstellung als Quadratsumme. D. h.: Ist γ nicht Quadrat, so ist es auch nicht Quadratsumme. Oder positiv gewendet: Jede Quadratsumme in P ist auch Quadrat in P.

Nunmehr erhalten wir

$$-\gamma = \frac{1 + \sum_{\nu=1}^{n} \beta_\nu^2}{\sum_{\nu=1}^{n} \alpha_\nu^2} .$$

Zähler und Nenner dieses Ausdrucks sind Quadratsummen, also selbst Quadrate; daher ist $-\gamma = c^2$, wo c in P liegt. Demnach gilt für jedes Element γ aus P mindestens eine der Gleichungen $\gamma = b^2$,

[1] Man hat die kurze Bezeichnung „reell-abgeschlossen" der präziseren „reell-algebraisch abgeschlossen" vorgezogen.

$-\gamma = c^2$; ist aber $\gamma \neq 0$, so können nicht beide bestehen, da sonst $-1 = \left(\frac{b}{c}\right)^2$ wäre, was nicht geht.

Auf Grund von Satz 1 nehmen wir im folgenden reell-abgeschlossene Körper stets als angeordnet an.

Satz 2. *In einem reell-abgeschlossenen Körper besitzt jedes Polynom ungeraden Grades mindestens eine Nullstelle.*

Der Satz ist für den Grad 1 trivial. Wir nehmen an, er sei bereits für alle ungeraden Grade $< n$ bewiesen; $f(x)$ sei ein Polynom des ungeraden Grades n (> 1). Ist $f(x)$ reduzibel in dem reell-abgeschlossenen Körper P, so besitzt mindestens ein irreduzibler Faktor einen ungeraden Grad $< n$, also auch eine Nullstelle in P. Die Annahme, $f(x)$ wäre irreduzibel, soll jetzt ad absurdum geführt werden. Es sei nämlich α eine symbolisch adjungierte Nullstelle von $f(x)$. $\mathsf{P}(\alpha)$ wäre dann nicht formal-reell; also hätten wir eine Gleichung

$$-1 = \sum_{\nu=1}^{r} (\varphi_\nu(\alpha))^2, \tag{1}$$

wobei die $\varphi_\nu(x)$ Polynome höchstens $(n-1)$-ten Grades mit Koeffizienten aus P sind. Aus (1) erhalten wir eine Identität

$$-1 = \sum_{\nu=1}^{r} (\varphi_\nu(x))^2 + f(x)\, g(x)\,. \tag{2}$$

Die Summe der φ_ν^2 hat geraden Grad, da die höchsten Koeffizienten Quadrate sind und sich also beim Addieren nicht wegheben können. Ferner ist der Grad positiv, da sonst schon (1) einen Widerspruch enthielte. Demnach hat $g(x)$ einen ungeraden Grad $\leqq n-2$; also besitzt $g(x)$ jedenfalls eine Nullstelle a in P. Setzen wir aber a in (2) ein, so haben wir

$$-1 = \sum_{\nu=1}^{r} (\varphi_\nu(a))^2,$$

womit wir bei einem Widerspruch angelangt sind, da die $\varphi_\nu(a)$ in P liegen.

Satz 3. *Ein reell-abgeschlossener Körper ist nicht algebraisch-abgeschlossen. Dagegen ist der durch Adjunktion von i[1] entstehende Körper algebraisch-abgeschlossen.*

Die erste Hälfte ist trivial. Denn die Gleichung $x^2 + 1 = 0$ ist in jedem formal-reellen Körper unlösbar.

Die zweite Hälfte folgt unmittelbar aus

Satz 3a. *Besitzt in einem angeordneten Körper K jedes positive Element eine Quadratwurzel und jedes Polynom ungeraden Grades mindestens eine Nullstelle, so ist der durch Adjunktion von i entstehende Körper algebraisch-abgeschlossen.*

[1] i bedeutet hier und im folgenden stets eine Nullstelle von $x^2 + 1$.

Zunächst bemerken wir, daß in $\mathsf{K}(i)$ jedes Element eine Quadratwurzel besitzt und daher jede quadratische Gleichung lösbar ist. Der Beweis geschieht durch dieselbe Rechnung wie für den Körper der komplexen Zahlen im § 66.

Zum Nachweis der algebraischen Abgeschlossenheit von $\mathsf{K}(i)$ genügt es nach § 60, zu zeigen, daß jedes in K irreduzible Polynom $f(x)$ in $\mathsf{K}(i)$ eine Nullstelle besitzt. $f(x)$ sei ein doppelwurzelfreies Polynom n-ten Grades, wo $n = 2^m q$, q ungerade. Wir wollen Induktion nach m anwenden, also annehmen, daß jedes doppelwurzelfreie Polynom mit Koeffizienten aus K, dessen Grad durch 2^{m-1}, aber nicht durch 2^m teilbar ist, in $\mathsf{K}(i)$ eine Wurzel besitzt. (Dies trifft für $m = 1$ nach Voraussetzung zu.) $\alpha_1, \alpha_2, \ldots, \alpha_n$ seien die Wurzeln von $f(x)$ in einer Erweiterung von K. Wir wählen c aus K so, daß die $\frac{n(n-1)}{2}$ Ausdrücke $\alpha_j\alpha_k + c(\alpha_j + \alpha_k)$ für $1 \leqq j < k \leqq n$ lauter verschiedene Werte haben[1]. Da diese Ausdrücke ersichtlich einer Gleichung vom Grade $\frac{n(n-1)}{2}$ in K genügen, so liegt nach Annahme mindestens einer von ihnen in $\mathsf{K}(i)$, etwa $\alpha_1\alpha_2 + c(\alpha_1 + \alpha_2)$. Zufolge der Bedingung, der c unterworfen war, ist aber (vgl. § 34)

$$\mathsf{K}(\alpha_1\alpha_2,\ \alpha_1 + \alpha_2) = \mathsf{K}(\alpha_1\alpha_2 + c(\alpha_1 + \alpha_2));$$

also finden wir α_1 und α_2 durch Auflösung einer quadratischen Gleichung in $\mathsf{K}(i)$.

Aus Satz 3a folgt gleichzeitig (in Verbindung mit § 66), daß der Körper der komplexen Zahlen algebraisch-abgeschlossen ist. Das ist der sogenannte „Fundamentalsatz der Algebra“[2].

Eine Umkehrung von Satz 3 lautet:

Satz 4. *Wenn ein formal-reeller Körper* K *durch Adjunktion von* i *algebraisch abgeschlossen werden kann, so ist er reell-abgeschlossen.*

Beweis. Es gibt keinen Zwischenkörper zwischen K und $\mathsf{K}(i)$, also keine algebraische Erweiterung von K außer K selbst und $\mathsf{K}(i)$. $\mathsf{K}(i)$ ist nicht formal-reell, da -1 in ihm ein Quadrat ist. Also ist K reell-abgeschlossen.

