Mathematisch-
Naturwissenschaftliche
Bibliothek

28

E. ARTIN

GALOISSCHE THEORIE

MATHEMATISCH-NATURWISSENSCHAFTLICHE
BIBLIOTHEK

28

GALOISSCHE THEORIE

Von

DR. E. ARTIN †
o. Professor der Mathematik an der Universität Hamburg

2. Auflage

B. G. TEUBNER VERLAGSGESELLSCHAFT · LEIPZIG
1 9 6 5

E. Artin, Galois Theory
Notre Dame Mathematical Lectures
2. Auflage,
erschienen im Eigenverlag der Notre Dame University, Indiana USA, 1948

Deutsche Übersetzung : Viktor Ziegler, Leipzig
Für die deutsche Ausgabe vom Verfasser neubearbeitet

VLN 294 - 375/38/65 - ES 19 B 2
Printed in the German Democratic Republic
Satz : (III/18/154) B.G.Teubner Leipzig
Druck : (III/18/6) VEB Reprocolor Leipzig

VORWORT

Die englische Ausgabe der vorliegenden Schrift entstand aus einer Ausarbeitung einer Vorlesung, die ich in einem Sommersemester an der Notre Dame University hielt. Es handelte sich damals um die Aufgabe, Studenten mit geringen algebraischen Vorkenntnissen in recht kurzer Zeit mit den Methoden und Problemstellungen der Galoisschen Theorie bekannt zu machen. Zu dieser Ausarbeitung hatte Herr *N. A. Milgram* einen Anhang geschrieben, der die Anwendungen der Theorie betrifft.

Als der Verlag dann mit dem Vorschlag einer deutschen Übersetzung an mich herantrat, tauchte die Frage auf, ob man nicht gleichzeitig eine Einführung in die mehr abstrakten Grundlagen der modernen Algebra geben sollte. Nach reiflicher Überlegung kam ich aber doch zum Entschluß, in dieser Schrift den ursprünglichen Plan beizubehalten, mich also im wesentlichen an den gleichen Leserkreis zu wenden. Es stehen heute genug Lehrbücher zur Verfügung, in denen die Grundzüge der Algebra dargestellt werden.

Nachdem Herr *Ziegler* eine vorläufige Übersetzung angefertigt hatte, stellte sich jedoch heraus, daß vieles in den beiden letzten Teilen verbesserungsbedürftig war. Von größeren Änderungen im zweiten Teil seien nur die folgenden erwähnt: Der Beweis des Fundamentalsatzes der Galoisschen Theorie wurde einheitlicher gestaltet. In dem Abschnitt über Einheitswurzeln wurde ein Beweis der Irreduzibilität der Kreisteilungspolynome aufgenommen, der ohne die Zerlegungseigenschaften ganzzahliger Polynome auskommt und sich an eine Landausche Beweismethode anlehnt. Der dritte Teil endlich wurde vollständig neu geschrieben.

Bei diesen Umarbeitungen hat mich Fräulein *Hel Braun* aufs tatkräftigste unterstützt. Viele wertvolle Vorschläge und Hilfe bei den Korrekturen verdanke ich Herrn *H. Reichardt*.

Hamburg, August 1959 *E. Artin*

INHALTSVERZEICHNIS

I. Lineare Algebra

II. Körpertheorie

III. Anwendungen

von N. A. Milgram

I. LINEARE ALGEBRA

A. Körper

Ein *Körper* ist eine Menge, für deren Elemente zwei Verknüpfungen, Multiplikation und Addition genannt, erklärt sind. Diese sind den Operationen der Multiplikation und Addition im System der reellen Zahlen, das selbst Beispiel eines Körpers ist, analog. In jedem Körper K gibt es eindeutig bestimmte, 0 und 1 genannte Elemente, die mit den anderen Elementen von K additiv oder multiplikativ verknüpft, diesen gegenüber genau das gleiche Verhalten zeigen wie die ihnen entsprechenden Begriffe im System der reellen Zahlen. In zweierlei Hinsicht ist die Analogie unvollständig: 1. Kommutativität der Multiplikation wird nicht in jedem Körper vorausgesetzt; 2. ein Körper kann auch aus nur endlich vielen Elementen bestehen.

Genauer, ein Körper ist eine Menge, deren Elemente hinsichtlich der Addition eine abelsche Gruppe und, abgesehen von der Null, eine multiplikative Gruppe bilden, wobei außerdem die beiden Gruppenoperatione ndistributiv verknüpft sind. Man sieht leicht, daß das Produkt aus der Null und einem beliebigen anderen Element Null ist.

Ist die Multiplikation in einem Körper kommutativ, so nennen wir ihn einen kommutativen Körper. Soll ausdrücklich die Möglichkeit einer Nichtkommutativität der Multiplikation betont werden, so sprechen wir von einem Schiefkörper.

B. Vektorräume

Es sei V eine additive abelsche Gruppe mit Elementen $A, B, \ldots$ und K ein Körper mit Elementen $a, b, \ldots$ Für jedes a aus K und jedes A aus V sei außerdem ein Produkt aA als ein Element von V erklärt. Die Menge V soll ein (linksseitiger) *Vektorraum* über K genannt werden, falls die folgenden Voraussetzungen erfüllt sind:

1. $a(A + B) = aA + aB$
2. $(a + b)A = aA + bA$
3. $a(bA) = (ab)A$
4. $1A = A$.

Ist V ein Vektorraum über K, so gilt, wie sich der Leser leicht überlegen kann, $oA = 0$ und $a0 = 0$, wobei o bzw. 0 das Nullelement von K bzw. V ist. Die erste Beziehung folgt z. B. aus den Gleichungen

$$aA = (a + o)A = aA + oA.$$

Sollte statt eines Produktes aA ein Produkt Aa mit analogen Gesetzen definiert sein, so wird V ein rechtsseitiger Vektorraum über K genannt. Falls in unserer Betrachtung linksseitige und rechtsseitige Vektorräume nicht gleichzeitig auftreten, wollen wir einfach von einem „Vektorraum" sprechen.

C. Homogene lineare Gleichungen

In einem Körper K seien $n \cdot m$ Elemente a_{ij}, $i = 1, 2, \ldots, m$, $j = 1, 2, \ldots, n$ gegeben. Wir fragen nach Lösungen x_i aus K des folgenden Gleichungssystems:

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 \cdots + a_{1n}x_n &= 0 \\ \vdots \quad\quad \vdots \quad\quad & \quad\quad \vdots \quad \vdots \\ a_{m1}x_1 + a_{m2}x_2 \ldots + a_{mn}x_n &= 0. \end{aligned} \tag{1}$$

Man nennt (1) ein homogenes, lineares Gleichungssystem in den Unbekannten $x_1, x_2, \ldots, x_n$. Sind die Elemente $x_1, x_2, \ldots, x_n$ nicht sämtlich o, so nennt man die Lösung nicht-trivial, anderfalls nennen wir sie trivial.

Satz 1. *Ein System linearer homogener Gleichungen besitzt stets eine nicht-triviale Lösung, wenn die Anzahl der Unbekannten die Anzahl der Gleichungen übertrifft.*

Den Beweis führen wir nach einer Methode, die dem Leser noch von der Schule her geläufig sein dürfte, nämlich durch sukzessive Elimination der Unbekannten. Liegen keine Gleichungen in $n > 0$ Variablen vor, so unterliegen unsere Unbekannten keinerlei Einschränkungen, und wir können sie alle $= 1$ setzen. Die Existenz einer nicht-trivialen Lösung ist in diesem Falle trivialerweise gesichert.

Nun gehen wir nach der Methode der vollständigen Induktion vor und nehmen an, daß jedes derartige System von k Gleichungen mit mehr als k Unbekannten für $k < m$ eine nicht-triviale Lösung besitzt. Im Gleichungssystem (1) nehmen wir $n > m$ an und bezeichnen den Ausdruck $a_{i1}x_1 + \cdots + a_{in}x_n$ mit L_i, $i = 1, 2, \ldots, m$. Wir

suchen Elemente $x_1, x_2, \ldots, x_n$, die nicht sämtlich verschwinden, derart, daß $L_1 = L_2 = \cdots = L_m = o$ ist. Gilt $a_{ij} = o$ für jedes i und j, so wird ein beliebig gewähltes System der $x_1, \ldots, x_n$ eine Lösung sein. Sind jedoch die a_{ij} nicht sämtlich o, so können wir $a_{11} \neq o$ annehmen, denn die Reihenfolge, in der die Gleichungen geschrieben bzw. die Unbekannten numeriert sind, ist ohne Einfluß auf die Existenz oder Nichtexistenz einer allen Gleichungen gemeinsamen Lösung. Eine nicht-triviale Lösung zu dem gegebenen Gleichungssystem läßt sich dann und nur dann finden, wenn das Gleichungssystem

$$\begin{aligned} &L_1 = o \\ &L_2 - a_{21}a_{11}^{-1}L_1 = o \\ &\cdots\cdots\cdots\cdots \\ &L_m - a_{m1}a_{11}^{-1}L_1 = o \end{aligned}$$

eine Lösung besitzt. Denn ist $x_1, \ldots, x_n$ eine Lösung des zuletzt betrachteten Systems, so verschwindet wegen $L_1 = o$ das zweite Glied in allen weiteren Gleichungen, und es ist demnach $L_2 = L_3 = \cdots = L_m = o$. Ist umgekehrt (1) erfüllt, so ist selbstverständlich auch das neue System erfüllt. Der Leser wird erkennen, daß das neue System so aufgestellt wurde, als wäre x_1 aus den letzten Gleichungen „eliminiert" worden. Existiert nunmehr eine nicht-triviale Lösung der letzten $m - 1$ Gleichungen, die hierbei als Gleichungen in $x_2, \ldots, x_n$ aufgefaßt seien, so erhalten wir, wenn wir $x_1 = -a_{11}^{-1}(a_{12}x_2 + a_{13}x_3 + \cdots + a_{1n}x_n)$ setzen, eine Lösung des gesamten Systems. Nach Induktionsvoraussetzung besitzen aber die letzten $m - 1$ Gleichungen eine nicht-triviale Lösung, und daraus folgt unsere Behauptung.

Anmerkung. Im System (1) sind alle Koeffizienten a_{ij} linksseitige Faktoren der x_j. Für ein Gleichungssystem, bei dem alle Koeffizienten rechtsseitige Faktoren sind, bei dem also das einzelne Glied $x_j a_{ij}$ lautet, gilt derselbe Satz mit einem analogen Beweis. Treten sowohl linksseitige wie rechtsseitige Koeffizienten auf, so kann im nichtkommutativen Fall keine derartige Aussage gemacht werden.

D. Abhängigkeit und Unabhängigkeit von Vektoren

In einem Vektorraum V über einem Körper K nennt man die Vektoren $A_1, A_2, \ldots, A_n$ *abhängig*, wenn es Elemente $x_1, x_2, \ldots, x_n$ von K, die nicht sämtlich o sind, gibt, für welche $x_1A_1 + x_2A_2 + \cdots$

$+ x_n A_n = 0$ gilt. Andernfalls nennt man die Vektoren $A_1, A_2, \ldots, A_n$ *unabhängig*.

Unter der *Dimension* eines Vektorraumes V über einem Körper K verstehe man die maximale Anzahl unabhängiger Vektoren aus V. Genauer gesagt, erhält ein Vektorraum die Dimension unendlich, wenn es beliebig viele unabhängige Vektoren in V gibt; sollte es in V ein System von n unabhängigen Vektoren geben, jedes System von mehr als n Vektoren jedoch abhängig sein, so erhält V die Dimension n.

Ein System $A_1, A_2, \ldots, A_m$ von Elementen in V nennt man ein *Erzeugendensystem* von V, wenn jedes Element A von V bei geeigneter Wahl von Elementen a_i aus K, $i = 1, \ldots, m$, sich linear durch die $A_1, A_2, \ldots, A_m$ ausdrücken läßt, d.h. $A = \sum_{i=1}^{m} a_i A_i$ gilt.

Satz 2. *Sollte V ein Erzeugendensystem $A_1, A_2, \ldots, A_m$ haben, so ist die Maximalzahl der unabhängigen Vektoren dieses Erzeugendensystems gleich der Dimension von V.*

Beweis. Sind alle $A_i = 0$, so besteht V nur aus dem Nullvektor. Dieser Nullvektor ist abhängig, wie die Relation $1 \cdot 0 = 0$ zeigt, die Dimension von V ist also o.

Andernfalls sei r die Maximalzahl unabhängiger Vektoren des Erzeugendensystems $A_1, A_2, \ldots, A_m$, und durch Umnumerieren kann erreicht werden, daß $A_1, A_2, \ldots, A_r$ unabhängig sind. Da r die Maximalzahl unabhängiger A_i war, sind die $r+1$ Vektoren $A_1, A_2, \ldots, A_r, A_i$ abhängig, es gibt also eine Relation

$$a_1 A_1 + a_2 A_2 + \cdots + a_r A_r + b A_i = o,$$

in der nicht alle Koeffizienten verschwinden. Wäre $b = 0$, so würden $A_1, A_2, \ldots, A_r$ abhängig sein. Wegen $b \neq o$ kann man schreiben

$$A_i = -b^{-1}(a_1 A_1 + a_2 A_2 + \cdots + a_r A_r).$$

Daraus folgt, daß $A_1, A_2, \ldots, A_r$ ebenfalls ein Erzeugendensystem ist; denn in dem linearen Ausdruck für einen beliebigen Vektor von V läßt sich jedes A_i durch eine Linearkombination von $A_1, A_2, \ldots, A_r$ ersetzen.

Nun sei $B_1, B_2, \ldots, B_t$ irgendein System von Vektoren in V mit $t > r$. Dann gibt es a_{ij} derart, daß $B_j = \sum_{i=1}^{r} a_{ij} A_i$ ist. Wir wollen zeigen, daß die Vektoren $B_1, B_2, \ldots, B_t$ abhängig sind, daß es also

nicht-triviale x_t in K gibt, für die

$$x_1 B_1 + x_2 B_2 + \cdots + x_t B_t = 0$$

gilt. Ersetzen wir in dieser Gleichung B_j durch $\sum_{i=1}^{r} a_{ij} A_i$, so erhalten wir eine Linearkombination der A_i, wobei $\sum_{j=1}^{r} x_j a_{ij}$ der Koeffizient von A_i ist. Es wird also genügen, nicht-triviale x_j zu finden, für die $\sum_{j=1}^{t} x_j a_{ij} = o$, $i = 1, 2, \ldots, r$, gilt. Wegen $t > r$ und Satz 1 gibt es solche x_j.

Da mehr als r Vektoren abhängig sind, die Vektoren $A_1, A_2, \ldots, A_r$ aber unabhängig, so ist r die Dimension von V.

Anmerkung. Je n beliebige unabhängige Vektoren $A_1, A_2, \ldots, A_n$ eines n-dimensionalen Vektorraumes bilden ein Erzeugendensystem. Denn für einen beliebigen Vektor A sind die Vektoren $A, A_1, \ldots, A_n$ abhängig, und der Koeffizient von A in der Abhängigkeitsbeziehung kann nicht Null sein. Auflösung nach A zeigt, daß die $A_1, A_2, \ldots, A_n$ ein Erzeugendensystem bilden.

Eine Teilmenge eines Vektorraumes heißt *Teilraum*, wenn sie Untergruppe des Vektorraumes ist und wenn außerdem die Multiplikation eines beliebigen Elementes der Teilmenge mit einem Körperelement nicht aus der Teilmenge hinausführt. Sind $A_1, A_2, \ldots, A_s$ Elemente eines Vektorraumes V, so bildet das System aller Elemente der Form $a_1 A_1 + \cdots + a_s A_s$ offenbar einen Teilraum von V. Aus der Definition der Dimension geht ferner hervor, daß die Dimension eines Teilraumes die Dimension des gesamten Vektorraumes nicht übertrifft.

Es sei V ein Vektorraum endlicher Dimension n und W ein Teilraum von V von gleicher Dimension n. Dann ist $W = V$. In der Tat enthält der Teilraum n unabhängige Vektoren, und diese bilden ein Erzeugendensystem von V.

Ein s-tupel $(a_1, a_2, \ldots, a_s)$ von Elementen aus einem Körper K nennen wir einen *Zeilenvektor*. Die Gesamtheit aller derartigen s-tupel bildet einen Vektorraum auf Grund der folgenden Definitionen:

α) Es heiße $(a_1, a_2, \ldots, a_s) = (b_1, b_2, \ldots b_s)$ dann und nur dann, wenn $a_i = b_i$, $i = 1, \ldots, s$ gilt;

β) $(a_1, a_2, \ldots, a_s) + (b_1, b_2, \ldots, b_s) = (a_1 + b_1, a_2 + b_2, \ldots, a_s + b_s)$;

γ) $b(a_1, a_2, \ldots, a_s) = (ba_1, ba_2, \ldots, ba_s)$ für b aus K.

Schreibt man die s-tupel senkrecht

$$\begin{pmatrix} a_1 \\ \vdots \\ a_s \end{pmatrix},$$

so nennt man sie *Spaltenvektoren.*

Satz 3. *Der Zeilen-(Spalten-)Vektorraum K^n aller n-tupel aus einem Körper K ist ein Vektorraum der Dimension n über K.*

Beweis. Die n Elemente (die sogenannten Einheitsvektoren)

$$\begin{aligned} \varepsilon_1 &= (1, 0, 0, \ldots, 0) \\ \varepsilon_2 &= (0, 1, 0, \ldots, 0) \\ &\vdots \\ \varepsilon_n &= (0, 0, \ldots, 0, 1) \end{aligned}$$

sind unabhängig und erzeugen K^n. Beides folgt aus der Beziehung $(a_1, a_2, \ldots, a_n) = \sum a_i \varepsilon_i$.

Wir nennen ein rechteckiges Schema

$$\begin{pmatrix} a_{11} a_{12} & \ldots & a_{1n} \\ a_{21} a_{22} & \ldots & a_{2n} \\ \vdots \quad \vdots & & \vdots \\ a_{m1} a_{m2} & \ldots & a_{mn} \end{pmatrix}$$

von Elementen eines Körpers K eine *Matrix.* Als *rechten Zeilenrang* einer Matrix bezeichnen wir die maximale Anzahl der unabhängigen Zeilenvektoren unter den Zeilen $(a_{i1}, a_{ik}, \ldots, a_{in})$ der Matrix, wobei die Multiplikation mit Körperelementen von rechts erfolgt. Entsprechend definieren wir den linken Zeilenrang sowie den rechten bzw. linken Spaltenrang.

Satz 4. *In jeder Matrix ist der rechte Spaltenrang gleich dem linken Zeilenrang und der linke Spaltenrang gleich dem rechten Zeilenrang. Ist der Körper kommutativ, so sind die vier Zahlen einander gleich und werden dann als Rang der Matrix bezeichnet.*

Beweis. Wir bezeichnen die Spaltenvektoren der Matrix mit $C_1, C_2, \ldots, C_n$ und ihre Zeilenvektoren mit $R_1, R_2, \ldots, R_m$. Der

Spaltenvektor 0 ist

$$\begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix},$$

und jede Abhängigkeit $C_1x_1 + C_2x_2 + \cdots + C_nx_n = 0$ ist äquivalent einer Lösung des Gleichungssystems

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= 0 \\ \vdots \qquad\qquad & \quad \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n &= 0\,. \end{aligned} \tag{1}$$

Irgendeine Änderung in der Reihenfolge der Zeilen der Matrix führt zu demselben Gleichungssystem und ändert daher den Spaltenrang der Matrix nicht. Auch der Zeilenrang bleibt ungeändert, da die geänderte Matrix dieselben Zeilenvektoren besitzt. Wir bezeichnen nun mit s den rechten Spaltenrang und mit z den linken Zeilenrang der Matrix. Auf Grund obiger Bemerkungen dürfen wir annehmen, daß die ersten z Zeilen der Matrix unabhängige Zeilenvektoren sind. Der von allen Zeilen der Matrix erzeugte Vektorraum der Zeilenvektoren hat nach Satz 2 die Dimension z und wird bereits von den ersten z Vektoren erzeugt. Daher läßt sich jede Zeile linear durch die ersten z Zeilen ausdrücken. Daraus folgt, daß eine beliebige Lösung der ersten z Gleichungen in (1) eine Lösung des ganzen Systems ist; denn jede Gleichung läßt sich als Linearkombination der ersten z gewinnen. Umgekehrt ist jede Lösung von (1) auch eine Lösung der ersten z Gleichungen. Das bedeutet, daß die Matrix

$$\begin{pmatrix} a_{11}a_{12}\cdots a_{1n} \\ \vdots \quad \vdots \quad\quad \vdots \\ a_{z1}a_{z2}\cdots a_{zn} \end{pmatrix},$$

die aus den ersten z Zeilen der ursprünglichen Matrix besteht, denselben rechten Spaltenrang hat wie die ursprüngliche Matrix. Sie hat auch denselben linken Zeilenrang, denn die z Zeilen waren unabhängig gewählt. Aber der Spaltenrang der neuen Matrix kann nach Satz 3 z nicht übersteigen. Demnach ist $s \leqq z$. Ähnlich erhalten wir, wenn wir mit s' den linken Spaltenrang und mit z' den rechten Zeilenrang bezeichnen, $s' \leqq z'$. Transponieren wir die ursprüngliche Matrix,

d. h., vertauschen wir in ihr Zeilen mit Spalten, so ist der linke Zeilenrang der transponierten Matrix gleich dem linken Spaltenrang der ursprünglichen Matrix. Wenden wir die oben angestellten Überlegungen auf die transponierte Matrix an, so erhalten wir $z \leqq s$ und $z' \leqq s'$.

E. Inhomogene lineare Gleichungen

Es soll nun die Frage der Lösbarkeit eines Systems inhomogener linearer Gleichungen

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &= b_1 \\ a_{21}x_1 + \cdots\cdots\cdots + a_{2n}x_n &= b_2 \\ \vdots \qquad\qquad\qquad\quad \vdots &\quad \vdots \\ a_{m1}x_1 + \cdots\cdots\cdots + a_{mn}x_n &= b_m \end{aligned} \tag{2}$$

untersucht werden. Wir ordnen diesem System zwei Matrizen M und N zu. M sei die Matrix der Koeffizienten a_{ij}; N entstehe aus M, indem man die i-te Zeile um das Element b_i vermehrt. Die Spaltenvektoren von N sollen mit $A_1, A_2, \ldots, A_n, B$ bezeichnet werden. Das System (2) kann dann abgekürzt in der Form

$$A_1x_1 + A_2x_2 + \cdots + A_nx_n = B$$

geschrieben werden.

Es sei K^m der rechtsseitige Vektorraum aller m-gliedrigen Spaltenvektoren. Die Vektoren $A_1, A_2, \ldots, A_n$ liegen in K^m und erzeugen einen Teilraum T von K^m. Die Lösbarkeit unserer Gleichungen besagt also einfach, daß B zu T gehört. Die Dimension von T ist der rechte Spaltenrang der Matrix M. Die Lösbarkeit unserer Gleichungen besagt also, daß M und N denselben rechten Spaltenrang haben. All dies ist nur eine andere Sprechweise für Lösbarkeit. Benutzt man Satz 4, so sieht man, daß die Gleichungen (2) genau dann eine Lösung haben, wenn die linken Zeilenränge von M und N dieselben sind, und diese Aussage kann unter Umständen nützlich sein.

Sollte $m = n$ sein, die Anzahl der Gleichungen also gleich der Anzahl der Unbekannten, so betrachtet man neben dem Gleichungssystem (2) auch das *zugehörige homogene Gleichungssystem*

$$A_1x_1 + A_2x_2 + \cdots + A_nx_n = 0.$$

Die am häufigsten auftretende Fragestellung ist die folgende:

Hat bei gegebenen Koeffizienten a_{ij} das System (2) eine Lösung bei *beliebigen* b_i aus K? Dies bedeutet dann, daß jeder Spaltenvektor B im Raum T liegt, daß also T der ganze Raum K^n ist. Da K^n die Dimension n hat, ist dies genau dann der Fall, wenn die Vektoren $A_1, A_2, \ldots, A_n$ linear unabhängig sind. Dies aber bedeutet, daß das zugehörige homogene Gleichungssystem nur die triviale Lösung hat. Ferner läßt sich jeder Vektor B nur auf eine Art als Linearkombination der Vektoren $A_1, A_2, \ldots, A_n$ ausdrücken. Wir haben also bewiesen

Satz 5. *Ist $m = n$ im Gleichungssystem (2), so existiert bei beliebigen rechten Seiten dann und nur dann eine Lösung, wenn das zugehörige homogene Gleichungssystem nur die triviale Lösung hat. Ist das der Fall, dann ist die Lösung überdies eindeutig.*

F. Determinanten

Die Determinantentheorie, die wir hier entwickeln wollen, wird in der Galoisschen Theorie nicht benötigt. Der Leser mag daher, falls er es wünscht, diesen Abschnitt überschlagen.

Wir nehmen an, unser Körper sei kommutativ, und betrachten die quadratische Matrix

$$\begin{pmatrix} a_{11} a_{12} \cdots a_{1n} \\ a_{21} a_{22} \cdots a_{2n} \\ \cdots\cdots\cdots \\ a_{n1} a_{n2} \cdots a_{nn} \end{pmatrix} \tag{1}$$

mit n Zeilen und n Spalten. Nun definieren wir eine gewisse Funktion dieser Matrix, deren Wert ein Element unseres Körpers ist, nennen diese Funktion Determinante und bezeichnen sie durch

$$\begin{vmatrix} a_{11} a_{12} \cdots a_{1n} \\ a_{21} a_{22} \cdots a_{2n} \\ \cdots\cdots\cdots \\ a_{n1} a_{n2} \cdots a_{nn} \end{vmatrix} \tag{2}$$

oder durch $D(A_1, A_2, \ldots, A_n)$, falls wir sie als Funktion der Spaltenvektoren $A_1, A_2, \ldots, A_n$ von (1) auffassen. Halten wir alle Spalten außer A_k fest und fassen wir die Determinante als Funktion von A_k auf, so schreiben wir $D_k(A_k)$ oder mitunter auch nur D.

Definition. Eine Funktion der Spaltenvektoren nennen wir Determinante, wenn sie den folgenden drei Axiomen genügt:

1. Als Funktion einer beliebigen Spalte A_k aufgefaßt, ist sie linear und homogen, d. h.

$$D_k(A_k + A_k') = D_k(A_k) + D_k(A_k'), \tag{3}$$

$$D_k(cA_k) = c \cdot D_k(A_k). \tag{4}$$

2. Ihr Wert ist $= 0$, wenn zwei benachbarte Spalten A_k und A_{k+1} gleich sind.

3. Ihr Wert ist $= 1$, wenn jedes A_k der Einheitsvektor U_k ist,

$$U_1 = \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \qquad U_2 = \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \ldots, U_n = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}. \tag{5}$$

Die Frage, ob Determinanten überhaupt existieren, soll zunächst offengelassen werden. Doch wollen wir aus unseren Axiomen Folgerungen ziehen:

a) Setzen wir in (4) $c = 0$, so erhalten wir: eine Determinante ist 0, wenn eine ihrer Spalten 0 ist.

b) $D_k(A_k) = D_k(A_k + cA_{k\pm1})$ oder: eine Determinante bleibt ungeändert, wenn wir ein Vielfaches einer Spalte zu einer benachbarten Spalte addieren. In der Tat, auf Grund des Axioms 2 und der Gleichungen (3) und (4) gilt

$$D_k(A_k + cA_{k\pm1}) = D_k(A_k) + cD_k(A_{k\pm1}) = D_k(A_k).$$

c) Wir betrachten die beiden Spalten A_k und A_{k+1}. Diese können wir durch A_k und $A_{k+1} + A_k$ ersetzen. Subtrahieren wir die zweite von der ersten, so sind die neuen Spalten $-A_{k+1}$ und $A_{k+1} + A_k$. Addieren wir die erste zu der zweiten, so erhalten wir $-A_{k+1}$ und A_k. Schließlich klammern wir -1 aus. Daraus schließen wir: Eine Determinante ändert ihr Vorzeichen, wenn wir zwei benachbarte Spalten vertauschen.

d) Eine Determinante verschwindet, wenn irgend zwei ihrer Spalten gleich sind. In der Tat, wir können zwei beliebige Spalten nebeneinander bringen, indem wir hinreichend oft benachbarte Spalten vertauschen, und brauchen dann nur noch das Axiom 2 anzuwenden.

In der gleichen Weise wie unter b) und c) können wir die folgenden allgemeineren Regeln beweisen:

e) Addiert man das Vielfache einer Spalte zu einer anderen Spalte, so bleibt der Wert der Determinante erhalten.

f) Vertauschung zweier beliebiger Spalten ändert lediglich das Vorzeichen von D.

g) Es sei $(\nu_1, \nu_2, \ldots, \nu_n)$ eine Permutation der Indizes $(1, 2, \ldots, n)$. Ordnen wir nun in $D(A_{\nu_1}, A_{\nu_2}, \ldots, A_{\nu_n})$ die Spalten solange um, bis sie wieder die ursprüngliche Anordnung angenommen haben, so erhalten wir

$$D(A_{\nu_1}, A_{\nu_2}, \ldots, A_{\nu_n}) = \pm D(A_1, A_2, \ldots, A_n).$$

Hierin ist $\pm$ ein wohlbestimmtes Vorzeichen, das von den speziellen Werten der A_k nicht abhängt. Ersetzen wir A_k durch U_k, so wird $D(U_{\nu_1}, U_{\nu_2}, \ldots, U_{\nu_n}) = \pm 1$ und das Vorzeichen ist somit nur von der Permutation der Einheitsvektoren abhängig[1]).

Nun ersetzen wir jeden Vektor A_k durch die folgende Linearkombination A_k' der $A_1, A_2, \ldots, A_n$:

$$A_k' = b_{1k}A_1 + b_{2k}A_2 + \cdots + b_{nk}A_n. \tag{6}$$

Bei der Berechnung von $D(A_1', A_2', \ldots, A_n')$ wenden wir zunächst das Axiom 1 auf A_1' an und zerlegen die Determinante in eine Summe; dann verfahren wir in jedem Glied in der gleichen Weise mit A_2' usw. Schließlich erhalten wir

$$\begin{aligned} D(A_1', A_2', \ldots, A_n') &= \sum_{\nu_1, \nu_2, \ldots, \nu_n} D(b_{\nu_1 1} A_{\nu_1}, b_{\nu_2 2} A_{\nu_2}, \ldots, b_{\nu_n n} A_{\nu_n}) \\ &= \sum_{\nu_1, \nu_2, \ldots, \nu_n} b_{\nu_1 1} b_{\nu_2 2} \ldots b_{\nu_n n} D(A_{\nu_1}, A_{\nu_2}, \ldots, A_{\nu_n}), \end{aligned} \tag{7}$$

wobei die ν_i unabhängig voneinander die Werte von 1 bis n durchlaufen. Sollten zwei der Indizes ν_i gleich sein, so ist $D(A_{\nu_1}, A_{\nu_2}, \ldots, A_{\nu_n}) = 0$; wir brauchen daher nur die Glieder beizubehalten, in denen $(\nu_1, \nu_2, \ldots, \nu_n)$ eine Permutation von $(1, 2, \ldots, n)$ ist. Dies ergibt

$$\begin{aligned} &D(A_1', A_2', \ldots, A_n') \\ &\quad = D(A_1, A_2, \ldots, A_n) \cdot \sum_{(\nu_1, \ldots, \nu_n)} \pm b_{\nu_1 1} \cdot b_{\nu_2 2} \cdot \ldots \cdot b_{\nu_n n}, \end{aligned} \tag{8}$$

wobei $(\nu_1, \nu_2, \ldots, \nu_n)$ sämtliche Permutationen von $(1, 2, \ldots, n)$ durchläuft; für $\pm$ wird das der betreffenden Permutation zugehörige

[1]) Seiner Herleitung nach hängt das Vorzeichen auch nicht von der gewählten Determinantenfunktion ab.

Vorzeichen gesetzt. Es ist wichtig zu bemerken, daß wir die gleiche Formel (8) erhalten hätten, wenn unsere Funktion D nur den ersten beiden Axiomen genügte.

Aus (8) lassen sich viele Folgerungen ziehen.

