Höhere Algebra

von

Dr. Helmut Hasse
o. Professor für Mathematik an der Universität Hamburg

II
Gleichungen höheren Grades

Mit 5 Figuren

Fünfte, durchgesehene Auflage

Sammlung Göschen Band 932

Walter de Gruyter & Co · Berlin 1967

vormals G. J. Göschen'sche Verlagshandlung · J. Guttentag,
Verlagsbuchhandlung · Georg Reimer · Karl J. Trübner · Veit & Comp.

 — Archiv-Nr. 77 11671. Satz und Druck: Walter de Gruyter & Co., Berlin — Printed in Germany.

Inhalt des zweiten Bandes.

Literatur und Quellen.

Siehe die auf beide Bändchen bezügliche Zusammenstellung zu Beginn des ersten Bändchens.

Inhalt des ersten Bandes.

Einleitung.

Methodische Vorbetrachtungen und Überblick.

In **1**, § 5 haben wir die uns als Leitfaden dienende Grundaufgabe der Algebra formuliert und zwei besonders wichtige Teilaufgaben hervorgehoben. Deren erste, das Auflösungsproblem linearer Gleichungssysteme, wurde in **1**, III und IV vollständig gelöst. Der vorliegende Band **2** ist der zweiten jener Teilaufgaben gewidmet:

Es sei K ein Körper und

$$f(x) \equiv a_0 + a_1 x + \cdots + a_n x^n \qquad (a_n \neq 0,\ n \geqq 1)$$

ein nicht zu K gehöriges Element aus $\mathsf{K}[x]$. Es sollen Methoden zur Gewinnung aller Lösungen der **algebraischen Gleichung**

$$f(x) \doteq 0$$

entwickelt werden.

Da die Gleichung $f(x) \doteq 0$ dasselbe fordert wie $\frac{f(x)}{a_n} = 0$, ist es keine Einschränkung, wenn wir uns im folgenden auf Gleichungen der Form

$$f(x) \equiv a_0 + a_1 x + \cdots + a_{n-1} x^{n-1} + x^n \doteq 0 \qquad (n \geqq 1)$$

beschränken. Wir nennen solche Elemente $f(x)$ aus $\mathsf{K}[x]$ Polynome (in x) **in** oder **aus**[1]) oder **über** K und den eindeutig bestimmten Index $n \geqq 1$ ihren Grad [vgl. **1**, § 5, (2.) [48]]. Für Lösungen einer algebraischen Gleichung $f(x) \doteq 0$ gebrauchen wir ferner die übliche Bezeichnung **Wurzeln des Polynoms $f(x)$.**

Die Behandlungsmethoden für unsere jetzige Aufgabe sind von den in **1** zur Behandlung linearer Gleichungssysteme ver-

[1]) Dies ist deshalb eigentlich nicht korrekt, weil die $f(x)$ Elemente aus $\mathsf{K}[x]$ sind. Unsere Ausdrucksweise bezieht sich also auf die Koeffizienten.

wendeten wegen der folgenden beiden eng zusammenhängenden Umstände grundsätzlich verschieden:

1.) Es kann (im Gegensatz zu **1**, IV) kein allein aus den im Grundkörper K definierten vier elementaren Rechenoperationen gebildetes Verfahren (kurz rationales Rechenverfahren) existieren, um über die Lösbarkeit einer algebraischen Gleichung zu entscheiden und im Lösbarkeitsfalle alle Lösungen zu berechnen.

2.) Lösbarkeit und Lösungsgesamtheit einer algebraischen Gleichung aus K sind (im Gegensatz zu **1**, Satz 84 [149]) abhängig von der Wahl des Grundkörpers, d. h. davon, ob man für die Lösungen nur den Körper K oder irgendeinen Erweiterungskörper von K in Betracht zieht, und im allgemeinen werden algebraische Gleichungen aus K überhaupt erst in geeigneten Erweiterungskörpern von K lösbar.

Für 2.) mag schon hier, die späteren allgemeinen Einsichten illustrierend, das einfache Beispiel der Gleichung $x^2-2 \doteq 0$ genannt werden, die im Körper der rationalen Zahlen keine Lösung, im Körper der reellen Zahlen dagegen die beiden Lösungen $\pm\sqrt{2}$ besitzt. Aus 2.) ergibt sich 1.); denn würde ein Verfahren, wie in 1.) genannt, existieren, so wäre dieses, wie in **1**, Satz 84 [149], unabhängig von der Wahl des Grundkörpers, was 2.) widerspricht [1]).

Wegen 1.) darf unsere Aufgabe nicht dahin verstanden werden, daß die Lösungen einer algebraischen Gleichung im obigen Sinne berechnet werden sollen. Was statt dessen zu erstreben ist, zeigt 2.). Da nämlich für abstrakte Grundkörper (d. h. unter alleiniger Voraussetzung der in **1**, § 1 zusammengestellten Gegebenheiten) nicht von vornherein etwas Entsprechendes zur Verfügung steht, wie im obigen

[1]) Damit soll natürlich nicht gesagt sein, daß nicht für spezielle Grundkörper, z. B. den Körper der rationalen Zahlen, wirkliche Auflösungsverfahren existieren. Nur gehören diese in dem Sinne nicht mehr zur Algebra, als dazu außer den vier elementaren Rechenoperationen noch andere, der Analysis angehörige Hilfsmittel herangezogen werden müssen. Vgl. auch dazu § 11 [77].

Beispiel der aus der Elementarmathematik (Grundlagen der Analysis) bekannte reelle Zahlkörper, da vielmehr im allgemeinen Falle über das Vorhandensein von Erweiterungskörpern, die die Lösung einer algebraischen Gleichung ermöglichen, zunächst keinerlei Kenntnis besteht, kommt es darauf an, solche Erweiterungskörper und damit die Wurzeln algebraischer Gleichungen zu konstruieren.

Unsere Entwicklungen werden demgemäß den folgenden Gang nehmen: Nachdem wir in I und II vorbereitende Tatsachen über die die linken Seiten algebraischer Gleichungen bildenden Polynome aus K einerseits und die (vorläufig hypothetischen) Wurzeln algebraischer Gleichungen aus K in Erweiterungskörpern andererseits auseinandergesetzt haben, konstruieren wir in III die Wurzelkörper algebraischer Gleichungen und damit deren Wurzeln. Dadurch ist dann die obige Aufgabe vom praktischen Standpunkt (analog zu 1, IV — Lösungsbestimmung) als gelöst anzusehen. Vom theoretischen Standpunkt erhebt sich darüber hinaus (analog zu 1, III — Struktur der Lösungsgesamtheit) die hier ganz besonders interessante Frage nach der Struktur der Wurzelkörper algebraischer Gleichungen, insbesondere nach ihrem Aufbau aus möglichst einfachen Bestandteilen. Diese im Mittelpunkt unseres Interesses stehende Frage behandeln wir in IV durch Darlegung der sogenannten Galoisschen Theorie, die die Struktur jener Körper mit der Struktur gewisser endlicher Gruppen, ihrer Galoisgruppen, in engen Zusammenhang bringt. In V beantworten wir schließlich mittels dieser Theorie die Frage nach der Auflösbarkeit algebraischer Gleichungen durch Wurzelzeichen, d. h. die berühmte Frage, wann die Wurzeln einer algebraischen Gleichung unter Hinzunahme der (bei festem Grundkörper nicht unbeschränkt und eindeutig definierten) Operation des Wurzelziehens berechnet werden können.

I. Die linken Seiten algebraischer Gleichungen.

Wir leiten in den §§ 1, 2 dieses Abschnittes im Anschluß an die Entwicklungen von **1**, I eine Reihe bedeutsamer Sätze über Polynome aus K her, die mit deren Auftreten als linke Seiten algebraischer Gleichungen zunächst nichts zu tun haben und erst in den folgenden Abschnitten in diesem Sinne angewendet werden. Diese auf den Integritätsbereich $\mathsf{K}[x]$ der ganzen rationalen Funktionen einer Unbestimmten x über einem Grundkörper K bezüglichen Sätze sind das genaue Analogon zu den in der elementaren Zahlentheorie behandelten Sätzen über den Integritätsbereich Γ der ganzen Zahlen, die sich um den Fundamentalsatz von der eindeutigen Zerlegbarkeit in Primzahlen gruppieren, — ebenso wie auch die Konstruktion des Körpers $\mathsf{K}(x)$ der rationalen Funktionen von x über K von $\mathsf{K}[x]$ aus ganz analog zu der Konstruktion des Körpers P der rationalen Zahlen von Γ aus verläuft, nämlich beidemal als Quotientenkörper. Da wir die später vielfach anzuwendende elementare Zahlentheorie hier nicht voraussetzen wollen, leiten wir die genannten Sätze für die beiden Fälle $\mathsf{K}[x]$ und Γ gleichzeitig, d. h. mit denselben, doppelte Bedeutung tragenden Worten und Zeichen her. In den §§ 1, 2 bezeichnen demnach $f, g, h, \ldots$ Elemente aus $\mathsf{K}[x]$ bzw. Γ. In den §§ 3, 4 dieses Abschnitts entwickeln wir dann mittels der auf den Fall Γ bezüglichen Resultate der §§ 1, 2 noch einige für die Folge wichtige Begriffe und Tatsachen über Gruppen, Integritätsbereiche und Körper, die bei Voraussetzung der elementaren Zahlentheorie schon an früherer Stelle (**1**, I und II) einzufügen gewesen wären.

§ 1. Der Fundamentalsatz von der eindeutigen Zerlegbarkeit in Primelemente in $\mathsf{K}[x]$ und Γ.

A. Teilbarkeitslehre in einem Integritätsbereich.

Der in der Überschrift genannte Fundamentalsatz setzt zu seiner genauen Formulierung die Begriffe der sog. Teilbarkeitslehre in $\mathsf{K}[x]$ bzw. Γ voraus. Da die gemeinsame Eigenschaft von $\mathsf{K}[x]$ und Γ, Integritätsbereich zu sein, hinreicht, um diese Teilbarkeitslehre zu entwickeln, legen wir dabei irgendeinen Integritätsbereich I zugrunde. $f, g, h, \ldots$ sollen dann Elemente aus I bezeichnen.

Definition 1. g heißt **teilbar** durch f oder ein **Vielfaches** von f und f ein **Teiler** von g oder in g **enthalten** (Bezeichnung $f \mid g$, Gegenteil $f \nmid g$), wenn ein $\bar{f}$ existiert, so daß $g = f\bar{f}$ ist.

Es wird natürlich gefordert, daß $\bar{f}$ in I existiere. Unsere Bezeichnungsfestsetzungen erlauben es, derartige Zusätze hier und an ähnlichen Stellen fortzulassen. Es sei aber ausdrücklich betont, daß darauf der Nachdruck in Def. 1 liegt. Würde man auch den Quotientenkörper zu I für die „Existenz" zulassen, so wäre Def. 1 bis auf die Unterscheidung von $f \neq 0$ und $f = 0$ trivial. Demgemäß wird die Teilbarkeitslehre inhaltlos, wenn I mit seinem Quotientenkörper zusammenfällt. Für $\mathsf{K}[x]$ und Γ ist das nicht der Fall.

Aus den in **1**, § 1 dargelegten Grundeigenschaften der Integritätsbereiche ergeben sich ohne weiteres die folgenden Sätze über Teilbarkeit, auf deren einfache Beweise wir verzichten dürfen [1].

Satz 1. Es gelten die Teilbarkeitsrelationen

$$e \mid f, \quad f \mid f, \quad f \mid 0 \text{ für jedes } f,$$
$$0 \nmid f \text{ für } f \neq 0.$$

Satz 2. Aus $f \mid g$, $g \mid h$ folgt $f \mid h$; aus $f_1 \mid g_1$, $f_2 \mid g_2$ folgt $f_1 f_2 \mid g_1 g_2$; aus $hf \mid hg$, $h \neq 0$ folgt $f \mid g$.

Satz 3. Aus $f \mid g_1$, $f \mid g_2$ folgt $f \mid g_1\bar{g}_1 + g_2\bar{g}_2$ für beliebige $\bar{g}_1, \bar{g}_2$.

Definition 2. f heißt **Einheit**, wenn $f \mid e$.

Wir bezeichnen Einheiten im folgenden mit a, b. Es gibt solche, z. B. e.

[1]) Auch für eine Reihe weiterer Sätze des § 1 deuten wir die ganz elementaren Beweise nur durch Hinweis auf die heranzuziehenden früheren Sätze an.

Satz 4. Die Einheiten von $\mathfrak{I}$ bilden eine Untergruppe (Normalteiler) der multiplikativen abelschen Gruppe aller Elemente $\neq 0$ des Quotientenkörpers zu $\mathfrak{I}$.

Beweis: Aus $a_1 \mid e$, $a_2 \mid e$ folgt $a_1 a_2 \mid e$ (Satz 2); es ist $e \mid e$ (Satz 1); aus $a \mid e$ folgt, daß $\frac{e}{a}$ zu $\mathfrak{I}$ gehört und $\frac{e}{a} \mid e$ ist (Def. 1). Daraus ergibt sich die Behauptung nach **1**, Satz 19, 26 [55, 60] (vgl. auch **1**, § 6, Beisp. 1 [53]).

Definition 3. Sind von 0 verschiedene f_1, f_2 nach dem Normalteiler der Einheiten kongruent, d. h. ist $\frac{f_1}{f_2} = a$, so heißen f_1 und f_2 **assoziiert.** Die Restklassen nach diesem Normalteiler heißen die **Klassen assoziierter Elemente.**

Die Klasse der zu einem Element $f \neq 0$ assoziierten Elemente wird hiernach durch alle af gebildet, wo a alle Einheiten durchläuft. Für $f = 0$ mag ebenfalls die Gesamtheit af, d. h. das einzige Element 0, als die zugehörige Klasse assoziierter Elemente angesehen werden. — Im Sinne von **1**, §§ 7—9 erstreckt sich die Restklasseneinteilung nach dem Normalteiler der Einheiten nicht nur auf den Integritätsbereich $\mathfrak{I}$, sondern auch auf dessen Quotientenkörper. Wir verfolgen sie hier aber nur im Integritätsbereich $\mathfrak{I}$ selbst. Wir können das um so eher tun, als die einem f aus $\mathfrak{I}$ entsprechende Klasse ganz zu $\mathfrak{I}$ gehört.

Aus Def. 1—3 folgt unmittelbar:

Satz 5. f_1 und f_2 sind dann und nur dann assoziiert, wenn $f_1 \mid f_2$ und $f_2 \mid f_1$ ist.

Nach Satz 2, 5 ist eine Teilbarkeitsrelation $f \mid g$ gleichbedeutend mit jeder Relation $f' \mid g'$, wo f' zu f, g' zu g assoziiert ist. Es genügt daher für die Teilbarkeitslehre, aus jeder Klasse assoziierter Elemente nur einen Repräsentanten zu betrachten; doch ist die Auszeichnung eines solchen nach einem durchgängigen Prinzip für allgemeines $\mathfrak{I}$ nicht möglich (vgl. aber Def. 7 [13]).

Nach dem Vorhergehenden besitzt jedes g als sog. triviale Teiler alle Einheiten und alle zu g assoziierten Elemente. Um diese bequem ausschließen zu können, setzen wir fest:

Definition 4. f heißt **echter Teiler** von g, wenn $f \mid g$ aber f weder Einheit noch zu g assoziiert ist.

Der zu beweisende Fundamentalsatz beruht dann auf folgender Definition:

Definition 5[1]. p heißt **Primelement,** wenn es nicht Null und keine Einheit ist und keine echten Teiler besitzt.

Ob es solche Primelemente gibt, wird in Def. 5 nicht gesagt und läßt sich auch ohne Hinzunahme weiterer Voraussetzungen über I nicht entscheiden. Fällt z. B. I mit seinem Quotientenkörper zusammen, so gibt es keine Primelemente.

B. Der absolute Betrag in $K[x]$ und Γ.

Um den (keineswegs allgemein in Integritätsbereichen gültigen) Fundamentalsatz von der eindeutigen Zerlegbarkeit in Primelemente in $K[x]$ und Γ beweisen zu können, müssen wir spezielle Eigenschaften dieser Integritätsbereiche heranziehen, nämlich in Γ die Anordnung der ganzen Zahlen nach ihrem absoluten Betrage, deren Gesetze wir hier als bekannt voraussetzen[2], in $K[x]$ die Anordnung der ganzen rationalen Funktionen von x nach ihrem Grade. Die Möglichkeit der weiteren gleichzeitigen Behandlung beider Fälle beruht dann auf der Tatsache, daß man die Anordnung nach dem Grade in $K[x]$ auch durch ein genaueres Analogon zum absoluten Betrag in Γ beschreiben kann, als es der Grad selbst ist. Wir setzen nämlich fest:

Definition 6. Unter dem **absoluten Betrage** $|f|$ eines Elementes f aus $K[x]$ werde verstanden

$$|f| = 0, \text{ wenn } f = 0,$$
$$|f| = k^n, \text{ wenn } f \text{ vom Grade } n.$$

Dabei sei k eine beliebige, aber ein für allemal fest gewählte ganze Zahl > 1.

[1]) Vgl. auch die spätere, zusätzliche Def. 8 [14].

[2]) Wir setzen ausführlicher gesagt als bekannt voraus: 1. die Relation $<$ in Γ und deren Gesetze, 2. die Beziehungen dieser Relation zu den Rechenoperationen, 3. die Definition des absoluten Betrages, 4. die aus 1. und 2. folgenden Beziehungen des absoluten Betrages zur Anordnung und den Rechenoperationen.

k könnte auch als irgendeine reelle Zahl > 1 angenommen werden; wir wollen jedoch hier aus methodischen Gründen die reellen Zahlen vermeiden.

Es gelten dann die folgenden, im Falle Γ gültigen Gesetze für den absoluten Betrag unverändert auch in $\mathsf{K}[x]$:

(1.) $$|f| \geqq 1, \text{ wenn } f \neq 0,$$

(2.) $$|f \pm g| \leqq |f| + |g|,$$

(3.) $$|f \cdot g| = |f| \cdot |g|.$$

Beweis: (1.) ist nach Def. 6 klar, ebenso auch (2.) und (3.) im Falle $f = 0$ oder $g = 0$. Ist aber $f \neq 0$, $g \neq 0$, also

$$f(x) \equiv a_0 + \cdots + a_n x^n \quad (a_n \neq 0), \qquad |f| = k^n,$$
$$g(x) \equiv b_0 + \cdots + b_m x^m \quad (b_m \neq 0), \qquad |g| = k^m,$$

so kommen in $f \pm g$ keine höheren Potenzen von x als $x^{\mathrm{Max}\,(n,m)}$ vor. Daher ist

$$|f \pm g| \leqq k^{\mathrm{Max}\,(n,m)} = \mathrm{Max}\,(k^n, k^m) \leqq k^n + k^m = |f| + |g|.$$

Im Falle $\mathsf{K}[x]$ gilt hiernach sogar die im Falle Γ nicht allgemein richtige Relation

(2a.) $$|f \pm g| \leqq \mathrm{Max}\,(|f|, |g|).$$

Ferner ist

$$\begin{aligned} f(x)\, g(x) &\equiv \sum_{\nu=0}^{n} a_\nu x^\nu \cdot \sum_{\mu=0}^{m} b_\mu x^\mu \equiv \sum_{\nu=0}^{n} \sum_{\mu=0}^{m} a_\nu b_\mu x^{\nu+\mu} \\ &\equiv \sum_{i=0}^{n+m} \Big(\sum_{\nu+\mu=i} a_\nu b_\mu \Big) x^i \qquad \begin{pmatrix} \nu = 0, \ldots, n \\ \mu = 0, \ldots, m \end{pmatrix} \\ &\equiv a_0 b_0 + (a_0 b_1 + a_1 b_0)\, x + \cdots \\ &\quad + (a_{n-1} b_m + a_n b_{m-1})\, x^{n+m-1} + a_n b_m x^{n+m} \\ &\qquad\qquad (a_n b_m \neq 0), \end{aligned}$$

also

$$|f \cdot g| = k^{n+m} = k^n \cdot k^m = |f| \cdot |g|.$$

Neben (1.)—(3.) haben wir im folgenden noch das nachstehende Prinzip wiederholt anzuwenden, dessen Richtigkeit sich aus der Tatsache ergibt, daß alle absoluten Beträge nach Def. 6 natürliche Zahlen oder 0 sind:

(4.) In jeder nicht leeren Teilmenge von $\mathsf{K}[x]$ bzw. Γ gibt es Elemente von kleinstmöglichem Betrage.

Der absolute Betrag in $K[x]$ bzw. Γ steht nun mit den unter A. erklärten Begriffen der Teilbarkeitslehre in diesen Integritätsbereichen in den folgenden Beziehungen:

Satz 6. Ist $f \mid g$, $g \neq 0$, so ist $1 \leqq |f| \leqq |g|$.

Beweis: Ist $g = f\bar{f}$, $g \neq 0$, so ist auch $f \neq 0$, $\bar{f} \neq 0$, also nach (1.) $|f| \geqq 1$, $|\bar{f}| \geqq 1$. Da ferner nach (3.) $|g| = |f| \cdot |\bar{f}|$ ist, folgt $1 \leqq |\bar{f}| = \frac{|g|}{|f|}$, d. h. $|f| \leqq |g|$.

Satz 7. f ist dann und nur dann Einheit, wenn $|f| = 1$ ist. Im Falle $K[x]$ sind also die Elemente $a \neq 0$ aus K, im Falle Γ die ganzen Zahlen $a = \pm 1$ die einzigen Einheiten.

Beweis: a.) Aus $f \mid e$ folgt wegen $|e| = 1$ nach Satz 6 $|f| = 1$.

b.) Daß die f mit $|f| = 1$, d. h. die im Satz genannten a Einheiten sind, ist nach Def. 2 [9] klar (im Falle $K[x]$ wegen der unbeschränkten Division in K).

Aus Satz 6, 7 ergibt sich mittels (3.):

Satz 8. Sind f_1 und f_2 assoziiert, so ist $|f_1| = |f_2|$. Ist $|f_1| = |f_2|$ und $f_1 \mid f_2$, so sind f_1 und f_2 assoziiert.

Die Nebenvoraussetzung $f_1 \mid f_2$ für die Umkehrung ist im Falle Γ entbehrlich, im Falle $K[x]$ aber nicht.

Aus Satz 6—8 ergibt sich:

Satz 9. Ist $f \mid g$, $g \neq 0$, so ist f dann und nur dann echter Teiler von g, wenn $1 < |f| < |g|$ ist.

C. Formulierung des Fundamentalsatzes.

In den speziellen Integritätsbereichen $K[x]$ und Γ können wir aus den Klassen assoziierter Elemente je einen speziellen Repräsentanten durch die folgende Festsetzung hervorheben:

Definition 7. f heißt **normiert,** wenn erstens $f \neq 0$ ist, und wenn zweitens

a.) im Falle $K[x]$ der Koeffizient a_n der höchsten in $f(x) \equiv a_0 + \cdots + a_n x^n$ $(a_n \neq 0)$ vorkommenden Potenz von x (kurz: der **höchste Koeffizient** von $f(x)$) gleich e ist;

b.) im Falle Γ $f > 0$ ist.

Es ist zweckmäßig, die Forderung $f \neq 0$ in normiert aufzunehmen, obwohl 0 ebenfalls ein ausgezeichneter (nämlich einziger) Repräsentant einer Klasse assoziierter Elemente ist. Im Falle $K[x]$ besagt also normiert dasselbe, wie die in der Einleitung eingeführte Bezeichnung Polynom, wenn man von dem einzigen normierten Element 0-ten Grades $f = e$ absieht, das wir der Zweckmäßigkeit halber nicht in den Begriff Polynom aufnahmen. Die von uns befolgte Ausdrucksweise, bei der nur die normierten Elemente aus $K[x]$ Polynome genannt werden, ist übrigens nicht allgemein üblich.

Aus Satz 7 folgt unmittelbar, daß Def. 7 wirklich das Gewünschte leistet:

Satz 10. In jeder von der Nullklasse verschiedenen Klasse assoziierter Elemente existiert ein und nur ein normierter Repräsentant.

Ferner gilt für normierte Elemente:

Satz 11. Mit f und g ist fg und, falls $g \mid f$, auch $\frac{f}{g}$ normiert.

Beweis: Im Falle Γ ist der Satz klar. Im Falle $K[x]$ folgt die Behauptung aus der vorher im Beweis für (3.) [12] verwendeten Multiplikationsformel, angewandt auf fg und auf $\frac{f}{g}g$.

Wir setzen im Anschluß an Def. 7 für später fest:

Definition 8. Ein normiertes Primelement heißt im Falle $K[x]$ **Primfunktion** oder **irreduzibles Polynom,** im Falle Γ **Primzahl.**

In §§ 1, 2 gebrauchen wir der Kombination der Fälle $K[x]$ und Γ halber noch die gemeinsame Bezeichnung normiertes Primelement.

Der zu beweisende **Fundamentalsatz** lautet nun folgendermaßen:

Satz 12. Jedes Element $f \neq 0$ aus $K[x]$ bzw. Γ besitzt eine Zerlegung

$$f = a p_1 \cdots p_r \text{ [1]}$$

in $r \geqq 0$ normierte Primelemente $p_1, \ldots, p_r$ und einen Einheitsfaktor a. Diese Zerlegung ist bis auf die Reihenfolge der Faktoren eindeutig, d. h. a und $p_1, \ldots, p_r$ sind durch f eindeutig bestimmt.

Es wird nicht behauptet, daß $p_1, \ldots, p_r$ verschieden seien. Die Eindeutigkeitsbehauptung bezieht sich aber auch auf die Häufigkeit des Auftretens der verschiedenen Primfaktoren.

Der Beweis zerfällt wie die Behauptung in zwei Teile, deren ersten, einfacheren wir unter D. durchführen, während der zweite, tieferliegende unter F. folgt, nachdem wir unter E. eine Reihe dazu erforderlicher, aber auch über diesen Zweck hinaus sehr wichtiger Sätze hergeleitet haben werden.

D. Möglichkeit der Zerlegung in normierte Primelemente.

Wir beweisen zunächst den Hilfssatz:

(D_1). Ist f keine Einheit, so hat f mindestens einen normierten Primteiler.

Beweis: Da im Falle $f = 0$ jedes normierte Element $\neq e$, im Falle $f \neq 0$ der zu f assoziierte normierte Repräsentant ein von Einheiten verschiedener, normierter Teiler von f ist, gibt es nach (4.) [12] einen von Einheiten verschiedenen normierten Teiler p von f von kleinstmöglichem Betrage. Dieser Teiler p ist normierter Primteiler von f. Denn nach Konstruktion ist er normiert und von Einheiten verschieden. Hätte ferner p einen echten Teiler, so wäre dessen normierter Repräsentant ein von Einheiten verschiedener, normierter Teiler von f (Satz 2 [9]) von kleinerem Betrage als p (Satz 9 [13]), was der Minimalauswahl des Betrages von p widerspricht.

Durch (D_1) ist insbesondere die Existenz von Primelementen nachgewiesen. Für den Spezialfall $f = 0$ ergibt unser Be-

[1]) Wir setzen fest, daß ein Produkt $p_1 \cdots p_r$ für $r = 0$ das Element e bedeuten soll (vgl. auch die Anm. in **1**, § 12 [84] zum Toeplitzschen Satz).

weis im Falle $\mathsf{K}[x]$ jedes Polynom 1-ten Grades $a_0 + x$, im Falle Γ die Zahl 2 als normiertes Primelement.

Aus (D_1) folgern wir nun D., d. h. den Satz:

(D_2). Jedes $f \neq 0$ besitzt eine Zerlegung

$$f = a p_1 \cdots p_r$$

in $r \geqq 0$ normierte Primelemente $p_1, \ldots, p_r$ und einen Einheitsfaktor a.

Beweis: Ist f Einheit, so ist die Behauptung klar ($r = 0$). Ist f keine Einheit, so kann nach (D_1)

$$f = p_1 f_1$$

mit einem normierten Primelement p_1 gesetzt werden. Ist f_1 Einheit, so ist dies eine Zerlegung, wie behauptet ($r = 1$). Ist f_1 keine Einheit, so kann nach (D_1)

$$f_1 = p_2 f_2, \quad \text{also} \quad f = p_1 p_2 f_2$$

mit einem normierten Primelement p_2 gesetzt werden. Nach endlich vielen Schritten muß man bei diesem Vorgehen auf eine Einheit f_r stoßen. Denn da $f \neq 0$ ist, gilt nach Satz 9 [13], solange f_i keine Einheit ist,

$$|f| > |f_1| > \cdots > |f_i| > 1,$$

was mit einer unendlichen Folge solcher f_i wegen der Ganzzahligkeit der Beträge $|f_i|$ unverträglich ist. Ist als erstes f_r Einheit, so gilt

$$f = a p_1 \cdots p_r,$$

wo $p_1, \ldots, p_r$ normierte Primelemente sind und a ($= f_r$) Einheit ist.

Damit ist (D_2), also D., bewiesen.

E. Division mit Rest, größter gemeinsamer Teiler.

Satz 13. Ist $f \neq 0$ und g beliebig, so existieren eindeutig bestimmte $\bar{f}$ und h derart, daß gilt

$$g = f\bar{f} + h \text{ und } \begin{cases} |h| < |f| & \text{im Falle } \mathsf{K}[x], \\ |h| < |f| \text{ und } h \geqq 0, & \text{d. h. } 0 \leqq h < |f| \\ & \text{im Falle } \Gamma. \end{cases}$$

Beweis: a.) Es sei $\bar{f}$ so gewählt, daß $h = g - f\bar{f}$ unter allen $g - ff^*$ einen kleinstmöglichen Betrag hat, was nach (4.) [12] möglich ist. Wäre dann $|h| \geqq |f|$, so folgte

1.) im Falle $\mathsf{K}[x]$, wenn l, n die Grade und c_l, a_n die höchsten Koeffizienten von h, f sind, daß $l \geqq n$, also

$$f_1(x) \equiv \frac{c_l}{a_n}\, x^{l-n}$$

ein Element aus $\mathsf{K}[x]$ wäre. Es hätte dann ff_1 den Grad l und den höchsten Koeffizienten c_l, genau wie h, so daß

$$h - ff_1 = g - ff - ff_1 = g - f(f + f_1)$$

einen niedrigeren Grad, also kleineren Betrag als h hätte.

2.) im Falle Γ, daß

$$h \mp f = g - ff \mp f = g - f(f \pm 1)$$

bei einem der beiden Vorzeichen einen kleineren Betrag als h hätte.

Die Existenz eines solchen $\bar{f}^* = \bar{f} + f_1$ bzw. $= \bar{f} \pm 1$ widerspricht aber in beiden Fällen der Minimalauswahl des Betrages von $h = g - f\bar{f}$. Also ist $|h| < |f|$.

Um im Falle Γ neben der hierdurch als möglich erwiesenen Bedingung $|h| < |f|$ auch noch $h \geqq 0$ zu erreichen, hat man, falls $h < 0$, also $-|f| < h < 0$ ist, nur

$$h_1 = h + |f| = h \pm f = g - f(\bar{f} \mp 1)$$

zu bilden, wofür dann $0 < h_1 < |f|$ gilt.

b.) Aus $g = f\bar{f} + h$, $g = f\bar{f}' + h'$, wo h und h' den Bedingungen des Satzes genügen, folgt

$$f(\bar{f} - \bar{f}') = h' - h, \quad \text{also} \quad f \mid h' - h.$$

Wäre nun $h' \neq h$, so folgte nach Satz 6 $|f| \leqq |h' - h|$. Daraus ergäbe sich gemäß den Bedingungen des Satzes für h, h'

1.) im Falle $\mathsf{K}[x]$ nach (2a.) [12]:

$$|f| \leqq \operatorname{Max}(|h|, |h'|) < |f|,$$

2.) im Falle Γ:

$$|f| \geqq (h' - h \quad \text{oder} \quad h - h') < |f| - 0 = |f|,$$

also in beiden Fällen ein Widerspruch. Somit ist $h = h'$ und dann wegen $f \neq 0$ auch $\bar{f} = \bar{f}'$. Damit ist Satz 13 bewiesen.

Da 0 den Bedingungen des Satzes 13 für h genügt, ergibt sich aus der Möglichkeit und Eindeutigkeit der dortigen Relationen noch:

Zusatz: Ist $f \neq 0$ und g beliebig, so ist dann und nur dann $f \mid g$, wenn das h aus Satz 13 gleich 0 ist.

Die Bestimmung von $\bar{f}$ und h zu $f \neq 0$ und g gemäß Satz 13 nennt man Division von g durch f mit Rest, $\bar{f}$ den Quotienten, h den Rest. Das auf die dezimale (oder irgendeine andere Ziffern-) Schreibweise der ganzen Zahlen gegründete Verfahren zur praktischen Ausführung der Division mit Rest im Falle Γ darf als bekannt vorausgesetzt werden, ebenso auch das in entsprechender Weise auf die Normaldarstellung (**1**, Def. 9 [38]) gegründete Verfahren hierzu im Falle $\mathsf{K}[x]$, das sich durch direkte Wendung des indirekten Beweises unter a.), 1.) ergibt. Insbesondere ermöglichen diese Verfahren nach dem Zusatz die praktische Entscheidung, ob eine Teilbarkeitsrelation $f \mid g$ besteht.

Aus Satz 13 folgern wir durch nochmalige Anwendung einer ähnlichen Schlußweise:

Satz 14. Sind f_1 und f_2 nicht beide 0, so existiert ein eindeutig bestimmtes, normiertes d derart, daß gilt

(1.) $$d \mid f_1, \quad d \mid f_2,$$

(2.) $$\text{aus } h \mid f_1,\ h \mid f_2 \text{ folgt } h \mid d.$$

d läßt sich in der Form

$$d = f_1\bar{f}_1 + f_2\bar{f}_2$$

darstellen. Im Hinblick auf die Eigenschaften (1.), (2.) heißt d der **größte gemeinsame Teiler** von f_1 und f_2 (Bezeichnung $d = (f_1, f_2)$).

Beweis: a.) Es seien $\bar{f}_1, \bar{f}_2$ so gewählt, daß $d = f_1\bar{f}_1 + f_2\bar{f}_2$ normiert ist und unter allen normierten Elementen der Form $f_1\bar{f}_1^* + f_2\bar{f}_2^*$ einen kleinstmöglichen Betrag hat. Das ist nach (4.) [12] möglich; denn ist etwa $f_1 \neq 0$, so ist der normierte Repräsentant $a_1 f_1$ zu f_1 ein normiertes Element der angegebenen Form ($\bar{f}_1^* = a_1, \bar{f}_2^* = 0$); die betr. Menge von Beträgen ist also nicht leer. Daß (2.) für das so bestimmte d erfüllt ist, ist klar (Satz 3) [9]. Wäre ferner (1.) nicht erfüllt und etwa $d \nmid f_1$, so existierte, weil d als normiertes Element $\neq 0$ ist, ein $h = f_1 - d\bar{d}$ mit $|h| < |d|$ (Satz 13), für das $h \neq 0$ gälte (Zusatz). Wird dann h durch den Faktor a normiert, so wäre

$$ah = af_1 - ad\bar{d} = f_1(a - a\bar{d}\bar{f}_1) + f_2(-a\bar{d}\bar{f}_2)$$

ein normiertes Element der Form $f_1\bar{f}_1^* + f_2\bar{f}_2^*$ von kleinerem Betrage als d, was der Minimalauswahl des Betrages von $d = f_1\bar{f}_1 + f_2\bar{f}_2$ widerspricht. Also ist $d \mid f_1$ und ebenso $d \mid f_2$.

b.) Genügt auch das normierte d' den Bedingungen (1.) und (2.), so folgt aus (1.) für d' und (2.) für d (mit d' als h), daß $d' \mid d$. Ebenso folgt umgekehrt $d \mid d'$. Daraus ergibt sich $d = d'$ (Satz 5, 10 [10, 14]).

Das oben angeführte Verfahren zur Division mit Rest liefert durch wiederholte Anwendung das folgende Verfahren zur praktischen Bestimmung des größten gemeinsamen Teilers, das unter dem Namen Euklidischer Algorithmus bekannt ist:

Es sei etwa $f_2 \neq 0$. Dann werden die folgenden Divisionen mit Rest ausgeführt, bis man auf einen Rest $f_{r+1} = 0$ stößt:

$$\begin{array}{ll} f_1 = f_2 g_1 + f_3, & |f_3| < |f_2| \\ f_2 = f_3 g_2 + f_4, & |f_4| < |f_3| \\ \cdots\cdots\cdots & \cdots\cdots\cdots \\ f_{r-2} = f_{r-1} g_{r-2} + f_r, & |f_r| < |f_{r-1}| \\ f_{r-1} = f_r g_{r-1} + f_{r+1}, & 0 = |f_{r+1}| < |f_r|. \end{array}$$

Wegen des dauernden Abnehmens der Beträge $|f_i|$ tritt $f_{r+1} = 0$ nach endlich vielen Schritten wirklich ein. Dann ist der normierte Repräsentant zu f_r der größte gemeinsame Teiler von f_1, f_2. Denn durch Zurückgehen von der letzten Relation aus folgt nach Satz 3 [9] sukzessive $f_r \mid f_{r-1}, f_r \mid f_{r-2}, \ldots, f_r \mid f_2, f_r \mid f_1$, also (1.), und durch Zurückgehen von der vorletzten Relation aus, daß f_r durch die Paare $f_{r-2}, f_{r-1}; \ldots; f_1, f_2$ in der Form des Satzes darstellbar ist, also (2.).

Wir vermerken noch die speziellen Relationen

$$\begin{array}{ll} (0, f) = f, \quad (f, f) = f & \text{für normiertes } f, \\ (a, f) = e & \text{für jedes } f. \end{array}$$

Aus dem grundlegenden Satz 14 ergeben sich nunmehr durch elementare Schlüsse die folgenden Tatsachen, die schrittweise zu dem erstrebten Eindeutigkeitsnachweis führen:

Satz 15. Ist g normiert, so ist $(f_1, f_2)g = (f_1 g, f_2 g)$.

Beweis: Ist $(f_1, f_2) = d$, $(f_1 g, f_2 g) = d'$, so ist einerseits $dg \mid f_1 g$, $dg \mid f_2 g$ (Satz 14, (1.) für d; Satz 2 [9]), also $dg \mid d'$ (Satz 14, (2.) für d'); andererseits $\frac{d'}{g} \mid f_1$, $\frac{d'}{g} \mid f_2$ (Satz 14, (1.) für d'; Satz 2), also $\frac{d'}{g} \mid d$ (Satz 14, (2.) für d), d. h. $d' \mid dg$ (Satz 2). Daraus folgt $d' = dg$ (Satz 5, 10 [10, 14]).

Definition 9. f_1 und f_2 heißen **relativ prim** oder **teilerfremd**, wenn $(f_1, f_2) = e$ ist.

Hiernach ist speziell 0 zu allen und nur den Einheiten, eine Einheit zu allen f relativ prim. Ist ferner $(f_1, f_2) = d$ und wird $f_1 = dg_1$, $f_2 = dg_2$ gesetzt, so sind g_1 und g_2 relativ prim (Satz 15).

Satz 16. Sind f und g_1 relativ prim und ist $f \mid g_1 g_2$, so ist $f \mid g_2$.

Beweis: Ist $g_2 = 0$, so ist die Behauptung klar. Ist $g_2 \neq 0$ und $\bar{g}_2$ der normierte Repräsentant zu g_2, so folgt nach Satz 15 aus $(f, g_1) = e$, daß $(f\bar{g}_2, g_1\bar{g}_2) = \bar{g}_2$, also nach Satz 14, (2.) und der Voraussetzung, daß $f \mid \bar{g}_2$, d. h. auch $f \mid g_2$ ist.

Satz 17. Ist p Primelement, so ist $(p, g) = e$ mit $p \nmid g$ gleichbedeutend, d. h. p ist dann und nur dann prim zu g, wenn p kein Teiler von g ist.

Beweis: Ist $\bar{p}$ der normierte Repräsentant zu p, so kann (p, g) als normierter Teiler von p nur e oder $\bar{p}$ sein (Def. 4, 5 [11]). Ist nun einerseits $p \nmid g$, so kann nicht $(p, g) = \bar{p}$ sein, weil sonst nach Satz 14, (1.) $\bar{p} \mid g$, also $p \mid g$ folgte; daher ist dann $(p, g) = e$. Ist andererseits $(p, g) = e$, so kann nicht $p \mid g$ sein, weil sonst nach Satz 14, (2.) $p \mid e$ folgte, entgegen Def. 5; daher ist dann $p \nmid g$.

Satz 18. Ist p Primelement und $p \mid g_1 g_2$, so ist $p \mid g_1$ oder $p \mid g_2$.

Beweis: Ist $p \nmid g_1$, so ist p prim zu g_1 (Satz 17), also wegen der Voraussetzung $p \mid g_2$ (Satz 16).

Satz 19. Ist p Primelement und $p \mid g_1 \cdots g_r$, so ist $p \mid g_1$ oder ... oder $p \mid g_r$.

Beweis: Folgt durch wiederholte Anwendung von Satz 18.

Auf dem letzten Satz beruht der nun zu erbringende Eindeutigkeitsnachweis.

F. Eindeutigkeit der Zerlegung in normierte Primelemente.

Es seien

$$f = a p_1 \cdots p_r = b q_1 \cdots q_s$$

zwei Zerlegungen eines $f \neq 0$ in $r \geqq 0$ bzw. $s \geqq 0$ normierte Primelemente $p_1, \ldots, p_r$ bzw. $q_1, \ldots, q_s$ und einen Einheitsfaktor a bzw. b. Durch Division mit b folgt dann zunächst nach Satz 11 [14], daß $\frac{a}{b}$ normiert, also $= e$, d. h. $a = b$ ist. Es ist daher

$$p_1 \cdots p_r = q_1 \cdots q_s .$$

Ist $r = 0$, so ist auch $s = 0$; denn sonst wäre $q_1 \mid e$ entgegen Def. 5 [11]. Dann stimmen also beide Zerlegungen $f = a$, $f = b$ überein.

Ist $r > 0$, so ist nach demselben Schluß auch $s > 0$. Dann folgt $p_1 \mid q_1 \cdots q_s$, also nach Satz 19 $p_1 \mid q_1$ oder $\cdots$ oder $p_1 \mid q_s$. Da die q_i keine echten Teiler haben, ist somit das von Einheiten verschiedene p_1 zu einem der q_i assoziiert, also gleich (Satz 10 [14]). Die Reihenfolge werde so angenommen, daß $p_1 = q_1$ ist. Es folgt dann

$$p_2 \cdots p_r = q_2 \cdots q_s .$$

Ist $r = 1$, so ist wie oben auch $s = 1$. Dann stimmen also beide Zerlegungen $f = a p_1$, $f = b q_1$ überein.

Ist $r > 1$, so ist auch $s > 1$, und die Fortsetzung der obigen Schlußweise liefert bei passender Wahl der Reihenfolge der q_i sukzessive

$$p_2 = q_2, \ldots, p_r = q_s \text{ und } r = s,$$

letzteres, da nach dem obigen Schluß die p_i bei demselben Schritte erschöpft sein müssen, wie die q_i. Beide Zerlegungen stimmen also bis auf die Reihenfolge der Faktoren überein.

Durch D. und F. ist nunmehr der Fundamentalsatz bewiesen.

G. Folgerungen aus dem Fundamentalsatz.

Durch Heranziehung der Zerlegung in Primelemente erhalten die unter A. und F. eingeführten Begriffe der Teilbarkeitslehre ein neues Gesicht. Es gelten nämlich die folgenden Tatsachen [1]):

Satz 20. Ist $g \neq 0$, so ist dann und nur dann $f \mid g$, wenn die normierten Primfaktoren von f unter denen von g vorkommen [2]). (Def. 1 [9], Satz 12 [14].)

Die daraus sich unmittelbar ergebenden Folgerungen für die Begriffe Einheit und assoziiert brauchen nicht erst besonders aufgeführt zu werden.

Satz 21. Sind f_1 und f_2 von 0 verschieden, so ist ihr größter gemeinsamer Teiler das Produkt der gemeinsamen normierten Primfaktoren von f_1 und f_2. (Satz 12, 14, 20.)

Satz 22. Von 0 verschiedene f_1 und f_2 sind dann und nur dann relativ prim, wenn sie keinen gemeinsamen Primfaktor besitzen. (Def. 9 [20], Satz 21.)

Aus Satz 22 ergibt sich ferner ohne weiteres die folgende Verallgemeinerung von Satz 18 [20] in der Richtung von Satz 16 [20]:

Satz 23. Ist f prim zu g_1 und g_2, so auch zu $g_1 g_2$.

---

1) Siehe die Anm. vor Satz 1 [9]. Die heranzuziehenden früheren Definitionen und Sätze sind in Klammern angemerkt.

2) Diese und die folgenden Aussagen sind mit Berücksichtigung der Häufigkeit des Auftretens der verschiedenen Primfaktoren gemeint (vgl. d. Bem. bei Satz 12 [15]).

H. Abhängigkeit vom Grundkörper.

Es ist für uns wichtig festzustellen, wie die im Vorhergehenden entwickelten Begriffe und Tatsachen für den Fall $\mathsf{K}[x]$ beeinflußt werden, wenn an Stelle von $\mathsf{K}[x]$ der Integritätsbereich $\overline{\mathsf{K}}[x]$ über einem Erweiterungskörper $\overline{\mathsf{K}}$ von K zugrunde gelegt wird. In dieser Hinsicht gilt folgendes:

Satz 24. Werden die vorkommenden Elemente aus $\mathsf{K}[x]$ als solche des Integritätsbereiches $\overline{\mathsf{K}}[x]$ über einem Erweiterungskörper $\overline{\mathsf{K}}$ von K angesehen, so bleiben die Relationen „$f \mid g, f \nmid g$, h ist der Rest bei der Division von g durch f, $(f_1, f_2) = d$" erhalten, dagegen nicht notwendig die Relation „p ist Primfunktion".

Beweis: a.) Die Bestimmung von h aus f und g und die Bestimmung von d aus f_1 und f_2 kann nach den Ausführungen hinter Satz 13 [18] und Satz 14 [19] durch Rechenverfahren ausgeführt werden, die in der Anwendung der vier elementaren Rechenoperationen auf die zu K gehörigen Koeffizienten der vorkommenden Elemente bestehen. Durch Auffassung dieser Koeffizienten als Elemente aus $\overline{\mathsf{K}}$ ändern sich jene Verfahren, also auch deren Ergebnisse h und d nicht. Auch die Alternative $h = 0, h \neq 0$ bleibt unbeeinflußt, was nach Satz 13, Zusatz [18] die Invarianz der Alternative $f \mid g, f \nmid g$ im Falle $f \neq 0$ ergibt. Für $f = 0$ ist deren Invarianz nach Satz 1 [9] trivial.

b.) Schon das in der Einleitung genannte Beispiel zeigt, daß die Primfunktion $x^2 - 2$ aus $\mathsf{P}[x]$[1]) bei Erweiterung von P zum Körper $\overline{\mathsf{P}}$ der reellen Zahlen die Zerlegung $(x - \sqrt{2})(x + \sqrt{2})$ in echte Teiler bekommt.

Wegen b.) kann analog wie in der Einleitung bei 1.) prinzipiell kein rationales Rechenverfahren zur Entscheidung darüber existie-

[1]) Daß $x^2 - 2$ in $\mathsf{P}[x]$ Primfunktion ist, kommt auf die Irrationalität von $\sqrt{2}$ hinaus, und diese kann leicht aus Satz 12 [14] für den Fall Γ gefolgert werden.

ren, ob ein vorgelegtes Element aus $K[x]$ Primfunktion ist, und ebensowenig ein solches zur Herstellung der Primfaktorzerlegung eines vorgelegten f aus $K[x]$. Hierzu ist man vielmehr in jedem konkreten Falle auf Probierverfahren angewiesen.

Wenn wir, wie im folgenden häufig, neben dem Grundkörper K Erweiterungskörper $\overline{K}$ von K zu betrachten haben, müssen wir bei Verwendung der Bezeichnungen Primfunktion, irreduzibel (Def. 8 [14]) angeben, ob sie in bezug auf $K[x]$ oder $\overline{K}[x]$ gemeint sind. Wir tun dies durch die Zusätze in K bzw. in $\overline{K}$ (vgl. die erste Anm. i. d. Einl. [5]).

Aus dem Fundamentalsatz (angewandt in $\overline{K}[x]$) ergibt sich noch ohne weiteres die im folgenden vielfach benutzte Tatsache:

Satz 25. Ist $\overline{K}$ ein Erweiterungskörper von K, so entsteht die Primfaktorzerlegung eines f aus $K[x]$ in $\overline{K}[x]$ aus der in $K[x]$, wenn man die Primfaktoren von f in $K[x]$ in ihre Primfaktoren in $\overline{K}[x]$ zerlegt.

§ 2. Restklassenringe in $K[x]$ und Γ.

In **1**, § 2 haben wir den allgemeinen Begriff der Kongruenzrelation in einem Bereich eingeführt. Die Resultate des § 1 setzen uns in Stand, alle in den Integritätsbereichen $K[x]$ und Γ möglichen Kongruenzrelationen in ganz entsprechendem Sinne zu übersehen, wie es durch **1**, Satz 34, 35 [65, 66] für die Kongruenzrelationen in Gruppen geschah. Wir erhalten diese Übersicht aus dem folgenden Satz:

Satz 26. Zu einer Kongruenzrelation $\equiv$ in $K[x]$ bzw. Γ existiert ein bis auf assoziierte eindeutig bestimmtes Element f derart, daß

(1.) $h_1 \equiv h_2$ dann und nur dann, wenn $f \mid h_1 - h_2$.

Umgekehrt entsteht so für jedes f eine Kongruenzrelation in $K[x]$ bzw. Γ.

Beweis: a.) Jede Kongruenzrelation $\equiv$ entspringt gemäß (1.) aus einem f. Es sei nämlich M die Menge aller Elemente $g \equiv 0$. Nach **1**, § 2, (α.), (β.), (γ.), (1.), (2.) [15, 21] ist dann $h_1 \equiv h_2$ mit $h_1 - h_2 \equiv 0$, d. h. mit dem Enthaltensein von $h_1 - h_2$ in M gleichbedeutend. Entweder besteht nun M nur aus dem Elemente 0. Dann ist $h_1 \equiv h_2$ mit $h_1 = h_2$ gleichbedeutend, unsere Kongruenzrelation also die Gleichheit und die Behauptung des Satzes mit $f = 0$ richtig (Satz 1 [9]). Oder aber M enthält von 0 verschiedene Elemente. Dann gibt es nach § 1, (4.) [12] unter den von Null verschiedenen Elementen von M ein f von kleinstmöglichem Betrage. Ist dann g irgendein Element aus M und wird nach Satz 13 [16]

$$g = f\bar{f} + h, \; |h| < |f|$$

gesetzt, so gehört auch $h = g - f\bar{f}$ zu M, weil nach der Definition der Kongruenzrelation in **1**, § 2 aus $f \equiv 0$ auch $f\bar{f} \equiv 0$ und dann aus $g \equiv 0$ auch $h = g - f\bar{f} \equiv 0$ folgt. Es muß also wegen der Minimalbestimmung des Betrages von f gelten $h = 0$, d. h. $f \mid g$. Da nun umgekehrt aus $f \equiv 0$ auch für jedes Vielfache $g = f\bar{f}$ von f folgt $g \equiv 0$, besteht somit M aus allen und nur den Vielfachen von f, ist also $g \equiv 0$ mit $f \mid g$ und daher nach dem schon Gesagten $h_1 \equiv h_2$ mit $f \mid h_1 - h_2$ gleichbedeutend.

b.) Die Relation (1.) ist für jedes feste f eine Kongruenzrelation. Denn die Bedingungen **1**, § 2, (α.), (β.), (γ.) [15] sind erfüllt, weil erstens $f \mid 0$ (Satz 1 [9]), zweitens aus $f \mid h_1 - h_2$ folgt $f \mid h_2 - h_1$ (Satz 3 [9]) und drittens aus $f \mid h_1 - h_2, f \mid h_2 - h_3$ folgt $f \mid h_1 - h_3$ (Satz 3); und die Bedingungen **1**, § 2, (1.), (2.) [21] sind erfüllt, weil aus $f \mid h_1 - h_2, f \mid g_1 - g_2$ erstens folgt $f \mid (h_1 + g_1) - (h_2 + g_2)$ (Satz 3) und zweitens zunächst folgt $f \mid h_1 g_1 - h_2 g_1, f \mid h_2 g_1 - h_2 g_2$ (Satz 3) und daraus wie eben $f \mid h_1 g_1 - h_2 g_2$.

c.) f ist bis auf assoziierte (unter denen man es natürlich beliebig wählen kann, ohne die Kongruenzrelation (1.) zu ändern) eindeutig durch die Kongruenzrelation bestimmt. Es sei nämlich die Kongruenzrelation $h_1 \equiv h_2$ sowohl mit $f \mid h_1 - h_2$ als auch mit $\bar{f} \mid h_1 - h_2$ gleichbedeutend. Aus $f \mid f - 0, \bar{f} \mid \bar{f} - 0$ folgt dann $f \equiv 0, \bar{f} \equiv 0$, also wegen der gemachten Annahme auch $f \mid \bar{f} - 0, \bar{f} \mid f - 0$, wonach f und $\bar{f}$ assoziiert sind (Satz 5 [10]).