---

[1] Dies ist möglich, weil $f(x)$ doppelwurzelfrei sein sollte.

[2] Der Satz wird so genannt, weil er in der früheren Algebra den einzigen Existenzbeweis bildete, der allen Betrachtungen über die Wurzeln einer algebraischen Gleichung zugrunde liegt. Gausz hat für den Satz fünf Beweise gegeben; der oben dargestellte ist im wesentlichen der zweite Gaußsche Beweis. Andere Beweise finden sich bei Cauchy: Cours d'analyse, S. 329 (siehe auch Weber-Fricke: Algebra I); Weyl: Math. Zeitschr. 20 (1914) S. 142.

In der modernen Algebra hat der Satz seine fundamentale Bedeutung verloren, weil man von der Existenz der Wurzeln in einem anderen, mehr symbolischen Sinn: im Sinne der Steinitzschen Konstruktion (§ 27 und § 29), zu reden gelernt hat und daher auch, ohne auf komplexe Zahlen Bezug zu nehmen, von den Eigenschaften der Wurzeln einer Gleichung reden kann.

Aus Satz 4 folgt insbesondere, daß der Körper der reellen Zahlen reell-abgeschlossen ist.

Die Wurzeln einer Gleichung $f(x) = 0$ mit Koeffizienten aus einem reell-abgeschlossenen Körper K liegen in $\mathsf{K}(i)$ und kommen daher, soweit sie nicht in K enthalten sind, immer als Paare konjugierter Wurzeln (in bezug auf K) vor. Ist $a + bi$ eine Wurzel, so ist $a - bi$ die konjugierte. Faßt man in der Zerlegung von $f(x)$ immer die Paare konjugierter Linearfaktoren zusammen, so ergibt sich eine Zerlegung von $f(x)$ in lineare und quadratische, in K irreduzible Faktoren.

Wir sind jetzt imstande, den „Weierstraßschen Nullstellensatz" für Polynome (§ 66) auf beliebige reell-abgeschlossene Körper auszudehnen.

Satz 5. *Es sei $f(x)$ ein Polynom mit Koeffizienten aus einem reell-abgeschlossenen Körper P und a, b Elemente aus P, für die $f(a) < 0$, $f(b) > 0$. Dann gibt es mindestens ein Element c in P zwischen a und b, für das $f(c) = 0$.*

Beweis. Wie wir eben sahen, zerfällt $f(x)$ in P in lineare und in irreduzible quadratische Faktoren. Ein irreduzibles quadratisches Polynom $x^2 + px + q$ ist in P beständig positiv; denn es kann in der Form $\left(x + \frac{p}{2}\right)^2 + \left(q - \frac{p^2}{4}\right)$ geschrieben werden, und hierin ist der erste Term stets $\geqq 0$ und der zweite wegen der vorausgesetzten Irreduzibilität positiv. Daher kann ein Vorzeichenwechsel von $f(x)$ nur durch Vorzeichenwechsel eines Linearfaktors, also durch eine Nullstelle zwischen a und b bewirkt werden.

Auf Grund dieses Satzes gelten für reell-abgeschlossene Körper auch alle Folgerungen, die in § 66 aus dem Weierstraßschen Nullstellensatz gezogen wurden, insbesondere das Theorem von STURM über die reellen Nullstellen.

Wir beweisen zum Schluß den

Satz 6. *Sei K ein angeordneter Körper, $\overline{\mathsf{K}}$ der Körper, der aus K durch Adjunktion der Quadratwurzeln aus allen positiven Elementen von K hervorgeht. Dann ist $\overline{\mathsf{K}}$ formal-reell.*

Es genügt offenbar, zu zeigen, daß keine Gleichung der Form

$$-1 = \sum_{\nu=1}^{n} c_\nu \xi_\nu^2 \tag{3}$$

besteht, wo die c_ν positive Elemente aus K, die ξ_ν aber Elemente aus $\overline{\mathsf{K}}$ sind. Angenommen, es gäbe eine solche Gleichung. In den ξ_ν könnten natürlich nur endlichviele der zu K adjungierten Quadratwurzeln wirklich auftreten, etwa $\sqrt{a_1}$, $\sqrt{a_2}$, ..., $\sqrt{a_r}$. Wir denken uns unter allen Gleichungen (3) eine solche gewählt, für die r möglichst klein ausfällt. (Sicher ist $r \geqq 1$, da in K keine Gleichung der Form (3) existiert.) ξ_ν läßt sich in der Gestalt $\xi_\nu = \eta_\nu + \zeta_\nu \sqrt{a_r}$ darstellen, wo η_ν, ζ_ν

in $\mathsf{K}(\sqrt{a_1}, \sqrt{a_2}, \ldots, \sqrt{a_{r-1}})$ liegen. Also hätten wir

$$(4) \qquad -1 = \sum_{\nu=1}^{n} c_\nu \eta_\nu^2 + \sum_{\nu=1}^{n} c_\nu a_r \zeta_\nu^2 + 2\sqrt{a_r} \sum_{\nu=1}^{n} c_\nu \eta_\nu \zeta_\nu .$$

Verschwindet in (4) der letzte Summand, so ist (4) eine Gleichung derselben Gestalt wie (3), enthält aber weniger als r Quadratwurzeln. Verschwindet er aber nicht, so läge $\sqrt{a_r}$ in $\mathsf{K}(\sqrt{a_1}, \ldots, \sqrt{a_{r-1}})$, und (3) könnte mit weniger als r Quadratwurzeln geschrieben werden. Unsere Annahme führt daher auf jeden Fall zu einem Widerspruch.

Aufgaben. 1. Der Körper der algebraischen Zahlen ist algebraisch-abgeschlossen, und der Körper der reellen algebraischen Zahlen ist reell-abgeschlossen.

2. Der nach § 60 rein algebraisch konstruierbare algebraisch-abgeschlossene algebraische Erweiterungskörper zum Körper Γ ist isomorph dem Körper A der algebraischen Zahlen.

3. Es sei P ein reeller Zahlkörper, Σ der Körper der reellen in bezug auf P algebraischen Zahlen. Dann ist Σ reell-abgeschlossen.

4. Ist P formal-reell und t transzendent in bezug auf P, so ist auch $\mathsf{P}(t)$ formal-reell. [Ist $-1 = \Sigma \varphi_\nu(t)^2$, so setze man für t eine passende gewählte Konstante aus P ein.]

§ 68. Existenzsätze für formal-reelle Körper.