Zunächst setzen wir die Gültigkeit des Axioms 3 voraus und spezialisieren die A_k zu den Einheitsvektoren U_k. Dann ist $A'_k = B_k$, wobei B_k der Spaltenvektor der Matrix b_{ik} ist. Gleichung (8) ergibt:

$$D(B_1, B_2, \ldots, B_n) = \sum_{(\nu_1, \nu_2, \ldots, \nu_n)} \pm b_{\nu_1 1} \cdot b_{\nu_2 2} \cdot \ldots \cdot b_{\nu_n n}. \tag{9}$$

Dies ist eine explizite Formel für Determinanten, welche zeigt, daß Determinanten durch unsere Axiome eindeutig bestimmt sind, falls sie überhaupt existieren. Formel (9) erlaubt es uns, Formel (8) in folgender Weise zu schreiben:

$$D(A'_1, A'_2, \ldots, A'_n) = D(A_1, A_2, \ldots, A_n)\, D(B_1, B_2, \ldots, B_n). \tag{10}$$

Dies ist der sogenannte *Multiplikationssatz für Determinanten*. Auf der linken Seite von (10) steht nämlich die Determinante einer n-reihigen quadratischen Matrix mit den Elementen

$$c_{ik} = \sum_{\nu=1}^{n} a_{i\nu} b_{\nu k}. \tag{11}$$

Die c_{ik} ergeben sich durch Multiplikation der Elemente der i-ten Zeile von $D(A_1, A_2, \ldots, A_n)$ mit den entsprechenden Elementen der k-ten Spalte von $D(B_1, B_2, \ldots, B_n)$ und anschließende Addition der so gewonnenen Produkte.

Nun wollen wir D in (8) durch eine Funktion $F(A_1, A_2, \ldots, A_n)$ ersetzen, die nur den ersten beiden Axiomen genügt. Durch Vergleich mit (9) erhalten wir

$$F(A'_1, A'_2, \ldots, A'_n) = F(A_1, A_2, \ldots, A_n)\, D(B_1, B_2, \ldots, B_n).$$

Setzen wir A_k speziell gleich dem Einheitsvektor U_k, so ergibt sich

$$F(B_1, B_2, \ldots, B_n) = c \cdot D(B_1, B_2, \ldots, B_n) \tag{12}$$

mit

$$c = F(U_1, U_2, \ldots, U_n).$$

Nun spezialisieren wir (10) wie folgt: Ist i ein bestimmter Index zwischen 1 und $n-1$, so setzen, wir $A_k = U_k$ für $k \neq i,\ i+1$, $A_i = U_i + U_{i+1}$, $A_{i+1} = 0$. Dann ist $D(A_1, A_2, \ldots, A_n) = 0$, denn eine Spalte ist 0. Also ist auch $D(A'_1, A'_2, \ldots, A'_n) = 0$; aber diese Determinante unterscheidet sich von der aus den Elementen b_{jk} gebildeten nur in der $(i+1)$-ten Zeile, die jetzt gleich der i-ten ist. Wir sehen daher:

Eine Determinante verschwindet, wenn zwei benachbarte *Zeilen* gleich sind.

Jeder Summand in (9) ist ein Produkt, in dem genau ein Faktor aus einer bestimmten Zeile, etwa der i-ten, stammt. Das zeigt, daß eine Determinante linear und homogen ist, wenn man sie als Funktion dieser Zeile auffaßt. Wählen wir schließlich für jede Zeile den entsprechenden Einheitsvektor, so ist die Determinante $= 1$; denn die Matrix hat auch als Spaltenvektoren die Einheitsvektoren. Somit genügt eine Determinante unseren drei Axiomen, wenn wir sie als Funktion ihrer Zeilenvektoren auffassen. Auf Grund der bereits bewiesenen Eindeutigkeit von Determinanten folgt:

Eine Determinante bleibt ungeändert, wenn wir die Zeilenvektoren in Spaltenvektoren transponieren, d.h., wenn wir die Matrix an ihrer Hauptdiagonale spiegeln.

Eine Determinante verschwindet, wenn irgend zwei Zeilen gleich sind. Sie ändert ihr Vorzeichen, wenn wir zwei Zeilen vertauschen. Sie bleibt ungeändert, wenn wir ein Vielfaches einer Zeile zu einer anderen addieren.

Nun wollen wir die Existenz der Determinanten nachweisen. Für eine einzeilige Matrix a_{11} ist das Element a_{11} selbst die Determinante. Es werde die Existenz $(n-1)$-reihiger Determinanten vorausgesetzt. Betrachten wir eine n-reihige Matrix (1), so können wir dieser gewisse $(n-1)$-reihige Determinanten wie folgt zuordnen: Es sei a_{ik} ein spezielles Element in (1). Wir streichen die i-te Zeile und die k-te Spalte in (1) und betrachten die Determinante der übriggebliebenen $(n-1)$-reihigen Matrix. Diese Determinate, mit $(-1)^{i+k}$ multipliziert, nennen wir das algebraische Komplement zu a_{ik} und bezeichnen es mit A_{ik}. Die Verteilung des Vorzeichens $(-1)^{i+k}$ folgt der Schachbrettanordnung, nämlich

$$\begin{pmatrix} + & - & + & - & \cdots \\ - & + & - & + & \cdots \\ + & - & + & - & \cdots \\ - & + & - & + & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots \end{pmatrix}.$$

Es sei i irgendeine Zahl zwischen 1 und n. Wir betrachten folgende Funktion D der Matrix (1):

$$D = a_{i1}A_{i1} + a_{i2}A_{i2} + \cdots + a_{in}A_{in}. \tag{13}$$

Sie ist die Summe der Produkte der i-ten Zeile und ihrer algebraischen Komplemente.

Dieses D betrachten wir in seiner Abhängigkeit von einer gegebenen Spalte, etwa A_k. Für $\nu \neq k$ hängt $A_{i\nu}$ linear von A_k ab, während $a_{i\nu}$ nicht von A_k abhängig ist. Für $\nu = k$ hängt A_{ik} nicht von A_k ab, aber a_{ik} ist ein Element dieser Spalte. Somit ist Axiom 1 erfüllt. Nun wollen wir annehmen, daß zwei benachbarte Spalten A_k und A_{k+1} gleich sind. Für $\nu \neq k, k+1$, haben wir zwei gleiche Spalten in $A_{i\nu}$, so daß $A_{i\nu} = 0$ ist. Die Determinanten, die bei der Berechnung von $A_{i,k}$ und $A_{i,k+1}$ benutzt wurden, sind dieselben, doch sind die Vorzeichen der Schachbrettanordnung entgegengesetzt; demnach gilt $A_{i,k} = -A_{i,k+1}$, wohingegen $a_{i,k} = a_{i,k+1}$ ist. Somit ist $D = 0$ und das Axiom 2 erfüllt. Für den Spezialfall $A_\nu = U_\nu$ $(\nu = 1, 2, \ldots, n)$ haben wir $a_{i\nu} = 0$ für $\nu \neq i$, während $a_{ii} = 1$ und $A_{ii} = 1$ ist. Es ergibt sich $D = 1$, und somit Axiom 3. Damit ist sowohl die Existenz einer n-reihigen Determinante als auch die Richtigkeit der Formel (13), der sogenannten Entwicklung einer Determinante nach ihrer i-ten Zeile, bewiesen. Die Formel (13) läßt sich wie folgt verallgemeinern: In unserer Determinante ersetze man die i-te Zeile durch die j-te Zeile und entwickele nach dieser neuen Zeile. Für $i \neq j$ ist diese Determinante 0, für $i = j$ ist sie D:

$$a_{j1}A_{i1} + a_{j2}A_{i2} + \cdots + a_{jn}A_{in} = \begin{cases} D & \text{für } j = i \\ 0 & \text{für } j \neq i\,. \end{cases} \tag{14}$$

Vertauschen wir Zeilen und Spalten, so erhalten wir die Formel

$$a_{1h}A_{1k} + a_{2h}A_{2k} + \cdots + a_{nh}A_{nk} = \begin{cases} D & \text{für } h = k \\ 0 & \text{für } h \neq k\,. \end{cases} \tag{15}$$

Nun möge A eine n-reihige und B eine m-reihige quadratische Matrix darstellen. Mit $|A|$ bzw. $|B|$ wollen wir deren Determinanten bezeichnen. Ferner sei C eine Matrix mit n Zeilen und m Spalten. Wir bilden die quadratische $(n+m)$-reihige Matrix

$$\begin{pmatrix} A & C \\ 0 & B \end{pmatrix}, \tag{16}$$

wobei die 0 eine Nullmatrix mit m Zeilen und n Spalten bedeuten soll. Fassen wir die Determinante der Matrix (16) als Funktion der Spalten von A allein auf, so genügt sie offenbar unseren ersten beiden Axiomen. Wegen (12) ist ihr Wert $c \cdot |A|$, wobei c die Determinante

von (16) nach Einsetzen der Einheitsvektoren an die Stelle der Spalten von A ist. Dieses c ist noch von B abhängig und genügt, als Funktion der Zeilen von B aufgefaßt, den ersten beiden Axiomen. Deshalb ist die Determinante von (16) gleich $d \cdot |A| \cdot |B|$, worin d der Spezialfall der Determinante von (16) ist, worin für die Spalten von A und B die Einheitsvektoren eingesetzt sind. Subtrahieren wir passende Vielfache der ersten n Spalten dieser neuen Determinante von den letzten m Spalten, so kann man C durch 0 ersetzen. Dies ergibt $d = 1$ und damit die Formel

$$\begin{vmatrix} A & C \\ 0 & B \end{vmatrix} = |A| \cdot |B|. \tag{17}$$

In ähnlicher Weise hätten wir auch die Formel

$$\begin{vmatrix} A & 0 \\ C & B \end{vmatrix} = |A| \cdot |B| \tag{18}$$

beweisen können.

Die Formeln (17) und (18) sind Spezialfälle eines allgemeinen Satzes von Lagrange, der sich andererseits aus unseren Spezialfällen ableiten läßt. Wir verweisen den Leser auf ein beliebiges Lehrbuch über Determinanten; denn für die meisten Anwendungen sind (17) und (18) ausreichend.

Wir untersuchen nun, was es für eine Matrix bedeutet, wenn ihre Determinante Null ist. Die folgenden Tatsachen lassen sich leicht beweisen:

a) Sind $A_1, A_2, \ldots, A_n$ linear abhängig, so ist $D(A_1, A_2, \ldots, A_n) = 0$. In der Tat, eine der Spalten, etwa A_k, ist dann eine Linearkombination der anderen Spalten. Subtrahieren wir diese Linearkombination von der Spalte A_k, so wird sie 0, und somit ist $D = 0$.

b) Die Vektoren $A_1, A_2, \ldots, A_n$ seien linear unabhängig. Dann sind sie ein Erzeugendensystem des Raumes K^n aller Spalten, und man kann in Gleichung (6) die b_{ik} so wählen, daß $A'_k = U_k$ wird. Verwendet man diese Werte von b_{ik} in Formel (8), so wird die linke Seite von (8) gleich 1, es muß also $D(A_1, A_2, \ldots, A_n) \neq 0$ sein.

Diese Ergebnisse verbinden wir nun und erhalten:

Eine Determinante verschwindet dann und nur dann, wenn ihre Spaltenvektoren (oder Zeilenvektoren) *linear* abhängig sind.

Eine andere Formulierung dieser Ergebnisse lautet:

Das System von n linearen homogenen Gleichungen

$$a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{in}x_n = 0 \qquad (i = 1, 2, \ldots, n)$$

in n Unbekannten hat eine nicht-triviale Lösung dann und nur dann, wenn seine Koeffizientendeterminante Null ist.

Offenbar haben wir auch bewiesen:

Das System der linearen Gleichungen

$$a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{in}x_n = b_i \qquad (i = 1, 2, \ldots, n) \quad (19)$$

hat dann und nur dann für beliebige Werte b_i eine Lösung, wenn die Determinante der a_{ik} ungleich 0 ist.

Schließlich drücken wir die Lösung von (19) für den Fall, daß die Determinante D der a_{ik} von Null verschieden ist, durch Determinanten aus:

Die Gleichungen (19) bedeuten

$$A_1x_1 + A_2x_2 + \cdots + A_nx_n = B$$

Ersetzen wir die i-te Spalte in $D(A_1, A_2, \ldots, A_n)$ durch B, so deuten wir dies durch $D(A_1, \ldots, B, \ldots, A_n)$ an. Subtrahiert man Vielfache der A_ν für $\nu \neq i$ von der Spalte B, so bleibt $A_i x_i$ übrig.
Es gilt also

$$D(A_1, \ldots, B, \ldots, A_n) = x_i D(A_1, A_2, \ldots, A_n),$$

und folglich

$$x_i = \frac{D(A_1, \ldots, B, \ldots, A_n)}{D(A_1, A_2, \ldots, A_n)}.$$

Diese Formel ist als *Cramersche Regel* bekannt.

II. KÖRPERTHEORIE

A. Erweiterungskörper

Alle betrachteten Körper werden als kommutativ vorausgesetzt. Ist E ein Körper und K eine Teilmenge von E, die hinsichtlich der in E erklärten Addition und Multiplikation selbst einen Körper bildet, d. h., daß K ein Unterkörper von E ist, so nennen wir E eine *Erweiterung* von K. Die Beziehung, daß E Erweiterung von K ist, wollen wir kurz durch $K < E$ bezeichnen. Sind $\alpha, \beta, \gamma, \ldots$ Elemente von E, so verstehen wir unter $K(\alpha, \beta, \gamma, \ldots)$ die Menge der Elemente in E,

die sich als Quotienten von Polynomen in den $\alpha, \beta, \gamma, \ldots$ mit Koeffizienten aus K ausdrücken lassen. Offenbar ist $K(\alpha, \beta, \gamma, \ldots)$ die kleinste Erweiterung von K, die die Elemente $\alpha, \beta, \gamma, \ldots$ enthält. Wir nennen $K(\alpha, \beta, \gamma, \ldots)$ den durch *Adjunktion* der Elemente $\alpha, \beta, \gamma, \ldots$ zu K gewonnenen bzw. *erzeugten* Körper.

Ist $K < E$, so können wir E als einen Vektorraum über K auffassen, indem wir die für den Vektorraum benötigten Operationen mit den in E definierten Operationen identifizieren. Unter dem *Grad* von E über K, in Zeichen (E/K), verstehen wir die Dimension des Vektorraumes E über K. Bei endlichem (E/K) sprechen wir von einer *endlichen Körpererweiterung*.

Satz 6. *Sind K, B, E drei Körper derart, daß $K < B < E$ gilt, so ist*

$$(E/K) = (B/K)(E/B).$$

Beweis. Es seien $A_1, A_2, \ldots, A_r$ Elemente von E, die über B linear unabhängig sind, und $C_1, C_2, \ldots, C_s$ Elemente von B, die über K linear unabhängig sind. Dann sind die Produkte $C_i A_j$ mit $i = 1, 2, \ldots, s$ und $j = 1, 2, \ldots, r$ Elemente von E, welche linear unabhängig über K sind. Denn ist $\sum_{i,j} a_{ij} C_i A_j = 0$, so ist $\sum_j \left(\sum_i a_{ij} C_i \right) A_j$ eine Linearkombination der A_j mit Koeffizienten aus B, und da die A_j hinsichtlich B unabhängig waren, erhalten wir $\sum_i a_{ij} C_i = 0$ für jedes j. Die lineare Unabhängigkeit der C_i bezüglich K ergibt dann aber, daß sämtliche $a_{ij} = 0$ sind. Da es aber $r \cdot s$ Elemente $C_i A_j$ gibt, haben wir damit für jedes $r \leqq (E/B)$ und jedes $s \leqq (B/K)$ gezeigt, daß der Grad $(E/K) \geqq r \cdot s$ ist. Daher ist $(E/K) \geqq (B/K)(E/B)$. Ist eine der letzten beiden Zahlen unendlich, so ist der Satz damit bereits bewiesen. Sind beide (E/B) und (B/K) endlich, etwa gleich r bzw. s, so können wir annehmen, daß die A_j bzw. C_i Erzeugendensysteme der Vektorräume E bzw. B sind. Wir wollen zeigen, daß die Menge der Produkte $C_i A_j$ ein Erzeugendensystem von E über K ist. Jedes A von E läßt sich linear durch die A_j mit Koeffizienten aus B ausdrücken. Somit ist $A = \sum B_j A_j$. Nunmehr kann jedes B_j als Element von B linear durch die C_i mit Koeffizienten aus K ausgedrückt werden, d.h., es gilt $B_j = \sum_i a_{ij} C_i$, $j = 1, 2, \ldots, r$. Es ist also $A = \sum a_{ij} C_i A_j$, und die $C_i A_j$ bilden ein unabhängiges Erzeugendensystem von E über K.

Folgerung. *Ist $K < K_1 < K_2 < \cdots < K_n$, so ist*
$(K_n/K) = (K_1/K) \cdot (K_2/K_1) \cdot \cdots \cdot (K_n/K_{n-1})$.

B. Polynome

Einen Ausdruck der Form $a_0 x^n + a_1 x^{n-1} + \cdots + a_n$ nennt man ein *Polynom* in K vom Grade n, wenn die Koeffizienten $a_0, \ldots, a_n$ Elemente des Körpers K sind und $a_0 \neq 0$ ist. Die Multiplikation und Addition der Polynome erfolgt in der üblichen Weise[1]).

Ein Polynom in K nennt man *reduzibel* in K, wenn es als Produkt zweier Polynome positiven Grades in K geschrieben werden kann. Nicht konstante Polynome, die in K nicht reduzibel sind, nennt man *irreduzibel* in K.

Genügen die Polynome $f(x)$, $g(x)$ und $h(x)$ des Körpers K einer Gleichung $f(x) = g(x) \cdot h(x)$, so sagen wir $g(x)$ teilt $f(x)$ bzw. $g(x)$ ist ein Faktor von $f(x)$. Man erkennt leicht, daß der Grad von $f(x)$ gleich der Summe der Grade von $g(x)$ und von $h(x)$ ist. Sollte weder $g(x)$ noch $h(x)$ eine Konstante sein, so haben beide einen kleineren Grad als $f(x)$. Daraus folgt, daß ein Polynom sich stets als Produkt endlich vieler im Körper K irreduzibler Polynome ausdrücken läßt.

Für zwei beliebige Polynome $f(x)$ und $g(x)$ gilt der Divisionsalgorithmus, d.h., es ist $f(x) = q(x) \cdot g(x) + r(x)$, wobei $q(x)$ und $r(x)$ eindeutig bestimmte Polynome in K sind und der Grad von $r(x)$ kleiner ist als der von $g(x)$. Dies läßt sich nach der gleichen Methode zeigen, wie sie dem Leser in der elementaren Algebra im Falle des Körpers der reellen oder komplexen Zahlen begegnet ist. Wir sehen auch, daß $r(x)$ das einzige Polynom mit kleinerem Grad als der von $g(x)$ ist, für das $f(x) - r(x)$ durch $g(x)$ teilbar ist. Wir nennen $r(x)$ den Rest von $f(x)$ modulo $g(x)$.

Auf dem üblichen Wege läßt sich ferner zeigen, daß $x - \alpha$ dann und nur dann ein Faktor von $f(x)$ ist ,wenn α eine Wurzel von $f(x)$, wenn also $f(\alpha) = 0$ ist. Daraus ergibt sich leicht, daß ein Polynom aus einem Körper nicht mehr Wurzeln in diesem Körper haben kann, als sein Grad beträgt.

Hilfssatz. *Ist $f(x)$ ein irreduzibles Polynom vom Grade n in K, so gibt es in K keine zwei von Null verschiedenen Polynome, deren Grad kleiner als n ist und deren Produkt durch $f(x)$ teilbar wäre.*

Wir wollen im Gegensatz zu unserer Behauptung annehmen, $g(x)$ und $h(x)$ seien Polynome vom Grade kleiner als n, deren Produkt

---

[1]) Sprechen wir von der Menge aller Polynome vom Grade kleiner als n, so wollen wir auch das Polynom 0 in diese Menge mit einbeziehen, obwohl es keinen Grad in dem üblichen Sinne besitzt.

durch $f(x)$ teilbar ist. Unter allen Möglichkeiten für solche Polynome $g(x)$ und $h(x)$ wähle man überdies $g(x)$ von möglichst kleinem Grad. Dann gibt es, da $f(x)$ ein Faktor von $g(x) \cdot h(x)$ ist, ein Polynom $k(x)$, mit welchem

$$k(x) \cdot f(x) = g(x) \cdot h(x)$$

gilt. Auf Grund des Divisionsalgorithmus ist

$$f(x) = q(x) \cdot g(x) + r(x),$$

wobei der Grad von $r(x)$ kleiner ist als der von $g(x)$. Überdies muß $r(x) \neq 0$ sein, da $f(x)$ irreduzibel ist. Durch Multiplikation dieser Gleichung mit $h(x)$ und anschließender Umformung erhalten wir

$$r(x) \cdot h(x) = f(x) \cdot h(x) - q(x) \cdot g(x) \cdot h(x) = f(x) \cdot h(x) - q(x) \cdot k(x) \cdot f(x),$$

woraus folgt, daß $r(x) \cdot h(x)$ durch $f(x)$ teilbar ist. Dies aber steht in Widerspruch zu unserer Wahl von $g(x)$, denn der Grad von $r(x)$ ist kleiner als der von $g(x)$. Damit ist der Hilfssatz bewiesen.

Wie wir gesehen haben, gelten viele Sätze der elementaren Algebra auch in einem beliebigen Körper K. Der sogenannte Fundamentalsatz der Algebra jedoch verliert, wenigstens in seiner üblichen Form, die Gültigkeit. Er wird durch einen von Kronecker stammenden Satz ersetzt, der für ein gegebenes Polynom in K die Existenz eines Erweiterungskörpers gewährleistet, in dem das Polynom Wurzeln besitzt. Wir werden außerdem zeigen, daß in einem gegebenen Körper ein Polynom sich nicht nur in irreduzible Faktoren zerlegen läßt, sondern daß diese Zerlegung bis auf konstante Faktoren eindeutig ist. Diese Eindeutigkeit hängt mit dem Satz von Kronecker zusammen.

C. Algebraische Elemente

Es sei K ein Körper und E ein Erweiterungskörper von K. Ist dann α ein Element von E, so können wir danach fragen, ob es Polynome mit Koeffizienten in K gibt, die α zur Wurzel haben. Man nennt α *algebraisch über* K, wenn es von Null verschiedene derartige Polynome gibt Nun sei α algebraisch. Unter allen nicht verschwindenden Polynomen in K, welche α als Wurzel haben, wählen wir eines von kleinstem Grade aus und multiplizieren es mit einer geeigneten Konstanten aus K, so daß das erhaltene Polynom, das mit $f(x)$ bezeichnet werde, überdies den höchsten Koeffizienten 1 besitzt.

Von diesem Polynom $f(x)$ zeigen wir nun 3 Eigenschaften:

1. Wenn $g(x)$ ein Polynom in K mit $g(\alpha) = 0$ ist, so ist $g(x)$ durch $f(x)$ teilbar,

2. $f(x)$ ist irreduzibel,

3. $f(x)$ ist durch die bei seiner Konstruktion benutzten Eigenschaften eindeutig bestimmt.

In der Tat, wenn $g(x)$ ein Polynom in K mit $g(\alpha) = 0$ ist, so können wir schreiben $g(x) = f(x)q(x) + r(x)$, wobei der Grad von $r(x)$ kleiner ist als der von $f(x)$. Durch Einsetzen von $x = \alpha$ erhalten wir $r(\alpha) = 0$. Da $r(x)$ die Wurzel α hat und von kleinerem Grad als $f(x)$ ist, muß $r(x)$ das Nullpolynom sein. Also ist $g(x)$ durch $f(x)$ teilbar und Eigenschaft 1. gezeigt. Damit ist gleichzeitig auch die Eindeutigkeit von $f(x)$, also 3., nachgewiesen. Wäre ferner $f(x)$ in K zerlegbar, so müßte einer der Faktoren für $x = \alpha$ verschwinden, was wiederum der Wahl von $f(x)$ widerspricht. Damit ist auch 2. gezeigt.

Wir betrachten nun die Teilmenge E_0 folgender Elemente θ von E:

$$\theta = g(\alpha) = c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_{n-1}\alpha^{n-1}.$$

Hierbei ist $g(x)$ ein Polynom in K vom Grade kleiner als n (n ist der Grad von $f(x)$). Diese Menge E_0 ist additiv und multiplikativ abgeschlossen. Das letztere läßt sich wie folgt zeigen:

Sind $g(x)$ und $h(x)$ zwei Polynome vom Grade kleiner als n, so setzen wir $g(x)h(x) = q(x)f(x) + r(x)$ und erhalten $g(\alpha)h(\alpha) = r(\alpha)$. Schließlich sehen wir, daß die Konstanten $c_0, c_1, \ldots, c_{n-1}$ durch das Element θ eindeutig bestimmt sind. In der Tat, zwei Ausdrücke für das gleiche θ würden nach Subtraktion zu einer Gleichung für α von einem geringeren Grad als n führen.

Wir bemerken, daß die innere Struktur der Menge E_0 nicht von der Beschaffenheit von α, sondern lediglich von dem irreduziblen $f(x)$ abhängt. Die Kenntnis dieses Polynoms gestattet uns, die Addition und Multiplikation in unserer Menge E_0 auszuführen. Wir werden sehr bald sehen, daß E_0 ein Körper ist; in Wirklichkeit ist E_0 nichts anderes als der Körper $K(\alpha)$. Sobald dies gezeigt ist, haben wir auch den Grad $(K(\alpha)/K)$ bestimmt. Er muß gleich n sein, denn der Raum $K(\alpha)$ wird durch die linear unabhängigen Elemente $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ erzeugt.

Wir versuchen nun, die Menge E_0 auch in solchen Fällen nachzubilden, in denen uns ein Erweiterungskörper E und ein Element α

nicht zur Verfügung stehen. Lediglich das irreduzible Polynom

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$$

nehmen wir als gegeben an.

Wir wählen ein Symbol ξ. Ferner sei E_1 die Menge aller formalen Polynome

$$g(\xi) = c_0 + c_1\xi + \cdots + c_{n-1}\xi^{n-1}$$

vom Grade kleiner als n. Diese Menge bildet eine additive Gruppe. Wir führen nun neben der üblichen Multiplikation eine neue Art der Multiplikation zweier Elemente $g(\xi)$ und $h(\xi)$ von E_1 ein und schreiben dafür $g(\xi) \times h(\xi)$. Dieses so bezeichnete Produkt ist definiert als der Rest $r(\xi)$ des gewöhnlichen Produkts $g(\xi)h(\xi)$ modulo $f(\xi)$. Zunächst bemerken wir, daß ein beliebiges Produkt von m Faktoren $g_1(\xi), g_2(\xi), \ldots, g_m(\xi)$ wieder der Rest des gewöhnlichen Produkts $g_1(\xi)g_2(\xi)\ldots g_m(\xi)$ ist. Dies ist für $m = 2$ nach Definition richtig und folgt für jedes m durch Induktion, falls wir den folgenden leichten Hilfssatz beweisen:

Sind $r_1(\xi)$ und $r_2(\xi)$ die Reste zweier beliebiger Polynome $g_1(\xi)$ und $g_2(\xi)$, so haben die Produkte $g_1(\xi)g_2(\xi)$ und $r_1(\xi)r_2(\xi)$ denselben Rest. Der Beweis sei dem Leser überlassen. Diese Tatsache zeigt, daß unser neues Produkt assoziativ und kommutativ ist, und auch, daß das neue Produkt $g_1(\xi) \times g_2(\xi) \times \cdots \times g_m(\xi)$ mit dem alten Produkt $g_1(\xi)g_2(\xi)\ldots g_m(\xi)$ übereinstimmt, falls der Grad des letzteren n nicht erreicht. Die Distributivität unserer neuen Multiplikation läßt sich ebenfalls leicht verifizieren.

Die Menge E_1 enthält unseren Körper K, und unsere Multiplikation in E_1 hat für K die Bedeutung der alten Multiplikation. Eines der Polynome von E_1 ist ξ. Multiplizieren wir dieses i-mal mit sich selbst, so erhalten wir offenbar ξ^i, solange nur $i < n$ ist. Für $i = n$ aber muß man den Rest des Polynoms ξ^n berechnen. Er ergibt sich zu

$$\xi^n - f(\xi) = -a_{n-1}\xi^{n-1} - a_{n-2}\xi^{n-2} - \cdots - a_0.$$

Wir geben nun unsere alte Multiplikation insgesamt auf und behalten nur die neue bei. Desgleichen ändern wir die Bezeichnungsweise, indem wir den Punkt (oder die Nebeneinanderstellung) als Symbol für die neue Multiplikation verwenden.

In diesem Sinne berechnen wir

$$c_0 + c_1\xi + c_2\xi^2 + \cdots + c_{n-1}\xi^{n-1}.$$

Dies führt leicht zu dem genau so bezeichneten Element, denn alle benötigten Grade liegen unterhalb n. Doch gilt

$$\xi^n = -a_{n-1}\xi^{n-1} - a_{n-2}\xi^{n-2} - \cdots - a_0,$$

also $f(\xi) = 0$.

Wir haben somit eine Menge E_1 sowie eine Addition und Multiplikation in E_1 konstruiert, die bereits den meisten Körperaxiomen genügt. E_1 enthält K als Unterkörper, und ξ genügt der Gleichung $f(\xi) = 0$. Als nächstes müssen wir zeigen: Wenn $g(\xi) \neq 0$ und $h(\xi)$ gegebene Elemente von E_1 sind, dann gibt es auch ein Element

$$X(\xi) = x_0 + x_1\xi + \cdots + x_{n-1}\xi^{n-1}$$

in E_1, für welches

$$g(\xi) \cdot X(\xi) = h(\xi)$$

gilt. Um dies zu beweisen, fassen wir die Koeffizienten x_i von $X(\xi)$ als Unbekannte auf und berechnen das Produkt auf der linken Seite, wobei wir die höheren als $(n-1)$-ten Potenzen von ξ mit Hilfe der Gleichung $f(\xi) = 0$ reduzieren. Das ergibt einen Ausdruck $L_0 + L_1\xi + \cdots + L_{n-1}\xi^{n-1}$, wobei jedes L_i eine Linearkombination der x_i mit Koeffizienten aus K ist. Weil dieser Ausdruck gleich $h(\xi)$ sein soll, erhält man n Gleichungen mit n Unbekannten

$$L_0 = b_0, \quad L_1 = b_1, \ldots, L_{n-1} = b_{n-1},$$

wobei die b_i die Koeffizienten von $h(\xi)$ sind. Dieses System ist lösbar, falls die entsprechenden homogenen Gleichungen

$$L_0 = 0, \quad L_1 = 0, \ldots, L_{n-1} = 0$$

nur die triviale Lösung besitzen.

Diese homogenen Gleichungen treten auf, wenn wir nach denjenigen Elementen $X(\xi)$ fragen, für die $g(\xi) \cdot X(\xi) = 0$ ist. Gehen wir für den Augenblick zur alten Multiplikation zurück, so bedeutet dies, daß das gewöhnliche Produkt $g(\xi)X(\xi)$ den Rest 0 hat und daher durch $f(\xi)$ teilbar ist. Nach dem auf Seite 18 bewiesenen Hilfssatz ist dies aber nur für $X(\xi) = 0$ möglich.

E_1 ist daher ein Körper.

Nun nehmen wir an, wir hätten außerdem unsere alte Erweiterung E, in der eine Wurzel α von $f(x)$ liegt, und demnach auch die dazugehörige Menge E_0. Wir sehen, daß E_0 in einem gewissen Sinne die gleiche Struktur hat wie E_1, wenn wir das Element $g(\xi)$ von E_1 auf das Element $g(\alpha)$ von E_0 abbilden. Diese Abbildung hat die Eigen-

schaft, daß das Bild einer Summe von Elementen die Summe der Bilder und das Bild des Produkts ebenfalls das Produkt der Bilder der einzelnen Elemente ist.

Diese Abbildung legt uns nahe, ganz allgemein Abbildungen σ eines Körpers K in einen anderen Körper K' zu betrachten, bei denen jedem Element α von K ein Bildelement $\sigma(\alpha)$ von K' zugeordnet wird. Diese Abbildungen sollen folgende Eigenschaften haben:

1. $\sigma(\alpha+\beta)=\sigma(\alpha)+\sigma(\beta)$
2. $\sigma(\alpha\beta)=\sigma(\alpha)\sigma(\beta)$

für alle Elemente α, β von K.