Auf Grund von Satz 26 definieren wir:

Definition 10. Das zu einer Kongruenzrelation $\equiv$ in $\mathsf{K}[x]$ bzw. Γ gemäß Satz 26 gehörige, bis auf assoziierte eindeutig bestimmte Element f heißt ihr **Modul.** Man schreibt dann ausführlicher

$h_1 \equiv h_2$ mod. f[1]) für $h_1 \equiv h_2$, d. h. für $f \mid h_1 - h_2$,

und nennt die zugehörigen Klassen die **Restklassen mod. f,** den durch sie gebildeten Ring[2]) den **Restklassenring mod. f.**

Falls $f \neq 0$, werde der Eindeutigkeit halber f als normiert angenommen. — Wir bezeichnen den Restklassenring mod. f im Falle $\mathsf{K}[x]$ mit $\mathsf{K}[x, \text{mod.} f(x)]$, im Falle Γ mit Γ_f, ferner schreiben wir gelegentlich $\{h\}$ für die durch das Element h bestimmte Restklasse nach dem jeweils betrachteten Modul.

Wenn auch das zum Restklassenring führende Rechnen mit den Restklassen (**1**, Satz 8 [22]) sich nicht auf irgendwelche speziellen Repräsentanten zu stützen braucht, so ist es doch für unsere späteren Anwendungen und auch zur Gewinnung eines Überblicks über die Restklassen wichtig, ein möglichst einfaches vollständiges Repräsentantensystem (**1**, § 2 [17]) für die Restklassen mod. f zu besitzen. Ein solches wird in folgendem Satz genannt:

Satz 27. Ist $f = 0$, so bildet jedes Element von

---

1) Im Falle $\mathsf{K}[x]$ wird übrigens durch diese Hinzufügung von „mod. $f(x)$" eine Verwechselung mit der Gleichheit in $\mathsf{K}[x]$ bei der Schreibweise mit Argument x (**1**, nach Satz 12 [42]) ausgeschlossen.

2) Wir reden hier, etwas allgemeiner als in **1**, Satz 8 [22], auch in dem dort ausgeschlossenen Falle, daß alle Elemente einander kongruent, also f wegen $e \equiv 0$ mod. f Einheit ist, von einem Ring. Dieser enthält dann nur ein einziges Element, erfüllt also nicht mehr die in **1**, § 1, (a.) [7] gestellte Forderung.

$\mathsf{K}[x]$ bzw. Γ für sich eine Restklasse. Ist $f \neq 0$, so wird ein vollständiges Repräsentantensystem der Restklassen mod. f gebildet durch die Elemente h mit der Eigenschaft

$$|h| < |f| \text{ im Falle } \mathsf{K}[x],$$
$$0 \leqq h < f \text{ im Falle } \Gamma.$$

Beweis: a.) Für $f = 0$ ist $h_1 \equiv h_2$ mod. 0 mit $0 \mid h_1 - h_2$, d. h. mit $h_1 = h_2$ gleichbedeutend.

b.) Für $f \neq 0$ ist wegen der Existenztatsache von Satz 13 [16] jedes Element einem der genannten mod. f kongruent, und wegen der Eindeutigkeitstatsache auch nur einem. Die genannten Elemente repräsentieren also alle Restklassen mod. f, jede einmal.

Ausführlich geschrieben lautet das vollständige Repräsentantensystem mod. f für $f \neq 0$

im Falle $\mathsf{K}[x]$: $c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}$, wenn f vom Grade $n > 0$, wobei $c_0, c_1, \ldots, c_{n-1}$ alle Systeme von n Elementen aus K durchläuft; 0, wenn f vom Grade 0 ($f = e$);

im Falle Γ: $0, 1, \ldots, f-1$; hier ist also die Anzahl der Restklassen mod. f endlich, nämlich f.

Aus dem Sachverhalt von Satz 27 motiviert sich die Bezeichnung Restklassen, insofern diese je durch alle Elemente gebildet werden, die bei der Division durch f ein und denselben Rest ergeben[1]).

Besonders wichtig ist für uns die Feststellung, für welche f der Restklassenring mod. f ein Integritätsbereich oder sogar ein Körper ist. Darüber gibt der folgende Satz Auskunft:

Satz 28. Der Restklassenring mod. f ist dann und nur dann Integritätsbereich, wenn $f = 0$ oder f Primelement ist. Ist f Primelement, so ist er sogar Körper.

---

[1]) Auch über die speziellen Integritätsbereiche $\mathsf{K}[x]$ und Γ hinaus lassen sich die Restklassen nach Kongruenzrelationen in allgemeinen Integritätsbereichen in eine ähnliche Beziehung zur Division setzen (vgl. **I**, Anm. zu Def. 6 [21]), wodurch die allgemeine Bezeichnung Restklassen gerechtfertigt wird.

Beweis: a.) Ist $f = 0$, so fällt nach Satz 27 der Restklassenring mit dem Integritätsbereich $K[x]$ bzw. Γ zusammen. Es sei ferner $f = p$ Primelement. Ist dann $g_1 g_2 \equiv 0$ mod. p, d. h. $p \mid g_1 g_2$, so ist nach Satz 18 [20] $p \mid g_1$ oder $p \mid g_2$, d. h. $g_1 \equiv 0$ mod. p oder $g_2 \equiv 0$ mod. p. Wenn also das Produkt zweier Restklassen $\{g_1\}\{g_2\} = 0$ ist, ist mindestens einer der Faktoren $\{g_1\}$ oder $\{g_2\} = 0$, d. h. es gilt das Analogon zu **1**, Satz 4 [12] im Restklassenring mod. p. Daß auch das Analogon zu **1**, Satz 3 [11] gilt, ist klar, weil $\{e\}$ das Einselement des Restklassenrings ist. Also ist dieser zunächst Integritätsbereich. Er ist aber sogar Körper. Denn ist $g \not\equiv 0$ mod. p, d. h. $p \nmid g$, also p prim zu g (Satz 17 [20]), so kann nach Satz 14 [18] $p\bar{h}^* + g\bar{g}^* = e$, also bei vorgegebenem h auch $p\bar{h} + g\bar{g} = h$ gesetzt werden. Die letztere Relation besagt aber, daß $g\bar{g} \equiv h$ mod. p ist, d. h. daß $\{g\}\{\bar{g}\} = \{h\}$ oder $\{\bar{g}\} = \frac{\{h\}}{\{g\}}$ ist. Hiernach ist also die Division durch von Null verschiedene Restklassen mod. p unbeschränkt ausführbar [**1**, § 1, (7.) [10]], so daß ein Körper vorliegt.

b.) Ist $f \neq 0$ und kein Primelement, so ist entweder f Einheit und es gibt dann nur eine einzige Restklasse, so daß also kein Integritätsbereich vorliegt [**1**, § 1, (a.) [7]]. Oder aber es besteht eine Zerlegung $f = g_1 g_2$ in echte Teiler g_1, g_2. Die Relation $g_1 g_2 \equiv 0$ mod. f, d. h. $\{g_1\}\{g_2\} = 0$ besagt dann, daß das Produkt zweier von 0 verschiedener Restklassen mod. f gleich 0 ist, so daß wiederum kein Integritätsbereich vorliegt.

Wir bezeichnen im folgenden den Restklassenkörper nach einer Primfunktion $p(x)$ mit $K(x, \text{mod. } p(x))$, den Restklassenkörper nach einer Primzahl p mit P_p[1]).

Der Restklassenkörper P_p ist nach Satz 27 ein endlicher Körper[2]) von p Elementen. Wir beweisen über ihn noch den fol-

---

[1]) Diese nach den Festsetzungen nach Def. 10 [26] an sich entbehrlichen, neuen Bezeichnungen sind des besseren Einklangs halber mit der in **1**, Def. 9 [38], 10 [39], Satz 5 [13] eingeschlagenen Bezeichnungsweise gewählt.

[2]) Für $p = 2$ ist P_2 der in **1**, § 1, Beisp. 4 [14] genannte und in **1** verschiedentlich als Beispiel herangezogene Körper.

genden, später anzuwendenden Satz:

Satz 29. Für jedes a aus P_p gilt $a^p = a$, für jedes $a \neq 0$ also $a^{p-1} = e$.

Beweis: Für $a = 0$ ist das klar. Sei $a \neq 0$ und seien $0, a_1, \ldots, a_{p-1}$ die p verschiedenen Elemente aus P_p. Wegen der Eindeutigkeit der Division durch a in P_p sind dann die p Elemente $a0 = 0, aa_1, \ldots, aa_{p-1}$ voneinander verschieden, also wieder die sämtlichen Elemente von P_p in irgendeiner Reihenfolge, und daher $aa_1, \ldots, aa_{p-1}$ mit $a_1, \ldots, a_{p-1}$ bis auf die Reihenfolge identisch. Daraus folgt durch Produktbildung

$$a^{p-1} a_1 \cdots a_{p-1} = a_1 \cdots a_{p-1}.$$

Da aber $a_1 \cdots a_{p-1} \neq 0$ ist, ergibt sich $a^{p-1} = e$, $ap = a$, wie behauptet.

Während im vollen Restklassenring mod. f nach Satz 28 die Division dann und nur dann unbeschränkt und eindeutig ist, wenn f ein Primelement ist, läßt sich in jedem Falle eine Teilmenge dieses Restklassenrings angeben, innerhalb deren dies der Fall ist. Zu dieser Teilmenge führt der folgende Satz und die anschließende Definition:

Satz 30. Alle Elemente einer Restklasse mod. f haben mit f ein- und denselben größten gemeinsamen Teiler, der somit Teiler dieser Restklasse genannt werden kann.

Beweis: Ist $g_1 \equiv g_2$ mod. f, d. h. $g_1 - g_2 = f\bar{f}$, so ist nach Satz 3 [9], 14 [18] $(g_1, f) \mid (g_2, f)$ und $(g_2, f) \mid (g_1, f)$, also $(g_1, f) = (g_2, f)$.

Definition 11. Die Restklassen mod. f vom Teiler e heißen die **primen Restklassen mod f.**

Diese stellen also die Restklasseneinteilung mod. f innerhalb der Menge aller zu f primen Elemente (Def. 9 [20]) dar.

Die obige Behauptung wird nun durch folgenden Satz bestätigt:

Satz 31. Die primen Restklassen mod. f bilden eine abelsche Gruppe $\mathfrak{P}_f$ bezüglich der Multiplikation[1]).

[1]) Für $f = 0$ vgl. übrigens Satz 4 [10].

Beweis: Da $\mathfrak{P}_f$ Teilmenge des Restklassenrings mod. f ist, genügt es zu zeigen, daß die Multiplikation nicht aus $\mathfrak{P}_f$ herausführt und daß die Division in $\mathfrak{P}_f$ eindeutig und ebenfalls unbeschränkt ist. Das erstere folgt unmittelbar aus Satz 23 [22], das letztere durch ganz entsprechende Schlüsse, wie im Beweis zu Satz 28 unter a.), jetzt mittels Satz 16 [20] anstelle von Satz 18 [20].

Satz 31 ist vor allem im Falle Γ von Bedeutung. Die Gruppe $\mathfrak{P}_f$ ist dann endlich, ihre Ordnung bezeichnet man mit $\varphi(f)$ (Eulersche Funktion). Es ist $\varphi(0) = 2$ [1], ferner nach Satz 17 [20], 27 [26] $\varphi(p) = p - 1$ für Primzahlen p. Die mittels der Sätze von § 1, E. unschwer zu beweisende allgemeine Formel

$$\varphi(f) = f \prod_{p \mid f} \left(1 - \frac{1}{p}\right), \quad (f > 0),$$

wo p die verschiedenen, in f aufgehenden Primzahlen durchläuft, brauchen wir im folgenden nicht, ebenso auch nicht die Satz 29 verallgemeinernde, ganz entsprechend zu beweisende Relation

$$a^{\varphi(f)} \equiv 1 \text{ mod. } f$$

für jedes zu f prime a aus Γ, den sog. kleinen Fermatschen Satz [2]. Wir führen diese Tatsachen hier nur an, um unsere auf den Fall Γ bezüglichen Entwicklungen, die ein wichtiges Kapitel der elementaren Zahlentheorie bilden, abzurunden.

§ 3. Zyklische Gruppen.

Wir machen in diesem Paragraphen eine für später wichtige Anwendung der auf den Fall Γ bezüglichen Resultate der §§ 1, 2 auf die Gruppentheorie.

Definition 12. Eine Gruppe $\mathfrak{Z}$ heißt **zyklisch**, wenn sie aus den ganzen Potenzen eines ihrer Elemente A besteht. $\mathfrak{Z}$ heißt dann auch **durch A erzeugt** und A ein **primitives Element** von $\mathfrak{Z}$.

Für die ganzen Potenzen von A gelten nach ihrer Erklärung (**1** [51]) die Rechenregeln

$$(1.) \qquad A^m A^n = A^{m+n}, \quad (A^m)^n = A^{mn}.$$

[1]) Vgl. Anm. 1 [29] sowie Satz 7 [13].

[2]) Von Fermat selbst nur für $f = p$ angegeben (Satz 29), in dieser allgemeinen Form erst von Euler.

Daraus folgt zunächst (**1**, Def. 13 [50]):

Satz 32. Jede zyklische Gruppe ist abelsch.

Aus (1.) folgern wir nun weiter den folgenden, grundlegenden Satz über zyklische Gruppen:

Satz 33. Es sei $\mathfrak{Z}$ eine durch A erzeugte zyklische Gruppe. Dann existiert eine eindeutig bestimmte ganze Zahl $f \geqq 0$ derart, daß $\mathfrak{Z}$ vermöge der Zuordnung

(2.) $$A^m \longleftrightarrow \{m\}$$

zur additiven Gruppe $\mathfrak{R}_f$ der Restklassen mod. f[1]) isomorph ist.

Beweis: a.) Durch die Festsetzung

(3.) $m_1 \equiv m_2$ dann und nur dann, wenn $A^{m_1} = A^{m_2}$,

wird eine Kongruenzrelation in Γ definiert.

Denn **1**, § 2, (α.), (β.), (γ.) [15] sind erfüllt, weil die Gleichheit in $\mathfrak{Z}$ ihnen genügt. Weiter gelten auch **1**, § 2, (1.), (2.) [21]; ist nämlich $m_1 \equiv m_2$, $n_1 \equiv n_2$, also $A^{m_1} = A^{m_2}$, $A^{n_1} = A^{n_2}$, so folgt nach (1.)

$$A^{m_1+n_1} = A^{m_1} A^{n_1} = A^{m_2} A^{n_2} = A^{m_2+n_2}$$

$$A^{m_1 n_1} = (A^{m_1})^{n_1} = (A^{m_2})^{n_1} = (A^{n_1})^{m_2} = (A^{n_2})^{m_2} = A^{m_2 n_2},$$

also $m_1 + n_1 \equiv m_2 + n_2$, $m_1 n_1 \equiv m_2 n_2$.

Ist f der Modul der Kongruenzrelation (3.), so gilt also

(4.) $A^{m_1} = A^{m_2}$ dann und nur dann, wenn $m_1 \equiv m_2$ mod. f.

Die Zuordnung (2.) zwischen $\mathfrak{Z}$ und $\mathfrak{R}_f$ ist nach (4.) eineindeutig. Sie ist ferner auch isomorph, weil nach (1.) der Multiplikation der Potenzen A^m die Addition der Exponenten m, also auch ihrer Restklassen $\{m\}$ entspricht. Somit ist $\mathfrak{Z} \cong \mathfrak{R}_f$ vermöge (2.).

b.) Für verschiedene $f \geqq 0$ unterscheiden sich die zugehörigen $\mathfrak{R}_f$ durch die Anzahl ihrer Elemente (Satz 27 [26]), sind also nicht isomorph. Somit ist f durch $\mathfrak{Z}$ eindeutig bestimmt.

---

[1]) Vgl. **1**, § 6, Beispiel 1 [53].

Nach Satz 33 lassen sich die möglichen Typen zyklischer Gruppen den nicht-negativen ganzen Zahlen $f = 0, 1, 2, \ldots$ eineindeutig zuordnen, und alle diese Typen existieren wirklich, da sie ja durch die $\mathfrak{R}_f$ repräsentiert werden. Ist $\mathfrak{Z}$ eine durch A erzeugte zyklische Gruppe vom Typus $\mathfrak{R}_f$, so sind die verschiedenen Elemente von $\mathfrak{Z}$ nach Satz 27 [26] gegeben

a.) für $f = 0$ durch die sämtlichen ganzen Potenzen

$$\ldots, A^{-2}, A^{-1}, A^0 = E, A^1, A^2, \ldots;$$

dann ist also $\mathfrak{Z}$ von unendlicher Ordnung.

b.) für $f > 0$ etwa durch die f Potenzen $A^0 = E, A^1, \ldots, A^{f-1}$, an die sich bei beiderseitiger Fortsetzung dasselbe System von f Elementen in gleicher Reihenfolge wiederholt anreiht[1]); dann ist also $\mathfrak{Z}$ endlich von der Ordnung f.

Um alle Untergruppen einer zyklischen Gruppe zu bestimmen, vermerken wir zunächst die nachstehende, nach **1**, Satz 19, 25 [55, 59] ohne weiteres klare Tatsache:

Satz 34. Ist A ein Element aus einer Gruppe $\mathfrak{G}$, so bilden die ganzen Potenzen von A eine zyklische Untergruppe $\mathfrak{A}$ von $\mathfrak{G}$, **die Periode von A,** deren Ordnung auch die **Ordnung von A** heißt. Ist $\mathfrak{G}$ endlich von der Ordnung n, so ist auch A von endlicher Ordnung m und $m \mid n$.

Falls A von endlicher Ordnung m ist, läßt sich m nach Satz 33 auch dadurch charakterisieren, daß

$$A^k = E \text{ mit } k \equiv 0 \text{ mod. } m, \text{ d. h. mit } m \mid k$$

gleichbedeutend ist, oder auch als kleinster der positiven Exponenten k, für die $A^k = E$ ist. Wir beweisen zur späteren Anwendung noch:

Satz 35. Sind A_1, A_2 vertauschbare Elemente aus $\mathfrak{G}$ von den endlichen Ordnungen m_1, m_2 und ist $(m_1, m_2) = 1$, so hat $A_1 A_2$ die Ordnung $m_1 m_2$.

Beweis: Soll $(A_1 A_2)^k = E$ sein, so folgt durch Potenzieren mit m_2 bzw. m_1, unter Berücksichtigung der Voraussetzung $A_2 A_1 = A_1 A_2$,

$$A_1^{m_2 k} = E, \quad A_2^{m_1 k} = E,$$

also $m_1 \mid m_2 k$, $m_2 \mid m_1 k$. Wegen $(m_1, m_2) = 1$ muß also $m_1 \mid k$, $m_2 \mid k$

[1]) Daher die Bezeichnung zyklisch. Als Bild des Falles a.) ist dabei ein zu einer Geraden ausgearteter Kreis zu denken.

sein (Satz 16 [20]). Daraus folgt $m_1 m_2 | k$ (Satz 22, 20 [22]). Da umgekehrt

$$(A_1 A_2)^{m_1 m_2} = (A_1^{m_1})^{m_2} (A_2^{m_2})^{m_1} = E$$

ist, ist also $(A_1 A_2)^k = E$ dann und nur dann, wenn $m_1 m_2 | k$, d. h. $m_1 m_2$ ist die Ordnung von $A_1 A_2$.

Durch Anwendung von Satz 34 auf eine zyklische Gruppe $\mathfrak{G} = \mathfrak{Z}$ erhalten wir leicht alle Untergruppen von $\mathfrak{Z}$:

Satz 36. Ist $\mathfrak{Z}$ eine durch A erzeugte zyklische Gruppe von der endlichen Ordnung n (von unendlicher Ordnung [1])), so entspricht jedem positiven Teiler j von n (jedem positiven j) ein Normalteiler $\mathfrak{A}_j$ von der Ordnung $m = \frac{n}{j}$ (von unendlicher Ordnung), nämlich die Periode von A^j. Deren Faktorgruppe $\mathfrak{Z}/\mathfrak{A}_j$ ist wieder zyklisch, von der Ordnung j. Auf diese Weise entstehen alle (von der identischen verschiedenen) Untergruppen von $\mathfrak{Z}$. Diese, sowie ihre Faktorgruppen, sind also insbesondere sämtlich wieder zyklisch.

Beweis: a.) Nach Satz 34 sind die Perioden $\mathfrak{A}_j$ der genannten A^j Untergruppen von den angegebenen Ordnungen, und nach **1**, Satz 26 [60] natürlich Normalteiler von $\mathfrak{Z}$.

b.) Für die Kongruenz nach $\mathfrak{A}_j$ gilt nach ihrer Erklärung (**1**, Def. 16 [56]) und nach Def. 10 [26]

$A^{m_1} \equiv A^{m_2} (\mathfrak{A}_j)$ dann und nur dann, wenn $m_1 \equiv m_2 \bmod. j$.

Die Restklassen nach $\mathfrak{A}_j$ können also durch $A^0 = E, A^1, \ldots, A^{j-1}$ repräsentiert werden. Hiernach ist $\mathfrak{Z}/\mathfrak{A}_j$ zyklisch von der Ordnung j, nämlich durch die Restklasse von A erzeugt.

c.) Ist $\mathfrak{Z}'$ irgendeine Untergruppe (also Normalteiler) von $\mathfrak{Z}$, so liefert analog zu (3.) [31] die Festsetzung

$m_1 \equiv m_2$ dann und nur dann, wenn $A^{m_1} \equiv A^{m_2} (\mathfrak{Z}')$,

[1]) Das auf diesen — weiterhin nicht benötigten — Fall Bezügliche ist in Klammern beigefügt.

eine Kongruenzrelation in Γ. Ist j deren Modul, so ist A^m dann und nur dann in $\mathfrak{Z}'$, wenn $m \equiv 0$ mod. j (1, Satz 35 [66]), d. h. $j \mid m$ ist; $\mathfrak{Z}'$ besteht also aus allen und nur den ganzen Potenzen von A^j, d. h. ist die Periode $\mathfrak{A}_j$ von A^j. Ist $\mathfrak{Z}$ endlich von der Ordnung n, so ist $j \mid n$, weil $A^n = E$ zu $\mathfrak{Z}'$ gehört; ist $\mathfrak{Z}$ unendlich, so entspricht $j = 0$ die identische Untergruppe, positiven j von der identischen verschiedene Untergruppen.

Der Satz 34 ermöglicht auch die Bestimmung aller primitiven Elemente einer zyklischen Gruppe:

Satz 37. Ist $\mathfrak{Z}$ eine durch A erzeugte zyklische Gruppe vom Typus $\mathfrak{R}_f$, so entsprechen die primitiven Elemente von $\mathfrak{Z}$ bei der Zuordnung (2.) den primen Restklassen mod. f, d. h. es ist dann und nur dann A^m primitiv, wenn m prim zu f ist.

Beweis: A^m ist dann und nur dann primitiv, wenn seine Periode gleich $\mathfrak{Z}$ ist, und das ist dann und nur dann der Fall, wenn sie A enthält, d. h. wenn ein $\bar{m}$ existiert, so daß $A^{m\bar{m}} = A$, also $m\bar{m} \equiv 1$ mod. f ist. Hierzu ist aber nach Satz 3, 14 [9, 18] notwendig und nach Satz 31 [29] hinreichend, daß m prim zu f ist.

Für $f = 0$ (also unendliches $\mathfrak{Z}$) sind hiernach A^1, A^{-1} die einzigen primitiven Elemente, für $f > 0$ (also endliches $\mathfrak{Z}$ der Ordnung f) gibt es unter den f Elementen $\varphi(f)$ primitive [30]. Speziell sind, wenn $f = p$ Primzahl ist, alle $\varphi(p) = p - 1$ Elemente $\neq E$ primitiv.

§ 4. Primintegritätsbereiche, Primkörper, Charakteristik.

Wir leiten in diesem Paragraphen eine auf die Resultate von §§ 1, 2 für den Fall Γ gestützte, grundlegende Unterscheidung der Integritätsbereiche und Körper her. Dazu bezeichne durchweg I irgendeinen Integritätsbereich, K dessen Quotientenkörper. Da sich jeder Körper K als Quotientenkörper eines Integritätsbereiches (nämlich wieder K) auffassen läßt, bedeutet das keinerlei Einschränkung bezüglich der in Betracht gezogenen Körper K.

Wir betrachten die ganzen Vielfachen me des Einselementes e von I, für die nach ihrer Erklärung (**1**, am Schluß von § 1 [13]) die Rechenregeln gelten:

(1.) $m_1 e + m_2 e = (m_1 + m_2)e, \quad (m_1 e)(m_2 e) = (m_1 m_2)e.$

Die me sind die ganzen „Potenzen" von e, d. h. die Periode von e in der durch die Elemente von I gebildeten additiven abelschen Gruppe, und in diesem Sinne sind die Formeln (1.) nichts anderes als die Formeln (1.) des § 3 [30], allerdings mit einer kleinen Abweichung in der zweiten Formel. In Analogie zu dem dortigen Satz 34 [32] (aber unter Berücksichtigung der in I neben der als Gruppenverknüpfung gedeuteten Addition überdies vorhandenen zweiten Verknüpfung Multiplikation) ergibt sich aus (1.) nach **1**, Satz 6 [19]:

Satz 38. Die ganzen Vielfachen des Einselementes von I bilden einen Teilintegritätsbereich I_0 von I. Dessen Quotientenkörper ist ein Teilkörper K_0 von K.

Da e und somit auch alle me in jedem Teilintegritätsbereich von I und die Quotienten der me in jedem Teilkörper von K enthalten sind, gilt:

Satz 39. I_0 ist der engste Teilintegritätsbereich (Durchschnitt aller solchen) von I. K_0 ist der engste Teilkörper (Durchschnitt aller solchen) von K.

Die in Satz 39 ausgesprochene Eigenschaft von I_0 bzw. K_0 rechtfertigt die Definition:

Definition 13. I_0 heißt der **Primintegritätsbereich** von I, K_0 der **Primkörper** von K.

Die angekündigte Unterscheidung der Integritätsbereiche I und der Körper K bezieht sich nun auf den Typus ihrer Primintegritätsbereiche I_0 bzw. Primkörper K_0. Wenn auch nach (1.) die Rechenoperationen mit den me aus I_0 isomorph zu den entsprechenden Rechenoperationen mit den m aus Γ

verlaufen, braucht deshalb doch nicht I_0 vom Typus Γ zu sein; denn, wie das Beispiel der P_p lehrt, ist die Zuordnung $me \longleftrightarrow m$ nicht notwendig eineindeutig, d. h. Gleichheit und Unterschiedenheit in I_0 und in Γ entsprechen sich bei dieser Zuordnung nicht notwendig. Für die möglichen Typen von I_0 gilt vielmehr ganz Entsprechendes, wei wir in § 3 (Satz 33 [31]) für die Typen zyklischer Gruppen festgestellt haben:

Satz 40. Zu I existiert eine eindeutig bestimmte ganze Zahl $f \geqq 0$, so daß I_0 vermöge der Zuordnung

(2.) $$me \longleftrightarrow \{m\}$$

zum Restklassenring Γ_f isomorph ist.

Beweis: Aus der Auffassung von I_0 als Periode von e in I resultiert nach § 3, (3.) [31], daß die Relation

(3.) $m_1 \equiv m_2$ dann und nur dann, wenn $m_1 e = m_2 e$ o

eine Kongruenzrelation in Γ ist. Ist f deren Modul, also

(4.) $m_1 e = m_2 e$ dann und nur dann, wenn $m_1 \equiv m_2$ mod. f,

so ist nach (4.) die Zuordnung (2.) zwischen I_0 und Γ_f eineindeutig. Wie im Bew. zu Satz 33 [31] ist sie ferner nach (1.) isomorph, hier außer für die Addition (die der dortigen Gruppenverknüpfung entspricht) auch für die in I_0 und Γ_f erklärte Multiplikation.

Auf Grund von Satz 40 definieren wir:

Definition 14. Die ganze Zahl $f \geqq 0$ aus Satz 40, d. h. der Modul der Kongruenzrelation (3.) heißt die **Charakteristik** von I und K.

Da nun das zu Γ_f isomorphe I_0 Integritätsbereich ist, ergibt sich aus Satz 28 [27]:

Satz 41. Die Charakteristik von I und K ist entweder 0 oder eine Primzahl p. Ist sie 0, so ist $\mathsf{I}_0 \cong \Gamma, \mathsf{K}_0 \cong \mathsf{P}$; ist sie p, so ist $\mathsf{I}_0 = \mathsf{K}_0 \cong \mathsf{P}_p$.

Durch Satz 41 motiviert sich die Bezeichnung Charakteristik von I und K, insofern diese den Typus des Primintegritätsbereiches I_0 bzw. Primkörpers K_0 charakterisiert. Daß alle nach Satz 41 möglichen Charakteristiken wirklich vorkommen, zeigen die Bereiche Γ, P, P_p, die ihre eigenen Primbereiche[1]) sind. Nach dem Verfahren von **1**, § 3, d) [29] kann man aus jedem Bereich I oder K einen isomorphen herleiten, der als Primbereich Γ oder P bzw. ein P_p (d. h. die ganzen oder rationalen Zahlen bzw. die Restklassen nach einer Primzahl p) selbst enthält. Wir reden daher im folgenden kurz von den Primbereichen Γ, P, P_p.

Man sieht ferner ohne weiteres folgende Tatsachen ein (vgl. schon Satz 39):

Satz 42. Alle Erweiterungs- und Teilbereiche eines Bereiches haben dieselbe Charakteristik.

Aus dem Gesetz (4.) für die ganzen Vielfachen von e ergibt sich vermöge der Umformung

$$m_1 a - m_2 a = (m_1 - m_2) a = (m_1 - m_2) e \cdot a = (m_1 e - m_2 e) \cdot a$$

leicht ein entsprechendes Gesetz für die ganzen Vielfachen eines $a \neq 0$:

Satz 43. Ist a ein Element eines Bereiches der Charakteristik f, so ist

$m_1 a = m_2 a$ dann und, falls $a \neq 0$, auch nur dann, wenn

$$\begin{Bmatrix} m_1 = m_2 \text{ (für } f = 0) \\ m_1 \equiv m_2 \bmod. p \text{ (für } f = p) \end{Bmatrix}.$$

Insbesondere ist also

$ma = 0$ dann und, falls $a \neq 0$, auch nur dann, wenn

$$\begin{Bmatrix} m = 0 \text{ (für } f = 0) \\ m \equiv 0 \bmod. p \text{ (für } f = p) \end{Bmatrix}.$$

Infolge des in diesem Satz zum Ausdruck kommenden abweichenden Verhaltens der Bereiche mit einer Charakteristik p gegenüber denen mit der Charakteristik 0 (z. B. allen Zahlbereichen) sind nicht alle aus der „Zahlenalgebra" geläufigen Schlußweisen in unserer abstrakten „Bereichalgebra" anwendbar, wie wir das ja in **1** mehrfach hervorhoben [Beweise zu Satz 12, d); Satz 13, d); Satz 70 [41, 44, 129]].

Auch die folgende, später anzuwendende Tatsache zeigt eine Abweichung der Bereiche mit einer Charakteristik p gegenüber den in der Zahlenalgebra vorliegenden Verhältnissen:

Satz 44. In Bereichen der Charakteristik p darf eine Summe gliedweise mit p potenziert werden:

$$\left(\sum_{k=1}^{n} a_k\right)^p = \sum_{k=1}^{n} a_k^p.$$

---

[1]) Bereich steht hier und in den folgenden Ausführungen für Integritätsbereich oder Körper.

Beweis: Es genügt, den Satz für $n = 2$ zu beweisen, da er dann durch Induktion allgemein folgt. Nach dem (aus den Elementen vorausgesetzten) binomischen Satz ist nun

$$(a_1 + a_2)^p = a_1^p + \sum_{\nu=1}^{p-1} \binom{p}{\nu} a_1^\nu a_2^{p-\nu} + a_2^p,$$

wo $\binom{p}{\nu}$ die Kombinationsanzahl von p Elementen zur ν-ten Klasse bezeichnet, für die die Formel

$$\binom{p}{\nu} = \frac{p!}{\nu!(p-\nu)!} = \frac{p \cdot (p-1) \cdots (p-(\nu-1))}{1 \cdot 2 \cdots \nu}$$

gilt (vgl. **1**, Bew. zu Satz 66 [123]). Da für $1 \leqq \nu \leqq p-1$ das Produkt $1 \cdot 2 \cdots \nu$ zu p prim ist (Satz 23 [22]) und wegen der Ganzzahligkeit der Anzahl $\binom{p}{\nu}$ in dem Produkt $p \cdot [(p-1) \cdots (p-(\nu-1))]$ aufgeht, muß es nach Satz 16 [20] in dem zweiten Faktor $[\ldots]$ dieses Produktes aufgehen, so daß $\binom{p}{\nu} \equiv 0 \bmod. p$ ist. Aus Satz 43 folgt daher

$$(a_1 + a_2)^p = a_1^p + a_2^p.$$

Es sei übrigens bemerkt, daß eine entsprechende Regel auch für die Subtraktion gilt; denn aus $(a_1 + a_2)^p - a_1^p = a_2^p$ folgt ja wegen der Unbeschränktheit der Subtraktion allgemein $b_1^p - b_2^p = (b_1 - b_2)^p$.

II. Die Wurzeln algebraischer Gleichungen.

Wir leiten in diesem Abschnitt eine Reihe von Sätzen über Wurzeln α von Polynomen $f(x)$ aus K in Erweiterungskörpern Λ von K her, ohne dabei auf die erst in III zu behandelnde Existenzfrage der Λ und α bei gegebenem K und $f(x)$ einzugehen. Diese Sätze sind also lediglich als Folgerungen aus der Voraussetzung anzusehen, daß ein Polynom aus K in einem Erweiterungskörper Λ von K eine oder mehrere Wurzeln hat.

Zur Vereinfachung der Ausdrucksweise treffen wir folgende

Bezeichnungsfestsetzungen für Abschnitt II—IV.

Große griechische Buchstaben, außer den bereits vergebenen M (Menge), B (Bereich), I (Integritätsbereich), Γ (Integritätsbereich der ganzen Zahlen), bedeuten stets Körper, ohne daß dies immer ausdrücklich gesagt wird, und zwar K den Grundkörper, Λ irgendeinen Erweiterungskörper (kurz Erweiterung) von K, weitere Buchstaben Erweiterungen von K mit speziellen, wie bei P (Körper der rationalen Zahlen) durch die Bezeichnung schon angedeuteten Eigenschaften, die wir aber der Deutlichkeit halber doch immer ausführlich nennen werden. Für das Enthaltensein und Enthalten bei Körpern (später auch bei Gruppen) verwenden wir sinngemäß die Zeichen $\leqq, \geqq, <, >$. Ist $K \leqq \overline{K} \leqq \Lambda$, so nennen wir $\overline{K}$ einen Körper zwischen K und Λ.

Elemente aus dem Grundkörper K bezeichnen wir mit $a, b, c, \ldots$, solche aus Erweiterungen Λ von K mit $\alpha, \beta, \gamma, \ldots$ (vgl. **1**, erste Anm. zu § 1 [9]), ebenso Elemente aus $K[x]$ mit $f(x), g(x), h(x), \ldots$, solche aus $\Lambda[x]$ mit $\varphi(x), \psi(x), \chi(x), \ldots$ [1]). Wir dürfen dann erläuternde Zusätze über die Körper, denen vorkommende Elemente angehören sollen, oft fortlassen.

Ebenso lassen wir auch die Zusätze „in K" bei „irreduzibel" und „Primfaktorzerlegung", sowie entsprechende Zusätze bei einigen im weiteren Verlaufe einzuführenden Begriffen, die sich auf einen bestimmten Grundkörper beziehen, gelegentlich fort, wenn nur ein in der gerade vorliegenden Betrachtung fester Grundkörper K in Betracht kommt. Definitionen, auf die diese Festsetzung Anwendung finden soll, werden durch * gekennzeichnet.

§ 5. Wurzeln und Linearfaktoren.

1.) Der in § 1 für $K[x]$ bewiesene Fundamentalsatz ermöglicht zunächst die Herstellung eines Zusammenhangs zwischen den Wurzeln eines Polynoms aus K in einer Erweiterung Λ von K und denen seiner Primfaktoren in K. Nach **1**, Satz 4 [12] und dem Einsetzungsprinzip gilt nämlich:

Satz 45. Ist

$$f(x) \equiv p_1(x) \cdots p_r(x)\,^{2)}$$

ein in seine Primfaktoren zerlegtes Polynom aus

[1]) Vorkommende gebrochene rationale Funktionen, die wir in **1** so bezeichneten, werden als Quotienten ganzer rationaler Funktionen dargestellt.

[2]) Nach der Definition von Polynom i. d. Einl., sowie nach Def. 8 [14] und Satz 11 [14] ist dabei der in Satz 12 [14] auftretende Einheitsfaktor $a = e$.

K, so ist jede Wurzel von $f(x)$ in Λ auch Wurzel von mindestens einem der $p_i(x)$ und umgekehrt jede Wurzel eines der $p_i(x)$ in Λ auch Wurzel von $f(x)$.

Man beherrscht somit die Wurzeln von $f(x)$, wenn man die der $p_i(x)$ beherrscht, und könnte sich demnach auf die Untersuchung der Wurzeln irreduzibler Polynome beschränken. Da sich diese Beschränkung aber für die in III, IV auseinanderzusetzende Theorie als überflüssig erweist, wollen wir sie nicht einführen. Das erscheint auch in Hinsicht auf das Nichtvorhandensein eines rationalen Rechenverfahrens zur Herstellung der Primfaktorzerlegung erwünscht.

2.) Wir beweisen ferner einige Sätze über den Zusammenhang der Wurzeln eines Polynoms aus K mit dessen Primfaktoren 1-ten Grades (sog. **Linearfaktoren**) in einer Erweiterung Λ von K.

Satz 46. Ist α Wurzel von $f(x)$ in Λ, so ist $f(x)$ durch den Linearfaktor $x-\alpha$ teilbar, d. h. es besteht in Λ eine Zerlegung

$$f(x) \equiv (x-\alpha)\,\varphi(x).$$

Umgekehrt folgt aus einer solchen Zerlegung, daß α Wurzel von $f(x)$ ist.

Beweis: a.) Nach Satz 13 [16] kann

$$f(x) \equiv (x-\alpha)\,\varphi(x) + \psi(x) \quad \text{mit} \quad |\psi(x)| < |x-\alpha|$$

gesetzt werden. Da $|x-\alpha| = k^1$ ist, muß $|\psi(x)| = k^0 = 1$ sein, so daß $\psi(x) \equiv \beta$ ein Element aus Λ ist. Für $x=\alpha$ folgt dann wegen $f(\alpha)=0$ auch $\beta = 0$, d. h. die behauptete Zerlegung.

b.) Die Umkehrung ist klar.

Satz 47. Sind $\alpha_1, \ldots, \alpha_\nu$ verschiedene Wurzeln von $f(x)$ in Λ, so besteht in Λ eine Zerlegung

$$f(x) \equiv (x-\alpha_1)\cdots(x-\alpha_\nu)\,\varphi(x).$$

Umgekehrt folgt aus einer solchen Zerlegung, daß $\alpha_1, \ldots, \alpha_\nu$ Wurzeln von $f(x)$ sind.

Beweis: a.) Die Primfunktionen $x-\alpha_1, \ldots, x-\alpha_\nu$ sind nach Voraussetzung verschieden, und jede kommt nach

Satz 46 in der Primfaktorzerlegung von $f(x)$ im Körper $\mathsf{\Lambda}$ vor. Wegen der Eindeutigkeit dieser Zerlegung muß also auch ihr Produkt in $f(x)$ enthalten sein, d. h. eine Zerlegung der behaupteten Art bestehen.

b.) Die Umkehrung ist klar.

Aus Satz 47 ergibt sich durch Vergleichung der beiderseitigen Grade unmittelbar die wichtige Tatsache:

Satz 48. Ein Polynom n-ten Grades aus K hat in keiner Erweiterung $\mathsf{\Lambda}$ von K mehr als n verschiedene Wurzeln.

Aus Satz 48 läßt sich der folgende, später anzuwendende Satz folgern:

Satz 49. Besteht K aus unendlich vielen Elementen und sind $g_1(x_1, \ldots, x_n), \ldots, g_r(x_1, \ldots, x_n)$ voneinander verschiedene Elemente aus $\mathsf{K}[x_1, \ldots, x_n]$, so gibt es in jeder unendlichen Teilmenge M von K Elementsysteme $a_1, \ldots, a_n$ derart, daß die Elemente $g_1(a_1, \ldots, a_n), \ldots, g_r(a_1, \ldots, a_n)$ aus K ebenfalls voneinander verschieden sind.

Beweis: Durch Betrachtung des Differenzenprodukts $g = \prod\limits_{\substack{i, k=1 \\ i<k}}^{r} (g_i - g_k)$ reduziert sich die Behauptung ohne weiteres auf jede der beiden folgenden, gleichbedeutenden:

(a.) Ist $g(x_1, \ldots, x_n) \not\equiv 0$, so gibt es $a_1, \ldots, a_n$ aus M, so daß $g(a_1, \ldots, a_n) \neq 0$ ist.

(b.) Ist $g(a_1, \ldots, a_n) = 0$ für alle $a_1, \ldots, a_n$ aus M, so ist $g(x_1, \ldots, x_n) \equiv 0$ [1]).

Diese beweisen wir durch vollständige Induktion: Für $n = 1$ ist (a.) eine Folge aus Satz 48; ist nämlich $g(x) \not\equiv 0$, so ist entweder $g(x) \equiv b \neq 0$ (Einheit) und also $g(a) = b \neq 0$ für alle a aus M, oder $g(x)$ ist bis auf einen von Null verschiedenen Faktor aus K ein Polynom und dann $g(a) = 0$ für nur endlich viele a aus K, so daß nach den Voraussetzungen über K und M Elemente a in M existieren, für die $g(a) \neq 0$ ist. Sei nun (a.) und somit (b.) für $n = \nu - 1$ schon bewiesen. Dann betrachten wir die Polynome

---

[1]) Hierdurch wird die in **1**, Bew. zu Satz 12, d) [41] ausgesprochene Behauptung [vgl. dazu **1**, Bew. zu Satz 13, d) [44]] bestätigt. Man hat dazu unter K den Quotientenkörper des dortigen Integritätsbereichs I und unter M das dortige I zu verstehen.

$$\bar{g}(x_\nu) \equiv g(x_1, \ldots, x_\nu) \text{ über } \mathsf{K}[x_1, \ldots, x_{\nu-1}],$$
$$\bar{g}^*(x_\nu) \equiv g(a_1, \ldots, a_{\nu-1}, x_\nu) \text{ über } \mathsf{K},$$

von denen die letzteren durch Einsetzung von Systemen $a_1, \ldots, a_{\nu-1}$ aus M für $x_1, \ldots, x_{\nu-1}$ aus dem ersteren entstehen. Ist nun $g(a_1, \ldots, a_\nu) = 0$ für alle $a_1, \ldots, a_\nu$ aus M, so ist nach (b.) ($n = 1$) zunächst jedes $\bar{g}^*(x_\nu) \equiv 0$. Folglich sind nach (b.) ($n = \nu - 1$) die Koeffizienten von $\bar{g}(x_\nu)$, d. h. $\bar{g}(x_\nu)$ selbst $\equiv 0$, was $g(x_1, \ldots, x_\nu) \equiv 0$ bedeutet. Also ist (b.) dann auch für $n = \nu$, und daher allgemein richtig.

Präziser als Satz 47, 48, insofern nicht mehr die Verschiedenheit der Wurzeln vorausgesetzt wird, ist der folgende Satz:

Satz 50. Zerfällt $f(x)$ in Λ in Linearfaktoren:
$$f(x) \equiv (x - \alpha_1) \cdots (x - \alpha_n),$$
so sind $\alpha_1, \ldots, \alpha_n$ Wurzeln von $f(x)$. Weitere Wurzeln von $f(x)$ existieren dann weder in Λ noch in irgendeiner Erweiterung $\bar{\Lambda}$ von Λ.

Beweis: a.) Der erste Teil des Satzes ist klar (Satz 47 [40]).

b.) Ist α Wurzel von $f(x)$ (in Λ oder einem $\bar{\Lambda}$), so folgt aus $f(\alpha) = 0$, daß $(\alpha - \alpha_1) \cdots (\alpha - \alpha_n) = 0$ ist, so daß α einer der Wurzeln α_i gleich sein muß (1, Satz 4 [12]).

Wir verabreden für die Folge, daß bei der Voraussetzung von Satz 50 unter den Wurzeln von $f(x)$ in Λ stets die den Linearfaktoren von $f(x)$ entsprechende volle Reihe $\alpha_1, \ldots, \alpha_n$ verstanden wird, ungeachtet ob darunter gleiche vorkommen oder nicht.

Durch die Sätze 46, 47, 50 ist der Weg für die in III auszuführende Konstruktion der Wurzeln eines Polynoms $f(x)$ aus K vorgezeichnet. Wir werden K schrittweise so zu erweitern haben, daß von $f(x)$ bei jedem Schritt mindestens ein Linearfaktor abgespalten wird. Ist auf diese Weise eine Erweiterung Λ gefunden, in der $f(x)$ vollständig in Linearfaktoren zerfällt, so dürfen wir mit dem Erweiterungsprozeß haltmachen, da eine Fortsetzung dann nach Satz 50 keine neuen Wurzeln mehr liefern kann.

3.) Wir beweisen schließlich einige Tatsachen über die Wurzeln irreduzibler Polynome.

Aus Satz 46 [40] und dem Begriff der Irreduzibilität folgt zunächst unmittelbar:

Satz 51. Ein irreduzibles Polynom aus K hat in K dann und nur dann eine Wurzel, wenn es vom Grade 1 ist.

Hierdurch wird der in der Einleitung hervorgehobene Umstand 2.) in Evidenz gesetzt, daß man i. a. den Grundkörper erweitern muß, um zu Wurzeln eines Polynoms zu gelangen. Man muß allerdings die hier nicht vollständig zu erörternde Tatsache hinzunehmen, daß der Grundkörper i. a. irreduzible Polynome von höherem als dem 1-ten Grade enthält. (Spezielle Sätze in dieser Richtung siehe in § 23.)

Satz 52. Zwei relativ prime Polynome, insbesondere also zwei verschiedene irreduzible Polynome aus K haben in keiner Erweiterung von K eine gemeinsame Wurzel.

Beweis: Ist α eine gemeinsame Wurzel von $f_1(x)$ und $f_2(x)$ in Λ, so ist $x-\alpha$ nach Satz 46 [40] ein gemeinsamer Teiler von $f_1(x)$ und $f_2(x)$ in Λ. Nach Satz 24 [23] ist dann also $(f_1(x), f_2(x)) \neq e$.

Aus Satz 52 ergibt sich der folgende sog. **Fundamentalsatz über irreduzible Polynome:**

Satz 53. Hat das in K irreduzible $f(x)$ mit irgendeinem $h(x)$ aus K in einer Erweiterung von K eine gemeinsame Wurzel, so ist $f(x) \mid h(x)$.

Beweis: Nach Satz 17 [20] wäre sonst $f(x)$ prim zu $h(x)$, was nach Satz 52 der Voraussetzung widerspricht.

In diesem Satz braucht $h(x)$ nicht ein Polynom, also von 0 und Einheiten verschieden und normiert zu sein. Insbesondere wird der Satz für $h(x) \equiv 0$ trivial, für $h(x) \equiv a$ inhaltlos.

Auf Satz 53 wird sich unsere in III auszuführende Konstruktion der Wurzeln von $f(x)$ vornehmlich stützen.

§ 6. Mehrfache Wurzeln, Ableitung.

Definition 15. Eine Wurzel α von $f(x)$ in Λ heißt **ν-fach,** wenn in Λ (und somit in jeder Erweiterung von Λ) eine Zerlegung

$$f(x) \equiv (x-\alpha)^{\nu}\varphi(x) \quad \text{mit} \quad \varphi(\alpha) \neq 0$$

besteht; **mehrfach,** wenn $\nu > 1$ ist.

Die Bezeichnung ν-fach rechtfertigt sich durch die Tatsache:

Satz 54. Ist α eine ν-fache Wurzel von $f(x)$ in Λ, so sind genau ν Wurzeln von $f(x)$ in Λ (und in jeder Erweiterung von Λ) gleich α.

Beweis: Nach Def. 15 enthält dann $f(x)$ den Primfaktor $x-\alpha$ mindestens ν-mal, wegen $\varphi(\alpha) \neq 0$ aber nach Satz 46 [40] nicht öfter.