Satz 7. *Es sei* K *ein formal-reeller Körper,* Ω *ein algebraisch-abgeschlossener Körper über* K. *Dann gibt es (mindestens) einen reell-abgeschlossenen Körper* P *zwischen* K *und* Ω, *für den* $\Omega = \mathsf{P}(i)$ *ist.*

Beweis. Wir können Ω als wohlgeordnet voraussetzen (§ 58). Diese Wohlordnung ist von den Anordnungen der vorigen Paragraphen wohl zu unterscheiden (Ω gestattet ja bestimmt keine Anordnung, da -1 in ihm ein Quadrat ist); wir schreiben daher jetzt $a \lessdot b$, wenn a in der Wohlordnung vor b kommt.

Wir ordnen jedem Element a von Ω zwei Unterkörper P_a, Σ_a von Ω zu, die durch folgende rekursiven Bestimmungsrelationen eindeutig bestimmt sind:

1. P_a ist die Vereinigung von K und allen Σ_b mit $b \lessdot a$.
2. $\Sigma_a = \mathsf{P}_a(a)$, wenn $\mathsf{P}_a(a)$ formal-reell ist, sonst $\Sigma_a = \mathsf{P}_a$.

Wir definieren schließlich P als die Vereinigung aller Σ_a.

Wir wollen nun beweisen, daß alle P_a sowie P formal-reell sind. Wir nehmen an, dieses sei für alle P_b mit $b \lessdot a$ (bzw., wenn es sich um P handelt, für alle P_b) schon erfüllt. Wir bemerken: Wenn P_b formal-reell ist, so ist Σ_b es auch (Definition von Σ_b). Sind aber K und alle Σ_b mit $b \lessdot a$ formal-reell, so ist ihre Vereinigung P_a es auch, denn wenn in P eine Darstellung $-1 = \Sigma a_\nu^2$ existiert, so gehören die a_ν alle schon einem einzigen Σ_b an. Durch transfinite Induktion folgt

also, daß alle P_b formal-reell sind, und daraus weiter, daß auch P formal-reell ist.

Es sei nun a ein Element von Ω, das nicht in P enthalten ist. Dann ist a auch nicht in Σ_a enthalten, also $\mathsf{P}_a(a)$ nicht formal-reell, also um so mehr $\mathsf{P}(a)$ nicht formal-reell. Das ist zunächst nur möglich, wenn a algebraisch über P ist; denn eine einfache transzendente Erweiterung eines formal-reellen Körpers ist wieder formal-reell (§ 67, Aufg. 4). Jedes Element von Ω ist also algebraisch über P; d. h. Ω ist algebraisch über P. Da man weiter für a ein beliebiges algebraisches Element von Ω außerhalb P nehmen kann, so ist keine einfache echte algebraische Erweiterung $\mathsf{P}(a)$ von P formal-reell, mithin P reell-abgeschlossen. Nach Satz 3 (§ 67) ist $\mathsf{P}(i)$ algebraisch-abgeschlossen, mithin mit Ω identisch. Damit ist der Satz bewiesen.

Bemerkung. In vielen wichtigen Spezialfällen ist Ω abzählbar unendlich und daher die Anwendung des Wohlordnungssatzes unnötig, z. B. wenn Ω der Körper der algebraischen Zahlen ist oder nur einen endlichen Transzendenzgrad in bezug auf diesen hat.

Einige Sonderfälle bzw. unmittelbare Folgerungen von Satz 7 mögen noch besonders formuliert werden.

Satz 7a. *Zu jedem formal-reellen Körper* K *gibt es (mindestens) eine reell-abgeschlossene algebraische Erweiterung.*

Wir brauchen zum Beweis bloß für Ω in Satz 7 die algebraisch-abgeschlossene, algebraische Erweiterung von K zu wählen.

Satz 7b. *Jeder formal-reelle Körper kann auf (mindestens) eine Weise angeordnet werden.*

Dies folgt ohne weiteres aus Satz 1 (§ 67) und 7a.

Ist ferner Ω irgend ein algebraisch-abgeschlossener Körper der Charakteristik Null und setzen wir in Satz 7 für K den Körper der rationalen Zahlen, so haben wir

Satz 7c. *Jeder algebraisch-abgeschlossene Körper* Ω *der Charakteristik Null enthält (mindestens) einen reell-abgeschlossenen Unterkörper* P, *für den* $\Omega = \mathsf{P}(i)$.

Für angeordnete Körper läßt Satz 7a sich wesentlich verschärfen:

Satz 8. *Ist* K *ein angeordneter Körper, so gibt es eine und — von äquivalenten Erweiterungen abgesehen — nur eine reell-abgeschlossene algebraische Erweiterung* P *von* K, *deren Anordnung eine Fortsetzung der Anordnung von* K *ist.* P *besitzt außer dem identischen keinen Automorphismus, der die Elemente aus* K *fest läßt.*

Beweis: Wie in Satz 6 (§ 67) werde mit $\overline{\mathsf{K}}$ der Körper bezeichnet, der aus K durch Adjunktion der Quadratwurzeln aus allen positiven Elementen von K entsteht. Es sei P eine algebraische, reell-abgeschlossene Erweiterung von $\overline{\mathsf{K}}$. Eine solche gibt es nach Satz 7a, da $\overline{\mathsf{K}}$ bereits als formal-reell erkannt ist. P ist auch algebraisch in bezug auf K,

und die Anordnung von P ist eine Fortsetzung der Anordnung von K, da doch jedes positive Element aus K in $\overline{\mathsf{K}}$ Quadrat ist, also erst recht in P. Damit ist die Existenz eines solchen P bewiesen.

Es sei jetzt P^* eine zweite algebraische, reell-abgeschlossene Erweiterung von K, deren Anordnung die von K nicht ändert. $f(x)$ sei ein (nicht notwendig irreduzibles) Polynom mit Koeffizienten aus K. Der Sturmsche Satz gestattet uns, bereits in K zu entscheiden, wieviele Wurzeln $f(x)$ in P oder P^* besitzt. Wir brauchen bloß eine Sturmsche Kette für $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n$ zu untersuchen. Daher hat $f(x)$ in P ebensoviele Wurzeln wie in P^*. Insbesondere besitzt jede Gleichung in K, die in P mindestens eine Wurzel besitzt, auch in P^* mindestens eine Wurzel und umgekehrt. Seien nun $\alpha_1, \alpha_2, \ldots, \alpha_r$ die Wurzeln von $f(x)$ in P, $\beta_1^*, \beta_2^*, \ldots, \beta_r^*$ die Wurzeln von $f(x)$ in P^*. Ferner sei ξ in P so gewählt, daß $\mathsf{K}(\xi) = \mathsf{K}(\alpha_1, \ldots, \alpha_r)$ ist, und $F(x) = 0$ die irreduzible Gleichung für ξ in K. $F(x)$ besitzt also in P die Wurzel ξ, daher auch in P^* mindestens eine Wurzel η^*; $\mathsf{K}(\xi)$ und $\mathsf{K}(\eta^*)$ sind äquivalente Erweiterungen von K. Da $\mathsf{K}(\xi)$ durch die r Nullstellen $\alpha_1, \ldots, \alpha_r$ von $f(x)$ erzeugt wird, muß auch $\mathsf{K}(\eta^*)$ durch r Wurzeln von $f(x)$ erzeugt werden; nun ist $\mathsf{K}(\eta^*)$ ein Unterkörper von P^*, also gilt $\mathsf{K}(\eta^*) = \mathsf{K}(\beta_1^*, \ldots, \beta_r^*)$. Demnach sind $\mathsf{K}(\alpha_1, \ldots, \alpha_r)$ und $\mathsf{K}(\beta_1^*, \ldots, \beta_r^*)$ äquivalente Erweiterungen von K.