Sollte es ein $\alpha \neq 0$ geben, für das $\sigma(\alpha)=0$ ist, so folgt wegen 2. für jedes β:

$$\sigma(\beta)=\sigma(\alpha\cdot\alpha^{-1}\beta)=\sigma(\alpha)\cdot\sigma(\alpha^{-1}\beta)=0\cdot\sigma(\alpha^{-1}\beta)=0,$$

und wir sehen, daß ganz K auf 0 abgebildet wird. Da diese Abbildung sicher ohne Interesse ist, fordern wir weiter

3. Aus $\alpha \neq 0$ folgt $\sigma(\alpha) \neq 0$.

Setzt man in 1. $\alpha=0$, so folgt $\sigma(\beta)=\sigma(0)+\sigma(\beta)$ und somit $\sigma(0)=0$. Ersetzt man nunmehr in 1. β durch $-\alpha$, so folgt $0=\sigma(\alpha)+\sigma(-\alpha)$ oder $\sigma(-\alpha)=-\sigma(\alpha)$, so daß auch die Regel $\sigma(\alpha-\beta)=\sigma(\alpha)-\sigma(\beta)$ gilt. Setzt man in 2. $\alpha=\beta=1$ und beachtet man, daß wegen 3. $\sigma(1)\neq 0$ sein muß, so folgt $\sigma(1)=1$. Setzt man $\beta=\alpha^{-1}$, so zeigt 2., daß $\sigma(\alpha^{-1})=(\sigma(\alpha)^{-1})$ ist, und es folgt nunmehr die Regel $\sigma\left(\frac{\alpha}{\beta}\right)=\frac{\sigma(\alpha)}{\sigma(\beta)}$. Schließlich folgt aus $\sigma(\alpha)=\sigma(\beta)$, daß $\sigma(\alpha-\beta)=0$ ist, und 3. zeigt, daß $\alpha=\beta$ sein muß. σ ist daher eine eineindeutige Abbildung von K in K', die alle Rechnungsarten erhält, und eine solche Abbildung soll als *Isomorphismus* von K *in* K' bezeichnet werden. Die Menge aller Bilder ist ein Teilkörper von K'.

Sollte die Abbildung σ den Körper K überdies auf den ganzen Körper K' abbilden, so werde sie ein Isomorphismus von K *auf* K' genannt. Wenn σ ein Isomorphismus von K auf K' ist, so kann man auch die inverse Abbildung σ^{-1} von K' zurück auf K betrachten, und man sieht leicht, daß sie ein Isomorphismus von K' auf K ist. Wenn ein Isomorphismus von K auf K' existiert, so sagt man auch, K und K' seien isomorph.

In diesen Definitionen ist es keineswegs ausgeschlossen, daß K' derselbe Körper wie K ist. Sollte σ eine isomorphe Abbildung von K auf sich selbst sein, so werde σ ein *Automorphismus* von K genannt

Dann ist auch σ^{-1} ein Automorphismus von K. Zum Beispiel ist die identische Abbildung von K auf sich selbst ein Automorphismus von K.

Aus diesen Definitionen ergibt sich nunmehr, daß die Menge E_0 auch ein Körper ist und daß E_0 und E_1 isomorph sind.

Es sei σ ein Isomorphismus von K auf K', und es werde das Bild $\sigma(a)$ eines Elementes a von K kurz mit a' bezeichnet. Wir dehnen die Abbildung σ auf Polynome $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ von K aus, indem wir als Bild $f'(x)$ von $f(x)$ das Polynom

$$f'(x) = a_0' + a_1' x + \cdots + a_n' x^n$$

definieren. Man sieht leicht, daß die beiden Gleichungen

$$(f(x) + g(x))' = f'(x) + g'(x)$$
$$(f(x)\, g(x))' = f'(x)\, g'(x)$$

gelten.

Ebenso leicht kann man erkennen, daß das Bild $f'(x)$ eines in K irreduziblen Polynoms $f(x)$ ein in K' irreduzibles Polynom ist.

Nun wollen wir einige Sätze formulieren, die sich aus unseren Betrachtungen ergeben.

Satz 7. (*Kronecker*). *Ist $f(x)$ ein nicht konstantes Polynom in einem Körper K, so existiert eine Erweiterung E von K, in der $f(x)$ eine Wurzel besitzt.*

Beweis: Wir konstruieren einen Erweiterungskörper, in dem ein irreduzibler Faktor von $f(x)$ eine Wurzel besitzt.

Satz 8. *Es sei σ eine isomorphe Abbildung eines Körpers K auf einen Körper K'. Ferner sei $f(x)$ ein in K irreduzibles Polynom und $f'(x)$ das entsprechende Bildpolynom in K'. Sind dann $E = K(\beta)$ und $E' = K'(\beta')$ Erweiterungen von K bzw. K', wobei $f(\beta) = 0$ in E und $f'(\beta') = 0$ in E' ist, so läßt sich σ zu einem Isomorphismus zwischen E und E' erweitern, bei dem β' das Bild von β ist.*

Beweis: Jedes Element θ von E hat die Form $\theta = g(\beta)$, wobei $g(x)$ ein Polynom in K ist, dessen Grad kleiner ist als der Grad von $f(x)$. Man ordne nun dem Element θ das Element $g'(\beta')$ als Bild zu. Diese Abbildung ist offenbar eine Erweiterung der gegebenen Abbildung σ und bildet E auf E' ab. Daß dabei die Summe zweier Elemente in die Summe übergeht, ist klar. Auch für das Produkt gilt die entsprechende Regel, denn $g(\beta)\, h(\beta) = r(\beta)$ bedeutet, daß $r(x)$ der Rest von $g(x)\, h(x)$ modulo $f(x)$ ist. Es gibt also ein Polynom $q(x)$,

so daß $g(x)h(x) = q(x)f(x) + r(x)$ ist. Geht man zu den Bildern der Polynome über, so folgt $g'(x)h'(x) = q'(x)f'(x) + r'(x)$, so daß für $x = \beta'$ gilt $g'(\beta')h'(\beta') = r'(\beta')$.

Satz 8 zeigt mit besonderer Deutlichkeit, daß der durch eine Wurzel einer irreduziblen Gleichung erzeugte Erweiterungskörper seiner Struktur nach nicht von der speziellen Natur dieser Wurzel abhängt.

D. Zerfällungskörper

Sind K, B und E drei Körper derart, daß $K \subset B \subset E$ gilt, so nennen wir B einen *Zwischenkörper*.

Es sei $p(x)$ ein Polynom in K und E ein Erweiterungskörper von K, in dem sich $p(x)$ in lauter Linearfaktoren zerlegen läßt. Eine solche lineare Zerlegung kann offenbar immer in der Form

$$p(x) = a(x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_s)$$

geschrieben werden. Dabei ist a offenbar der höchste Koeffizient von $p(x)$, gehört also zu K.

Ein Unterkörper von E, in dem die Zerlegung möglich ist, muß offenbar die Wurzeln $\alpha_1, \ldots, \alpha_s$ von $p(x)$ enthalten. Es ergibt sich, daß der kleinste Zwischenkörper, in dem unsere Zerlegung möglich ist, der Körper $K(\alpha_1, \alpha_2, \ldots, \alpha_s)$ ist. Dieser Körper werde *Zerfällungskörper* von $p(x)$ über K genannt oder, wenn kein Mißverständnis zu befürchten ist, Zerfällungskörper von $p(x)$.

Die Existenz von Zerfällungskörpern wird durch folgende Überlegung gesichert. Auf Grund von Satz 7 kann man K zunächst so erweitern, daß eine Zerlegung $p(x) = (x - \alpha_1)p_1(x)$ möglich ist. Wiederholt man dieses Verfahren mit dem Polynom $p_1(x)$, so gelangt man schließlich zu einem Erweiterungskörper von K, in dem $p(x)$ in Linearfaktoren zerfällt. Wir können daher aussprechen

Satz 9. *Ist $p(x)$ ein Polynom in einem Körper K, so existiert ein Zerfällungskörper E von $p(x)$.*

Zum Zerfällungskörper $E = K(\alpha_1, \alpha_2, \ldots, \alpha_s)$ kann man in einer endlichen Körperkette aufsteigen: $K = E_0 \subset E_1 \subset \cdots \subset E_s = E$, wobei $E_i = K(\alpha_1, \alpha_2, \ldots, \alpha_i) = E_{i-1}(\alpha_i)$ ist. Da $p(\alpha_i) = 0$ und $p(x)$ natürlich auch ein Polynom von E_{i-1} ist, ist α_i algebraisch über E_{i-1}. Der Grad (E_i/E_{i-1}) ist daher endlich, und folglich ist auch der Grad (E/K) des Zerfällungskörpers von $p(x)$ endlich.

Der nachstehende Satz zeigt unter anderem, daß der Zerfällungskörper eines Polynoms bis auf Isomorphismen eindeutig bestimmt ist.

Satz 10. *Es sei σ ein Isomorphismus, der den Körper K auf den Körper K' abbildet. Ferner sei $p(x)$ ein Polynom in K und $p'(x)$ das Bildpolynom in K'. Schließlich sei E ein Zerfällungskörper von $p(x)$ und E' ein Zerfällungskörper von $p'(x)$. Dann läßt sich der Isomorphismus σ zu einem Isomorphismus zwischen E und E' erweitern.*

Beweis: Es sei $p(x) = a(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_s)$ die Zerlegung von $p(x)$ in E. Sollten alle α_i zu K gehören, also $E = K$ sein, so kann man σ auf diese Zerlegung direkt anwenden und erhält eine Zerlegung von $p'(x)$ in K'. Es ist also $E' = K'$ und der Satz in diesem Falle bewiesen.

Wir führen nun eine Induktion nach der Anzahl n der *nicht* in K gelegenen α_i durch. Wir können dabei $n > 1$ voraussetzen und annehmen, daß der Satz in allen Fällen bewiesen ist, in denen die Anzahl der Wurzeln außerhalb K kleiner als n ist. Es sei etwa α_1 nicht in K gelegen und $f(x)$ das in K irreduzible Polynom mit der Wurzel α_1. Da $p(\alpha_1) = 0$ ist, gilt eine Zerlegung $p(x) = f(x)g(x)$, woraus auch $p'(x) = f'(x)g'(x)$ folgt. Nun sei $p'(x) = a'(x-\beta_1)(x-\beta_2)\ldots(x-\beta_s)$ die Zerlegung von $p'(x)$ in E'. In einem Erweiterungskörper von E' hat $f'(x)$ eine Wurzel γ, und es gilt $p'(\gamma) = 0$; also ist $a'(\gamma-\beta_1)(\gamma-\beta_2)\ldots(\gamma-\beta_s) = 0$. Daraus folgt, daß eines der β_i, etwa β_1, unsere Wurzel γ von $f'(x)$ ist. Auf Grund von Satz 8 kann der Isomorphismus σ zu einem Isomorphismus τ von $K(\alpha_1)$ auf $K'(\beta_1)$ erweitert werden. Man betrachte nun das Polynom $p(x)$ in $K(\alpha_1)$ und das Polynom $p'(x)$ (es ist das Bild von $p(x)$ unter τ) in $K'(\beta_1)$. E ist der Zerfällungskörper von $p(x)$ über $K(\alpha_1)$ und E' derjenige von $p'(x)$ über $K'(\beta_1)$. Die Anzahl der Wurzeln, die $p(x)$ in $K(\alpha_1)$ hat, ist mindestens um Eins größer als die Anzahl der Wurzeln von $p(x)$, die in K liegen. Daher ist die Anzahl der Wurzeln, die nicht in $K(\alpha_1)$ liegen, kleiner als n. Nach Induktionsannahme läßt sich also τ zu einem Isomorphismus von E auf E' erweitern, und das ist offenbar auch eine Erweiterung von σ.

Folgerung. *Ist $p(x)$ ein Polynom in einem Körper K, so sind zwei beliebige Zerfällungskörper von $p(x)$ einander isomorph.*

Dies folgt aus Satz 10, wenn wir $K = K'$ setzen und für σ die identische Abbildung, d. h. $\sigma(x) = x$ nehmen.

Auf Grund dieser Folgerung sind wir berechtigt, einfach den Terminus „Zerfällungskörper von $p(x)$" zu verwenden, da zwei beliebige Zerfällungskörper von $p(x)$ isomorph sind. Sollte $p(x)$ in einem Zerfällungskörper mehrfache Wurzeln haben, so gilt das auch in jedem anderen Zerfällungskörper. Die Aussage „$p(x)$ hat mehrfache Wurzeln", ist also vom Zerfällungskörper unabhängig.

Die Bedeutung der bewiesenen Eindeutigkeitssätze wird dem Leser klar werden, wenn er den speziellen Fall betrachtet, in welchem K der Körper der rationalen Zahlen ist. Wenn $p(x)$ ein in diesem Körper irreduzibles Polynom ist, und wir suchen nach einem Erweiterungskörper $K(\alpha)$, so daß $p(\alpha) = 0$ ist, so stehen uns zwei Methoden zur Konstruktion eines solchen Körpers zur Verfügung. Die erste Methode ist die abstrakte in C beschriebene, die zweite folgt aus dem sogenannten Fundamentalsatz der Algebra, auf Grund dessen man eine komplexe Zahl α' finden kann, so daß $p(\alpha') = 0$ ist. Diese zweite Methode ist radikal von der ersten verschieden, denn bei der Konstruktion von α' werden Limiten und andere Hilfsmittel der Analysis herangezogen. Auf Grund von Satz 8 wissen wir aber, daß die beiden Körper $K(\alpha)$ und $K(\alpha')$ isomorph sind. Ähnliche Aussagen gelten wegen Satz 10 für Zerfällungskörper von Polynomen. Für die Begründung von algebraischen Aussagen ist also der Fundamentalsatz der Algebra entbehrlich.

E. Eindeutige Zerlegbarkeit von Polynomen in irreduzible Faktoren

Satz 11. *Ist $p(x)$ ein Polynom in einem Körper K und sind $p(x) = p_1(x) \cdot p_2(x) \cdot \cdots \cdot p_r(x) = q_1(x) \cdot q_2(x) \cdot \cdots \cdot q_s(x)$ zwei Faktorisierungen von $p(x)$ in irreduzible Polynome aus K von jeweils mindestens dem Grade Eins, so ist $r = s$, und bei geeigneter Numerierung der q_i gilt $p_i(x) = c_i q_i(x)$, wobei die c_i, $i = 1, 2, \ldots, r$, Elemente aus K sind.*

Beweis. Man nehme eine Erweiterung von K, in der $p_1(x)$ eine Nullstelle α hat. Setzt man $x = \alpha$ in $p_1(x)p_2(x) \ldots p_r(x) = q_1(x)q_2(x) \ldots q_s(x)$ ein, so hat man $0 = q_1(\alpha)q_2(\alpha) \ldots q_s(\alpha)$, so daß einer der Faktoren, etwa $q_1(\alpha)$, Null sein muß. Es muß also $q_1(x)$ durch $p_1(x)$ teilbar sein, und da auch $q_1(x)$ irreduzibel ist, folgt eine Gleichung $p_1(x) = c_1 q_1(x)$ mit einem Element c_1 aus K. Setzt man dies in unseren Zerlegungen ein und kürzt man den Faktor $q_1(x)$, so folgt $c_1 p_2(x) \ldots p_r(x) = q_2(x) \ldots q_s(x)$. Induktion führt zum Ziel.

F. Gruppencharaktere

Es sei G eine multiplikative Gruppe und K ein Körper. Wir werden uns mit Abbildungen σ von G in K beschäftigen, für die $\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta)$ für alle α, β aus G gilt. Ist für auch nur ein α das Bild $\sigma(\alpha) = 0$, so gilt $\sigma(\beta) = \sigma(\alpha \cdot \alpha^{-1}\beta) = \sigma(\alpha)\sigma(\alpha^{-1}\beta) = 0$, und unsere Abbildung σ ist dann ohne Interesse. Wir fordern daher auch noch $\sigma(\alpha) \neq 0$ für alle α aus G. Eine solche Abbildung σ soll ein *Charakter* von G in K genannt werden.

Satz 12. *Es sei G eine Gruppe, und $\sigma_1, \sigma_2, \ldots, \sigma_n$ seien paarweise verschiedene Charaktere von G in einen Körper K. Dann sind $\sigma_1, \sigma_2, \ldots, \sigma_n$ linear unabhängig, d. h., sollte für Elemente $a_1, a_2, \ldots, a_n$ aus K die Gleichung $a_1\sigma_1(x) + a_2\sigma_2(x) + \cdots + a_n\sigma_n(x) = 0$ für alle x aus G erfüllt sein, so ist $a_1 = a_2 = \cdots = a_n = 0$.*

Der Beweis dieses Satzes wird durch Induktion nach n geführt. Für $n = 1$ folgt aus $a_1\sigma_1(x) = 0$ sofort $a_1 = 0$, da $\sigma_1(x) \neq 0$ ist. Es sei nun $n > 1$, und es werde angenommen, daß der Satz für weniger als n Charaktere bewiesen ist. Eine hypothetische Relation $a_1\sigma_1(x) + a_2\sigma_2(x) + \cdots + a_n\sigma_n(x) = 0$ werde auf zweierlei Art umgeformt:

Es sei α ein später noch zu bestimmendes Element von G. Die erste Umformung besteht darin, daß man x durch αx ersetzt, die zweite darin, daß man die ursprüngliche Relation mit $\sigma_n(\alpha)$ multipliziert. Die beiden so erhaltenen Relationen lauten

$$a_1\sigma_1(\alpha)\sigma_1(x) + a_2\sigma_2(\alpha)\sigma_2(x) + \cdots + a_n\sigma_n(\alpha)\sigma_n(x) = 0,$$
$$a_1\sigma_n(\alpha)\sigma_1(x) + a_2\sigma_n(\alpha)\sigma_2(x) + \cdots + a_n\sigma_n(\alpha)\sigma_n(x) = 0.$$

Subtraktion führt auf

$$a_1\{\sigma_1(\alpha) - \sigma_n(\alpha)\}\sigma_1(x) + \cdots + a_{n-1}\{\sigma_{n-1}(\alpha) - \sigma_n(\alpha)\}\sigma_{n-1}(x) = 0.$$

Nach Induktionsannahme folgt insbesondere

$$a_1\{\sigma_1(\alpha) - \sigma_n(\alpha)\} = 0.$$

Da $n > 1$ ist, sind σ_1 und σ_n verschiedene Charaktere. Es muß also ein α in G geben, für welches $\sigma_1(\alpha) \neq \sigma_n(\alpha)$ ist. Bei dieser Wahl von α muß $a_1 = 0$ sein. Trägt man dies in die ursprüngliche Relation ein, so folgt aus der Induktionsannahme auch $a_2 = \cdots = a_n = 0$.

Wir wenden diesen Satz auf den Fall an, in welchem G die multiplikative Gruppe eines Körpers E ist und die Charaktere Isomorphismen von E in einen Körper E' sind. Unter der multiplikativen Gruppe von

E versteht man die Menge der von Null verschiedenen Elemente von E mit der Körpermultiplikation als Operation.

Folgerung. *Sind E und E' zwei Körper und $\sigma_1, \sigma_2, \ldots, \sigma_n$ paarweise verschiedene Isomorphismen von E in E', so sind $\sigma_1, \sigma_2, \ldots, \sigma_n$ linear unabhängig.*

Sind $\sigma_1, \sigma_2, \ldots, \sigma_n$ Isomorphismen eines Körpers E in einen Körper E', so nennt man jedes Element a von E mit der Eigenschaft $\sigma_1(a) = \sigma_2(a) = \cdots = \sigma_n(a)$ einen Fixpunkt von E gegenüber $\sigma_1, \sigma_2, \ldots, \sigma_n$. Die Bezeichnung wurde so gewählt, weil im Falle, daß die σ_i Automorphismen und σ_1 speziell die identische Abbildung ist, $\sigma_i(a) = \sigma_1(a) = a$ für den Fixpunkt gilt.

Hilfssatz. *Die Menge der Fixpunkte von E ist ein Unterkörper von E. Wir nennen diesen Unterkörper den Fixpunktkörper bezüglich $\sigma_1, \sigma_2, \ldots, \sigma_n$.*

Denn sind a und b Fixpunkte, so gilt

$$\sigma_i(a \pm b) = \sigma_i(a) \pm \sigma_i(b) = \sigma_j(a) \pm \sigma_j(b) = \sigma_j(a \pm b)$$

und

$$\sigma_i(a \cdot b) = \sigma_i(a) \cdot \sigma_i(b) = \sigma_j(a) \cdot \sigma_j(b) = \sigma_j(a \cdot b).$$

Aus $\sigma_i(a) = \sigma_j(a)$ erhalten wir auch

$$\sigma_i(a^{-1}) = (\sigma_i(a))^{-1} = (\sigma_j(a))^{-1} = \sigma_j(a^{-1}).$$

Somit sind Summe, Differenz und Produkt zweier Fixpunkte wieder Fixpunkte, und das Inverse eines Fixpunktes ist auch Fixpunkt.

Satz 13. *Sind $\sigma_1, \ldots, \sigma_n$ paarweise verschiedene Isomorphismen eines Körpers E in einen Körper E' und ist K der Fixpunktkörper von E, so ist $(E/K) \geq n$.*

Beweis. Wir leiten aus der Annahme $(E/K) = r < n$ einen Widerspruch ab. Es sei $\omega_1, \omega_2, \ldots, \omega_r$ ein Erzeugendensystem des Vektorraumes E über K. In den homogenen linearen Gleichungen

$$\begin{array}{c}
\sigma_1(\omega_1)x_1 + \sigma_2(\omega_1)x_2 + \cdots + \sigma_n(\omega_1)x_n = 0 \\
\sigma_1(\omega_2)x_1 + \sigma_2(\omega_2)x_2 + \cdots + \sigma_n(\omega_2)x_n = 0 \\
\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
\sigma_1(\omega_r)x_1 + \sigma_2(\omega_r)x_2 + \cdots + \sigma_n(\omega_r)x_n = 0
\end{array}$$

haben wir mehr Unbekannte als Gleichungen, so daß eine nichttriviale Lösung existiert, die mit $x_1, x_2, \ldots, x_n$ bezeichnet sei. Für

ein beliebiges Element α aus E können wir Elemente $a_1, a_2, \ldots, a_r$ in K so finden, daß $\alpha = a_1\omega_1 + \cdots + a_r\omega_r$ ist. Wir multiplizieren die erste unserer Gleichungen mit $\sigma_1(a_1)$, die zweite mit $\sigma_1(a_2)$ usw. Weil a_i Fixpunkt und folglich $\sigma_1(a_i) = \sigma_j(a_i)$ ist, erhalten wir

$$\sigma_1(a_1\omega_1)x_1 + \cdots + \sigma_n(a_1\omega_1)x_n = 0$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$\sigma_1(a_r\omega_r)x_1 + \cdots + \sigma_n(a_r\omega_r)x_n = 0.$$

Addieren wir diese Gleichungen, so erhalten wir

$$\sigma_1(\alpha)x_1 + \sigma_2(\alpha)x_2 + \cdots + \sigma_n(\alpha)x_n = 0.$$

Da nicht alle x_i verschwinden, bedeutet diese Gleichung einen Widerspruch zu der linearen Unabhängigkeit der $\sigma_1, \sigma_2, \ldots, \sigma_n$.

Folgerung. *Sind $\sigma_1, \sigma_2, \ldots, \sigma_n$ Automorphismen des Körpers E und ist K der Körper aller derjenigen Elemente von E, die bei allen σ_i fest bleiben, so ist $(E|K) \geq n$.*

Beweis. Wenn unter den σ_i die Identität vorkommt, so folgt unsere Behauptung unmittelbar. Kommt die Identität nicht vor, so füge man sie zu den Automorphismen hinzu und erhält sogar $(E|K) \geq n+1$.

Ist K ein Unterkörper des Körpers E und σ ein Automorphismus von E, so sagen wir, daß σ *den Körper K invariant läßt*, wenn für jedes Element a von K gilt $\sigma(a) = a$.

Sind σ und τ zwei Automorphismen von E, so ist die Abbildung $\sigma(\tau(x))$, kurz $\sigma\tau$ geschrieben, wie der Leser selbst leicht verifizieren kann, ein Automorphismus.

[z.B. $\sigma\tau(x \cdot y) = \sigma(\tau(x \cdot y)) = \sigma(\tau(x) \cdot \tau(y)) = \sigma(\tau(x)) \cdot \sigma(\tau(y))$].

Wir nennen $\sigma\tau$ das *Produkt* von σ und τ. Wir haben schon gesehen, daß das Inverse σ^{-1} eines Automorphismus σ ebenfalls ein Automorphismus ist. Es folgt nunmehr, daß die Menge aller Automorphismen bei dieser Multiplikation eine Gruppe bildet.

Wenn zwei Automorphismen von E einen Unterkörper K invariant lassen, so lassen auch Produkt und Inverse den Körper K invariant. Die Menge G derjenigen Automorphismen von E, die K invariant lassen, bildet also eine Gruppe. Wenn man nun von dieser Gruppe G ausgeht und den Fixpunktkörper K' von G bestimmt, so kann man im allgemeinen nur sagen, daß K ein Unterkörper von K' ist.

G. Anwendungen und Beispiele zu Satz 13

Satz 13 hat, wie die nachfolgenden Beispiele zeigen, weittragende Konsequenzen:

1. Es sei k ein Körper. Wir betrachten den Körper $E = k(x)$ aller rationalen Funktionen der Variablen x. Bilden wir jede der Funktionen $f(x)$ von E auf $f\left(\frac{1}{x}\right)$ ab, so erhalten wir offenbar einen Automorphismus von E. Auch die Abbildung, bei der $f(x)$ auf $f(1-x)$ abgebildet wird, ist ein Automorphismus von E. Kombiniert man diese beiden Automorphismen auf alle möglichen Weisen, so erhält man im ganzen nur sechs verschiedene Automorphismen, nämlich

$$\sigma_1(f(x)) = f(x) \text{ (Identität)}, \qquad \sigma_2(f(x)) = f\left(\frac{1}{x}\right)$$

$$\sigma_3(f(x)) = f(1-x), \qquad \sigma_4(f(x)) = f\left(1-\frac{1}{x}\right)$$

$$\sigma_5(f(x)) = f\left(\frac{1}{1-x}\right), \qquad \sigma_6(f(x)) = f\left(\frac{x}{x-1}\right).$$

Den zugehörigen Fixpunktkörper bezeichnen wir mit K. K besteht aus allen rationalen Funktionen, die den Gleichungen

$$f(x) = f(1-x) = f\left(\frac{1}{x}\right) = f\left(1-\frac{1}{x}\right) = f\left(\frac{1}{1-x}\right) = f\left(\frac{x}{x-1}\right)$$

genügen. Es genügt, die ersten zwei Gleichungen zu überprüfen, da sich die anderen als Folgerungen ergeben. Die Funktion

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

gehört, wie man leicht sieht, zu K. Demnach gehört der Körper $S = k(I)$ aller rationalen Funktionen von I dem Körper K an.

Wir wollen zeigen, daß $K = S$ und $(E/K) = 6$ ist. In der Tat, nach Satz 13 erhalten wir $(E/K) \geq 6$. Wegen $S < K$ genügt es, $(E/S) \leqq 6$ zu beweisen. Nun ist aber $E = S(x)$. Somit reicht es aus, eine Gleichung sechsten Grades mit Koeffizienten in S zu finden, die von x erfüllt wird. Die nachstehende Gleichung

$$(x^2-x+1)^3 - I \cdot x^2(x-1)^2 = 0$$

hat diese Eigenschaft.

Wir empfehlen dem Leser die Untersuchung dieses Körpers als Übung. An späterer Stelle wird er in die Lage versetzt, alle Zwischenkörper herzuleiten.

2. Es sei k ein Körper und $E = k(x_1, x_2, \ldots, x_n)$ der Körper aller rationalen Funktionen der n Variablen $x_1, x_2, \ldots, x_n$. Ist $(\nu_1, \nu_2, \ldots, \nu_n)$ eine Permutation von $(1, 2, \ldots, n)$, so ersetzen wir in jeder Funktion $f(x_1, x_2, \ldots, x_n)$ von E die Variable x_1 durch x_{ν_1}, x_2 durch $x_{\nu_2}, \ldots, x_n$ durch x_{ν_n}. Die auf diese Weise gewonnene Abbildung von E auf sich selbst ist offenbar ein Automorphismus. Wir können auf diesem Wege $n!$ Automorphismen konstruieren (einschließlich des identischen). Es sei K der Fixpunktkörper, d.h. die Menge aller sogenannten „symmetrischen Funktionen". Der Satz 13 zeigt, daß $(E/K) \geq n!$ ist. Wir betrachten nun das Polynom

$$f(t) = (t - x_1)(t - x_2) \cdots (t - x_n) = t^n + a_1 t^{n-1} + \cdots + a_n,$$

wobei $a_1 = -(x_1 + x_2 + \cdots + x_n)$, $a_2 = +(x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n)$ und allgemein a_i die $(-1)^i$-fache Summe sämtlicher Produkte von i verschiedenen Variablen aus dem System $x_1, x_2, \ldots, x_n$ ist. Die Funktionen $a_1, a_2, \ldots, a_n$ nennt man die *elementarsymmetrischen Funktionen*, und der Körper $S = k(a_1, a_2, \ldots, a_n)$ aller rationalen Funktionen der $a_1, a_2, \ldots, a_n$ ist offenbar eine Teilmenge von K. Ähnlich wie bei dem vorangehenden Beispiel soll gezeigt werden, daß $S = K$ und $(E/K) = n!$ ist. Dazu genügt es $(E/S) \leqq n!$ zu beweisen. Wir konstruieren zu diesem Zweck die nachstehende Folge von Körpern:

$$S = S_n \subset S_{n-1} \subset S_{n-2} \subset \cdots \subset S_1 \subset S_0 = E,$$

indem wir

$$S_n = S; \quad S_i = S(x_{i+1}, x_{i+2}, \ldots, x_n) = S_{i+1}(x_{i+1})$$

definieren. Es genügt zu beweisen, daß $(S_{i-1}/S_i) \leqq i$ ist. Da man S_{i-1} aus S_i durch Adjunktion von x_i erhält, muß man eine Gleichung für x_i mit Koeffizienten aus S_i vom Grade höchstens i finden. Das gewünschte Polynom ist

$$F_i(t) = \frac{f(t)}{(t - x_{i+1})(t - x_{i+2}) \cdots (t - x_n)} = \frac{F_{i+1}(t)}{(t - x_{i+1})}$$

und $F_n(t) = f(t)$. Führt man die Division nach dem üblichen Divisionsalgorithmus aus, so ergibt sich $F_i(t)$ als Polynom in t vom Grade i mit dem höchsten Koeffizienten 1, die übrigen Koeffizienten sind Polynome in den Variablen $a_1, a_2, \ldots, a_n$ und $x_{i+1}, x_{i+2}, \ldots, x_n$. Nur ganze Zahlen treten als Koeffizienten in diesen Ausdrücken auf. Offenbar ist x_i eine Wurzel von $F_i(t) = 0$.

Aus unserem bisherigen Resultat folgt dann nachträglich, daß $(S_{i-1}/S_i) = i$ ist, so daß der Vektorraum S_{i-1} über S_i von den Elementen $1, x_i, x_i^2, \ldots, x_i^{i-1}$ aufgespannt wird. Aus dem Beweis von Satz 6 ergibt sich dann, daß der Vektorraum von E über S von den folgenden $n!$ Elementen aufgespannt wird:

$$(*) \qquad x_1^{\nu_1} x_2^{\nu_2} \ldots x_n^{\nu_n} \quad \text{wobei jedes} \quad \nu_i \leqq i-1 \text{ ist.}$$

Ein beliebiges Element von E kann also eindeutig als Linearkombination dieser $n!$ Elemente mit Koeffizienten aus S geschrieben werden. Wählt man aus E ein *Polynom* von $x_1, x_2, \ldots, x_n$, so soll nun nachträglich gezeigt werden, daß dann auch die Koeffizienten *Polynome* in $a_1, a_2, \ldots, a_n$ sind. Angenommen, dies wäre bereits gezeigt, dann würde man speziell den Hauptsatz über symmetrische Funktionen in der üblichen Form bewiesen haben. Dieser Hauptsatz sagt aus, daß ein *Polynom* $g(x_1, x_2, \ldots, x_n) = g$ aus dem Fixpunktkörper K auch als Polynom von $a_1, a_2, \ldots, a_n$ geschrieben werden kann. Wegen $K = S$ kann nämlich g trivialerweise als Linearkombination unserer Elemente (*) geschrieben werden, wobei alle Terme den Koeffizienten 0 erhalten, mit Ausnahme des zu $\nu_1 = \nu_2 = \cdots = \nu_n = 0$ gehörigen Termes, der g selbst als Koeffizienten hat. Sollte unsere Aussage bewiesen sein, so folgt aus der Eindeutigkeit der Darstellung, daß g ein Polynom in $a_1, a_2, \ldots, a_n$ ist.