Die Vielfachheit einer Wurzel von $f(x)$ steht in Zusammenhang mit der aus der Analysis bekannten Ableitung $f'(x)$ von $f(x)$. Natürlich können wir die Ableitung hier, für unsere abstrakten Grundkörper nicht auf die in der Analysis übliche Weise durch einen Grenzprozeß definieren. Wir geben daher die folgende, formale Definition:

Definition 16. Unter der **Ableitung** von

$$f(x) \equiv a_0 + a_1 x + \cdots + a_n x^n \equiv \sum_{k=0}^{\infty} a_k x^k \text{ [1]}$$

verstehen wir

$$f'(x) \equiv a_1 + 2a_2 x + \cdots + n a_n x^{n-1} \equiv \sum_{k=1}^{\infty} k a_k x^{k-1}$$

$$\equiv \sum_{k=0}^{\infty} (k+1) a_{k+1} x^k.$$

Für diesen formal mit der entsprechenden Differentiationsregel der Analysis übereinstimmenden Prozeß der Ableitungsbildung gelten wie dort die Formeln

(1.) $\quad (f(x) \pm g(x))' \equiv f'(x) \pm g'(x),$

(2.) $\quad (f(x)\, g(x))' \equiv f'(x)\, g(x) + f(x)\, g'(x),$

insbesondere also

$$(af(x))' \equiv af'(x),$$

$$(f(x)^n)' \equiv nf(x)^{n-1} f'(x).$$

Beweis: Ist

[1]) Vgl. 1, Anm. 3 zu Satz 11 [32].

$$f(x) \equiv \sum_{k=0}^{\infty} a_k x^k, \qquad g(x) \equiv \sum_{k=0}^{\infty} b_k x^k,$$

also

$$f'(x) \equiv \sum_{k=1}^{\infty} k a_k x^{k-1} \equiv \sum_{k=0}^{\infty} (k+1)\, a_{k+1} x^k,$$

$$g'(x) \equiv \sum_{k=1}^{\infty} k b_k x^{k-1} \equiv \sum_{k=0}^{\infty} (k+1)\, b_{k+1} x^k,$$

so folgt nach **1**, § 4, (2.), (3.) [33] (vgl. auch **1**, Schluß von § 1 [13])

$$(f(x)+g(x))' \equiv \Big(\sum_{k=0}^{\infty} (a_k+b_k)\, x^k\Big)' \equiv \sum_{k=1}^{\infty} k(a_k+b_k)\, x^{k-1}$$

$$\equiv \sum_{k=1}^{\infty} k a_k x^{k-1} + \sum_{k=1}^{\infty} k b_k x^{k-1} \equiv f'(x)+g'(x),$$

$$(f(x)\,g(x))' \equiv \Big(\sum_{k=0}^{\infty} \Big(\sum_{\nu+\mu=k} a_\nu b_\mu\Big) x^k\Big)' \equiv \sum_{k=1}^{\infty} \Big(k \sum_{\nu+\mu=k} a_\nu b_\mu\Big) x^{k-1}$$

$$\equiv \sum_{k=1}^{\infty} \Big(\sum_{\nu+\mu=k} (\nu+\mu)\, a_\nu b_\mu\Big) x^{k-1}$$

$$\equiv \sum_{k=1}^{\infty} \Big(\sum_{\nu+\mu=k} \nu a_\nu b_\mu\Big) x^{k-1} + \sum_{k=1}^{\infty} \Big(\sum_{\nu+\mu=k} \mu a_\nu b_\mu\Big) x^{k-1}$$

$$\equiv \sum_{k=0}^{\infty} \Big(\sum_{\nu+\mu=k} (\nu+1)\, a_{\nu+1} b_\mu\Big) x^k + \sum_{k=0}^{\infty} \Big(\sum_{\nu+\mu=k} (\mu+1)\, a_\nu b_{\mu+1}\Big) x^k$$

$$\equiv f'(x)\,g(x) + f(x)\,g'(x).$$

Ferner gilt, sozusagen als Ersatz für die fehlende Grenzrelation:

Satz 55. Wird für ein α

$$\varphi(x) \equiv \frac{f(x)-f(\alpha)}{x-\alpha}$$

gesetzt, so ist

$$\varphi(\alpha) = f'(\alpha).$$

Beweis: Da α Wurzel von $f(x)-f(\alpha)$ ist, ist $\varphi(x)$ nach Satz 46 [40] wirklich eine ganze rationale Funktion. Aus

$$f(x) \equiv f(\alpha) + (x-\alpha)\,\varphi(x)$$

folgt daher nach (1.), (2.)

$$f'(x) \equiv \varphi(x) + (x-\alpha)\,\varphi'(x),$$

also

$$f'(\alpha) = \varphi(\alpha).$$

Aus Satz 55 ergibt sich nun der folgende Zusammenhang zwischen der Mehrfachheit einer Wurzel α von $f(x)$ und dem Ableitungswert $f'(\alpha)$:

Satz 56. Eine Wurzel α von $f(x)$ ist dann und nur dann mehrfach, wenn $f'(\alpha) = 0$ ist.

Beweis: Ist α Wurzel von $f(x)$, so hat in der nach Satz 46 [40] bestehenden Zerlegung

$$f(x) \equiv (x-\alpha)\,\varphi(x)$$

$\varphi(x)$ dieselbe Bedeutung wie in Satz 55. Nun ist nach Def. 15 [43] die Mehrfachheit von α mit $\varphi(\alpha) = 0$, also nach Satz 55 mit $f'(\alpha) = 0$ gleichbedeutend.

Der hierin liegende Zusammenhang führt zu einer wichtigen Folgerung über die Vielfachheit der Wurzeln eines irreduziblen Polynoms. Diese Folgerung beruht auf dem Analogon zu dem Satz der Analysis, daß aus $f'(x) \equiv 0$ folgt $f(x) \equiv a_0$. Wegen des Auftretens der ganzen Vielfachen ka_k der a_k als Koeffizienten von $f'(x)$ findet aber hier eine Abweichung gegenüber der Analysis statt:

Satz 57. Hat K die Charakteristik 0, so haben alle und nur die Einheiten $f(x) \equiv a_0$ aus $\mathsf{K}[x]$ die Ableitung $f'(x) \equiv 0$. Hat K die Charakteristik p, so haben alle und nur die Elemente von der Form

$$(3.) \qquad f(x) \equiv \sum_{l=0}^{\infty} a_{lp}\, x^{lp}, \text{ also } f(x) \equiv f_0(x^p)$$

aus $\mathsf{K}[x]$ die Ableitung $f'(x) \equiv 0$.

Beweis: a.) Daß für die genannten $f(x)$ durchweg $f'(x) \equiv 0$ ist, ist nach Satz 43 [37] und Def. 16 [44] klar.

b.) Ist $f(x) \equiv \sum_{k=0}^{\infty} a_k x^k$ und ist $f'(x) \equiv \sum_{k=1}^{\infty} k a_k x^{k-1} \equiv 0$, also $ka_k = 0$ $(k = 1, 2, \ldots)$, so folgt nach Satz 43 im Falle der Charakteristik 0

$$a_k = 0 \quad (k = 1, 2, \ldots),$$

d. h. $f(x) \equiv a_0$, im Falle der Charakteristik p dagegen nur

$$a_k = 0 \text{ für } k \not\equiv 0 \text{ mod. } p,$$

so daß $f(x)$ von der Form (3.) ist.

Die in Satz 57 liegende Abweichung für den Fall der Charakteristik p bedingt nun, daß die angekündigte Folgerung über die Vielfachheit der Wurzeln eines irreduziblen Polynoms im Fall der Charakteristik p auf solche irreduziblen Polynome zu beschränken ist, die nicht von der Form (3.) sind. Steinitz[1]) nennt solche irreduziblen Polynome von erster Art, die von der Form (3.) von zweiter Art.

Dem Vorgang v. d. Waerdens folgend, wollen wir die in der nachstehenden Definition gegebene Bezeichnung gebrauchen:

Definition 17. Ein **irreduzibles Polynom** $f(x)$ aus K heißt **separabel,** wenn seine Ableitung $f'(x) \not\equiv 0$ ist, also, falls K die Charakteristik 0 hat, stets; falls K die Charakteristik p hat, dann und nur dann, wenn es nicht von der Form (3.) in Satz 57 ist.

Andernfalls heißt $f(x)$ **inseparabel.**

Die Bezeichnung separabel spielt auf die folgende Tatsache, die bereits angekündigte Folgerung aus Satz 56, an:

Satz 58. Ist ein irreduzibles Polynom $f(x)$ separabel, so hat $f(x)$ nur einfache Wurzeln.

Beweis: Wäre α eine mehrfache Wurzel von $f(x)$, so wäre $f'(\alpha) = 0$ (Satz 56) und daher $f(x) \mid f'(x)$ (Satz 53 [43]). Wegen der vorausgesetzten Separabilität von $f(x)$ ist nun $f'(x) \not\equiv 0$ (Def. 17). $f'(x)$ kommt also ein Grad zu, und dieser ist kleiner als der von $f(x)$ (Def. 16 [44]). Das steht aber im Widerspruch zu $f(x) \mid f'(x)$ (Satz 6 [13]). Also ist die Annahme, $f(x)$ habe eine mehrfache Wurzel, unzutreffend.

---

[1]) Wir meinen bei Nennung des Namens Steinitz hier und im folgenden stets dessen in **1**, Lit. Verz. I zitierte Arbeit, deren Abschnitte I und II bis auf das die Erweiterungen zweiter Art Betreffende in unseren Abschnitten **1**, I und **2**, I—IV verarbeitet sind, ja geradezu deren Inhalt ausmachen. In diese grundlegende Originalarbeit zur Körpertheorie sollte jeder Algebraiker einmal hineingesehen haben.

Satz 58 läßt übrigens folgende Umkehrung zu:

Satz 59. Hat ein irreduzibles Polynom $f(x)$ eine nur einfache Wurzel α, so ist $f(x)$ separabel.

Beweis: Es ist dann $f'(\alpha) \neq 0$ (Satz 56), also gewiß $f'(x) \not\equiv 0$, und daher $f(x)$ separabel (Def. 17).

Wir definieren ferner noch im Anschluß an Def. 17:

***Zusatz zu Definition 17** [1]). Ein **beliebiges Polynom** aus K heißt **separabel** in K, wenn seine Primfaktoren in K separabel sind, sonst **inseparabel** in K.

Im Falle der Charakteristik 0 ist also jedes Polynom separabel. Für den Fall der Charakteristik p sei ausdrücklich bemerkt, daß die Entscheidung über die Separabilität beliebiger Polynome nicht etwa, wie gemäß Def. 17 für irreduzible Polynome, einfach durch Bilden der Ableitung getroffen werden kann. Es kann sehr wohl $f'(x) \equiv 0$ auch für separables $f(x)$ sein (z. B. wenn $f(x) \equiv f_0(x)^p$ mit separablem irreduziblem $f_0(x)$ ist), und $f'(x) \not\equiv 0$ für inseparables $f(x)$ (z. B. wenn $f(x) \equiv x f_0(x)$ mit inseparablem irreduziblem $f_0(x)$ ist). Auch der in Satz 58, 59 gegebene Zusammenhang mit der Wurzelvielfachheit, der die Bezeichnung separabel rechtfertigte, überträgt sich nicht auf beliebige Polynome. Dennoch ist die im Zusatz zu Def. 17 gegebene Ausdehnung dieser Bezeichnung auf beliebige Polynome für die späteren Zwecke nützlich.

Über ein Verfahren zur Entscheidung über die Separabilität beliebiger Polynome, das nicht die Zerlegung in Primfaktoren erfordert (was nach dem im Anschluß an Satz 24 [23] Gesagten erwünscht sein muß), sei des knappen Raumes halber auf Steinitz verwiesen. Hier sei nur die folgende für unsere Zwecke ausreichende Tatsache vermerkt, die sich gemäß Def. 17, Zusatz unmittelbar aus Satz 59 ergibt:

Zusatz zu Satz 59. Zerfällt ein beliebiges Polynom $f(x)$ aus K in einer Erweiterung von K in verschiedene Linearfaktoren, d. h. sind die Wurzeln $\alpha_1, \ldots, \alpha_n$ von

$$f(x) \equiv (x - \alpha_1) \cdots (x - \alpha_n)$$

voneinander verschieden, so ist $f(x)$ separabel (in K und jeder Erweiterung von K).

---

[1]) Über die Bedeutung von * vgl. die Einl. zu II [39].

Von Bedeutung sind diejenigen Körper, in denen jedes Polynom separabel ist. Sie heißen vollkommene Körper. Wir wollen unter Benutzung teilweise erst später zu gewinnender Resultate ganz kurz einige Angaben über vollkommene Körper machen.

Zunächst ist jeder Körper der Charakteristik 0 vollkommen, wie wir den obigen Betrachtungen unmittelbar entnehmen können. — Soll ferner ein Körper K der Primzahlcharakteristik p vollkommen sein, so muß insbesondere jedes Polynom $x^p - a$ aus K separabel sein. Dann ist die Gleichung $x^p \doteq a$ in K lösbar. Denn aus ihrer Unlösbarkeit in K folgte nach dem späteren Satz 123, b.) [137] die Irreduzibilität des Polynoms $x^p - a$ in K und daher nach Def. 17 seine Inseparabilität. Die Lösung von $x^p \doteq a$ in K ist überdies eindeutig. Aus $a_1^p = a$, $a_2^p = a$ folgt ja $0 = a_1^p - a_2^p = (a_1 - a_2)^p$ (Satz 44 [37]), also $a_1 - a_2 = 0$, $a_1 = a_2$. Wir bezeichnen diese eindeutige Lösung von $x^p \doteq a$ mit $\sqrt[p]{a}$.

Sei umgekehrt in dem Körper K der Primzahlcharakteristik p die Gleichung $x^p \doteq a$ für jedes a aus K lösbar. Wäre dann das irreduzible Polynom $f(x)$ aus K inseparabel, so wäre $f(x)$ nach Def. 17 von der Form

$$f(x) = \sum_{\nu=0}^{n} a_\nu x^{\nu p} = \sum_{\nu=0}^{n} \left(\sqrt[p]{a_\nu}\right)^p x^{\nu p},$$

und Satz 44 [37] lieferte

$$f(x) = \left(\sum_{\nu=0}^{n} \sqrt[p]{a_\nu}\, x\right)^p,$$

im Widerspruch zur Irreduzibilität von $f(x)$. — Wir haben demnach gefunden:

Ein Körper K der Primzahlcharakteristik p ist dann und nur dann vollkommen, wenn mit a stets auch $\sqrt[p]{a}$ in K enthalten ist.

Hiernach und nach Satz 29 [29] sind die Primkörper P_p vollkommene Körper. — Daß nicht jeder Körper vollkommen ist, d. h. daß es sogenannte unvollkommene Körper gibt, zeigt das Beispiel $P_p(x)$; denn dieser Körper hat die Charakteristik p, und das Element x besitzt keine p-te Wurzel in ihm. Wäre nämlich $\left(\frac{f(x)}{g(x)}\right)^p \equiv x$, d. h. $(f(x))^p \equiv x(g(x))^p$ (wobei natürlich $f(x)$, $g(x) \not\equiv 0$ sein müßten), und wären n, m die Grade von $f(x)$, $g(x)$, so folgte nach § 1, B., (3.) [12] $pn = 1 + pm$, d. h. $0 \equiv 1 \bmod. p$, was nicht der Fall ist.

III. Die Körper der Wurzeln algebraischer Gleichungen.

Wir führen in diesem Abschnitt die Konstruktion der Wurzeln eines Polynoms $f(x)$ aus K nach dem bei Satz 50 [42] gegebenen Schema aus, indem wir zunächst eine Erweiterung Σ (Stammkörper) herstellen, in der sich von $f(x)$ ein Linearfaktor abspaltet (§ 8), und von da aus schrittweise zu einer Erweiterung W (Wurzelkörper) aufsteigen, in der $f(x)$ vollständig in Linearfaktoren zerfällt (§ 10). Daneben entwickeln wir, um unsere Untersuchungen in IV über die Struktur dieser Wurzelkörper vorzubereiten, eine allgemeine Theorie der Erweiterungen eines Körpers, bei der deren Entspringen aus bestimmten Polynomen keine Rolle spielt (§§ 7, 9). Zum Abschluß (§ 11) fügen wir eine nur von methodischen und historischen Gesichtspunkten aus interessierende Digression über den sog. Fundamentalsatz der Algebra an.

§ 7. Allgemeine Theorie der Erweiterungen 1. Grundlegende Begriffe und Tatsachen.

In 1, § 4 haben wir die speziellen Erweiterungsbereiche $\mathsf{I}[x_1, \ldots, x_n]$ und $\mathsf{K}(x_1, \ldots, x_n)$ eines Grundbereiches I bzw. K konstruiert und untersucht. Für die jetzt zu gebende Vertiefung und Ausdehnung dieser Entwicklungen beschränken wir uns der Kürze halber auf den Fall eines Grundkörpers K, der im folgenden allein zur Anwendung kommen wird.

A. Adjunktion, einfache und endliche Erweiterungen.

Definition 18. Es sei Λ ein Erweiterungskörper von K und M eine Teilmenge von Λ. Dann heißt der Integritätsbereich aller ganzen rationalen Funktionen über K von je endlich vielen Elementen aus M **der durch Adjunktion von M zu K entstehende Teil-**

integritätsbereich von Λ (Bezeichnung $K[M]$), und der Körper aller rationalen Funktionen über K von je endlich vielen Elementen aus M **der durch Adjunktion von** M **zu** K **entstehende Teilkörper von** Λ (Bezeichnung $K(M)$).

Daß $K[M]$ wirklich ein Teilintegritätsbereich, $K(M)$ ein Teilkörper von Λ ist, folgt aus **1**, Satz 6 [19] und den Eigenschaften der ganzen rationalen bzw. rationalen Funktionen über K. Da ferner unter den ganzen rationalen Funktionen über K speziell die Elemente aus K vorkommen, sind $K[M]$ und $K(M)$ Erweiterungsbereiche von K. Es gilt somit

$$K \leqq K[M] \leqq K(M) \leqq \Lambda.$$

Unter Verwendung des in **1**, Satz 7 [20] eingeführten Begriffs Durchschnitt kann man (mit Steinitz) $K[M]$ und $K(M)$ auch als Durchschnitt aller Integritätsbereiche bzw. Körper zwischen K und Λ erklären, die die Teilmenge M von Λ enthalten.

Wenn auch der Körper Λ in Def. 18 nur die Rolle eines Hilfskörpers spielt, dessen Ersetzung durch irgendeine andere, M enthaltende Erweiterung $\bar{\Lambda}$ von K keine Änderung von $K[M]$ und $K(M)$ bewirkt, der also auf die Ergebnisse der Adjunktion keinerlei Einfluß hat, so ist doch sein Vorhandensein für den Prozeß der Adjunktion unbedingt erforderlich. Wir betonen hinsichtlich des leicht mißzuverstehenden Wortes Adjunktion ausdrücklich, daß die Adjunktion einer Menge M zu K auf die beiden in Def. 18 erklärten Weisen nur dann einen Sinn hat, wenn sie innerhalb einer Erweiterung Λ von K, also sozusagen von oben her, vor sich geht, wenn man also weiß, daß man die Elemente von M untereinander und mit den Elementen von K nach den Körpergesetzen durch die vier elementaren Rechenoperationen miteinander verknüpfen kann. Eine Adjunktion von unten her, d. h. ohne Kenntnis einer M enthaltenden Erweiterung Λ von K ist auf alle Fälle unzulässig. Denn unter alleiniger Voraussetzung der in **1**, § 1 zusammengestellten Körperaxiome über K hat man nicht das mindeste Recht, ohne weiteres die Existenz einer Menge M von Elementen außerhalb K anzunehmen, die man mit den Elementen von K zusammen den vier elementaren Rechenoperationen unterwerfen kann. Man kann also z. B. nicht durch die Definition der Adjunktion die in **1**, § 4 geführten Existenzbeweise für die Bereiche $\mathsf{K}[x_1, \ldots, x_n]$ und $\mathsf{K}(x_1, \ldots, x_n)$ über K umgehen, die ja (trivialerweise) durch Adjunktion von $x_1, \ldots, x_n$ zu K auf die beiden Arten der Def. 18 entstehen, eben weil hierbei der in Def. 18 vorkommende nicht entbehrliche Körper Λ mit $\mathsf{K}(x_1, \ldots, x_n)$ (oder einem noch weiteren Körper) zu identifizieren ist. Entsprechendes gilt auch für den in **1**, § 3 geführten Existenzbeweis des Quotientenkörpers K, der durch Adjunktion aller Quotienten aus Elementen des Integritätsbereiches I entsteht, wobei K die Rolle von Λ hat[1]), sowie für die in den folgenden §§ 8, 10 zu erbringenden Existenzbeweise der Stammkörper und Wurzelkörper.

Über die Abhängigkeit der Adjunktion vom Grundkörper K stellt man ohne weiteres folgende Tatsachen fest, die wir der Kürze halber nur für den später allein gebrauchten Fall der Körperadjunktion $\mathsf{K}(\mathsf{M})$ aussprechen:

Satz 60. Dann und nur dann, wenn M Teilmenge von K ist, ist $\mathsf{K}(\mathsf{M}) = \mathsf{K}$.

Satz 61. Ist $\Lambda \geqq \overline{\mathsf{K}} \geqq \mathsf{K}$ und $\Lambda = \mathsf{K}(\mathsf{M})$, so ist auch $\Lambda = \overline{\mathsf{K}}(\mathsf{M})$.

Satz 62. Ist $\Lambda \geqq \overline{\mathsf{K}} \geqq \mathsf{K}$ und $\Lambda = \overline{\mathsf{K}}(\overline{\mathsf{M}})$, $\overline{\mathsf{K}} = \mathsf{K}(\mathsf{M})$, so ist $\Lambda = \mathsf{K}(\mathsf{M}, \overline{\mathsf{M}})$, wo $(\mathsf{M}, \overline{\mathsf{M}})$ die Vereinigungsmenge von M und $\overline{\mathsf{M}}$ ist.

Nach Satz 62 ist die sukzessive Adjunktion von erst M und dann $\overline{\mathsf{M}}$ gleichbedeutend mit der simultanen Adjunktion von $\mathsf{M}, \overline{\mathsf{M}}$. Unter Verwendung des in **1**, Def. 5 [20] eingeführten Begriffs Kompositum ist übrigens $\mathsf{K}(\mathsf{M}, \overline{\mathsf{M}})$ das Kompositum von $\mathsf{K}(\mathsf{M})$ und $\mathsf{K}(\overline{\mathsf{M}})$, nämlich der engste $\mathsf{K}(\mathsf{M})$ und $\mathsf{K}(\overline{\mathsf{M}})$ enthaltende Teilkörper von Λ.

Wir definieren nunmehr speziell, wieder unter Beschränkung auf die Körperadjunktion:

***Definition 19.** Eine Erweiterung Λ von K heißt **einfach** bzw. **endlich** über K, wenn sie durch Adjunktion eines bzw. endlich vieler ihrer Elemente zu K

[1]) Vgl. die „Vorbemerkungen zum Existenzbeweis" in **1**, §§ 3, 4 [27, 34].

hergeleitet werden kann, wenn sie also aus den rationalen Funktionen über K eines Elements α bzw. endlich vieler Elemente $\alpha_1, \ldots, \alpha_n$[1]) besteht. Jedes solche Element α bzw. Elementsystem $\alpha_1, \ldots, \alpha_n$ aus Λ, für das $\Lambda = \mathsf{K}(\alpha)$ bzw. $\Lambda = \mathsf{K}(\alpha_1, \ldots, \alpha_n)$ ist, heißt dann ein **primitives Element** bzw. **primitives Elementsystem** von Λ bzgl. K.

Speziell ist also der Körper $\mathsf{K}(x)$ der rationalen Funktionen über K von einer Unbestimmten x einfach über K und der Körper $\mathsf{K}(x_1, \ldots, x_n)$ der rationalen Funktionen über K von n Unbestimmten $x_1, \ldots, x_n$ endlich über K. Natürlich besagt Def. 19 nicht etwa, daß jede einfache bzw. endliche Erweiterung von dieser Art ist; denn α bzw. $\alpha_1, \ldots, \alpha_n$ brauchen keine Unbestimmten zu sein. Da uns gerade dieser letztere Fall in der Folge ausschließlich beschäftigen wird, gehen wir nachher unter B. auf das Gegenteil zu Unbestimmte genauer ein.

Wir fügen noch folgende Bemerkungen an, die die in Def. 18 eingeführte Adjunktion, sowie die in Def. 19 eingeführte Einfachheit und Endlichkeit mit der bereits in **1**, Def. 7, Zusatz [24] eingeführten relativen Isomorphie in Beziehung setzen:

Sind die durch Adjunktion entstehenden Erweiterungen $\Lambda = \mathsf{K}(\mathsf{M})$ und $\Lambda' = \mathsf{K}(\mathsf{M}')$ isomorph bzgl. K und sind bei einem Isomorphismus bzgl. K zwischen ihnen die Mengen M und M' einander zugeordnet, so sind durch Angabe der Zuordnungen

$$(1.) \qquad \alpha \longleftrightarrow \alpha', \quad \beta \longleftrightarrow \beta', \ldots \begin{pmatrix} \alpha, \beta, \ldots & \text{aus } \mathsf{M} \\ \alpha', \beta', \ldots & \text{aus } \mathsf{M}' \end{pmatrix}$$

die Zuordnungen für alle übrigen Elemente von Λ und Λ' zwangsläufig bestimmt, nämlich gemäß den Bedingungen für einen Isomorphismus bzgl. K (vgl. **1**, Satz 9 und Zusatz, Def. 7 und Zusatz [23, 24], sowie die angeschlossenen Bemerkungen) zu

[1]) Die in dieser Formulierung gegenüber Def. 18 vorliegende Abweichung ist nur scheinbar, da die rationalen Funktionen über K jedes Teilsystems von $\alpha_1 \ldots, \alpha_n$ unter denen von $\alpha_1, \ldots, \alpha_n$ vorkommen.

$$(2.)\qquad \frac{g(\alpha,\beta,\ldots,\gamma)}{h(\alpha,\beta,\ldots,\gamma)} \longleftrightarrow \frac{g(\alpha',\beta',\ldots,\gamma')}{h(\alpha',\beta',\ldots,\gamma')}\,.$$

Zur Beschreibung des Isomorphismus (2.) genügt es daher vollständig, die Zuordnungen (1.) anzugeben, wovon wir im folgenden häufig Gebrauch machen werden. Zur Vereinfachung der Ausdrucksweise dabei definieren wir:

Definition 20. Sind $\mathsf{\Lambda} = \mathsf{K}(\mathsf{M})$ und $\mathsf{\Lambda}' = \mathsf{K}(\mathsf{M}')$ isomorph bzgl. K und sind bei einem Isomorphismus bzgl. K zwischen ihnen die Mengen M und M' gemäß (1.) einander zugeordnet, so heißt der volle Isomorphismus (2.) **durch die Zuordnungen (1.) erzeugt,** und $\mathsf{\Lambda}$ und $\mathsf{\Lambda}'$ heißen **auf Grund der Zuordnungen (1.)** isomorph bzgl. K.

Sind insbesondere $\mathsf{\Lambda}$ und $\mathsf{\Lambda}'$ einfache bzw. endliche, bzgl. K isomorphe Erweiterungen von K, so läßt sich ein Isomorphismus bzgl. K zwischen ihnen durch eine einzige bzw. endlich viele Zuordnungen

$$\alpha \longleftrightarrow \alpha' \text{ bzw. } \alpha_1 \longleftrightarrow \alpha_1', \ldots, \alpha_r \longleftrightarrow \alpha_r'$$

zweier primitiver Elemente $\alpha;\alpha'$ bzw. zweier primitiver Elementsysteme $\alpha_1,\ldots,\alpha_r;\ \alpha'_1,\ldots,\alpha_r'$ von $\mathsf{\Lambda}$ und $\mathsf{\Lambda}'$ erzeugen. Natürlich braucht aber dann nicht für beliebige primitive α_i und α_i' durch $\alpha_i \longleftrightarrow \alpha_i'$ ein Isomorphismus bzgl. K zwischen $\mathsf{\Lambda}$ und $\mathsf{\Lambda}'$ erzeugt zu werden, sondern nur, wenn die α_i' zu den α_i geeignet bestimmt werden.

B. (Separable) algebraische Elemente, (separable) algebraische Erweiterungen [1]).

***Definition 21.** Ein **Element** α einer Erweiterung $\mathsf{\Lambda}$ von K heißt **(separabel) algebraisch** über K, wenn es Wurzel eines (separablen) Polynoms aus K ist; ist es nicht algebraisch über K, so heißt es **transzendent** über K.

Nach **1**, § 4 (vgl. insbesondere die dortige Erläuterung zu Def. 9 [38]) besagt transzendent über K dasselbe wie Unbestimmte über K, so daß algebraisch über K das Gegenteil zu Un-

[1]) Wenn im folgenden separabel in Klammern beigefügt ist, soll der Text sowohl durchweg ohne diesen als auch durchweg mit diesem Zusatz gelesen werden.

bestimmte über K ist. — Algebraische Elemente (vorläufig allerdings hypothetische) haben uns schon in II beschäftigt.

Satz 63. Ist α (separabel) algebraisch über K, so existiert ein und nur ein irreduzibles Polynom $f(x)$ in K, das α zur Wurzel hat (und dieses ist separabel).

Beweis: a.) Nach Def. 21 ist α Wurzel eines (separablen) Polynoms $\bar{f}(x)$ aus K, nach Satz 45 [39] also mindestens eines der (separablen — Def. 17, Zusatz [48]) irreduziblen Faktoren von $\bar{f}(x)$ in K.

b.) Nach Satz 52 [43] kann α nicht Wurzel zweier verschiedener irreduzibler Polynome aus K sein.

Definition 22. Das Polynom $f(x)$ aus Satz 63 heißt **das zu α gehörige irreduzible Polynom** aus K, sein Grad n auch der **Grad von α** über K (Bezeichnung: $n = [\alpha : \mathsf{K}]$).

Aus Satz 51 [43] ergibt sich ohne weiteres:

Satz 64. Dann und nur dann, wenn α Element aus K ist, ist $[\alpha : \mathsf{K}] = 1$.

Ferner gilt:

Satz 65. Ist $\Lambda \geqq \overline{\mathsf{K}} \geqq \mathsf{K}$ und das Element α aus Λ (separabel) algebraisch über K, so ist α auch (separabel) algebraisch über $\overline{\mathsf{K}}$ und das zugehörige irreduzible Polynom aus $\overline{\mathsf{K}}$ Teiler des zugehörigen irreduziblen Polynoms aus K, also speziell

$$[\alpha : \overline{\mathsf{K}}] \leqq [\alpha : \mathsf{K}].$$

Beweis: Die Behauptungen ohne „separabel“ ergeben sich ohne weiteres aus Satz 53 [43]. Ist zudem α separabel über K, so ist es nach Satz 63, 58 [47] nur einfache Wurzel des zugehörigen irreduziblen Polynoms in K, also erst recht desjenigen in $\overline{\mathsf{K}}$, und daher nach Satz 59 [48], Def. 21 separabel auch über $\overline{\mathsf{K}}$.

***Definition 23.** Eine **Erweiterung** $\mathsf{\Lambda}$ von K heißt **(separabel) algebraisch** über K, wenn jedes ihrer Elemente (separabel) algebraisch über K ist; ist sie nicht algebraisch über K, so heißt sie **transzenpent** über K.

Die einfache Erweiterung $\mathsf{K}(x)$ ist transzendent über K, weil nach obigem die Unbestimmte x transzendent über K ist. Entsprechendes gilt für die endliche Erweiterung $\mathsf{K}(x_1, \ldots, x_n)$. Algebraische Erweiterungen werden wir im folgenden ausführlich kennenlernen.

Über die Abhängigkeit der Def. 23 von den Körpern K und $\mathsf{\Lambda}$ haben wir, analog zu Satz 61 [52], 65, nach Satz 65 unmittelbar:

Satz 66. Ist $\mathsf{\Lambda} \geqq \overline{\mathsf{K}} \geqq \mathsf{K}$ und $\mathsf{\Lambda}$ über K (separabel) algebraisch, so ist auch $\mathsf{\Lambda}$ über $\overline{\mathsf{K}}$ und natürlich $\overline{\mathsf{K}}$ über K (separabel) algebraisch.

Die Umkehrung (analog zu Satz 62 [52]) können wir erst später (Satz 86 [72], Satz 92 [83]) beweisen, nachdem wir sie für die anschließend unter C. definierte, spezielle Klasse algebraischer Erweiterungen bewiesen (Satz 71 [59]) und diese genauer kennen gelernt haben werden (Satz 84 [72], Satz 91 [83]).

C. Erweiterungen endlichen Grades.

Wir setzen zunächst in Analogie zu den in **1**, Def. 23, 24 [69] eingeführten Begriffen fest:

***Definition 24.** 1.) n Elemente $\alpha_1, \ldots, \alpha_n$ einer Erweiterung $\mathsf{\Lambda}$ von K heißen **linear abhängig** bzgl. K, wenn eine lineare homogene Relation

$$\sum_{k=1}^{n} a_k \alpha_k = 0$$

mit Koeffizienten a_k aus K besteht, die nicht sämtlich 0 sind, andernfalls **linear unabhängig** bzgl. K.

2.) Ein Element α aus $\mathsf{\Lambda}$ heißt **linear abhängig von** $\alpha_1, \ldots, \alpha_n$ bzgl. K, wenn es eine lineare homogene Darstellung

$$\alpha = \sum_{k=1}^{n} a_k \alpha_k$$

mit Koeffizienten a_k aus K besitzt, andernfalls **linear unabhängig von** $\alpha_1, \ldots, \alpha_n$ bzgl. K.

Unter Hinweis auf die Beweise in **1**, § 10 stellen wir fest, daß sich die dortigen Sätze 38, 39, 41, 42 [70, 71] sinngemäß auf die in Def. 24 erklärten Begriffe übertragen, wenn man für die dortigen Linearformen (Vektoren) in K Elemente einer Erweiterung Λ von K setzt.

Nunmehr definieren wir die uns interessierende, spezielle Klasse algebraischer Erweiterungen folgendermaßen:

***Definition 25.** Eine Erweiterung Λ von K heißt **von endlichem Grade** über K, wenn ein endliches Maximalsystem bzgl. K linear unabhängiger Elemente von Λ existiert. Jedes solche Maximalsystem $\alpha_1, \ldots, \alpha_n$ heißt eine **Basis von** Λ bzgl. K und die eindeutig bestimmte Anzahl n der **Grad von** Λ über K (Bezeichnung: $n = [\Lambda : \mathsf{K}]$).

Die Bezeichnung Basis soll ausdrücken, daß dann jedes Element α aus Λ von $\alpha_1, \ldots, \alpha_n$ linear abhängig ist, also eine Basisdarstellung

$$\alpha = a_1 \alpha_1 + \cdots + a_n \alpha_n$$

mit Koeffizienten $a_1, \ldots, a_n$ aus K besitzt. Nach **1**, Satz 41 [71] ist diese Basisdarstellung eindeutig. Umgekehrt folgt nach diesem Satz aus der Eindeutigkeit der Basisdarstellung durch $\alpha_1, \ldots, \alpha_n$ deren lineare Unabhängigkeit und aus der Möglichkeit für jedes α deren Maximaleigenschaft. Daher gilt:

Zusatz zu Definition 25. Die Forderung von Def. 25 läßt sich auch dahin aussprechen, daß alle Elemente von Λ eine eindeutige Basisdarstellung durch endlich viele solche besitzen sollen.

Der folgende Satz zeigt, was aus Def. 25 zunächst nicht ersichtlich ist, daß die Erweiterungen endlichen Grades eine spezielle Klasse algebraischer Erweiterungen sind und noch etwas mehr:

Satz 67. Ist Λ von endlichem Grade über K, so ist Λ algebraisch über K. Genauer:

Ist $[\Lambda : \mathsf{K}] = n$, so ist jedes Element α aus Λ algebraisch über K von einem Grade $[\alpha : \mathsf{K}] \leqq n$.

Beweis: Dann sind die $n+1$ Elemente $\alpha^0 = e$, $\alpha^1 = \alpha$, $\alpha^2, \ldots, \alpha^n$ linear abhängig (Def. 25). Es besteht also eine Relation

$$a_0 + a_1\alpha + \cdots + a_n\alpha^n = 0$$

mit Koeffizienten a_k aus K, die nicht sämtlich 0 sind (Def. 24). Diese besagt, daß α Wurzel eines Polynoms $\bar{f}(x)$ aus K von höchstens n-tem Grade ist. Da dann das zu α gehörige irreduzible Polynom $f(x)$ aus K als Teiler von $\bar{f}(x)$ ebenfalls höchstens den Grad n hat, ist α algebraisch über K von einem Grade $\leqq n$ (Def. 21, 22 [54, 55]).

Eine der Einschränkungen, die den algebraischen Erweiterungen Λ von K durch die Forderung, von endlichem Grade über K zu sein, auferlegt wird, besteht hiernach darin, daß es in Λ keine Elemente beliebig hohen Grades über K gibt. Diese Einschränkung ist aber zur Endlichkeit des Grades von Λ im allgemeinen nicht hinreichend[1]) (vgl. jedoch den späteren Satz 91, Zusatz [83]). Daß es überhaupt algebraische Erweiterungen gibt, die nicht von endlichem Grade sind, zeigt der Körper aller algebraischen Zahlen über P, in dem ja Elemente beliebig hohen Grades vorkommen (siehe dazu den späteren Satz 123 [137]).

Wir beweisen ferner:

Satz 68. Ist Λ von endlichem Grade über K, so ist Λ endlich über K.

Beweis: Ist $\alpha_1, \ldots, \alpha_n$ eine Basis von Λ, so gehört vermöge der Basisdarstellung jedes Element aus Λ zu dem Integritätsbereich $\mathsf{K}[\alpha_1, \ldots, \alpha_n]$. Da nun andererseits

$$\mathsf{K} \leqq \mathsf{K}[\alpha_1, \ldots, \alpha_n] \leqq \mathsf{K}(\alpha_1, \ldots, \alpha_n) \leqq \Lambda$$

ist, folgt $\Lambda = \mathsf{K}[\alpha_1, \ldots, \alpha_n] = \mathsf{K}(\alpha_1, \ldots, \alpha_n)$, also die Endlichkeit von Λ über K.

In den weiteren Sätzen stellen wir fest, wie die in Def. 25 erklärten Begriffe von den Körpern K und Λ abhängen:

Satz 69. Dann und nur dann, wenn $\Lambda = \mathsf{K}$ ist, ist $[\Lambda : \mathsf{K}] = 1$.

Beweis: a.) Ist $\Lambda = \mathsf{K}$, so ist das allein aus e bestehende

[1]) Gegenbeispiele ergeben sich aus Steinitz, l. c. (1, Lit.-Verz. I).

System Basis von $\mathsf{\Lambda}$ bzgl. K, weil ja dann jedes a aus $\mathsf{\Lambda}$ die eindeutige Basisdarstellung $a = a \cdot e$ besitzt. Also ist dann $[\mathsf{\Lambda} : \mathsf{K}] = 1$.

b.) Ist $[\mathsf{\Lambda} : \mathsf{K}] = 1$, so ist nach Satz 67 $[\alpha : \mathsf{K}] \leqq 1$ also $= 1$ für jedes α aus $\mathsf{\Lambda}$, also nach Satz 64 [55] jedes α aus $\mathsf{\Lambda}$ Element von K, d. h. $\mathsf{\Lambda} = \mathsf{K}$.

Satz 70. Ist $\mathsf{\Lambda} \geqq \overline{\mathsf{K}} \geqq \mathsf{K}$ und $\mathsf{\Lambda}$ über K von endlichem Grade, so ist auch $\mathsf{\Lambda}$ über $\overline{\mathsf{K}}$ und $\overline{\mathsf{K}}$ über K von endlichem Grade, und es gilt $[\mathsf{\Lambda} : \overline{\mathsf{K}}] \leqq [\mathsf{\Lambda} : \mathsf{K}]$, $[\overline{\mathsf{K}} : \mathsf{K}] \leqq [\mathsf{\Lambda} : \mathsf{K}]$.

Beweis: Ist $[\mathsf{\Lambda} : \mathsf{K}] = n$, so sind mehr als n Elemente von $\mathsf{\Lambda}$ linear abhängig bzgl. K, also a fortiori bzgl. $\overline{\mathsf{K}}$, und mehr als n Elemente von $\overline{\mathsf{K}}$ als solche von $\mathsf{\Lambda}$ linear abhängig bzgl. K. Daher existiert beidemal ein endliches Maximalsystem von höchstens n linear unabhängigen Elementen.

Von besonderer Wichtigkeit für die Folge ist die nachstehende Umkehrung von Satz 70, die gleichzeitig die dortigen Gradrelationen präzisiert:

Satz 71. Ist $\mathsf{\Lambda} \geqq \overline{\mathsf{K}} \geqq \mathsf{K}$ und $\mathsf{\Lambda}$ über $\overline{\mathsf{K}}$ sowie $\overline{\mathsf{K}}$ über K von endlichem Grade, so ist auch $\mathsf{\Lambda}$ über K von endlichem Grade und $[\mathsf{\Lambda} : \mathsf{K}] = [\mathsf{\Lambda} : \overline{\mathsf{K}}] \cdot [\overline{\mathsf{K}} : \mathsf{K}]$.

Beweis: Ist $[\mathsf{\Lambda} : \overline{\mathsf{K}}] = m$ und $\alpha_1, \ldots, \alpha_m$ eine Basis von $\mathsf{\Lambda}$ bzgl. $\overline{\mathsf{K}}$, ferner $[\overline{\mathsf{K}} : \mathsf{K}] = j$ und $\overline{\alpha}_1, \ldots, \overline{\alpha}_j$ eine Basis von $\overline{\mathsf{K}}$ bzgl. K, so zeigen wir, daß die mj Elemente $\alpha_i \overline{\alpha}_k$ $(i = 1, \ldots, m; k = 1, \ldots, j)$ eine Basis von $\mathsf{\Lambda}$ bzgl. K bilden.

a.) Da jedes α aus $\mathsf{\Lambda}$ eine Darstellung

$$\alpha = \sum_{i=1}^{m} \overline{a}_i \alpha_i$$

mit $\overline{a}_i$ aus $\overline{\mathsf{K}}$ hat und diese $\overline{a}_i$ aus $\overline{\mathsf{K}}$ ihrerseits Darstellungen

$$\overline{a}_i = \sum_{k=1} a_{ik} \overline{\alpha}_k \qquad (i = 1, \ldots, m)$$

mit a_{ik} aus K haben, so hat jedes α aus Λ eine Darstellung

$$\alpha = \sum_{i=1}^{m} \sum_{k=1}^{j} a_{ik} \alpha_i \overline{\alpha}_k .$$

Somit ist jedes α aus Λ von den $\alpha_i \overline{\alpha}_k$ linear abhängig bzgl. K.

b.) Aus

$$\sum_{i=1}^{m} \sum_{k=1}^{j} a_{ik} \alpha_i \overline{\alpha}_k = 0$$

folgt zunächst wegen der linearen Unabhängigkeit der α_i bzgl. $\overline{\mathsf{K}}$, daß

$$\sum_{k=1}^{j} a_{ik} \overline{\alpha}_k = 0 \qquad (i = 1, \ldots, m)$$

ist, und daraus wegen der linearen Unabhängigkeit der $\overline{\alpha}_k$ bzgl. K, daß

$$a_{ik} = 0 \;\; (i = 1, \ldots, m;\; k = 1, \ldots, j)$$

ist. Somit sind die $\alpha_i \overline{\alpha}_k$ linear unabhängig bzgl. K.

Aus a.) und b.) folgt, daß die mj Elemente $\alpha_i \overline{\alpha}_k$ ein Maximalsystem bzgl. K linear unabhängiger Elemente von Λ bilden, was die Behauptung ergibt.

Speziell gilt nach Satz 71 unter Berücksichtigung von Satz 69:

Satz 72. Sind Λ und $\overline{\Lambda}$ von endlichem Grade über K und ist $\Lambda \leqq \overline{\Lambda}$, so ist dann und nur dann $\Lambda = \overline{\Lambda}$, wenn $[\Lambda : \mathsf{K}] = [\overline{\Lambda} : \mathsf{K}]$ ist.

D. Konjugierte Erweiterungen, konjugierte Elemente.

Wie in **1**, bei Def. 7, Zusatz [24] ausgeführt wurde, sind zwar bzgl. K isomorphe Erweiterungen Λ_1 und Λ_2 von K aus nicht zu unterscheiden, doch kann eine solche Unterscheidung von einer sie enthaltenden Erweiterung Λ aus notwendig werden. Wir definieren in dieser Hinsicht die folgende Äquivalenzrelation:

***Definition 26.** Zwei bzgl. K isomorphe Körper Λ_1 und Λ_2 zwischen K und Λ heißen auch **konjugiert**

bzgl. K. Bei einem Isomorphismus bzgl. K zugeordnete Elemente α_1 und α_2 heißen dann ebenfalls **konjugiert** bzgl. K.

Analog wie in Def. 18 [50] spielt auch hier Λ nur die Rolle eines Hilfskörpers, der zwar die Relation Λ_1 und Λ_2 konjugiert ermöglicht, aber ohne sie zu beeinflussen durch irgendeine Λ_1 und Λ_2 enthaltende Erweiterung $\overline{\Lambda}$ von K ersetzt werden kann. Ist ohne Bezugnahme auf einen solchen Hilfskörper Λ von bzgl. K konjugierten Körpern Λ_1, Λ_2 die Rede, so soll damit insbesondere stets gesagt sein, daß überhaupt eine Erweiterung Λ existiert, die sowohl Λ_1 als auch Λ_2 enthält. Als Beispiel wirklich verschiedener, konjugierter Erweiterungen von K seien etwa die n in $K(x_1, \ldots, x_n)$ enthaltenen Körper $K(x_1), \ldots, K(x_n)$ genannt, in denen z. B. $x_1, \ldots, x_n$, allgemein $\frac{g(x_1)}{h(x_1)}, \ldots, \frac{g(x_n)}{h(x_n)}$ konjugierte Elemente sind.

Für konjugierte, über K algebraische Elemente gilt nach den Ausführungen zu **1**, Def. 7, Zusatz [24] ersichtlich die folgende Tatsache:

Satz 73. Ist α ein über K algebraisches Element einer Erweiterung Λ von K und $f(x)$ das zugehörige irreduzible Polynom aus K, so sind alle zu α konjugierten Elemente aus Λ ebenfalls Wurzeln von $f(x)$.

§ 8. Stammkörper.

Wir führen in diesem Paragraphen den ersten Schritt zur Konstruktion der Wurzeln eines Polynoms $f(x)$ aus K aus, indem wir durch tatsächliche Konstruktion die Existenz einer speziellen Erweiterung von K beweisen, in der sich von $f(x)$ ein Linearfaktor abspaltet. Überdies werden wir eine Übersicht über alle solchen Erweiterungen erhalten. Methodisch werden unsere Entwicklungen ganz analog zu den in **1**, § 4 geführten Existenz- und Eindeutigkeitsbeweisen sein [1]), nur daß wir hier die Hauptarbeit schon im voraus geleistet haben,

[1]) Der Existenz- und Eindeutigkeitsbeweis für $K(x)$ in **1**, § 4 ist in der Tat nichts anderes als der für $f(x) \equiv 0$ geführte Beweis dieses Paragraphen.

indem wir in § 2 den Restklassenkörper $\mathsf{K}(x, \text{mod. } f(x))$ für ein irreduzibles Polynom $f(x)$ konstruierten. Darauf stützt sich nämlich unser jetziger Existenzbeweis.

Nach Satz 45 [39] dürfen wir ohne Einschränkung $f(x)$ als irreduzibel voraussetzen. Unser Hauptsatz lautet dann:

Satz 74. Es sei $f(x)$ ein irreduzibles Polynom vom Grade n aus K. Dann existiert eine Erweiterung Σ von K mit den Eigenschaften:

(I.) $f(x)$ hat in Σ eine Wurzel α, also eine Zerlegung $f(x) \equiv (x - \alpha)\,\varphi(x)$.

(II.) Σ ist einfach über K und α primitives Element von Σ, d. h. es ist $\Sigma = \mathsf{K}(\alpha)$.

(III.) Σ ist algebraisch von endlichem Grade über K; es ist nämlich $\alpha^0, \alpha^1, \ldots, \alpha^{n-1}$ eine Basis von Σ, also $[\Sigma : \mathsf{K}] = n$. Hiernach ist auch $\Sigma = \mathsf{K}[\alpha]$.

Ist Σ^* irgendeine (I.), (II.) genügende Erweiterung von K und α^* die in (I.), (II.) vorliegende Wurzel von $f(x)$, so ist Σ^* zu Σ auf Grund der Zuordnung $\alpha^* \longleftrightarrow \alpha$ isomorph bzgl. K (und hat daher auch die Eigenschaft (III.)). Der Erweiterungstypus von K ist also durch (I.), (II.) eindeutig bestimmt.

a.) Existenzbeweis.

Der Restklassenkörper $\mathsf{K}(x, \text{mod. } f(x))$ enthält in Gestalt der speziellen, durch Elemente a aus K gelieferten Restklassen $\{a\}$ einen Teilbereich K', der vermöge der Zuordnung

$$\{a\} \longleftrightarrow a \tag{1.}$$

ein zu K isomorpher Körper ist.

Da nämlich, weil das Polynom $f(x)$ keine Einheit ist, $a \equiv b$ mod. $f(x)$ mit $a = b$ gleichbedeutend ist, ist (1.) eine eineindeutige Zuordnung zwischen K' und K, die nach der Definition des Rechnens mit Restklassen auch die Isomorphiebedingungen erfüllt.

Analog wie in **1**, Bew. zu Satz 10, d) [29] und 11, d) [35] können wir daher, indem wir die Elemente des Teilkörpers K'

durch die ihnen nach (1.) zugeordneten von K unter Beibehaltung aller Verknüpfungsbeziehungen ersetzen, einen zu $\mathsf{K}(x, \text{mod.}\, f(x))$ isomorphen Körper Σ bilden, der K selbst als Teilkörper enthält. Dieser Körper Σ hat dann, wie wir jetzt zeigen werden, die Eigenschaften (I.)—(III.).

(I.) Betrachten wir die Normaldarstellung

$$f(x) \equiv x^n + a_1 x^{n-1} + \cdots + a_n$$

als Relation zwischen den Elementen $f(x)$, x, $a_1, \ldots, a_n$ aus $\mathsf{K}[x]$, so besagt sie nach **1**, Satz 8 [22] das Bestehen der entsprechenden Relation

$$\{f(x)\} = \{x\}^n + \{a_1\}\{x\}^{n-1} + \cdots + \{a_n\}$$

zwischen den zugehörigen Restklassen mod. $f(x)$, also Elementen aus $\mathsf{K}(x, \text{mod.}\, f(x))$. Da nun $f(x) \equiv 0 \text{ mod. } f(x)$, also $\{f(x)\}$ die Null von $\mathsf{K}(x, \text{mod.}\, f(x))$ ist, gilt in $\mathsf{K}(x, \text{mod.}\, f(x))$

$$\{x\}^n + \{a_1\}\{x\}^{n-1} + \cdots + \{a_n\} = 0.$$

Führen wir dann in dieser Relation den Übergang (1.) von $\mathsf{K}(x, \text{mod.}\, f(x))$ zu Σ aus und geben dabei dem nicht zu K' gehörigen, also beizubehaltenden Element $\{x\}$ die neue Bezeichnung α, so folgt in Σ die Relation

$$\alpha^n + a_1\alpha^{n-1} + \cdots + a_n = 0, \text{ d. h. } f(\alpha) = 0.$$

Es ist also das Element $\alpha = \{x\}$ aus Σ Wurzel von $f(x)$.

Es kam uns bei diesem Beweis, durch den die vorher nicht vorhandene Wurzel α geschaffen wird, auf größtmögliche begriffliche Schärfe an. Kürzer, aber weniger präzis, ließe sich unser Gedankengang so aussprechen: Weil die Restklasse x mod. $f(x)$ der Relation $f(x) \equiv 0$ mod. $f(x)$ genügt, ist sie Wurzel von $f(x)$ in $\mathsf{K}(x, \text{mod.}\, f(x))$[1].

(II.) Sei β ein nicht zu K gehöriges Element von Σ, das somit nach Konstruktion von Σ eine Restklasse mod. $f(x)$ ist. Ist $h(x)$ irgendein Element aus dieser Restklasse, also $\beta = \{h(x)\}$, so folgt durch Zurückgehen auf die Normaldar-

[1]) Man wende gegen den obigen Beweis nicht ein, daß er „trivial" sei und „gar nichts Neues" liefere. Denn dann muß man denselben Einwand auch gegen die Konstruktion der ganzen Zahlen aus den natürlichen und der rationalen aus den ganzen erheben.

stellung

$$h(x) \equiv \sum_{k=0}^{\infty} c_k\, x^k$$

in $\mathsf{K}[x]$, und die daraus folgende Relation

$$\{h(x)\} = \sum_{k=0}^{\infty} \{c_k\}\, \{x_k\}^k$$

in $\mathsf{K}(x, \text{mod.}\ f(x))$, das Bestehen der Relation

$$\beta = \{h(x)\} = \sum_{k=0}^{\infty} c_k \{x\}^k = \sum_{k=0}^{\infty} c_k\, \alpha^k = h(\alpha)$$

in Σ. Falls β zu K gehört, gilt natürlich Entsprechendes (mit einem $h(x)$ vom Grade 0). Hiernach erschöpft schon der in Σ enthaltene Teilintegritätsbereich $\mathsf{K}[\alpha]$, umsomehr also der ebenfalls in Σ enthaltene Teilkörper $\mathsf{K}(\alpha)$ alle Elemente β von Σ (Def. 19 [52]), d. h. es ist $\Sigma = \mathsf{K}[\alpha] = \mathsf{K}(\alpha)$.

(III.) Durch Benutzung des reduzierten Restsystems von Satz 27 [26] folgt aus dem Beweis für (II.), daß man in den Darstellungen $\beta = h(\alpha)$ die $h(x)$ eindeutig in der Form

$$c_0 + c_1 x + \cdots + c_{n-1}\, x^{n-1}$$

annehmen darf, daß also alle β aus Σ eindeutig linear-homogen durch $\alpha^0, \alpha^1, \ldots, \alpha^{n-1}$ mit Koeffizienten aus K darstellbar sind. Somit ist $\alpha^0, \alpha^1, \ldots, \alpha^{n-1}$ eine Basis von Σ (Def. 25, Zusatz [57]) und daher $[\Sigma : \mathsf{K}] = n$.

b.) Eindeutigkeitsbeweis.