Um nun zu zeigen, daß P und P^* äquivalente Erweiterungen von K sind, bemerken wir, daß eine isomorphe Abbildung von P auf P^* notwendig die Anordnung erhalten muß, da diese sich ja (nach dem Beweis von Satz 1, § 67) durch die Eigenschaft, Quadrat zu sein oder nicht zu sein, erklären läßt. Wir definieren daher folgende Abbildung σ von P auf P^*. Sei α ein Element aus P, $p(x)$ das irreduzible Polynom in K, dessen Nullstelle α ist, und $\alpha_1, \alpha_2, \ldots, \alpha_r$ die sämtlichen Wurzeln von $p(x)$ in P, so numeriert $\alpha_1 < \alpha_2 < \cdots < \alpha_r$ ist; speziell sei $\alpha = \alpha_k$. Sind dann $\alpha_1^*, \alpha_2^*, \ldots, \alpha_r^*$ die Wurzeln von $p(x)$ in P^* und ist $\alpha_1^* < \alpha_2^* \cdots < \alpha_r^*$, so sei $\sigma(\alpha) = \alpha_k^*$. Offenbar ist σ eineindeutig und läßt die Elemente aus K fest. Es ist nachzuweisen, daß σ eine isomorphe Abbildung ist. Sei zu diesem Zweck $f(x)$ wieder irgend ein Polynom in K; $\gamma_1, \gamma_2, \ldots, \gamma_s$ seine Wurzeln in P; $\gamma_1^*, \gamma_2^*, \ldots, \gamma_s^*$ die in P^*. Ferner sei $g(x)$ das Polynom in K, dessen Nullstellen die Quadratwurzeln aus den positiven Wurzeldifferenzen von $f(x)$ sind. $\delta_1, \delta_2, \ldots, \delta_t$ seien die Nullstellen von $g(x)$ in P; $\delta_1^*, \delta_2^*, \ldots, \delta_t^*$ die in P^*. Nach dem oben Bewiesenen sind

$$\Lambda = \mathsf{K}(\gamma_1, \ldots, \gamma_s, \delta_1, \ldots, \delta_t) \quad \text{und} \quad \Lambda^* = \mathsf{K}(\gamma_1^*, \ldots, \gamma_s^*, \delta_1^*, \ldots, \delta_t^*)$$

äquivalente Erweiterungen von K. Es gibt also eine isomorphe Abbildung τ von Λ auf Λ^*, die K elementweise fest läßt. Durch τ wird jedem γ ein γ^*, jedem δ ein δ^* zugeordnet. Die Bezeichnung sei so gewählt, daß $\tau(\gamma_k) = \gamma_k^*$, $\tau(\delta_h) = \delta_h^*$ ist. Ist nun $\gamma_k < \gamma_l$ (in P), so ist $\gamma_l - \gamma_k = \delta_h^2$ für einen gewissen Index h, also auch $\gamma_l^* - \gamma_k^* = \delta_h^{*2}$,

demnach $\gamma_k^* < \gamma_l^*$ (in P^*). τ ordnet also die Wurzeln von $f(x)$ in P und P^* einander der Größe nach zu. Da dies folglich auch für die Nullstellen der in K irreduziblen Faktoren von $f(x)$ gilt, haben wir $\tau(\gamma_k) = \sigma(\gamma_k)$ $(k = 1, 2, \ldots, s)$. Indem wir also dafür sorgen, daß zwei beliebig vorgegebene Elemente α, β aus P sowie $\alpha + \beta$ und $\alpha \cdot \beta$ unter den Wurzeln von $f(x)$ vorkommen, erkennen wir, daß σ eine isomorphe Abbildung von P auf P^* ist, und zwar die einzige, die K elementweise fest läßt. Wählen wir $\mathsf{P}^* = \mathsf{P}$, so ergibt sich die Richtigkeit unserer Behauptung über die Automorphismen von P.

Da sich der Körper Γ der rationalen Zahlen nach § 63 nur in einer Weise anordnen läßt, so folgt aus Satz 8 unmittelbar:

Satz 8a. *Es gibt — von isomorphen Körpern abgesehen — einen und nur einen reell-abgeschlossenen algebraischen Körper über* Γ.

Für diesen Körper kann man natürlich den Körper der reellen algebraischen Zahlen im gewöhnlichen Sinn (§ 64) nehmen, der durch Aussonderung der algebraischen unter den reellen Zahlen entsteht. Das ist aber ein transzendenter Umweg, den man durch die rein algebraische Konstruktion aus Satz 7 (wobei man $\mathsf{K} = \Gamma$ und für Ω den algebraisch-abgeschlossenen algebraischen Erweiterungskörper A über Γ nimmt) vermeiden kann. Damit ist also auf rein algebraischem Wege der *Körper der reellen algebraischen Zahlen*, den wir mit P bezeichnen, konstruiert. Da A abzählbar ist, ist die ganze Konstruktion sogar ohne Wohlordnung, in abzählbar vielen wirklich ausführbaren Schritten, durchzuführen. Der Körper aller algebraischen Zahlen hat die Gestalt $\mathsf{A} = \mathsf{P}(i)$.

Wie wir noch sehen werden, ist P in A nicht der einzige reell-abgeschlossene Körper, sondern nur einer unter unendlichvielen äquivalenten.

Satz 9. *Jeder formal-reelle algebraische Erweiterungskörper* K^* *von* Γ *ist mit einem Unterkörper von* P, *also mit einem reellen algebraischen Zahlkörper isomorph.*

Beweis. Nach Satz 7a können wir zu K^* stets einen algebraischen, reell-abgeschlossenen Erweiterungskörper P^* konstruieren, der nach Satz 8a notwendig zu P isomorph ausfällt. Daraus folgt die Behauptung.

Eine gewisse isomorphe Abbildung von K^* auf $\mathsf{K} \leqq \mathsf{P}$ ergibt natürlich auch eine gewisse Anordnung von K^*, da alle Unterkörper K von P von Haus aus angeordnet sind. Umgekehrt kann auch jede Anordnung von K^* in dieser Weise erhalten werden, da der im Beweis von Satz 9 konstruierte reell-abgeschlossene Erweiterungskörper P^* nach Satz 8 so konstruiert werden kann, daß bei seiner Anordnung die von K^* erhalten bleibt. Diese Anordnung geht dann beim Isomorphismus über in die (einzig mögliche) Anordnung von P.