Um diese zusätzliche Aussage zu beweisen, sei nunmehr $g(x_1, x_2, \ldots, x_n)$ ein beliebiges Polynom von E. Da $F_1(x_1) = 0$ vom Grade 1 in x_1 ist, können wir x_1 als Polynom der a_i und der $x_2, x_3, \ldots, x_n$ ausdrücken. Wir führen diesen Ausdruck in $g(x_1, x_2, \ldots, x_n)$ ein. Wegen $F_2(x_2) = 0$ können wir x_2^2 oder höhere Potenzen als ein Polynom in den $x_2, x_3, \ldots, x_n$ und den a_i ausdrücken, wobei x_2 jedoch höchstens in der ersten Potenz auftritt. Wegen $F_3(x_3) = 0$ lassen sich x_3^3 und höhere Potenzen von x_3 als Polynome von $x_3, x_4, \ldots, x_n$ und von den a_i darstellen, wobei x_3 höchstens quadratisch vorkommt. Führen wir diese Ausdrücke in $g(x_1, x_2, \ldots, x_n)$ ein, so sehen wir, daß es sich als ein Polynom in den x_ν und den a_ν schreiben läßt, wobei der Grad in x_i niedriger als i ist. Somit ist $g(x_1, x_2, \ldots, x_n)$ eine Linearkombination der $n!$ Terme (*). Die Koeffizienten dieser Terme sind aber jetzt Polynome in den a_i.

H. Normale Körpererweiterungen

Wir kehren zu der Situation zurück, die in der Folgerung zu Satz 13 beschrieben wurde. Es sei also E ein Körper, $\sigma_1, \sigma_2, \ldots, \sigma_n$ seien Automorphismen von E, und K sei der Unterkörper aller derjenigen Elemente von E, die bei jedem σ_i fest bleiben. Wir hatten $(E/K) \geq n$ bewiesen. Sollten die σ_i keine Gruppe bilden, so gibt es entweder ein Produkt zweier σ_i, oder ein Inverses eines σ_i, welches ein neuer Automorphismus von E ist. Fügen wir ihn zu den σ_i hinzu, so ändert sich K nicht, und es folgt demnach $(E/K) \geq n + 1$. In der Folgerung zu Satz 13 gilt in diesem Falle das Gleichheitszeichen also nicht. Wir wollen daher von nun an voraussetzen, daß die Automorphismen σ_i eine Gruppe G bilden. In diesem Falle spielt die Funktion

$$S(\alpha) = \sigma_1(\alpha) + \sigma_2(\alpha) + \cdots + \sigma_n(\alpha)$$

für α aus E eine Rolle. Wenden wir auf $S(\alpha)$ ein σ_i an, so ergibt dies die Summe

$$\sigma_i\,\sigma_1(\alpha) + \sigma_i\sigma_2(\alpha) + \cdots + \sigma_i\,\sigma_n(\alpha).$$

Da G eine Gruppe ist, sind aber die Automorphismen $\sigma_i\sigma_1$, $\sigma_i\sigma_2$, $\ldots$, $\sigma_1\sigma_n$ nichts anderes als $\sigma_1, \sigma_2, \ldots, \sigma_n$ in permutierter Reihenfolge. Dies zeigt, daß $S(\alpha)$ unter allen σ_i fest bleibt, also zu K gehört. Die Funktion $S(\alpha)$, die auch die *Spur* von α genannt wird, ist nicht identisch Null, denn dies stünde im Widerspruch zur linearen Unabhängigkeit der $\sigma_1, \sigma_2, \ldots, \sigma_n$. Nun wollen wir zeigen

Satz 14. *Wenn $\sigma_1, \sigma_2, \ldots, \sigma_n$ eine Gruppe G von Automorphismen eines Körpers E bilden, und K der zugehörige Fixpunktkörper ist, dann gilt $(E/K) = n$.*

Beweis. Wegen Satz 13 genügt es folgendes zu zeigen: $n + 1$ Elemente $\alpha_1, \alpha_2, \ldots, \alpha_{n+1}$ von E sind immer linear abhängig in bezug auf K. Zu diesem Zweck betrachten wir das folgende System linearer, homogener Gleichungen

$$\begin{aligned}
x_1\,\sigma_1^{-1}(\alpha_1) + x_2\,\sigma_1^{-1}(\alpha_2) + \cdots + x_{n+1}\,\sigma_1^{-1}(\alpha_{n+1}) &= 0\\
x_1\,\sigma_2^{-1}(\alpha_1) + x_2\,\sigma_2^{-1}(\alpha_2) + \cdots + x_{n+1}\,\sigma_2^{-1}(\alpha_{n+1}) &= 0\\
\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots &\\
x_1\,\sigma_n^{-1}(\alpha_1) + x_2\,\sigma_n^{-1}(\alpha_2) + \cdots + x_{n+1}\,\sigma_n^{-1}(\alpha_{n+1}) &= 0
\end{aligned}$$

in E. Es hat eine nicht-triviale Lösung, weil die Anzahl der Unbekannten größer ist als die Anzahl der Gleichungen. Es sei etwa $x_1 \neq 0$. Da man die Gleichungen noch mit einem beliebigen Faktor aus E multiplizieren darf, können wir erreichen, daß x_1 ein Element von E ist, dessen Spur von Null verschieden ist. Nun wenden wir auf die i-te dieser Gleichungen σ_i an. Das Ergebnis ist

$$\sigma_i(x_1)\,\alpha_1 + \sigma_i(x_2)\,\alpha_2 + \cdots + \sigma_i(x_{n+1})\,\alpha_{n+1} = 0.$$

Summieren wir dies über i, so ergibt sich

$$S(x_1)\,\alpha_1 + S(x_2)\,\alpha_2 + \cdots + S(x_{n+1})\,\alpha_{n+1} = 0.$$

Da $S(x_\nu)$ zu K gehört und $S(x_1) \neq 0$ ist, ergibt sich die behauptete lineare Abhängigkeit.

Folgerung 1. *Unter den gleichen Bedingungen wie in Satz* 14 *gilt: Ein Automorphismus σ von E, der den Körper K invariant läßt, gehört zu G.*

Beweis. Wäre σ von allen σ_i verschieden, so füge man σ zu G hinzu. Das ändert K nicht, und Satz 13 würde ergeben $(E/K) \geq n+1$ im Widerspruch zu Satz 14.

Daraus ergibt sich sofort

Folgerung 2. *Verschiedene endliche Gruppen von Automorphismen von E haben verschiedene Fixpunktkörper.*

Definition. Ein Erweiterungsköper E eines Körpers K heiße eine *normale* Erweiterung, wenn K der Fixpunktkörper einer endlichen Gruppe von Automorphismen von E ist.

Ist $f(x)$ ein Polynom in K, so nennt man $f(x)$ *separabel*, wenn seine irreduziblen Faktoren keine mehrfachen Wurzeln besitzen. Ist E eine Erweiterung des Körpers K, so nennt man das *Element α von E separabel*, wenn es Wurzel eines separablen Polynoms $f(x)$ in K ist. Man nennt E eine *separable Erweiterung* von K, wenn jedes Element von E separabel ist.

Satz 15. *Es sei E eine normale Erweiterung von K mit der Gruppe G. Dann ist E eine separable Erweiterung von K. Genauer gilt: Ist α ein Element von E und sind $\alpha_1, \alpha_2, \ldots, \alpha_r$ die paarweise verschiedenen Bilder von α, wenn man auf α die n Automorphismen von G anwendet, so ist das Polynom*

$$p(x) = (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_r)$$

ein in K irreduzibles Polynom mit der Wurzel α.

Beweis. Multipliziert man die n Elemente von G mit σ_i, so erhält man alle Elemente von G. Dies zeigt, daß die r Elemente

$$\sigma_i(\alpha_1),\ \sigma_i(\alpha_2),\ \ldots,\ \sigma_i(\alpha_r)$$

nur eine Permutation der Elemente $\alpha_1, \alpha_2, \ldots, \alpha_r$ sind. Also bleiben die Koeffizienten des Polynoms $p(x)$ bei Anwendung von σ_i fest. Also ist $p(x)$ ein Polynom in K, und $p(x)$ ist offenbar separabel. Da α selbst unter den Bildern von α vorkommt, hat $p(x)$ die Wurzel α. Wenn $f(x)$ irgendein Polynom in K ist, so daß $f(\alpha) = 0$ ist, so folgt auch $\sigma_i(f(\alpha)) = 0$ und demnach $f(\sigma_i(\alpha)) = 0$. Daher hat $f(x)$ die Wurzeln $\alpha_1, \alpha_2, \ldots, \alpha_r$ und ist infolgedessen durch $p(x)$ teilbar. Dies zeigt die Irreduzibilität von $p(x)$, und unser Satz ist vollständig bewiesen.

Folgerung. *Es sei E eine normale Erweiterung von K, $p(x)$ ein irreduzibles Polynom in K, welches in E eine Wurzel α hat. Dann zerfällt $p(x)$ in E in lauter Linearfaktoren.*

Beweis. Wegen der Eindeutigkeit des zu α gehörigen irreduziblen Polynoms muß $p(x)$ das in Satz 15 konstruierte Polynom sein, welches offenbar in E in lauter Linearfaktoren zerfällt.

Satz 16. *Es sei E eine normale Erweiterung von K mit der Gruppe G, und B sei ein Zwischenkörper. Dann ist E eine normale Erweiterung von B, deren Gruppe U aus denjenigen Automorphismen von G besteht, die den Körper B invariant lassen.*

Beweis. Es sei U die Untergruppe derjenigen Automorphismen von G, die den Körper B invariant lassen. Die Ordnung der Gruppe U werde mit r bezeichnet, der Fixpunktkörper von U sei B'. Dann ist $B < B'$, und wir haben $B = B'$ zu zeigen. Es ist $(E/B') = r$, also $(E/B) \geq r$, und es genügt $(E/B) = r$ zu zeigen. Wendet man die Automorphismen σ_i von G auf B an, so wird B isomorph abgebildet. Es kann aber durchaus vorkommen, daß verschiedene Automorphismen die gleiche Abbildung auf B erzeugen. Sei etwa $\sigma_i(\beta) = \sigma_j(\beta)$ für alle β aus B. Dies ist gleichwertig mit $\sigma_i^{-1}\sigma_j(\beta) = \beta$, also gleichwertig damit, daß $\sigma_i^{-1}\sigma_j$ zu U gehört. Das ist wiederum gleichwertig damit, daß σ_j zur Nebengruppe $\sigma_i U$ gehört. Die Elemente einer Nebengruppe $\sigma_i U$ sind also genau diejenigen, die auf dem Körper B den gleichen Isomorphismus erzeugen. Setzt man also $n = rs$, so ist s die Anzahl dieser Nebengruppen. Die Elemente von G ergeben also, auf B angewandt, genau s verschiedene isomorphe Abbildungen. Der Fixpunktkörper dieser s verschiedenen Abbildungen ist einerseits natürlich der Körper K, andererseits weiß man wegen Satz 13,

daß $(B/K) \geqq s$ sein muß. Die beiden Ungleichungen $(E/B) \geqq r$, $(B/K) \geqq s$ ergeben multipliziert $(E/K) \geqq n$. Da hierin aber das Gleichheitszeichen gilt, muß es auch in den vorherigen Ungleichungen gelten. Es ist also $(E/B) = r$ und $(B/K) = s$. Unser Satz ist damit vollkommen bewiesen.

Aus dem Beweis geht hervor, daß es zu jedem Zwischenkörper B vom Grade s über K sicher s verschiedene Isomorphismen von B in E gibt, die jedes Element von K festlassen, und daß jeder dieser Isomorphismen von einem Element von G erzeugt wird. Man sieht nun leicht, daß es keinen weiteren Isomorphismus von B in irgendeinen Erweiterungskörper von E geben kann, der jedes Element von K fest läßt. Andernfalls füge man ihn zu den s bekannten Isomorphismen hinzu. K bleibt dann der Fixpunktkörper dieser $s+1$ Isomorphismen, so daß nach Satz 13 der Grad $(B/K) \geqq s+1$ sein müßte.

Zu jeder Untergruppe U von G gehört, wie wir bereits wissen, ein Zwischenkörper B, nämlich der Fixpunktkörper zu U (der K enthält). Verschiedene Untergruppen führen auf verschiedene Zwischenkörper, nach Folgerung 2 von Satz 14. Schließlich wurde in Satz 16 gezeigt, daß jeder Zwischenkörper B Fixpunktkörper zu einer Untergruppe U von G ist. Diese Zuordnung von Untergruppe zu Zwischenkörper ist also umkehrbar eindeutig.

Sind U_1 und U_2 Untergruppen mit den Fixpunktkörpern B_1 und B_2, und gilt $U_1 < U_2$, so ist offenbar $B_1 > B_2$. Gilt $B_1 > B_2$, so läßt jeder Automorphismus, der B_1 invariant läßt, auch B_2 invariant; es gilt dann also $U_1 < U_2$. Unsere Zuordnung kehrt also die Enthaltenseinsbeziehung um. Schließlich entspricht bei dieser Zuordnung der Gesamtgruppe G der Körper K, und der Untergruppe, die nur aus der Identität besteht, entspricht der ganze Körper E. Man kann also Untergruppen von G dazu benutzen, um Zwischenkörper zu beschreiben. Dies soll in einer Anwendung erläutert werden:

Es sei B ein Zwischenkörper, der zur Untergruppe U gehört und σ ein Element von G. Das Bild $\sigma(B)$ von B bei Anwendung von σ ist ein Zwischenkörper. Wir fragen nach der Untergruppe, zu der $\sigma(B)$ gehört. Die Elemente von $\sigma(B)$ haben die Form $\sigma(\beta)$, wobei β zu B gehört. Wir müssen nach denjenigen τ aus G fragen, die jedes $\sigma(\beta)$ fest lassen, für die also $\tau\sigma(\beta) = \sigma(\beta)$. Diese Gleichung ist äquivalent mit $\sigma^{-1}\tau\sigma(\beta) = \beta$, und dies besagt, daß $\sigma^{-1}\tau\sigma$ zu U, τ selbst also zu $\sigma U\sigma^{-1}$ gehört. $\sigma U\sigma^{-1}$ ist also die Gruppe, zu der $\sigma(B)$ gehört.

Wir können nun auch entscheiden, unter welchen Bedingungen B eine normale Erweiterung von K ist. Wenn $(B/K) = s$ ist, so haben wir gesehen, daß es überhaupt nur s Isomorphismen von B (die K

invariant lassen) in einen Erweiterungskörper von E geben kann, und daß alle diese Isomorphismen von Elementen aus G erzeugt werden. Wenn B normal über K ist, so muß es andererseits s Automorphismen von B geben, jeder unserer Isomorphismen muß also ein Automorphismus von B sein. Es muß also $\sigma(B) = B$ sein für alle σ aus G. Nach dem Vorhergehenden bedeutet das $\sigma U \sigma^{-1} = U$ für alle σ aus G. Eine Untergruppe U dieser Art nennt man bekanntlich einen *Normalteiler von G*. Es ist also B genau dann eine normale Erweiterung von K, wenn U Normalteiler von G ist.

Nehmen wir nun an, der Zwischenkörper B sei eine normale Erweiterung von K, also U ein Normalteiler von G. Jeder Automorphismus von B, der K invariant läßt, wird also durch Anwendung eines Elementes σ von G auf B erzeugt. Da aber jeder Automorphismus der Nebengruppe σU bei Anwendung auf B den gleichen Automorphismus wie σ erzeugt, stehen die gesuchten Automorphismen von B in eineindeutiger Beziehung zu den Nebengruppen σU. Sind σU und τU zwei solche Nebengruppen, so entsprechen sie Automorphismen von B, die durch Anwendung von σ bzw. τ erhalten werden. Ihre Komposition wird daher durch den Automorphismus $\sigma\tau$ erhalten, der in der Nebengruppe $\sigma\tau U$ liegt. Da U Normalteiler ist, ist diese Nebengruppe das Produkt von σU und τU. Wir sehen, daß sich die Automorphismen von B wie die Nebengruppen komponieren. Die Gruppe der Nebengruppen eines Normalteilers U nennt man bekanntlich die *Faktorgruppe* G/U. In diesem Sinne hat also die normale Erweiterung B von K die Automorphismengruppe G/U.

Zusammenfassend ist bewiesen

Satz 17. (*Fundamentalsatz*). *Es sei E eine normale Erweiterung von K mit der Gruppe G. Ordnet man jeder Untergruppe U von G den Fixpunktkörper B zu, so ist dadurch eine umkehrbar eindeutige Zuordnung zwischen Untergruppen und Zwischenkörpern gegeben. Diese Zuordnung kehrt die Enthaltenseinsrelation um. Für einen gegebenen Zwischenkörper B besteht die zugehörige Gruppe aus denjenigen Elementen von G, die B invariant lassen. Es gilt* (E/B) = *Ordnung von U,* (B/K) = *Index von U in G* = *Anzahl der Nebengruppen. Jeder Isomorphismus von B in einen Erweiterungskörper von E, der die Elemente von K fest läßt, kann durch Anwendung eines Elementes* σ *von G auf B erhalten werden, wobei die Elemente der Nebengruppe* σU *stets den gleichen Isomorphismus von B ergeben. B ist genau dann eine normale Erweiterung von K, wenn U Normalteiler von G ist. In diesem Fall ist die Automorphismengruppe dieser Erweiterung B die Faktorgruppe* G/U.

Wir benötigen nun eine einfache Bedingung dafür, daß eine Erweiterung E von K normal ist. Wir sprechen sie aus in

Satz 18. *E ist genau dann eine normale Erweiterung von K, wenn E der Zerfällungskörper eines separablen Polynoms $p(x)$ in K ist.*

Beweis. 1. E sei eine normale Erweiterung von K und $\omega_1, \omega_2, \ldots, \omega_n$ Erzeugende des Vektorraumes E über K. Es sei $p_i(x)$ das irreduzible Polynom aus K mit der Wurzel ω_i. Wir haben schon gesehen, daß $p_i(x)$ separabel ist und in E in Linearfaktoren zerfällt. Man setze

$$p(x) = p_1(x)p_2(x)\ldots p_n(x).$$

Dann ist $p(x)$ separabel und zerfällt in E in lauter Linearfaktoren. Da unter den Wurzeln von $p(x)$ alle ω_i vorkommen, ist der Zerfällungskörper genau E.

2. Es sei $p(x)$ ein separables Polynom aus K und E sein Zerfällungskörper. Es sei G die Gruppe aller Automorphismen von E, die K invariant lassen. Da (E/K) endlich ist, ist nach der Folgerung zu Satz 13 auch G eine endliche Gruppe. Es genügt zu zeigen, daß ein Element θ aus E, welches bei allen Elementen von G fest bleibt, notwendig zu K gehört; denn dann ist K der Fixpunktkörper von G. Wenn alle Wurzeln von $p(x)$ in K liegen, so ist $E = K$ und unsere Aussage trivialerweise richtig. Nehmen wir daher an, daß von den Wurzeln von $p(x)$ genau n nicht in K liegen, wobei $n \geqq 1$ ist. Unsere Behauptung sei ferner in allen denjenigen Fällen bewiesen, in denen weniger als n Wurzeln von $p(x)$ nicht in K liegen. Es sei α_1 eine Wurzel von $p(x)$, die nicht in K liegt, und $p_1(x)$ das irreduzible Polynom in K mit $p_1(\alpha_1) = 0$. Da $p(x)$ separabel ist, hat $p_1(x)$ keine mehrfachen Wurzeln. Wir ersetzen nun den Grundkörper K durch $K(\alpha_1)$. Dann ist $p(x)$ ein separables Polynom dieses Körpers und E noch immer sein Zerfällungskörper. Es liegen aber jetzt weniger als n Wurzeln von $p(x)$ außerhalb von $K(\alpha_1)$. Nach Induktionsannahme ist also E eine normale Erweiterung von $K(\alpha_1)$. Die Gruppe U derjenigen Automorphismen von E, die $K(\alpha_1)$ invariant lassen, hat also $K(\alpha_1)$ als Fixpunktkörper und ist eine Untergruppe von G. Nun sei θ ein Element, das bei allen Automorphismen aus G invariant bleibt. Dann bleibt es sicher bei allen Automorphismen aus U invariant und gehört daher zu $K(\alpha_1)$. Nun sei s der Grad von $p_1(x)$. Dann hat θ die Form

$$(**) \qquad \theta = c_0 + c_1\alpha_1 + c_2\alpha_1^2 + \cdots + c_{s-1}\alpha_1^{s-1},$$

wobei alle c_i in K liegen.

Andererseits hat $p_1(x)$ keine mehrfache Wurzeln. Wir bezeichnen die Wurzeln von $p_1(x)$ mit $\alpha_1, \alpha_2, \ldots, \alpha_s$. Auf Grund von Satz 8 gibt es einen Isomorphismus σ_i, der $K(\alpha_1)$ auf $K(\alpha_i)$ abbildet, wobei K elementweise fest bleibt und α_1 in α_i übergeht. σ_i führt $p(x)$ über in $p(x)$. Der Körper E ist Zerfällungskörper von $p(x)$ über $K(\alpha_1)$, und auch Zerfällungskörper von $p(x)$ über $K(\alpha_i)$. Auf Grund von Satz 10 läßt sich der Isomorphismus σ_i zu einem Isomorphismus τ_i fortsetzen, der E auf E abbildet und daher ein Element von G ist. Daher muß θ auch bei τ_i fest bleiben. Wir wenden τ_i auf (**) an und erhalten

$$\theta = c_0 + c_1\alpha_i + c_2\alpha_i^2 + \cdots + c_{s-1}\alpha_i^{s-1}.$$

Das Polynom $c_{s-1}x^{s-1} + c_{s-2}x^{s-2} + \cdots + c_1x + (c_0 - \theta)$ hat daher die s voneinander verschiedenen Wurzeln $\alpha_1, \alpha_2, \ldots, \alpha_s$. Das sind mehr Wurzeln als sein Grad beträgt, so daß alle seine Koeffizienten, insbesondere das konstante Glied, Null sein müssen. Also ist $\theta = c_0$, d. h. ein Element von K.

Es seien noch einige Bemerkungen über das Rechnen mit Automorphismen hinzugefügt. Eine normale Erweiterung E von K wird durch praktisch gewählte Erzeugende beschrieben sein, $E = K(\alpha_1, \alpha_2, \ldots, \alpha_r)$. Das bedeutet, daß jedes Element θ eine rationale Funktion von $\alpha_1, \alpha_2, \ldots, \alpha_r$ mit Koeffizienten aus K ist. Kennt man die Wirkung eines Elementes σ von G auf die Erzeugenden α_i von E, so ist σ genau beschrieben. Es wird also σ durch Angabe aller $\sigma(\alpha_i)$ festgelegt. Wenn man für α_i ein Polynom $f(x)$ in K mit $f(\alpha_i) = 0$ kennt, so folgt durch Anwendung von σ, daß $f(\sigma(\alpha_i)) = 0$ sein muß. Dann muß $\sigma(\alpha_i)$ notwendig eine der Wurzeln von $f(x)$ sein. Wenn z. B. E der Zerfällungskörper eines Polynoms ohne mehrfache Wurzeln ist, und wenn $\alpha_1, \alpha_2, \ldots, \alpha_n$ diese Wurzeln sind, so könnte man die α_i als Erzeugende von E nehmen, und weiß dann, daß σ unter den Wurzeln eine gewisse Permutation hervorrufen wird. Bei dieser Beschreibung, die aber nicht in allen Fällen die praktische ist, kann also G mit einer gewissen Permutationsgruppe identifiziert werden.

Wir illustrieren dieses an einem Beispiel, bei dem wir viele Einzelheiten dem Leser überlassen. Es sei K der Körper der rationalen Zahlen und E der Zerfällungsköper des Polynoms $x^4 - 2$. Da es nach früheren Bemerkungen gleichgültig ist, wie wir den Zerfällungskörper konstruieren, beziehen wir die Wurzeln aus dem Körper der komplexen Zahlen, in welchem $x^4 - 2$ die Nullstellen

$$\sqrt[4]{2}, \quad -\sqrt[4]{2}, \quad i\sqrt[4]{2}, \quad -i\sqrt[4]{2}$$

hat. E enthält sowohl $\sqrt[4]{2}$ als auch i. Praktische Erzeugende für E sind diese beiden Elemente. Die Gleichung $x^4 - 2$ ist irreduzibel in K, und folglich ist

$$\left(K\left(\sqrt[4]{2}\right)/K\right) = 4.$$

Da $K\left(\sqrt[4]{2}\right)$ nur reelle Zahlen enthält, ist $x^2 + 1$ irreduzibel in $K\left(\sqrt[4]{2}\right)$, und wir sehen nunmehr $(E/K) = 8$. Als Zerfällungskörper eines separablen Polynoms ist E eine separable Erweiterung, besitzt also genau 8 Automorphismen. Für das Bild von $\sqrt[4]{2}$ bestehen vier Möglichkeiten, für das von i zwei Möglichkeiten. Wir sehen also, daß in diesem Fall alle 8 Kombinationen von Bildern für $\sqrt[4]{2}$ und i wirklich zu Automorphismen führen. Nennen wir nun σ den Automorphismus, der $\sqrt[4]{2}$ in $i\sqrt[4]{2}$ überführt und überdies i fest läßt; ferner τ den Automorphismus, der $\sqrt[4]{2}$ fest läßt, aber i in $-i$ überführt. Eine leichte Rechnung zeigt, daß die 8 Automorphismen die folgenden sind:

$$1,\ \sigma,\ \sigma^2,\ \sigma^3,\ \tau,\ \sigma\tau,\ \sigma^2\tau,\ \sigma^3\tau$$

(dabei bedeutet 1 die Identität). Es ergibt sich ferner $\sigma^4 = 1$, $\tau^2 = 1$ und $\tau\sigma\tau^{-1} = \sigma^{-1}$. Der Leser kann sich davon überzeugen, daß diese Gruppe isomorph ist zur Drehgruppe eines Quadrats im dreidimensionalen Raum. Der Vektorraum E über K wird aufgespannt von den Elementen

$$(***) \quad 1,\ \sqrt[4]{2},\ \left(\sqrt[4]{2}\right)^2,\ \left(\sqrt[4]{2}\right)^3,\ i,\ i\sqrt[4]{2},\ i\left(\sqrt[4]{2}\right)^2,\ i\left(\sqrt[4]{2}\right)^3.$$

Es ist eine nützliche Übungsaufgabe, alle Untergruppen von G zu bestimmen, und zu jeder dieser Untergruppen den Zwischenkörper zu konstruieren. Der zu einer Untergruppe U gehörige Zwischenkörper kann etwa wie folgt bestimmt werden: Man schreibe ein Element θ als Linearkombination der Elemente (***) mit unbestimmten Koeffizienten aus K, berechne für jedes λ aus U das Element $\lambda(\theta)$ und untersuche die Bedingungen, unter welchen $\lambda(\theta) = \theta$ ist für alle λ aus U. Unter den so erhaltenen Zwischenkörpern wird man zwei finden, die man nicht ohne weiteres erraten wird.

I. Algebraische und separable Erweiterungen

Eine Erweiterung E eines Körpers K heißt *algebraisch*, wenn jedes Element von E algebraisch über K ist. Wir zeigen

Satz 19. *Wenn (E/K) endlich ist, so ist E eine algebraische Erweiterung von K.*

Beweis. Es sei $(E/K) = n$ und α ein Element von E. Dann sind die $n+1$ Elemente $1, \alpha, \alpha^2, \ldots, \alpha^n$ linear abhängig über K, und eine solche lineare Abhängigkeit gibt uns eine Gleichung für α mit Koeffizienten aus K.

Es sei nun E eine Erweiterung von K, die durch Adjunktion endlich vieler algebraischer Elemente $\alpha_1, \alpha_2, \ldots, \alpha_r$ erhalten wird. In der Körperkette $K < K(\alpha_1) < K(\alpha_1, \alpha_2) < \ldots < K(\alpha_1, \alpha_2, \ldots, \alpha_r) = E$ ist jeder Körper von endlichem Grad in bezug auf den vorhergehenden, so daß (E/K) auch endlich ist. Also ist E algebraisch über K. Wird E durch Adjunktion unendlich vieler algebraischer Elemente zu K erhalten, so liegt jedes einzelne Element bereits in einem Teilkörper, der durch Adjunktion endlich vieler algebraischer Elemente zu K erhalten wird, ist also algebraisch über K. Wir haben also

Satz 20. *Eine Erweiterung, die durch Adjunktion algebraischer Elemente zu K entsteht, ist eine algebraische Erweiterung.*

Darüber hinaus beweisen wir noch

Satz 21. *Es sei $K < E_1 < E_2$, wobei E_1 eine algebraische Erweiterung von K und E_2 eine algebraische Erweiterung von E_1 ist. Dann ist E_2 eine algebraische Erweiterung von K.*

Beweis. Es sei α ein Element von E_2. Nach Voraussetzung genügt α einer algebraischen Gleichung in E_1, deren Koeffizienten $\alpha_1, \alpha_2, \ldots, \alpha_r$ seien. Dann ist α algebraisch über dem Körper $E' = K(\alpha_1, \alpha_2, \ldots, \alpha_r)$. Der Körper $E'(\alpha)$ ist also von endlichem Grad über E'. E' ist von endlichem Grad über K, also ist $(E'(\alpha)/K)$ endlich. Folglich ist α algebraisch über K.

Es sei nun $E = K(\alpha_1, \alpha_2, \ldots, \alpha_r)$ und jedes α_i separabel über K. Das in K irreduzible Polynom $p_i(x)$ mit der Wurzel α_i hat also keine mehrfachen Wurzeln. Man setze $f(x) = p_1(x)p_2(x)\ldots p_r(x)$ und bezeichne mit E' den Zerfällungskörper von $f(x)$ über E. Dann ist E'

auch Zerfällungskörper von $f(x)$ über K, und enthält E als Zwischenkörper. Nach Satz 18 ist E' eine normale Erweiterung von K. Nach Satz 15 ist also E' eine separable Erweiterung von K, und daher auch E. Die normale Erweiterung E' von K hat nur endlich viele Zwischenkörper, nämlich ebenso viele, wie es Untergruppen der Automorphismengruppe gibt. Also liegen auch nur endlich viele Körper zwischen K und E. Wir erhalten damit

Satz 22. *Es sei $E = K(\alpha_1, \alpha_2, \ldots, \alpha_r)$ und jedes α_i separabel über K. Dann ist E eine separable Erweiterung von K, und es gibt nur endlich viele Körper zwischen K und E. Es läßt sich E zu einem Körper E' erweitern, der normal ist über K.*

Hilfssatz. Es sei σ ein Isomorphismus, der K auf K' abbildet, $p(x)$ ein Polynom aus K ohne mehrfache Wurzeln und $p\ (x)$ sein Bild bei σ. Dann hat auch $p\ (x)$ keine mehrfachen Wurzeln.

Beweis. Es sei E ein Zerfällungskörper von $p(x)$ über K und E' ein Zerfällungskörper von $p\ (x)$ über K'. Nach Satz 10 läßt sich σ zu einem Isomorphismus τ von E auf E' fortsetzen. Man wende τ auf die Zerlegung von $p(x)$ in Linearfaktoren aus E an und erhält die Zerlegung von $p\ (x)$ in verschiedene Linearfaktoren in E'.

Satz 23. *Es sei $K \subset E_1 \subset E_2$, wobei E_1 über K und E_2 über E_1 separabel und von endlichem Grad sind. Dann ist E_2 separabel über K.*

Beweis. Sei α ein Element von E_2 und $p(x)$ das zugehörige irreduzible Polynom aus E_1. Nach Voraussetzung hat $p(x)$ keine mehrfachen Wurzeln. Man erweitere E_1 zu einer über K normalen Erweiterung E, deren Automorphismengruppe mit G bezeichnet werde. Die irreduziblen Faktoren von $p(x)$ in E seien $p_1(x), p_2(x), \ldots, p_r(x)$. Sie sind paarweise verschieden und haben keine mehrfachen Wurzeln. Man wende auf diese Polynommenge alle Automorphismen von G an. Die *verschiedenen* so erhaltenen Polynome sollen mit $q_1(x), q_2(x), \ldots, q_s(x)$ bezeichnet werden. Es ist also jedes $q_i(x)$ Bild eines $p_j(x)$. Wegen des Hilfssatzes hat jedes $q_i(x)$ einfache Wurzeln. Wegen der Eindeutigkeit der irreduziblen Gleichung zu gegebener Wurzel haben keine zwei $q_i(x)$ eine gemeinsame Wurzel. Die Bilder der $q_i(x)$ bei einem Automorphismus σ von G sind s voneinander verschiedene Polynome, deren jedes, wegen der Gruppeneigenschaft von G, wieder Bild eines $p_j(x)$ ist. Wir sehen also, daß σ die Polynome $q_i(x)$ nur permutiert. Setzt man $f(x) = q_1(x)q_2(x)\cdots q_s(x)$, so ist $f(x)$ ein Polynom, dessen Koeffizienten invariant sind bei G, welches also zu K

gehört. $f(x)$ hat keine mehrfachen Wurzeln und ist durch $p(x)$ teilbar, weil ja jedes $p_i(x)$ unter den $q_j(x)$ vorkommt. Folglich ist $f(\alpha) = 0$ und daher α separabel über K.