Es sei Σ^* eine (I.), (II.) genügende Erweiterung von K und α^* die in (I.), (II.) vorliegende Wurzel von $f(x)$. Wir zeigen dann zunächst, daß der in Σ^* enthaltene Teilintegritätsbereich $\mathsf{K}[\alpha^*]$ zu $\mathsf{K}\ (x, \text{mod.}\ f(x))$ auf Grund der Zuordnung

(2.) $\qquad \beta^* \longleftrightarrow \{h(x)\}$, wenn $\beta^* = h(\alpha^*)$,

isomorph ist. Es sind nämlich erfüllt: **1**, § 2, (δ.), (δ'.) [17] nach Def. 19 [52]; **1**, § 2, (ε.), (ε'.) [17], weil aus $\beta_1^* = \beta_2^*$, also $h_1(\alpha^*) = h_2(\alpha^*)$ nach Satz 53 [43] wegen $f(\alpha^*) = 0$ folgt $f(x) \mid h_1(x) - h_2(x)$, d. h. $h_1(x) \equiv h_2(x)$ mod. $f(x)$, also $\{h_1(x)\} = \{h_2(x)\}$, und weil diese Schlußweise auch in umgekehrter Richtung ausführbar ist; **1**, § 2, (3.), (4.) [23] nach den Rechenregeln für Restklassen.

Somit ist, da $\mathsf{K}\,(x, \text{mod.}\, f(x))$ ein Körper ist, auch der Integritätsbereich $\mathsf{K}[\alpha^*]$ ein Körper und daher mit seinem Quotientenkörper $\mathsf{K}\,(\alpha^*) = \Sigma^*$ identisch. Es stellt also (2.) einen Isomorphismus zwischen Σ^* und $\mathsf{K}\,(x, \text{mod.}\, f(x))$ dar. Da nun nach a.) (oder wegen der Anwendbarkeit des eben Gezeigten auf Σ für Σ^*) die Zuordnung

(3.) $$\beta \longleftrightarrow \{h(x)\}, \text{ wenn } \beta = h(\alpha)\,,$$

ein Isomorphismus zwischen Σ und $\mathsf{K}\,(x, \text{mod.}\, f(x))$ ist, ist Σ^* zu Σ isomorph bzgl. K auf Grund der durch Kombination von (2.) und (3.) entstehenden Zuordnung

$$\beta^* \longleftrightarrow \beta, \text{ wenn } \beta^* = h(\alpha^*),\ \beta = h(\alpha)\,,$$

bei der in der Tat die Elemente von K je sich selbst zugeordnet sind, und die durch die im Satz genannte Zuordnung $\alpha^* \longleftrightarrow \alpha$ erzeugt wird.

Damit ist Satz 74 bewiesen. Wie wir später sehen werden, kann eine Erweiterung von K verschiedene Körper Σ mit den Eigenschaften (I.), (II.) von Satz 74 enthalten. Daher definieren wir hier, abweichend gegenüber der den bestimmten Artikel verwendenden Formulierung der Def. 8—10 in **1** [31, 38, 39]:

***Definition 27.** Jede Erweiterung Σ von K mit den Eigenschaften (I.), (II.) und daher auch (III.) von Satz 74 heißt ein **Stammkörper** für $f(x)$ über K.

Aus Satz 74 ergibt sich dann:

Satz 75. Hat das irreduzible Polynom $f(x)$ aus K in einer Erweiterung Λ von K eine Wurzel α, so enthält Λ einen Stammkörper für $f(x)$, nämlich $\mathsf{K}(\alpha)$.

Beweis: $\mathsf{K}(\alpha)$ hat die Eigenschaften (I.), (II.) von Satz 74.

Hiernach übersehen wir die Gesamtheit aller Erweiterungen von K, in denen ein irreduzibles $f(x)$ aus K eine Wurzel hat, jedenfalls soweit nur der Erweiterungstypus in Frage kommt:

Abgesehen von bzgl. K isomorphen sind es nämlich alle und nur die Erweiterungen eines Stammkörpers für $f(x)$. Die Stammkörper selbst repräsentieren also den engsten derartigen Erweiterungstypus.

§ 9. Allgemeine Theorie der Erweiterungen 2. Einfache und endliche algebraische Erweiterungen.

Wir leiten in diesem Paragraphen mittels der Ergebnisse des § 8 einige wichtige Beziehungen zwischen den in § 7 eingeführten allgemeinen Begriffen her.

A. Einfache algebraische Erweiterungen.

Im ersten Teil des Satzes 74 [62] wurde festgestellt, daß die Stammkörper über K einfach und algebraisch von endlichem Grade sind. Umgekehrt ergibt sich nun aus dem zweiten Teil dieses Satzes unmittelbar:

Satz 76. Ist Λ einfach über K und ist ein primitives Element α von Λ algebraisch vom Grade n über K, so ist $\Lambda = K(\alpha)$ Stammkörper für das zu α gehörige irreduzible Polynom n-ten Grades $f(x)$ aus K. Es ist also dann Λ algebraisch von endlichem Grade, nämlich vom Grade n über K.

Insbesondere gilt hiernach folgende Relation zwischen den beiden in Def. 22 [55] und Def. 25 [57] unabhängig voneinander erklärten Graden:

Satz 77. Der Grad eines algebraischen Elements α über K ist gleich dem Grad des zugehörigen Stammkörpers $K(\alpha)$ über K:

$$[\alpha : K] = [K(\alpha) : K].$$

Die Aussage von Satz 76 läßt sich dahingehend verschärfen, daß auch die Separabilität einbezogen wird. Dazu leiten wir zunächst das folgende Kriterium für die Separabilität her:

Satz 78. Ist K von der Charakteristik p, so ist ein über K algebraisches Element α dann und nur dann separabel über K, wenn $K(\alpha^p) = K(\alpha)$ ist.

Beweis: a.) Es sei α separabel. Ist dann

$$f(x) \equiv x^n + a_1 x^{n-1} + \cdots + a_n$$

das zu α gehörige, nach Satz 63 [55] separable, irreduzible Polynom, so ist

$$f_1(x) \equiv x^n + a_1^p x^{n-1} + \cdots + a_n^p$$

das zu α^p gehörige irreduzible Polynom.

Erstens ist nämlich nach Satz 44 [37] $f_1(\alpha^p) = f(\alpha)^p = 0$. Zweitens ist $f_1(x)$ irreduzibel; denn aus $h(x) \mid f_1(x)$ folgt $h(x^p) | f_1(x^p) \equiv f(x)^p$ (Satz 44), wegen der Irreduzibilität von $f(x)$ also $h(x^p) \equiv f(x)^r$ mit $0 \leqq r \leqq p$, durch beiderseitige Ableitungsbildung weiter $0 \equiv r f'(x)$ (Satz 57 [46]), und daraus $r = 0$ oder p — weil $f'(x) \not\equiv 0$ ist (Def. 17 [47]) — also $h(x^p) \equiv f(x)^0 \equiv e$ oder $h(x^p) \equiv f(x)^p \equiv f_1(x^p)$, und somit $h(x) \equiv e$ oder $h(x) \equiv f_1(x)$.

Hiernach ist

$$[\alpha : K] = n = [\alpha^p : K],$$

also nach Satz 77

$$[K(\alpha) : K] = [K(\alpha^p) : K],$$

und daher nach Satz 72 [60]

$$K(\alpha) = K(\alpha^p).$$

b.) Es sei α inseparabel. Dann ist das zu α gehörige irreduzible Polynom inseparabel (Satz 63 [55]), also von der Gestalt $f(x) \equiv f_0(x^p)$ (Def. 17 [47]). Hierbei ist $f_0(x)$ das zu α^p gehörige irreduzible Polynom.

Denn erstens ist $f_0(\alpha^p) = f(\alpha) = 0$. Zweitens ist $f_0(x)$ irreduzibel, weil aus $h(x) \mid f_0(x)$ folgt $h(x^p) \mid f_0(x^p) \equiv f(x)$ und $f(x)$ irreduzibel vorausgesetzt ist.

Hiernach ist

$$[\alpha : K] = p[\alpha^p : K] > [\alpha^p : K],$$

also nach Satz 77

$$[K(\alpha) : K] > [K(\alpha^p) : K],$$

und somit nach Satz 72 [60]

$$\mathsf{K}(\alpha) > \mathsf{K}(\alpha^p).$$

Wenn $\mathsf{K}(\alpha) = \mathsf{K}(\alpha^p)$ ist, muß daher α separabel sein.

Wir beweisen nunmehr die angekündigte Verschärfung von Satz 76:

Satz 79. Ist K von der Charakteristik p, und wird in Satz 76 α separabel über K vorausgesetzt, so ist auch $\Lambda = \mathsf{K}(\alpha)$ separabel über K.

Beweis: Gemäß Def. 23 [56] ist zu zeigen, daß jedes Element β aus $\mathsf{K}(\alpha)$ separabel ist. Nach dem Kriterium von Satz 78 kann das gezeigt werden, indem aus der nach der Voraussetzung richtigen Relation $\mathsf{K}(\alpha^p) = \mathsf{K}(\alpha)$ die entsprechende Relation $\mathsf{K}(\beta^p) = \mathsf{K}(\beta)$ gefolgert wird.

Sei dazu

$$[\mathsf{K}(\alpha):\mathsf{K}(\beta)] = m, \qquad [\mathsf{K}(\beta):\mathsf{K}] = j,$$
$$[\mathsf{K}(\alpha):\mathsf{K}(\beta^p)] = [\mathsf{K}(\alpha^p):\mathsf{K}(\beta^p)] = m', \qquad [\mathsf{K}(\beta^p):\mathsf{K}] = j'$$

gesetzt. Dann ist nach Satz 71 [59]

$$mj = m'j'$$

und nach Satz 70 [59]

$$m \leqq m', \qquad j' \leqq j.$$

Ist nun

$$\varphi(x) \equiv x^m + \alpha_1 x^{m-1} + \cdots + \alpha_m$$

das zu α gehörige irreduzible Polynom in $\mathsf{K}(\beta)$ (vgl. Satz 77), dessen Koeffizienten gemäß Satz 74, (III.) [62] und Satz 76 in der Form

$$\alpha_k = \sum_{i=0}^{j-1} a_{ik}\beta^i \qquad (k = 0, \ldots, m-1)$$

darstellbar sind, so folgt aus der Relation $\varphi(\alpha) = 0$ durch Potenzieren mit p nach Satz 44 [37], daß α^p Wurzel des Polynoms

$$\varphi_1(x) \equiv x^m + \alpha_1' x^{m-1} + \cdots + \alpha_m'$$

vom Grade m mit den Koeffizienten

$$\alpha_k' = \sum_{i=0}^{j-1} a_{ik}^p \beta^{pi} \qquad (k = 0, \ldots, m-1)$$

aus $\mathsf{K}(\beta^p)$ ist. Das zu α^p gehörige irreduzible Polynom in $\mathsf{K}(\beta^p)$ ist dann nach Satz 53 [43] ein Teiler von $\varphi_1(x)$. Daraus folgt für seinen Grad (vgl. Satz 77)

$$m' \leqq m\,.$$

Nach den obigen Relationen ergibt sich damit

$$m' = m, \text{ also } j' = j\,,$$

d. h. nach Satz 72 [60] in der Tat $\mathsf{K}(\beta^p) = \mathsf{K}(\beta)$.

Nach Satz 76 sind für eine einfache Erweiterung Λ von K nur die beiden folgenden Fälle möglich: Entweder liegen die Verhältnisse von Satz 76 vor. Oder aber jedes primitive Element α von Λ, also auch Λ selbst, ist transzendent über K; dann hat jedes solche α den Charakter einer Unbestimmten über K (siehe bei Def. 21 [54]), und $\Lambda = \mathsf{K}(\alpha)$ ist vom Erweiterungstypus des Körpers $\mathsf{K}(x)$ der rationalen Funktionen einer Unbestimmten x über K [1]). Satz 76 besagt hiernach (siehe auch Satz 79):

Satz 80. Die Begriffe **Stammkörper für ein (separables) irreduzibles Polynom** und **einfache (separable) algebraische Erweiterung** decken sich (ebenso auch die Begriffe **Körper der rationalen Funktionen einer Unbestimmten** und **einfache transzendente Erweiterung**). Hinsichtlich der Separabilität gilt genauer, daß jedes irreduzible Polynom, für das eine einfache separable algebraische Erweiterung Stammkörper ist, separabel ist.

Diese Begriffe sind also nur methodisch unterschieden, insofern bei Stammkörpern an die Entstehung aus einem bestimmten

[1]) Die einfachen Erweiterungen sind das genaue Analogon zu den (von der identischen verschiedenen) zyklischen Gruppen (siehe Def. 12 [30] und Def. 19 [52]). Die hier resultierende Unterscheidung der einfachen Erweiterungen in algebraische, die dann $\cong \mathsf{K}(x, \text{mod. } f(x))$ mit $f(x) \not\equiv 0, e$ und von endlichem Grade (Grad von $f(x)$) sind, und transzendente, die dann $\cong \mathsf{K}(x, \text{mod. } f(x))$ mit $f(x) \equiv 0$ und von unendlichem Grade sind, entspricht der im Anschl. an Satz 33 [32] getroffenen Unterscheidung der (von der identischen verschiedenen) zyklischen Gruppen in solche, die $\cong \mathfrak{R}_f$ mit $f \neq 0, 1$ und dann von endlicher Ordnung (Betrag von f) sind, und solche, die $\cong \mathfrak{R}_f$ mit $f = 0$ und dann von unendlicher Ordnung sind.

irreduziblen Polynom $f(x)$ gedacht ist, während einfache algebraische Erweiterung frei von einer derartigen Bezugnahme auf ein bestimmtes $f(x)$, d. h. auf ein bestimmtes primitives Element α ist. Diese letztere, allgemeinere Auffassung ist deswegen nützlich, weil sie es als naturgemäß erscheinen läßt, neben dem speziellen $f(x)$ und dessen Wurzel α, durch die ein Stammkörper erzeugt wird, auch andere seiner Elemente auf ihre Eigenschaft als primitive Elemente zu untersuchen, was anschließend geschieht.

Ist Λ eine einfache algebraische Erweiterung von K und n ihr Grad, so ist jedes Element β aus Λ algebraisch über K, und zwar nach Satz 67 [57] von einem Grade $\leqq n$. Da nun nach Satz 77 $[\beta : K] = [K(\beta) : K]$ ist, erhalten wir unter Anwendung von Satz 71 [59] und Satz 72 [60] genauer:

Satz 81. Ist Λ eine einfache algebraische Erweiterung vom Grade n über K und β ein Element aus Λ vom Grade j über K, so ist $j \mid n$ und $m = \frac{n}{j}$ der Grad von Λ über $K(\beta)$.

Insbesondere ist β dann und nur dann primitives Element von Λ, wenn es vom Grade n über K ist.

Wir heben noch die aus Satz 74, (II.) und (III.) [62] folgende bemerkenswerte Tatsache hervor:

Satz 82. Für ein algebraisches Element α über K gilt $K[\alpha] = K(\alpha)$.

Dieser gegenüber transzendenten Elementen abweichende Umstand, der natürlich für das Rechnen mit einem algebraischen Element sehr willkommen ist, geht vermöge der in § 8 geleisteten Zurückführung von $K(\alpha)$ auf den Restklassenkörper $K(x, \text{mod. } f(x))$ für das α zugehörige $f(x)$ letzten Endes auf den Satz 28 [27] zurück, dessen Beweis, verbunden mit der Zurückführung des § 8, auch die praktische Handhabung jenes Umstandes beim Rechnen mit einem algebraischen Element lehrt (Beseitigung aller vorkommenden, nicht zu K gehörigen Nenner!).

B. Endliche algebraische Erweiterungen.

Wir beweisen zunächst in Analogie zu Satz 76 [66]:

Satz 83. Ist Λ endlich über K und ist ein primitives Elementsystem $\alpha_1, \ldots, \alpha_r$ von $\mathsf{\Lambda}$ algebraisch über K, so ist $\mathsf{\Lambda} = \mathsf{K}(\alpha_1, \ldots, \alpha_r)$ algebraisch von endlichem Grade über K.

Beweis: Die von K zu $\mathsf{\Lambda}$ führende simultane Adjunktion von $\alpha_1, \ldots, \alpha_r$ kann durch die sukzessiven Adjunktionen $\mathsf{K} = \mathsf{\Lambda}_0$, $\mathsf{\Lambda}_0(\alpha_1) = \mathsf{\Lambda}_1$, $\mathsf{\Lambda}_1(\alpha_2) = \mathsf{\Lambda}_2, \ldots, \mathsf{\Lambda}_{r-1}(\alpha_r) = \mathsf{\Lambda}_r = \mathsf{\Lambda}$ ersetzt werden (Satz 62 [52]). Dabei ist für $i = 1, \ldots, r$ α_i algebraisch über $\mathsf{\Lambda}_{i-1}$ (Satz 65 [55]), also $\mathsf{\Lambda}_i$ von endlichem Grade über $\mathsf{\Lambda}_{i-1}$ (Satz 76 [66]), also $\mathsf{\Lambda}$ von endlichem Grade über K (Satz 71 [59]) und dann auch algebraisch über K (Satz 67 [57]).

Eine zu Satz 79 [68] analoge Verschärfung von Satz 83 durch Einbeziehung der Separabilität kann erst später (Satz 90 [80]) bewiesen werden.

Für endliche Erweiterungen $\mathsf{\Lambda} = \mathsf{K}(\alpha_1, \ldots, \alpha_r)$ sind außer den beiden Extremen: $\alpha_1, \ldots, \alpha_r$ algebraisch über K und $\alpha_1, \ldots, \alpha_r$ transzendent über K, die den beiden einzigen Möglichkeiten bei den einfachen Erweiterungen entsprechen, natürlich noch weitere Möglichkeiten vorhanden, daß nämlich die α_i teils algebraisch, teils transzendent über K sind. Nur der erstgenannte, in Satz 83 vorliegende Fall interessiert uns hier, weil allein in ihm $\mathsf{\Lambda}$ algebraisch über K sein kann und es nach Satz 83 auch ist; diesem Fall wenden wir uns des weiteren zu.

Nachdem wir in Satz 83 festgestellt haben, wann eine endliche Erweiterung algebraisch ist, untersuchen wir jetzt umgekehrt, wann eine algebraische Erweiterung endlich ist. Während nun aus den algebraischen Erweiterungen durch die Forderung der Einfachheit nach Satz 80 [69] die spezielle Klasse derjenigen herausgehoben wird, die von endlichem Grade sind und in denen eine Basis der besonderen Form $\alpha^0, \alpha^1, \ldots, \alpha^{n-1}$ (also aus den ersten n Potenzen eines einzigen Elements α) existiert, wird aus den algebraischen Erweiterungen durch die Forderung der Endlichkeit genau die Klasse aller Erweiterungen endlichen Grades herausgehoben. Aus den Resultaten von Satz 67, 68 [57, 58] einerseits und Satz 83 andererseits ergibt sich nämlich unmittelbar:

Satz 84. Die Begriffe **endliche algebraische Erweiterung** und **Erweiterung endlichen Grades** decken sich.

Durch sukzessive Anwendung von Satz 82 auf die im Beweis von Satz 83 auftretende Kette einfacher algebraischer Erweiterungen erhalten wir ferner die folgende Verallgemeinerung des erstgenannten Satzes:

Satz 85. Für endlich viele über K algebraische Elemente $\alpha_1, \ldots, \alpha_r$ einer Erweiterung von K gilt $\mathsf{K}[\alpha_1, \ldots, \alpha_r] = \mathsf{K}(\alpha_1, \ldots, \alpha_r)$.

Satz 83 erlaubt übrigens in Verbindung mit Satz 71 [59] noch, die nach Satz 66 [56] angekündigte Umkehrung dieses Satzes zu beweisen[1]):

Satz 86. Ist $\Lambda \geqq \overline{\mathsf{K}} \geqq \mathsf{K}$ und Λ über $\overline{\mathsf{K}}$, $\overline{\mathsf{K}}$ über K algebraisch, so ist auch Λ über K algebraisch.

Beweis: Sei α ein Element aus Λ und $\varphi(x) \equiv x^r + \alpha_1 x^{r-1} + \cdots + \alpha_r$ das zugehörige irreduzible Polynom aus $\overline{\mathsf{K}}$. Es ist dann einerseits α algebraisch über $\mathsf{K}(\alpha_1, \ldots, \alpha_r)$, also $\mathsf{K}(\alpha_1, \ldots, \alpha_r, \alpha)$ von endlichem Grade über $\mathsf{K}(\alpha_1, \ldots, \alpha_r)$ (Satz 76 [66]), andererseits sind $\alpha_1, \ldots, \alpha_r$ algebraisch über K, also ist $\mathsf{K}(\alpha_1, \ldots, \alpha_r)$ von endlichem Grade über K (Satz 83). Somit ist auch $\mathsf{K}(\alpha_1, \ldots, \alpha_r, \alpha)$ von endlichem Grade über K (Satz 71 [59]), also α algebraisch über K (Satz 67 [57]). Daher ist auch Λ algebraisch über K (Def. 23 [56]).

§ 10. Wurzelkörper.

Wir konstruieren in diesem Paragraphen die Wurzeln eines Polynoms $f(x)$ aus K, indem wir durch wiederholte Anwendung der Stammkörperkonstruktion des § 8 die Existenz einer speziellen Erweiterung von K beweisen, in der $f(x)$ voll-

---

[1]) Ohne Einbeziehung der Separabilität. — Dies kann erst später (Satz 92 [83]) geschehen.

ständig in Linearfaktoren zerfällt. Überdies werden wir eine Übersicht über alle derartigen Erweiterungen erhalten.

Unser zu Satz 74 [62] analoger Hauptsatz lautet:

Satz 87. Es sei $f(x)$ ein Polynom aus K. Dann existiert eine Erweiterung W von K mit den Eigenschaften:

(I.) $f(x)$ zerfällt in W in Linearfaktoren:
$$f(x) \equiv (x-\alpha_1)\cdots(x-\alpha_r).$$

(II.) W ist endlich über K und $\alpha_1,\ldots,\alpha_r$ ein primitives Elementsystem, d. h. es ist $\mathsf{W}=\mathsf{K}(\alpha_1,\ldots,\alpha_r)$.

(III.) W ist also algebraisch von endlichem Grade über K, und auch $\mathsf{W}=\mathsf{K}[\alpha_1,\ldots,\alpha_r]$.

Ist W^* irgendeine (I.), (II.) (und dann auch (III.)) genügende Erweiterung von K und sind $\alpha_1^*,\ldots,\alpha_r^*$ die Wurzeln von $f(x)$ in W^*, so ist W^* zu W bei geeigneter Reihenfolge der $\alpha_1^*,\ldots,\alpha_r^*$ auf Grund der Zuordnungen
$$\alpha_1^* \longleftrightarrow \alpha_1,\ldots,\alpha_r^* \longleftrightarrow \alpha_r$$
isomorph bzgl. K. Der Erweiterungstypus von W ist also durch (I.), (II.) eindeutig bestimmt.

a.) Existenzbeweis.

Wir kommen in folgenden r Schritten zum Ziel, deren schematische Andeutung genügen mag:

1.) $f(x)=p_1(x)\bar{f}(x)$, $p_1(x)$ Primfaktor in K, Σ_1 Stammkörper zu $p_1(x)$ über K, α_1 Wurzel von $p_1(x)$ in Σ_1, also
$$f(x)\equiv(x-\alpha_1)\,\varphi_1(x) \text{ in } \Sigma_1,\ \Sigma_1=\mathsf{K}(\alpha_1).$$

2.) $\varphi_1(x)=\pi_2(x)\,\bar{\varphi}_1(x)$, $\pi_2(x)$ Primfaktor in Σ_1, Σ_2 Stammkörper zu $\pi_2(x)$ über Σ_1, α_2 Wurzel von $\pi_2(x)$ in Σ_2, also $\varphi_1(x)\equiv(x-\alpha_2)\,\varphi_2(x)$ in Σ_2, $\Sigma_2=\Sigma_1(\alpha_2)$,
$$f(x)\equiv(x-\alpha_1)(x-\alpha_2)\,\varphi_2(x) \text{ in } \Sigma_2,\ \Sigma_2=\mathsf{K}(\alpha_1,\alpha_2).$$

....

$r.)\ \ldots f(x)\equiv(x-\alpha_1)\ldots(x-\alpha_r)$ in Σ^r, $\Sigma^r=\mathsf{K}(\alpha_1,\ldots,\alpha_r)$.

Die durch diese r Schritte erreichte Erweiterung $\mathsf{\Sigma}_r = \mathsf{W}$ hat die behaupteten Eigenschaften.

b.) Eindeutigkeitsbeweis.

Es sei W^* eine (I.), (II.) genügende Erweiterung von K, und es seien $\alpha_1^*, \ldots, \alpha_r^*$ die Wurzeln von $f(x)$ in W^*. Wir zeigen dann in den folgenden r Schritten, daß eine Kette von Körpern zwischen K und W^*:

$$\mathsf{K} \leqq \mathsf{\Sigma}_1^* \leqq \mathsf{\Sigma}_2^* \leqq \cdots \leqq \ \mathsf{\Sigma} \leqq \mathsf{W}^*$$

existiert, die je zu den entsprechenden Körpern der Kette aus a.) bei geeigneter Reihenfolge der $\alpha_1^*, \ldots, \alpha_r^*$ auf Grund der Zuordnungen des Satzes isomorph bzgl. K sind.

1.) Der in K gelegene Primfaktor $p_1(x)$ von $f(x)$ ist nach Satz 25 [24] ein Produkt aus gewissen der Primfaktoren $x - \alpha_1^*, \ldots, x - \alpha_r^*$ von $f(x)$ in W^*. Es hat also $p_1(x)$ eins der $\alpha_1^*, \ldots, \alpha_r^*$ zur Wurzel, und wir dürfen deren Reihenfolge so annehmen, daß α_1^* Wurzel von $p_1(x)$ ist. Nach Satz 74, 75 [62, 65] enthält dann W^* den Stammkörper $\mathsf{\Sigma}_1^* = \mathsf{K}(\alpha_1^*)$ für $p_1(x)$ über K, und dieser ist auf Grund der Zuordnung $\alpha_1^* \longleftrightarrow \alpha_1$ zu $\mathsf{\Sigma}_1$ isomorph bzgl. K.

2.) In $\mathsf{\Sigma}_1^*$ gilt eine Zerlegung $f(x) \equiv (x - \alpha_1^*)\, \varphi_1^*(x)$. Da sich die Koeffizienten von $\varphi_1^*(x) \equiv \dfrac{f(x)}{x - \alpha_1^*}$ aus α_1^* und denen von $f(x)$ in derselben rationalen Weise berechnen (vgl. die Bemerkung nach Satz 13 [18]), wie die von ${}_1(x) \equiv \dfrac{f(x)}{x - \alpha_1}$ aus α_1 und denen von $f(x)$, so sind die Koeffizienten von $\varphi_1^*(x)$ und $\varphi_1(x)$ einander bei dem Isomorphismus $\alpha_1^* \longleftrightarrow \alpha_1$ zwischen $\mathsf{\Sigma}_1^*$ und $\mathsf{\Sigma}_1$ zugeordnet. Nach den Ausführungen zu **1**, Def. 7, Zusatz [24] ist also das dem Primfaktor $\pi_2(x)$ von $\varphi_1(x)$ bei diesem Isomorphismus zugeordnete Polynom $\pi_2^*(x)$ ein Primfaktor von $\varphi_1^*(x)$ in $\mathsf{\Sigma}_1^*$, der dann ein Produkt aus gewissen der Primfaktoren $x - \alpha_2^*, \ldots, x - \alpha_r^*$ von $\varphi_1^*(x)$ in W^* ist. Es hat also $\pi_2^*(x)$ eins der $\alpha_2^*, \ldots, \alpha_r^*$ zur

Wurzel, und wir dürfen deren Reihenfolge so annehmen, daß α_2^* Wurzel von $\pi_2^*(x)$ ist. Dann enthält W^* den Stammkörper $\Sigma^* = \Sigma_1^*(\alpha_2^*) = \mathsf{K}(\alpha_1^*, \alpha_2^*)$ für $\pi_2^*(x)$ über Σ_1^*, und dieser ist nach den Ausführungen zu **1**, Def. 7, Zusatz zum Stammkörper Σ_2 für $\pi_2(x)$ über Σ_1 auf Grund der Zuordnung $\alpha_2^* \longleftrightarrow \alpha_2$ verbunden mit dem Isomorphismus $\alpha_1^* \longleftrightarrow \alpha_1$ zwischen den Teilkörpern Σ_1^* und Σ_1 isomorph bzgl. K.

. . . .

$r.$) . . . W^* enthält den Körper $\Sigma_r^* = \mathsf{K}(\alpha_1^*, \ldots, \alpha_r^*)$, und dieser ist zu $\Sigma_r = \mathsf{K}(\alpha_1, \ldots, \alpha_r)$ auf Grund der Zuordnungen $\alpha_1^* \longleftrightarrow \alpha_1, \ldots, \alpha_r^* \longleftrightarrow \alpha_r$ isomorph bzgl. K.

Da nach (II.) $\Sigma_r^* = \mathsf{W}^*$, $\Sigma_r = \mathsf{W}$ ist, ergibt der Schritt $r.$) die Behauptung.

Damit ist Satz 87 bewiesen. In Analogie zu Def. 27 [65] definieren wir hier, zunächst ebenfalls mit dem unbestimmten Artikel:

***Definition 28.** Jede Erweiterung W von K mit den Eigenschaften (I.), (II.) und daher auch (III.) von Satz 87 heißt ein **Wurzelkörper** für $f(x)$ über K.

Aus Satz 87 ergibt sich dann, analog zu Satz 75 [65]:

Satz 88. Zerfällt das Polynom $f(x)$ aus K in einer Erweiterung Λ von K in Linearfaktoren: $f(x) \equiv (x - \alpha_1) \cdots (x - \alpha_r)$, so enthält Λ einen Wurzelkörper für $f(x)$, nämlich $\mathsf{K}(\alpha_1, \ldots, \alpha_r)$.

Beweis: $\mathsf{K}(\alpha_1, \ldots, \alpha_r)$ hat die Eigenschaften (I.), (II.) von Satz 87.

Hiernach übersehen wir die Gesamtheit aller Erweiterungen von K, in denen ein Polynom $f(x)$ aus K in Linearfaktoren zerfällt, jedenfalls soweit nur der Erweiterungstypus in Frage kommt: Abgesehen von bzgl. K isomorphen sind es nämlich alle und nur die Erweiterungen eines Wurzelkörpers für $f(x)$. Die Wurzelkörper selbst repräsentieren also den engsten derartigen Erweiterungstypus.

Während nun in der Def. 27 [65] der Stammkörper für ein irreduzibles $f(x)$ eine Formulierung mit **bestimmtem** Artikel deshalb nicht angängig ist, weil ein Wurzelkörper $\mathsf{W} = \mathsf{K}(\alpha_1, \ldots, \alpha_n)$ für $f(x)$ nach Satz 75 [65] die n Stammkörper $\Sigma_1 = \mathsf{K}(\alpha_1), \ldots, \Sigma_n = \mathsf{K}(\alpha_n)$ enthält, die nach unseren späteren Ausführungen sehr wohl verschieden sein können, haben wir für Wurzelkörper nach Satz 50 [42]:

Satz 89. Unter der Voraussetzung von Satz 88 enthält Λ außer dem Wurzelkörper $\mathsf{K}(\alpha_1, \ldots, \alpha_r)$ für $f(x)$ keinen weiteren solchen.

Da also hiernach in keiner Erweiterung von K zwei verschiedene Wurzelkörper für $f(x)$ vorkommen können, dürfen wir (wie beim Quotientenkörper — vgl. **1**, Satz 10, Zusatz [30]) schlechthin von **dem** Wurzelkörper zu $f(x)$ reden, und somit auch von **den** Wurzeln von $f(x)$ ohne ausdrückliche Nennung einer sie enthaltenden Erweiterung. Geht man dabei, wie es im folgenden öfter geschehen wird, von einer Wurzel α von $f(x)$, also von einem Stammkörper $\Sigma = \mathsf{K}(\alpha)$ eines der Primfaktoren $p(x)$ von $f(x)$ aus, so darf, wie aus dem Beweis zu Satz 87, a.) 1.) ohne weiteres zu entnehmen ist, der Wurzelkörper $\mathsf{W} = \mathsf{K}(\alpha_1, \ldots, \alpha_r)$ von $f(x)$ so angenommen werden, daß er α, also $\Sigma = \mathsf{K}(\alpha)$ enthält.

Wir sehen damit prinzipiell ab von der **Natur** der Wurzeln, auf die wir für den Spezialfall eines Grundkörpers aus Zahlen in der Digression des folgenden § 11 nur aus historischen Gründen eingehen, haben vielmehr nur die **Struktur** (den Erweiterungstypus) des aus ihnen entspringenden Wurzelkörpers im Auge, deren Untersuchung die weiteren Abschnitte gewidmet sind.

Durch die Konstruktionen in §§ 8, 10 ist das Auflösungsproblem algebraischer Gleichungen, wie es in der Einleitung formuliert und erläutert wurde, vollständig gelöst. Für unsere weiteren Betrachtungen sind demnach die Wurzeln eines Polynoms nicht mehr als **Unbekannte**, d. h. zu **bestimmende Elemente**, sondern als durch die Konstruktionen in §§ 8, 10 **gegebene, völlig bestimmte Elemente** anzusehen.

§ 11. Der sog. Fundamentalsatz der Algebra.

Wie schon im Anschluß an Def. 18 [51] hervorgehoben wurde, kann man die Existenzbeweise der §§ 8, 10 nicht dadurch umgehen, daß man eine Wurzel α bzw. die Wurzeln $\alpha_1, \ldots, \alpha_r$ von $f(x)$ „von unten her" zum Grundkörper K adjungiert. Nur wenn man vorher auf irgendeine Weise in den Besitz einer Erweiterung von K gelangt ist, in der $f(x)$ einen Linearfaktor hat bzw. in Linearfaktoren zerfällt, kann man diesen einfacheren Weg einschlagen. Das geschieht nun in der bisherigen Literatur meist auf Grund des sog. Fundamentalsatzes der Algebra. Dieser besagt nämlich, daß im Körper der komplexen Zahlen jedes Polynom aus einem Zahlkörper in Linearfaktoren zerfällt, insbesondere also auch jedes Polynom aus dem engstmöglichen Zahlkörper P. Hiernach wird durch die einmalige Konstruktion des komplexen Zahlkörpers und Nachweis dieser Tatsache über ihn die Existenz der Wurzeln aller algebraischen Gleichungen mit Zahlkoeffizienten bewiesen.

Dieser zuerst von Gauß bewiesene Satz gehört nun aber nicht mehr in die Algebra im heutigen Sinne —, selbst wenn man unter diese wie am Schluß von **1**, Einl. alles das einbegreift, was aus den Körperaxiomen (d. h. den allgemeinen Rechengesetzen der rationalen Zahlen) oder einem Teil von ihnen (Ring, Integritätsbereich, Gruppe) gefolgert werden kann, also nicht nur lediglich den speziellen Sätzekomplex über die Auflösung von Gleichungen. — Jener Satz bedarf nämlich zum Beweise Hilfsmittel aus der Analysis (Grenzwert, Stetigkeit), mögen diese, wie in manchen der äußerst zahlreichen Beweise, auch auf ein noch so kleines Maß zurückgedrängt sein [1]). Auch reicht die Tragweite des sog. Fundamentalsatzes der Algebra nicht über die speziellen Zahlkörper hinaus, was ihm ebenfalls von unserem in **1**, Einleitung formulierten Standpunkt aus seine fundamentale Rolle für die Algebra nimmt (vgl. den zweiten und dritten Absatz von **1**, Einl.) [2]). Wir durften daher mit Recht den Gaußschen sog. Fundamentalsatz der Algebra aus

[1]) Wie einfach der Beweis unter voller Ausnutzung analytischer (komplex-funktionentheoretischer) Hilfsmittel wird, und wie naturgemäß sich der Satz in die komplexe Funktionentheorie einreiht, kann man nachlesen bei K. Knopp, Funktionentheorie I, 9. Aufl. 1957, § 28, Satz 3, S. 115 und § 35, S. 141 (Slg. Göschen 668).

[2]) Allerdings haben E. Artin und O. Schreier [Algebraische Konstruktion reeller Körper, Abh. a. d. Math. Sem. d. Univ. Hamburg 5 (1926)] das Feld der Algebra dadurch erweitert, daß sie auch die allgemeinen Anordnungsgesetze der rationalen Zahlen in den Kreis algebraischer (axiomatischer) Betrachtungen gezogen haben. Der sog. Fundamentalsatz der Algebra als spezieller Satz über den komplexen Zahlkörper ordnet sich dann einem entsprechenden Satz über eine allgemeine Klasse von Körpern unter und erhält in diesem neuen, erweiterten Gewande erneut Bürgerrecht in der modernen Algebra.

unserer Darstellung verweisen und dafür den von Kronecker ersonnenen und von Steinitz ausgebauten Existenzbeweis der §§ 8, 10 für die Wurzeln algebraischer Gleichungen aufnehmen, der auf ganz abstrakter und damit viel weiter tragender Grundlage steht.

Steinitz hat übrigens, und das ist wohl sein Hauptverdienst auf algebraischem Gebiete, bewiesen, daß analog, wie zu den Zahlkörpern der komplexe Zahlkörper, so auch zu jedem Grundkörper K Erweiterungen Λ existieren, in denen gleichzeitig alle Polynome aus K in Linearfaktoren zerfallen und daß der engstmögliche solche Körper A, ebenso wie unsere Stammkörper und Wurzelkörper, bis auf Isomorphismen bzgl. K durch K eindeutig bestimmt ist, nämlich als Körper aller algebraischen Elemente über K. Dieser Körper A hat überdies die Eigenschaft, daß keine echten algebraischen Erweiterungen von A existieren, daß also auch jedes Polynom aus A in A in Linearfaktoren zerfällt. Steinitz nennt ihn daher algebraisch abgeschlossen. Im Spezialfall des Grundkörpers P ist A der Körper aller algebraischen Zahlen. Da sich der Steinitzsche Existenzbeweis für A auf die speziellen Existenzbeweise der §§ 8, 10 stützen muß, kann man diese nicht etwa, ausgehend von der Existenz von A, umgehen.

Um Mißverständnissen anläßlich der bei Satz 89 eingeführten Redeweise mit bestimmtem Artikel zu begegnen, sei hier noch ausdrücklich auf folgendes hingewiesen: Unsere Existenzbeweise in §§ 8—10 liefern für den Spezialfall, daß K ein Zahlkörper ist, keineswegs die Existenz der Wurzeln eines Polynoms aus K und ihrer rationalen Funktionen über K als komplexe Zahlen, sondern lediglich als abstrakte Rechenelemente. Inwieweit man diese Elemente dann Zahlen nennen kann, kommt auf den nicht universell feststehenden Umfang des Begriffs Zahl an. Um sie aber dem Begriff komplexe Zahl unterordnen zu können, wäre über unsere Existenzbeweise hinaus erst zu zeigen, daß sie in der Form $a + bi$ darstellbar sind, wo i eine Wurzel des Polynoms $x^2 + 1$ ist und a, b Elemente eines solchen Körpers sind, der zu einem Teilkörper des reellen Zahlkörpers isomorph ist. Ein solcher Nachweis würde allgemein auf den Beweis des sog. Fundamentalsatzes der Algebra (bzw. dessen a. S. 77, Anm. 2 erwähnter Verallgemeinerung) hinauslaufen. Nur für den speziellen Fall des Polynoms $x^2 + 1$ selbst, in einem Körper K aus reellen Zahlen, liegt er unmittelbar auf der Hand: Ist i eine Wurzel dieses in K irreduziblen Polynoms in einem Stammkörper Σ über K (der übrigens dann gleichzeitig Wurzelkörper mit der Zerlegung $x^2 + 1 \equiv (x - i)(x + i)$ ist), so haben nach Satz 74 [62] die

Elemente von Σ eindeutige Darstellungen $a + bi$ mit Zahlen a, b aus K, und das Rechnen mit diesen Elementen verläuft wegen der Gleichung $i^2 = -1$ isomorph zum bekannten Rechnen mit den komplexen Zahlen. Cauchy, der Begründer der konkreten komplexen Funktionentheorie, ist der erste gewesen, der vom reellen Zahlkörper K ausgehend diesen abstrakten Weg zur Einführung des „imaginären“ i gegangen ist[1]), und der somit den Grundstein gelegt hat zu dem durch Kronecker und Steinitz auf breitere Grundlage gestellten und bis in die neueste Zeit in stetem Wachstum begriffenen Bau der abstrakten Algebra.

IV. Die Struktur der Wurzelkörper algebraischer Gleichungen.

Wir leiten in diesem Abschnitt zunächst (§§ 12, 13) einige mit den bisherigen Mitteln zugängliche Eigenschaften der Wurzelkörper her, führen sodann (§§ 14—16) als neues Hilfsmittel gewisse, durch die Erweiterungen endlichen Grades bestimmte, endliche Gruppen, ihre Galoisgruppen ein, und entwickeln schließlich (§§ 17, 18) auf dieser Grundlage die Galoissche Theorie, durch die man dann die Struktur der Wurzelkörper vollständig beherrscht, wie es in der Einleitung als Hauptziel dieses Bandes hingestellt wurde.

Dabei haben wir uns durchweg auf separable Polynome und Erweiterungen zu beschränken. Für inseparable Polynome und Erweiterungen erfährt die im folgenden zu entwickelnde Theorie, wie Steinitz gezeigt hat, wesentliche Abweichungen, auf die wir hier des knappen Raumes halber nicht eingehen können.

§ 12. Einfachheit und Separabilität der Wurzelkörper separabler Polynome, allgemeiner der endlichen algebraischen Erweiterungen mit separablem primitivem Elementsystem.

Die in der Überschrift dieses Paragraphen genannte, für

[1]) Cauchy führte die komplexen Zahlen nach dem Schema des Existenzbeweises in § 8, also als Restklassen mod. $x^2 + 1$, speziell i als die Restklasse x mod. $x^2 + 1$ ein. (Exerc. d'anal. et de phys. math. 4 (1847), S. 87.)

die Folge grundlegende Eigenschaft der Wurzelkörper separabler Polynome kommt allgemein den endlichen algebraischen Erweiterungen mit separablem primitivem Elementsystem zu, zu denen ja die Wurzelkörper separabler Polynome gehören (Satz 87 [73]).

Im Beweis müssen wir uns aus methodischen Gründen auf Grundkörper K mit unendlich vielen Elementen beschränken. Diese Einschränkung kann man indes auf anderem Wege als in Wahrheit überflüssig erkennen (siehe Schluß von § 20 [134ff.]). Daher dürfen wir den folgenden Satz, sowie alle weiteren auf ihn gestützten, ohne sie formulieren.

Der zu beweisende Satz, den man nach seinem Entdecker den **Abelschen Satz** nennt, lautet:

Satz 90. Jede endliche algebraische Erweiterung Λ von K mit separablem primitivem Elementsystem, insbesondere also der Wurzelkörper jedes separablen Polynoms $f(x)$ aus K ist einfach algebraisch und separabel über K, also Stammkörper für ein separables irreduzibles Polynom $g(x)$ aus K.

Beweis[1]): Es sei $\Lambda = \mathsf{K}(\alpha_1, \ldots, \alpha_r)$, wo $\alpha_1, \ldots, \alpha_r$ separabel algebraisch über K sind. Für $r = 1$ ist dann nichts mehr zu beweisen (Satz 76, 79 [66, 68]).

a.) $r = 2$.

Seien $f_1(x)$, $f_2(x)$ die zu α_1, α_2 gehörigen, nach der Voraussetzung und Satz 63 [55] separablen, irreduziblen Polynome aus K, ferner W der Wurzelkörper für das Polynom $f_1(x) f_2(x)$ aus K und

$$f_1(x) \equiv \prod_{\nu_1=1}^{n_1} (x - \alpha_{1\nu_1}), \quad f_2(x) \equiv \prod_{\nu_2=1}^{n_2} (x - \alpha_{2\nu_2})$$

die Zerlegungen von $f_1(x)$ und $f_2(x)$ in W in Linearfaktoren. Es ist dann α_1 eines der $\alpha_{1\nu_1}$, α_2 eines der $\alpha_{2\nu_2}$. Ferner sind

[1]) Dieser Beweis wurde bisher fast immer unter Anwendung des Satzes von den symmetrischen Funktionen (siehe den späteren Satz 131 [153]) geführt. Der Grundgedanke des im Text gegebenen, ohne jenen Satz auskommenden Beweises wurde aber schon von Galois zu dem entsprechenden Zwecke verwandt.

die $\alpha_{1\nu_1}$ und die $\alpha_{2\nu_2}$ je untereinander verschieden (Satz 58 [47]).

Daher sind die $n_1 n_2$ linearen Funktionen

$$\vartheta_{\nu_1\nu_2}(\bar{x}) = \alpha_{1\nu_1} + \bar{x}\alpha_{2\nu_2}$$

aus $W[\bar{x}]$ sämtlich voneinander verschieden, weil ja zwei von ihnen sich entweder im Koeffizienten der Unbestimmten $\bar{x}$ oder im von $\bar{x}$ freien Koeffizienten unterscheiden. Wenn also, wie wir hier voraussetzen, K unendlich viele Elemente besitzt, so existiert nach Satz 49 [41] (angewandt auf W für K, K für M) ein Element $a \neq 0$ in K, so daß die $n_1 n_2$ Elemente

$$\vartheta_{\nu_1\nu_2} = \vartheta_{\nu_1\nu_2}(a) = \alpha_{1\nu_1} + a\alpha_{2\nu_2}$$

sämtlich voneinander verschieden sind.

Es sei nun

$$\vartheta = \alpha_1 + a\alpha_2$$

das dem System $(\alpha_{1\nu_1}, \alpha_{2\nu_2}) = (\alpha_1, \alpha_2)$ entsprechende Element unter den $\vartheta_{\nu_1\nu_2}$. Dann bilden wir das Polynom $\varphi(x)$ gemäß[1])

$$(-a)^{n_1}\varphi(x)$$

$$\equiv \prod_{\nu_1=1}^{n_1}(\vartheta - (\alpha_{1\nu_1} + ax)) \equiv \prod_{\nu_1=1}^{n_1}((\alpha_1 + a\alpha_2) - (\alpha_{1\nu_1} + ax))$$

$$\equiv \prod_{\nu_1=1}^{n_1}((\vartheta - ax) - \alpha_{1\nu_1}) \equiv f_1(\vartheta - ax).$$

Die erstere Darstellung läßt erkennen, daß $\varphi(x)$ zwar die Wurzel α_2 hat — entsprechend dem Linearfaktor $\vartheta - (\alpha_1 + ax)$ —, dagegen keine der von α_2 verschiedenen Wurzeln $\alpha_{2\nu_2}$ von $f_2(x)$ zur Wurzel hat; denn sonst folgte ja die Gleichheit von $\vartheta = \alpha_1 + a\alpha_2$ mit einem $\vartheta_{\nu_1\nu_2} = \alpha_{1\nu_1} + a\alpha_{2\nu_2}$, wo $(\alpha_{1\nu_1}, \alpha_{2\nu_2}) \neq (\alpha_1, \alpha_2)$, entgegen unserer Konstruktion der $\vartheta_{\nu_1\nu_2}$[2]). Die letztere Darstellung lehrt, daß $\varphi(x)$ ein Polynom aus $K(\vartheta)$ ist.

[1]) Der vorgesetzte Faktor $(-a)^{n_1}$ bewirkt, daß $\varphi(x)$ ein Polynom wird, d. h. den höchsten Koeffizienten e bekommt.

[2]) Wie man sich leicht überzeugt, wird für diesen Schluß und damit für den ganzen Beweis die Separabilität von α_1 nicht benötigt. Ein Analogon zu Satz 90 gilt daher auch, wenn nur alle bis auf eins der primitiven Elemente separabel sind. Indessen werden wir von diesem (für die Theorie der inseparablen Erweiterungen wesentlichen) Umstand keinen Gebauch zu machen haben.

Wegen dieser beiden Eigenschaften von $\varphi(x)$ ist der größte gemeinsame Teiler $(\varphi(x), f_2(x))$ einerseits gleich dem einzigen gemeinsamen Linearfaktor $x - \alpha_2$ (Satz 21 [22]), andererseits ein Polynom in $\mathsf{K}(\vartheta)$ (Satz 24, 14 [23, 18]). Daher gehört α_2 zu $\mathsf{K}(\vartheta)$, somit auch $\alpha_1 = \vartheta - a\alpha_2$, d. h. es ist $\Lambda = \mathsf{K}(\alpha_1, \alpha_2) \leqq \mathsf{K}(\vartheta)$. Da umgekehrt $\vartheta = \alpha_1 + a\alpha_2$ zu $\Lambda = \mathsf{K}(\alpha_1, \alpha_2)$ gehört, ergibt sich also, daß $\Lambda = \mathsf{K}(\alpha_1, \alpha_2) = \mathsf{K}(\vartheta)$ einfach algebraisch über K ist.

Um zu zeigen, daß $\Lambda = \mathsf{K}(\vartheta)$ auch separabel über K ist, genügt es nach Satz 78, 79 [66, 68], im Falle der Charakteristik p aus den nach der Voraussetzung richtigen Relationen

$$\alpha_1 \text{ in } \mathsf{K}(\alpha_1^p), \qquad \alpha_2 \text{ in } \mathsf{K}(\alpha_2^p)$$

die entsprechende Relation

$$\vartheta \text{ in } \mathsf{K}(\vartheta^p)$$

zu folgern. Nun ergibt die Potenzierung mit p der Darstellungen von α_1 und α_2 als Elemente aus $\mathsf{K}[\vartheta]$ nach Satz 44 [37]

$$\alpha_1^p \text{ in } \mathsf{K}(\vartheta^p), \qquad \alpha_2^p \text{ in } \mathsf{K}(\vartheta^p).$$

Daraus ergibt sich zusammen mit den beiden obigen Relationen weiter

$$\alpha_1 \text{ in } \mathsf{K}(\vartheta^p), \qquad \alpha_2 \text{ in } \mathsf{K}(\vartheta^p)$$

und somit in der Tat auch

$$\vartheta \ (= \alpha_1 + a\alpha_2) \text{ in } \mathsf{K}(\vartheta^p).$$

Damit sind die Behauptungen des Satzes für $r = 2$ bewiesen.

b.) $$r > 2.$$

Dann folgen die Behauptungen durch vollständige Induktion. Seien sie schon bis $r-1$ bewiesen, so ist also $\mathsf{K}(\alpha_1, \ldots, \alpha_{r-1}) = \mathsf{K}(\overline{\alpha}_{r-1})$ mit einem geeigneten über K separablen algebraischen $\overline{\alpha}_{r-1}$. Nach Satz 62 [52] ist dann $\Lambda = \mathsf{K}(\alpha_1, \ldots, \alpha_{r-1}, \alpha_r) = \mathsf{K}(\overline{\alpha}_{r-1}, \alpha_r)$, und somit nach dem Beweise a.) Λ einfach algebraisch und separabel über K, d. h. die Behauptung ist auch für r richtig.

Das aus diesem Beweise leicht zu entnehmende weitere Resultat, daß man ein primitives Element ϑ von $\Lambda = \mathsf{K}(\alpha_1, \ldots, \alpha_r)$ speziell unter den linearen Komposita $a_1\alpha_1 + \cdots + a_r\alpha_r$ eines primitiven Elementsystems $\alpha_1, \ldots, \alpha_r$ vorfindet, ist für die Konstruktion eines solchen ϑ in konkreten Fällen nützlich.