Nehmen wir für K^* speziell einen endlichen algebraischen Zahlkörper, der nur endlichviele Isomorphismen in A besitzt, so folgt:

Die Anzahl der Isomorphismen, die K^* *in einen reellen algebraischen Zahlkörper überführen, ist gleich der Anzahl der verschiedenen Anordnungen, deren* K^* *fähig ist (und insbesondere Null, wenn* K^* *nicht formal-reell ist).*

Die Tatsache, daß jeder in A gelegene formal-reelle Körper zu einem reell-abgeschlossenen Körper $\mathsf{P}^* \subset \mathsf{A}$ erweitert werden kann, führt zugleich zu der Erkenntnis, daß es unendlichviele solche Körper P^* in A gibt (wiewohl diese nach Satz 8 a alle untereinander isomorph sind). Denn die Körper $\mathsf{K}_\zeta^* = \Gamma(\zeta \sqrt[n]{2})$, wo n eine ungerade natürliche Zahl und ζ eine n-te Einheitswurzel ist, sind alle isomorph zu $\Gamma(\sqrt[n]{2})$, also formal-reell. Sie führen also zu je einem reell-abgeschlossenen Erweiterungskörper P_ζ^*, und diese Körper bei festem n müssen alle verschieden sein, da ein angeordneter Körper nur eine n-te Wurzel aus 2 enthalten kann (§ 63, Aufg. 5). Die Anzahl n dieser Körper kann aber beliebig hoch gewählt werden.

Aufgaben. 1. Es sei Θ eine Wurzel der in Γ irreduziblen Gleichung $x^4 - x - 1 = 0$. Auf wieviel Arten kann der Körper $\Gamma(\Theta)$ angeordnet werden?

2. Der Körper $\Gamma(t)$, wo t eine Unbestimmte ist, kann auf unendlichviele Arten angeordnet werden, und zwar sowohl archimedisch als auch nichtarchimedisch. Auch kann t sowohl unendlichgroß als unendlichklein gewählt werden [vgl. § 63, Aufg. 1].

3. Wieviele Nullstellen hat das Polynom $(z^2 - t)^2 - t^3$ in einem reell-abgeschlossenen Erweiterungskörper von $\Gamma(t)$, wenn t unendlichklein ist? Wo liegen diese Nullstellen?

§ 69. Die Beträge der komplexen Zahlen.

Unter dem *Betrag* $|\alpha|$ der komplexen Zahl $\alpha = a + bi$ versteht man die reelle Zahl

$$|\alpha| = \sqrt{a^2 + b^2} = \sqrt{\alpha\bar{\alpha}},$$

wo $\bar{\alpha}$ die konjugiert-komplexe, d. h. in bezug auf den Körper der reellen Zahlen konjugierte Zahl $a - bi$ ist.

Offenbar ist $|\alpha| \geqq 0$, und zwar $|\alpha| = 0$ nur für $\alpha = 0$. Weiter ist $\sqrt{\alpha\beta\bar{\alpha}\bar{\beta}} = \sqrt{\alpha\bar{\alpha}} \cdot \sqrt{\beta\bar{\beta}}$, also

$$|\alpha\beta| = |\alpha| \cdot |\beta|.$$

Um die andere Relation

$$|\alpha + \beta| \leqq |\alpha| + |\beta|$$

nachzuweisen, gehen wir von der offenbar richtigen Relation

$$|\alpha| = \sqrt{a^2 + b^2} \geqq \sqrt{a^2} = |a| \geqq a = \frac{\alpha + \bar{\alpha}}{2}$$

aus, die, auf $\alpha\bar{\beta}$ angewandt, ergibt

$$2|\alpha\bar{\beta}| \geqq \alpha\bar{\beta} + \bar{\alpha}\beta,$$

$$(|\alpha| + |\beta|)^2 = (|\alpha| + |\bar{\beta}|)^2 = |\alpha|^2 + 2|\alpha\bar{\beta}| + |\bar{\beta}|^2$$

$$\geqq \alpha\bar{\alpha} + \alpha\bar{\beta} + \bar{\alpha}\beta + \bar{\beta}\beta = (\alpha + \beta)(\bar{\alpha} + \bar{\beta}) = |\alpha + \beta|^2,$$

$$|\alpha| + |\beta| \geqq |\alpha + \beta|.$$

Die Beträge $|a|$ bilden also eine „Bewertung" des Körpers der komplexen Zahlen im Sinne von § 65.

Für die Zahlen α eines algebraischen Erweiterungskörpers K^* von Γ kann man die Beträge $|\alpha|$ algebraisch definieren, indem man K^* auf einen Unterkörper K von $\mathsf{A} = \mathsf{P}(i)$ isomorph abbildet und dann die Beträge der Zahlen in der Abbildung bestimmt. Die Abbildung kann bei endlichem K^* auf so viele verschiedene Arten geschehen, als der Grad von K^* beträgt (§ 32), und das ergibt ebensoviele „Bewertungen" von K^*. Aber diese Bewertungen sind nicht alle verschieden; denn zu jeder Abbildung $\mathsf{K}^* \cong \mathsf{K}$ gibt es eine konjugiert-komplexe Abbildung (die jeder Zahl α^* die Zahl $\bar{\alpha}$ zuordnet, wenn die erstere Abbildung die Zahl α ergab), welche dieselben Beträge liefert. Ist also r_1 die Anzahl derjenigen Isomorphismen, die K^* in reelle Zahlkörper überführen, und r_2 die Anzahl der Paare konjugiert-komplexer Abbildungen, die K^* in nicht-reelle Zahlkörper überführen, so ist die Anzahl der Bewertungen, die man so erhält, $r_1 + r_2$. Daß diese $r_1 + r_2$ Bewertungen wirklich verschieden sind, sieht man etwa so: Es sei $\mathsf{K}^* = \Gamma(\Theta^*)$. Wenn zwei Isomorphismen $\Theta^* \to \Theta_1$ und $\Theta^* \to \Theta_2$ dieselben Beträge ergeben, so muß

$$|\Theta_1| = |\Theta_2|,$$

$$|1 - \Theta_1| = |1 - \Theta_2|,$$

also

$$\begin{cases} \Theta_1\bar{\Theta}_1 = \Theta_2\bar{\Theta}_2, \\ (1-\Theta_1)(1-\bar{\Theta}_1) = (1-\Theta_2)(1-\bar{\Theta}_2), \end{cases}$$

$$\begin{cases} \Theta_1\bar{\Theta}_1 = \Theta_2\bar{\Theta}_2 \\ \Theta_1 + \bar{\Theta}_1 = \Theta_2 + \bar{\Theta}_2, \end{cases}$$

mithin entweder $\Theta_1 = \Theta_2$ oder $\Theta_1 = \bar{\Theta}_2$ sein; d. h. die beiden Abbildungen müssen identisch oder konjugiert-komplex sein.