Es soll nun untersucht werden, welche Körpererweiterungen durch Adjunktion eines einzigen algebraischen Elements α erhalten werden können. Man nennt eine solche Erweiterung *einfach* und das Element α ein *primitives Element*. Wir beweisen

Satz 24. *Eine Erweiterung E von K, von endlichem Grad, ist dann und nur dann einfach, wenn es nur endlich viele Zwischenkörper gibt.*

Beweis. 1. Es sei $E = K(\alpha)$ eine einfache Erweiterung und $p(x)$ das zu α gehörige in K irreduzible Polynom mit höchstem Koeffizienten 1. Es sei B ein Zwischenkörper und $p_1(x)$ das zu α gehörige in B irreduzible Polynom mit höchstem Koeffizienten 1. Dann ist $p_1(x)$ ein Teiler von $p(x)$, so daß es für alle Zwischenkörper B nur endlich viele Möglichkeiten für $p_1(x)$ gibt. Es sei nun B_0 der Zwischenkörper, der aus K durch Adjunktion aller Koeffizienten von $p_1(x)$ entsteht. Es ist $B_0 \subset B$, und sollte der Nachweis $B_0 = B$ gelingen, so würde folgen, daß es für B nur endlich viele Möglichkeiten gibt. Dazu würde der Nachweis von $(E/B) \geqq (E/B_0)$ genügen. Nun ist $p_1(x)$ auch ein Polynom von B_0 mit der Wurzel α. Da $E = B_0(\alpha) = B(\alpha)$ ist, ist (E/B_0) höchstens so groß wie der Grad von $p_1(x)$, der seinerseits gleich (E/B) ist.

2. Es sei E eine Erweiterung endlichen Grades von K, für die es nur endlich viele Zwischenkörper gibt. Es werde aber noch die zusätzliche Voraussetzung gemacht, daß K unendlich viele Elemente enthält. Es seien α und β zwei Elemente aus E. Für jedes c aus K bilde man das Element $\gamma_c = \alpha + c\beta$ und die einfache Erweiterung $K_c = K(\gamma_c)$. Alle K_c sind Zwischenkörper. Da es nur endlich viele Zwischenkörper, aber unendlich viele Möglichkeiten für c gibt, kann man c und d so bestimmen, daß $c \neq d$, wohl aber $K_c = K_d$ ist. Sowohl γ_c als auch γ_d liegen in K_c, daher auch ihre Differenz $(c - d)\beta$. Es folgt, daß β in K_c liegt, demnach auch α, so daß $K(\alpha, \beta) \subset K_c$. Da $K_c \subset K(\alpha, \beta)$, hat man $K(\alpha, \beta) = K(\gamma_c)$. Die Adjunktion von zwei Elementen aus E zu K kann also durch Adjunktion eines Elementes ersetzt werden. Da nun E aus K durch Adjunktion endlich vieler Elemente (etwa der Erzeugenden des Vektorraumes E über K) erhalten werden kann, folgt daher, daß E eine einfache Erweiterung von K ist.

3. Wenn K nur endlich viele Elemente enthält und E eine Erweiterung endlichen Grades ist, so enthält auch E nur endlich viele Elemente. Für diesen Fall wird der Beweis im anschließenden Abschnitt gegeben werden.

Folgerung. Wenn E eine separable Erweiterung endlichen Grades von K ist, so ist E eine einfache Erweiterung.

Beweis. Nach Satz 22 gibt es nur endlich viele Zwischenkörper.

Es sollen nun noch einige einfachere Eigenschaften von Körpern betrachtet werden. Wir beginnen mit Beispielen von Körpern. Bekannt ist uns der Körper der rationalen Zahlen, der mit Q bezeichnet werde. Weitere Körper können den Anfangsgründen der Zahlentheorie entnommen werden:

Es sei p eine gewöhnliche Primzahl. Dann kann man die ganzen Zahlen in p Restklassen modulo p zerlegen. Eine Addition und Multiplikation zwischen diesen Restklassen ist dadurch erklärt, daß man Vertreter addiert bzw. multipliziert. Unter diesen Operationen bilden diese p Restklassen einen mit Q_p bezeichneten Körper. Dies folgt aus dem Satz der elementaren Zahlentheorie, daß eine Kongruenz $ax \equiv b \pmod{p}$ eindeutig lösbar ist, wenn a nicht durch p teilbar ist.

Es sei nun K ein beliebiger Körper. Wir studieren die additive Gruppe von K. Das Analogon zur Potenz a^n eines Elements in einer multiplikativen Gruppe ist in einer additiven Gruppe das Vielfache na. Das Analogon zur Ordnung eines Elementes, der kleinsten positiven Zahl (wenn sie existiert) n, für die $a^n = 1$ ist, ist jetzt die kleinste positive Zahl n, für die $na = 0$ ist. Wir behaupten nun, daß alle von Null verschiedenen Elemente aus K die gleiche additive Ordnung haben. Aus $na = 0$ folgt nämlich $na \cdot a^{-1}b = 0$ für jedes b, also ist $nb = 0$. Sollten nun alle von Null verschiedenen Elemente von K eine endliche Ordnung p haben, so muß p eine Primzahl sein. Wäre nämlich $p = rs$ mit $r < p$ und $s < p$, so wäre $sa \neq 0$ und hätte die kleinere Ordnung r. Wir sagen in diesem Fall, daß K ein Körper der *Charakteristik* p ist. Sollten die von Null verschiedenen Elemente keine endliche Ordnung haben, so sagt man, daß K die *Charakteristik* 0 hat. Diese Bezeichnung ist gerechtfertigt, weil in jedem Körper irgendeiner Charakteristik die folgende Aussage richtig ist:

Ist n eine ganze Zahl und a ein Element von K, so ist $na = 0$ genau dann, wenn entweder $a = 0$ oder n ein Vielfaches der Charakteristik ist.

Um das Einselement von K von der Zahl 1 zu unterscheiden, bezeichnen wir es vorübergehend mit e. Es sei K ein Körper mit Charakteristik $p > 0$. Da e die additive Ordnung p hat, ergeben die Vielfachen von e nur p verschiedene Elemente von K, und es ist $ne = me$ genau dann, wenn n und m derselben Restklasse modulo p angehören. Die Vielfachen von e sind also umkehrbar eindeutig den Restklassen modulo p zugeordnet. Die Addition $ne + me = (n+m)e$ und die Multiplikation $ne \cdot me = nme^2 = nme$ dieser Vielfachen entsprechen dabei der Addition bzw. Multiplikation der zugehörigen Restklassen. Die Vielfachen von e bilden also einen mit Q_p isomorphen Körper. Nun ist es üblich, lediglich n anstelle von ne zu schreiben, wobei zu beachten ist, daß dann n nur modulo p zu lesen ist. Man sagt dann auch, daß die Vielfachen von e den Körper Q_p bilden. In diesem Sinne ist Q_p ein Unterkörper von K. Da jeder Unterkörper von K notwendig e, also auch die Vielfachen von e enthält, ist dann Q_p der kleinste Unterkörper von K.

Es sei noch immer K ein Körper der Charakteristik $p > 0$. Für $1 \leqq i \leqq p-1$ ist der Binomialkoeffizient $\binom{p}{i} = \frac{p!}{i!\,(p-i)!}$ eine ganze durch p teilbare Zahl, weil der Nenner nicht durch die Primzahl p teilbar ist, wohl aber der Zähler. Entwickelt man $(a+b)^p$ nach dem binomischen Satz, so fallen also alle Mittelglieder $\binom{p}{i} a^i b^{p-i}$ weg, und man erhält

$$(a+b)^p = a^p + b^p.$$

Da außerdem

$$(ab)^p = a^p b^p$$

ist, so folgt, daß die Abbildung von K *in* sich, die jedes Element auf seine p-te Potenz abbildet, ein Isomorphismus ist. Insbesondere sieht man, daß auch

$$(a-b)^p = a^p - b^p$$

ist. Und da die Abbildung eineindeutig ist, folgt aus $a^p = b^p$, daß $a = b$ ist. Gelegentlich ist dies ein Isomorphismus von K *auf* K, zum Beispiel dann, wenn K nur endlich viele Elemente enthält (wie aus der Eineindeutigkeit der Abbildung hervorgeht). In einem solchen Fall hat man also einen Automorphismus von K konstruiert.

Nun habe K die Charakteristik 0. Die Vielfachen ne von e sind jetzt alle voneinander verschieden. Da K ein Körper ist, enthält K auch alle Quotienten $\frac{ne}{me}$, vorausgesetzt, daß $m \neq 0$ ist. Eine Gleichheit

zweier Quotienten $\frac{ne}{me} = \frac{n'e}{m'e}$ ist gleichwertig mit $nm'e = mn'e$, also mit $nm' = mn'$, und folglich mit $\frac{n}{m} = \frac{n'}{m'}$. Ordnet man also der rationalen Zahl $\frac{n}{m}$ den Quotienten $\frac{ne}{me}$ zu, so ist damit eine umkehrbar eindeutige Zuordnung zwischen den rationalen Zahlen und unseren Quotienten definiert. Der Leser überzeugt sich unmittelbar davon, daß der Summe bzw. dem Produkt rationaler Zahlen die Summe bzw. das Produkt der zugeordneten Quotienten entspricht. Unsere Zuordnung ergibt also einen Isomorphismus des Körpers Q der rationalen Zahlen mit der Menge der Quotienten $\frac{ne}{me}$. Wie im Fall der Charakteristik $p > 0$ ist es auch hier üblich, $\frac{ne}{me}$ mit der rationalen Zahl $\frac{n}{m}$ zu identifizieren, so daß jetzt Q der kleinste Unterkörper von K ist.

Differentiation. Ist $f = f(x) = a_0 + a_1 x + \cdots + a_n x^n$ ein Polynom in einem Körper K, so definieren wir $f' = a_1 + 2a_2 x + \cdots + na_n x^{n-1}$. Wie der Leser sich selbst leicht überzeugen kann, haben wir für je zwei Polynome f und g

$$(f+g)' = f' + g'$$
$$(f \cdot g)' = fg' + gf'$$
$$(f^n)' = nf^{n-1} \cdot f'.$$

Satz 25. *Das Polynom f aus K hat dann und nur dann mehrfache Wurzeln, wenn im Zerfällungskörper E die Polynome f und f' eine gemeinsame Wurzel haben. Diese Bedingung ist äquivalent mit der Behauptung, daß f und f' im Körper K einen gemeinsamen Faktor höheren als nullten Grades haben.*

Ist α eine Wurzel von $f(x)$ mit der Vielfachheit k, so ist

$$f = (x-\alpha)^k Q(x) \text{ mit } Q(\alpha) \neq 0.$$

Daraus folgt

$$f' = (x-\alpha)^k Q'(x) + k(x-\alpha)^{k-1} Q(x) = (x-\alpha)^{k-1}[(x-\alpha)Q'(x) + kQ(x)].$$

Ist $k > 1$, so ist α eine Wurzel von f' von mindestens der Vielfachheit $k-1$. Ist $k = 1$, so ist $f'(x) = Q(x) + (x-\alpha)Q'(x)$ und $f'(\alpha) = Q(\alpha) \neq 0$. Somit haben f und f' eine Wurzel α dann und nur dann gemeinsam, wenn α eine Wurzel von f von mindestens der Vielfachheit 2 ist.

Haben f und f' eine Wurzel α gemeinsam, so ist das irreduzible Polynom in K, das α zur Wurzel hat, sowohl Teiler von f als auch von f'. Umgekehrt ist eine beliebige Wurzel eines gemeinsamen Faktors von f und f' Wurzel sowohl von f als auch von f'.

Folgerung 1. Ein irreduzibles Polynom $f(x)$ in K hat dann und nur dann keine mehrfachen Wurzeln, wenn $f'(x)$ *nicht* das Nullpolynom ist.

Beweis. Wenn $f'(x)$ nicht das Nullpolynom ist, so hat es einen kleineren Grad als $f(x)$. Ein gemeinsamer Teiler von $f(x)$ und $f'(x)$ hat also auch kleineren Grad als $f(x)$. Da $f(x)$ irreduzibel ist, kann ein solcher gemeinsamer Teiler nur eine Konstante sein. Also hat $f(x)$ keine mehrfachen Wurzeln. Wenn jedoch $f'(x)$ das Nullpolynom ist, so ist $f(x)$ selbst ein gemeinsamer Teiler von $f(x)$ und $f'(x)$, also hat $f(x)$ mehrfache Wurzeln.

Folgerung 2. Wenn K die Charakteristik 0 hat, so ist jedes Polynom separabel.

Beweis. Die einzigen Polynome mit der Ableitung 0 sind in diesem Fall die Konstanten. Also hat jedes irreduzible Polynom nur einfache Wurzeln.

Bemerkung: Wenn K die Charakteristik $p > 0$ hat, so gibt es nicht konstante Polynome, z.B. x^p, deren Ableitung 0 ist.

J. Abelsche Gruppen und deren Anwendung auf die Körpertheorie

Häufig treten endliche Untermengen eines Körpers auf, die bezüglich der Körpermultiplikation eine Gruppe bilden. Die Struktur solcher Gruppen ist besonders einfach:

Satz 26. *Jede endliche Untergruppe S der multiplikativen Gruppe eines Körpers ist zyklisch.*

Der Beweis beruht auf den folgenden Hilfssätzen über abelsche Gruppen:

Hilfssatz 1. Sind in einer abelschen Gruppe A und B zwei Elemente der Ordnungen a bzw. b und ist c das kleinste gemeinsame Vielfache von a und b, so gibt es in der Gruppe ein Element C von der Ordnung c.

Beweis: (a) Sind a und b relativ prim, so hat $C = AB$ die geforderte Ordnung ab.

In der Tat, wenn $C^r = 1$ ist, so folgt $C^{rb} = A^{rb} B^{rb} = A^{rb} = 1$, also ist rb durch a teilbar, und folglich r durch a teilbar. Genau so zeigt man, daß r durch b, und daher durch ab teilbar ist. Andererseits ist $C^{ab} = 1$, und daher ab die Ordnung von C.

(b) Ist d ein Teiler von a, so können wir in der Gruppe ein Element der Ordnung d finden. Offenbar ist $A^{\frac{a}{d}}$ ein solches Element.

(c) Nun betrachten wir den allgemeinen Fall. Es seien $p_1, p_2, \ldots p_r$ die Primzahlen, die entweder in a oder in b aufgehen, und es sei

$$a = p_1^{n_1} p_2^{n_2} \ldots p_r^{n_r}$$
$$b = p_1^{m_1} p_2^{m_2} \ldots p_r^{m_r}.$$

Wir bezeichnen mit t_i die größere der beiden Zahlen n_i und m_i. Dann ist

$$c = p_1^{t_1} p_2^{t_2} \ldots p_r^{t_r}.$$

Auf Grund von (b) läßt sich in der Gruppe ein Element der Ordnung $p_i^{n_i}$ und auch eines der Ordnung $p_i^{m_i}$ finden. Somit existiert ein Element der Ordnung $p_i^{t_i}$. Der Teil (a) zeigt, daß das Produkt dieser Elemente die geforderte Ordnung c hat.

Hilfssatz 2. *Gibt es in einer abelschen Gruppe ein Element C, dessen Ordnung c maximal ist (das ist in einer endlichen Gruppe stets der Fall), so ist c durch die Ordnung a jedes anderen Elementes A der Gruppe teilbar; demnach ist $x^c = 1$ durch jedes Element der Gruppe erfüllt.*

Beweis. Wäre a nicht Teiler von c, so wäre das kleinste gemeinsame Vielfache von a und c größer als c, und wir könnten ein Element dieser Ordnung angeben, was der Wahl von c widerspricht.

Nun beweisen wir Satz 26. Es sei n die Ordnung von S und r die größte Ordnung, die ein Element von S haben kann. Dann ist $x^r - 1 = 0$ für alle Elemente von S erfüllt. Da dieses Polynom vom Grade r im Körper nicht mehr als r Wurzeln besitzen kann, folgt hieraus $r \geqq n$. Andererseits ist aber $r \leqq n$; denn die Ordnung eines jeden Elements ist Teiler von n. Es gibt daher in S ein Element ε der Ordnung n, d.h., die Elemente $1, \varepsilon, \varepsilon^2, \ldots, \varepsilon^{n-1}$ sind alle verschieden und stellen daher alle Elemente von S dar. S ist daher zyklisch.

Satz 26 hätte auch mit Hilfe des Basissatzes für abelsche Gruppen (mit endlich vielen Erzeugenden) bewiesen werden können. Da dieser Satz später benötigt wird, wollen wir hier einen Beweis dafür einschieben.

Es sei G eine abelsche Gruppe, deren Gruppenoperation wir additiv schreiben wollen. Wir sagen, daß die Elemente $g_1, g_2, \ldots, g_k$ die Gruppe G erzeugen, wenn jedes Element g von G sich als Summe von Vielfachen der g_i, also in der Form $g = n_1 g_1 + \cdots + n_k g_k$, schreiben läßt. Falls es kein System von weniger als k Elementen gibt, das G erzeugt, so nennen wir $g_1, g_2, \ldots, g_k$ ein minimales Erzeugendensystem. Jede Gruppe, die ein endliches Erzeugendensystem hat, besitzt auch ein minimales Erzeugendensystem. Insbesondere hat eine endliche Gruppe stets ein minimales Erzeugendensystem.

Aus der Identität $n_1(g_1 + mg_2) + (n_2 - n_1 m)g_2 = n_1 g_1 + n_2 g_2$ folgt: wenn $g_1, g_2, \ldots, g_k$ die Gruppe G erzeugen, dann auch $g_1 + mg_2, g_2, \ldots, g_k$.

Eine Gleichung $m_1 g_1 + m_2 g_2 + \cdots + m_k g_k = 0$ nennen wir eine *Relation* zwischen den Erzeugenden und $m_1, m_2, \ldots, m_k$ die Koeffizienten dieser Relation.

Wir sagen, daß eine abelsche Gruppe G das *direkte Produkt* der Untergruppen $G_1, G_2, \ldots, G_k$ ist, wenn sich jedes Element g aus G eindeutig als Summe $g = x_1 + x_2 + \cdots + x_k$ darstellen läßt, wobei x_i ein Element von G_i ist, $i = 1, 2, \ldots, k$.

Basissatz. Jede abelsche Gruppe mit endlich vielen Erzeugenden ist direktes Produkt zyklischer Untergruppen $G_1, G_2, \ldots, G_k$, wobei die Ordnung von G_i Teiler der Ordnung von G_{i+1}, $i = 1, \ldots, k-1$, und k die Anzahl der Elemente eines minimalen Erzeugendensystems ist. Dabei ist unter der Ordnung einer unendlichen Gruppe die Zahl 0 zu verstehen.

Sollte $k = 1$ sein, so ist die Gruppe zyklisch und der Satz trivial. Wir nehmen an, der Satz wäre richtig für alle Gruppen mit einem minimalen Erzeugendensystem von $k-1$ Elementen. Es sei G eine abelsche Gruppe mit einem minimalen Erzeugendensystem von k Elementen. Falls kein minimales Erzeugendensystem eine nichttriviale Relation erfüllt, so sei $g_1, g_2, \ldots, g_k$ ein minimales Erzeugendensystem und es seien $G_1, G_2, \ldots, G_k$ die von diesen Elementen erzeugten zyklischen Gruppen. Für jedes Element g aus G gilt $g = n_1 g_1 + \cdots + n_k g_k$, wobei der Ausdruck eindeutig ist, denn andernfalls würden wir eine nicht-triviale Relation erhalten. Für diesen Fall wäre der Satz richtig. Nun nehmen wir an, daß eine nicht-triviale

Relation für ein gewisses minimales Erzeugendensystem erfüllt ist. Unter allen Relationen zwischen den minimalen Erzeugendensystemen sei

$$m_1 g_1 + \cdots + m_k g_k = 0$$

eine Relation, in welcher der kleinste positive Koeffizient auftritt. Nach einer etwaigen Umordnung der Erzeugenden können wir annehmen, daß dieser Koeffizient m_1 ist. In einer beliebigen anderen Relation zwischen $g_1, g_2, \ldots, g_k$,

$$n_1 g_1 + \cdots + n_k g_k = 0 \tag{2}$$

muß m_1 ein Teiler von n_1 sein. Andernfalls wäre $n_1 = q m_1 + r$, $0 < r < m_1$ und q-fache Subtraktion der Relation (1) von der Relation (2) würde eine Relation mit einem Koeffizienten $r < m_1$ nach sich ziehen. In der Relation (1) muß m_1 auch ein Teiler von m_i, $i = 2, \ldots, k$ sein. Andernfalls wäre etwa $m_2 = q m_1 + r$, $0 < r < m_1$. Im Erzeugendensystem $g_1 + q g_2, g_2, \ldots, g_k$ würden wir eine Relation $m_1(g_1 + q g_2) + r g_2 + m_3 g_3 + \cdots + m_k q_k = 0$ haben, wobei der Koeffizient r der Wahl von m_1 widerspräche. Somit ist $m_2 = q_2 m_1$, $m_3 = q_3 m_1, \ldots, m_k = q_k m_1$. Das System $\bar{g}_1 = g_1 + q_2 g_2 + \cdots + q_k g_k$, $g_2, \ldots, g_k$ ist ein minimales Erzeugendensystem, und es gilt $m_1 \bar{g}_1 = 0$. Sei $0 = n_1 \bar{g}_1 + n_2 g_2 + \cdots + n_k g_k$ irgendeine Relation zwischen $\bar{g}_1, g_2, \ldots, g_k$. Betrachten wir diese Relation als Relation (2) und $m_1 \bar{g}_1 = 0$ als Relation (1), so ergibt sich die Teilbarkeit von n_1 durch m_1 und daher insbesondere die Relation $n_1 \bar{g}_1 = 0$.

Es sei G' die von $g_2, \ldots, g_k$ erzeugte Untergruppe von G und G_1 die zyklische Gruppe der Ordnung m_1, die von $\bar{g}_1$ erzeugt wird. Dann ist G das direkte Produkt von G_1 und G'. In der Tat kann jedes Element g von G in der Form

$$g = n_1 \bar{g}_1 + n_2 g_2 + \cdots + n_k g_k = n_1 \bar{g}_1 + g'$$

geschrieben werden, wobei g' zu G' gehört. Diese Darstellung ist eindeutig, denn aus $n_1 \bar{g}_1 + g' = n_1 \bar{g}_1 + g''$ folgt $(n_1 - n_1') \bar{g}_1 + (g' - g'') = 0$, und wir haben eben gesehen, daß aus einer solchen Relation $(n_1 - n_1') \bar{g}_1 = 0$, also $n_1 \bar{g}_1 = n_1' \bar{g}_1$ folgt. Eingesetzt zieht dieses natürlich auch $g' = g''$ nach sich.

Auf Grund unserer Induktionsvoraussetzung ist G' das direkte Produkt von $k - 1$ zyklischen Gruppen, die von Elementen $\bar{g}_2, \bar{g}_3, \ldots, \bar{g}_k$ erzeugt werden, deren jeweilige Ordnungen $t_2, \ldots, t_k$ für $i = 2, \ldots, k - 1$ den Bedingungen genügen, daß t_i ein Teiler von

t_{i+1} ist. Betrachtet man die Erzeugenden $\bar{g}_1, \bar{g}_2, \ldots, \bar{g}_k$ und die Relation $m_1\bar{g}_1 + t_2\bar{g}_2 = 0$, so zeigt ein früheres Argument, daß m_1 Teiler von t_2 ist. Das vervollständigt den Beweis.

Es sollen nun endliche Körper untersucht werden, d. h. Körper mit einer endlichen Anzahl von Elementen.

K sei ein endlicher Körper mit q Elementen. Die von Null verschiedenen Elemente von K bilden eine multiplikative Gruppe der Ordnung $q-1$ und folglich gilt $\alpha^{q-1} = 1$ für alle $\alpha \neq 0$ von K. Multiplizieren wir diese Gleichung mit α, so erhalten wir $\alpha^q = \alpha$, und dies gilt nun auch für $\alpha = 0$. Auf Grund von Satz 26 ist die multiplikative Gruppe von K zyklisch, es gibt also ein Element ε, so daß die Potenzen $1, \varepsilon, \varepsilon^2, \ldots, \varepsilon^{q-2}$ alle von Null verschiedenen Elemente von K durchlaufen; ε selbst ist ein Element der Ordnung $q-1$. Wendet man dieses Resultat auf eine Erweiterung E von endlichem Grade über K an, so sieht man, daß die von Null verschiedenen Elemente von E Potenzen eines einzigen Elements α sind, und folglich $E = K(\alpha)$ ist. Damit ist die beim Beweis von Satz 24 gebliebene Lücke ausgefüllt.

Es sei nun $(E/K) = n$ und $\omega_1, \omega_2, \ldots, \omega_n$ Erzeugende des Vektorraumes über K. Jedes Element θ von E ist eine eindeutige Linearkombination

$$\theta = c_1\omega_1 + c_2\omega_2 + \cdots + c_n\omega_n,$$

wobei die c_i dem Körper K angehören. Daraus folgt, daß die Anzahl der Elemente von E gleich q^n ist. Die q^n Elemente von E genügen alle der Gleichung q^n-ten Grades $x^{q^n} - x = 0$. Da diese Gleichung sicher nicht mehr als q^n Wurzeln haben kann, sind es alle Wurzeln dieser Gleichung, und jede von ihnen ist einfach. Es gilt also die Zerlegung

$$x^{q^n} - x = \prod_{\alpha}(x - \alpha),$$

wobei das Produkt über alle Elemente α von E zu erstrecken ist. Daraus folgt, daß E Zerfällungskörper des Polynoms $x^{q^n} - x$ über K ist. Auf Grund der Folgerung zu Satz 10 ergibt sich, daß je zwei Erweiterungen gleichen Grades n von K isomorph sind, wobei dieser Isomorphismus jedes Element von K fest läßt.

Da K ein endlicher Körper ist, hat er sicher nicht die Charakteristik 0. Ist $p > 0$ die Charakteristik von K, so enthält K den Unterkörper Q_p mit p Elementen. Wenn r der Grad von K über Q_p ist, so folgt aus dem Vorhergehenden, daß K genau p^r Elemente besitzt, d. h., $q = p^r$ ist. Wir hatten gesehen, daß in einem endlichen Körper

der Charakteristik p das Erheben in die p-te Potenz ein Automorphismus ist. Wendet man den Automorphismus zweimal an, so sieht man, daß auch das Potenzieren mit p^2 ein Automorphismus ist. Allgemein ist für jede natürliche Zahl s die Abbildung, die jedes α aus K auf α^{p^s} abbildet, ein Automorphismus von K. Es gelten also die Gleichungen $(\alpha \pm \beta)^{p^s} = \alpha^{p^s} \pm \beta^{p^s}$, $(\alpha\beta)^{p^s} = \alpha^{p^s}\beta^{p^s}$ für alle α, β aus K.

Bei gegebenem endlichem Körper K mit $q = p^r$ Elementen und gegebenem $n \geqq 1$ soll nun auch die Existenz eines Erweiterungskörpers E vom Grade n bewiesen werden. Zu diesem Zweck sei E der Zerfällungskörper des Polynoms $x^{p^n} - x$ über K. Es soll gezeigt werden, daß $(E/K) = n$ ist. Dazu genügt nach dem Vorhergehenden der Nachweis, daß die Anzahl der Elemente von E gleich q^n ist. Ist α eine Wurzel unseres Polynoms, gilt also $\alpha^{q^n} - \alpha = 0$, so kann unser Polynom auch in der Form $(x^{q^n} - \alpha^{q^n}) - (x - \alpha)$ geschrieben werden. Dividiert man durch $x - \alpha$, und setzt $x = \alpha$, so erhält man $q^n \cdot \alpha^{q^n - 1} - 1$. Da q durch die Charakteristik teilbar, als Körperelement also 0 ist, ist dies einfach -1. Dies zeigt, daß α eine einfache Wurzel ist, daß $x^{q^n} - x$ also genau q^n verschiedene Wurzeln hat. Weil q^n eine Potenz von p ist, ist das Erheben in die q^n-te Potenz ein Automorphismus. Sind α und β zwei Wurzeln unserer Gleichung, so zeigt die folgende Rechnung, daß $\alpha \pm \beta$, $\alpha\beta$ und $\frac{\alpha}{\beta}$ $(\beta \neq 0)$ auch Wurzeln unserer Gleichung sind:

$$(\alpha \pm \beta)^{q^n} = \alpha^{q^n} \pm \beta^{q^n} = \alpha \pm \beta,$$

$$(\alpha\beta)^{q^n} = \alpha^{q^n}\beta^{q^n} = \alpha\beta,$$

$$\left(\frac{\alpha}{\beta}\right)^{q^n} = \frac{\alpha^{q^n}}{\beta^{q^n}} = \frac{\alpha}{\beta}.$$

Wir sehen also, daß die Wurzeln unserer Gleichung selbst einen Körper mit q^n Elementen bilden; und aus der Minimaleigenschaft eines Zerfällungskörpers folgt, daß E dieser Körper ist, also q^n Elemente besitzt.

Wendet man dies auf Q_p als Grundkörper mit r als Grad an, so sieht man insbesondere, daß es zu gegebenem $q = p^r$ einen Körper mit q Elementen gibt. Aus der früher bewiesenen Eindeutigkeit der Erweiterung folgt, daß je zwei endliche Körper mit der gleichen Anzahl von Elementen isomorph sind.

Ist K ein gegebener Körper mit q Elementen und E ein Erweiterungskörper n-ten Grades, so haben wir schon gesehen, daß sich E durch Adjunktion eines einzigen Elementes erzeugen läßt. Die irreduzible Gleichung aus K mit der Wurzel α ist daher vom Grad n. Dies zeigt, daß es in K irreduzible Polynome jedes gegebenen Grades gibt.

Es soll nun die Automorphismengruppe G einer Erweiterung n-ten Grades E des endlichen Körpers K bestimmt werden (d. h. diejenigen Automorphismen, die K fest lassen). Wir haben schon gesehen, daß die Abbildung σ, für welche $\sigma(\alpha) = \alpha^q$ für alle α aus E ist, einen Automorphismus darstellt. Für α aus K wissen wir, daß $\alpha^q = \alpha$ ist, daß also σ jedes Element von K fest läßt. Um die Ordnung von σ zu bestimmen, nehmen wir an, es sei $\sigma^s = 1$. Dann müßte also $\alpha^{q^s} = \alpha$ sein für alle α aus E. Da das Polynom $x^{q^s} - x$ nur dann q^n Wurzeln haben kann, wenn $s \geqq n$ ist, und da andrerseits $\alpha^{q^n} = \alpha$ für alle α aus E erfüllt ist, hat σ die Ordnung n. Wir erhalten also in $1, \sigma, \sigma^2, \ldots, \sigma^{n-1}$ jetzt n verschiedene Automorphismen. Mehr Automorphismen kann eine Erweiterung n-ten Grades nicht haben. Damit ist G bestimmt und als zyklische Gruppe der Ordnung n nachgewiesen.

K. Einheitswurzeln

Wenn K irgendein Körper ist und ε ein Element eines Erweiterungskörpers, welches Wurzel von $x^n - 1$ ist, so heißt ε eine n-te *Einheitswurzel.*

Sollte die Charakteristik p von K größer als 0 sein und $n = pm$, so ist $x^n - 1 = (x^m - 1)^p$, jede n-te Einheitswurzel also bereits eine m-te. Wir nehmen bei Charakteristik $p > 0$, da das keine Einschränkung der Allgemeinheit bedeutet, daher an, daß n und p teilerfremd sind.

Die Ableitung von $x^n - 1$ ist nx^{n-1}, sie hat nur die Wurzel 0, also keine Wurzel mit $x^n - 1$ gemeinsam. Der Zerfällungskörper E von $x^n - 1$ über K ist daher eine normale Erweiterung und enthält genau n Wurzeln von $x^n - 1$. Da Produkt und Quotient zweier n-ten Einheitswurzeln wieder eine n-te Einheitswurzel ist, bilden die n-ten Einheitswurzeln in E eine multiplikative Gruppe. Auf Grund von Satz 26 bilden sie also eine zyklische Gruppe. Es gibt also eine n-te Einheitswurzel ε, die genau die Ordnung n hat. Alle n-ten Einheitswurzeln sind Potenzen von ε. Eine Einheitswurzel ε dieser Art soll

eine *primitive* n-te Einheitswurzel genannt werden. Eine Potenz ε^i ist genau dann *primitive* n-te Einheitswurzel, wenn i zu n teilerfremd ist. Die Anzahl der verschiedenen primitiven n-ten Einheitswurzeln wird also durch die Eulersche Funktion $\varphi(n)$ gegeben, die wir aus den Elementen der Zahlentheorie als bekannt voraussetzen.