Da nach Def. 19 [52] eine einfache algebraische Erweiterung a fortiori endlich algebraisch ist, besagt Satz 90 in Verbindung mit Satz 80 [69] und 84 [72] insbesondere:

Satz 91. Die Begriffe **separable Erweiterung endlichen Grades, endliche separable algebraische Erweiterung, einfache separable algebraische Erweiterung, Stammkörper für ein separables irreduzibles Polynom** decken sich.

Hinsichtlich des letzteren gilt genauer, daß **jedes** irreduzible Polynom, für das eine solche Erweiterung Stammkörper ist, separabel ist.

Wir fügen diesem Satz im Anschluß an die Bemerkung nach Satz 67 [58] noch an:

Zusatz. Mit den Begriffen von Satz 91 deckt sich auch noch der Begriff **separable algebraische Erweiterung mit beschränkten Elementgraden,** und zwar ist dann der für eine solche Erweiterung $\mathsf{\Lambda}$ von K vorhandene „Maximalgrad" eines Elements von $\mathsf{\Lambda}$ über K gleich dem Grade von $\mathsf{\Lambda}$ über K.

Beweis: Sei ϑ ein Element aus $\mathsf{\Lambda}$ vom Maximalgrade. Wäre ϑ nicht primitives Element von $\mathsf{\Lambda}$ und dementsprechend β ein nicht rational durch ϑ darstellbares Element von $\mathsf{\Lambda}$, so wäre

$$\mathsf{K} \leqq \mathsf{K}(\vartheta) < \mathsf{K}(\vartheta, \beta) \leqq \mathsf{\Lambda}$$

(Satz 60 [52]), und da $\mathsf{K}(\vartheta, \beta) = \mathsf{K}(\vartheta')$ gesetzt werden kann (Satz 90), $[\vartheta : \mathsf{K}] < [\vartheta' : \mathsf{K}]$ (Satz 72, 77 [60, 66]) entgegen der Maximalbestimmung des Grades von ϑ. Also ist ϑ primitives Element von $\mathsf{\Lambda}$ und daher $\mathsf{\Lambda} = \mathsf{K}(\vartheta)$ einfach algebraisch über K, sowie $[\mathsf{\Lambda} : \mathsf{K}] = [\vartheta : \mathsf{K}]$.

Jetzt kann auch die für den Fall der Charakteristik p noch ausstehende Verschärfung von Satz 86 [72] durch Einbeziehung der Separabilität erfolgen:

Satz 92. Ist $\mathsf{\Lambda} \geqq \overline{\mathsf{K}} \geqq \mathsf{K}$ und $\mathsf{\Lambda}$ über $\overline{\mathsf{K}}$, $\overline{\mathsf{K}}$ über K separabel algebraisch, so ist auch $\mathsf{\Lambda}$ über K separabel algebraisch.

Beweis: Sei α ein Element aus $\mathsf{\Lambda}$ und $f(x)$ das zugehörige (gemäß Satz 86 [72] vorhandene) irreduzible Polynom aus K.

Es sei dann s der größte Exponent, für den noch $f(x) \equiv f_0(x^{p^s})$ mit einem Polynom $f_0(x)$ aus K ist. $f_0(x)$ ist dabei wegen der Irreduzibilität von $f(x)$ irreduzibel und wegen der Maximaleigenschaft von s separabel.

Da nach Voraussetzung $\alpha, \alpha^p, \ldots, \alpha^{p^{s-1}}$ separabel über $\overline{K}$ sind, ist nun nach Satz 78 [66]

$$\overline{K}(\alpha) = \overline{K}(\alpha^p) = \cdots = \overline{K}(\alpha^{p^s}).$$

Hiernach (siehe auch Satz 82 [70]) besitzt α eine Darstellung

$$\alpha = \varphi(\alpha^{p^s}) = h(\alpha^{p^s}, \alpha_1, \ldots, \alpha_r),$$

wo $\varphi(x)$ ein Polynom in x über $\overline{K}$ ist, das sich auch als ganze rationale Funktion $h(x, \alpha_1, \ldots, \alpha_r)$ über K von x und den zu $\overline{K}$ gehörigen Koeffizienten α_i von φ auffassen läßt. Da aber die α_i nach Voraussetzung und α^{p^s} als Wurzel von $f_0(x)$ über K separabel sind, ergibt Satz 90, daß auch α über K separabel ist. Daher ist Λ separabel über K (Def. 23 [56]).

§ 13. Normalität der Wurzelkörper und ihrer primitiven Elemente. Galoissche Resolventen.

1.) Eine weitere wichtige Eigenschaft der Wurzelkörper (beliebiger Polynome) ist die in der folgenden Definition genannte:

***Definition 29.** Eine Erweiterung N von K heißt **normal** (oder **galoissch**) über K, wenn jede zu N bzgl. K konjugierte Erweiterung N* mit N identisch ist, d. h. (vgl. Def. 26 [60]) wenn aus $\Lambda \geqq N \geqq K$, $\Lambda \geqq N^* \geqq K$ und N* isomorph zu N bzgl. K stets folgt $N^* = N$.

In teilweiser Analogie zu Satz 66, 70 [56, 59] haben wir hier:

Satz 93. Ist $N \geqq \overline{K} \geqq K$ und N normal über K, so ist N normal auch über $\overline{K}$.

Beweis: Jede mit N bzgl. K konjugierte Erweiterung N* von $\overline{K}$ ist gemäß Def. 26 [60] auch eine mit N bzgl. K konjugierte Erweiterung von K.

Es braucht aber weder, wie in Satz 66, 70 [56, 59], dann auch $\overline{K}$ über K, noch umgekehrt, wie in Satz 71, 86 [59, 72], mit N über $\overline{K}$ und $\overline{K}$ über K auch N über K normal zu sein. Beispiele dafür kann man mittels des in § 17 zu beweisenden Fundamentalsatzes bilden, der gleichzeitig den tieferen Grund für diese Tatsachen erkennen läßt.

Wir beweisen nun:

Satz 94. Der Wurzelkörper W eines Polynoms $f(x)$ ist normal über K.

Beweis: Es sei $f(x) \equiv (x-\alpha_1)\cdots(x-\alpha_r)$ und $\mathsf{W} = \mathsf{K}(\alpha_1, \ldots, \alpha_r)$. Diese beiden Relationen für $\alpha_1, \ldots, \alpha_r$ bleiben nach Def. 26 [60] und den Ausführungen zu **1**, Def. 7, Zusatz [24] beim Übergang zu einem mit W bzgl. K konjugierten Körper W^* für die zu ihnen konjugierten Elemente $\alpha_1^*, \ldots, \alpha_r^*$ erhalten. W^* ist also ebenfalls Wurzelkörper zu $f(x)$ und somit nach Satz 89 [76] mit W identisch, d. h. W ist normal über K.

2.) Um die Bedeutung der Normalität für eine einfache algebraische Erweiterung Λ näher kennenzulernen, müssen wir uns zunächst in jedem Falle einen Überblick über die sämtlichen konjugierten zu Λ verschaffen, sei Λ normal oder nicht. Wir erreichen dies dadurch, daß wir Λ als Stammkörper eines irreduziblen Polynoms $f(x)$ darstellen (Satz 76 [66]) und dann als Teilkörper des Wurzelkörpers W von $f(x)$ studieren (siehe das im Anschluß an Satz 89 Gesagte [76]). In dieser Hinsicht haben wir nach Satz 74, 75 [62, 65] und gemäß Def. 26 [60] (vgl. auch das schon vor Satz 89 [76] Gesagte) unmittelbar:

Satz 95. Es sei $f(x)$ ein irreduzibles Polynom in K, α eine Wurzel von $f(x)$, $\Lambda = \mathsf{K}(\alpha)$ der zugehörige Stammkörper und $\beta = h(\alpha)$ irgendein Element aus Λ. Sind dann $\alpha_1, \ldots, \alpha_r$ die Wurzeln von $f(x)$, so enthält der (α, also $\Lambda = \mathsf{K}(\alpha)$ enthaltende) Wurzelkörper $\mathsf{W} = \mathsf{K}(\alpha_1, \ldots, \alpha_r)$ von $f(x)$ die r Stammkörper

$$\Lambda_1 = \mathsf{K}(\alpha_1), \ldots, \Lambda_r = \mathsf{K}(\alpha_r)\,.$$

Diese sind zu $\Lambda = \mathsf{K}(\alpha)$ konjugiert, und zwar wird in ihnen durch

$$\beta_1 = h(\alpha_1), \ldots, \beta_r = h(\alpha_r)$$

je ein System zu $\beta = h(\alpha)$ konjugierter Elemente repräsentiert.

In den Bezeichnungen dieses Satzes ist α irgendeine der Wurzeln α_i, $\mathsf{\Lambda}$ der entsprechende der Körper $\mathsf{\Lambda}_i$ und β das entsprechende der Elemente β_i. Wir treffen aber hier und bei ähnlichen Betrachtungen im folgenden (siehe auch schon im Beweis zu Satz 90 [80]) keine feste Verabredung darüber, welches der α_i gleich α sein soll, weil dadurch eine im Hinblick auf die Nichtunterscheidbarkeit der α_i, $\mathsf{\Lambda}_i$, β_i von K aus (1, bei Def. 7, Zusatz [24]) ganz unberechtigte Unsymmetrie geschaffen würde [1]).

Nach Satz 95 sind speziell die α_i sämtlich konjugiert zu α. Umgekehrt folgt aus Satz 73 [61]:

Satz 96. Es liege der Sachverhalt von Satz 95 vor. Dann sind die Wurzeln $\alpha_1, \ldots, \alpha_r$ die einzigen konjugierten zu α innerhalb W oder irgendeiner Erweiterung von W.

Die konjugierten zu einem algebraischen Element sind also mit den Wurzeln des zugehörigen irreduziblen Polynoms identisch.

Wir sagen daher im folgenden auch kürzer die konjugierten zu α für „die Wurzeln des zu α gehörigen irreduziblen Polynoms".

Für die $\mathsf{\Lambda}_i$ gilt Entsprechendes; denn ein zu $\mathsf{\Lambda}$ konjugierter Körper (innerhalb irgendeiner Erweiterung von W) ist nach einer analogen Schlußweise, wie im Beweis zu Satz 94, ebenfalls Stammkörper für $f(x)$, entsteht also durch Adjunktion einer Wurzel von $f(x)$, d. h. eines α_i (Satz 50 [42]):

Satz 97. Es liege der Sachverhalt von Satz 95 vor. Dann sind die Körper $\mathsf{\Lambda}_1, \ldots, \mathsf{\Lambda}_r$ die einzigen konjugierten zu $\mathsf{\Lambda}$ innerhalb W oder irgendeiner Erweiterung von W.

Bezüglich der β_i können wir das Entsprechende vorläufig deshalb noch nicht aussprechen, weil ja in W oder in Erweiterungen von W außer den $\mathsf{\Lambda}_i$ noch andere Erweiterungen von K enthalten sein und diese dann das Vorhandensein von den β_i verschiedener

1) In der Literatur findet man vielfach die Verabredung $\alpha = \alpha_1$.

zu β konjugierter Elemente bewirken könnten (siehe dazu Def. 26 [60]). Wir kommen darauf nachher (Satz 103 [91]) zurück.

3.) Auf Grund der in 2.) festgestellten Tatsachen können wir nunmehr der Bedeutung der Normalität für einfache algebraische Erweiterungen und damit insbesondere auch der Bedeutung des Zusammentreffens von Einfachheit und Normalität für die Wurzelkörper separabler Polynome, nachgehen. Es ist zweckmäßig, der Def. 29 die folgende, auf sie gestützte Definition zur Seite zu stellen:

***Definition 30.** Ein Element ϑ heißt **normal** (oder **galoissch**) über K, wenn der Körper $\mathsf{K}(\vartheta)$ normal über K ist.

Ein über K normales Element ist von selbst auch algebraisch über K, da für ein über K transzendentes Element x nach der Bemerkung hinter Def. 26 [60] von $\mathsf{K}(x)$ verschiedene konjugierte existieren.

Durch Kombination von Def. 19 [52] und Def. 30 ergibt sich dann ohne weiteres:

Satz 98. Es sei N eine einfache algebraische Erweiterung von K. Ist N normal über K, so ist jedes primitive Element von N normal über K. Ist umgekehrt ein primitives Element von N normal über K, so ist N normal über K.

Dieser Satz ist vom bisherigen Standpunkt natürlich tautologisch mit Def. 29, 30, sagt also vorläufig nichts Neues aus. Wir können ihm aber unter Beibehaltung seines Wortlautes dadurch einen neuen, mehr besagenden Inhalt geben, daß wir den Begriff Normalelement auf eine andere Weise charakterisieren. Das geschieht, auf Grund der in 2.) festgestellten Tatsachen, in dem folgenden Satz:

Satz 99. Es seien ϑ ein algebraisches Element über K, $q(x)$ das zu ϑ gehörige irreduzible Polynom aus K und $\vartheta_1, \ldots, \vartheta_n$ seine Wurzeln — die konjugierten zu ϑ. Ist ϑ normal über K, so gilt:

(I.) $\mathsf{K}(\vartheta) = \mathsf{K}(\vartheta_1, \ldots, \vartheta^n)$, d. h. der Wurzelkörper von $q(x)$ fällt mit einem Stammkörper von $q(x)$ zusammen.

(II.) $\mathsf{K}(\vartheta_1) = \cdots = \mathsf{K}(\vartheta_n)$, d. h. die den konjugierten zu ϑ entsprechenden konjugierten Stammkörper von $q(x)$ fallen zusammen.

(III.) $\vartheta_1 = g_1(\vartheta), \ldots, \vartheta_n = g_n(\vartheta)$, d. h. die konjugierten zu ϑ gehören zu $\mathsf{K}(\vartheta)$.

Umgekehrt folgt aus (I.) oder (II.) oder (III.), daß ϑ normal über K ist.

Beweis: a.) Ist ϑ normal über K, so folgt nach Def. 29, 30 und Satz 95 zunächst (II.), und daraus (I.) nach Satz 60 [52], sowie (III.) nach Def. 18 [50] und Satz 82 [70].

b.) Aus (III.) oder (I.) folgt zunächst $\mathsf{K}(\vartheta_i) \leqq \mathsf{K}(\vartheta)$ und daraus (II.) nach Satz 72 [60]. Es genügt also zu zeigen, daß aus (II.) die Normalität von ϑ folgt. Das ist aber nach Satz 97 und Def. 29, 30 der Fall.

Satz 99 besagt insbesondere, daß mit ϑ auch alle seine konjugierten ϑ_i normal bzw. nicht normal über K sind. Daher ist es sinnvoll, festzusetzen:

Zusatz zu Definition 30. Ein **Polynom** $q(x)$ aus K heißt **normal** (oder **galoissch**) über K, wenn es erstens irreduzibel ist, und wenn zweitens eine seiner Wurzeln ϑ normal über K ist.

Satz 99 läßt wegen seiner schon geschilderten Bedeutung für die Aussagen in Satz 98 erkennen, welche Einschränkung die Forderung der Normalität für eine einfache algebraische Erweiterung N von K bedeutet: Jedes primitive Element ϑ von N muß den Bedingungen (I.)—(III.) genügen; umgekehrt reicht schon eine dieser Bedingungen für nur ein primitives Element ϑ zur Normalität von N hin.

Die Form (I.) jener Einschränkung zeigt, daß in Umkehrung zu Satz 90, 94 [80, 85] auch jede einfache (separable) normale Erweiterung von K Wurzelkörper für ein (separables) Polynom aus K ist. Im Falle der Separabilität ist genauer jedes Polynom, für das eine solche Erweiterung Wurzelkörper ist, separabel; denn gemäß Satz 63 [55] und Def. 17, Zusatz [48] kann ein separables Element nur von separablen Polynomen Wurzel sein.

Die Form (II.) weist eine bemerkenswerte Analogie zu den entsprechend benannten Begriffen der Gruppentheorie auf (1, §9, insbesondere Satz 31 [64]). Der in §17 zu beweisende Fundamentalsatz wird diese formale Analogie als Ausfluß eines sachlichen Zusammenhangs erkennen lassen.

Die Form (III.) ist am greifbarsten und wird in konkreten Fällen zweckmäßig zur Feststellung der Normalität benutzt.

Nach dem über (I.) Gesagten gilt in Analogie zu Satz 91 [83]:

Satz 100. Die Begriffe **Wurzelkörper eines separablen Polynoms f(x), separable normale Erweiterung endlichen Grades, endliche separable normale Erweiterung, einfache separable normale Erweiterung, Stammkörper für ein separables normales Polynom q(x)** decken sich.

Genauer ist **jedes** Polynom $f(x)$, für das eine solche Erweiterung Wurzelkörper ist, und **jedes** normale Polynom $q(x)$, für das sie Stammkörper ist, separabel.

Diese Begriffe sind also nur methodisch voneinander unterschieden. (Vgl. das in dieser Hinsicht bei Satz 80 Gesagte [69].)

Um bei der in den folgenden Paragraphen auseinanderzusetzenden Galoisschen Theorie, die sich mit der genaueren Struktur der in Satz 100 charakterisierten Erweiterungen befaßt, auch dem Wortlaute nach weder auf ein bestimmtes Polynom noch auf ein bestimmtes primitives Element oder primitives Elementsystem Wert zu legen, entwickeln wir diese als Theorie der separablen normalen Erweiterungen endlichen Grades und schalten nur vorläufig ein, wie sich die darzulegenden Verhältnisse gestalten, wenn man das Entspringen einer solchen Erweiterung als Wurzelkörper eines bestimmten Polynoms oder als Stammkörper eines bestimmten normalen Polynoms hervorhebt.

4.) Zur Vorbereitung der letzteren Untersuchungen fassen wir die im vorigen und in diesem Paragraphen erhaltenen Resultate über die Struktur des Wurzelkörpers eines separablen Polynoms (Satz 90, 94, 98, 99) in folgendem Satz zusammen und geben anschließend eine in dieser Hinsicht grundlegende Definition:

Satz 101. Es seien $f(x)$ ein separables Polynom aus K und $\alpha_1, \ldots, \alpha_r$ seine Wurzeln. Dann existiert in seinem Wurzelkörper $\mathsf{W} = \mathsf{K}(\alpha_1, \ldots, \alpha_r)$ ein primitives Element

$$\vartheta = h(\alpha_1, \ldots, \alpha_r),$$

so daß also $\mathsf{W} = \mathsf{K}(\vartheta)$ ist und demgemäß Darstellungen

$$\alpha_1 = k_1(\vartheta), \ldots, \alpha_r = k_r(\vartheta)$$

bestehen. Jedes solche ϑ ist normal über K, d. h. ist $q(x)$ das zugehörige irreduzible Polynom aus K und sind $\vartheta_1, \ldots, \vartheta_n$ seine Wurzeln — die konjugierten zu ϑ —, so bestehen Darstellungen

$$\vartheta_1 = g_1(\vartheta), \ldots, \vartheta_n = g_n(\vartheta).$$

***Definition 31.** Jedes gemäß Satz 101 zu $f(x)$ bestimmte Normalpolynom $q(x)$ (gelegentlich auch ein zugehöriges ϑ) heißt eine **Galoissche Resolvente** für $f(x)$ bzgl. K.

Die Bezeichnung Resolvente entstammt der älteren Literatur und soll zum Ausdruck bringen, daß die Gleichung $f(x) \doteq 0$ als gelöst anzusehen ist, wenn die Resolvente $q(x) \doteq 0$ gelöst ist. Denn nach Satz 101 ergeben sich ja die Wurzeln von $f(x)$ durch rationale Rechnung aus einer Wurzel von $q(x)$. Die dabei zugrunde liegende Vorstellung eines Auflösungsprozesses für die Gleichung $f(x) \doteq 0$ können und wollen wir uns aber hier nicht zu eigen machen. Denn erstens ist — abgesehen von dem Spezialfall, wo $q(x)$ den Grad 1 hat, wo also $f(x)$ in K in Linearfaktoren zerfällt — die Gleichung $f(x) \doteq 0$ entweder ebensowenig lösbar wie die Gleichung $q(x) \doteq 0$ (nämlich durch kein rationales Rechenverfahren) oder ebensogut lösbar (nämlich durch die Konstruktionen in §§ 8, 10), und zweitens kann aus entsprechenden Gründen, wie den in der Einleitung für 1.) angeführten, prinzipiell kein rationales Rechenverfahren existieren, um die Koeffizienten einer Galoisschen Resolvente $q(x)$ aus denen von $f(x)$ zu bestimmen. Für uns hat vielmehr die Galoissche Resolvente eine lediglich theoretische Bedeutung, indem ihre Wurzel ϑ den Wurzelkörper $\mathsf{K}(\alpha_1, \ldots, \alpha_r)$ in die „einfache" Gestalt $\mathsf{K}(\vartheta)$ zu setzen gestattet.

Aus Satz 99, (I.) ergibt sich noch ohne weiteres:

Satz 102. Dann und nur dann, wenn $f(x)$ ein Normalpolynom ist, ist es Galoissche Resolvente für sich selbst.

Aus diesem Grunde nennt man, wie in Def. 29, 30 [84, 87] gesagt, die normalen Polynome gelegentlich auch galoissche Polynome und dementsprechend die normalen Erweiterungen, die ja, sofern sie einfach sind, Stammkörper galoisscher Polynome sind, auch galoissche Erweiterungen. Dabei wird das Wort galoissch klein geschrieben, weil es anders als in Def. 31 nicht mehr auf Galois hinweist, sondern nur noch ein mit normal gleichbedeutendes Eigenschaftswort ist (ähnlich wie abelsch in **1,** Def. 13 [50]).

5.) Wir kommen jetzt auf die auf S. 87 zurückgestellte Frage nach den sämtlichen konjugierten zu $\beta = h(\alpha)$ zurück. Analog zu Satz 96, 97 [86] beweisen wir, allerdings nur für separables $f(x)$:

Satz 103. Es liege der Sachverhalt von Satz 95 [85] vor, und es sei überdies $f(x)$ separabel. Dann sind die Elemente $\beta_1, \ldots, \beta_r$ die einzigen zu β konjugierten innerhalb W oder innerhalb irgendeiner Erweiterung von W.

Beweis: Sei β^* ein zu β konjugiertes Element (in einer Erweiterung von W). Nach Satz 73 [61] ist dann β^* Wurzel desselben irreduziblen Polynoms in K wie β. Nach Satz 74, 75 [62, 65] ist daher der zugehörige Stammkörper $\mathsf{K}(\beta^*)$ auf Grund der Zuordnung $\beta \longleftrightarrow \beta^*$ zum Stammkörper $\mathsf{K}(\beta)$ isomorph bzgl. K.

Gemäß Satz 101 sei nun $\mathsf{W} = \mathsf{K}(\vartheta)$. Ferner seien $q(x)$ und $\varphi(x)$ die zu ϑ gehörigen irreduziblen Polynome in K und $\mathsf{K}(\beta)$. Dann ist $\varphi(x) \mid q(x)$ (Satz 53 [43]); und $\mathsf{W} = \mathsf{K}(\vartheta) = \mathsf{K}(\beta, \vartheta)$ ist Stammkörper zu $\varphi(x)$ über $\mathsf{K}(\beta)$ (Satz 75 [65]).

Durch den genannten Isomorphismus bzgl. K geht $q(x)$ in sich über, während aus $\varphi(x)$ ein Polynom $\varphi^*(x)$ mit den folgenden Eigenschaften entsteht: $\varphi^*(x)$ ist irreduzibel in $\mathsf{K}(\beta^*)$; es ist $\varphi^*(x) \mid q(x)$ (also sind die Wurzeln von $\varphi^*(x)$ unter denen von $q(x)$ enthalten, d. h. gewisse der konjugierten zu ϑ); ist ϑ^* eine Wurzel von $\varphi^*(x)$, so ist (vgl. Satz 101, 99) $\mathsf{W} = \mathsf{K}(\vartheta^*) = \mathsf{K}(\beta^*, \vartheta^*)$ Stammkörper zu $\varphi^*(x)$ über $\mathsf{K}(\beta^*)$.

Nach den Ausführungen zu **1,** Def. 7, Zusatz [24] erzeugen daher (analog wie im Beweis zu Satz 87 unter b.) [74]) die Zuordnungen $\beta \longleftrightarrow \beta^*$, $\vartheta \longleftrightarrow \vartheta^*$ einen Isomorphismus bzgl. K von W zu sich selbst (einen sogen. Automorphismus bzgl. K von W — siehe des näheren den folgenden § 14); oder, anders gesagt, bei dem durch $\vartheta \longleftrightarrow \vartheta^*$ erzeugten Isomorphismus von $\mathsf{W} = \mathsf{K}(\vartheta) = \mathsf{K}(\vartheta^*)$ zu sich selbst ist $\beta \longleftrightarrow \beta^*$. Bei diesem Isomorphismus ist nun dem (gemäß Satz 101 dargestellten) Element $\alpha = k(\vartheta)$ das Element $\alpha^* = k(\vartheta^*)$ zugeordnet, das nach Satz 96 [86] eins der α_i sein muß. Das dem Element β zugeordnete Element β^* hat dann wegen der Darstellung $\beta = h(\alpha)$ die durch jenen Isomorphismus entstehende Darstellung $\beta^* = h(\alpha^*)$, ist also in der Tat eins der $\beta_i = h(\alpha_i)$.

Aus Satz 103 folgt mit Hinsicht auf Satz 96 [86] und Satz 58 [47], daß die verschiedenen unter den β_i die Wurzeln des zu β gehörigen irreduziblen Polynoms $g(x)$, d. h. die konjugierten zu β im dort eingeführten Sinne sind. Häufig findet man als die konjugierten zu β auch die sämtlichen β_i bezeichnet; i. a. sind das die Wurzeln von $g(x)$, jede eine gewisse Anzahl von Malen gesetzt. Näheres darüber werden wir in Satz 113 [111] kennenlernen.

§ 14. Die Automorphismengruppe eines Erweiterungsbereichs.

Wir bereiten in diesem Paragraphen die im folgenden zu machende Anwendung der Gruppentheorie auf die Strukturuntersuchung der normalen Erweiterungen endlichen Grades vor, indem wir die in Frage kommenden Gruppen einführen. Um zu den Elementen dieser Gruppen zu gelangen, erinnern wir daran, wie wir in **1**, § 2 aus dem für Mengen definierten Begriff eineindeutige Zuordnung durch Hinzunahme der beiden auf die Verknüpfungen bezüglichen Forderungen (3.), (4.) [23] den auf Bereiche bezüglichen Begriff Isomorphismus bildeten. Ganz analog schaffen wir jetzt aus dem in **1**, § 16 für Mengen definierten Begriff Permutation den entsprechenden auf Bereiche bezüglichen Begriff Automorphismus[1]):

[1]) Der Begriff Automorphismus läßt sich ebenso wie Isomorphismus

Definition 32. Eine Permutation eines Bereiches B, d.h. also eine eineindeutige Zuordnung mit bestimmter Zuordnungsrichtung von B zu sich selbst (Bezeichnung $\rightarrow$) heißt ein **Automorphismus** von B, wenn sie außerdem zu den in B definierten Verknüpfungen in den Beziehungen steht:

(1.) aus $a \rightarrow a'$, $b \rightarrow b'$ folgt $a + b \rightarrow a' + b'$,

(2.) aus $a \rightarrow a'$, $b \rightarrow b'$ folgt $ab \rightarrow a'b'$,

d.h. wenn sie den Isomorphiebedingungen [**1**, § 2, (3.), (4.) [23]] genügt.

Hiernach übertragen sich die an **1**, Def. 35 [104] geknüpften Bemerkungen über Permutationen sinngemäß auf Automorphismen.

In anderer Gegenüberstellung wie oben verhalten sich auch die beiden Mengenbegriffe eineindeutige Zuordnung, Permutation zueinander wie die beiden Bereich-Begriffe Isomorphismus, Automorphismus, d.h. Automorphismus von B bedeutet soviel wie Isomorphismus von B zu sich selbst mit bestimmter Zuordnungsrichtung.

Daher übertragen sich auch die an **1**, Def. 7 [24] geknüpften Bemerkungen über Isomorphismen sinngemäß auf Automorphismen.

Aus **1**, Satz 56, 57 [105] ergibt sich nun mittels **1**, Satz 19 [55] ohne weiteres:

Satz 104. Die Automorphismen eines Bereiches B bilden eine Gruppe, wenn unter dem Produkt zweier Automorphismen von B ihr Produkt als Permutationen, d. h. der durch ihre Nacheinanderausführung entstehende Automorphismus von B verstanden wird. Der Typus dieser Gruppe ist durch den Typus des Bereiches B eindeutig bestimmt.

Wir bezeichnen mit a_A das durch Anwendung des Automorphismus A aus dem Elemente a entstehende Element. (1.) und (2.)

(**1**, Def. 17 [56]) auch für Gruppen einführen; doch brauchen wir das hier nicht.

können dann auch in die Form gesetzt werden:

$$(1.)\quad (a+b)_A = a_A + b_A, \qquad (2.)\quad (ab)_A = a_A b_A .$$

Nach der Erklärung des Automorphismenprodukts gilt ferner

$$(3.)\qquad (a_A)_B = a_{AB} .$$

Geht a durch alle Automorphismen aus einer Automorphismenmenge $\mathfrak{M}$ in ein- und dasselbe Element über, so bezeichnen wir dieses sinngemäß mit $a_{\mathfrak{M}}$.

Nach Satz 104 besitzt jeder Bereich mindestens den identischen Automorphismus $a \to a$. Daß weitere Automorphismen nicht notwendig vorhanden zu sein brauchen, zeigt das Beispiel der Primbereiche Γ, P, P_p. Da nämlich, wie für Isomorphismen, auch für jeden Automorphismus eines Integritätsbereiches $0 \to 0$, $e \to e$ gilt (vgl. das in **1** bei Def. 7 [24] Gesagte), so sind für die genannten Bereiche nach (1.), (2.) alle übrigen Übergänge zwangsläufig zu $a \to a$ festgelegt. Beispiele für Bereiche (Körper) mit von der Einsgruppe verschiedenen Automorphismengruppen werden wir im folgenden ausführlich kennenlernen.

Ebenso wie wir für das Studium der Erweiterungsbereiche B eines Bereiches B_0 den schärferen Begriff Isomorphismus von B bzgl. B_0 brauchten, haben wir auch hier den schärferen Begriff Automorphismus von B bzgl. B_0 heranzuziehen:

Zusatz zu Definition 32. Ist B ein Erweiterungsbereich von B_0, so heißen diejenigen Automorphismen von B, bei denen jedes Element von B_0 in sich übergeht, die **Automorphismen von B bzgl. B_0.**

Automorphismus von B bzgl. B_0 bedeutet also soviel wie Isomorphismus von B zu sich selbst bzgl. B_0 mit bestimmter Zuordnungsrichtung.

Daher übertragen sich die an **1**, Def. 7, Zusatz [24] geknüpften Bemerkungen über relative Isomorphismen sinngemäß auf relative Automorphismen. Ist ferner, entsprechend zu den Ausführungen vor Def. 20 [53], $\Lambda = \mathsf{K}(\mathsf{M})$ und führt ein Automorphismus A von Λ bzgl. K die Menge M in M' über, so daß also auch $\Lambda = \mathsf{K}(\mathsf{M}')$ ist, so wird, wie dort, A schon durch Angabe der von M zu M' führenden Substitutionen

$$\alpha \to \alpha',\ \beta \to \beta', \ldots \begin{pmatrix} \alpha, \beta, \ldots \text{ aus } \mathsf{M} \\ \alpha', \beta', \ldots \text{ aus } \mathsf{M}' \end{pmatrix}$$

vollständig beschrieben. Analog zu Def. 20 [54] definieren wir in dieser Hinsicht wieder:

Definition 33. Ein Automorphismus bzgl. K von $\Lambda = \mathsf{K}(\mathsf{M})$ heißt durch die bei ihm stattfindenden Substitutionen der Elemente aus M **erzeugt.**

Insbesondere kann dabei $\mathsf{M} = \mathsf{M}'$ sein; dann stellen jene Substitutionen eine Permutation von M dar, und Λ wird durch diese Permutation von M erzeugt.

Mittels **1**, Satz 19 [55] folgt schließlich aus Satz 104 ohne weiteres:

Zusatz zu Satz 104. Die Automorphismen von B bzgl. B_0 bilden eine Untergruppe der Gruppe aller Automorphismen von B. Der Typus dieser Untergruppe ist durch den Erweiterungstypus von B eindeutig bestimmt.

Nach dem oben Bemerkten ist diese Untergruppe die volle Automorphismengruppe von B, wenn B ein Integritätsbereich (Körper) und B_0 sein Primintegritätsbereich (Primkörper) ist, dagegen die Einsgruppe, wenn B mit B_0 zusammenfällt.

§ 15. Die Galoisgruppe einer separablen normalen Erweiterung endlichen Grades.

Wir wenden jetzt die Begriffe des § 14, insbesondere den Zusatz zu Satz 104, auf eine normale Erweiterung N endlichen Grades von K an, die dann (wenn separabel) nach Satz 100 [89] auch einfach algebraisch über K ist. Zu Ehren von Galois, der die weitgehende Bedeutung der Automorphismengruppe für diesen Fall zuerst erkannte [1]), hat man die folgende Bezeichnung eingeführt:

***Definition 34.** Die Gruppe $\mathfrak{G}$ der Automorphismen bzgl. K einer **normalen Erweiterung** N **endlichen Grades** von K heißt die **Galoisgruppe** von N bzgl. K.

Ist speziell $\mathfrak{G}$ abelsch oder zyklisch, so heißt auch N **abelsch** oder **zyklisch** über K.

---

[1]) Allerdings nicht in der hier gegebenen abstrakten Gestalt, sondern in der konkreten Darstellung von § 16. — E. Galois fiel am 30. Mai 1832 im Alter von 20 Jahren im Duell. Am Vorabend seines Todes schrieb er einen langen Brief an einen Freund, in dem er (u. a.) dem der Pariser Akademie bereits eingereichten ersten Entwurf seiner Theorie der algebraischen Gleichungen weitere wichtige Resultate anreihte. Der Brief ist in seinen Werken abgedruckt.

Diese Galoisgruppe übersehen wir im Falle eines separablen N auf Grund des folgenden Satzes vollständig:

Satz 105. Es seien N eine separable normale Erweiterung vom Grade n über K, ϑ ein primitives Element von N und $\vartheta_1, \ldots, \vartheta_n$ seine konjugierten. Dann ist die Galoisgruppe $\mathfrak{G}$ von N endlich von der Ordnung n, und ihre n Automorphismen werden durch die n Substitutionen $\vartheta \rightarrow \vartheta_i$ $(i = 1, \ldots, n)$ erzeugt, führen also jedes Element $\beta = h(\vartheta)$ aus N in die n konjugierten $\beta_i = h(\vartheta_i)$ über.

Beweis: a.) Da ein Automorphismus bzgl. K von N nach Def. 32, Zusatz [94] auch als Isomorphismus bzgl. K von N zu sich selbst (mit bestimmter Zuordnungsrichtung) angesehen werden kann, führt er nach Def. 26 [60] jedes Element aus N in ein konjugiertes über, speziell also ϑ in ein ϑ_i (Satz 96 [86]) und dann die $\beta = h(\vartheta)$ in $\beta_i = h(\vartheta_i)$. Es gibt somit höchstens die im Satz angegebenen n Möglichkeiten für einen Automorphismus bzgl. K von N.

b.) Umgekehrt führt jede dieser n Möglichkeiten nach Satz 95 [85] zu einem Isomorphismus bzgl. K von N $=$ K(ϑ) zu einem seiner n konjugierten Stammkörper K(ϑ_i), nach Satz 99, (II.) [88] also von N zu sich selbst, und liefert daher nach Def. 32, Zusatz einen Automorphismus bzgl. K von N.

Aus a.) und b.) ergeben sich die Behauptungen des Satzes, wenn man noch hinzunimmt, daß wegen der Separabilität von N die n konjugierten $\vartheta_1, \ldots, \vartheta_n$ zu ϑ, als die Wurzeln des zu ϑ gehörigen irreduziblen Polynoms, untereinander verschieden sind (Satz 58 [47]), also auch die durch die n Substitutionen $\vartheta \rightarrow \vartheta_i$ erzeugten n Automorphismen.

Um die Nacheinanderausführung der durch die Substitutionen $\vartheta \rightarrow \vartheta_i$ erzeugten Automorphismen, d. h das Rechnen in der Galoisgruppe $\mathfrak{G}$ zu übersehen, ist es zweckmäßig, die Elemente von $\mathfrak{G}$ durch Übergang zu einer isomorphen Gruppe in eine besser greifbare Gestalt zu setzen, als es die bisherigen Automorphismen sind, oder, wie man in der Gruppentheorie sagt, eine geeignete Darstellung von $\mathfrak{G}$ zu geben. Das geschieht durch den folgenden Satz:

Satz 106. Es mögen die Voraussetzungen und Bezeichnungen von Satz 105 gelten; ferner sei

$$q(x) \equiv (x - \vartheta_1) \cdots (x - \vartheta_n)$$

das zu ϑ gehörige, irreduzible Polynom aus K und gemäß Satz 99, (III.) [88]

$$(1.) \qquad \vartheta_i = g_i(\vartheta), \qquad (i = 1, \ldots, n).$$

Dann wird in der Menge $\mathfrak{F}$ der durch die $g_i(x)$ repräsentierten Restklassen mod. $q(x)$ durch die Festsetzung

$$(2.) \qquad \{g_i\} \times \{g_k\} = \{g_l\}, \text{ wenn } \{g_i(g_k(x))\} = \{g_l(x)\}$$

eine unbeschränkte und eindeutige Verknüpfung erklärt, die zu $\mathfrak{G}$ vermöge der Zuordnungen

$$(3.) \qquad (\vartheta \to \vartheta_i) \leftrightarrow \{g_i(x)\} \qquad (i = 1, \ldots, n)$$

isomorph ist.

Beweis: Es sei zunächst an die eineindeutige Zuordnung (3.) (S. 65) zwischen den Elementen aus N und den Restklassen mod. $q(x)$ erinnert.

a.) Da $g_i(g_k(\vartheta))$ aus $g_i(\vartheta)$ durch $\vartheta \to g_k(\vartheta)$, also aus ϑ_i durch $\vartheta \to \vartheta_k$ entsteht, ist es nach Satz 105 ebenfalls ein ϑ_l und daher dann $g_i(g_k(\vartheta)) = g_l(\vartheta)$, $\{g_i(g_k(x))\} = \{g_l(x)\}$. Somit wird durch (2.) eine Verknüpfung in $\mathfrak{F}$ unbeschränkt und eindeutig erklärt.

b.) Da die ϑ_i wegen der Separabilität von K verschieden sind, sind auch die $\{g_i\}$ verschieden. Somit ist (3.) eine eineindeutige Zuordnung zwischen $\mathfrak{G}$ und $\mathfrak{F}$.

c.) Da durch Nacheinanderausführung der durch $\vartheta \to \vartheta_i$ und $\vartheta \to \vartheta_k$ erzeugten Automorphismen erst ϑ in $\vartheta_i = g_i(\vartheta)$ und dann dies weiter in $g_i(\vartheta_k) = g_i(g_k(\vartheta)) = g_l(\vartheta) = \vartheta_l$ übergeht, also zusammengenommen der durch $\vartheta \to \vartheta_l$ erzeugte Automorphismus resultiert, entspricht bei der Zuordnung (3.) der Multiplikation in $\mathfrak{G}$ die durch (2.) definierte Verknüpfung in $\mathfrak{F}$. Somit ist bei (3.) auch die Isomorphiebedingung (**1**, Satz 23 [56]) erfüllt.

Aus a.), b.), c.) folgen die Behauptungen.

Die in Satz 106 angegebene Darstellung der Galoisgruppe $\mathfrak{G}$ als Substitutionsgruppe $\mathfrak{F}$ ganzer rationaler Funktionen mod. $q(x)$ ist bei gegebenem $q(x)$ (für die Anwendung auf den Wurzelkörper eines separablen Polynoms $f(x)$ also bei gegebener Galoisscher Resolvente dieses Polynoms) und gegebenen Darstellungen (1.) der praktischen Rechnung ohne weiteres zugänglich. Man reduziert dazu zweckmäßig die $g_i(x)$ auf ihren eindeutig bestimmten Rest mod. $q(x)$ von niedrigerem als dem n-ten Grade (Satz 13, 27 [16, 26]; siehe insbesondere die Bemerkung hinter Satz 13) und bekommt dann ein vollständiges Bild der Verknüpfungen innerhalb $\mathfrak{F}$ (also auch derer innerhalb $\mathfrak{G}$), wenn man dasselbe für alle $g_i(g_k(x))$ tut. In der bisherigen Literatur wird meist diese Darstellung $\mathfrak{F}$ von $\mathfrak{G}$ für die Definition der Galoisgruppe verwendet. Das hat aber den Nachteil, daß man sich dabei auf ein bestimmtes primitives Element ϑ bezieht. Man hat dann also nachzuweisen, daß für alle primitiven Elemente $\vartheta, \vartheta', \ldots$ isomorphe Gruppen $\mathfrak{F}, \mathfrak{F}', \ldots$ resultieren. Unsere nur von den Körpern N und K abhängige Definition hat den Vorteil, diesen Umstand dadurch von vornherein in Evidenz zu setzen, daß sie einen Schritt tiefer eindringt, nämlich alle Gruppen $\mathfrak{F}, \mathfrak{F}', \ldots$ als Darstellungen ein- und derselben Gruppe $\mathfrak{G}$, der Automorphismengruppe von N bzgl. K, erscheinen läßt.

§ 16. Die Galoisgruppe eines separablen Polynoms.

Wenn man die Methoden des § 15 anwenden will, um zu einer konkreten Darstellung der Galoisgruppe $\mathfrak{G}$ des Wurzelkörpers W eines separablen Polynoms $f(x)$ aus K zu gelangen, so braucht man dazu die Kenntnis einer Galoisschen Resolvente $q(x)$ für $f(x)$, auf die man dann die Sätze 105, 106 anwenden kann. Da nach Satz 102 [90] $f(x)$ selbst i. a. keine Galoissche Resolvente für sich selbst ist, und da man ferner nach dem bei Def. 31 [90] Bemerkten eine solche nicht durch ein rationales Rechenverfahren aus $f(x)$ herleiten kann, ist es also von Interesse, eine konkrete Darstellung von $\mathfrak{G}$ anzugeben, die sich nicht auf eine Galoissche Resolvente $q(x)$ für $f(x)$, sondern lediglich auf $f(x)$ und seine Wurzeln stützt.

Wir definieren zunächst:

***Definition 35.** Unter der **Galoisgruppe eines Polynoms** $f(x)$ aus K versteht man die Galoisgruppe $\mathfrak{G}$ seines Wurzelkörpers W über K.

Ist speziell $\mathfrak{G}$ abelsch oder zyklisch, so heißt (wie W nach Def. 34 [95]) auch $f(x)$ **abelsch** oder **zyklisch** über K.

Wir beweisen nun den folgenden Satz, der die gewünschte Darstellung der Galoisgruppe von W, oder, wie wir jetzt sagen können, der Galoisgruppe eines separablen Polynoms $f(x)$ gibt:

Satz 107. Die Galoisgruppe $\mathfrak{G}$ eines separablen Polynoms $f(x)$ aus K ist isomorph zur Gruppe $\mathfrak{P}$ der durch die Automorphismen aus $\mathfrak{G}$ gelieferten Permutationen der verschiedenen unter den Wurzeln $\alpha_1, \ldots, \alpha_r$ von $f(x)$. Diese Permutationen lassen sich auch dadurch charakterisieren, daß bei ihrer Anwendung jede bestehende ganzrationale Beziehung

$$f(\alpha_1, \ldots, \alpha_r) = 0$$

zwischen den Wurzeln von $f(x)$ richtig bleibt.

Beweis: 1.) Wir zeigen zunächst, daß sich $\mathfrak{G}$ überhaupt als Permutationsgruppe $\mathfrak{P}$ der verschiedenen $\alpha_1, \ldots, \alpha_{\bar{r}}$ unter den Wurzeln $\alpha_1, \ldots, \alpha_r$ darstellen läßt.

a.) Bei einem Automorphismus A bzgl. K des Wurzelkörpers W von $f(x)$ geht nach Satz 105 [96] jede der Wurzeln von $f(x)$ in ein konjugiertes Element, also nach Satz 73 [61] wieder in eine Wurzel von $f(x)$ über. Da A als eineindeutige Zuordnung verschiedene Elemente in verschiedene überführt, erfahren somit die verschiedenen $\alpha_1, \ldots, \alpha_{\bar{r}}$ durch A eine eindeutig bestimmte Permutation P.

b.) Da $\mathsf{W} = \mathsf{K}(\alpha_1, \ldots, \alpha_r) = \mathsf{K}(\alpha_1, \ldots, \alpha_{\bar{r}})$ ist, wird A durch P erzeugt (Def. 33 [95]), und es entsprechen daher verschiedenen A auch verschiedene P. Somit ist die Zuordnung zwischen der Galoisgruppe $\mathfrak{G}$ von W und der Menge $\mathfrak{P}$ der durch ihre Automorphismen bewirkten Permutationen P der $\alpha_1, \ldots, \alpha_{\bar{r}}$ eineindeutig.

c.) Da für Automorphismen wie für Permutationen die Multiplikation als Nacheinanderausführung erklärt ist, ist bei dieser Zuordnung auch die Isomorphiebedingung (1, Satz 23 [56]) erfüllt.

Nach a.), b.), c.) ist $\mathfrak{P}$ eine zu $\mathfrak{G}$ isomorphe Permutationsgruppe.

2.) Wir zeigen jetzt, daß die Permutationen aus $\mathfrak{P}$ durch die im Satz genannte Eigenschaft charakterisiert sind.

a.) Daß jede bestehende Relation $\bar{f}(\alpha_1, \ldots, \alpha_r) = 0$ bei Anwendung der Permutationen aus $\mathfrak{P}$ richtig bleibt, ist klar. Denn die Anwendung einer solchen kommt nach 1.) der Anwendung des durch sie erzeugten Automorphismus aus $\mathfrak{G}$ gleich, und hierbei ist dies ja nach Def. 32, Zusatz [94] und den Ausführungen zu 1, Def. 7, Zusatz [24] der Fall.

b.) Es sei gemäß Satz 101 [89] ϑ ein primitives Element von W, $q(x) \equiv (x - \vartheta_1) \cdots (x - \vartheta_n)$ die zugehörige Galoissche Resolvente für $f(x)$ und

$$\alpha_\nu = k_\nu(\vartheta) \qquad (\nu = 1, \ldots, r),$$
$$\vartheta = h(\alpha_1, \ldots, \alpha_r).$$

Die Galoisgruppe $\mathfrak{G}$ von W besteht dann nach Satz 105 [96] aus den durch die Substitutionen $\vartheta \to \vartheta_i$ $(i = 1, \ldots, n)$ erzeugten Automorphismen. Ist nun $\begin{pmatrix} \alpha_1, \ldots, \alpha_{\bar{r}} \\ \alpha_{i_1}, \ldots, \alpha_{i_{\bar{r}}} \end{pmatrix}$ eine Permutation der $\alpha_1, \ldots, \alpha_{\bar{r}}$, bei der jede bestehende Relation $\bar{f}(\alpha_1, \ldots, \alpha_r) = 0$ richtig bleibt, und werden durch $\begin{pmatrix} \alpha_1, \ldots, \alpha_r \\ \alpha_{i_1}, \ldots, \alpha_{i_r} \end{pmatrix}$ die durch sie bewirkten Übergänge für die volle Reihe $\alpha_1, \ldots, \alpha_r$ bezeichnet, so gehen die speziellen Relationen

$$\alpha_\nu = k_\nu\bigl(h(\alpha_1, \ldots, \alpha_r)\bigr) \qquad (\nu = 1, \ldots, r),$$
$$q\bigl(h(\alpha_1, \ldots, \alpha_r)\bigr) = 0$$

bei ihrer Anwendung in die Relationen

$$\alpha_{i_\nu} = k_\nu\bigl(h(\alpha_{i_1}, \ldots, \alpha_{i_r})\bigr) \qquad (\nu = 1, \ldots, r),$$
$$q\bigl(h(\alpha_{i_1}, \ldots, \alpha_{i_r})\bigr) = 0$$

über, die somit ebenfalls richtig sind. Wegen der letzteren ist also $h(\alpha_{i_1}, \ldots, \alpha_{i_r}) = \vartheta_i$ eins der konjugierten zu ϑ, so daß wegen der ersteren Relationen $\alpha_{i_\nu} = k_\nu(\vartheta_i)$ aus $\alpha_\nu = k_\nu(\vartheta)$ durch den Automorphismus $\vartheta \to \vartheta_i$ entsteht. Die Permutation $\begin{pmatrix} \alpha_1, \ldots, \alpha_{\bar r} \\ \alpha_{i_1}, \ldots, \alpha_{i_{\bar r}} \end{pmatrix}$ entspringt daher wirklich gemäß 1.) aus einem Automorphismus aus $\mathfrak{G}$ und gehört mithin zu $\mathfrak{P}$.

Damit ist Satz 107 bewiesen. Er leistet übrigens vom praktischen Standpunkt aus nicht ebensoviel, wie der auf die Kenntnis einer Galoisschen Resolvente von $f(x)$ gestützte Satz 106 [97]. Denn die Entscheidung darüber, welche Permutationen die Eigenschaft von Satz 107 haben, kann ohne Kenntnis einer Galoisschen Resolvente von $f(x)$ i. a. nicht in endlich vielen Schritten getroffen werden. Wir vermerken als Folge aus Satz 107 noch:

Satz 108. Ist $f(x)$ ein separables Polynom vom Grade r aus K und $\bar r$ die Anzahl der verschiedenen unter seinen Wurzeln, so ist der Grad n seines Wurzelkörpers W über K ein Teiler von $\bar r!$ (also erst recht von $r!$).

Beweis: n ist nach Satz 105 [96] gleichzeitig die Ordnung der Galoisgruppe $\mathfrak{G}$ von W. Da nun nach Satz 107 die zu $\mathfrak{G}$ isomorphe Permutationsgruppe $\mathfrak{P}$ Untergruppe der symmetrischen Gruppe $\mathfrak{S}_{\bar r}$ von $\bar r$ Elementen ist, ist nach **1**, Satz 25, 58 [59, 107] $n \mid \bar r!$.

§ 17. Der Fundamentalsatz der Galoisschen Theorie.

Der große Nutzen, den die Betrachtung der Galoisgruppe $\mathfrak{G}$ einer separablen normalen Erweiterung N endlichen Grades von K bietet, besteht darin, daß man mit ihrer Hilfe einen genauen Einblick in die Struktur des Erweiterungstypus von N erhält. Sie ermöglicht es nämlich, die von K zu N führenden Bausteine, d. h. die zwischen K und N liegenden Körper, in ihren gegenseitigen Beziehungen vollständig zu übersehen, wenn man nur die Struktur von $\mathfrak{G}$, insbesondere die sämtlichen Untergruppen von $\mathfrak{G}$ in ihren gegenseitigen Beziehungen kennt. Da $\mathfrak{G}$ eine endliche Gruppe ist, ist das letztere eine, wenigstens in jedem konkreten Fall, in endlich vielen Schritten zu bewältigende Aufgabe.

1.) Wir beweisen den folgenden **Fundamentalsatz der Galoisschen Theorie:**

Satz 109. Es sei N eine separable normale Erweiterung vom Grade n über K und $\mathfrak{G}$ ihre Galoisgruppe von der Ordnung n. Dann besteht eine eineindeutige Zuordnung zwischen den sämtlichen in N enthaltenen Erweiterungskörpern $\mathsf{\Lambda}$ von K und den sämtlichen ($\mathfrak{E}$ enthaltenden[1])) Untergruppen $\mathfrak{H}$ von $\mathfrak{G}$, die durch jede der beiden folgenden, für einander zugeordnete $\mathsf{\Lambda}$ und $\mathfrak{H}$ geltenden Tatsachen (Ia), (Ib) vollständig festgelegt wird:

(Ia) $\mathfrak{H}$ besteht aus allen und nur den Automorphismen aus $\mathfrak{G}$, die jedes Element aus $\mathsf{\Lambda}$ invariant lassen.