Aufgaben. 1. Die Zahlen r_1 und r_2 sind gleich den Anzahlen der reellen bzw. der Paare konjugiert-komplexer Wurzeln der definierenden Gleichung des Körpers $\mathsf{K}^* = \Gamma(\Theta^*)$.

2. Für einen Galoisschen Körper K^* ist $r_1 = 0$ oder $r_2 = 0$, je nachdem K^* formal-reell ist oder nicht.

§ 70. Summen von Quadraten.

Wir wollen nun die Frage untersuchen, welche Elemente eines Körpers K sich als Summen von Quadraten von Elementen aus K darstellen lassen.

Dabei kann man sich zunächst auf formal-reelle Körper beschränken. Ist nämlich K nicht formal-reell, so ist -1 Quadratsumme, etwa:

$$-1 = \sum_1^n \alpha_\nu^2.$$

Wenn nun K eine von 2 verschiedene Charakteristik hat, so folgt daraus für ein beliebiges Element γ von K die Zerlegung in $n+1$ Quadrate:

$$\gamma = \left(\frac{1+\gamma}{2}\right)^2 + (\sum \alpha_\nu^2)\left(\frac{1-\gamma}{2}\right)^2.$$

Hat aber K die Charakteristik 2, so erledigt sich die Frage durch die Bemerkung, daß jede Quadratsumme selbst Quadrat ist:

$$\sum \alpha_\nu^2 = (\sum \alpha_\nu)^2.$$

Daß Summe und Produkt von Quadratsummen wieder Quadratsummen sind, leuchtet ein. Aber auch ein Quotient von Quadratsummen ist wieder Quadratsumme:

$$\frac{\alpha}{\beta} = \alpha \cdot \beta \cdot (\beta^{-1})^2.$$

Für formal-reelle Körper K beweisen wir nun den Satz:

Ist γ in K nicht Summe von Quadraten, so gibt es eine Anordnung von K, in der γ negativ ausfällt.

Beweis. Es sei γ nicht Quadratsumme. Wir zeigen zunächst, daß $\mathsf{K}(\sqrt{-\gamma})$ formal-reell ist. Liegt $\sqrt{-\gamma}$ bereits in K, so ist die Behauptung klar. Andernfalls schließt man so: Wäre

$$-1 = \sum_1^n (\alpha_\nu \sqrt{-\gamma} + \beta_\nu)^2,$$

so würde man durch genau dieselben Schlüsse wie bei Satz 1 (§ 67) erhalten:

$$\gamma = \frac{1 + \sum \beta_\nu^2}{\sum \alpha_\nu^2},$$

mithin wäre γ doch Quadratsumme, entgegen der Voraussetzung. Daher ist $\mathsf{K}(\sqrt{-\gamma})$ formal-reell. Wird nun $\mathsf{K}(\sqrt{-\gamma})$ nach Satz 7b (§ 68) angeordnet, so muß $-\gamma$, als Quadrat, positiv ausfallen. Damit ist die Behauptung bewiesen.

Auf formal-reelle algebraische Zahlkörper angewandt, ergibt das (wenn man beachtet, daß alle möglichen Anordnungen eines solchen nach § 68 durch die isomorphen Abbildungen auf konjugierte reelle Zahlkörper erhalten werden können) den Satz:

Ein Element γ eines algebraischen Zahlkörpers K ist Summe von Quadraten dann und nur dann, wenn bei den Isomorphismen, welche K in seine reellen konjugierten Körper überführen, die Zahl γ niemals in eine negative Zahl übergeführt wird.

Der Satz gilt auch noch, wenn K nicht formal-reell ist, da dann alle Zahlen von K Quadratsummen sind, während es keine Isomorphismen der verlangten Art gibt.

Solche Zahlen eines algebraischen Zahlkörpers K, die bei jeder isomorphen Abbildung von K auf einen konjugierten reellen Zahlkörper stets in positive Zahlen übergehen, heißen *total-positiv in* K. Hat K keine reell-konjugierten Körper, so ist demnach jede Zahl von K total-positiv zu nennen. Der Begriff total-positiv kann auf beliebige Körper K ausgedehnt werden, indem man als total-positiv diejenigen Elemente von K bezeichnet, welche bei jeder überhaupt möglichen Anordnung von K positiv ausfallen. (Insbesondere sind wieder alle Zahlen von K total-positiv, wenn es keine Anordnung von K gibt, also wenn K nicht formal-reell ist.) Die Ergebnisse dieses Paragraphen lassen sich dann dahin zusammenfassen, daß *in einem Körper der Charakteristik* $\neq 2$ *jedes total-positive Element sich als Quadratsumme darstellen läßt.*

Literatur zum Kap. 10.

Weitere Sätze über die Anzahl der Quadrate, die zur Darstellung der total-positiven Zahlen eines Zahlkörpers hinreichen, findet man bei E. Landau: *Über die Zerlegung total positiver Zahlen in Quadrate*, Göttinger Nachr. 1919, S. 392. Für den Fall eines Funktionenkörpers siehe vor allem E. Artin: *Über die Zerlegung definiter Funktionen in Quadrate*. Abhandlungen aus dem Math. Seminar der Hamburgischen Universität, Bd. 5, S. 100—115. 1926.

Sachverzeichnis.

Die Zahlen geben die Seiten an, wo die Begriffe zum erstenmal vorkommen.

Abbildung 6.
Abelsche Gleichung 150.
— Gruppe 15.
Abelscher Erweiterungskörper 150.
— Satz 174.
Abhängigkeit, algebraische 204.
— lineare 95.
Ableitung 67.
Abschnitt der Zahlenreihe 9.
abzählbare Mengen 12.
abzählbar-unendliche Mengen 12.
additive Gruppe 19.
— — eines Ringes 37.
Adjunktion (Körperadj.) 88.
— einer Unbestimmten 51.
ähnlich geordnete Mengen 29.
ähnlich-isomorphe Körper 210.
algebraisch-abgeschlossen 198.
algebraische Abhängigkeit 204.
— Größe 90.
— Körpererweiterung 99.
— Zahl 221.
— Zahlkörper 222.
Algorithmus, euklidischer 61.
allgemeine Gleichung n-ten Grades 172.
alternierende Gruppe 24.
angeordnete Körper 209.
Anzahl 12.
äquivalente Erweiterungen 92.
— Systeme 96, 205.
Äquivalenzrelation 14.
archimedisch angeordnete Körper 211.
Archimedisches Axiom 211.
arithmetische Reihe n-ter Ordnung 73.
assoziatives Gesetz 8, 15, 37.
assoziierte Größen 63.
auflösbare Gruppe 141.
Auflösung durch Radikale 169.
Austauschsatz 96.
Auswahlpostulat 194.
Automorphismen, äußere 30.
— innere 30.
Automorphismengruppe 30.
Automorphismenring 133.
Automorphismus 29.
Axiome von PEANO 7.