Wenn d ein Teiler von n ist, so ist $x^d - 1$ ein Teiler von $x^n - 1$. Die d-ten Einheitswurzeln kommen also alle unter den n-ten Einheitswurzeln vor. Eine beliebige Potenz ε^i hat als Ordnung d einen Teiler von n und ist dann primitive d-te Einheitswurzel. Bezeichnen wir mit $\Phi_d(x)$ das Polynom $\Pi(x - \eta)$, wobei η alle *primitiven* d-ten Einheitswurzeln durchläuft, so gilt

$$(*) \qquad x^n - 1 = \prod_d \Phi_d(x),$$

wobei d alle Teiler von n durchläuft; denn die rechte Seite besteht ja nur in einer Gruppierung der linken Seite je nach der Ordnung d der betreffenden Einheitswurzel. Es ist $\Phi_1(x) = x - 1$, und es soll durch Induktion nach n gezeigt werden, daß $\Phi_n(x)$ ein ganzzahliges Polynom ist. Nach Induktionsvoraussetzung folgt aus (*)

$$x^n - 1 = \Phi_n(x)\, g(x),$$

wobei $g(x)$ ein ganzzahliges Polynom mit höchstem Koeffizienten 1 ist. Also ist auch $\Phi_n(x)$ ein ganzzahliges Polynom mit dem höchsten Koeffizienten 1, wie sich aus dem Divisionsalgorithmus ergibt. Das Polynom $\Phi_n(x)$ hat den Grad $\varphi(n)$ und wird das n-te *Kreisteilungspolynom* genannt. Formel (*) gibt eine, in einem beliebigen Körper K gültige Zerlegung von $x^n - 1$ an; die Faktoren werden aber im allgemeinen nicht irreduzibel sein.

Wenn ε eine primitive n-te Einheitswurzel ist, so enthält der Körper $K(\varepsilon)$ bereits alle n-ten Einheitswurzeln, ist also der Zerfällungskörper E von $x^n - 1$. Da $\Phi_n(\varepsilon) = 0$ ist, ist $(E/K) \leqq \varphi(n)$. Es sei G die Automorphismengruppe von E bezüglich K und σ ein Element von G. Da das Bild einer primitiven n-ten Einheitswurzel bei einem Automorphismus wieder eine primitive n-te Einheitswurzel ist, muß $\sigma(\varepsilon) = \varepsilon^i$ sein mit einem zu n teilerfremden i. Dann ist $\sigma(\varepsilon^j) = \varepsilon^{ij} = (\varepsilon^j)^i$, es ersetzt also σ jede n-te Einheitswurzel durch ihre i-te Potenz. Dies zeigt, daß die Zahl i nur von σ, und nicht von der Auswahl der primitiven n-ten Einheitswurzel ε abhängt, wobei allerdings i nur bis auf Vielfache von n bestimmt ist. Ferner braucht nicht jedes zu n teilerfremde i einen Automorphismus zu liefern. Wenn zum Beispiel ε zu K selbst gehört, also $E = K$ ist, muß σ die Identität, also $i \equiv 1 \pmod{n}$ sein.

Bezeichnen wir nun σ in Abhängigkeit von i mit σ_i, dann ist $\sigma_i\sigma_j(\varepsilon) = \sigma_i(\varepsilon^j) = \varepsilon^{ij}$, also $\sigma_i\sigma_j = \sigma_{ij}$. Jedem σ_i ist eindeutig eine zu n teilerfremde Restklasse modulo n zugeordnet, und dem Produkt zweier Automorphismen das Produkt der Restklassen. Die Gruppe G ist also isomorph mit einer Untergruppe der Gruppe der teilerfremden Restklassen modulo n, *insbesondere daher eine abelsche Gruppe*, wie man auch aus $\sigma_i\sigma_j = \sigma_{ij} = \sigma_j\sigma_i$ sieht.

Genauere Aussagen kann man nur für spezielle Körper K erwarten. Das wichtigste Ergebnis in dieser Richtung ist

Satz 27. *Für $K = Q$, den Körper der rationalen Zahlen, ist das Polynom $\Phi_n(x)$ irreduzibel, also $(E/Q) = \varphi(n)$. Die Abbildung $\sigma_i(\varepsilon) = \varepsilon^i$ liefert bei beliebigem, zu n teilerfremdem i einen Automorphismus aus G, und G ist mit der multiplikativen Gruppe aller zu n teilerfremden Restklassen isomorph. Wenn n eine Primzahl p ist, so ist die Gruppe G zyklisch von der Ordnung $p - 1$ und*

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1.$$

Beweis. Es sei das Polynom $f(x)$ ein Teiler von $x^n - 1$ und habe rationale Koeffizienten. Nach Multiplikation mit einer geeigneten Konstanten kann angenommen werden, daß $f(x)$ ganze Koeffizienten hat. (Hätten wir den Gaußschen Satz über ganzzahlige Polynome zur Verfügung, so könnten wir auch noch annehmen, daß $f(x)$ den höchsten Koeffizienten 1 hat; doch soll davon nicht Gebrauch gemacht werden). Ist s eine natürliche Zahl und $r_s(x)$ Divisionsrest von $f(x^s)$ bei der Division durch $f(x)$, dann hat $r_s(x)$ rationale Koeffizienten, und im Nenner dieser Koeffizienten treten nur Primfaktoren auf, die den höchsten Koeffizienten von $f(x)$ teilen. Addiert man zu $f(x^s)$ ein Polynom der Form $f(x)g(x)$, so ändert sich der Divisionsrest nicht. Ist ax^m ein Term von $f(x)$, so liefert dieser Term zur Differenz $f(x^{s+n}) - f(x^s)$ den Beitrag $ax^{m(s+n)} - ax^{ms} = ax^{ms}(x^{mn} - 1)$, der durch $x^n - 1$, also durch $f(x)$ teilbar ist. Dies zeigt $r_{s+n}(x) = r_s(x)$, so daß also $r_s(x)$ nur von der Restklasse von s modulo n abhängt. Insbesondere gibt es nur endlich viele verschiedene unter den Polynomen $r_s(x)$.

Es sei nun p eine Primzahl, die nicht in dem höchsten Koeffizienten von $f(x)$ aufgeht. Das Polynom $r_p(x)$ ist auch der Divisionsrest des Polynoms $f(x^p) - (f(x))^p$. Da $f(x)$ ganze Koeffizienten hat, hat es die Form $f(x) = \sum \pm x^m$, wobei jedes einzelne Glied mehrfach auftreten kann. Wegen der Teilbarkeitseigenschaften der Binomialkoeffizienten sieht man wie bei einer früheren Gelegenheit, daß sich $(f(x))^p$ von

$\sum \pm x^{m_\nu}$ nur um ein ganzzahliges Polynom mit durch p teilbaren Koeffizienten unterscheidet. Weil $f(x^p) = \sum \pm x^{p m_\nu}$ ist, gilt $(f(x^p) - (f(x))^p = pg(x)$, mit ganzzahligem Polynom $g(x)$. Es ist also $r_p(x)$ das p-fache des Divisionsrestes von $g(x)$ und da p nicht im höchsten Koeffizienten von $f(x)$ aufgeht, so folgt, daß p den Zähler jedes Koeffizienten von $r_p(x)$ teilt.

Nun sei M eine ganze Zahl, die den höchsten Koeffizienten von $f(x)$ übertrifft und größer ist als die Zähler der Koeffizienten aller Polynome $r_s(x)$ (wir hatten schon gesehen, daß es nur endlich viele verschiedene $r_s(x)$ gibt). Wenn p eine Primzahl $\geqq M$ ist, so kann also p jeden Zähler der Koeffizienten von $r_p(x)$ nur dann teilen, wenn $r_p(x) = 0$ ist. Wir wissen also, $r_p(x) = 0$ für alle Primzahlen $p \geqq M$.

Es seien nun s und t ganze Zahlen, für die $r_s(x) = 0$ und $r_t(x) = 0$ ist. Dies bedeutet die Teilbarkeit von $f(x^s)$ durch $f(x)$ und daher die Teilbarkeit von $f(x^t)$ durch $f(x^t)$. Da auch $f(x^t)$ durch $f(x)$ teilbar ist, folgt $r_{st}(x) = 0$. Es ist also $r_s(x) = 0$, sobald alle Primfaktoren von s größer oder gleich M sind.

Nunmehr sei s eine beliebige zu n teilerfremde Zahl. Wir setzen $s_1 = s + n\Pi p$, wobei p alle diejenigen Primzahlen kleiner M durchläuft, die nicht in s aufgehen. Der Leser überlegt sich leicht, daß s_1 durch keine Primzahl unterhalb M teilbar ist, so daß also $r_{s_1}(x) = 0$ ist. Da s in der gleichen Restklasse modulo n wie s_1 liegt, folgt $r_s(x) = 0$. Damit haben wir die Teilbarkeit von $f(x^s)$ durch $f(x)$ gezeigt, vorausgesetzt, daß s zu n teilerfremd ist.

Von $f(x)$ sei nun überdies vorausgesetzt, daß es die primitive Einheitswurzel ε als Nullstelle hat. Ist s teilerfremd zu n, so ist $f(x^s) = f(x)h(x)$, also ist auch $f(\varepsilon^s) = 0$. Daher sind alle primitiven n-ten Einheitswurzeln Nullstellen von $f(x)$, der Grad von $f(x)$ ist daher $\geqq \varphi(n)$. Da das Kreisteilungspolynom $\Phi_n(x)$ genau den Grad $\varphi(n)$ hat, muß es also irreduzibel sein. Weil die Gruppe G genau $\varphi(n)$ Elemente enthalten muß, liefert σ_i für beliebiges, zu n teilerfremdes i einen Automorphismus.

Wenn n eine Primzahl p ist, so ist die Gruppe G isomorph zur multiplikativen Gruppe der zu p teilerfremden Restklassen modulo p. Das ist aber die multiplikative Gruppe des Körpers Q_p, und daher ist sie zyklisch. Aus $x^p - 1 = \Phi_p(x)\Phi_1(x)$ folgt der angegebene Wert von $\Phi_p(x)$.

Damit sind alle Teile von Satz 27 bewiesen.

L. Noethersche Gleichungen

Es sei E ein Körper und G eine endliche Gruppe von Automorphismen von E. Jedem Element σ aus G sei ein Element $x_\sigma \neq 0$ aus E zugeordnet, und es werde vorausgesetzt, daß diese Elemente folgende Gleichungen erfüllen:

$$x_\sigma \cdot \sigma(x_\tau) = x_{\sigma\tau},$$

für alle σ und τ aus G. Wir sagen dann, daß die x_σ eine Lösung der *Noetherschen Gleichungen* sind.

Satz 28. *Die einzigen Lösungen der Noetherschen Gleichungen haben die Form* $x_\sigma = \frac{\alpha}{\sigma(\alpha)}$ *für alle* σ, *wobei* α *ein festes, aber beliebig wählbares, von Null verschiedenes Element aus* E *ist.*

Beweis. Für ein beliebiges α ist es klar, daß $x_\sigma = \frac{\alpha}{\sigma(\alpha)}$ eine Lösung der Gleichungen ist, denn es gilt

$$\frac{\alpha}{\sigma(\alpha)} \cdot \sigma\left(\frac{\alpha}{\tau(\alpha)}\right) = \frac{\alpha}{\sigma(\alpha)} \cdot \frac{\sigma(\alpha)}{\sigma\tau(\alpha)} = \frac{\alpha}{\sigma\tau(\alpha)}.$$

Nun sei umgekehrt das System x_σ eine Lösung. Da die Automorphismen linear unabhängig sind, kann die Gleichung $\sum_\tau x_\tau \tau(z) = 0$ (summiert über alle τ) nicht für alle z aus E erfüllt sein. Es gibt daher ein Element a in E, so daß $\sum_\tau x_\tau \tau(a) = \alpha \neq 0$ ist. Wenden wir σ auf α an, so folgt

$$\sigma(\alpha) = \sum_\tau \sigma(x_\tau) \cdot \sigma\tau(a).$$

Multiplikation mit x_σ ergibt

$$x_\sigma \cdot \sigma(\alpha) = \sum_\tau x_\sigma \sigma(x_\tau) \cdot \sigma\tau(a).$$

Ersetzen wir $x_\sigma \cdot \sigma(x_\tau)$ durch $x_{\sigma\tau}$ und beachten wir, daß $\sigma\tau$ mit τ die Gruppe G durchläuft, so erhalten wir

$$x_\sigma \cdot \sigma(\alpha) = \sum_\tau x_\tau \tau(a) = \alpha,$$

so daß

$$x_\sigma = \frac{\alpha}{\sigma(\alpha)}$$

gilt.

Es sei K der Fixpunktkörper von G. Betrachtet man nur solche Lösungen der Noetherschen Gleichungen, die in K liegen, so vereinfachen sich die Gleichungen zu:

$$x_{\sigma\tau} = x_\sigma x_\tau,$$

da ja σ die Elemente von K fest läßt. Faßt man x_σ als eine Abbildung von G in K auf, so bedeuten diese Gleichungen, daß x_σ ein Charakter von G in K ist. Kombinieren wir dies mit Satz 28, so erhalten wir

Satz 29. *Es sei E eine normale Erweiterung von K mit der Gruppe G. Zu jedem Charakter $C(\sigma)$ von G in K kann man ein Element $\alpha \neq 0$ aus E finden, so daß $C(\sigma) = \frac{\alpha}{\sigma(\alpha)}$ ist. Ist umgekehrt $\alpha \neq 0$ ein Element aus E, so daß $C(\sigma) = \frac{\alpha}{\sigma(\alpha)}$ für alle σ in K liegt, so ist $C(\sigma)$ ein Charakter von G in K. Das Element α hat dann die Eigenschaft, daß α^r in K liegt, wobei r das kleinste gemeinsame Vielfache der Ordnungen der Gruppenelemente von G ist.*

Wir haben bereits alles bewiesen bis auf die letzte Aussage von Satz 29. Um diese zu beweisen, brauchen wir nur zu zeigen, daß $\sigma(\alpha^r) = \alpha^r$ für jedes σ aus G gilt. Es ist aber

$$\frac{\alpha^r}{\sigma(\alpha^r)} = \left(\frac{\alpha}{\sigma(\alpha)}\right)^r = (C(\sigma))^r = C(\sigma^r) = C(1) = 1.$$

Wir bringen noch eine weitere Anwendung von Satz 28. Das Produkt aller Bilder eines Elementes α aus E bei Anwendung aller Automorphismen aus G ist ein Element von K, da es offenbar zum Fixpunktkörper von G gehört. Es wird die *Norm* von α genannt und mit $N(\alpha)$ bezeichnet. Offenbar ist $N(\alpha)N(\beta) = N(\alpha\beta)$, $N\left(\frac{\alpha}{\beta}\right) = \frac{N(\alpha)}{N(\beta)}$. Gehört σ zu G, so hat $\sigma(\alpha)$ dieselben Bilder wie α, es ist also $N(\sigma(\alpha)) = N(\alpha)$. Für $\alpha \neq 0$ ist also $N\left(\frac{\alpha}{\sigma(\alpha)}\right) = 1$. Man verdankt *Hilbert* den Satz, daß in Körpern mit zyklischer Gruppe die Umkehrung gilt:

Satz 30. *Ist die Gruppe G der normalen Erweiterung E von K zyklisch von der Ordnung n und σ eine Erzeugende von G, so sind die Elemente $\beta = \frac{\alpha}{\sigma(\alpha)}$, mit $\alpha \neq 0$ aus E, die einzigen Lösungen der Gleichung $N(\beta) = 1$.*

Beweis. Die Gruppe G besteht aus den Elementen σ^i, wobei wir für i alle positiven ganzen Zahlen nehmen. Es sei $N(\beta) = \prod_{\nu=0}^{n-1} \sigma^\nu(\beta) = 1$. Wir setzen für jedes i

$$x_{\sigma^i} = \prod_{\nu=0}^{i-1} \sigma^\nu(\beta).$$

Vermehrt man i um n, so nimmt das Produkt genau den Faktor $N(\beta) = 1$ an, es hängt also x_{σ^i} wirklich nur von σ^i ab. Man findet

$$x_{\sigma^i}\sigma^i(x_{\sigma^k}) = \prod_{\nu=0}^{i-1} \sigma^\nu(\beta) \prod_{\mu=0}^{k-1} \sigma^{i+\mu}(\beta) = \prod_{\nu=0}^{i+k-1} \sigma^\nu(\beta) = x_{\sigma^{i+k}}.$$

Das System x_{σ^i} ist also eine Lösung der Noetherschen Gleichungen, und es gibt daher nach Satz 28 ein Element $\alpha \neq 0$ in E, so daß $x_{\sigma^i} = \frac{\alpha}{\sigma^i(\alpha)}$ ist. Für $i = 1$ folgt einerseits $x_\sigma = \beta$, andererseits ist $x_\sigma = \frac{\alpha}{\sigma(\alpha)}$. Unser Satz ist damit bewiesen.

M. Kummersche Körper

Es sei K ein Körper, der primitive r-te Einheitswurzeln enthält, und G eine endliche abelsche multiplikative Gruppe vom Exponenten r, d.h. eine abelsche Gruppe, in der die Ordnung jedes Elements ein Teiler von r ist. Die Charaktere von G in K sollen der Kürze halber *Charaktere von G* genannt werden. Für jeden Charakter $C(\sigma)$ gilt $(C(\sigma))^r = C(\sigma^r) = C(1) = 1$, man sieht also, daß die Werte der Charaktere r-te Einheitswurzeln sind. Wenn C_1 und C_2 Charaktere sind, so ist auch $C_1(\sigma)C_2(\sigma)$ ein Charakter, der mit C_1C_2 bezeichnet werde. Da auch $(C_1(\sigma))^{-1}$ ein Charakter ist, bilden die Charaktere bei dieser Komposition eine Gruppe $\hat{G}$, die *Charakterengruppe*, oder auch die *duale Gruppe* von G.

Schreibt man den Basissatz für abelsche Gruppen auf multiplikative Gruppen um, so sieht man, daß es k Elemente $\tau_1, \tau_2, \ldots, \tau_k$ in der Gruppe G gibt mit den Ordnungen $m_1, m_2, \ldots, m_k$, so daß jedes Element σ sich in der Form

$$(*) \qquad \sigma = \tau_1^{i_1}\tau_2^{i_2}\ldots\tau_k^{i_k}$$

schreiben läßt. Dabei ist i_ν modulo m_ν eindeutig bestimmt.

Ist C ein Charakter und $\varepsilon_\nu = C(\tau_\nu)$ (eine m_ν-te Einheitswurzel wegen der Ordnung von τ_ν), so ist $C(\sigma) = \varepsilon_1^{i_1}\varepsilon_2^{i_2}\dots\varepsilon_k^{i_k}$. Wählt man umgekehrt jedes ε_ν als m_ν-te Einheitswurzel, so wird durch diese Formel ein Charakter von G definiert. Jeder Charakter C kann also durch einen Vektor $(\varepsilon_1, \varepsilon_2, \dots, \varepsilon_k)$ beschrieben werden, und dem Produkt zweier Charaktere entspricht das komponentenweise Produkt der zugeordneten Vektoren. Es sei C_s derjenige Charakter, bei dem ε_s eine feste *primitive* m_s-te Einheitswurzel ist, die anderen ε_ν dagegen 1 sind. Dann läßt sich offenbar jeder Charakter C in der Form $C = C_1^{l_1}C_2^{l_2}\dots C_k^{l_k}$ schreiben, wobei l_ν modulo m_ν eindeutig bestimmt ist. Dies zeigt, daß die Gruppe G mit der Gruppe $\hat{G}$ isomorph ist, insbesondere dieselbe Ordnung wie G hat. Ist $\sigma \neq 1$ ein gegebenes Element von G, geschrieben in der Form (*), so ist einer der Exponenten i_ν nicht durch m_ν teilbar. Es ist dann das betreffende $C_\nu(\sigma) \neq 1$. Zu jedem Element $\sigma \neq 1$ kann man also einen Charakter C finden, so daß $C(\sigma) \neq 1$ ist.

Es sei σ ein Element von G. Man betrachte bei variablem Charakter C das Element $C(\sigma)$ als Funktion von C. Da wir das Produkt C_1C_2 von Charakteren durch die Formel $C_1C_2(\sigma) = C_1(\sigma)C_2(\sigma)$ erklärt hatten, ist diese Funktion von C ein Charakter von $\hat{G}$. Es ist dadurch jedem Element σ von G ein Charakter von $\hat{G}$ zugeordnet. Das Produkt zweier solcher Charaktere $C(\sigma)$ und $C(\tau)$ von $\hat{G}$ muß durch $C(\sigma)C(\tau) = C(\sigma\tau)$ erklärt werden, und wir sehen, daß diesem Produkt das Element $C(\sigma\tau)$ entspricht. Es sei $\sigma \neq \tau$. Können die beiden Charaktere $C(\sigma)$ und $C(\tau)$ übereinstimmen? Das bedeutete $C(\sigma) = C(\tau)$ für alle C, d.h., $C(\sigma\tau^{-1}) = 1$. Wegen $\sigma\tau^{-1} \neq 1$ gibt es aber ein C mit $C(\sigma\tau^{-1}) \neq 1$. Da die Charakterengruppe von $\hat{G}$ die gleiche Ordnung wie $\hat{G}$, also wie G hat, liefert $C(\sigma)$ *alle* Charaktere von $\hat{G}$, wenn σ die Gruppe G durchläuft. Man kann also G in natürlicher Weise als die Charakterengruppe von $\hat{G}$ auffassen.

Die in L. bewiesenen Sätze sollen nun auf gewisse Körpererweiterungen angewendet werden. Es sei K ein Körper, der eine primitive r-te Einheitswurzel enthält, und E eine normale Erweiterung von K, deren Automorphismengruppe G eine *abelsche* Gruppe vom Exponenten r ist. Unter anderem soll gezeigt werden, daß der Körper E durch Adjunktion r-ter Wurzeln aus Elementen von K erhalten werden kann. Es liegt also nahe, die Menge A aller derjenigen Elemente $\alpha \neq 0$ von E zu betrachten, die r-te Wurzeln aus Elementen von K sind, für die also α^r in K liegt. Die Menge A ist eine multiplikative

Gruppe und enthält trivialerweise als Untergruppe die Menge K^* aller von Null verschiedenen Elemente von K. Die Faktorgruppe A/K^* ist aufs engste mit der Charakterengruppe $\hat{G}$ von G verknüpft. Es sei nämlich C ein Charakter von G. Auf Grund von Satz 29 gibt es ein Element α von E, so daß $C(\sigma) = \frac{\alpha}{\sigma(\alpha)}$ für jedes σ erfüllt ist; überdies liegt α^r in K, es ist also α ein Element von A. Wenn $\frac{\alpha}{\sigma(\alpha)} = \frac{\beta}{\sigma(\beta)}$ für alle σ gilt, so folgt $\frac{\alpha}{\beta} = \sigma\left(\frac{\alpha}{\beta}\right)$, so daß $\frac{\alpha}{\beta}$ in K^* liegen muß. Jedem Charakter C ist also genau eine Nebengruppe αK^* zugeordnet. Ist umgekehrt α ein Element von A, so ist $\alpha^r = a$ ein Element von K, also $(\sigma(\alpha))^r = a$, so daß $\frac{\alpha}{\sigma(\alpha)}$ eine r-te Einheitswurzel, also ein Element von K ist. Auf Grund von Satz 29 ist dann $\frac{\alpha}{\sigma(\alpha)}$ ein Charakter von G. Diese Zuordnung gibt also eine umkehrbar eindeutige Abbildung von $\hat{G}$ auf die Faktorgruppe A/K^*. Sind $C_1(\sigma) = \frac{\alpha}{\sigma(\alpha)}$, $C_2(\sigma) = \frac{\beta}{\sigma(\beta)}$, so folgt $C_1 C_2(\sigma) = \frac{\alpha\beta}{\sigma(\alpha\beta)}$. Dies zeigt, daß unsere Abbildung ein Isomorphismus von $\hat{G}$ auf A/K^* ist. Insbesondere ist A/K^* eine endliche Gruppe. Man adjungiere nun alle Elemente von A zu K und bezeichne den erhaltenen Zwischenkörper mit E_0, und mit U die Untergruppe von G, zu der E_0 gehört, die also alle Elemente von E_0 fest läßt. U läßt insbesondere die Elemente von A fest. Enthielte U ein Element $\sigma \neq 1$, so könnte man, weil G eine abelsche Gruppe ist, einen Charakter C finden, so daß $C(\sigma) \neq 1$ ist. Wegen $C(\sigma) = \frac{\alpha}{\sigma(\alpha)}$ bei geeignetem α aus A, würde also σ dieses α nicht fest lassen, was ein Widerspruch ist. Aus $U = 1$ folgt aber jetzt $E_0 = E$.

Jeder Körper E_1 zwischen K und E gehört zu einer Untergruppe U von G. Da G abelsch ist, ist U Normalteiler von G, also ist E_1 eine normale Erweiterung von K, deren Automorphismengruppe G/U wieder abelsch vom Exponenten r ist. Also kann die entwickelte Theorie auch auf E_1 angewendet werden. Man erhält E_1 aus K durch Adjunktion einer Menge B zu K; dabei besteht B aus denjenigen Elementen $\beta \neq 0$ von E_1, für die β^r in K liegt. Offenbar ist B eine K^* enthaltende Untergruppe von A. Es müssen daher zwischen K^* und A mindestens so viele Zwischengruppen liegen, als es Zwischenkörper E_1 gibt, d. h. als es Untergruppen U von G gibt. Eine beliebige Zwischengruppe B entspricht aber genau einer Untergruppe B/K^* von

A/K^*. Es ist A/K^* mit $\hat{G}$, also mit G isomorph. Dies zeigt, daß die Anzahl der Zwischengruppen genau sogroß ist wie die Anzahl der Untergruppen U. Wir haben also eine umkehrbar eindeutige Abbildung der Zwischenkörper E_1 auf die Zwischengruppen B hergestellt. Insbesondere erhält man durch Adjunktion einer von A verschiedenen Zwischengruppe niemals den ganzen Körper E.

Bezeichnen wir mit A^i die Menge aller r-ten Potenzen von Elementen aus A und mit K^{*r} die Menge aller r-ten Potenzen der Elemente von K^*, deren r-te Wurzeln in E liegen. Die Faktorgruppe A^r/K^{*r} besteht aus Nebengruppen aK^{*r}, und die r-ten Wurzeln der Elemente von aK^{*r} unterscheiden sich von $\sqrt[r]{a}$ lediglich um einen trivialen Faktor aus K^*. Der Leser überlegt sich leicht, daß die Abbildung von A/K^* auf A^r/K^{*r}, bei welcher der Nebengruppe αK^* die Nebengruppe $\alpha^r K^{*r}$ zugeordnet ist, einen Isomorphismus darstellt. Dadurch ist die Charakterengruppe $\hat{G}$ mit Hilfe von Elementen des Grundkörpers beschreibbar.

Nehmen wir nun überdies an, daß die Gruppe G zyklisch ist. Dann ist auch A/K^* zyklisch, besteht also aus den Potenzen einer einzigen Nebengruppe αK^*. Statt A zu K zu adjungieren, genügt es vollauf, das einzige Element α zu adjungieren. In diesem Fall ist also E durch Adjunktion einer einzigen r-ten Wurzel zu K zu erhalten.

Wir fassen unsere bisherigen Resultate zusammen in

Satz 31. *Es sei K ein Körper, der eine primitive r-te Einheitswurzel enthält, und E eine normale Erweiterung von K, deren Automorphismengruppe G abelsch vom Exponenten r ist. Eine solche Erweiterung wird ein Kummerscher Körper genannt. Ist A die Menge derjenigen Elemente $\alpha \neq 0$ von E, für die α^r in K liegt, so ist $\hat{G}$ mit A/K^* und mit A^r/K^{*r} isomorph. E wird aus K durch Adjunktion der Elemente von A erhalten. Ist B eine zwischen A und K^* gelegene Gruppe, so ist $K(B)$ ein Zwischenkörper, und die Beziehung zwischen den B und den Zwischenkörpern ist umkehrbar eindeutig. Sollte G zyklisch sein, so kann E aus K durch Adjunktion einer einzigen r-ten Wurzel eines Elementes von K erhalten werden.*

Sind $a_1, a_2, \ldots, a_t$ gegebene von Null verschiedene Elemente von K, so interpretiert man das Symbol $E = K\left(\sqrt[r]{a_1}, \sqrt[r]{a_2}, \ldots, \sqrt[r]{a_t}\right)$ als den Zerfällungskörper des Polynoms $(x^r - a_1)(x^r - a_2) \ldots (x^r - a_t)$ (da sich ja die verschiedenen Wurzeln eines Faktors $x^r - a$ nur um Einheitswurzeln voneinander unterscheiden und diese zu K gehören).

Die Ableitung des Polynoms $x^r - a_\nu$ ist rx^{r-1} und hat nur die Wurzel 0, weil ja r nicht durch die Charakteristik von K teilbar sein kann, wenn in K primitive r-te Einheitswurzeln liegen. Jeder Faktor $x^r - a_\nu$ hat also nur einfache Wurzeln, E ist also eine normale Erweiterung von K. Unter dem Symbol $\sqrt[r]{a_\nu}$ ist irgendeine fest gewählte Wurzel α_ν von $x^r - a_\nu$ zu verstehen. Bei einem Automorphismus σ von E wird α_ν nur eine r-te Einheitswurzel $\varepsilon_\nu(\sigma)$ als Faktor annehmen; denn $\alpha_\nu^r = a_\nu$ zieht $(\sigma(\alpha_\nu))^r = a_\nu$ nach sich. Es gilt also $\sigma(\alpha_\nu) = \varepsilon_\nu(\sigma)\alpha_\nu$, $\nu = 1, 2, \ldots, t$, und da die α_ν den Körper E erzeugen, ist durch diese Formeln σ beschrieben. Sind σ und τ Elemente der Automorphismengruppe G von E, so folgt $\tau(\sigma(\alpha_\nu)) = \varepsilon_\nu(\sigma)\tau(\alpha_\nu) = \varepsilon_\nu(\sigma)\varepsilon_\nu(\tau)\alpha_\nu$, weil $\varepsilon_\nu(\sigma)$ in K liegt. Andererseits ist $\tau(\sigma(\alpha_\nu)) = \varepsilon_\nu(\tau\sigma)\alpha_\nu$ und folglich $\varepsilon_\nu(\tau\sigma) = \varepsilon_\nu(\sigma)\varepsilon_\nu(\tau)$. Daraus folgt $\varepsilon_\nu(\tau\sigma) = \varepsilon_\nu(\sigma\tau)$, G ist also eine abelsche Gruppe. Ferner ist $\varepsilon_\nu(\sigma^r) = (\varepsilon_\nu(\sigma))^r = 1$, also ist G vom Exponenten r.

Sollte $t = 1$ sein, also $E = K\left(\sqrt[r]{a_1}\right)$, so tritt nur ein einziges $\varepsilon_1(\sigma)$ auf, und die Gruppe G ist isomorph mit der Gruppe der dabei vorkommenden Einheitswurzeln. Als endliche Gruppe in einem Körper ist sie zyklisch, und als Untergruppe der Gruppe der r-ten Einheitswurzeln ist ihre Ordnung ein Teiler von r.

Kehren wir wieder zu beliebigem t zurück und betrachten wir die multiplikative Gruppe aller Elemente der Form $\alpha_1^{\nu_1} \cdot \alpha_2^{\nu_2} \ldots \alpha_t^{\nu_t} \cdot a$, wobei die ν_i beliebige ganze Zahlen und a ein beliebiges Element von K^* ist. Diese Gruppe ist Untergruppe von A und enthält K^*. Sie erzeugt den Körper E, wenn man sie zu K adjungiert. Folglich muß sie die ganze Gruppe A des Körpers E sein.

Die Gruppe A^r besteht aus den Elementen $a_1^{\nu_1} a_2^{\nu_2} \ldots a_t^{\nu_t} \cdot a^r$ bei beliebigen ν_i und beliebigen Elementen a aus K^*, Die Gruppe $\hat{G}$ ist dann isomorph mit der Faktorgruppe A^r/K^{*r}.