(Iaa) $\mathfrak{H}$ ist also die Galoisgruppe von N bzgl. $\mathsf{\Lambda}$, und daher ist die Ordnung m von $\mathfrak{H}$ (der Index von $\mathfrak{E}$ in $\mathfrak{H}$) gleich dem Grade von N über $\mathsf{\Lambda}$ und der Index j von $\mathfrak{H}$ in $\mathfrak{G}$ gleich dem Grade von $\mathsf{\Lambda}$ über K.

(Ib) $\mathsf{\Lambda}$ besteht aus allen und nur den Elementen aus N, die bei jedem Automorphismus aus $\mathfrak{H}$ invariant bleiben.

Für diese eineindeutige Zuordnung gilt überdies, wenn gleich indizierte $\mathsf{\Lambda}$ und $\mathfrak{H}$ einander zugeordnet sind:

(II) Ist $\mathsf{\Lambda}$ Erweiterungskörper von $\mathsf{\Lambda}'$ vom Grade k über $\mathsf{\Lambda}'$, so ist $\mathfrak{H}$ Untergruppe von $\mathfrak{H}'$ vom Index k in $\mathfrak{H}'$ und umgekehrt.

---

[1]) $\mathfrak{E}$ bezeichnet, wie in **I**, die identische Untergruppe (Einsgruppe). Bezüglich dieses an sich überflüssigen Zusatzes vgl. die angeschlossenen Bemerkungen.

(III) Sind Λ, $\bar{\Lambda}$ konjugierte Erweiterungskörper von K, so sind $\mathfrak{H}$, $\bar{\mathfrak{H}}$ konjugierte Untergruppen von $\mathfrak{G}$ und umgekehrt. Genauer: Entsteht $\bar{\Lambda}$ aus Λ durch den Automorphismus S, so entsteht $\bar{\mathfrak{H}}$ aus $\mathfrak{H}$ durch Transformation mit dem Element S und umgekehrt.

(IV) Ist Λ Normalkörper über K, so ist $\mathfrak{H}$ Normalteiler von $\mathfrak{G}$ und umgekehrt.

(V) Im Falle (IV) ist (neben dem in (Iaa) Gesagten) die Faktorgruppe $\mathfrak{G}/\mathfrak{H}$ isomorph zur Galoisgruppe von Λ bzgl. K, indem die Ausübung aller Automorphismen einer Restklasse von $\mathfrak{G}$ nach $\mathfrak{H}$ auf die Elemente aus Λ immer ein- und denselben Automorphismus von Λ bzgl. K liefert.

Wegen der Eineindeutigkeit der durch (Ia) oder (Ib) charakterisierten Zuordnung ist insbesondere die Anzahl der Körper Λ zwischen K und N endlich.

Bemerkungen: Zum besseren Verständnis dieses Satzes und seines Beweises werde die eineindeutige Zuordnung (Ia), (Ib) durch die nachstehende Fig. 1 veranschaulicht, in der auf gleicher Höhe stehende Körper und Gruppen einander zugeordnet sein sollen. Speziell sind nach (Ia) K und $\mathfrak{G}$, nach (Ib) N und $\mathfrak{E}$ einander zugeordnet[1]), und es entspricht daher immer dem „bzgl. K" das „in $\mathfrak{G}$" und dem „in N" das „bzgl. $\mathfrak{E}$", wie wir es in der Formulierung des Satzes möglichst deutlich zum Ausdruck zu bringen versuchten. Nach (II) entspricht ferner dem „Aufsteigen" von K zu N das „Absteigen" von $\mathfrak{G}$ zu $\mathfrak{E}$ und den relativen Graden

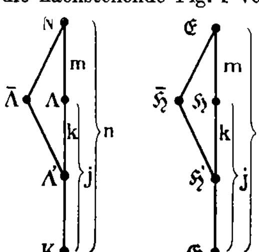

Fig. 1.

[1]) Es ist also nicht, wie man zunächst meinen möchte, N seiner Galoisgruppe $\mathfrak{G}$ zugeordnet. Vielmehr ist $\mathfrak{H}$ die Galoisgruppe von N bzgl. des $\mathfrak{G}$ zugeordneten K, ebenso wie $\mathfrak{H}$ die Galoisgruppe von N bzgl. des $\mathfrak{H}$ zugeordneten Λ ist.

n, m, j, k der Körper die relativen Indizes n, m, j, k der entsprechenden Gruppen, wobei zweckmäßig auch die Ordnungen der Gruppen als Indizes (von $\mathfrak{E}$ in ihnen) aufgefaßt werden. Durch (III) und (IV) rechtfertigt sich, wie in der Bem. zu Satz 99, (II.) [89] angekündigt, die gleiche Wahl der Benennungen normal und konjugiert in Körper- und Gruppentheorie (vgl. jetzt auch die Bem. bei Satz 93 [84]). In (III)—(V) kann (analog zu (II)) das spezielle zugeordnete Paar K, $\mathfrak{G}$ durch irgendein zugeordnetes Paar Λ', $\mathfrak{H}'$ ersetzt werden [1]), wie sich durch Anwendung des ganzen Satzes auf Λ' als Grundkörper und (gemäß (Iaa)) $\mathfrak{H}'$ als Galoisgruppe von N bzgl. Λ' ohne weiteres ergibt (vgl. dazu auch Satz 66, 70 [56, 59]). Dann erscheint (Iaa) als Spezialfall von (V), indem in (V) $\mathfrak{G}$ und $\mathfrak{H}$ durch $\mathfrak{H}$ und $\mathfrak{E}$ und demgemäß K und Λ durch Λ und N ersetzt werden können. In der Tat ist ja $\mathfrak{H}/\mathfrak{E} \cong \mathfrak{H}$.

Teilbeweis (I).

Um zu zeigen, daß durch (Ia), (Ib) ein und dieselbe eineindeutige Zuordnung zwischen allen Λ und allen $\mathfrak{H}$ geliefert wird, genügt es, folgendes festzustellen:

(1a) jedem Λ ist gemäß (Ia) eindeutig ein $\mathfrak{H}$ zugeordnet (Bezeichnung $\Lambda \to \mathfrak{H}$),

(1b) jedem $\mathfrak{H}$ ist gemäß (Ib) eindeutig ein Λ zugeordnet (Bezeichnung $\mathfrak{H} \to \Lambda$),

(2a) aus $\Lambda \to \mathfrak{H}$ folgt $\mathfrak{H} \to \Lambda$,

(2b) aus $\mathfrak{H} \to \Lambda$ folgt $\Lambda \to \mathfrak{H}$.

Denn dann ist für die nach (2a), (2b) dasselbe besagenden eindeutigen Zuordnungen (1a), (1b) das Erfülltsein von **1**, § 2, (δ.), (ε.) [17] durch (1a), von **1**, § 2, (δ'.), (ε'.) [17] durch (1b) garantiert.

(1a) Das ist klar, weil nach **1**, Satz 19 [55] und der Definition des Automorphismenprodukts (Satz 104 [93]) die Menge $\mathfrak{H}$ derjenigen Automorphismen aus $\mathfrak{G}$, die jedes Element aus Λ invariant lassen, eine Untergruppe von $\mathfrak{G}$ ist.

Dabei ist, wie in (Iaa) festgestellt, $\mathfrak{H}$ die Galoisgruppe von

---

[1]) Fig. 1 entspricht einem solchen Fall, wo dies auch für (III) möglich ist, indem Λ, $\bar{\Lambda}$ konjugiert sogar bzgl. Λ' und $\mathfrak{H}$, $\bar{\mathfrak{H}}$ konjugiert sogar bzgl. $\mathfrak{H}'$ angenommen sind.

N bzgl. Λ (Def. 34 [95]) und daher die Ordnung von $\mathfrak{H}$ gleich dem Grade von N über Λ (Satz 105 [96]) und der Index von $\mathfrak{H}$ in $\mathfrak{G}$ gleich dem Grade von Λ über K (Satz 71 [59] und **1**, Satz 25 [59]).

(1b) Das ist klar, weil nach **1**, Satz 6 [19] und den Bedingungen für Automorphismen bzgl. K [Def. 32, (1.), (2.) [93] und Zusatz [94]] die Menge Λ derjenigen Elemente aus N, die bei allen Automorphismen aus $\mathfrak{H}$ invariant bleiben, ein K enthaltender Teilkörper von N ist.

(2a) Sei $\Lambda \to \mathfrak{H}$ gemäß (1a). Dann bilden wir $\mathfrak{H} \to \bar{\Lambda}$ gemäß (1b) und $\bar{\Lambda} \to \bar{\mathfrak{H}}$ gemäß (1a). Es gehören dann die

$$\left\{\begin{array}{l}\text{Elemente aus } \Lambda \\ \text{Automorphismen aus } \mathfrak{H}\end{array}\right\},$$

weil sie nach $\left\{\begin{array}{l}\text{(Ia) bei } \mathfrak{H} \text{ invariant sind} \\ \text{(Ib) die Elemente von } \bar{\Lambda} \text{ invariant lassen}\end{array}\right\}$, nach $\left\{\begin{array}{c}\text{(Ib)} \\ \text{(Ia)}\end{array}\right\}$ zu der Gesamtheit $\left\{\begin{array}{c}\bar{\Lambda} \\ \bar{\mathfrak{H}}\end{array}\right\}$ aller solchen $\left\{\begin{array}{l}\text{Elemente aus } \mathsf{N} \\ \text{Automorphismen aus } \mathfrak{G}\end{array}\right\}$, d. h. es ist $\left\{\begin{array}{c}\Lambda \leqq \bar{\Lambda} \\ \mathfrak{H} \leqq \bar{\mathfrak{H}}\end{array}\right\}$. Aus der ersteren dieser Relationen folgt $[\mathsf{N} : \Lambda] \geqq [\mathsf{N} : \bar{\Lambda}]$ (Satz 70 [59]), aus der letzteren dagegen $[\mathsf{N} : \Lambda] \leqq [\mathsf{N} : \bar{\Lambda}]$, weil $\mathfrak{H}$, $\bar{\mathfrak{H}}$ nach (Iaa) die Galoisgruppen von N bzgl. Λ, $\bar{\Lambda}$ sind, deren Ordnungen nach Satz 105 [96] gleich den Graden von N über Λ, $\bar{\Lambda}$ sind. Somit ergibt sich $[\mathsf{N} : \Lambda] = [\mathsf{N} : \bar{\Lambda}]$, d. h. $\Lambda = \bar{\Lambda}$ (Satz 72 [60]) und nach Wahl von $\bar{\Lambda}$ daher $\mathfrak{H} \to \Lambda$ gemäß (1b), wie in (2a) behauptet.

(2b) Sei $\mathfrak{H} \to \Lambda$ gemäß (1b). Dann bilden wir $\Lambda \to \bar{\mathfrak{H}}$ gemäß (1a).

Einerseits folgt dann wie eben $\mathfrak{H} \leqq \bar{\mathfrak{H}}$. Daraus ergibt sich für die Ordnungen m, $\bar{m}$ von $\mathfrak{H}$, $\bar{\mathfrak{H}}$

$$m \leqq \bar{m}.$$

Andererseits bilden wir mittels eines primitiven Elements ϑ von N das Polynom

$$\psi(x) \equiv (x - \vartheta_{A_1}) \cdots (x - \vartheta_{A_m}),$$

wo $A_1, \ldots, A_m$ die Automorphismen aus $\mathfrak{H}$ sind. Seine Koeffizienten sind symmetrische ganze rationale Funktionen der Wurzeln $\vartheta_{A_\mu} (\mu = 1, \ldots, m)$. Bei Anwendung eines Automorphismus A aus $\mathfrak{H}$ gehen die ϑ_{A_μ} in die $(\vartheta_{A_\mu})_A = \vartheta_{A_\mu A}$ über, erfahren also nur eine Permutation (**1**, Satz 16 [52]). Die Koeffizienten von $\psi(x)$ sind daher bei allen Automorphismen A aus $\mathfrak{H}$ invariant und gehören somit gemäß (Ib) zu Λ. $\psi(x)$ ist also ein Polynom in Λ; es hat $\vartheta = \vartheta_E$ als Wurzel, und sein Grad ist gleich der Ordnung m von $\mathfrak{H}$. Daraus folgt

$$[\mathsf{N} : \Lambda] = [\mathsf{K}(\vartheta) : \Lambda] = [\Lambda(\vartheta) : \Lambda] = [\vartheta : \Lambda] \leqq m$$

(Satz 61, 77 [52, 66], Def. 22 [55], Satz 53 [43]). Nach (Iaa) und Satz 105 [96] folgt aber aus $\Lambda \to \overline{\mathfrak{H}}$, daß $[\mathsf{N} : \Lambda] = \overline{m}$ ist. Somit ergibt sich

$$\overline{m} \leqq m.$$

Zusammengenommen folgt also $m = \overline{m}$, d. h. $\mathfrak{H} = \overline{\mathfrak{H}}$, und nach Wahl von $\overline{\mathfrak{H}}$ daher $\Lambda \to \mathfrak{H}$ gemäß (1a), wie in (2b) behauptet.

Aus $\overline{m} = [\mathsf{N} : \Lambda] = [\mathsf{K}(\vartheta) : \Lambda] = m$ folgt übrigens in Hinblick auf Satz 77 [66] und Def. 22 [55] noch, daß $\psi(x)$ das zu ϑ gehörige irreduzible Polynom in Λ ist.

Wir bezeichnen nunmehr die eindeutigen Zuordnungen (1a), (1b), die nach (2a), (2b) in ein und dieselbe eineindeutige Zuordnung zwischen allen Λ und allen $\mathfrak{H}$ zusammenfallen, durch $\Lambda \longleftrightarrow \mathfrak{H}$.

Teilbeweis (II).

a.) Ist $\Lambda \longleftrightarrow \mathfrak{H}$, $\Lambda' \longleftrightarrow \mathfrak{H}'$ und $\Lambda \geqq \Lambda'$, so lassen nach (Ia) die Automorphismen aus $\mathfrak{H}$ speziell die Elemente des Teilkörpers Λ' von Λ invariant, gehören also nach (Ia) zu der Gesamtheit $\mathfrak{H}'$ aller solchen Automorphismen aus $\mathfrak{G}$. Somit ist dann $\mathfrak{H} \leqq \mathfrak{H}'$.

b.) Ist $\mathsf{\Lambda} \longleftrightarrow \mathfrak{H}$, $\mathsf{\Lambda}' \longleftrightarrow \mathfrak{H}'$ und $\mathfrak{H} \leqq \mathfrak{H}'$, so bleiben nach (Ib) die Elemente aus $\mathsf{\Lambda}'$ speziell bei den Automorphismen aus der Untergruppe $\mathfrak{H}$ von $\mathfrak{H}'$ invariant, gehören also nach (IIb) zu der Gesamtheit $\mathsf{\Lambda}$ aller solchen Elemente aus N. Somit ist dann $\mathsf{\Lambda} \geqq \mathsf{\Lambda}'$.

Daß beidemal der Grad von $\mathsf{\Lambda}$ über $\mathsf{\Lambda}'$ gleich dem Index von $\mathfrak{H}$ in $\mathfrak{H}'$ ist, ergibt sich unmittelbar aus (Iaa), wenn man dort $\mathsf{\Lambda}', \mathfrak{H}'$ statt K, $\mathfrak{G}$ setzt.

Teilbeweis (III).

Dazu bemerken wir zunächst, daß ein Körper $\mathsf{\Lambda}$ zwischen K und N durch einen Automorphismus S von N bzgl. K in einen zu ihm bzgl. K isomorphen, also konjugierten Körper $\mathsf{\Lambda}_S$ zwischen K und N übergeht, wie sich ohne weiteres aus Def. 32, Zusatz [94] und Def. 26 [60] ergibt.

Ist nun $\mathsf{\Lambda} \longleftrightarrow \mathfrak{H}$, $\mathsf{\Lambda}_S \longleftrightarrow \mathfrak{H}_S$ und β ein Element aus $\mathsf{\Lambda}$, β_S das zugeordnete aus $\mathsf{\Lambda}_S$, so folgt aus $\beta_{\mathfrak{H}} = \beta$, daß

$$(\beta_S)_{S^{-1}\mathfrak{H}S} = \beta_{SS^{-1}\mathfrak{H}S} = \beta_{\mathfrak{H}S} = \beta_S,$$

also β_S bei der zu $\mathfrak{H}$ konjugierten Untergruppe $S^{-1}\,\mathfrak{H}\,S$ von $\mathfrak{G}$ invariant ist. Somit ist $S^{-1}\,\mathfrak{H}S \leqq \mathfrak{H}_S$. Da $\mathsf{\Lambda}_S$ wegen $SS^{-1} = E$ durch S^{-1} wieder in $\mathsf{\Lambda}$ übergeht, folgt ebenso $S\mathfrak{H}_S S^{-1} \leqq \mathfrak{H}$, oder auch $\mathfrak{H}_S \leqq S^{-1}\,\mathfrak{H}\,S$. Somit ist $\mathfrak{H}_S = S^{-1}\,\mathfrak{H}\,S$, d. h. $\mathsf{\Lambda}_S \longleftrightarrow S^{-1}\,\mathfrak{H}S$. Um den Beweis von (III) zu vollenden, haben wir also in Hinsicht auf die Eineindeutigkeit unserer Zuordnung nur noch festzustellen, daß durch $S^{-1}\mathfrak{H}\,S$ bzw. $\mathsf{\Lambda}_S$ alle konjugierten zu $\mathfrak{H}$ in $\mathfrak{G}$ bzw. $\mathsf{\Lambda}$ in N repräsentiert werden, wenn S die Gruppe $\mathfrak{G}$ durchläuft.

a.) Für $\mathfrak{H}$ ist das nach **1**, Def. 21 [62] unmittelbar klar.

b.) Für $\mathsf{\Lambda}$ ergibt es sich so: Wird $\mathsf{\Lambda} = \mathsf{K}(\beta)$ gesetzt, so ist $\mathsf{\Lambda}_S = \mathsf{K}(\beta_S)$. Durchläuft nun S die Gruppe $\mathfrak{G}$, so durchläuft β_S alle konjugierten zu β (Satz 105 [96]), also $\mathsf{\Lambda}_S$ alle konjugierten zu $\mathsf{\Lambda}$ (Satz 97 [86]).

Teilbeweis (IV).

Da nach (III) und wegen der Eineindeutigkeit unserer Zuordnung das Zusammenfallen der konjugierten zu $\mathsf{\Lambda}$ und das Zusammenfallen der konjugierten zu $\mathfrak{H}$ für ein zugeordnetes Paar $\mathsf{\Lambda} \longleftrightarrow \mathfrak{H}$ sich gegenseitig bedingen, ergibt sich (IV) unmittelbar aus Satz 99, (II.) [88] einerseits und **1**, Satz 31 [64] andererseits.

Teilbeweis (V).

Es sei $\mathsf{\Lambda} \longleftrightarrow \mathfrak{H}$ und gemäß (IV) $\mathsf{\Lambda}$ Normalkörper über K, $\mathfrak{H}$ Normalteiler von $\mathfrak{G}$. Jeder Automorphismus S aus $\mathfrak{G}$ bewirkt dann wegen $\mathsf{\Lambda}_S = \mathsf{\Lambda}$ (vgl. Teilbeweis (III)) einen Automorphismus P bzgl. K von $\mathsf{\Lambda}$, und da jedes Element von $\mathsf{\Lambda}$ bei $\mathfrak{H}$ invariant ist, wird so durch alle Automorphismen einer Restklasse $\mathfrak{H}S$ ein und derselbe Automorphismus P von $\mathsf{\Lambda}$ bewirkt. Umgekehrt entspringt jeder Automorphismus P bzgl. K von $\mathsf{\Lambda}$ auf diese Weise aus einen Automorphismus S aus $\mathfrak{G}$; denn ist β ein primitives Element von $\mathsf{\Lambda}$, so ist nach Satz 105 [96] β_P eines der konjugierten zu β, und es existiert daher, wiederum nach Satz 105, ein Automorphismus S aus $\mathfrak{G}$, der β in β_P überführt und somit für die Elemente aus $\mathsf{\Lambda} = \mathsf{K}(\beta)$ den Automorphismus P bewirkt. Hiernach sind den sämtlichen Restklassen von $\mathfrak{G}$ nach $\mathfrak{H}$, d. h. den Elementen der Faktorgruppe $\mathfrak{G}/\mathfrak{H}$, eindeutig die sämtlichen Elemente der Galoisgruppe von $\mathsf{\Lambda}$ bzgl. K zugeordnet. Diese Zuordnung ist dann auch eineindeutig, weil die Ordnung von $\mathfrak{G}/\mathfrak{H}$, d. h. der Index von $\mathfrak{H}$ nach (Iaa) gleich dem Grad von $\mathsf{\Lambda}$, nach Satz 105 also gleich der Ordnung der Galoisgruppe von $\mathsf{\Lambda}$ ist. Schließlich erfüllt die betrachtete Zuordnung nach der Erklärung der Restklassenmultiplikation (**1**, Satz 22 [56]) auch die Isomorphiebedingung (**1**, Satz 23 [56]). Somit ist die Galoisgruppe von $\mathsf{\Lambda}$ bzgl. K zur Faktorgruppe $\mathfrak{G}/\mathfrak{H}$ isomorph und entsteht aus ihr auf die in (V) angegebene Weise.

Damit ist der Fundamentalsatz vollständig bewiesen.

Beachten wir, daß sich bei der in ihm angegebenen eineindeutigen Zuordnung nach (II) alle Enthaltensein-Relationen und daher auch auf solche bezügliche Maximal- und Minimaleigenschaften in umgekehrter Folge entsprechen, so erhalten wir die folgenden weiteren Eigenschaften jener Zuordnung:

Satz 110. Ist im Sinne von Satz 109

$$\mathsf{\Lambda}_1 \longleftrightarrow \mathfrak{H}_1, \ldots, \mathsf{\Lambda}_r \longleftrightarrow \mathfrak{H}_r$$

und bezeichnet $[\cdots]$ den Durchschnitt, $\{\cdots\}$ das Kompositum für Körper und Gruppen[1]), so gilt

$$[\mathsf{\Lambda}_1, \ldots, \mathsf{\Lambda}_r] \longleftrightarrow \{\mathfrak{H}_1, \ldots, \mathfrak{H}_r\},$$
$$\{\mathsf{\Lambda}_1, \ldots, \mathsf{\Lambda}_r\} \longleftrightarrow [\mathfrak{H}_1, \ldots, \mathfrak{H}_r].$$

Insbesondere gilt also nach der bei Satz 62 [52] gemachten Bemerkung:

Zusatz. Sind $\alpha_1, \ldots, \alpha_r$ Elemente aus N und ist im Sinne von Satz 109

$$\mathsf{K}(\alpha_1) \longleftrightarrow \mathfrak{H}_1, \ldots, \mathsf{K}(\alpha_r) \longleftrightarrow \mathfrak{H}_r,$$

so gilt

$$\mathsf{K}(\alpha_1, \ldots, \alpha_r) \longleftrightarrow [\mathfrak{H}_1, \ldots, \mathfrak{H}_r].$$

2.) Die Anwendung des Fundamentalsatzes auf die Strukturuntersuchung der Erweiterung N von K ist nach dem eingangs Bemerkten so zu denken, daß man aus der als bekannt anzusehenden[2]) Struktur der Galoisgruppe $\mathfrak{G}$ von N bzgl. K Schlüsse über die Struktur von N über K zieht. Um so den zu untersuchenden Schritt von K nach N durch Einfügung einer Zwischenkörperkette

$$\mathsf{K} = \mathsf{\Lambda}_0 < \mathsf{\Lambda}_1 < \cdots < \mathsf{\Lambda}_s = \mathsf{N}$$

in eine Folge einfacherer Schritte zu zerlegen, hat man ausgehend von einer Untergruppenkette

$$\mathfrak{G} = \mathfrak{H}_0 > \mathfrak{H}_1 > \cdots > \mathfrak{H}_s = \mathfrak{E},$$

die $\mathsf{\Lambda}_i$ als die zugeordneten Zwischenkörper zu den Untergruppen $\mathfrak{H}_i$ zu bestimmen. Das sukzessive Vordringen von

---

[1]) Vgl. hierzu **I**, Satz 7 [20], Def. 5 [20], Satz 21 [55], Def. 15 [56], insbesondere die im Anschl. an Def. 5 gegebene Charakterisierung von Durchschnitt und Kompositum.

[2]) Vgl. Satz 106 [97], jedoch auch die Bem. vor Def. 35 [98] und nach Satz 107 [100].

K nach N ist dann, wenn man die Zwischenstufen Λ_i je als neue Grundkörper ansieht, mit einer sukzessiven Reduktion der Galoisgruppe $\mathfrak{G}$ von N bzgl. K auf die Untergruppen $\mathfrak{H}_i$ verbunden, die ja nach (Iaa) die Galoisgruppen von N bzgl. der Λ_i sind. Der volle Schritt von K nach N ist zurückgelegt, wenn $\mathfrak{G}$ vollständig, d.h. auf $\mathfrak{E}$ reduziert ist. Wählt man insbesondere die $\mathfrak{H}_i$ so, daß $\mathfrak{H}_{i+1}$ Normalteiler von $\mathfrak{H}_i$ ist, so ist nach (IV) Λ_{i+1} Normalkörper über Λ_i, und die diesem Schritt entsprechende Galoisgruppe ist $\mathfrak{H}_i/\mathfrak{H}_{i+1}$.

Um eine Reduktion der Galoisgruppe $\mathfrak{G}$ von N auf eine Untergruppe $\mathfrak{H}$ im angegebenen Sinne zu leisten, hat man den $\mathfrak{H}$ zugeordneten Teilkörper Λ von N zu bestimmen. Dies wird zwar durch die Zuordnungsvorschrift (Ib) geleistet, aber dadurch allein beherrscht man den Körper Λ nicht in dem Maße, wie etwa durch Angabe eines primitiven Elements β von Λ. Für ein solches führen wir die folgende Definition ein:

Definition 36. Ist im Sinne von Satz 109 $\Lambda \longleftrightarrow \mathfrak{H}$ und ist $\Lambda = \mathsf{K}(\beta)$, d. h. ist β ein primitives Element des $\mathfrak{H}$ zugeordneten Λ, so heißt β ein **zu $\mathfrak{H}$ gehöriges Element** aus N.

Auf die Bestimmung eines solchen β aus einem primitiven Element ϑ von N gehen wir hier nicht ein (siehe darüber **3**, § 17, Aufg. 4). Wir leiten nur nachstehend eine Reihe von Tatsachen her, die in dieser Hinsicht von theoretischer Bedeutung sind.

Weil natürlich auch umgekehrt jedes Element β aus N zu einer gewissen Untergruppe $\mathfrak{H}$ von $\mathfrak{G}$ gehört, nämlich der gemäß $\mathsf{K}(\beta) = \Lambda \longleftrightarrow \mathfrak{H}$ (eindeutig) bestimmten, so stellen diese Tatsachen überdies eine Erweiterung und gruppentheoretische Vertiefung der früher gemachten Aussagen über die konjugierten eines algebraischen Elements (Satz 95, 96, 103 [85, 86, 91]) dar.

Satz 111. Unter den Voraussetzungen von Satz 109 sei β ein zur Untergruppe $\mathfrak{H}$ von $\mathfrak{G}$ gehöriges Element aus N, und j der Index von $\mathfrak{H}$ sowie

$$\mathfrak{G} = \mathfrak{H}S_1 + \cdots + \mathfrak{H}S_j$$

die vordere Zerlegung von $\mathfrak{G}$ nach $\mathfrak{H}$. Bei Anwendung der Automorphismen S aus $\mathfrak{G}$ entsteht dann immer durch alle Automorphismen aus einer Restklasse $\mathfrak{H}S$ ein und dasselbe konjugierte $\beta_{\mathfrak{H}S}$ zu β, und die den j Restklassen $\mathfrak{H}S, \ldots, \mathfrak{H}S_j$ entsprechenden konjugierten $\beta_{\mathfrak{H}S_1}, \ldots, \beta_{\mathfrak{H}S_j}$ sind voneinander verschieden; oder, wie man kurz sagt, das Element β ist bei $\mathfrak{H}$ invariant und bei $\mathfrak{G}$ j-wertig.

Insbesondere ist also

$$(1.) \qquad g(x) \equiv (x - \beta_{\mathfrak{H}S_1}) \cdots (x - \beta_{\mathfrak{H}S_j})$$

das zu β gehörige irreduzible Polynom in K.

Beweis: Da gemäß Def. 36 die Elemente von $\Lambda = \mathsf{K}(\beta)$ bei den Automorphismen aus $\mathfrak{H}$ invariant bleiben, gilt speziell $\beta_{\mathfrak{H}} = \beta$ und daher $\beta_{\mathfrak{H}S} = \beta_S$ für jedes S aus $\mathfrak{G}$. Die β_S stellen nun sämtliche konjugierte zu β dar (Satz 103, 105 [91, 96]). Weil ferner nach Satz 109 $\Lambda = \mathsf{K}(\beta)$, also β den Grad j hat, gibt es im ganzen genau j verschiedene konjugierte zu β (Satz 96, 58 [86, 47]). Da aber nach dem bereits Gezeigten unter den β_S höchstens die j Elemente $\beta_{\mathfrak{H}S_\nu} (\nu = 1, \ldots, j)$ voneinander verschieden sind, können unter diesen keine gleichen mehr vorkommen, was die Behauptung ergibt.

Satz 111 läßt sich auch umkehren:

Satz 112. Unter den Voraussetzungen von Satz 109 sei β ein bei der Untergruppe $\mathfrak{H}$ von $\mathfrak{G}$ vom Index j invariantes, bei $\mathfrak{G}$ j-wertiges Element aus N. Dann ist β ein zu $\mathfrak{H}$ gehöriges Element.

Beweis: Ist $\mathsf{K}(\beta) = \Lambda \longleftrightarrow \mathfrak{H}'$, d. h. β ein zu $\mathfrak{H}'$ gehöriges Element, so ist nach (Ia) zunächst $\mathfrak{H} \leqq \mathfrak{H}'$, weil die Elemente aus $\Lambda = \mathsf{K}(\beta)$ nach der Voraussetzung sicherlich bei $\mathfrak{H}$ invariant sind. Ferner ist nach Satz 111 β bei $\mathfrak{G}$ j'-wertig, wo j' den Index von $\mathfrak{H}'$ bezeichnet. Gemäß der Voraussetzung ist also $j' = j$, d. h. $\mathfrak{H}' = \mathfrak{H}$, und somit β ein zu $\mathfrak{H}$ gehöriges Element, wie behauptet.

Bemerkenswert sind die beiden Grenzfälle von Satz 111, 112:

Zusatz. Unter den Voraussetzungen von Satz 109 ist ein Element β aus N dann und nur dann ein primitives Element von N, wenn es bei $\mathfrak{G}$ n-wertig ist, und dann und nur dann ein Element von K, wenn es bei $\mathfrak{G}$ 1-wertig (invariant) ist[1]).

Die in Satz 111 ausgesprochenen Resultate lassen sich (nach Satz 94 [85]) auf den in Satz 95 [85] zugrunde gelegten Sachverhalt anwenden, wenn wieder (wie schon in Satz 103 [91]) das irreduzible Polynom $f(x)$, dessen Stammkörper $\mathsf{\Lambda} = \mathsf{K}(\alpha)$ und Wurzelkörper $\mathsf{W} = \mathsf{K}(\alpha_1, \ldots, \alpha_r)$ studiert werden, als zudem separabel vorausgesetzt wird. Wir beweisen in dieser Hinsicht, in Ergänzung zu Satz 95 und Satz 103:

Satz 113. Es liege der Sachverhalt von Satz 95 [85] vor, und es sei überdies $f(x)$ separabel. Ist dann

$$[\mathsf{K}(\alpha):\mathsf{K}(\beta)] = k, \qquad [\mathsf{K}(\beta):\mathsf{K}] = j,$$

also

$$kj = [\mathsf{K}(\alpha):\mathsf{K}] = r,$$

so zerfallen die zu β konjugierten Elemente $\beta_1, \ldots, \beta_r$ in j verschiedene Serien von je k einander gleichen.

Insbesondere ist also

$$\bar{g}(x) \equiv (x - \beta_1) \cdots (x - \beta_r)$$

ein Polynom in K, das mit dem zu β gehörigen irreduziblen Polynom $g(x)$ in K in der Beziehung steht

$$\bar{g}(x) \equiv g(x)^k.$$

Beweis: Wir wenden auf α, und damit auf $\beta = h(\alpha)$, alle Automorphismen der Galoisgruppe $\mathfrak{G}$ von W an. Es sei (außer den bereits im Satz eingeführten Gradbezeichnungen

[1]) Diese Tatsachen ergeben sich am einfachsten direkt aus dem im Fundamentalsatz festgestellten Zusammenfallen der Zuordnungen (I a) und (I b), wenn man zum Ausdruck bringt, daß K und $\mathfrak{G}$ nicht nur (wie schon in den dort angeschlossenen Bemerkungen hervorgehoben, trivialerweise) gemäß (I a), sondern auch gemäß (I b) zugeordnet sind, und ebenso N und $\mathfrak{E}$ nicht nur gemäß (I b), sondern auch gemäß (I a).

in der Körperreihe $\mathsf{W} \geqq \mathsf{K}(\alpha) \geqq \mathsf{K}(\beta) \geqq \mathsf{K}$)

$$l = [\mathsf{W} : \mathsf{K}(\alpha)], \qquad m = [\mathsf{W} : \mathsf{K}(\beta)], \qquad n = [\mathsf{W} : \mathsf{K}],$$

also

$$lk = m, \qquad mj = n.$$

Nach Satz 111 entsteht nun einerseits aus α durch Anwendung von $\mathfrak{G}$ l-mal die Reihe der r verschiedenen zu α konjugierten $\alpha_1, \ldots, \alpha_r$ (Satz 58 [47]) und daher aus β ebenfalls l-mal die Reihe der konjugierten $\beta_1, \ldots, \beta_r$; andererseits entsteht aber aus β durch $\mathfrak{G}$ nach Satz 111 m-mal die Reihe der j verschiedenen zu β konjugierten. Daher muß die (1-mal gesetzte) Reihe $\beta_1, \ldots, \beta_r$ gerade $k = \frac{m}{l}$-mal diese verschiedenen konjugierten repräsentieren, wie behauptet.

Analog dem Zusatz zu Satz 111, 112 folgt aus Satz 113 noch:

Zusatz. Es liege der Sachverhalt von Satz 95 [85] vor, und es sei überdies $f(x)$ separabel. Dann ist ein Element β aus Λ dann und nur dann ein primitives Element von Λ, wenn die konjugierten $\beta_1, \ldots, \beta_r$ alle voneinander verschieden sind, und dann und nur dann ein Element von K, wenn diese konjugierten alle einander gleich sind.

Im Anschluß an Satz 111 stellen wir ferner fest:

Satz 114. Es sei im Sinne von Satz 109 [101] $\Lambda \longleftrightarrow \mathfrak{H}$. Es sei ferner ϑ ein zu $\mathfrak{E}$ gehöriges und β ein zu $\mathfrak{H}$ gehöriges Element aus N, also $\mathsf{N} = \mathsf{K}(\vartheta)$ und $\Lambda = \mathsf{K}(\beta)$. Es seien schließlich $A_1, \ldots, A_m$ die Elemente von $\mathfrak{H}$ und $\mathfrak{H}S_1, \ldots, \mathfrak{H}S_j$ die vorderen Restklassen von $\mathfrak{G}$ nach $\mathfrak{H}$. Dann gehören die j konjugierten Elemente $\beta_{\mathfrak{H}S_\nu}$ je zu den j konjugierten Untergruppen $S_\nu^{-1}\mathfrak{H}S_\nu$.

Ferner ist

(2.) $\qquad \psi(x) \equiv (x - \vartheta_{A_1}) \cdots (x - \vartheta_{A_m})$

zu ϑ gehörige irreduzible Polynom aus Λ. Das zu ϑ gehörige irreduzible Polynom $q(x)$ aus K besitzt die Zerlegung

$$q(x) \equiv \psi_{\mathfrak{H}S_1}(x) \cdots \psi_{\mathfrak{H}S_j}(x), \tag{3.}$$

wo

$$\psi_{\mathfrak{H}S_\nu}(x) \equiv (x - \vartheta_{A_1 S_\nu}) \cdots (x - \vartheta_{A_m S_\nu}) \qquad (\nu = 1, \ldots, j). \tag{4.}$$

Dabei sind die Faktoren $\psi_{\mathfrak{H}S_\nu}(x)$ die zu $\psi(x)$ konjugierten, also ebenfalls irreduziblen Polynome in den konjugierten Körpern

$$\Lambda_{\mathfrak{H}S_\nu} = \mathsf{K}(\beta_{\mathfrak{H}S_\nu}) \text{ zu } \Lambda.$$

Ist insbesondere $\mathfrak{H}$ Normalteiler von $\mathfrak{G}$, also Λ Normalkörper über K, so stellt demnach (3.) die Zerlegung von $q(x)$ in seine irreduziblen Faktoren (4.) im Körper Λ dar. Diese sind also dann sämtlich von gleichem Grade und setzen sich der Zerlegung von $\mathfrak{G}$ nach $\mathfrak{H}$ entsprechend aus den Linearfaktoren von $q(x)$ zusammen.

Beweis: Die Behauptung über die $\beta_{\mathfrak{H}S_\nu}$ folgt aus (III). Die Behauptung über $\psi(x)$ wurde bereits im Teilbeweis (I) zu Satz 109 unter (2b) gezeigt. Durch Anwendung der Automorphismen S_ν auf $\Lambda_{\mathfrak{H}} = \Lambda$, $\psi_{\mathfrak{H}}(x) \equiv \psi(x)$ folgt schließlich, daß die $\psi_{\mathfrak{H}S_\nu}(x)$ Polynome aus den $\Lambda_{\mathfrak{H}S_\nu}$ sind.

Ist N der Wurzelkörper eines separablen Polynoms $f(x)$ aus K, also $q(x)$ eine Galoissche Resolvente für $f(x)$, so hat man in der älteren Literatur für die in Satz 111, 114 geschilderten Verhältnisse folgende Ausdrucksweise (zu der aber Entsprechendes wie zu Def. 31 [90] zu sagen ist):

Die Galoisgruppe $\mathfrak{G}$ des Polynoms $f(x)$ aus K wird durch Adjunktion einer zur Untergruppe $\mathfrak{H}$ (Index j, Ordnung m) gehörigen Irrationalität β aus N, d. h. bei Zugrundelegung von $\Lambda = \mathsf{K}(\beta)$ als Grundkörper, auf $\mathfrak{H}$ reduziert. Diese Adjunktion wird ermöglicht durch Lösung der Resolvente j-ten Grades (1.) und bewirkt eine Zerfällung (3.) der Galoisschen Resolvente $q(x)$ in irreduzible Faktoren m-ten Grades (4.), die den j konjugierten

Körpern zu $\mathsf{\Lambda} = \mathsf{K}(\beta)$ angehören. Nach der Adjunktion von β bleibt zur Bestimmung einer Wurzel ϑ der Galoisschen Resolvente $q(x)$ noch die Resolvente m-ten Grades (2.), die Galoissche Resolvente von $f(x)$ bzgl. $\mathsf{\Lambda}$, zu lösen, die sich als der dem Körper $\mathsf{\Lambda}$ entsprechende unter den Faktoren (4.) von $q(x)$ ergibt. Ist insbesondere $\mathfrak{H}$ Normalteiler von $\mathfrak{G}$, so ist $\mathsf{\Lambda} = \mathsf{K}(\beta)$ Normalkörper über K und die Resolvente (1.) Galoissche Resolvente für sich selbst mit der Galoisgruppe $\mathfrak{G}/\mathfrak{H}$.

Die konjugierten $\beta_{\mathfrak{H}S_\nu}$ zu β sind zu den konjugierten Untergruppen $S_\nu^{-1}\mathfrak{H}S_\nu$ von $\mathfrak{H}$ gehörige Irrationalitäten aus N. Die gleichzeitige Adjunktion aller konjugierten $\beta_{\mathfrak{H}S_\nu}$, d. h. aller Wurzeln der Hilfsgleichung (1.) reduziert somit nach Satz 110, Zusatz [108] die Galoisgruppe $\mathfrak{G}$ auf den Durchschnitt $[S_1^{-1}\mathfrak{H}S_1, \ldots, S_j^{-1}\mathfrak{H}S_j]$ aller zu $\mathfrak{H}$ konjugierten Untergruppen, d. h. nach **1**, Satz 33 [65] auf einen Normalteiler von $\mathfrak{G}$, wie es nach Satz 94 [85] und Satz 109, (IV) [102] auch sein muß.

3.) Es sei schließlich bemerkt, daß man den Fundamentalsatz auch zur Strukturuntersuchung einer beliebigen (nicht notwendig normalen) separablen Erweiterung $\mathsf{\Lambda}$ endlichen Grades von K verwenden kann. Denn ist $\mathsf{\Lambda} = \mathsf{K}(\alpha)$ und sind $\alpha_1, \ldots, \alpha_r$, die konjugierten zu α, so ist $\mathsf{\Lambda}$ Teilkörper des Normalkörpers $\mathsf{N} = \mathsf{K}(\alpha_1, \ldots, \alpha_r)$ über K. Ist dann $\mathfrak{G}$ dessen Galoisgruppe, $\mathfrak{H}$ die $\mathsf{\Lambda}$ zugeordnete Untergruppe, so stehen die Gruppen zwischen $\mathfrak{G}$ und $\mathfrak{H}$ in eineindeutiger Zuordnung mit den Eigenschaften von Satz 109 [101] zu den Körpern zwischen K und $\mathsf{\Lambda}$. Der Beweis von Satz 113 [111] ist ein Beispiel für diese Behandlungsweise.

A. Loewy[1]) hat des weiteren sogar gezeigt, daß man den ganzen Gedankengang der Galoisschen Theorie von vornherein für eine beliebige endliche separable algebraische Erweiterung $\mathsf{\Lambda} = \mathsf{K}(\alpha_1, \ldots, \alpha_r)$ (wo also $\alpha_1, \ldots \alpha_r$ nicht notwendig die Wurzeln eines Polynoms sind), nicht nur für eine normale, durchführen kann. An Stelle der Automorphismen und Permutationen treten dann Isomorphismen und sog. Transmutationen (eineindeutige Zuordnungen mit bestimmter Zuordnungsrichtung der

[1]) Neue elementare Begründung und Erweiterung der Galoisschen Theorie, Sitzungsber. d. Heidelb. Ak. d. Wiss., Math.-Nat.-Wiss. Kl. 1925.

$\alpha_1, \ldots, \alpha_r$ zu einem System je konjugierter $\alpha_{1\nu_1}, \ldots, \alpha_{r\nu_r}$, vgl. den Beweis von Satz 90 [80]), die nicht mehr eine Gruppe, sondern ein sog. Gruppoid bilden. Auf diese Weise gelangte Loewy übrigens ebenfalls zu einer von dem Satz von den symmetrischen Funktionen unabhängigen Begründung der Galoisschen Theorie (vgl. die erste Anm. zum Beweis von Satz 90).

§ 18. Abhängigkeit vom Grundkörper.

Durch den Fundamentalsatz der Galoisschen Theorie und die daran geknüpften Ausführungen wird die Frage beantwortet, wie die Struktur einer separablen normalen Erweiterung N von endlichem Grade eines Grundkörpers K beeinflußt wird, wenn man von K zu einer in N enthaltenen Erweiterung Λ von K als Grundkörper übergeht. Wir wenden uns jetzt noch der Frage zu, wie sich die Verhältnisse gestalten, wenn man den Grundkörper K durch eine beliebige Erweiterung $\overline{\mathsf{K}}$ von K ersetzt. Diese Frage entspringt, wie die Betrachtungen am Schluß von § 17, aus dem Bestreben, eine vorgelegte Erweiterung N der angegebenen Art von K aus in möglichst einfachen Schritten zu erreichen oder — und darin liegt die Verallgemeinerung gegenüber § 17 — auch nur einzufangen. Man hat dabei vornehmlich im Auge, diesen Schritten irgendeine allgemeine Einfachheitsbedingung aufzuerlegen, die mit dem vorgegebenen N nichts zu tun hat, z. B., wie wir es in V durchführen werden, die Bedingung, durch Adjunktion von Wurzeln $\sqrt[n]{a}$ im speziellen Sinne des Wortes zustande zu kommen.

1.) Ist N der Wurzelkörper W eines Polynoms $f(x) \equiv (x - \alpha_1) \cdots (x - \alpha_r)$ aus K, so hat man bei Übergang zu einer Erweiterung $\overline{\mathsf{K}}$ von K als Grundkörper auch den Wurzelkörper $\mathsf{W} = \mathsf{K}(\alpha_1, \ldots, \alpha_r)$ von $f(x)$ über K durch den erweiterten Wurzelkörper $\overline{\mathsf{W}} = \overline{\mathsf{K}}(\alpha_1, \ldots, \alpha_r)$ von $f(x)$ über $\overline{\mathsf{K}}$ zu ersetzen, und nach Satz 60 [52] ist dann und nur dann $\overline{\mathsf{W}} = \mathsf{W}$, wenn $\overline{\mathsf{K}} \leqq \mathsf{W}$ ist, wenn also der Fall des vorigen Paragraphen vorliegt. Da nach Satz 100 [89] jede Erweiterung N von K der angegebenen Art als Wurzelkörper W eines Polynoms $f(x)$ aus K darstellbar ist, läßt sich auf diese Weise erklären, was unter der Betrachtung von N über einer Erweiterung $\overline{\mathsf{K}}$ von K als Grundkörper zu verstehen ist, nämlich der Übergang zu der Erweiterung $\overline{\mathsf{N}} = \overline{\mathsf{W}}$ von $\overline{\mathsf{K}}$. Diese Erklärung scheint zunächst abhängig von der Wahl des Polynoms $f(x)$ zu sein. Wir beweisen jedoch:

Satz 115. Ist N eine separable normale Erweiterung endlichen Grades von K und $\overline{\mathsf{K}}$ eine beliebige Erweiterung von K, so legen die Wurzelkörper über $\overline{\mathsf{K}}$ aller Polynome aus K, für die N der Wurzelkörper über K ist, sämtlich ein und dieselbe separable normale Erweiterung $\overline{\mathsf{N}}$ endlichen Grades von $\overline{\mathsf{K}}$ fest.

Beweis: Es seien

$$f(x) \equiv (x - \alpha_1) \cdots (x - \alpha_r),$$
$$f^*(x) \equiv (x - \alpha_1^*) \cdots (x - \alpha_{r^*}^*)$$

zwei Polynome aus K, für die N der Wurzelkörper über K ist, und $\overline{\mathsf{N}}, \overline{\mathsf{N}}^*$ die Wurzelkörper für $f(x), f^*(x)$ über $\overline{\mathsf{K}}$. Da dann $\overline{\mathsf{N}}^* = \overline{\mathsf{K}}(\alpha_1^*, \ldots, \alpha_{r^*}^*) \geqq \mathsf{K}(\alpha_1^*, \ldots, \alpha_{r^*}^*) = \mathsf{N} = \mathsf{K}(\alpha_1, \ldots, \alpha_r)$ ist, enthält $\overline{\mathsf{N}}^*$ einerseits $\overline{\mathsf{K}}$, andererseits $\alpha_1, \ldots, \alpha_r$, also auch $\overline{\mathsf{K}}(\alpha_1, \ldots, \alpha_r) = \overline{\mathsf{N}}$, d. h. es ist $\overline{\mathsf{N}}^* \geqq \overline{\mathsf{N}}$. Ebenso folgt $\overline{\mathsf{N}} \geqq \overline{\mathsf{N}}^*$. Somit ist $\overline{\mathsf{N}} = \overline{\mathsf{N}}^*$.

Die demnach von der Wahl des Polynoms $f(x)$ unabhängige Erweiterung $\overline{\mathsf{N}}$ von $\overline{\mathsf{K}}$ ist natürlich separabel und normal von endlichem Grade über $\overline{\mathsf{K}}$ (Satz 100 [89]).

Die Erweiterung $\overline{\mathsf{N}}$ von $\overline{\mathsf{K}}$ aus Satz 115 ist durch die Eigenschaft, Wurzelkörper über $\overline{\mathsf{K}}$ für alle Polynome aus K zu sein, für die N Wurzelkörper über K ist, in demselben Sinne eindeutig[1]) bestimmt, wie der Wurzelkörper eines Polynoms gemäß Satz 87, 89 [73, 76], d. h. irgend zwei solche Erweiterungen von $\overline{K}$ sind bzgl. $\overline{K}$ isomorph, und keine Erweiterung von $\overline{K}$ enthält zwei verschiedene solche Erweiterungen. Wir können daher definieren:

Definition 37. Die durch $K, N, \overline{K}$ eindeutig bestimmte Erweiterung $\overline{N}$ von $\overline{K}$ aus Satz 115 heißt **die Erweiterung N von K betrachtet über $\overline{K}$ als Grundkörper.**

Es ist für uns wichtig, diese Erweiterung $\overline{N}$ noch auf eine andere Weise zu charakterisieren:

Satz 116. Ist unter den Voraussetzungen von Satz 115 $\overline{N}$ die Erweiterung N von K betrachtet über $\overline{K}$ als Grundkörper, so gilt:

1.) $\overline{N}$ enthält N,

2.) kein Körper zwischen $\overline{K}$ und $\overline{N}$ außer N selbst enthält N.

$\overline{N}$ ist durch 1.), 2.) eindeutig bestimmt.

Beweis: a.) Daß 1.), 2.) für $\overline{N}$ gelten, folgt unmittelbar aus der zur Definition benutzten Eigenschaft von $\overline{N}$ sowie aus der Minimaleigenschaft der Wurzelkörper (Satz 88 [75]).

b.) Es habe die Erweiterung $\overline{N}^*$ von $\overline{K}$ die Eigenschaften 1.), 2.). Dann enthält $\overline{N}^*$ nach 1.) die Wurzeln $\alpha_1, \ldots, \alpha_r$ jedes Polynoms $f(x)$ aus K, für das N der Wurzelkörper über K ist, also auch den Körper $\overline{N}$ aus Satz 115. Es ist dann also $\overline{N}$ ein Körper zwischen $\overline{K}$ und $\overline{N}^*$, der N enthält, und daher $\overline{N} = \overline{N}^*$, weil 2.) für $\overline{N}^*$ vorausgesetzt ist.

[1]) Diese Eindeutigkeit ist wesentlich beingt durch die Normalität von N. Für beliebige Erweiterungen endlichen Grades $\Lambda = K(\alpha_1, \ldots, \alpha_r)$, wo $\alpha_1, \ldots, \alpha_r$ nicht notwendig die Wurzeln eines Polynoms aus K sind, würde sich bei Betrachtung über $\overline{K}$ die Unterscheidung der konjugierten zu $\overline{\Lambda} = \overline{K}(\alpha_1, \ldots, \alpha_r)$ notwendig machen.

Die Eigenschaften 1.), 2.) besagen, daß $\overline{N}$ der engste N und $\overline{K}$ enthaltende Teilkörper von $\overline{N}$, also das Kompositum $\{N, \overline{K}\}$ ist.

Da hierbei $\overline{N}$ selbst als der zum Zustandekommen des Kompositums $\{N, \overline{K}\} = \overline{N}$ erforderliche, N und $\overline{K}$ gemeinsam enthaltende Hilfskörper (Körper K von **1**, Def. 5 [20]) anzusehen ist, kann $\overline{N}$ nicht von vornherein als das Kompositum $\{N, \overline{K}\}$ definiert werden. Vielmehr wird die Darstellung von $\overline{N}$ als Kompositum $\{N, \overline{K}\}$ erst durch die gemäß Satz 115 ausgeführte Konstruktion von $\overline{N}$ ermöglicht, und die bestimmte Ausdrucksweise „das Kompositum $\{N, \overline{K}\}$" erst durch die in Satz 115 bewiesene eindeutige Bestimmtheit von $\overline{N}$ allein durch N und $\overline{K}$. Wir geben diesem logischen Verhältnis, daß die Körper N und $\overline{K}$ vor der gemäß Satz 115 vollzogenen Komposition voneinander „frei", d. h. nicht in einer gemeinsamen Erweiterung enthalten sind, im Anschluß an Def. 37 wie folgt Ausdruck:

Zusatz zu Definition 37. Die im Sinne von Satz 115 und Def. 37 verstandene Erweiterung N von K, betrachtet über $\overline{K}$ als Grundkörper, heißt auch das **freie Kompositum** von N und $\overline{K}$ (Bezeichnung $\{N, \overline{K}\}$).