Basis (Idealbasis) 54.
— (Körperbasis) 97.
Basiselement 43.
Betrag 209, 235.
Bewertete Körper 218.
Bild 6.
Binomialsatz 41.

Cantorsche Konstruktion der reellen Zahlen 212.
Charakteristik 87.
charakteristische Untergruppe 132.
Cardanische Auflösungsformel 177.
Casus irreducibilis 177.
Cauchys Konvergenzsatz 217.

definierende Gleichung 91.
Definition durch vollständige Induktion 9.
Definitionsbereich 6.
Delisches Problem 184.
Differentialquotient 68.
Differentiation 67.
Differenzenprodukt 174.
Differenzenrechnung 71.
Differenzenschema 72.
direktes Produkt 141.
Diskriminante einer Gleichung 174.
— eines Polynoms 85.
Distributivgesetz 8, 37.
Division 18.
Divisionsalgorithmus 52.
Doppelte Komposition 37.
Durchschnitt 5.

Echte Untermenge 5.
echter Teiler 63.

Eindeutigkeitssatz über symmetrische Funktionen 83.
ein-eindeutige Abbildung 6.
einfache Gruppen 137.
— Körpererweiterungen 89.
— transzendente Erweiterungen 125.
Einfachheit der alternierenden Gruppe 144.
Einheit 63.
Einheitsformen 74.
Einheitsideal 54.
Einheitsoperator 133.
Einheitswurzeln 105.
Einselement 15, 40.
Eisensteinscher Satz 77.
Element einer Menge 4.
Element, unzerlegbares 63.
elementarsymmetrische Funktionen 81.
endliche kommutative Körper 109.
endlicher Erweiterungsring (Körper) 97.
erstes Element 193.
Erweiterungen, algebraische 99.
— einfache 89.
— erster und zweiter Art 113.
— rein transzendente 205.
Erweiterungskörper 88.
erzeugte Untergruppe 25.
erzeugtes Ideal 54.
euklidischer Algorithmus 61.
Eulersche Differentialgleichung 68.
— φ-Funktion 106.
explizit gegebener Körper 128.
Exponent 114, 117.

Faktoren einer Normalreihe 137.
Faktorgruppe 35.
Faktorzerlegung 63, 73, 79.
Fermatscher Satz 112.
Form 52.
formal-reeller Körper 226.
Fortsetzung eines Isomorphismus 100.
fremde Mengen 5.
Fundamentalfolge 213.
Fundamentalsatz der Algebra 229.
Funktion 6.

Galois-Feld 109.
Galoissche Erweiterungskörper 103.
— Gleichungen 104.
— Gruppe 149.
— Körper, zugehöriger 148.
— Resolvente 104.
— Theorie 148.
ganze rationale Funktionen 51.
ganze Zahlen 10.
— Gaußsche Zahlen 44.
ganzzahlige Polynome 51.
Gaußsche Formel 162.
— Summe 165.
— Zahlen 44.
Gaußscher Satz 74.
— Zahlkörper 62.
geordnete Menge 192.
Gewicht eines Polynoms 81.
G. G. T. = größter gemeinsamer Teiler 60.
gleichmächtige Mengen 6.
Gleichungen, auflösbare 170.
Grad einer endlichen Erweiterung 97.
— — algebraischen Größe 91.
— — Permutationsgruppe 148.
— — rationalen Funktion 125.
— eines Polynoms 51.
Gruppe 15.
— einfache 137.
— einer Gleichung 149.
— eines Körpers 149.
— mit Operatoren 132.
Gruppenring 44.
Gruppentafel 20.

Hauptideal 54.
Hauptidealring 60.
Hauptsatz der Galoisschen Theorie 151.
— über endliche Mengen 11.
— — symmetrische Funktionen 81.
— — Normalreihen 139.
Hensels p-adische Zahlen 219.
homogenes Polynom 52.
Homomorphismus für Gruppen 32.
— — Ringe 44.
Homomorphiesatz für Gruppen 35, 134.
— — Ringe 57.
hyperkomplexe Zahlen 43.

Ideal 53.
— teilerloses 59.
— zweiseitiges 53, 133.
Idealbasis 54.
identische Transformation 17.
imprimitive Gruppe 146.
Imprimitivitätsgebiet 146.
Index einer Untergruppe 27.
Induktion, transfinite 196.
— vollständige 7.
Inhalt von $f(x)$ 74.
Innere Automorphismen 30.
inseparabel 114.

Integritätsbereich 39.
Interpolationsformeln 71.
intransitive Gruppen 146.
invariante Untergruppe 28.
inverse Abbildung 6.
— Transformation 17.
inverses Element 15, 40.
Irreduzibilitätskriterien 77.
irreduzible Mengen 205.
— Radikale 171.
— Systeme 205.
irreduzibles Polynom 63.
isobarer Ausdruck 83.
isomorphe Gruppen 29.
— Mengen 29.
— Normalreihen 138.
— Ringe 45.
Isomorphiesätze 135.
Isomorphismus 29, 45.
— mehrstufiger 32.

Jordan-Hölderscher Satz 140.

Kette, Θ-Kette 194.
K. G. V. = kleinstes gemeinsames Vielfaches 60.
Klasse 4.
Klasseneinteilung 14.
Klassen in einer Gruppe 32.
Kleinsche Vierergruppe 31.
Koeffizienten 49.
kommutativer Ring 37.
kommutatives Gesetz 8, 37.
Kommutatorgruppe 35.
komplexe Zahl 221.
Kompositionsfaktoren 138.
Kompositionsreihe 137.
Kongruenz nach einem Ideal 54.
— — — Modul 36.
konjungiert-komplex 235.
konjugierte Erweiterungen 92.
— Größen 92.
— Gruppenelemente 30.
— Körperelemente 92.
— Resolventen 167.
— Untergruppen 30.
Konstante 51.
Konstruktion der regulären Polygone 185.
— des reg. 17-Ecks 165.
— durch vollständige Induktion 9.
Konstruktionen mit Zirkel und Lineal 181.
Konvergenzsatz von CAUCHY 217.
Körper 41.
Körper der algebraischen Zahlen 221.
— — komplexen Zahlen 221.
— — p-adischen Zahlen 219.
— — rationalen Zahlen 49.
Körperbasis 97.
Körpererweiterung 88.
Kreiskörper 156.
Kreisteilungsgleichung 78, 109, 156.
Kreisteilungskörper 156.
Kreisteilungspolynome 107.
kubische Resolvente 179.
Kubusverdoppelung 184.