Es ergibt sich

Satz 32. *Es sei K ein Körper, der eine primitive r-te Einheitswurzel enthält und $a_1, a_2, \ldots, a_t$ beliebige Elemente aus K^*. Dann ist die Erweiterung $E = K\left(\sqrt[r]{a_1}, \sqrt[r]{a_2}, \ldots, \sqrt[r]{a_t}\right)$ ein Kummerscher Körper. Die Charakterengruppe $\hat{G}$ seiner Automorphismengruppe ist isomorph zu A^r/K^{*r}, wobei A^r die Menge aller Elemente der Form $a_1^{\nu_1} a_2^{\nu_2} \ldots a_t^{\nu_t} a^r$ mit ganzzahligen ν_i und beliebigem a aus K^* ist.*

Für $t = 1$ ist die Automorphismengruppe zyklisch, und ihre Ordnung ein Teiler von r.

N. Existenz einer normalen Basis

Der folgende Satz ist für jeden Körper richtig, obwohl wir ihn nur für den Fall beweisen, daß K unendlich viele Elemente enthält.

Satz 33. *Ist E eine normale Erweiterung von K und sind $\sigma_1, \sigma_2, \ldots, \sigma_n$ die Elemente ihrer Automorphismengruppe G, so gibt es ein Element θ in E derart, daß die n Elemente $\sigma_1(\theta), \sigma_2(\theta), \ldots, \sigma_n(\theta)$ bezüglich K linear unabhängig sind.*

Beweis. Auf Grund der Folgerung zu Satz 24 gibt es ein α derart, daß $E = K(\alpha)$ ist. Es sei $f(x)$ das irreduzible Polynom zu α. Wir setzen $\sigma_i(\alpha) = \alpha_i$,

$$g(x) = \frac{f(x)}{(x-\alpha) f'(\alpha)} \quad \text{und} \quad g_i(x) = \sigma_i(g(x)) = \frac{f(x)}{(x-\alpha_i) f'(\alpha_i)}.$$

$g_i(x)$ ist ein Polynom in E, das α_k für $k \neq i$ zur Wurzel hat, und es ist daher

$$g^i(x) g_k(x) \equiv 0 \,(\mathrm{mod}\, f(x)) \quad \text{für} \quad i \neq k. \tag{1}$$

In der Gleichung

$$g_1(x) + g_2(x) + \cdots + g_n(x) - 1 = 0 \tag{2}$$

ist die linke Seite von höchstens dem Grade $n-1$. Ist (2) für n verschiedene Werte von x richtig, so muß die linke Seite identisch 0 sein. Solche n Werte sind $\alpha_1, \alpha_2, \ldots, \alpha_n$, denn es ist $g_i(\alpha_i) = 1$ und $g_k(\alpha_i) = 0$ für $k \neq i$.

Wir multiplizieren (2) mit $g_i(x)$, verwenden (1) und erhalten

$$(g_i(x))^2 \equiv g_i(x) \,(\mathrm{mod}\, f(x)). \tag{3}$$

Wir werden jetzt zeigen, daß die Determinante

$$D(x) = |\sigma_i \sigma_k(g(x))|, \qquad i, k = 1, 2, \ldots, n \tag{4}$$

von Null verschieden ist. Wir berechnen ihr Quadrat modulo $f(x)$, indem wir Spalten mit Spalten multiplizieren. Wegen (1), (2) und (3) ergeben sich in der Hauptdiagonale Einsen und an allen übrigen Stellen Nullen. Somit ist

$$(D(x))^2 \equiv 1 \,(\mathrm{mod}\, f(x)),$$

also insbesondere $D(x) \neq 0$.

In Gleichung (4) wird die Variable x auf der rechten Seite so behandelt, als ob sie bei allen Automorphismen fest bliebe. Man kann

daher für x in Formel (4) spezielle Werte einsetzen, wenn auch diese bei allen Automorphismen fest bleiben, d. h., man kann Elemente von K eintragen.

$D(x)$ kann nur endlich viele Wurzeln in K haben. Wählen wir a aus K verschieden von diesen Wurzeln, so ist $D(a) \neq 0$. Nun setzen wir $\theta = g(a)$. Dann ist die Determinante

$$|\sigma_i \sigma_k(\theta)| \neq 0. \tag{5}$$

Betrachten wir nun eine beliebige lineare Relation $x_1 \sigma_1(\theta) + x_2 \sigma_2(\theta) + \cdots + x_n \sigma_n(\theta) = 0$ mit x_i aus K. Wenden wir alle Automorphismen σ_i darauf an, so erhalten wir n homogene Gleichungen in den n Unbekannten x_i und mit der Determinante (5). Daher sind alle $x_i = 0$, unser Satz ist also bewiesen.

Mit Hilfe eines solchen Elementes θ, dessen Bilder bei G eine *Normalbasis* liefern, kann man in besonders einfacher Weise den zu einer Untergruppe U von G gehörigen Zwischenkörper berechnen. Jedes Element α von E läßt sich eindeutig in der Form

$$\alpha = \sum_{\sigma} c_\sigma \sigma(\theta) \tag{6}$$

schreiben, wobei σ die Gruppe G durchläuft, und jedes c_σ in K liegt. Das Element α wird dann und nur dann zum Fixpunktkörper von U gehören, wenn $\tau(\alpha) = \alpha$ für alle τ aus U ist. Wenden wir τ auf (6) an, und ersetzen σ in der Summation durch $\tau^{-1}\sigma$, so folgt $\tau(\alpha) = \sum_{\sigma} c_{\tau^{-1}\sigma} \sigma(\theta)$. Das Element α ist also genau dann im Fixpunktkörper, wenn $c_{\tau^{-1}\sigma} = c_\sigma$ für alle τ aus U und alle σ aus G. Das Element $\tau^{-1}\sigma$ durchläuft bei festem σ die Nebengruppe $U\sigma$. Die erhaltene Bedingung bedeutet also, daß c_σ auf vollen Nebengruppen den gleichen Wert annimmt. Wir verwenden das Symbol $U\sigma(\theta)$ für die Summe der Bilder von θ bei allen Automorphismen der Nebengruppe $U\sigma$. Sind also $U\sigma_1, U\sigma_2, \ldots, U\sigma_j$ alle Nebengruppen, so besteht der Fixpunktköper zu U aus allen Elementen der Form

$$\alpha = c_1 \sigma_1 U_1(\theta) + c_2 U\sigma_2(\theta) + \cdots + c_j U\sigma_j(\theta),$$

wobei die c_i in K liegen. Die j Elemente $U\sigma_i(\theta)$ spannen also den Vektorraum des Fixpunktkörpers zu U über K auf.

Sollte U Normalteiler von G sein, so ist $U\sigma_i = \sigma_i U$ und folglich $U\sigma_i(\theta) = \sigma_i(U(\theta))$. Das bedeutet, daß $U(\theta)$ eine Normalbasis des Fixpunktkörpers ergibt.

0. Der Translationssatz

Es sei K ein Körper, $p(x)$ ein separables Polynom in K und E ein Zerfällungskörper für $p(x)$. Ferner sei B eine beliebige Erweiterung von K. Wir bezeichnen mit EB den Zerfällungskörper von $p(x)$, wenn $p(x)$ als Polynom in B aufgefaßt wird. Sind dann $\alpha_1, \alpha_2, \ldots, \alpha_s$ die Wurzeln von $p(x)$ in EB, so ist $K(\alpha_1, \alpha_2, \ldots, \alpha_s)$ ein Unterkörper von EB, und natürlich ein Zerfällungskörper für $p(x)$ über K. Nach der Folgerung aus Satz 10 sind E und $K(\alpha_1, \alpha_2, \ldots, \alpha_s)$ isomorph. Es bedeutet daher keine Einschränkung der Allgemeinheit, wenn wir in der Folge $E = K(\alpha_1, \alpha_2, \ldots, \alpha_s)$ setzen und daher annehmen, daß E ein Unterkörper von EB ist. Ferner ist $EB = B(\alpha_1, \alpha_2, \ldots, \alpha_s)$. Der Körper EB ist der kleinste Körper, der sowohl E als auch B enthält. Er wird der aus E und B *komponierte* Körper genannt, und dies erklärt das Symbol EB.

Wir bezeichnen mit $E \wedge B$ die Menge derjenigen Elemente, die sowohl in E als auch in B liegen. Wie man leicht sieht, ist $E \wedge B$ ein Körper, und zwar ein Zwischenkörper zu K und E.

Satz 34. (Translationssatz). *Ist G die Automorphismengruppe von E über K und H die Gruppe von EB über B, so ist H isomorph zu der Untergruppe von G, die $E \wedge B$ zum Fixpunktkörper hat.*

Beweis. Es sei σ ein Element von H. Es läßt den Körper B und daher auch den Körper K invariant. Der Körper E wird dabei isomorph in EB abgebildet,und auf Grund von Satz 17 wird diese Abbildung durch ein Element $\bar{\sigma}$ von G bewirkt, ist also einfach $\bar{\sigma}$. Kennt man $\bar{\sigma}$, so kennt man die Bilder der Erzeugenden α_i von E bei σ; und da die α_i auch Erzeugende von EB über B sind, ergibt das die Kenntnis von σ. Unsere Zuordnung ist also eine eineindeutige Abbildung von H *in* G. Daß dem Produkt $\sigma\tau$ zweier Elemente von H das Produkt $\bar{\sigma}\bar{\tau}$ zugeordnet ist, ist unmittelbar evident. Es liegt also ein Isomorphismus von H *in* G vor.

Um H näher zu beschreiben, können wir nach der Natur der Bildgruppe $\bar{H}$ fragen, insbesondere nach dem Fixpunktkörper von $\bar{H}$. Er besteht aus denjenigen Elementen α von E, die bei jedem σ von $\bar{H}$, d. h. aber bei jedem σ aus H fest bleiben. Da B der ganze Fixpunktkörper von H ist, so ist also der Fixpunktkörper von $\bar{H}$ der Körper $E \wedge B$.

III. ANWENDUNGEN VON A. N. MILGRAM

A. Hilfsbetrachtungen aus der Gruppentheorie

Es seien M und M' Mengen. Ist f eine Abbildung von M in M' und A eine Teilmenge von M, so werde mit $f(A)$ die Menge der Bilder $f(a)$ aller Elemente a aus A bezeichnet; $f(A)$ heiße das Bild von A. Ist B eine Teilmenge von M', so werde mit $f^{-1}(B)$ die Menge aller m aus M bezeichnet, für die $f(m)$ zu B gehört; man nennt $f^{-1}(B)$ das Urbild von B. Da f nicht notwendig eine Abbildung von M *auf* M' ist, kann es auch bei nicht leerem B vorkommen, daß $f^{-1}(B)$ die leere Menge ist. Wie schon früher, bezeichnen wir mit $A_1 \cap A_2$ den *Durchschnitt* der Mengen A_1 und A_2, mit $A_1 \cup A_2$ die *Vereinigungsmenge* von A_1 und A_2. Die Aussage „a ist ein Element von A", werde durch $a \in A$ abgekürzt.

Es seien nun G und G' zwei Gruppen und f eine Abbildung von G in G. Wir nennen f einen *Homomorphismus* von G in G', wenn $f(\sigma\tau) = f(\sigma)f(\tau)$ gilt für alle $\sigma, \tau \in G$. Man sieht leicht, daß $f(1) = 1$ und $f(\sigma^{-1}) = (f(\sigma))^{-1}$ ist.

Ist N' eine Untergruppe von G', so ist das Urbild $N = f^{-1}(N')$ eine Untergruppe von G. In der Tat bedeutet $\sigma, \tau \in N$, daß $f(\sigma), f(\tau) \in N'$ ist. Dann ist aber auch $f(\sigma\tau) = f(\sigma)f(\tau) \in N'$, also $\sigma\tau \in N$. Ebenso folgt $\sigma^{-1} \in N$. Sollte N' Normalteiler von G' sein, so ist auch N Normalteiler von G, denn für $\sigma \in G$, $\tau \in N$ folgt $f(\sigma\tau\sigma^{-1}) = f(\sigma)f(\tau)(f(\sigma))^{-1} \in f(\sigma)N'(f(\sigma))^{-1} = N'$, so daß $\sigma\tau\sigma^{-1} \in N$ ist.

Das Bild N' einer Untergruppe N von G kann in ähnlicher Weise als Untergruppe von G' nachgewiesen werden. Sollte N Normalteiler von G sein, und sollte die Abbildung f eine Abbildung *auf* G' sein, so kann man für $\sigma' \in G'$, $\tau' \in N'$ Elemente $\sigma \in G$, $\tau \in N$ finden, für die $f(\sigma) = \sigma'$ und $f(\tau) = \tau'$ gilt. Da $\sigma\tau\sigma^{-1} \in N$, folgt durch Anwendung von f, daß $\sigma'\tau'\sigma'^{-1} \in N'$ ist. Demnach ist N' Normalteiler von G'.

Da das Einselement von G' ein Normalteiler von G' ist, so ist das Urbild K ein Normalteiler von G. Man nennt K den *Kern* des Homomorphismus f. Er besteht aus denjenigen Elementen $k \in G$, für die $f(k) = 1$ ist. Wir wollen nun bestimmen, welche Elemente von G die gleichen Bilder bei der Abbildung f haben. Die Gleichung

$f(\sigma) = f(\tau)$ ist gleichbedeutend mit $f(\sigma\tau^{-1}) = 1$, also auch mit $\sigma\tau^{-1} \in K$, oder $\sigma \in K\tau = \tau K$. Es haben also genau alle Elemente einer Nebengruppe modulo K gleiche Bilder. Man ordne nun jeder Nebengruppe σK das Element $f(\sigma) \in f(G)$ zu, welches das gemeinsame Bild aller Elemente von σK ist. Es ist dies eine umkehrbar eindeutige Abbildung der Faktorgruppe G/K *auf* das Bild $f(G)$ von G. Man sieht leicht, daß diese Abbildung auch ein Homomorphismus ist. Da sie umkehrbar eindeutig ist, ist sie ein Isomorphismus zwischen G/K und $f(G)$.

Schließlich zeigen wir, daß jeder Normalteiler N von G als Kern eines Homomorphismus vorkommen kann. Man bilde nämlich G auf die Faktorgruppe G/N ab, indem man $f(\sigma) = \sigma N$ setzt. Man sieht unmittelbar, daß f ein Homomorphismus ist, der jedes Element auf diejenige Nebengruppe abbildet, in der das Element liegt. Das Einselement von G/N ist N, das Urbild dieses Einselements daher die Menge N. Also ist N der Kern dieser Abbildung f, die wir den *kanonischen* Homomorphismus von G auf G/N nennen.

Satz 35. *Es sei f ein Homomorphismus von G auf G', N ein Normalteiler von G, und $N' = f(N)$. Dann induziert f in kanonischer Weise einen Homomorphismus g von G/N auf G'/N'. Sollte außerdem $N = f^{-1}(N')$ gelten, so ist dieser Homomorphismus ein Isomorphismus.*

Beweis. Als Bild der Nebengruppe σN bei g werde $f(\sigma N) = f(\sigma)N'$ definiert. Daß g ein Homomorphismus ist, ist unmittelbar zu sehen. Daß G/N *auf* G'/N' abgebildet wird, folgt daraus, daß f eine Abbildung *auf* ist. Bestimmen wir den Kern unseres Homomorphismus: xN gehört zum Kern, wenn $f(x)N' = N'$, wenn also $f(x) \in N'$ ist, d. h. x also zu $f^{-1}(N')$ gehört. Sollte also $f^{-1}(N') = N$ sein, so muß $x \in N$ und $xN = N$ sein. Der Kern unseres Homomorphismus ist dann das Einselement von G/N. Unser Homomorphismus ist daher ein Isomorphismus.

Satz 36. *Es sei H eine Untergruppe von G und N ein Normalteiler von G. Dann ist $H \cap N$ ein Normalteiler von H, und die Faktorgruppe $H/H \cap N$ ist isomorph zu HN/N (einer Untergruppe von G/N).*

Beweis. Es sei f die kanonische Abbildung von G auf G/N. Beschränkt man die Abbildung f auf die Untergruppe H, so erhält man einen Homomorphismus g von H in G/H. Das Bild $g(H)$ besteht aus den Nebengruppen σN mit $\sigma \in H$, und man sieht leicht, daß es die

Faktorgruppe HN/N ist. Der Kern von g ist $H \cap N$. Also ist $H \cap N$ Normalteiler von H und die Faktorgruppe $H/H \cap N$ isomorph dem Bild von H bei dem Homomorphismus g.

Folgerung. Haben G, H und N die gleiche Bedeutung wie in Satz 36 und ist G/N eine abelsche Gruppe, so ist auch $H/H \cap N$ eine abelsche Gruppe.

Definition. Eine Gruppe G heißt *auflösbar*, wenn es eine absteigende Kette von Untergruppen

$$G = G_0 > G_1 > G_2 > \cdots > G_s = 1$$

gibt, so daß G_i Normalteiler von G_{i-1} ist und daß die Faktorgruppen G_{i-1}/G_i für $i = 1, 2, \ldots, s$ *abelsch* sind.

Satz 37. *Jede Untergruppe einer auflösbaren Gruppe ist auflösbar.*

Beweis. Es sei G auflösbar, und G_i die zugehörige Normalteilerkette. H sei eine Untergruppe von G und man setze $H_i = H \cap G_i$. Dann ist auch $H_{i-1} \cap G_i = H \cap G_{i-1} \cap G_i = H \cap G_i = H_i$. Es ist G_i Normalteiler von G_{i-1} und H_{i-1} Untergruppe von G_{i-1}. Da G_{i-1}/G_i abelsch ist, ist auch $H_{i\,1}/H_{i\,1} \cap G_i$ nach der Folgerung aus Satz 36 abelsch. Dies ist aber H_{i-1}/H_i.

Satz 38. *Das homomorphe Bild einer auflösbaren Gruppe ist auflösbar.*

Beweis. Es sei G auflösbar und G_i die zugehörige Normalteilerkette. f sei ein Homomorphismus, und man setze $f(G) = G'$. Wir zeigen, daß $G_i' = f(G_i)$ eine zu G gehörige Normalteilerkette ist. Schränkt man nämlich f auf G_{i-1} ein, so erhält man einen Homomorphismus von G_{i-1} auf G_{i-1}'. Es ist G_i Normalteiler von G_{i-1} und G_i' sein Bild. Auf Grund von Satz 35 wird dadurch auch eine homomorphe Abbildung von G_{i-1}/G_i *auf* G_{i-1}'/G_i' induziert. Nun ist G_{i-1}/G_i abelsch, und ein homomorphes Bild einer abelschen Gruppe ist trivialerweise abelsch.

Es soll nun gezeigt werden, daß eine Gruppe von Primzahlpotenzordnung immer auflösbar ist. Zum Beweis werden einige weitere Begriffe der Gruppentheorie benötigt.

Es sei G eine Gruppe. Zwei Elemente a und b heißen *konjugiert*, wenn es ein $x \in G$ gibt, so daß $b = xax^{-1}$ ist. Man sieht leicht, daß jedes Element mit sich selbst konjugiert ist; ist a mit b konjugiert, so ist auch b mit a konjugiert; ist endlich a mit b und b mit c konjugiert, so ist auch a mit c konjugiert. Es liegt also, wie man sagt, eine

Äquivalenzrelation vor. Die Gruppe G kann also mit elementfremden Klassen so überdeckt werden, daß die Elemente einer Klasse wohl untereinander konjugiert sind, nicht aber mit einem Element einer andern Klasse. Eine Klasse kann sehr wohl nur aus einem Element bestehen. Dies ist genau dann der Fall, wenn $xax^{-1} = a$ ist für alle $x \in G$. Das bedeutet $xa = ax$, das Element a ist also mit jedem Element $x \in G$ vertauschbar. Man sieht mühelos, daß die Menge Z dieser Elemente a eine abelsche Untergruppe von G bildet, die das *Zentrum* von G genannt wird. Z ist natürlich mit jedem Element von G vertauschbar, so daß Z also ein Normalteiler von G ist.

Es sei $a \in G$. Um die mit a konjugierten Elemente zu erhalten, muß man alle xax^{-1} berechnen, wobei x die Gruppe G durchläuft. Verschiedene x können sehr wohl das gleiche konjugierte Element ergeben. Die Gleichung $xax^{-1} = yay^{-1}$ ist mit $(y^{-1}x)a = a(y^{-1}x)$ und daher mit der Vertauschbarkeit der Elemente a und $y^{-1}x$ gleichbedeutend. Es sei nun N_a die Menge aller mit a vertauschbaren z, so daß unsere vorige Gleichung $y^{-1}x \in N_a$ oder auch $x \in yN_a$ geschrieben werden kann. Man überlegt sich nun leicht, daß N_a eine Gruppe ist. Damit ist gezeigt, daß die Elemente x aus einer Nebengruppe yN_a genau diejenigen sind, die jeweils a in dasselbe Konjugierte überführen. Die Anzahl der verschiedenen Konjugierten von a, mit anderen Worten die Anzahl der Elemente in der Klasse von a, ist also gleich der Anzahl der Nebengruppen von N_a. Es sei nun G eine endliche Gruppe der Ordnung n. Dann ist die Anzahl der Elemente in jeder Klasse ein Teiler von n. Die Klassen überdecken die Gruppe G, die Summe der Klassenanzahlen ist also n. Die Klassenanzahl 1 tritt bei z Klassen auf, wobei z die Ordnung des Zentrums ist. Man erhält also eine Formel der Form

$$n = z + d_1 + d_2 + \cdots,$$

wobei jedes d_i ein von 1 verschiedener Teiler von n ist. Nehmen wir nun an, es sei $n = p^r$, wobei $r \geqq 1$ und p eine Primzahl ist. Dann sind sowohl n als auch alle d_i durch p teilbar, so daß z durch p teilbar ist. Das aber bedeutet, daß die Gruppe G ein nicht-triviales Zentrum Z besitzt. Die Auflösbarkeit der Gruppe G kann nun leicht durch Induktion nach der Ordnung gezeigt werden. Eine Gruppe der Ordnung 2 ist abelsch und daher auflösbar. Die Faktorgruppe G/Z hat eine Primzahlpotenzordnung kleiner als n, so daß wir annehmen können, daß ihre Auflösbarkeit gezeigt ist. Es sei G_i/Z eine Normalteilerkette für G/Z, welche diese Auflösbarkeit zeigt. Es sei f der kanonische Homomorphismus von G_{i-1} *auf* G_{i-1}/Z. Das Urbild einer Menge von

Nebengruppen von Z in G_{i-1} ist einfach die Vereinigungsmenge dieser Nebengruppen. $G_i/Z = N'$ ist ein Normalteiler von G_{i-1}/Z mit abelscher Faktorgruppe, und sein Urbild ist G_i. Also ist G_i ein Normalteiler von G_{i-1}, und sein Bild bei f ist wieder N'. Auf Grund von Satz 35 ist die Faktorgruppe G_{i-1}/G_i isomorph mit der Faktorgruppe von G_i/Z in G_{i-1}/Z, also abelsch. Die G_i bilden nun eine absteigende Normalteilerkette, deren letztes Glied Z selbst ist. Fügt man als weitere Gruppe die 1 hinzu, so hat man eine Normalteilerkette, die die Auflösbarkeit von G zeigt, weil ja Z abelsch ist.

Hiermit ist bewiesen

Satz 39. *Jede Gruppe von Primzahlpotenzordnung ist auflösbar.*

Im Gegensatz hierzu soll nun von gewissen Gruppen die Nichtauflösbarkeit gezeigt werden.

Es sei M eine endliche Menge und φ eine umkehrbar eindeutige Abbildung von M auf sich selbst. Wir nennen eine solche Abbildung eine *Permutation* von M. Sind φ und ψ Permutationen von M, so sind auch $\varphi\psi$ (man wende erst ψ und dann φ an) und φ^{-1} Permutationen. Da das Assoziativgesetz bei Hintereinanderausführen von Abbildungen trivial ist, bilden die Permutationen von M eine Gruppe. Ist n die Anzahl der Elemente von M, so heißt diese Gruppe *die symmetrische Gruppe* von n Elementen und wird mit S_n bezeichnet. Ihre Ordnung ist $n!$. Eine Untergruppe von S_n nennt man eine *Permutationsgruppe*. Sind a, b, c drei voneinander verschiedene Elemente von M, so verstehe man unter dem Symbol (a, b, c) diejenige Permutation von M, welche a auf b, b auf c und c auf a abbildet, dagegen alle übrigen Elemente von M fest läßt. Wir nennen (a, b, c) einen *Dreierzyklus*. Es ist $(a, b, c)^{-1} = (c, b, a)$. Wir beweisen nun den folgenden

Hilfssatz. *Es sei G eine Permutationsgruppe von mindestens 5 Elementen, die jeden Dreierzyklus enthält, und N ein Normalteiler von G mit abelscher Faktorgruppe. Dann enthält auch N jeden Dreierzyklus.*

Beweis. Es sei f der kanonische Homomorphismus von G auf G/N und (a, b, c) ein beliebiger Dreierzyklus. Wir wählen aus M zwei weitere Elemente d und e. Man setze $x = (d, b, a)$ und $y = (a, e, c)$. Das Bild des Elements $x^{-1}y^{-1}xy$ bei f ist $x'^{-1}y'^{-1}x'y'$, wobei x' und y' die Bilder von x und y sind. Dieses Bild ist deswegen 1, weil die Bild-

gruppe nach Voraussetzung abelsch ist. Daher gehört $x^{-1}y^{-1}xy$ zum Kern N von f. Nun ist

$$x^{-1}y^{-1}xy = (a, b, d)(c, e, a)(d, b, a)(a, e, c) = (a, b, c).$$

Satz 40. *Für $n \geqq 5$ ist die symmetrische Gruppe S_n nicht auflösbar.*

Beweis. Es liege eine mit S_n beginnende Normalteilerkette mit abelschen Faktorgruppen vor. Da S_n alle Dreierzyklen enthält, muß nach dem Hilfssatz jede Gruppe der Kette alle Dreierzyklen enthalten. Die Kette kann also nicht mit der Gruppe 1 enden.

B. Auflösbarkeit von Gleichungen durch Radikale

Um Schwierigkeiten mit der Charakteristik zu vermeiden, beschränken wir uns bei den folgenden Sätzen auf Körper der Charakteristik 0.

Es sei K ein Körper, K_i eine aufsteigende Folge von Erweiterungen mit dem Endglied F:

$$K = K_0 < K_1 < K_2 < \cdots < K_s = F.$$

Die Erweiterung F von K soll eine *Radikalerweiterung* genannt werden, wenn für $i = 1, 2, \ldots, s$ der Körper $K_i = K_{i-1}(\alpha_i)$ ist, wobei α_i eine Wurzel eines Polynoms $x^{n_i} - a_i$ in K_{i-1} ist.

Die Erweiterung F heiße *halbabelsch*, wenn K_i eine normale Erweiterung von K_{i-1} mit *abelscher Automorphismengruppe* ist.

Hilfssatz 1. *Jede Radikalerweiterung F von K kann in eine halbabelsche Erweiterung eingebettet werden.*

Beweis. Es sei F eine Radikalerweiterung von K und K_i die zugehörige Folge von Körpern. Ferner sei m das kleinste gemeinsame Vielfache aller n_i. Man adjungiere zu F eine primitive m-te Einheitswurzel. Wir betrachten die folgende Kette von Körpern:

$$K_0 = K < K_0(\varepsilon) < K_1(\varepsilon) < \cdots < K_s(\varepsilon) = F(\varepsilon).$$

Unmittelbar vor Satz 27 wurde gezeigt, daß die Automorphismengruppe von $K(\varepsilon)$ über K abelsch ist. Der Körper $K_i(\varepsilon)$ wird aus $K_{i-1}(\varepsilon)$ durch Adjunktion von α_i erhalten. Da $K_{i-1}(\varepsilon)$ die n_i-ten Einheitswurzeln enthält, folgt aus Satz 32, daß die Automorphismengruppe von $K_i(\varepsilon)$ über $K_{i-1}(\varepsilon)$ sogar zyklisch ist. $F(\varepsilon)$ ist daher eine halbabelsche Erweiterung von K, die F enthält.

Hilfssatz 2. *Die Erweiterungen F_1 und F_2 von K seien halbabelsche und in einem gemeinsamen Oberkörper von K enthalten. Dann ist der aus F_1 und F_2 komponierte Körper F_1F_2 auch eine halbabelsche Erweiterung von K.*

Beweis. Es seien

$$K = K_0 \subset K_1 \subset \cdots \subset K_s = F_1$$

und

$$K = K_0' \subset K_1' \subset \cdots \subset K_t' = F_2$$

zugehörige Körperketten. Wir bilden die neue Kette

$$K = K_0 \subset K_1 \subset \cdots \subset K_s =$$
$$= F_1K_0' \subset F_1K_1' \subset F_1K_2' \subset \cdots \subset F_1K_t' = F_1F_2.$$

K_i ist nach Voraussetzung abelsch über K_{i-1}. Wir müssen zeigen, daß F_1K_i' über F_1K_{i-1}' abelsch ist. Nach Voraussetzung ist K_i' über K_{i-1}' abelsch. F_1K_{i-1}' ist eine Erweiterung von K_{i-1}', deren Komposition mit K_i' der Körper F_1K_i' ist. Nach Satz 34 ist F_1K_i' eine normale Erweiterung von F_1K_{i-1}', deren Automorphismengruppe mit einer Untergruppe der Automorphismengruppe von K_i' über K_{i-1}' isomorph ist. Daher ist auch diese Gruppe abelsch, F_1F_2 also eine halbabelsche Erweiterung von K.

Hilfssatz 3. *Es sei F eine halbabelsche Erweiterung von K. Man kann F in eine normale, halbabelsche Erweiterung von K einbetten.*

Beweis. Der Körper F ist separabel. Daher kann F in eine normale Erweiterung Ω eingebettet werden. Es seien $F_1, F_2, \ldots, F_e$ die Bilder von F bei allen Automorphismen von Ω über K, und $\Omega_0 = F_1F_2 \ldots F_e$ der aus diesen Bildern komponierte Körper. Mit F ist auch jedes Bild von F halbabelsch und Hilfssatz 2 zeigt, daß auch Ω_0 eine halbabelsche Erweiterung von K ist, die natürlich F enthält. Es braucht daher nur noch gezeigt zu werden, daß Ω_0 eine normale Erweiterung von K ist. Nun wird jeder Isomorphismus von Ω_0 in Ω durch einen Automorphismus σ von Ω über K erzeugt. σ permutiert aber nur die Körper F_i, führt also Ω_0 in sich über. Jeder Isomorphismus von Ω_0 in Ω ist also ein Automorphismus. Ω_0 ist daher eine normale Erweiterung von K.

Definition. Es sei $f(x)$ ein irreduzibles Polynom in K. Das Polynom $f(x)$ heißt *durch Radikale lösbar*, wenn es eine Radikalerweiterung F von K gibt, in der $f(x)$ eine Wurzel hat.

Satz 41. *Es sei $f(x)$ ein irreduzibles Polynom in K und E ein Zerfällungskörper von $f(x)$ mit der Automorphismengruppe G. Es ist $f(x)$ dann und nur dann durch Radikale lösbar, wenn die Gruppe G auflösbar ist, und es gibt dann sogar eine Radikalerweiterung von K, in der $f(x)$ in Linearfaktoren zerfällt.*

Beweis. 1. Wenn $f(x)$ durch Radikale lösbar ist, so gibt es eine Radikalerweiterung von K, die eine Wurzel α von $f(x)$ enthält. Auf Grund der Hilfssätze 1 und 3 gibt es also eine normale halbabelsche Erweiterung Ω_0 von K, in der $f(x)$ die Wurzel α hat. Der Folgerung aus Satz 15 entnehmen wir, daß $f(x)$ in Ω_0 in Linearfaktoren zerfällt. Ω_0 enthält daher einen Zerfällungskörper E' von $f(x)$. Die Automorphismengruppe von Ω_0 über K ist auflösbar und hat die Automorphismengruppe von E' über K als Faktorgruppe, d. h. als homomorphes Bild. Auf Grund von Satz 38 ist daher die Automorphismengruppe von E' über K auflösbar. Ist E der ursprünglich gegebene Zerfällungskörper zu $f(x)$, so sind E und E' isomorph, haben also auch isomorphe Automorphismengruppen.