Zum besseren Verständnis sei noch angefügt, daß man das freie Kompositum von vornherein als das gewöhnliche Kompositum von N und $\overline{K}$ definieren kann, wenn man von der durch Steinitz bewiesenen Existenz und Eindeutigkeit des Körpers $\overline{A}$ aller algebraischen Elemente über $\overline{K}$ (siehe § 11) Gebrauch macht. Denn dann kann dieser Körper $\overline{A}$, der auch den Körper A aller algebraischen Elemente über K, also insbesondere den Körper N enthält, als Hilfskörper für die Komposition von N und $\overline{K}$ zugrunde gelegt werden [1]).

[1]) Dasselbe geht dann auch für eine beliebige algebraische Erweiterung Λ von K, und sogar eindeutig, da die „von unten her", d. h. bei freier Komposition durch ein Satz 115 verallgemeinerndes Verfahren, nicht zu unterscheidenden konjugierten zu $\overline{\Lambda} = \{\Lambda, \overline{K}\}$ „von oben her", d. h. innerhalb $\overline{A}$ von vornherein unterschieden sind.

Die in Satz 116 erhaltene Charakterisierung der Erweiterung N von K betrachtet über $\overline{\mathsf{K}}$ als freies Kompositum $\{\mathsf{N}, \overline{\mathsf{K}}\}$ ist für uns deshalb wichtig, weil sie zeigt, daß der in Satz 115 und Def. 37 eingehende Grundkörper K in Wahrheit nur die Rolle eines Hilfskörpers spielt. Da nämlich in Satz 116, 1.), 2.) von K gar nicht die Rede ist, gilt:

Satz 117. Ist N eine separable normale Erweiterung endlichen Grades von K, $\overline{\mathsf{K}}$ eine Erweiterung von K und $\overline{\mathsf{N}}$ die Erweiterung N von K betrachtet über $\overline{\mathsf{K}}$, so ist $\overline{\mathsf{N}}$ auch die Erweiterung N von K^* betrachtet über $\overline{\mathsf{K}}$, wenn K^* irgendeinen gemeinsamen Teilkörper von N und $\overline{\mathsf{K}}$ bezeichnet, über dem N separabel und normal von endlichem Grade ist.

Insbesondere kann also auch der weiteste gemeinsame Teilkörper von N und $\overline{\mathsf{K}}$, d. h. der Durchschnitt $[\mathsf{N}, \overline{\mathsf{K}}]$ als Grundkörper angesehen werden, für den ja die erforderlichen Bedingungen erfüllt sind (Satz 70, 92, 93 [59, 83, 84]). Um weiterhin mit den Bezeichnungen von § 17 in Einklang zu kommen, schreiben wir jetzt $\overline{\mathsf{\Lambda}}$ statt $\overline{\mathsf{K}}$, so daß $\overline{\mathsf{N}} = \{\mathsf{N}, \overline{\mathsf{\Lambda}}\}$ ist, setzen $\mathsf{\Lambda} = [\mathsf{N}, \overline{\mathsf{\Lambda}}]$ und veranschaulichen die in Betracht zu ziehenden Körper und ihre Beziehungen zueinander, in sinngemäßer Ausdehnung der in Fig 1 zu Satz 109 [102] verwendeten zeichnerischen Veranschaulichung, durch die nebenstehende Fig. 2. Nach Satz 117 hat dann $\overline{\mathsf{N}}$ die Eigenschaft von Satz 115 auch für $\mathsf{\Lambda}$ als Grundkörper. Ferner gilt wegen der Symmetrie des Kompositums $\{\mathsf{N}, \overline{\mathsf{\Lambda}}\}$ in N und $\overline{\mathsf{\Lambda}}$:

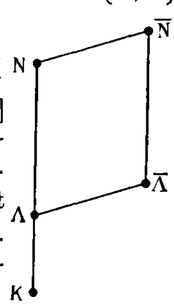

Fig. 2.

Satz 118. Sind N und $\overline{\mathsf{\Lambda}}$ separable normale Erweiterungen endlichen Grades von K, so ist das freie Kompositum $\overline{\mathsf{N}} = \{\mathsf{N}, \overline{\Lambda}\}$ sowohl die Erweiterung N von K betrachtet über $\overline{\Lambda}$ als auch die Erweiterung $\overline{\Lambda}$ von K betrachtet über N. Es ist dann also $\overline{\mathsf{N}}$ sowohl über $\overline{\Lambda}$ als auch über N separabel und normal von endlichem Grade.

2.) Wir beweisen nunmehr den folgenden Hauptsatz, der unsere eingangs gestellte Frage vollständig beantwortet:

Satz 119. Es sei N eine separable normale Erweiterung endlichen Grades von K und $\mathfrak{G}$ die Galoisgruppe von N bzgl. K. Ferner sei $\overline{\Lambda}$ irgendeine Erweiterung von K und

$$\overline{\mathsf{N}} = \{\mathsf{N}, \overline{\Lambda}\}, \Lambda = [\mathsf{N}, \overline{\Lambda}] .$$

Schließlich sei $\mathfrak{H}$ die dem Körper Λ zwischen K und N zugeordnete Untergruppe von $\mathfrak{G}$.

(I) Dann ist die Galoisgruppe $\overline{\mathfrak{H}}$ von $\overline{\mathsf{N}}$ bzgl. $\overline{\Lambda}$ isomorph zur Galoisgruppe $\mathfrak{H}$ von N bzgl. Λ. Es lassen sich nämlich die Automorphismen aus $\mathfrak{H}$ und $\overline{\mathfrak{H}}$ erzeugen:

a.) Durch ein und dieselben Substitutionen irgendeines primitiven Elements ϑ von N bzgl. Λ (also speziell eines solchen von N bzgl. K).

b.) Durch ein und dieselben Permutationen der Wurzeln $\alpha_1, \ldots, \alpha_r$ irgendeines Polynoms $\varphi(x)$ aus Λ, für das N der Wurzelkörper über Λ ist (also speziell eines solchen aus K, für das N der Wurzelkörper über K ist).

Insbesondere ist hiernach (Fig. 3)

$$[\overline{\mathsf{N}} : \overline{\Lambda}] = [\mathsf{N} : \Lambda] ,$$

und wenn $\overline{\Lambda}$ von endlichem Grade über Λ ist, auch

$$[\overline{\mathsf{N}} : \mathsf{N}] = [\overline{\Lambda} : \Lambda] .$$

(II) Ordnet man die Körper Λ^* zwischen Λ und N und die Körper $\overline{\Lambda}^*$ zwischen $\overline{\Lambda}$ und $\overline{\mathsf{N}}$ auf Grund des unter (I) beschriebenen Isomorphismus zwischen $\mathfrak{H}$ und $\overline{\mathfrak{H}}$ und gemäß Satz 109 [101] einander zu, so ist das eine eineindeutige Zuordnung zwischen den Λ^* und $\overline{\Lambda}^*$, bei der die Relationen „ent-

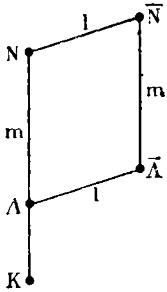

Fig. 3.

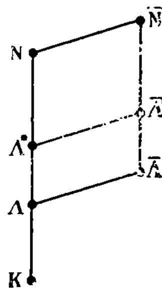

Fig. 4.

halten, konjugiert, normal", soweit sie sich auf einander zugeordnete Körper und Grundkörper der angegebenen Art beziehen, einander entsprechen. Bei dieser Zuordnung ist überdies (Fig. 4)

$$\Lambda^* = [\mathsf{N}, \overline{\Lambda}^*], \quad \overline{\mathsf{N}} = \{\mathsf{N}, \overline{\Lambda}^*\},$$
$$\Lambda = [\Lambda^*, \overline{\Lambda}], \quad \overline{\Lambda}^* = \{\Lambda^*, \overline{\Lambda}\}.$$

(III) Ist speziell $\overline{\Lambda}$ normal über K, so ist auch Λ normal über K (aber nicht notwendig umgekehrt).

Teilbeweis (I).

a.) [1]. Es sei ϑ ein primitives Element von N bzgl. Λ und $\psi(x)$ bzw. $\overline{\psi}(x)$ das zugehörige irreduzible Polynom aus Λ bzw. $\overline{\Lambda}$. Dann ist zunächst $\overline{\psi}(x)$ ein Teiler von $\psi(x)$ (Satz 53

[1]) Man vergegenwärtige sich zu diesem Beweis, daß die Elemente von N zu $\overline{\mathsf{N}}$ gehören (Satz 116, 1 [117]), also mit denen von $\overline{\Lambda}$ in rechnerische Beziehungen gesetzt werden können. Ohne das Vorhandensein einer gemeinsamen Erweiterung von N und $\overline{\Lambda}$ wäre das unzulässig. Es könnte dann z. B. das Polynom $\overline{\psi}(x)$ nicht wie im Text definiert werden.

[43]). Da ferner $\psi(x)$ in N in Linearfaktoren zerfällt (Satz 93 [84]; 98 [87]; 99, (III.) [88]), ist $\overline{\psi}(x)$ ein Produkt aus gewissen dieser Linearfaktoren, also auch Polynom in N. Somit gehört $\overline{\psi}(x)$ sogar zum Durchschnitt $\Lambda = [\mathsf{N}, \overline{\Lambda}]$. Wegen der Irreduzibilität von $\psi(x)$ ist also $\overline{\psi}(x) \equiv \psi(x)$.

Aus $\overline{\mathsf{N}} = \{\mathsf{N}, \overline{\Lambda}\} = \{\Lambda(\vartheta), \overline{\Lambda}\} = \overline{\Lambda}(\vartheta)$ folgt ferner, daß ϑ auch primitives Element von $\overline{\mathsf{N}}$ bzgl. $\overline{\Lambda}$ ist.

Hieraus und aus der zuvor bewiesenen Tatsache $\overline{\psi}(x) \equiv \psi(x)$ ergibt sich die Behauptung (I) a.) nach Satz 105 [96].

b.) Ist N der Wurzelkörper von $\varphi(x) \equiv (x - \alpha_1) \cdots (x - \alpha_r)$ über Λ, also $\overline{\mathsf{N}}$ der Wurzelkörper von $\varphi(x)$ über $\overline{\Lambda}$ (Satz 115, 117), so werden nach Satz 107 [98] die Automorphismen der Galoisgruppe $\mathfrak{H}$ bzw. $\overline{\mathfrak{H}}$ erzeugt durch diejenigen Permutationen der verschiedenen unter den $\alpha_1, \ldots, \alpha_r$, bei deren Anwendung jede bestehende ganz-rationale Beziehung $\chi(\alpha_1, \ldots, \alpha_r) = 0$ bzw. $\overline{\chi}(\alpha_1, \ldots, \alpha_r) = 0$ mit Koeffizienten aus Λ bzw. $\overline{\Lambda}$ in eine ebenfalls richtige übergeht. Die Gruppen $\mathfrak{P}$ bzw. $\overline{\mathfrak{P}}$ dieser Permutationen, die zu $\mathfrak{H}$ bzw. $\overline{\mathfrak{H}}$ isomorph sind, sind wegen der durch a.) bewiesenen Isomorphie von $\mathfrak{H}$ und $\overline{\mathfrak{H}}$ auch zueinander isomorph, haben also insbesondere die gleiche, endliche Ordnung. Da nun die Permutationen aus $\overline{\mathfrak{P}}$ die genannte, auf den Körper $\overline{\Lambda}$ bezügliche Eigenschaft a fortiori für den Teilkörper Λ haben, weil die Relationen $\chi(\alpha_1, \ldots, \alpha_r) = 0$ unter den Relationen $\overline{\chi}(\alpha_1, \ldots, \alpha_r) = 0$ vorkommen, ist $\overline{\mathfrak{P}} \leqq \mathfrak{P}$ und somit nach obigem $\overline{\mathfrak{P}} = \mathfrak{P}$, wie unter (I) b.) behauptet.

Die unter (I) genannten Gradrelationen ergeben sich ohne weiteres aus Satz 109, (Iaa) [101], bzw. doppelter Anwendung von Satz 71 [59] gemäß Fig. 3.

Teilbeweis (II).

Der erste Teil der Behauptung (II) ist nach (I) und Satz 109 [101] klar. Sei ferner $\Lambda^*, \overline{\Lambda}^*$ ein demgemäß zugeordnetes Körperpaar. Wir schließen dann unter Ausnutzung der elementaren Eigenschaften von Durchschnitt und Kompositum so:

Erstens ist $\Lambda^* = [\mathsf{N}, \overline{\Lambda}^*]$. Sind nämlich $\mathfrak{H}^*, \overline{\mathfrak{H}}^*$ die

$\mathsf{\Lambda}^*, \overline{\mathsf{\Lambda}}^*$ zugeordneten Untergruppen von $\mathfrak{H}, \overline{\mathfrak{H}}$ und ϑ ein primitives Element von N bzgl. $\mathsf{\Lambda}$, also nach dem Beweis für (I) a.) auch von $\overline{\mathsf{N}}$ bzgl. $\overline{\mathsf{\Lambda}}$, so besteht $\mathsf{\Lambda}^*$ bzw. $\overline{\mathsf{\Lambda}}^*$ nach unserer Zuordnungsvorschrift in (II) und nach Satz 109, (Ib) [101] aus allen rationalen Funktionen über $\mathsf{\Lambda}$ bzw. $\overline{\mathsf{\Lambda}}$ von ϑ, die bei $\mathfrak{H}^*$ bzw. $\overline{\mathfrak{H}}^*$ invariant sind. Nach (I) a.) ist daher $\mathsf{\Lambda}^* \leqq \overline{\mathsf{\Lambda}}^*$, und somit auch $\mathsf{\Lambda}^* \leqq [\mathsf{N}, \overline{\mathsf{\Lambda}}^*]$. Da umgekehrt die Elemente des Durchschnitts $[\mathsf{N}, \overline{\mathsf{\Lambda}}^*]$ als solche von N rationale Funktionen von ϑ über $\mathsf{\Lambda}$ sind und als solche von $\overline{\mathsf{\Lambda}}^*$ bei $\overline{\mathfrak{H}}^*$ invariant sind, sind sie nach (I) a.) bei $\mathfrak{H}^*$ invariant, d. h. es ist auch $[\mathsf{N}, \overline{\mathsf{\Lambda}}^*] \leqq \mathsf{\Lambda}^*$. Zusammengenommen ergibt sich also $\mathsf{\Lambda}^* = [\mathsf{N}, \overline{\mathsf{\Lambda}}^*]$, wie behauptet.

Zweitens folgt $\overline{\mathsf{N}} = \{\mathsf{N}, \overline{\mathsf{\Lambda}}^*\}$ trivialerweise aus $\overline{\mathsf{N}} \geqq \{\mathsf{N}, \overline{\mathsf{\Lambda}}^*\} \geqq \{\mathsf{N}, \overline{\mathsf{\Lambda}}\} = \overline{\mathsf{N}}$.

Drittens folgt $\mathsf{\Lambda} = [\mathsf{\Lambda}^*, \overline{\mathsf{\Lambda}}]$ trivialerweise aus $\mathsf{\Lambda} \leqq [\mathsf{\Lambda}^*, \overline{\mathsf{\Lambda}}] \leqq [\mathsf{N}, \overline{\mathsf{\Lambda}}] = \mathsf{\Lambda}$.

Viertens ist $\overline{\mathsf{\Lambda}}^* = \{\mathsf{\Lambda}^*, \overline{\mathsf{\Lambda}}\}$. Aus der zuvor bewiesenen Relation $\mathsf{\Lambda}^* \leqq \overline{\mathsf{\Lambda}}^*$ folgt nämlich jedenfalls $\overline{\mathsf{\Lambda}}^* \geqq \{\mathsf{\Lambda}^*, \overline{\mathsf{\Lambda}}\}$. Wäre nun $\overline{\mathsf{\Lambda}}^* > \{\mathsf{\Lambda}^*, \overline{\mathsf{\Lambda}}\}$, so ergäbe die Ausführung der im ersten Teil von (II) festgestellten eineindeutigen Zuordnung mittels des unter „erstens" bereits als gültig erwiesenen Durchschnittsmechanismus auch

$$\mathsf{\Lambda}^* = [\mathsf{N}, \overline{\mathsf{\Lambda}}^*] > [\mathsf{N}, \{\mathsf{\Lambda}^*, \overline{\mathsf{\Lambda}}\}],$$

während doch trivialerweise $\mathsf{\Lambda}^* \leqq [\mathsf{N}, \{\mathsf{\Lambda}^*, \overline{\mathsf{\Lambda}}\}]$ ist.

Durch die letzteren Nachweise rechtfertigt sich die Art, wie in Fig. 4 die Querverbindung zwischen $\mathsf{\Lambda}^*$ und $\overline{\mathsf{\Lambda}}^*$ gezogen ist.

Teilbeweis (III).

Ist neben N auch $\overline{\mathsf{\Lambda}}$ normal über K, so sind die konjugierten bzgl. K zu einem primitiven Element des Durchschnitts

$\Lambda = [\mathsf{N}, \overline{\Lambda}]$ nach Satz 98 [87]; 99, (III.) [88]; 103 [91] sowohl in N als auch in $\overline{\Lambda}$, also auch im Durchschnitt Λ enthalten. Nach denselben Sätzen ist daher dann Λ normal über K. Damit ist Satz 119 bewiesen.

3.) Das in Satz 119 unter (I) ausgesprochene Resultat besagt im Anschluß an die Ausführungen in § 17, 2.) [108], daß die Galoisgruppe $\mathfrak{G}$ von N bzgl. K durch Übergang zu einer beliebigen Erweiterung $\overline{\Lambda}$ von K als Grundkörper ebenso reduziert wird, wie durch Übergang zu dem Durchschnitt $\Lambda = [\mathsf{N}, \overline{\Lambda}]$, d. h. dem in N enthaltenen Teil Λ von $\overline{\Lambda}$.

Da hiernach die Adjunktion von nicht in N enthaltenen Elementen zu K den Aufbau von N nicht weiter fördert als die Adjunktion von geeigneten in N enthaltenen Elementen zu K, nennt man nach Kronecker die ersteren (soweit über K algebraisch) akzessorische Irrationalitäten, die letzteren natürliche Irrationalitäten für die Erweiterung N von K. Daß man trotz der in Satz 119, (I) erhaltenen Ergebnisse bei gewissen Untersuchungen akzessorische Irrationalitäten heranziehen muß, liegt daran, daß sehr wohl die Adjunktion einer akzessorischen Irrationalität einer vorgeschriebenen Einfachheitsbedingung genügen kann, während dies für die Adjunktion einer gemäß Satz 119, (I) äquivalenten natürlichen Irrationalität nicht der Fall ist.

Das in Satz 119, (II) ausgesprochene Resultat besagt, daß der nach Übergang zu $\overline{\Lambda}$ als Grundkörper zum Einfangen von N noch zu machende Schritt von $\overline{\Lambda}$ nach $\overline{\mathsf{N}}$ [vgl. Satz 116, 2.)] dem Schritt von Λ nach N in jeder für uns in Frage kommenden Hinsicht äquivalent ist, und daß überdies dabei jedes im Sinne von Satz 119, (II) einander zugeordnete Körperpaar Λ^* und $\overline{\Lambda}^*$ die Rollen von Λ und $\overline{\Lambda}$ übernehmen kann.

Legt man nun in Verallgemeinerung der Ausführungen in § 17, 2.) [108] eine beliebige Erweiterungskette

$$\text{(1.)} \qquad \mathsf{K} = \overline{\Lambda}_0 < \overline{\Lambda}_1 < \overline{\Lambda}_2 < \cdots < \overline{\Lambda}_r$$

zugrunde, so entspricht dem eine Kette

(2.) $\quad \mathsf{K} = \Lambda_0 \leqq \Lambda_1 \leqq \Lambda_2 \leqq \cdots \leqq \Lambda_r \leqq \mathsf{N}$

von Körpern zwischen K und N, deren Zustandekommen wir durch die nachstehende Fig. 5 veranschaulichen.

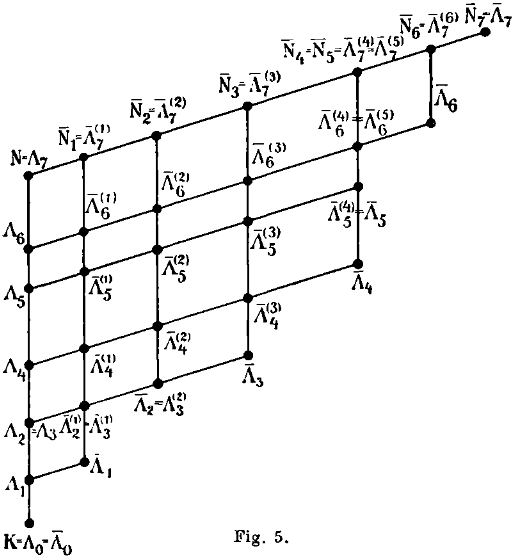

Fig. 5.

Nach der sukzessiven Konstruktion ist dabei

(3.) $\quad \overline{\mathsf{N}}_i = \{\overline{\mathsf{N}}_{i-1}, \overline{\Lambda}_i\}, \qquad \overline{\Lambda}_i^{(i-1)} = [\overline{\mathsf{N}}_{i-1}, \overline{\Lambda}_i]$,

und es sind die Körper $\overline{\Lambda}_i^{(i-1)}, \overline{\Lambda}_i^{(i-2)}, \ldots, \overline{\Lambda}_i^{(1)}, \Lambda_i$ die $\overline{\Lambda}_i^{(i-1)}$ im Sinne von Satz 119, (II) zugeordneten Teilkörper von $\overline{\mathsf{N}}_{i-1}, \overline{\mathsf{N}}_{i-2}, \ldots, \overline{\mathsf{N}}_1, \mathsf{N}$.

Aus Satz 119, (III) folgt, daß dabei $\overline{\Lambda}_i^{(i-1)}$ über $\overline{\Lambda}_{i-1}$, also nach Satz 119, (II) auch Λ_i über Λ_{i-1} normal ist, wenn $\overline{\Lambda}_i$ über $\overline{\Lambda}_{i-1}$ normal ist (aber nicht notwendig umgekehrt).

Durch sukzessive Anwendung von Satz 119, (II) unter Berücksichtigung der Minimaleigenschaft des Kompositums (**1**, hinter Def. 5 [21] oder **2**, Satz 116, 2.)) und der Maximaleigenschaft des Durchschnitts (**1**, hinter Def. 5) ergibt sich ferner leicht, daß in jedem Parallelogramm unserer schematischen Figur (mag es eine „Grundmasche" sein oder aus mehreren „Grundmaschen" zusammengesetzt) der Körper links unten der Durchschnitt und der Körper rechts oben das Kompositum der beiden Körper links oben und rechts unten ist. Insbesondere bestehen also neben den rekursiven Darstellungen (3.) auch die alle Zwischenschritte überschlagenden Darstellungen

$$(4.)\qquad \overline{\mathsf{N}}_i = \{\mathsf{N}, \overline{\Lambda}_i\}, \qquad \Lambda_i = [\mathsf{N}, \overline{\Lambda}_i]\,,$$

aus denen nach Satz 119, (I) folgt, daß das sukzessive Aufsteigen zu den Grundkörpern der Kette (1.) mit einer sukzessiven Reduktion der Galoisgruppe $\mathfrak{G}$ von N bzgl. K auf die der Kette (2.) nach dem Fundamentalsatz zugeordnete Untergruppenkette

$$(5.)\qquad \mathfrak{G} = \mathfrak{H}_0 \geqq \mathfrak{H}_1 \geqq \mathfrak{H}_2 \geqq \cdots \geqq \mathfrak{H}_r \geqq \mathfrak{E}$$

verbunden ist. Nach (4.) und den Eigenschaften von Kompositum und Durchschnitt ist dann und nur dann, wenn einmal $\Lambda_r = \mathsf{N}$ und damit $\overline{\Lambda}_r = \overline{\mathsf{N}}_r$ ist, d. h. wenn gemäß (5.) die Galoisgruppe $\mathfrak{G}$ auf $\mathfrak{H}_r = \mathfrak{E}$ reduziert ist, $\overline{\Lambda}_r \geqq \mathsf{N}$, d. h. N, wie es als Ziel vorschwebte, durch die Kette (1.) eingefangen.

V. Auflösbarkeit algebraischer Gleichungen durch Wurzelzeichen.

Die in IV entwickelte Theorie verdankt ihre Entstehung und bildet demgemäß die Grundlage für die Behandlung der schon zu Beginn von § 18 erwähnten, berühmten Frage, *unter welchen Bedingungen eine algebraische Gleichung durch Wurzelzeichen auflösbar ist.* Deren Beantwortung für Grundkörper der Charakteristik 0 ist der vorliegende, letzte Abschnitt gewidmet. Wir präzisieren dazu zunächst die Frage durch die Definition der Auflösbarkeit durch Wurzelzeichen (§ 19), entwickeln sodann als notwendige Hilfsmittel die Theorie der Kreisteilungskörper (§ 20) sowie der reinen und der zyklischen Erweiterungen von Primzahlgrad (§ 21) und leiten darauf durch Anwendung der in IV behandelten Galoisschen Theorie ein gruppentheoretisches Kriterium für die Auflösbarkeit durch Wurzelzeichen her (§ 22). Schließlich skizzieren wir noch den durch die Galoissche Theorie gelieferten Beweis für die auf anderem Wege zuerst von Abel gefundene Nichtauflösbarkeit durch Wurzelzeichen der allgemeinen algebraischen Gleichung höheren als vierten Grades (§ 23).

In § 20 fügen wir einen kurzen Abriß der Theorie der endlichen Körper an und beseitigen dabei insbesondere die in dieser Hinsicht im Beweis von Satz 90 [80] noch gebliebene Unvollständigkeit.

§ 19. Definition der Auflösbarkeit durch Wurzelzeichen.

Wir geben in diesem Paragraphen eine exakte Formulierung dafür, was unter der Ausdrucksweise durch Wurzelzeichen auflösbar zu verstehen ist. Der aus den Elementen geläufige Begriff $\sqrt[n]{a}$, wo a ein Element eines Körpers K und n eine natürliche Zahl ist, wird dort bekanntlich als Lösung der Gleichung $x^n - a \doteq 0$ erklärt. Wegen der hierbei i. a. vorliegenden Mehrdeutigkeit wollen wir die Bezeichnung $\sqrt[n]{a}$ nicht verwenden, operieren vielmehr an Stelle des Wurzelzeichens mit der zugehörigen Gleichung:

Definition 38. Ein **Polynom** der Form $x^n - a$ heißt **rein.**

Damit die zu Eingang dieses Abschnitts gestellte Frage nicht trivial wird, hat man natürlich neben der in ihr genannten Operation des Wurzelziehens auch die, von diesem Standpunkte aus untergeordneten, vier elementaren Rechenoperationen mit in den Kreis der zulässigen Operationen aufzunehmen[1]). Mit einer Wurzel α eines reinen Polynoms gelten dann also auch alle ihre rationalen Funktionen über dem Grundkörper K, d. h. alle Elemente von $\mathsf{K}(\alpha)$ als bekannt. Der Sinn unserer Frage geht aber noch weiter: Es wäre unsystematisch, wenn man der Operation des Wurzelziehens nach einem solchen Schritt Halt gebieten wollte. Vielmehr ist es vernünftig, weiter auch die Wurzeln reiner, dem so erreichten Körper $\mathsf{K}(\alpha)$ angehöriger Polynome als bekannt anzusehen usf. Unsere Frage kommt dann also darauf hinaus, unter welchen Bedingungen man die Wurzeln, d. h. den Wurzelkörper eines Polynoms $f(x)$ aus K oder allgemeiner irgendeine Erweiterung Λ von K durch von K ausgehende sukzessive[2]) Adjunktion von Wurzeln reiner Polynome erreichen oder einfangen kann. Hieraus ergibt sich leicht eine Reduktion bezüglich der in Betracht zu ziehenden Wurzelzeichen: Ist nämlich $x^n - a$ ein reines Polynom aus K von zusammengesetztem Grade $n = n_1 n_2$ und α eine seiner Wurzeln, so ist $\alpha^{n_2} = \alpha_1$ eine Wurzel des reinen Polynoms $x^{n_1} - a$ aus K und weiter α eine Wurzel des reinen Polynoms $x^{n_2} - \alpha_1$ aus $\mathsf{K}(\alpha_1)$. Somit kann man sich auf die sukzessive Adjunktion von Wurzeln reiner Polynome von Primzahlgrad beschränken. Je nach Geschmack kann nun hierbei noch die Einschränkung hinzugefügt werden, daß diese Polynome in dem jeweils erreichten Körper irreduzibel sein sollen oder nicht. Da die irreduziblen Polynome die einfachsten Bausteine für die Konstruktion algebraischer Erweiterungen sind, erscheint es theoretisch richtiger, diese Beschränkung aufzunehmen[3]). Wir definieren demgemäß:

***Definition 39.** Eine **Erweiterung** Λ von K heißt **rein** über K, wenn sie durch Adjunktion einer Wurzel eines irreduziblen reinen Polynoms aus K herleitbar ist.

---

[1]) Sonst wären eben nur die reinen Gleichungen durch Wurzelzeichen auflösbar.

[2]) Nicht nur durch simultane. Das besagt hier (anders als bei Satz 62 [52]) mehr, denn α kann sehr wohl Wurzel eines reinen Polynoms aus einer Erweiterung $\overline{\mathsf{K}}$ von K sein, ohne doch Wurzel eines reinen Polynoms aus K zu sein.

[3]) Tatsächlich ist die in Satz 127 [144] gegebene Antwort auf unsere Frage (für Grundkörper der Charakteristik 0) von dieser Beschränkung unabhängig, wie sich aus den späteren Sätzen 123, 126 [137, 141] leicht ergibt. Gerade in Hinsicht auf Satz 126 erscheint es mir aber richtiger, die Irreduzibilität zu fordern, da die „gröbere" Fragestellung an der algebraisch interessanten „feineren" Struktur der Kreisteilungskörper ganz vorbeisieht.

***Definition 40.** Eine **Erweiterung** endlichen Grades Λ von K heißt **durch Wurzelzeichen auflösbar** über K, wenn eine Erweiterungskette

$$K = \overline{\Lambda}_0 < \overline{\Lambda}_1 < \cdots < \overline{\Lambda}_r \quad \text{mit} \quad \overline{\Lambda}_r \geqq \Lambda$$

existiert, in der $\overline{\Lambda}_i$ rein und von Primzahlgrad über $\overline{\Lambda}_{i-1}$ ist.

Ein **Polynom** $f(x)$ aus K heißt **durch Wurzelzeichen auflösbar** über K, wenn sein Wurzelkörper über K es ist.

§ 20. Kreisteilungskörper. Endliche Körper.

Um die Frage nach der Auflösbarkeit durch Wurzelzeichen behandeln zu können, haben wir die Theorie des speziellen reinen Polynoms $x^n - e$ vorauszuschicken, dessen Wurzeln im Falle des rationalen Grundkörpers P, wenn man sie gemäß dem sog. Fundamentalsatz der Algebra als komplexe Zahlen darstellt, die Teilung der Peripherie des Einheitskreises in n gleiche Teile leisten. In Hinsicht auf unsere Anwendungen wollen wir uns hier nicht auf diesen Spezialfall P beschränken, sondern allgemeinere Grundkörper K zulassen, nennen aber in Anlehnung an jenen Spezialfall auch allgemein $x^n - e \doteq 0$ die **Kreisteilungsgleichung** und ihren Wurzelkörper T_n den **Kreisteilungskörper** für n über K. Über die Wurzeln der Kreisteilungsgleichung für n über K, die sog. n-ten **Einheitswurzeln** über K, beweisen wir dann zunächst den folgenden Satz:

Satz 120. Es sei K ein Körper, dessen Charakteristik 0 oder eine nicht in n aufgehende Primzahl ist. Dann bilden die n-ten Einheitswurzeln über K bezüglich der Multiplikation eine zyklische Gruppe $\mathfrak{Z}$ der Ordnung n. Es existieren also n verschiedene n-te Einheitswurzeln über K, die sich als die Potenzen

$$\zeta^0 = e, \quad \zeta^1, \ldots, \zeta^{n-1}$$

einer unter ihnen, einer sog. **primitiven n-ten Einheitswurzel** ζ, darstellen lassen.

Beweis: Es seien $\zeta_1, \ldots, \zeta_n$ die Wurzeln von $f_n(x) \equiv x^n - e$. Dann ist die Ableitung

$$f'_n(\zeta_i) = n\,\zeta_i^{n-1} \neq 0 \qquad (i = 1, \ldots, n),$$

weil natürlich $\zeta_i \neq 0$, also nach der Voraussetzung über die Charakteristik von K dann auch $n\zeta_i^{n-1} \neq 0$ ist (Satz 43 [37]). Nach Satz 56 [46] sind also die n Wurzeln ζ_i voneinander verschieden. Da ferner aus $\zeta_i^n = e$, $\zeta_k^n = e$ folgt $(\zeta_i \zeta_k)^n = e$, bilden die n verschiedenen n-ten Einheitswurzeln eine abelsche Gruppe $\mathfrak{Z}$ der Ordnung n (1, Satz 20 [55] angewandt auf die multiplikative Gruppe der Elemente $\neq 0$ des Kreisteilungskörpers T_n).

Nach Satz 34 [32] hat dann jedes Element ζ_i von $\mathfrak{Z}$ einen bestimmten Teiler m_i von n als Ordnung. Es sei nun ζ ein Element aus $\mathfrak{Z}$ von möglichst hoher Ordnung m. Wir haben zu zeigen, daß $m = n$ ist, woraus ja folgt, daß die n Potenzen $\zeta^0, \zeta^1, \ldots, \zeta^{n-1}$ verschieden sind und somit die Gruppe $\mathfrak{Z}$ erschöpfen. Sei dazu p eine beliebige Primzahl und werde (gemäß Satz 12, 22 [14, 22])

$$m = p^{\mu}\overline{m}, \quad m_i = p^{\mu_i}\overline{m}_i \quad \text{mit} \quad (\overline{m}, p) = 1, \quad (\overline{m}_i, p) = 1$$

gesetzt. Dann haben offenbar $\zeta_i^{\overline{m}_i}, \zeta^{p^{\mu}}$ die Ordnungen $p^{\mu_i}, \overline{m}$, also nach Satz 35 [32] $\zeta_i^{\overline{m}_i}\zeta^{p^{\mu}}$ die Ordnung $p^{\mu_i}\overline{m}$. Wegen der Maximalauswahl von m ist somit $p^{\mu_i}\overline{m} \leqq p^{\mu}m$, d. h. $\mu_i \leqq \mu$. Es enthält also m_i jede Primzahl p höchstens in der Potenz, in der p in m vorkommt, d. h. es ist $m_i \mid m$ (Satz 20 [22]) und somit $\zeta_i^m = e$. Die n verschiedenen n-ten Einheitswurzeln ζ_i sind also sämtlich Wurzeln des Polynoms m-ten Grades $x^m - e$. Daraus folgt $m \geqq n$ (Satz 48 [41]), was mit $m \mid n$ zusammen $m = n$ und damit unsere Behauptung ergibt.

Nach Satz 37 [34] (vgl. auch das zu Satz 31 [30] Gesagte) haben wir noch ohne weiteres:

Zusatz. Ist ζ eine primitive n-te Einheitswurzel über K, so sind alle und nur die Potenzen ζ^m, die den $\varphi(n)$ primen Restklassen m mod. n entsprechen, ebenfalls primitiv.

Hierauf beruht die in folgendem Satz enthaltene Bestimmung der Galoisgruppe des Kreisteilungskörpers T_n:

Satz 121. Ist K ein Körper wie in Satz 120 und ζ eine primitive n-te Einheitswurzel über K, so ist das Polynom

$$g_n(x) \equiv \prod_{\substack{m=0 \\ (m,n)=1}}^{n-1} (x - \zeta^m),$$

dessen Wurzeln die $\varphi(n)$ verschiedenen primitiven Einheitswurzeln sind, ein Polynom in K. Ist

$$\bar{g}_n(x) \equiv \prod_{\bar{m}} (x - \zeta^{\bar{m}})$$

der zu ζ gehörige irreduzible (nach Satz 59 [48] separable, nach Satz 99, (III) [88] normale) Faktor von $g_n(x)$, so repräsentieren die $\bar{m}$ eine Untergruppe $\bar{\mathfrak{P}}_n$ der primen Restklassengruppe $\mathfrak{P}_n$ mod. n. Die Galoisgruppe $\mathfrak{G}_n$ des (separablen, normalen) Kreisteilungskörpers T_n ist dann zu dieser Gruppe $\bar{\mathfrak{P}}_n$ isomorph auf Grund der Zuordnung des durch $\zeta \rightarrow \zeta^{\bar{m}}$ erzeugten Automorphismus von T_n zu der Restklasse $\bar{m}$ mod. n.

Insbesondere ist also T_n abelsch (Def. 34 [95]) und ferner der Grad von T_n über K ein Teiler von $\varphi(n)$ (Satz 105 [96]).

Beweis: a.) Da nach Satz 107 [98] ein Automorphismus von T_n bzgl. K einerseits die n verschiedenen Wurzeln ζ_i von $x^n - e$ nur untereinander vertauscht, andererseits deren Potenzdarstellungen $\zeta_i = \zeta^{i-1}$ invariant läßt, geht ζ durch ihn wieder in eine primitive n-te Einheitswurzel über, so daß auch die $\varphi(n)$ verschiedenen primitiven n-ten Einheitswurzeln durch ihn nur untereinander vertauscht werden. Hiernach sind die Koeffizienten von $g_n(x)$ bei allen Automorphismen von T_n bzgl. K invariant und gehören somit zu K (Satz 112, Zusatz [111]).

b.) Da $\mathsf{T}_n = \mathsf{K}(\zeta^0, \ldots, \zeta^{n-1}) = \mathsf{K}(\zeta)$, also eine primitive n-te Einheitswurzel über K gleichzeitig auch primitives Element von T_n bzgl. K ist, können (Satz 105 [96]) die Automorphismen von T_n bzgl. K durch die ihnen entsprechenden Substitutionen von ζ beschriebenw erden. Hat also $\bar{g}_n(x)$ die Bedeutung aus dem Satze, so wird die Galoisgruppe $\mathfrak{G}_n$ von T_n bzgl. K durch die Substitutionen $\zeta \to \zeta^{\overline{m}}$ dargestellt, und ihre Elemente sind hierdurch der Menge $\overline{\mathfrak{P}}_n$ der durch die $\overline{m}$ repräsentierten primen Restklassen mod. n eineindeutig zugeordnet. Da nun $\zeta \to \zeta^{\overline{m}_1}$ und $\zeta \to \zeta^{\overline{m}_2}$ nacheinander ausgeführt $\zeta \to (\zeta^{\overline{m}_2})^{\overline{m}_1} = \zeta^{\overline{m}_1 \overline{m}_2}$ ergeben, kommt bei dieser Zuordnung die Multiplikation in $\mathfrak{G}_n$ auf die Multiplikation der Restklassen in $\overline{\mathfrak{P}}_n$ hinaus. Daher ist diese Zuordnung isomorph und $\overline{\mathfrak{P}}_n$ eine zu $\mathfrak{G}_n$ isomorphe Untergruppe von $\mathfrak{P}_n$.

Bei der Untersuchung der Auflösbarkeit durch Wurzelzeichen spielen gemäß Def. 40 [129] die Einheitswurzeln von Primzahlordnung $n = p$ eine besondere Rolle. Wir beweisen für diesen Fall in Erweiterung des Satzes 121:

Satz 122. Es sei p eine Primzahl und K ein Körper mit von p verschiedener Charakteristik. Dann ist der Kreisteilungskörper T_p zyklisch über K von einem in $p-1$ aufgehenden Grade.

Beweis: Nach Satz 121 ist der Grad von T_p über K ein Teiler von $\varphi(p)$ und die Galoisgruppe $\mathfrak{G}_p$ von T_p bzgl. K isomorph zu einer Untergruppe $\overline{\mathfrak{P}}_p$ der primen Restklassengruppe $\mathfrak{P}_p$. Nun bilden die Restklassen mod. p nach Satz 28 [27] sogar einen Körper, den Primkörper P_p (Def. 13 [35], Satz 41 [36]). Die $\varphi(p)$ Elemente von $\mathfrak{P}_p$ sind dann die $p-1$ von Null verschiedenen Elemente von P_p (Satz 17 [20]) und sind als solche Wurzeln der Kreisteilungsgleichung $x^{p-1}-e \doteq 0$ (Satz 29 [29]), also die sämtlichen $(p-1)$-ten Einheitswurzeln über P_p. Nach Satz 120 [129] bilden sie somit bezüglich der Multiplikation eine zyklische Gruppe. Daher ist $\mathfrak{P}_p$, nach Satz 36 [33] also auch die Untergruppe $\overline{\mathfrak{P}}_p$, d. h. $\mathfrak{G}_p$ zyklisch und also T_p zyklisch über K (Def. 34 [95]) von einem in $p-1$ aufgehenden Grade.

Trivialerweise folgt übrigens aus Satz 44 [37]:

Zusatz. Hat K die Charakteristik p, so ist $x^p - e \equiv (x-e)^p$, also e die einzige p-te Einheitswurzel über K, und $\mathsf{T}_p = \mathsf{K}$.

Es ist bemerkenswert, wie die abstrakte Körpertheorie, durch die ohne weitere Schwierigkeiten mögliche Ausdehnung des in der Zahlentheorie gewöhnlich nur für den Grundkörper P bewiesenen Satzes 120 [129] auch auf P_p, auf einfachste Weise zu dem Schluß führt, daß die prime Restklassengruppe $\mathfrak{P}_p$ zyklisch ist, oder, wie man in der Zahlentheorie sagt, daß eine **primitive Wurzel mod. p** existiert, nämlich eine solche ganze Zahl r, daß für jedes zu p prime ganze m eine Potenzdarstellung

$$m \equiv r^{\mu} \bmod. p \quad (\mu = 0, \ldots, p-2)$$

besteht.

Wir fügen noch eine Bemerkung über den Spezialfall des Kreisteilungskörpers T_p über dem rationalen Grundkörper P an. Mit zahlentheoretischen Hilfsmitteln (Eisenstein-Schönemannscher Satz, siehe **3**, § 20, Aufg. 6) zeigt man, daß das Polynom

$$g_p(x) \equiv \frac{x^p - 1}{x - 1} \equiv x^{p-1} + x^{p-2} + \cdots + x + 1$$

aus Satz 121 in P irreduzibel ist, also T_p den Grad $\varphi(p) = p-1$ über P hat. Ist nun $p - 1 = 2^{\nu}$ ($\nu \geqq 0$) eine Potenz von 2, so kann nach Satz 109 [101] T_p von P aus durch sukzessive Adjunktion quadratischer Irrationalitäten erreicht werden, weil dann die nach Satz 122 zyklische Galoisgruppe $\mathfrak{G}_p$ von T_p bzgl. P die Ordnung 2^{ν} hat und folglich nach Satz 36 [33] eine Untergruppenkette

$$\mathfrak{G}_p = \mathfrak{H}_0 > \mathfrak{H}_1 > \cdots > \mathfrak{H}_{\nu} = \mathfrak{E}$$

derart besitzt, daß $\mathfrak{H}_i$ Untergruppe vom Index 2 von $\mathfrak{H}_{i-1}$ ist. Kann umgekehrt T_p von P aus durch sukzessive Adjunktion quadratischer Irrationalitäten erreicht (oder auch nur eingefangen) werden, so enthält die Gruppe $\mathfrak{G}$ nach den Ausführungen in § 17, 2.) [108] und § 18, 3.) [124] eine Untergruppenkette der eben beschriebenen Art[1]), und somit ist dann ihre Ordnung $p-1$ eine Potenz von 2. Daraus ergibt sich das berühmte

Resultat von Gauß. Das reguläre p-Eck für eine Primzahl p ist dann und nur dann mit Zirkel und Lineal konstruierbar, wenn p eine Primzahl von der Form $2^\nu + 1$ ist.

Man weiß bis heute nicht, ob die mit $p = 2, 3, 5, 17, 257, 65537$ beginnende Folge der Primzahlen dieser Form abbricht oder nicht. (Siehe hierzu auch **3**, § 20, Aufg. 14, 15.)

Auf analoge Weise werden wir aus Satz 122 im nächsten Paragraphen als das hauptsächlichste Ziel der Digression dieses Paragraphen die Auflösbarkeit von T_p durch Wurzelzeichen über bestimmten Grundkörpern K folgern.

Auf Grund von Satz 120 [129] kann jetzt mit Leichtigkeit gegeben werden:

Kurzer Abriß der Theorie der endlichen Körper.

A. Wir haben bereits endliche Körper, d. h. solche aus nur endlich vielen Elementen, kennengelernt, nämlich für jede Primzahl p den Primkörper P_p (Restklassenkörper mod. p) aus genau p Elementen (§ 4).

Sei jetzt E ein beliebiger endlicher Körper. Dann ist auch der in E enthaltene Primkörper endlich, also nicht zum rationalen Zahlkörper isomorph. Daher gilt (Satz 41 [36]):

(I) Die Charakteristik von E ist eine Primzahl p.

Nach dem im Anschluß an Satz 41 Gesagten kann dann E als Erweiterung des Primkörpers P_p angesehen werden. Trivialerweise ist dabei E von endlichem Grade über P_p (Def. 25 [57]). Aus der eindeutigen Darstellung $\alpha = a_1\alpha_1 + \cdots + a_m\alpha_m$ der Elemente α aus E durch eine Basis $\alpha_1, \ldots, \alpha_m$ von E bzgl. P_p mit Koeffizienten $a_1, \ldots, a_m$ aus P_p folgt dann:

(II) Ist $[\mathsf{E} : \mathsf{P}_p] = m$, so hat E genau p^m Elemente.

Wir verallgemeinern jetzt die für den Primkörper P_p selbst im Beweis zu Satz 122 angewandte Schlußweise auf E. Die multiplikative Gruppe der von Null verschiedenen Elemente von E (**1**, § 6, Beisp. 1 [53]) hat nach (II) die Ordnung $p^m - 1$. Diese

---

[1]) Für den allgemeinen Fall des Einfangens siehe den ausführlichen Beweis zu dem späteren Satz 127, Teil a), Anm. 1 [145].

$p^m - 1$ von Null verschiedenen Elemente genügen daher der Gleichung $x^{p^m-1} - e \doteq 0$ (Satz 34 [32]), sind also die sämtlichen $(p^m - 1)$-ten Einheitswurzeln über P_p, und daher ist die aus ihnen gebildete Gruppe zyklisch (Satz 120):

(III) Ist $[\mathsf{E} : \mathsf{P}_p] = m$, so ist E der Kreisteilungskörper T_{p^m-1} über P_p.

Die von Null verschiedenen Elemente von E sind die Wurzeln der Gleichung $x^{p^m-1} - e \doteq 0$, die sämtlichen Elemente von E also die Wurzeln der Gleichung $x^{p^m} - x \doteq 0$.

In E existiert ein primitives Element ϱ derart, daß die $p^m - 1$ von Null verschiedenen Elemente von E als die Potenzen

$$\varrho^0 = e, \quad \varrho^1, \ldots, \varrho^{p^m-2}$$

darstellbar sind.

Umgekehrt gilt:

(IV) Für beliebiges m ist der Kreisteilungskörper T_{p^m-1} über P_p ein endlicher Körper mit $[\mathsf{T}_{p^m-1} : \mathsf{P}_p] = m$.

Denn T_{p^m-1} ist als Erweiterung endlichen Grades des endlichen Körpers P_p (Satz 83 [70]) selbst ein endlicher Körper (Def. 25, Zusatz [57]). Dieser hat genau p^m Elemente; seine Elemente werden nämlich bereits durch Null und die $p^m - 1$ Wurzeln von $x^{p^m-1} - e$, d. h. durch die p^m Wurzeln von $x^{p^m} - x$ erschöpft; denn diese p^m Wurzeln bilden bereits einen Körper, weil aus $\alpha^{p^m} = \alpha$, $\beta^{p^m} = \beta$ nicht nur (wie im Beweis zu Satz 120) folgt $(\alpha\beta)^{p^m} = \alpha\beta$ und (falls $\beta \neq 0$) $\left(\frac{\alpha}{\beta}\right)^{p^m} = \frac{\alpha}{\beta}$, sondern nach Satz 44 [37] auch $(\alpha \pm \beta)^{p^m} = \alpha \pm \beta$. Nach (II) folgt daher $p^{[\mathsf{T}_{p^m-1} : \mathsf{P}_p]} = p^m$, d. h. in der Tat $[\mathsf{T}_{p^m-1} : \mathsf{P}_p] = m$.

Da durch die Elementanzahl p^m die Charakteristik p und der Grad m eindeutig bestimmt sind, gilt nach (III) und (IV):

(V) Für jede Elementanzahl der Form p^m gibt es genau einen endlichen Körpertypus, nämlich den Kreisteilungskörper T_{p^m-1} über P_p.

Ferner gilt:

(VI) Die Teilkörper von T_{p^m-1} sind alle und nur die Körper $\mathsf{T}_{p^\mu-1}$ mit $\mu \mid m$, und es ist dabei

$$[\mathsf{T}_{p^m-1} : \mathsf{T}_{p^\mu-1}] = \frac{m}{\mu}.$$

Denn einerseits ist, wenn $\mathsf{T}_{p^\mu-1} \leqq \mathsf{T}_{p^m-1}$ ist, nach Satz 71 [59] $\mu = [\mathsf{T}_{p^\mu-1} : \mathsf{P}_p] \mid [\mathsf{T}_{p^m-1} : \mathsf{P}_p] = m$, und $[\mathsf{T}_{p^m-1} : \mathsf{T}_{p^\mu-1}] = \frac{m}{\mu}$. Andererseits ist, wenn $\mu \mid m$ ist und dementsprechend $m = \mu\mu'$ gesetzt wird,

$$p^m - 1 = p^{\mu\mu'} - 1 = (p^\mu - 1)(p^{\mu(\mu'-1)} + \cdots + p^\mu + 1),$$

also $p^\mu - 1 \mid p^m - 1$, und daher $\mathsf{T}_{p^\mu-1} \leqq \mathsf{T}_{p^m-1}$, da dann die $(p^\mu - 1)$-ten Einheitswurzeln unter den $(p^m - 1)$-ten vorkommen.

Durch (V) und (VI) ist eine vollständige Übersicht über alle endlichen Körpertypen und ihre gegenseitigen Beziehungen gewonnen.

B. Sei jetzt $\mathsf{E} = \mathsf{T}_{p^m-1}$ ein endlicher Grundkörper und H eine endliche Erweiterung von E. Trivialerweise ist dann zunächst H von endlichem Grade n über E (Def. 25 [57]) und daher wieder ein endlicher Körper (Def. 25, Zusatz [57]), der nach (VI) die Form $\mathsf{H} = \mathsf{T}_{p^{mn}-1}$ hat. Ist dann ϱ ein primitives Element von H im Sinne von (III), so ist ϱ erst recht primitives Element im Sinne von Def. 19 [52] von H bzgl. jedes Teilkörpers. Also:

(VII) H ist einfach über E.

Hiermit ist die im Beweis von Satz 90 [80] zurückgebliebene Unvollständigkeit beseitigt.

Da die Charakteristik p von H in der Ordnungszahl $p^{mn} - 1$ der Einheitswurzeln, die H bilden, nicht aufgeht, gilt ferner nach dem in Satz 121 [131] Bemerkten:

(VIII) H ist separabel über E.

Schließlich gilt nach Satz 94 [85]:

(IX) H ist normal über E.

Daher sind die Sätze der Galoisschen Theorie auf die Erweiterung H von E anwendbar. Wenn auch eine Übersicht über die Körper zwischen H und E durch (VI) bereits ohne Verwendung der Galoisschen Theorie gewonnen ist — es sind alle und nur die $\mathsf{T}_{p^{m\nu}-1}$ mit $\nu \mid n$ —, so interessiert doch theoretisch die Feststellung:

(X) H ist zyklisch über E.