Lagrangesche Interpolationsformel 71.
— Resolvente 166.
Länge einer Normalreihe 137.
leere Menge 4.
lexikographische Ordnung 84.
Limes 217.
lineare Abhängigkeit 95.
— Interpolation 73.
— unabhängig 95.
Linksideal 53, 132.
Linksinverses 40.
Lürothscher Satz 126.

Mehrstufiger Isomorphismus 32, 44.
Menge 4.
— abzählbare 12.
— endliche 11.
— geordnete 192.
— umfassende 5.
— unendliche 11.
— wohlgeordnete 193.
metazyklisch 172.
Minimalbasis 97.
Mittelwertsatz 226.
Möbiussche Funktion $\mu(n)$ 107.
Modul = additive Gruppe 19.
Modul, Zahlenmodul 16.
Modulbasis 97.
Moduleigenschaft 53.
Modulhomomorphismus 135.
Modul in bezug auf einen Ring 133.
modulo 54.
multiplikative Gruppe eines Körpers 42.

Natürliche Zahl 7.
Nebengruppe 26.
Nebenklasse 26.
negative Zahlen 10.
Newtonsche Interpolationsformel 71.
Norm 123.
— einer Gaußschen Zahl 62.

normaler Erweiterungskörper 103.
Normalisator 32, 35.
Normalreihe 137.
— ohne Wiederholungen 137.
Normalteiler 28.
— zulässiger 132.
Null 10, 19, 37.
Nullelement 37.
Nullfolge 213.
Nullideal 53.
Nullring 39.
Nullstelle erster Art 114.
— k-fache 70.
Nullstellen 69.
— reeller Funktionen 220.
Nullteiler 39.

Obere Grenze 212.
— Schranke 212.
Obermenge 5.
— echte 5.
Objekt einer Transformation 16.
Operatoren 132.
Operatorenbereich 132.
Operatorhomomorphismus 134.
Operatorisomomorphismus 134.
Ordnung einer Gruppe 19.
— eines Elements 26.

p-adische Bewertung 219.
— Zahlen 219.
perfekter Körper 219.
Perioden der Kreisteilungsgleichung 160.
Permutation 16.
— gerade 24.
Polynom 49.
— ganzzahliges 51.
— primitives 74, 76.
— reguläres 76.
Polynomring 50.
— in mehreren Unbestimmten 51.
positive Fundamentalfolge 215.
— Restklasse 215.
Positivsein 208.
Potenzen 21, 40.
Potenzsummen 84.
Primelement 63.
Primhauptideal 59.
Primideal 58.
primitive Einheitswurzel 106.
— Gleichungen 150.
— Gruppe 146.
— Polynome 74, 76.
primitives Element 120.
Primitivzahl 112.
Primkörper 86.
Primzahl 63.
Prinzip der vollständigen Induktion 7.
Produkt zweier Transformationen 17.
— zweier Zahlen 8.
Produkte, zusammengesetzte 20.

Quadratur des Kreises 184.
Quaternionen 44.
Quotientenkörper 46.
Quotientenring 49.

Radikale 169.
Rang einer endlichen Erweiterung 97.
rationale Kurve 127.
— Zahl 49.
Rationalitätsbereich 41.
Rechengesetze in einem Ring 37.
Rechtsideal 53, 133.
Rechtsinverses 40.
Rechtsvielfache 53.
reduzierter Grad eines Körpers 117.
— — — Polynoms 114.
reell-abgeschlossen 227.
reelle Zahlen 13, 217.
reflexive Relationen 14.
rein transzendente Erweiterungen 205.
reine Gleichungen 165.
rekursive Bestimmungsrelationen 9, 197.
relative Isomorphismen 115.
relativ-prim 61.
Repräsentanten einer Klasse 14.
Resolvente, kubische 179.
— von LAGRANGE 166.
Restklassen 26, 36, 54.
Restklassenmodul 36.
Restklassenring 57.
Ring 37.
— mit Einselement 40.
— ohne Nullteiler 39.
Ringadjunktion 89.
Ringhomomorphismus 44.

Satz vom primitiven Element 120.
— von der oberen Grenze 216.
— — ROLLE 226.
SCHREIERS Hauptsatz über Formalreihen 139.
separable Erweiterungen 114.
— Nullstellen 114.
separables Polynom 114.
skalare Vielfache 43.
Spur 123.

Steinitz' Satz über irreduzible Systeme 206.
stetige Funktion 220.
Sturmsche Kette 224.
Sturmsches Theorem 223.
Substitution 149.
sukzessive Divisionen 61.
Summe zweier Zahlen 7.
Summen von Quadraten 236.
symbolische Adjunktion 94.
symmetrische Funktionen 80
— Gruppe 17.
— Relationen 14.
System doppelter Komposition 37.

Teilbarkeit von Idealen 58.
Teiler 58.
teilerfremd 61.
teilerloses Ideal 59.
Teilmenge 5.
total-positive Zahlen 238.
transzendente Erweiterungen 204.
transzendente Größen 90.
Transzendenzgrad 207.
transfinite Induktion 196.
Transformationsgruppe 16.
transitive Permutationsgruppe 145.
— Relationen 14.
Transitivitätsgebiet 146.
Transposition 24.
Trisektion des Winkels 184.

Unbestimmte 49.
unendliche Körpererweiterungen 198.
— Menge 11.
unendlich große (kleine) Elemente 211.
untere Schranke 212.
Untergruppe 23.
— konjugierte 30.
— zulässige 132.
Untergruppen, charakteristische 132.
Unterkörper 86.
Untermenge 5.
— echte 5.
Unterring 53.
unzerlegbar 63.
— im Körper 90.
Urbild 6.

Variable 51.
Vektoren 43.
Vereinigungsmenge 5.
Verfeinerung einer Normalreihe 137.
Vielfache 41, 58.
Vielfachheit einer Wurzel 102.
Vierergruppe 31.
vollkommene Körper 118.
vollständig reduzible Gruppen 143.
Vorzeichen einer Zahl 223.
Vorzeichenwechsel 223.

Weierstraßscher Nullstellensatz 220.
Wertevorrat einer Funktion 6.
Wilsonscher Satz 112.
wohlgeordnete Mengen 193.
Wohlordnungssatz 194.
Wurzel 69, 221.
Wurzelkörper 119.

Zahl, algebraische 221.
— komplexe 221.
— natürliche 7.
— rationale 49.
— reelle 13, 217.
Zahlen, hyperkomplexe 43.
— p-adische 219.
Zahlenmodul 16.
Zahlreihe 7.
Zentrum einer Gruppe 28.
Zerfällungskörper 99.
Zermelos Auswahlpostulat 194.
— Wohlordnungssatz 194.
zulässige Untergruppe 132.
Zwischengruppe 31.
Zykel 24.
zyklische Gleichung 150.
— Gruppe 25.
zyklischer Erweiterungskörper 150.