2. Die Automorphismengruppe G eines Zerfällungskörpers E von $f(x)$ sei auflösbar; n sei die Ordnung von G. Es sei ε eine primitive n-te Einheitswurzel und $K' = K(\varepsilon)$. Trivialerweise ist K' eine Radikalerweiterung von K. Der Körper $E' = EK'$ ist Zerfällungskörper von $f(x)$ über K', und die Automorphismengruppe G' von E' über K' ist auf Grund von Satz 34 isomorph zu einer Untergruppe, auf Grund von Satz 37 also auflösbar. Es sei nun

$$G' = G_0 > G_1 > G_2 > \cdots > G_s = 1$$

eine Normalteilerkette mit abelschen Faktorgruppen. Die zugehörigen Fixpunktkörper von E' bilden eine aufsteigende Folge von Körpern:

$$K' = K_0' < K_1' < K_2' < \cdots < K_s' = E'.$$

Es ist dann E' eine normale Erweiterung von K_{i-1}', deren Automorphismengruppe G_{i-1} ist. Weil G_i Normalteiler von G_{i-1} ist, ist K_i' eine normale Erweiterung von K_{i-1}', deren Automorphismengruppe G_{i-1}/G_i also abelsch ist. Da K_{i-1}' die n-ten Einheitswurzeln enthält, ist K_i' ein Kummerscher Körper über K_{i-1}', und daher durch Adjunktion von Radikalen zu erhalten. Man sieht unmittelbar, daß K_i' eine Radikalerweiterung von K_{i-1}' ist. Im ganzen ist nunmehr E' eine Radikalerweiterung von K und $f(x)$ zerfällt in E' in lauter Linearfaktoren.

C. Die Galoissche Gruppe einer Gleichung

In diesem Abschnitt kann die Charakteristik der betrachteten Körper wieder beliebig sein.

Es sei K ein Körper, $f(x)$ ein Polynom in K ohne mehrfache Wurzeln, E der Zerfällungskörper von $f(x)$ und $f(x) = (x - \alpha_1)\ (x - \alpha_2) \ldots (x - \alpha_n)$ die Zerlegung von $f(x)$ in E. Die Elemente $\alpha_1, \alpha_2, \ldots, \alpha_n$ sind Erzeugende von E. Wie schon bemerkt, kann jedes Element σ der Automorphismengruppe G von E über K eindeutig durch den Effekt von σ auf alle α_i beschrieben werden. Jedes σ permutiert die Elemente α_i, es kann also G als Permutationsgruppe einer Menge von n Elementen aufgefaßt werden. Zur Vereinfachung faßt man G überdies nur als Permutationsgruppe der Indizes i der α_i auf, so daß G die Ziffern $1, 2, \ldots, n$ permutiert. In dieser Auffassung ist es üblich, G als die *Galoissche Gruppe* der Gleichung $f(x) = 0$ zu bezeichnen. Das Polynom $f(x)$ braucht in K nicht irreduzibel zu sein. Es sei $p(x)$ ein in K irreduzibler Faktor von $f(x)$. Ein Element σ aus G kann eine Wurzel von $p(x)$ nur in eine andere Wurzel von $p(x)$ überführen. Sind andrerseits α_i und α_j zwei Wurzeln von $p(x)$, so sind die beiden Körper $K(\alpha_i)$ und $K(\alpha_j)$ isomorph, und dieser Isomorphismus kann durch ein Element von G bewirkt werden. Nach einer Umnumerierung der Wurzeln können wir annehmen, daß etwa $\alpha_1, \alpha_2, \ldots, \alpha_r$ die Wurzeln von $p(x)$ sind. Die Elemente von G permutieren dann einerseits die Ziffern $1, 2, \ldots, r$ nur unter sich; ein geeignetes Element von G wird andrerseits eine beliebige dieser ersten r Ziffern in eine beliebige andere dieser ersten r Ziffern überführen. Wir nennen eine Teilmenge der Ziffern $1, 2, \ldots, n$ mit dieser Eigenschaft ein *Transitivitätsgebiet* von G. Es ist jetzt klar, daß die Ziffern $1, 2, \ldots, n$ in elementfremde Transitivitätsgebiete zerlegt sind, die in einer umkehrbar eindeutigen Beziehung zu den irreduziblen Faktoren von $f(x)$ stehen. Kennt man also die Permutationsgruppe G, so kann man daraus die Zerlegung von $f(x)$ in irreduzible Faktoren aus K ablesen. $f(x)$ ist dann und nur dann irreduzibel, wenn die Ziffern $1, 2, \ldots, n$ ein einziges Transitivitätsgebiet bilden. Man sagt dann, die Gruppe G sei transitiv. Ist U eine Untergruppe von G und B der zugehörige Fixpunktkörper, so ist U die *Galoissche Gruppe* von $f(x)$, wenn $f(x)$ als Polynom in B aufgefaßt wird. Die Transitivitätsgebiete von U entsprechen dann der Zerlegung von $f(x)$ in irreduzible Faktoren aus B.

Es sei $f(x)$ irreduzibel in K, die Gruppe G also transitiv. U sei ein Normalteiler von G, also B eine *normale* Erweiterung von K. Man wähle irgendeinen irreduziblen Faktor $p(x)$ von $f(x)$ in B. Wenn σ ein Element von G ist, so bewirkt σ einen Automorphismus von B. Das Bild $\sigma(p(x))$ ist also wieder ein irreduzibler Faktor in B. Nun ist G transitiv. Es gibt also ein $\sigma \in G$, welches eine Wurzel von $p(x)$ in jede andere Wurzel von $f(x)$ überführt. Jeder in B irreduzible Faktor von $f(x)$ hat also die Form $\sigma(p(x))$. Es folgt, daß die Transitivitätsgebiete von U alle gleiche Länge haben. Sollte n eine Primzahl sein, so ist also entweder U selbst transitiv, oder alle Transitivitätsgebiete haben die Länge 1, d.h., U besteht nur aus der Identität. Da dieses Resultat später gebraucht wird, formulieren wir es als

Satz 42. *Ist G eine transitive Permutationsgruppe der Ziffern $1, 2, \ldots, q$, wobei q eine Primzahl ist, so ist jeder von 1 verschiedene Normalteiler von G wieder transitiv.*

Definition. Es seien k ein Körper, $u_1, u_2, \ldots, u_n$ unabhängige Veränderliche und $K = k(u_1, u_2, \ldots, u_n)$ der Körper aller rationalen Funktionen von $u_1, u_2, \ldots, u_n$ mit Koeffizienten aus k. Das zu K gehörige Polynom

$$f(x) = x^n + u_1 x^{n-1} + \cdots + u_n$$

werde die *allgemeine Gleichung* n-ten Grades über k genannt.

Es soll nun die Galoissche Gruppe der allgemeinen Gleichung n-ten Grades bestimmt werden. Wir bestimmen einen Zerfällungskörper E' von $f(x)$ und nehmen an, daß in E'

$$f(x) = (x - \xi_1)(x - \xi_2) \cdots (x - \xi_n)$$

gilt. Die u_i sind Polynome in den ξ_j, es ist u_i die mit $(-1)^i$ multiplizierte Summe aller Produkte von je i verschiedenen der Wurzeln ξ_j. Andererseits hatten wir in II, G das folgende Beispiel betrachtet: Wir wählten n unabhängige Veränderliche $x_1, x_2, \ldots, x_n$ und betrachteten den Körper $E = k(x_1, x_2, \ldots, x_n)$ und das Polynom

$$g(x) = (x - x_1)(x - x_2) \ldots (x - x_n) = x^n + a_1 x^{n-1} + \cdots + a_n.$$

Im Körper E betrachteten wir die $n!$ Permutationen der x_i und zeigten, daß der Fixpunktkörper der Körper $k(a_1, a_2, \ldots, a_n)$ ist. Die Elemente a_i drücken sich durch die x_j in derselben Weise aus, wie die u_i durch die ξ_j. (Die genauere Polynomeigenschaft der symmetrischen Funktionen wird hier nicht gebraucht werden.)

Es sei nun $\varphi(u_1, u_2, \ldots, u_n)$ ein Polynom der u_i mit Koeffizienten aus k, welches die Eigenschaft hat, daß sein Wert für $u_i = a_i$ verschwindet, für welches also $\varphi(a_1, a_2, \ldots, a_n) = 0$ ist. Trägt man für die a_i die Ausdrücke in den x_i ein, so soll sich also ein Ausdruck in den x_i ergeben, in dem sich alle Glieder wegkürzen. Ersetzt man hierin jedes x_i durch ξ_i, so erhält man auch einen Ausdruck, in dem sich alle Terme wegheben, der also Null ist. Diese Ersetzung läuft aber einfach darauf hinaus, daß man jedes a_i durch u_i ersetzt, so daß also bereits das ursprüngliche Polynom $\varphi(u_1, u_2, \ldots, u_n) = 0$ sein mußte.

Damit ist gezeigt, daß verschiedene Polynome $\varphi(u_1, u_2, \ldots, u_n)$ verschiedene Werte $\varphi(a_1, a_2, \ldots, a_n)$ haben. Ordnet man also jedem Polynom $\varphi(u_1, u_2, \ldots, u_n)$ seinen Wert $\varphi(a_1, a_2, \ldots, a_n)$ zu, so ist eine umkehrbar eindeutige Abbildung der Polynome in den u_i auf die Polynome in den a_j gegeben. Der Körper K besteht aus den Quotienten von Polynomen in den u_i, der Körper $k(a_1, a_2, \ldots, a_n)$ aus den Quotienten von Polynomen in den a_i. Der Leser überlegt sich leicht, daß aus unseren Betrachtungen die Isomorphie von K auf $k(a_1, a_2, \ldots, a_n)$ folgt, wobei die Elemente von k fest bleiben und jedes u_i auf a_i abgebildet wird. Das Bild des Polynoms $f(x)$ ist dabei das Polynom $g(x)$. Auf Grund von Satz 10 kann dieser Isomorphismus zu einem Isomorphismus zwischen E und E' erweitert werden, wobei die Wurzeln ξ_i von $f(x)$ nach möglicher Umnumierung auf die Wurzeln x_i von $g(x)$ abgebildet werden.

Nun war $k(a_1, a_2, \ldots, a_n)$ der Fixpunktkörper unter der symmetrischen Gruppe S_n. Aus der bewiesenen Isomorphie folgt der berühmte *Satz von Abel*:

Satz 43. *Die Galoissche Gruppe der allgemeinen Gleichung n-ten Grades über k ist die symmetrische Gruppe S_n. Hat k die Charakteristik 0 und ist $n \geqq 5$, so ist die allgemeine Gleichung n-ten Grades nicht durch Radikale lösbar.*

Der letzte Teil dieses Satzes ergibt sich aus den Sätzen 40 und 41.

Man kann die Frage aufwerfen, ob eine beliebig vorgegebene Permutationsgruppe als Galoissche Gruppe einer passenden Gleichung auftreten kann. Dies ist bei geeigneter Wahl des Grundkörpers in der Tat möglich. Es sei also G eine gegebene Permutationsgruppe von n Ziffern, $f(x)$ die allgemeine Gleichung n-ten Grades über k und die beiden Körper K und E' wie vorher definiert. G ist Untergruppe von S_n und folglich ist G die Galoissche Gruppe von $f(x)$, wenn $f(x)$ als Polynom des Fixpunktkörpers B unter G aufgefaßt wird. Da jede

endliche abstrakte Gruppe als Permutationsgruppe dargestellt werden kann, so folgt auch noch, daß es bei geeignetem Grundkörper normale Erweiterungen gibt, deren Automorphismengruppe isomorph zur gegebenen abstrakten Gruppe ist. Dagegen ist es ein ungelöstes Problem, ob es solche normale Erweiterungen über dem Körper der rationalen Zahlen gibt.

Es sei K ein beliebiger Körper, $f(x)$ ein in K irreduzibles Polynom von *Primzahlgrad* q, dessen Galoissche Gruppe auflösbar sei. Es soll gezeigt werden, daß die Struktur von G in diesem Falle besonders einfach ist. Zunächst existiert also eine Normalteilerkette

$$G = G_0 > G_1 > G_2 > \cdots > G_s = 1,$$

wobei sukzessive Faktorgruppen abelsch sind. Insbesondere ist G_{s-1} selbst eine abelsche Gruppe. Da jede Untergruppe von G_{s-1} ein Normalteiler von G_{s-1} ist, und eine von 1 verschiedene Gruppe sicher zyklische Untergruppen enthält, so kann man annehmen, daß $G_{s-1} \neq 1$ und zyklisch ist, indem man nötigenfalls noch eine weitere Gruppe zu unserer Kette hinzufügt. Es sei G_{s-1} die von σ erzeugte zyklische Gruppe. Da die Gruppe G transitiv ist, so folgt aus Satz 42, daß auch jede Gruppe G_i, insbesondere also G_{s-1}, transitiv ist. Die Potenzen von σ erfüllen die Gruppe G_{s-1}, sie müssen wegen der Transitivität die Ziffer 1 in alle anderen Ziffern überführen. Ist $\sigma^i(1) = \sigma^j(1)$, so folgt $\sigma^{i-j}(1) = 1$. Ist also d die kleinste positive Zahl, für die $\sigma^d(1) = 1$ ist, so sind die Ziffern $1, \sigma(1), \sigma^2(1), \ldots, \sigma^{d-1}(1)$ alle voneinander verschieden und sind alle Ziffern, in die 1 durch eine Potenz von σ übergeführt werden kann. Aus der Transitivität folgt also, daß $d = q$ sein muß. Bei passender Numerierung unserer Ziffern können wir erreichen, daß die Ziffern $1, 2, \ldots, q$ gerade die Ziffern $1, \sigma(1), \sigma^2(1), \ldots, \sigma^{q-1}(1)$ sind. Für $i \leqq q-1$ gilt dann $\sigma(i) = i+1$. Da $\sigma^q(1) = 1$ ist, folgt $\sigma(q) = 1$. Es ist offenbar viel zweckmäßiger, die Ziffern durch die Elemente des Restklassenkörpers Q_q zu ersetzen, weil man dann für jede Ziffer x die Formel $\sigma(x) = x+1$ hat. Offenbar ist $\sigma^i(x) = x+i$. Wenn a, b Elemente von Q_q sind, $a \neq 0$, so ist die Funktion $\Phi(x) = ax+b$ eine umkehrbar eindeutige Abbildung von Q_q auf sich, also eine Permutation.

Definition. Eine Permutationsgruppe der Elemente von Q_q heiße *linear*, wenn jede Permutation dieser Gruppe die Form $\tau(x) = ax+b$, mit festen a, $b \in Q_q$, $a \neq 0$, hat, und wenn die Gruppe die spezielle Permutation $\sigma(x) = x+1$ enthält.

Es sei $a \neq 0, 1$ und $\tau(x) = ax + b$. Dann ist $\tau^2(x) = a^2x + ab + b$. Durch vollständige Induktion folgt

$$\tau^i(x) = a^i x + (a^{i-1} + a^{i-2} + \cdots + 1)b.$$

Da $a \neq 1$ ist, kann dies auch in der Form $\tau^i(x) = a^i x + \frac{a^i - 1}{a - 1} b$ geschrieben werden. Weil $a \neq 0$ ist, gilt in Q_q, daß $a^{q-1} = 1$ ist, und es folgt $\tau^{q-1}(x) = x$. Die Ordnung von τ ist also ein Teiler von $q - 1$, genauer sieht man, daß sie das kleinste i ist, mit $a^i = 1$.

Für $a = 1$ und $b \neq 0$ wird $\tau(x) = x + b$, $\tau^i(x) = x + ib$, und es hat τ die Ordnung q.

Die *einzigen* Elemente der Ordnung q in einer linearen Gruppe sind also die von 1 verschiedenen Potenzen von σ, wobei wie zuvor $\sigma(x) = x + 1$ ist.

Hilfssatz. *Es sei H eine Permutationsgruppe von q Ziffern, q Primzahl, N ein Normalteiler von H und N eine lineare Gruppe. Dann ist H eine lineare Gruppe.*

Beweis. N enthält die Permutation σ. Es sei τ irgendeine Permutation von H. Dann ist $\tau\sigma\tau^{-1}$ ein Element von N, das die Ordnung q hat. Es ist also $\tau\sigma\tau^{-1}$ eine von 1 verschiedene Potenz von σ, etwa $\tau\sigma\tau^{-1} = \sigma^a$, mit einem nicht durch q teilbaren a. Deshalb gilt $\tau\sigma = \sigma^a\tau$, also $\tau\sigma(y) = \sigma^a\tau(y)$. Hieraus folgt $\tau(y + 1) = \tau(y) + a$. Man erhält $\tau(y + 2) = \tau(y) + 2a$, allgemein $\tau(y + x) = \tau(y) + ax$. Setzen wir $y = 0$ und $b = \tau(0)$, so folgt $\tau(x) = ax + b$. Also ist H linear.

Satz 44. *Ist die Galoissche Gruppe G einer irreduziblen Gleichung von Primzahlgrad auflösbar, so ist sie linear.*

Beweis. Die Gruppe G_{s-1} besteht aus den Potenzen von σ, ist also linear. Unser Hilfssatz zeigt durch wiederholte Anwendung auf die Normalteilerkette, daß die Gruppe G linear ist.

Es sei G linear, $\tau \in G$, $\tau(x) = ax + b$. Dann ist $\tau' = \sigma^{b'-b}\tau$ auch in G und hat die Form $\tau'(x) = ax + b'$. Tritt also ein gegebenes a bei einem τ auf, so kommt es mit allen möglichen $b \in Q_q$ in G vor. Insbesondere enthält G ein τ_a mit $\tau_a(x) = ax$. Offenbar gilt $\tau_{a_1} \cdot \tau_{a_2} = \tau_{a_1 a_2}$ und das zeigt, daß die vorkommenden a eine multiplikative Gruppe bilden. Diese multiplikative Gruppe ist Untergruppe der multiplikativen Gruppe aller von Null verschiedenen Elemente von Q_q, sie ist zyklisch und ihre Ordnung d ein Teiler von $q - 1$. Bei gegebenem d

sind die zugehörigen a einfach alle d-ten Einheitswurzeln aus Q_q. Die Ordnung von G ist dann dq, und die Struktur von G ist durch Angabe der Ordnung dq eindeutig bestimmt. Die größtmögliche Ordnung ist $(q-1)q$.

Satz 45. *Jede lineare Gruppe ist auflösbar.*

Beweis. G sei linear und N die von σ erzeugte zyklische Untergruppe. Für alle $\tau \in G$ gilt $\tau\sigma\tau^{-1} = \sigma^a \in N$, so daß N Normalteiler von G ist. Die Auflösbarkeit von G wird gezeigt, indem wir die Faktorgruppe G/N als abelsch nachweisen. Ist τ_a die Permutation $\tau_a(x) = ax$, so besteht die Nebengruppe $N\tau_a$ aus den Permutationen $\tau(x) = ax + b$, mit diesem festen a. Die Nebengruppen sind also die verschiedenen $N\tau_a$. Es ist nun $N\tau_{a_1} \cdot N\tau_{a_2} = N\tau_{a_1}\tau_{a_2} = N\tau_{a_1 a_2} = N\tau_{a_2}N\tau_{a_1}$ und damit ist der Beweis erbracht.

Es sei $\tau(x) = ax + b$. Wir untersuchen die Fixpunkte von τ, also die Lösungen von $ax + b = x$. Für $a \neq 1$ ist dies $\frac{-b}{a-1}$; für $a = 1$ und $b \neq 0$ gibt es keinen Fixpunkt; $a = 1$, $b = 0$ ist die Identität. Keine von der Identität verschiedene Permutation aus G hat also 2 Fixpunkte.

Es seien nun α_i und α_j zwei verschiedene gegebene Wurzeln von $f(x)$. Wir untersuchen den Zwischenkörper $K(\alpha_i, \alpha_j)$. Ein Element τ der zugehörigen Untergruppe muß sowohl α_i als auch α_j fest lassen, hat also zwei Fixpunkte. Auf Grund des Vorhergehenden muß also $\tau = 1$ sein. Das bedeutet aber, daß der Körper $K(\alpha_i, \alpha_j)$ der volle Zerfällungskörper E von $f(x)$ ist. Wir haben damit bewiesen

Satz 46. *Ist die Gruppe G einer irreduziblen Gleichung von Primzahlgrad auflösbar, so wird der Zerfällungskörper bereits durch Adjunktion zweier Wurzeln erzeugt.*

Von diesem Satz soll eine kleine Anwendung gemacht werden. Es sei K Unterkörper des Körpers der reellen Zahlen (K also insbesondere von der Charakteristik 0), $f(x)$ eine in K irreduzible Gleichung von ungeradem Primzahlgrad, die durch Radikale lösbar ist. Es habe ferner das Polynom $f(x)$ zwei reelle Wurzeln. Adjungiert man sie zu K, so erhält man einen reellen Zahlkörper, der wegen Satz 46 Zerfällungskörper von $f(x)$ ist. Es hat dann also $f(x)$ lauter reelle Wurzeln. Im allgemeinen hat also eine solche Gleichung $f(x)$ lauter reelle Wurzeln oder nur eine. Man erhält so die

Folgerung. *Eine in einem reellen Zahlkörper irreduzible Gleichung von ungeradem Primzahlgrad, die durch Radikale lösbar ist, hat entweder genau eine reelle Wurzel oder lauter reelle Wurzeln.*

Der Leser kann sich mühelos eine Gleichung 5-ten Grades mit rationalen Koeffizienten verschaffen, die in Q irreduzibel ist und genau drei reelle Wurzeln hat. Eine solche Gleichung ist dann nicht durch Radikale lösbar. Das Polynom $x^5 - 10x - 2$ ist ein Beispiel dieser Art.

D. Konstruktionen mit Zirkel und Lineal

Unter einer Konstruktionsaufgabe wollen wir das Problem verstehen, aus einem gegebenen geometrischen Objekt ein anderes geometrisches Objekt abzuleiten. Dabei sollen die geometrischen Objekte durch die Bedingung eingeschränkt werden, daß ihre Natur durch eine endliche Anzahl von Punkten und Strecken beschrieben werden kann (Beispielsweise: bei einem Dreieck die drei Eckpunkte; bei einem Kreis Mittelpunkt und Radius).

Man sagt, daß die Konstruktion mit Zirkel und Lineal ausgeführt werden kann, wenn sie in eine endliche Zahl von Schritten zerlegbar ist, deren jeder in einer fest gegebenen Ebene stattfindet und eine der folgenden Möglichkeiten darstellt:

1. Wahl eines beliebigen Punktes in einem, durch die vorangehenden Schritte bestimmten Gebiet der Ebene,

2. Konstruktion der Verbindungsgeraden zweier bereits konstruierter oder gewählter Punkte,

3. Konstruktion eines Kreises mit vorher konstruiertem Mittelpunkt, auf dessen Peripherie ein vorher konstruierter Punkt liegt,

4. Bestimmung der Schnittpunkte zweier vorher konstruierter Geraden oder einer bereits konstruierten Geraden mit einem bereits konstruierten Kreis oder zweier solcher Kreise.

Die Bedingung 1. ist sicher notwendig, da man auf einer leeren Ebene bestimmt mit der Wahl eines Punktes anfangen muß. Dabei denken wir uns diejenigen Strecken in der Ebene gegeben, welche die Natur des ursprünglichen geometrischen Objektes beschreiben, und müssen durch die Konstruktion Strecken erhalten, welche das ge-

suchte geometrische Objekt beschreiben. Die Übersetzung dieser geometrischen Aufgabe in ein algebraisches Problem soll hier nur skizziert werden.

Man führe in der Ebene ein rechtwinkliges kartesisches Koordinatensystem ein und denke sich die gegebenen Strecken etwa auf der positiven x-Achse vom Nullpunkt aus abgetragen. Ihre Endpunkte mögen auf der x-Achse die Werte $a_1, a_2, \ldots, a_r$ haben. Man beginne nunmehr mit der Konstruktion. Nach einer gewissen Anzahl i von Schritten wird man eine gewisse Punktmenge konstruiert haben. Die Menge aller Koordinaten aller konstruierten Punkte werde mit $b_1, b_2, \ldots, b_s$ bezeichnet; die a_ϱ bilden eine Teilmenge davon. Man adjungiert $b_1, b_2, \ldots, b_s$ zum Körper Q der rationalen Zahlen und erhält so einen reellen Zahlkörper K_i. Die bisher konstruierten Geraden und Kreise werden jetzt Gleichungen haben, deren Koeffizienten in K_i liegen. Beim $i+1$-ten Schritt werden neue Punkte nur dann auftreten, wenn der Schritt entweder von der Art 1. oder Art 4. ist. Sollte er von der Art 1. sein, so kann man erreichen, daß der gewählte Punkt rationale Koordinaten hat, und es ist dann $K_{i+1} = K_i$. Ist der Punkt von der Art 4., so tritt bei der Berechnung der Koordinaten der Schnittpunkte höchstens eine Quadratwurzel eines Elements von K_i auf, es ist also entweder $K_{i+1} = K_i$ oder $(K_{i+1}/K_i) = 2$. Die Konstruktion soll als ausgeführt gelten, wenn man die Strecken, die das gewünschte geometrische Objekt beschreiben, vom Nullpunkt aus auf der positiven x-Achse abgetragen hat. Die Koordinaten der Endpunkte dieser Strecken seien $\xi_1, \xi_2, \ldots, \xi_t$. Ist n die Gesamtlänge der Konstruktion, so ist K_n ein Körper, der $\xi_1, \xi_2, \ldots, \xi_t$ enthält. Es werde der Körper $K = Q(a_1, a_2, \ldots, a_r)$ als Grundkörper betrachtet. Dann ist der Körper K_n eine halbabelsche Erweiterung von K, bei der überdies jede Teilerweiterung quadratisch ist. Der Leser gehe nun zu dem Beweis der Hilfssätze in III, B zurück. Setzen wir von der beiden Erweiterungen F_1 und F_2 in Hilfssatz 2 noch überdies voraus, daß die Teilerweiterungen immer quadratisch sind, so hat die Erweiterung F_1F_2 die gleiche Eigenschaft, weil ja die Gruppe von F_1K_i' über F_1K_{i-1}' mit einer Untergruppe der Gruppe von K_i' über K_{i-1}' isomorph ist. Der Beweis von Hilfssatz 3 zeigt dann, daß K_n in eine normale Erweiterung Ω von K eingebettet werden kann, die von K aus durch sukzessive quadratische Erweiterungen erreicht werden kann. Dieser Körper Ω enthält sicher den Körper $F = K(\xi_1, \xi_2, \ldots, \xi_t)$ und folglich auch die kleinste normale Erweiterung E von K, die den Körper F enthält. Der Körper Ω hat als Grad eine Potenz von zwei, folglich auch die beiden Körper F und E.

Unser Standpunkt ist nun folgender: Unabhängig von der geometrischen Konstruktion kann aus dem geometrischen Problem selbst die Natur der zu konstruierenden Größen $\xi_1, \xi_2, \ldots, \xi_t$ abgelesen werden. Die algebraische Natur der beiden Körper E und F muß sich also aus der geometrischen Aufgabe bestimmen lassen. Sollte sich dabei ergeben, daß (F/K) oder (E/K) nicht eine Potenz von zwei sind, so ist nach dem Vorangehenden eine Konstruktion mit Zirkel und Lineal unmöglich.

Es soll nun gezeigt werden

Satz 47. *Es seien $a_1, a_2, \ldots, a_r$ die Daten eines geometrischen Problems, $\xi_1, \xi_2, \ldots, \xi_t$ die zu bestimmenden Größen und $K = Q(a_1, a_2, \ldots, a_r)$. Das geometrische Problem ist genau dann mit Zirkel und Lineal lösbar, wenn alle ξ_i algebraisch über K sind, und wenn überdies die kleinste normale Erweiterung E von K, die $\xi_1, \xi_2, \ldots, \xi_t$ enthält, als Grad eine Potenz von 2 hat.*

Beweis. Die Notwendigkeit dieser Bedingung ist bereits gezeigt. Wir nehmen also an, daß (E/K) eine Potenz von 2 ist, und wollen zeigen, daß jedes Element von E „konstruierbar" ist. Die Automorphismengruppe G von E über K ist nach Satz 39 auflösbar. Es gibt also eine Normalteilerkette

$$G = G_0 \supset G_1 \supset G_2 \supset \cdots \supset G_s = 1.$$

so daß jede Faktorgruppe G_{i-1}/G_i abelsch ist. Jede dieser Faktorgruppen hat als Ordnung eine Potenz von 2. Ist die Ordnung größer als 2, so gibt es eine Untergruppe H/G_i der Ordnung 2, und wir können die neue Gruppe H zwischen G_{i-1} und G_i einschalten. Es kann also angenommen werden, daß alle Faktorgruppen die Ordnung 2 haben. Zu dieser absteigenden Gruppenkette gehört eine aufsteigende Körperkette

$$K = K_0 \subset K_1 \subset \cdots \subset K_s = E.$$

Dabei tritt die eine Schwierigkeit auf, daß einige dieser Körper nicht mehr reell zu sein brauchen. Man nenne nun eine komplexe Zahl konstruierbar, wenn Real- und Imaginärteil konstruierbar sind. Dem Leser ist sicher aus der Schule bekannt, wie man aus Strecken der Längen a, b Strecken der Längen $a \pm b$, ab, $\frac{a}{b}$ (mit ähnlichen Dreiecken) konstruiert. Auch eine Strecke der Länge $\sqrt{a}$ kann konstruiert werden (mittlere Proportionale). Aus den gegebenen Daten $a_1, a_2, \ldots, a_r$

kann also jedes Element von K konstruiert werden. Es sei die Konstruierbarkeit aller Elemente von K_{i-1} bewiesen. Da $(K_i/K_{i-1}) = 2$ ist, kann man K_i durch Adjunktion von $\sqrt{\alpha}$ erhalten, wobei α eine bereits konstruierte komplexe Zahl ist. In der Gaußschen Zahlenebene läuft dies auf die Halbierung eines Winkels und Ziehen einer Quadratwurzel aus einer positiven konstruierbaren Zahl hinaus. Es ist also auch K_i konstruierbar, und unser Satz durch Induktion nach i bewiesen.

Beispiele. 1. *Konstruktion eines regelmäßigen n-Ecks, das einem Kreis vom Radius* 1 *einzuschreiben ist.* Hier ist $K = Q$, $\xi_1 = \cos\frac{2\pi}{n}$, $\xi_2 = \sin\frac{2\pi}{n}$. Gleichwertig damit ist die Konstruktion von

$$\varepsilon = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n},$$

also einer primitiven n-ten Einheitswurzel. Es ist $E = Q(\varepsilon)$ bereits eine normale Erweiterung von Q, so daß es genügt, den Grad dieser Erweiterung zu untersuchen. Auf Grund von Satz 27 ist dieser Grad $\varphi(n)$. Es sei nun $n = p_1^{\nu_1} p_2^{\nu_2} \dots p_r^{\nu_r}$ die Zerlegung von n in verschiedene Primzahlpotenzen. Dann ist

$$\varphi(n) = p_1^{\nu_1-1}(p_1-1)\, p_2^{\nu_2-1}(p_2-1) \dots p_r^{\nu_r-1}(p_r-1).$$

Ist $p_1 = 2$, so ist der Exponent ν_1 beliebig. Ist aber p_i ungerade, so muß $\nu_i = 1$ sein und außerdem $p_i - 1$ eine Potenz von 2, etwa 2^m. Dann ist $p_i = 2^m + 1$. Ist $m = ab$, $a > 1$ und a ungerade, so ist das Polynom $x^{ab} + 1 = (x^b)^a + 1$ durch $x^b + 1$ teilbar, die Zahl $2^m + 1$ also durch $2^b + 1$ teilbar, und $2^m + 1$ ist keine Primzahl. Es muß also m eine Potenz von 2 sein. Für die p_i kommen also nur Zahlen der Form $2^{2^k} + 1$ in Frage. Für $k = 0, 1, 2, 3, 4$ erhält man die Primzahlen 3, 5, 17, 257, 65537. Für $k = 5$ ist die Zahl durch 641 teilbar, und es ist bisher keine weitere Primzahl der Form $2^{2^k} + 1$ gefunden worden. Es sind also genau diejenigen n-Ecke mit Zirkel und Lineal konstruierbar, bei denen n die Form $n = 2^\nu p_1 p_2 \dots p_r$ hat, wobei die p_i verschiedene Primzahlen der Form $2^{2^k} + 1$ sind. Die tatsächliche Konstruktion etwa eines 17-Eckes kann der Leser in der Literatur finden.

2. *Dreiteilung des Winkels.* Ein Winkel von 60° ist konstruierbar. Die Konstruktion des zugehörigen Winkeldrittels würde die Konstruktion eines 18-Eckes nach sich ziehen, und das ist nach 1. unmöglich.

3. *Delisches Problem.* Apollo forderte die Verdoppelung eines vorhandenen würfelförmigen Altars dem Volumen nach (unter Beibehaltung der Würfelgestalt). Gibt man dem ursprünglich vorhandenen Altar die Kantenlänge 1, so soll also die Zahl $\xi = \sqrt[3]{2}$ konstruiert werden. Es ist also $K = Q$, $F = Q(\sqrt[3]{2})$. Da $x^3 - 2$ in Q irreduzibel ist, ist $(F/K) = 3$, die geforderte Konstruktion also unmöglich.