Die Galoisgruppe von H bzgl. E besteht nämlich aus den Potenzen des Automorphismus

$$A : \alpha \to \alpha^{p^m} \text{ für jedes } \alpha \text{ aus } \mathsf{H},$$

mit $A^n = E$, d. h. aus den n Automorphismen

$$A : \alpha \to \alpha^{p^{m\nu}} \text{ für jedes } \alpha \text{ aus } \mathsf{H} \ (\nu = 0, 1, \ldots, n-1).$$

Nach Satz 44 [37] [siehe auch schon die Schlußweise im Beweis zu (IV)] sind das nämlich in der Tat Automorphismen von H, bei denen jedes Element von E als Wurzel von $x^{p^m} - x$ invariant bleibt, also Automorphismen von H bzgl. E. Diese n Automorphismen von H bzgl. E sind ferner voneinander verschieden, weil für ein primitives Element ϱ von H (im Sinne von (III)) die sämtlichen Potenzen ϱ^i $(i = 1, \ldots, p^{mn} - 1)$, also insbesondere die n Potenzen $\varrho^{p^{m\nu}}$ $(\nu = 0, 1, \ldots, n-1)$ voneinander verschieden sind. Also sind es alle $n = [\mathsf{H} : \mathsf{E}]$ Automorphismen der Galoisgruppe von H bzgl. E (Satz 105 [96]).

§ 21. Reine und zyklische Erweiterungen von Primzahlgrad.

Zur Behandlung der Frage nach der Auflösbarkeit durch Wurzelzeichen haben wir den speziellen Entwicklungen des vorigen Paragraphen noch die Theorie der irreduziblen reinen Polynome von Primzahlgrad an die Seite zu stellen, auf die sich ja die Def. 40 [129] der Auflösbarkeit durch Wurzelzeichen stützt. Wir beweisen zunächst den folgenden Satz über die Irreduzibilität eines reinen Polynoms von Primzahlgrad:

Satz 123. Es sei p eine Primzahl und $x^p - a$ ein reines Polynom mit $a \neq 0$ aus K. Dann enthält der Wurzelkörper W dieses Polynoms den Kreisteilungskörper T_p über K, und es sind nur die folgenden beiden Fälle möglich:

a.) $x^p - a$ hat eine Wurzel in K, d. h. a ist eine p-te Potenz in K. Dann ist $x^p - a$ reduzibel in K und $\mathsf{W} = \mathsf{T}_p$.

b.) $x^p - a$ hat keine Wurzel in K, d. h. a ist keine p-te Potenz in K. Dann ist $x^p - a$ irreduzibel in K und sogar in T_p, und überdies normal über T_p, also W rein vom Grade p über T_p.

Beweis: Es seien $\alpha_1, \ldots, \alpha_p$ die Wurzeln von $x^p - a$ und α eine von ihnen. Aus $\alpha^p = a$ folgt dann, weil $a \neq 0$, also auch $\alpha \neq 0$ ist,

$$\left(\frac{x}{\alpha}\right)^p - e \equiv \frac{x^p - \alpha^p}{\alpha^p} \equiv \frac{x-\alpha_1}{\alpha} \cdots \frac{x-\alpha_p}{\alpha}$$
$$\equiv \left(\frac{x}{\alpha} - \frac{\alpha_1}{\alpha}\right) \cdots \left(\frac{x}{\alpha} - \frac{\alpha_p}{\alpha}\right).$$

Nach dem Einsetzungsprinzip (**1**, Satz 12 [40], angewandt auf $\mathsf{I}\,[x']$ mit $\mathsf{I} = \mathsf{W}[x]$ und die Einsetzung $x' = \alpha x$) darf hierin αx für x gesetzt werden, so daß

$$x^p - e \equiv \left(x - \frac{\alpha_1}{\alpha}\right) \cdots \left(x - \frac{\alpha_p}{\alpha}\right)$$

resultiert. Die Quotienten $\frac{\alpha_i}{\alpha}$ sind also die p-ten Einheitswurzeln über K, d. h. es ist $\mathsf{W} \geqq \mathsf{T}_p$. Ist ferner ζ eine primitive p-te Einheitswurzel (Satz 120 [129]; — falls K die Charakteristik p hat, $\zeta = e$ [Satz 122, Zusatz]), so gilt bei geeigneter Reihenfolge

$$\alpha_i = \zeta^i \alpha \quad (i = 1, \ldots, p).$$

a.) Liegt nun α in K, so liegen hiernach die α_i in T_p, d. h. es ist $\mathsf{W} \leqq \mathsf{T}_p$ und somit nach obigem $\mathsf{W} = \mathsf{T}_p$.

b.) Liegt aber keins der α in K, und wäre dann

$$h(x) \equiv x^\nu + \cdots + a_0 \quad (1 \leqq \nu \leqq p-1)$$

ein irreduzibler Faktor von $x^p - a$ in K, so hätte $\pm a_0$ als Produkt von gewissen ν Faktoren α_i eine Darstellung

$$\pm a_0 = \zeta^\mu \alpha^\nu.$$

Wird nach Satz 14, 17 [18, 20] $\nu\nu' = 1 + kp$ gesetzt, so folgte wegen $\alpha^p = a$

$$(\pm a_0)^{\nu'} = \zeta^{\mu\nu'} \alpha\, a^k,$$

so daß wegen $a \neq 0$ die Wurzel $\alpha_{\mu\nu'} = \zeta^{\mu\nu'}\alpha = \frac{(\pm a_0)^{\nu'}}{a^k}$ doch in K läge. Also ist dann $x^p - a$ irreduzibel in K und somit $\mathsf{K}(\alpha)$ vom Grade p über K. Wird nun in den gemachten Schlüssen $h(x)$ als irreduzibler Faktor von $x^p - a$ in T_p angenommen, so folgte, daß α und somit $\mathsf{K}(\alpha)$ in T_p enthalten wäre. T_p hätte also ein Multiplum von p zum Grade über K, während doch nach Satz 121 [131] dieser Grad ein Teiler von $p-1$ ist. Somit ist dann $x^p - a$ auch in T_p irreduzibel und nach Satz 99, (III.) [88]) überdies normal über T_p, also nach Satz 99, (I.) $\mathsf{W} = \mathsf{T}_p(\alpha)$ und daher rein vom Grade p über T_p (Def. 39 [128]).

Für die Frage nach der Auflösbarkeit durch Wurzelzeichen hat uns naturgemäß der Fall b.) des Satzes 123 besonders zu interessieren. Wenn K die Charakteristik p hat, ist dann $x^p - a$ ein inseparables irreduzibles Polynom (Def. 17 [47]). Seine einzige Wurzel α ist p-fach. Im Sinne unserer durchgängigen Beschränkung auf separable Erweiterungen schließen wir diese Möglichkeit im folgenden aus, indem wir bei der Betrachtung reiner Erweiterungen vom Primzahlgrad p die Charakteristik von K als von p verschieden voraussetzen. Dann ist $x^p - a$ (und allgemeiner jedes irreduzible Polynom aus K vom Grade p) a fortiori separabel (Def. 17).

Ferner ist $x^p - a$ im Falle b.) i. a. nicht über K, wohl aber über T_p normal, so daß es für die beabsichtigte Anwendung zweckmäßig erscheint, vor der Adjunktion einer Wurzel eines reinen Polynoms $x^p - a$ vom Primzahlgrad p jeweils erst eine primitive p-te Einheitswurzel ζ zu K zu adjungieren, also zunächst zu dem erweiterten Grundkörper $\overline{\mathsf{K}} = \mathsf{K}(\zeta) = \mathsf{T}_p$ überzugehen, der mit dem Körper $\overline{\mathsf{T}}_p = \{\mathsf{T}_p, \overline{\mathsf{K}}\}$ (Def. 37, Zusatz [118]) der p-ten Einheitswurzeln über $\overline{\mathsf{K}}$ zusammenfällt.

In dieser Hinsicht ist der nachstehende, aus Satz 123 ohne weiteres folgende Satz für uns von Interesse (in dem K sozusagen mit dem eben genannten $\overline{\mathsf{K}}$ zu identifizieren ist):

Satz 124. Ist p eine Primzahl und K ein Körper mit von p verschiedener Charakteristik, der die p-ten Einheitswurzeln über K enthält, so ist jede reine Erweiterung p-ten Grades Λ von K normal (separabel und zyklisch) über K.

Daß $\mathsf{\Lambda}$ als separable normale Erweiterung vom Primzahlgrade p zyklisch über K ist, ist trivial. Denn seine Galoisgruppe bzgl. K hat nach Satz 105 [96] die Primzahlordnung p und muß daher nach Satz 34 [32] mit der Periode jedes ihrer von E verschiedenen Elemente zusammenfallen.

In Umkehrung zu Satz 124 beweisen wir nun den für unsere Anwendung grundlegenden Satz:

Satz 125. Ist p eine Primzahl und K ein Körper mit von p verschiedener Charakteristik, der die p-ten Einheitswurzeln über K enthält, so ist jede normale Erweiterung p-ten Grades $\mathsf{\Lambda}$ von K (a fortiori separabel, zyklisch und) rein über K.

Beweis: Es sei A ein primitives Element der zyklischen Galoisgruppe von $\mathsf{\Lambda}$ bzgl. K, ϑ ein primitives Element von $\mathsf{\Lambda}$ bzgl. K und ζ eine primitive p-te Einheitswurzel über K Dann bilden wir die sog. **Lagrangesche Resolvente** von ϑ:

$$\alpha = \vartheta_E + \zeta^{-1}\vartheta_A + \cdots + \zeta^{-(p-1)}\vartheta_{A^{p-1}}.$$

Wenn dies Element α aus $\mathsf{\Lambda}$ von Null verschieden ist, schließen wir folgendermaßen:

Durch Anwendung von A auf α entsteht wegen $A^p = E$, $\zeta^p = e$ und der Invarianz des Elements ζ aus K bei A

$$\begin{aligned}\alpha_A &= \vartheta_A + \zeta^{-1}\vartheta_{A^2} + \cdots + \zeta^{-(p-1)}\vartheta_{A^p}\\ &= (\vartheta_E + \zeta^{-1}\vartheta_A + \cdots + \zeta^{-(p-1)}\vartheta_{A^{p-1}})\zeta = \alpha\zeta,\end{aligned}$$

also durch wiederholte Anwendung von A

$$\alpha_{A^\nu} = \alpha\zeta^\nu.$$

Hiernach sind die infolge der Annahme $\alpha \neq 0$ voneinander verschiedenen Elemente $\alpha, \alpha\zeta, \ldots, \alpha\zeta^{p-1}$ die konjugierten zu α bzgl. K, d. h. es ist

$$g(x) \equiv (x-\alpha)(x-\alpha\zeta)\cdots(x-\alpha\zeta^{p-1})$$

das zu α gehörige irreduzible Polynom aus K, und α ist ein primitives Element von $\mathsf{\Lambda}$ (Satz 111, 112 [109, 110] nebst Zusatz). Aus

$$x^p - e \equiv (x-e)(x-\zeta)\cdots(x-\zeta^{p-1})$$

folgt nun wie im Beweis zu Satz 123

$$g(x) \equiv x^p - \alpha^p,$$

und somit ist

$$g(x) \equiv x^p - a$$

mit $a = \alpha^p$ in K, also α Wurzel des irreduziblen reinen Polynoms $x^p - a$ aus K. Daher ist dann in der Tat $\Lambda = \mathsf{K}(\alpha)$ rein über K (Def. 39 [128]).

Wir zeigen nun, daß man durch passende Wahl der primitiven p-ten Einheitswurzel ζ erreichen kann, daß $\alpha \neq 0$ ist. Wäre nämlich für jede der $p-1$ primitiven p-ten Einheitswurzeln ζ^ν $(\nu = 1, \ldots, p-1)$ die zugehörige Lagrangesche Resolvente $\alpha_\nu = 0$, so bestände das Gleichungssystem

$$\alpha_\nu = \sum_{\mu=0}^{p-1} (\zeta^\nu)^{-\mu}\, \vartheta_{A^\mu} = 0 \quad (\nu = 1, \ldots, p-1).$$

Multipliziert man dessen ν-te Gleichung mit $\zeta^{\nu\mu'}$ und summiert über ν, so folgte nach Vertauschung der Summationsfolge

$$\sum_{\mu=0}^{p-1} \left(\sum_{\nu=1}^{p-1} \zeta^{\nu(\mu'-\mu)}\right) \vartheta_{A^\mu} = 0.$$

Da nun

$$\sum_{\nu=1}^{p-1} (\zeta^{\mu'-\mu})^\nu = \begin{cases} -e & \text{für } \mu' \not\equiv \mu \text{ mod. } p \\ pe - e & \text{für } \mu' \equiv \mu \text{ mod. } p \end{cases}$$

ist, weil im ersteren Falle $\zeta^{\mu'-\mu}$ primitive p-te Einheitswurzel, also Wurzel von $\frac{x^p - e}{x - e} \equiv x^{p-1} + x^{p-2} + \cdots + x + e$ ist, während im letzteren Falle $(p-1)$-mal der Summand e steht, so resultierten auf diese Weise die Relationen

$$\sum_{\mu=0}^{p-1} \vartheta_{A^\mu} = p\vartheta_{A^{\mu'}} \quad (\mu' = 0, 1, \ldots, p-1).$$

Da K nicht die Charakteristik p hat, wären also alle $\vartheta_{A^{\mu'}}$ einander gleich, was für ein primitives Element ϑ von Λ nach Satz 112, Zusatz [111] nicht der Fall ist.

Wir wenden zum Schluß noch die vorstehenden Resultate an, um die Auflösbarkeit durch Wurzelzeichen von T_p über bestimmten Grundkörpern K zu beweisen:

Satz 126. Es sei p eine Primzahl und K ein Körper, dessen Charakteristik 0 oder eine Primzahl $> p$ ist. Dann ist der Kreisteilungskörper T_p durch Wurzelzeichen auflösbar über K, und überdies existiert sogar eine Körperkette

$$\mathsf{K} = \overline{\Lambda}_0 < \overline{\Lambda}_1 < \cdots < \overline{\Lambda}_r \quad \text{mit} \quad \overline{\Lambda}_r \geqq \mathsf{T}_p,$$

in der $\overline{\Lambda}_i$ nicht nur (gemäß Def. 40 [129]) rein von Primzahlgrad, sondern auch normal über $\overline{\Lambda}_{i-1}$ ist.

Beweis: Wir wenden vollständige Induktion an und setzen dazu die Behauptungen für alle Primzahlen $< p$ (und alle dabei nach der Formulierung des Satzes zulässigen Grundkörper) als bereits bewiesen voraus. Es sei nun d der nach Satz 122 [132] in $p-1$ aufgehende Grad von T_p über K und $d = p_1 \cdots p_\nu$ die Zerlegung von d in (nicht notwendig verschiedene) Primzahlen p_k. Weil nach Voraussetzung die Charakteristik von K, wenn $\neq 0$, auch größer als jede dieser Primzahlen ist, existiert dann nach der Induktionsannahme zunächst eine Körperkette

$$\mathsf{K} = \overline{\Lambda}_0 < \overline{\Lambda}_1 < \cdots < \overline{\Lambda}_{r_1} \quad \text{mit} \quad \overline{\Lambda}_{r_1} \geqq \mathsf{T}_{p_1},$$

in der $\overline{\Lambda}_i$ rein und normal von Primzahlgrad über $\overline{\Lambda}_{i-1}$ ist, ferner (jetzt von $\overline{\Lambda}_{r_1}$ statt K als Grundkörper ausgehend) eine Körperkette

$$\overline{\Lambda}_{r_1} < \overline{\Lambda}_{r_1+1} < \cdots < \overline{\Lambda}_{r_2} \quad \text{mit} \quad \overline{\Lambda}_{r_2} \geqq \mathsf{T}_{p_1}, \mathsf{T}_{p_2}\,^{1)},$$

in der $\overline{\Lambda}_{r_1+i}$ rein und normal von Primzahlgrad über $\overline{\Lambda}_{r_1+i-1}$ ist, usf., zusammengenommen also eine Körperkette

$$\mathsf{K} = \overline{\Lambda}_0 < \overline{\Lambda}_1 < \cdots < \overline{\Lambda}_{r_\nu} \quad \text{mit} \quad \overline{\Lambda}_{r_\nu} \geqq \mathsf{T}_{p_1}, \ldots, \mathsf{T}_{p_\nu},$$

in der durchweg $\overline{\Lambda}_i$ rein und normal von Primzahlgrad über $\overline{\Lambda}_{i-1}$ ist. Es sei nun $\overline{\mathsf{T}}_p$ der Kreisteilungskörper für p über $\overline{\Lambda}_{r_\nu}$ und $\bar{d}$ sein nach Satz 119 [120] in d aufgehender Grad über $\overline{\Lambda}_{r_\nu}$. Dann existiert nach ganz entsprechenden Schlüssen wie beim Resultat von Gauss [133/34] (Satz 36, 109, 122 [33,

---

[1]) Der Kreisteilungskörper $\overline{\mathsf{T}}_{p_2}$ für p_2 über $\overline{\Lambda}_{r_1}$ enthält natürlich den Kreisteilungskörper T_{p_2} für p_2 über K.

101, 132]) eine Körperkette
$$\overline{\Lambda}_{r_\nu} < \overline{\Lambda}_{r_\nu+1} < \cdots < \overline{\Lambda}_r = \overline{\mathsf{T}}_p,$$
in der $\overline{\Lambda}_{r_\nu+i}$ normal von Primzahlgrad über $\overline{\Lambda}_{r_\nu+i-1}$ ist. Die sukzessiven Grade in dieser letzten Kette sind als Teiler von $\overline{d}$ gewisse der Primzahlen p_k. Da nun in den $\overline{\Lambda}_{r_\nu+i}$ nach Konstruktion die p_k-ten Einheitswurzeln enthalten sind, ist nach dem — wegen der Voraussetzung über die Charakteristik von K — (vgl. auch Satz 42 [37]) anwendbaren Satz 125 $\overline{\Lambda}_{r_\nu+i}$ rein über $\overline{\Lambda}_{r_\nu+i-1}$. Die volle Kette
$$\mathsf{K} = \overline{\Lambda}_0 < \cdots < \overline{\Lambda}_r = \overline{\mathsf{T}}_p$$
hat somit, wenn man noch bedenkt, daß $\mathsf{T}_p \leqq \overline{\mathsf{T}}_p$ ist, alle für die Behauptungen des Satzes erforderlichen Eigenschaften.

Da für die kleinste Primzahl $p = 2$ die Behauptungen wegen $\mathsf{T}_2 = \mathsf{K}$ trivialerweise zutreffen, ist hiermit der Satz durch vollständige Induktion bewiesen.

§ 22. Kriterium für die Auflösbarkeit durch Wurzelzeichen.

Um das in diesem Paragraphen herzuleitende Kriterium für die Auflösbarbeit durch Wurzelzeichen bequem aussprechen zu können, stellen wir die folgende Definition voran:

***Definition 41.** Eine separable normale Erweiterung N von endlichem Grade eines Körpers K heißt **metazyklisch** über K, wenn eine Zwischenkörper-Kette
$$\mathsf{K} = \Lambda_0 < \Lambda_1 < \cdots < \Lambda_r = \mathsf{N}$$
derart existiert, daß Λ_i normal von Primzahlgrad über Λ_{i-1} ist, oder — was nach dem Fundamentalsatz der Galoisschen Theorie dasselbe besagt —, wenn die Galoisgruppe $\mathfrak{G}$ von N bzgl. K eine Untergruppenkette
$$\mathfrak{G} = \mathfrak{H}_0 > \mathfrak{H}_1 > \cdots > \mathfrak{H}_r = \mathfrak{E}$$

derart enthält, daß $\mathfrak{H}_i$ Normalteiler von Primzahlindex von $\mathfrak{H}_{i-1}$ ist.

Ein separables **Polynom** $f(x)$ aus K heißt metazyklisch über K, wenn sein Wurzelkörper **metazyklisch** über K ist.

Der Ausdruck metazyklisch rührt daher, daß dann die einzelnen Schritte Λ_i über Λ_{i-1} bzw. $\mathfrak{H}_{i-1}/\mathfrak{H}_i$ zyklisch sind. Man nennt übrigens **Gruppen** $\mathfrak{G}$ von der in Def. 41 angegebenen Art ebenfalls **metazyklisch.**

Wir beweisen nun das folgende Kriterium für die Auflösbarkeit durch Wurzelzeichen normaler Erweiterungen endlichen Grades, wobei wir uns wegen der im vorigen Paragraphen für Primzahlcharakteristiken zutage getretenen Komplikationen auf Grundkörper der Charakteristik 0 beschränken, so daß also insbesondere die Voraussetzung der Separabilität trivialerweise stets erfüllt ist:

Satz 127. Eine normale Erweiterung N von endlichem Grade über einem Körper K der Charakteristik 0 ist dann und nur dann durch Wurzelzeichen auflösbar, wenn sie metazyklisch ist.

Ein Polynom $f(x)$ aus K ist also dann und nur dann durch Wurzelzeichen auflösbar, wenn es metazyklisch ist.

Beweis: a.) Es sei N durch Wurzelzeichen auflösbar über K. Gemäß Def. 40 [129] existiert dann eine Körperkette

$$\mathsf{K} = \overline{\Lambda}_0' < \overline{\Lambda}_1' < \cdots < \overline{\Lambda}_r' \text{ mit } \overline{\Lambda}_r' \geqq \mathsf{N}\,,$$

in der $\overline{\Lambda}_i'$ rein vom Primzahlgrade p_i über $\overline{\Lambda}_{i-1}'$ ist. Nach Satz 126 existiert (ähnlich wie im Beweise jenes Satzes) eine Körperkette

$$\mathsf{K} = \overline{\Lambda}_0 < \overline{\Lambda}_1 < \cdots < \overline{\Lambda}_s \text{ mit } \overline{\Lambda}_s \geqq \mathsf{T}_{p_1}, \ldots, \mathsf{T}_{p_r}\,,$$

in der $\overline{\Lambda}_i$ (rein und) normal von Primzahlgrad über $\overline{\Lambda}_{i-1}$ ist. Es sei nun α_i eine Folge von Elementen aus den $\overline{\Lambda}_i'$ derart, daß α_i Wurzel eines reinen irreduziblen Polynoms $x^{p_i} - a_i$ aus $\overline{\Lambda}_{i-1}'$, also $\overline{\Lambda}_i' = \overline{\Lambda}_{i-1}'(\alpha_i)$ und $\overline{\Lambda}_r' = \mathsf{K}(\alpha_1, \ldots, \alpha_r)$ ist. Entweder ist $x^{p_1} - a_1$ auch irreduzibel in $\overline{\Lambda}_s$; dann ist sein Wurzelkörper $\overline{\Lambda}_{s+1}$ über $\overline{\Lambda}_s$ nach Satz 123 [137] und wegen $\mathsf{T}_{p_1} \leqq \overline{\Lambda}_s$ (rein und) normal vom Primzahlgrade p_1 über $\overline{\Lambda}_s$ und zudem $\overline{\Lambda}_{s+1} = \overline{\Lambda}_s(\alpha_1)$. Oder es ist $x^{p_1} - a_1$ reduzibel in $\overline{\Lambda}_s$; dann ist nach demselben Satze $\overline{\Lambda}_{s+1} = \overline{\Lambda}_s$ und zudem $\overline{\Lambda}_{s+1} = \overline{\Lambda}_s(\alpha_1)$. Ebenso schließt man, daß der Wurzelkörper $\overline{\Lambda}_{s+2}$ von $x^{p_2} - a_2$ über $\overline{\Lambda}_{s+1}$ entweder (rein und) normal vom Primzahlgrade p_2 über $\overline{\Lambda}_{s+1}$ oder $= \overline{\Lambda}_{s+1}$ und beidemal zudem $\overline{\Lambda}_{s+2} = \overline{\Lambda}_{s+1}(\alpha_2)$ ist, usf. So ergibt sich bei Fortgehen bis zu $\overline{\Lambda}_{s+r}$ bei nur einmaliger Zählung mehrfach hintereinander auftretender Körper eine Körperkette

$$\mathsf{K} = \overline{\Lambda}_0 < \overline{\Lambda}_1 < \cdots < \overline{\Lambda}_{\bar{r}} \text{ mit } \overline{\Lambda}_{\bar{r}} \geqq \mathsf{N}$$

(letzteres wegen $\overline{\Lambda}_{\bar{r}} = \overline{\Lambda}_s(\alpha_1, \ldots, \alpha_r) \geqq \mathsf{K}(\alpha_1, \ldots, \alpha_r) = \overline{\Lambda}'_r \geqq \mathsf{N}$), in der durchweg $\overline{\Lambda}_i$ (rein und) normal von Primzahlgrad über $\overline{\Lambda}_{i-1}$ ist. Dieser Kette entspricht nach den Ausführungen in § 18, 3.) (vgl. Fig. 5 [125]) eine Zwischenkörperkette

$$\mathsf{K} = \Lambda_0 \leqq \Lambda_1 \leqq \cdots \leqq \Lambda_{\bar{r}} = \mathsf{N}\,,$$

in der Λ_i normal über Λ_{i-1} ist, und zwar von Primzahlgrad, falls nicht $\Lambda_i = \Lambda_{i-1}$ ist (und somit Λ_i ausgelassen werden kann); denn der Grad $[\Lambda_i : \Lambda_{i-1}]$ ist als Teiler des Primzahlgrades $[\overline{\Lambda}_i : \overline{\Lambda}_{i-1}]$ entweder 1 oder eben diese Primzahl [1]) Gemäß Def. 41 ist dann N metazyklisch über K.

b.) Es sei N metazyklisch über K. Gemäß Def. 41 existiert dann eine Zwischenkörperkette

$$\mathsf{K} = \Lambda_0 < \Lambda_1 < \cdots < \Lambda_r = \mathsf{N}\,,$$

in der Λ_i normal vom Primzahlgrad p_i über Λ_{i-1} ist. Wie unter a.) existiert eine Körperkette

$$\mathsf{K} = \overline{\Lambda}_0 < \overline{\Lambda}_1 < \cdots < \overline{\Lambda}_s \text{ mit } \overline{\Lambda}_s \geqq \mathsf{T}_{p_1}, \ldots, \mathsf{T}_{p_r},$$

[1]) Derselbe Schluß wurde übrigens — ohne daß es ausdrücklich hervorgehoben wurde — schon in dem Beweise des Resultats von Gauß in § 20 [134] für die dort auftretenden Primzahlgrade 2 gemacht.

in der $\overline{\Lambda}_i$ rein (und normal) von Primzahlgrad über $\overline{\Lambda}_{i-1}$ ist. Es sei nun ϑ_i eine Folge von Elementen aus den Λ_i derart, daß ϑ_i Wurzel eines normalen Polynoms $g_i(x)$ vom Primzahlgrad p_i aus Λ_{i-1}, also $\Lambda_i = \Lambda_{i-1}(\vartheta_i)$ und $\mathsf{N} = \Lambda_r = \mathsf{K}(\vartheta_1, \ldots, \vartheta_r)$ ist. Entweder ist $g_1(x)$ irreduzibel und somit auch normal in $\overline{\Lambda}_s$; dann ist sein Wurzelkörper $\overline{\Lambda}_{s+1} = \overline{\Lambda}_s(\vartheta_1)$ über $\overline{\Lambda}_s$ wegen $\mathsf{T}_{p_1} \leqq \overline{\Lambda}_s$ nach Satz 125 [140] rein (und normal) vom Primzahlgrad p_1 über Λ_s. Oder es ist $g_1(x)$ reduzibel in $\overline{\Lambda}_s$; dann ist $\overline{\Lambda}_{s+1} = \overline{\Lambda}_s(\vartheta_1) = \Lambda_s$, weil dann $[\overline{\Lambda}_{s+1} : \overline{\Lambda}_s]$ einerseits $< p_1$ ($\leqq$ wegen der Normalität von $g_1(x)$ in Λ_0 und sogar $<$ wegen der Reduzibilität in $\overline{\Lambda}_s$), andererseits ein Teiler von p_1 (nach Satz 119 [120], angewandt auf $\mathsf{K} = \Lambda_0$, $\mathsf{N} = \Lambda_1$, $\overline{\Lambda} = \overline{\Lambda}_s$, $\overline{\mathsf{N}} = \overline{\Lambda}_{s+1}$), also $[\overline{\Lambda}_{s+1} : \overline{\Lambda}_s] = 1$ ist. Ebenso schließt man, daß der Wurzelkörper $\overline{\Lambda}_{s+2} = \overline{\Lambda}_{s+1}(\vartheta_2)$ von $g_2(x)$ über $\overline{\Lambda}_{s+1}$ entweder rein (und normal) vom Primzahlgrad p_2 über $\overline{\Lambda}_{s+1}$ oder $= \overline{\Lambda}_{s+1}$ ist, usf. So ergibt sich durch Fortgehen bis zu $\overline{\Lambda}_{s+r}$ bei nur einmaliger Zählung mehrfach hintereinander auftretender Körper eine Körperkette

$$\mathsf{K} = \overline{\Lambda}_0 < \overline{\Lambda}_1 < \cdots < \overline{\Lambda}_{\bar{r}} \quad \text{mit} \quad \overline{\Lambda}_{\bar{r}} \geqq \mathsf{N}$$

(letzteres wegen $\overline{\Lambda}_{\bar{r}} = \overline{\Lambda}_s(\vartheta_1, \ldots, \vartheta_r) \geqq \mathsf{K}(\vartheta_1, \ldots, \vartheta_r) = \mathsf{N}$), in der durchweg $\overline{\Lambda}_i$ rein (und normal) von Primzahlgrad über $\overline{\Lambda}_{i-1}$ ist. Gemäß Def. 40 [129] ist dann N durch Wurzelzeichen auflösbar über K.

Wie aus jedem der beiden Teilbeweise ersichtlich ist, gilt auch allgemein eine entsprechende Verschärfung, wie sie schon in dem speziellen Satz 126 [141] erhalten wurde:

Zusatz. Ist unter den Voraussetzungen von Satz 127 N durch Wurzelzeichen auflösbar über K, so existiert sogar eine Körperkette

$$\mathsf{K} = \overline{\Lambda}_0 < \overline{\Lambda}_1 < \cdots < \overline{\Lambda}_r \quad \text{mit} \quad \overline{\Lambda}_r \geqq \mathsf{N},$$

in der $\overline{\Lambda}_i$ nicht nur (gemäß Def. 40) rein von Primzahlgrad, sondern auch normal über $\overline{\Lambda}_{i-1}$ ist.

Durch Satz 127 in Verbindung mit dem schon in Def. 41 Gesagten wird unsere zu Beginn dieses Abschnitts gestellte Frage entschieden, unter welchen Bedingungen eine algebraische Gleichung $(x) \doteq 0$ in einem Grundkörper K der Charakteristik 0 durch Wurzelzeichen auflösbar ist[1]), wann also ihre Wurzeln durch Rechenausdrücke darstellbar sind, die mittels der vier elementaren Rechenoperationen und der Operation des Wurzelziehens gebildet sind. Stellt man die etwas andere Frage, wann eine Wurzel eines irreduziblen Polynoms $f(x)$ aus K auf diese Weise darstellbar ist, so kommt das auf die Frage nach der Auflösbarkeit durch Wurzelzeichen einer beliebigen Erweiterung Λ endlichen Grades von K hinaus, die umgekehrt auch nicht allgemeiner ist, weil jede solche Erweiterung Λ als Stammkörper eines irreduziblen Polynoms $f(x)$ aufgefaßt werden kann. Wir führen in dieser Hinsicht an, daß die Bedingungen hierfür genau dieselben sind, wie für die oben behandelte Frage, daß nämlich eine beliebige Erweiterung endlichen Grades Λ von K dann und nur dann durch Wurzelzeichen auflösbar ist, wenn dies für die zugehörige normale Erweiterung N (den Wurzelkörper irgendeines irreduziblen Polynoms $f(x)$, für das Λ Stammkörper ist) der Fall ist. Daß mit N auch Λ durch Wurzelzeichen auflösbar ist, ist klar. Umgekehrt zeigt man durch Übergang von einer Körperkette gemäß Def. 41 für Λ zu deren konjugierten, daß mit Λ auch alle konjugierten Erweiterungen durch Wurzelzeichen auflösbar sind, woraus sich dann leicht die Auflösbarkeit durch Wurzelzeichen von N ergibt.

Beispiele durch Wurzelzeichen auflösbarer algebraischer Gleichungen über Grundkörpern der Charakteristik 0.

1.) Alle Gleichungen zweiten, dritten, vierten Grades.

Deren Galoisgruppen sind nämlich isomorph zu Untergruppen der symmetrischen Gruppen $\mathfrak{S}_2, \mathfrak{S}_3, \mathfrak{S}_4$ (Satz 107 [98]). Die letzteren erweisen sich aber (samt ihren sämtlichen Untergruppen) leicht als metazyklisch.

2.) Alle zyklischen und allgemeiner abelschen Gleichungen, speziell also nach Satz 121 [131] die allgemeine Kreisteilungsgleichung $x^n - 1 \doteq 0$.

Nach Satz 36 [33] ist nämlich jede endliche zyklische Gruppe metazyklisch. Auf die allgemeine Theorie der endlichen abelschen

[1]) Genau genommen liegt übrigens keine Entscheidung der Frage sondern nur eine Zurückführung auf die Aufstellung und Untersuchung der Galoisgruppe vor.

Gruppen, aus der insbesondere leicht folgt, daß diese Gruppen sämtlich metazyklisch sind, können wir hier nicht näher eingehen [1]).

§ 23. Existenz nicht durch Wurzelzeichen auflösbarer algebraischer Gleichungen.

Die Existenz nicht durch Wurzelzeichen auflösbarer Gleichungen wurde durch Abel entdeckt, der zuerst die Unmöglichkeit bewies, die allgemeine Gleichung höheren als vierten Grades durch Wurzelzeichen aufzulösen. Wir wollen in diesem letzten Paragraphen einen modernen Beweis dieses Abelschen Satzes skizzieren.

Zunächst definieren wir:

Definition 42. Ist $K_n = K(x_1, \ldots, x_n)$ der Körper der rationalen Funktionen von n Unbestimmten $x_1, \ldots, x_n$ über K, so heißt das Polynom

$$(1.) \qquad f_n(x) \equiv x^n + x_1 x^{n-1} + \cdots + x_n$$

über K_n das **allgemeine Polynom n-ten Grades** über K.

Dieses allgemeine Polynom n-ten Grades über K ist als eine „unbestimmte" Zusammenfassung aller speziellen Polynome n-ten Grades über K anzusehen, die ja aus ihm durch Einsetzung irgendwelcher Elementsysteme $a_1, \ldots, a_n$ aus K für die Unbestimmten $x_1, \ldots, x_n$ über K gewonnen werden können.

Wir betrachten nun die Zerlegung in Linearfaktoren

$$(2.) \quad f_n(x) \equiv x^n + x_1 x^{n-1} + \cdots + x_n \equiv (x - \xi_1) \cdots (x - \xi_n)$$

des allgemeinen Polynoms n-ten Grades über K in seinem Wurzelkörper $W_n = K_n(\xi_1, \ldots, \xi_n)$. Denkt man sich die n Linearfaktoren rechts ausmultipliziert, so müssen nach **1**, Satz 11 [32] die Koeffizienten gleich hoher Potenzen von x links und rechts übereinstimmen. So erhält man das Formelsystem [2])

---

[1]) Wir verweisen deswegen auf **3**, § 3 Aufg. 9—20 und bezüglich weiterer Sätze über metazyklische Gruppen auf das Buch von Speiser (**1**, Lit.-Verz. 16).

[2]) Wir bezeichnen hier, abweichend von der Festsetzung in **1**, S. 42 die Gleichheit in $K_n = K(x_1, \ldots, x_n)$ und in der algebraischen Erweiterung $W_n = Kn(\xi_1, \ldots, \xi_n)$ nur mit $=$, um $\equiv$ der Gleichheit bei Hinzunahme weiterer

$$(3.)\qquad \begin{cases} x_1 = -(\xi_1 + \cdots + \xi_n) \\ x_2 = \xi_1 \xi_2 + \cdots + \xi_{n-1}\xi_n \\ \dots\dots\dots\dots\dots\dots \\ x_n = (-1)^n \xi_1 \cdots \xi_n \end{cases}$$

oder zusammengefaßt

$$x_\nu = (-1)^\nu \sum_{\{i_1,\ldots,i_\nu\}} \xi_{i_1} \cdots \xi_{i_\nu} \qquad (\nu = 1, \ldots, n),$$

wo die Summe rechts über alle $\binom{n}{\nu}$ Kombinationen ν-ter Ordnung (**1**, § 16 [108]) der Ziffern $1, \ldots, n$ zu erstrecken ist. Nach diesen Formeln ist speziell

$$(4.)\qquad \mathsf{W}_n = \mathsf{K}_n(\xi_1, \ldots, \xi_n) = \mathsf{K}(x_1, \ldots, x_n; \xi_1, \ldots, \xi_n) \\ = \mathsf{K}(\xi_1, \ldots, \xi_n).$$

Neben der bisherigen von (1.) über (2.) zu (3.) und (4.) führenden Auffassungsweise kann man auch umgekehrt von (4.), d. h. dem Körper $\mathsf{W}_n = \mathsf{K}(\xi_1, \ldots, \xi_n)$ der rationalen Funktionen von n jetzt als Unbestimmte vorausgesetzten $\xi_1, \ldots, \xi_n$ über K ausgehen, dann $x_1, \ldots, x_n$ durch die Formeln (3.) als Elemente dieses Körpers W_n und $f_n(x)$ durch die Formel (2.) als Polynom in dem Teilkörper $\mathsf{K}_n = \mathsf{K}(x_1, \ldots, x_n)$ von $\mathsf{W}_n = \mathsf{K}(\xi_1, \ldots, \xi_n)$ definieren, wobei dann W_n wieder der Wurzelkörper zu $f_n(x)$ über K_n ist und die Darstellungen (4.) besitzt. Allerdings steht bei dieser letzteren Auffassungsweise die Frage offen, ob das so gebildete Polynom $f_n(x)$ das allgemeine Polynom n-ten Grades über K ist. Da die genannte zweite Auffassungsweise für die beabsichtigte Anwendung handlicher ist, ist es für uns von Bedeutung, diese Frage in bejahendem Sinne zu beantworten:

Satz 128. Ist $\mathsf{W}_n = \mathsf{K}(\xi_1, \ldots, \xi_n)$ der Körper der rationalen Funktionen von n Unbestimmten $\xi_1, \ldots, \xi_n$ über K, so haben die durch die Formeln (3.) definierten Elemente $x_1, \ldots, x_n$ aus W_n ebenfalls

---

Unbestimmten (etwa x in (1.) und (2.) sowie $\bar{x}_1, \ldots, \bar{x}_n$ im Beweise des folgenden Satzes 128) vorzubehalten.

den Charakter von n Unbestimmten über K[1]), d. h. der Teilkörper $\mathsf{K}_n = \mathsf{K}(x_1, \ldots, x_n)$ von $\mathsf{W}_n = \mathsf{K}(\xi_1, \ldots, \xi_n)$ ist ebenfalls vom Erweiterungstypus des Körpers der rationalen Funktionen von n Unbestimmten über K. Insbesondere ist dann also das durch (2.) definierte Polynom $f_n(x)$ über K_n das allgemeine Polynom n-ten Grades über K.

Beweis: Es ist zu zeigen, daß die Normaldarstellungen (**1**, Def. 9 [38]) der Elemente des Integritätsbereiches $\mathsf{K}[x_1, \ldots, x_n]$ durch $x_1, \ldots, x_n$ eindeutig sind, und dazu genügt es nachzuweisen, daß aus einer Relation

$$(5.)\qquad g(x_1, \ldots, x_n) = 0,$$

wo $g(\bar{x}_1, \ldots, \bar{x}_n)$ eine ganze rationale Funktion von n Unbestimmten $\bar{x}_1, \ldots, \bar{x}_n$ über K ist, die Relation

$$(6.)\qquad g(\bar{x}_1, \ldots, \bar{x}_n) \equiv 0$$

folgt. Diesen Nachweis führen wir durch doppelte vollständige Induktion[2]), erstens nach der Anzahl n der Unbestimmten, zweitens nach dem Grade ν_n von g in $\bar{x}_n$.

Für $n = 1$ ist $x_1 = -\xi_1$, also die Behauptung ersichtlich auf Grund des vorausgesetzten Unbestimmtencharakters von ξ_1 richtig. Sei sie schon bis $n-1$ bewiesen. Dann sei

$$(7.)\qquad g(\bar{x}_1, \ldots, \bar{x}_n) \equiv \sum_{k=0}^{\nu_n} \bar{x}_n^k\, g_k(\bar{x}_1, \ldots, \bar{x}_{n-1})$$

die (aus der Normaldarstellung durch Zusammenfassung folgende) Darstellung von g als ganze rationale Funktion von $\bar{x}_n$ über $\mathsf{K}[\bar{x}_1, \ldots, \bar{x}_{n-1}]$, also speziell

$$(8.)\qquad g(\bar{x}_1, \ldots, \bar{x}_{n-1}, 0) \equiv g_0(\bar{x}_1, \ldots, \bar{x}_{n-1}).$$

Setzt man nun in (5.) $\xi_n = 0$, so entsteht nach dem Einsetzungsprinzip (**1**, Satz 12 [40]), das wegen des Unbestimmtencharakters von ξ_n anwendbar ist, die Relation

$$(9.)\qquad g(x_1', \ldots, x_{n-1}', 0) = 0,$$

[1]) Vgl. **1**, Def. 9 [38] nebst anschließender Erläuterung.

[2]) Den Gedanken, in diesem Beweise **doppelte** vollständige Induktion anzuwenden, verdanke ich einer brieflichen Mitteilung von **Ph. Furtwängler**.

wo $x'_1, \ldots, x'_{n-1}$ aus $x_1, \ldots, x_{n-1}$ durch die Einsetzung $\xi_n = 0$ in (3.) hervorgehen; setzt man dann in (8.) $(\bar{x}_1, \ldots, \bar{x}_{n-1}) = (x'_1, \ldots, x'_{n-1})$, so folgt aus (9.) nach dem Einsetzungsprinzip weiter die Relation

$$(10.) \qquad g_0(x'_1, \ldots, x'_{n-1}) = 0.$$

Da nun $x'_1, \ldots, x'_{n-1}$ nach ihrer Erklärung für $\xi_1, \ldots, \xi_{n-1}$ die entsprechende Bedeutung haben, wie $x_1, \ldots, x_n$ für $\xi_1, \ldots, \xi_n$, so ergibt sich aus (10.) nach der gemachten ersten Induktionsannahme die Relation

$$g_0(\bar{x}_1, \ldots, \bar{x}_{n-1}) \equiv 0,$$

also nach (7.) weiter die Relation

$$(11.) \quad g(\bar{x}_1, \ldots, \bar{x}_n) \equiv \bar{x}_n \sum_{k=0}^{\nu_{n-1}} \bar{x}_n^k g_{k+1}(\bar{x}_1, \ldots, \bar{x}_{n-1}) \equiv \bar{x}_n g^{(1)}(\bar{x}_1, \ldots, \bar{x}_n),$$

wo $g^{(1)}(\bar{x}_1, \ldots, \bar{x}_n)$ wieder eine ganze rationale Funktion von $\bar{x}_1, \ldots, \bar{x}_n$ über K ist, die (falls $\nu_n > 0$) in $\bar{x}_n$ den Grad $\nu_n - 1$ hat.

Ist nun der Grad $\nu_n = 0$, so ist $g^{(1)}(\bar{x}_1, \ldots, \bar{x}_n) \equiv 0$ und also die Behauptung (6.) nach (11.) richtig. Sei sie (für das betrachtete feste n) schon bis zum Grade $\nu_n - 1$ bewiesen, so ist, weil aus (11.) durch die Einsetzung $(\bar{x}_1, \ldots, \bar{x}_n) = (x_1, \ldots, x_n)$ die Relation

$$g(x_1, \ldots, x_n) = x_n g^{(1)}(x_1, \ldots, x_n)$$

und aus dieser nach (5.) und wegen $x_n \neq 0$ weiter die Relation

$$g^{(1)}(x_1, \ldots, x_n) = 0$$

folgt, nach dieser zweiten Induktionsannahme

$$g^{(1)}(\bar{x}_1, \ldots, \bar{x}_n) \equiv 0,$$

woraus die Behauptung (6.) nach (11.) folgt. Hiermit ist die Behauptung des Satzes durch doppelte vollständige Induktion bewiesen.

Aus Satz 128 läßt sich übrigens auch leicht die umgekehrte Tatsache folgern, daß die ausgehend von Unbestimmten $x_1, \ldots, x_n$ durch (2.) definierten Elemente $\xi_1, \ldots, \xi_n$ den Charakter von Unbestimmten über K haben. Wir brauchen das jedoch hier nicht.

Wir beweisen nunmehr:

Satz 129. Das allgemeine Polynom n-ten Grades über K ist separabel und seine Galoisgruppe bzgl. K_n ist zur symmetrischen Gruppe $\mathfrak{S}_n$ isomorph.

Beweis: Gemäß Satz 128 denken wir uns das allgemeine Polynom n-ten Grades $f_n(x)$ über K nach der vor Satz 128 besprochenen zweiten Auffassungsweise, d. h. vom Wurzelkörper $\mathsf{W}_n = \mathsf{K}(\xi_1, \ldots, \xi_n)$ ausgehend durch die Formeln (3.), (2.) gebildet. Daß zunächst $f_n(x)$ separabel ist, folgt dann ohne weiteres aus der Verschiedenheit seiner als n Unbestimmte über K gewählten Wurzeln $\xi_1, \ldots, \xi_n$ (Satz 59, Zusatz [48]). Es sei ferner $\begin{pmatrix} 1 & \ldots & n \\ i_1 & \ldots & i_n \end{pmatrix}$ irgendeine Permutation aus $\mathfrak{S}_n$. Nach **1**, Satz 10, 11 [26, 32] ist dann $\mathsf{K}(\xi_{i_1}, \ldots, \xi_n)$ zu $\mathsf{K}(\xi_1, \ldots, \xi_n)$ auf Grund der Zuordnungen

$$\xi_1 \longleftrightarrow \xi_{i_1}, \ldots, \xi_n \longleftrightarrow \xi_{i_n}$$

isomorph bzgl. K. Da aber die Formeln (3.) symmetrisch in $\xi_1, \ldots, \xi_n$ sind, entsprechen bei dieser Zuordnung die Elemente $x_1, \ldots, x_n$ und somit alle Elemente von $\mathsf{K}_n = \mathsf{K}(x_1, \ldots, x_n)$ sich selbst, so daß die genannte Isomorphie sogar bzgl. K_n gilt. Da

$$\mathsf{W}_n = \mathsf{K}(\xi_1, \ldots, \xi_n) = \mathsf{K}(\xi_{i_1}, \ldots, \xi_{i_n})$$

ist, erzeugt also jede Permutation aus $\mathfrak{S}_n$ einen Automorphismus von W_n bzgl. K_n und wird daher umgekehrt durch einen solchen Automorphismus im Sinne von Satz 107 [98] geliefert. Aus diesem Satz ergibt sich daher mit Rücksicht auf die bereits hervorgehobene Verschiedenheit der Wurzeln $\xi_1, \ldots, \xi_n$, daß die Galoisgruppe von W_n, d. h. die von $f_n(x)$ bzgl. K_n zur symmetrischen Gruppe $\mathfrak{S}_n$ isomorph ist.

Aus Satz 129 ergibt sich übrigens speziell:

Satz 130. Das allgemeine Polynom n-ten Grades über K ist irreduzibel in K_n.

Beweis: Ist $\bar{f}_n(x)$ das zu einer Wurzel ξ von $f_n(x)$ gehörige irreduzible Polynom in K_n, so ist einerseits $\bar{f}_n(x) \mid f_n(x)$ (Satz 53 [43]), andererseits $\bar{f}_n(\xi_i) = 0$ für jede Wurzel ξ_i von $f_n(x)$ (Satz 73 [61], 129), also wegen der Verschiedenheit der Wurzeln ξ_i auch $f_n(x) \mid \bar{f}_n(x)$ (Satz 47 [40]). Beides zusammen ergibt $\bar{f}_n(x) \equiv f_n(x)$, wie behauptet.

Wir verweilen noch einen Augenblick bei den Formeln (3.), wieder unter der vor Satz 128 [149] besprochenen zweiten Auffassungsweise. Man nennt dann die Elemente $x_1, \ldots, x_n$ aus $K(\xi_1, \ldots, \xi_n)$ die **symmetrischen Grundfunktionen** der Unbestimmten $\xi_1, \ldots, \xi_n$. Allgemein nennt man ferner eine rationale Funktion über K der Unbestimmten $\xi_1, \ldots, \xi_n$ symmetrisch in $\xi_1, \ldots, \xi_n$, wenn sie bei allen Permutationen der n Elemente $\xi_1, \ldots, \xi_n$ in sich übergeht. Durch Anwendung der Sätze 107, 112 [98, 110] nebst Zusatz ergibt sich dann aus Satz 129 unmittelbar:

Satz 131. Eine rationale Funktion über K der Unbestimmten $\xi_1, \ldots, \xi_n$ [d. h. ein Element aus $K(\xi_1, \ldots, \xi_n)$] ist dann und nur dann symmetrisch, wenn sie rationale Funktion über K der symmetrischen Grundfunktionen $x_1, \ldots, x_n$ von $\xi_1, \ldots, \xi_n$ ist [d. h. ein Element aus dem Teilkörper $K(x_1, \ldots, x_n)$ von $K(\xi_1, \ldots, \xi_n)$ ist].

Die tiefer liegende Aussage dieses Satzes, nämlich die durch „nur dann" ausgedrückte, die also aussagt, daß jede symmetrische rationale Funktion über K von $\xi_1, \ldots, \xi_n$ eine rationale Funktion über K von $x_1, \ldots, x_n$ ist, ist eine Teilaussage des unter dem Namen **Satz von den symmetrischen Funktionen** bekannten Theorems, das bisher fast immer der Galoisschen Theorie zugrunde gelegt wurde (vgl. die erste Anm. zum Bew. von Satz 90 [80]). Dieses Theorem geht insofern noch über die Aussage von Satz 131 hinaus, als es weiterhin behauptet:

1.) Jede ganze rationale symmetrische Funktion über K von $\xi_1, \ldots, \xi_n$ ist eine ganze rationale Funktion von $x_1, \ldots, x_n$.

2.) Das letztere gilt auch noch, wenn an Stelle des Körpers K ein Integritätsbereich I steht.

Diese weiteren Aussagen können aber nicht, wie Satz 131, aus der Galoisschen Theorie gefolgert werden [1]).

Wir kehren nunmehr zu der eigentlichen Aufgabe dieses Paragraphen zurück, die wir jetzt auf Grund von Satz 129 in

---

[1]) Auf einen — mir von Ph. Furtwängler mitgeteilten — Beweis der Aussagen 1), 2.), der ganz analog, wie der Beweis von Satz 128, mit doppelter vollständiger Induktion geführt wird, kann hier nicht eingegangen werden: siehe **3, § 23, Aufg. 3.**

Angriff nehmen können. Da die symmetrische Gruppe $\mathfrak{S}_n$ für $n > 1$ stets den Normalteiler $\mathfrak{A}_n$ vom Index 2 hat (**1**, Satz 63 [113]), ergibt sich eine Reduktion des Wurzelkörpers $W_n = K_n(\xi_1, \ldots, \xi_n)$ vom Grade $n!$ über K_n auf einen Körper vom Grade $\frac{n!}{2}$ über einem aus K_n durch Adjunktion einer Quadratwurzel entstehenden Körper V_n:

Satz 132. Der Wurzelkörper $W_n = K_n(\xi_1, \ldots, \xi_n)$ des allgemeinen Polynoms n-ten Grades $(n > 1)$ über K besitzt einen Teilkörper V_n vom Grade 2 über K_n. Dieser wird, falls K nicht die Charakteristik 2 hat, durch Adjunktion des Elementes

$$\delta = \begin{vmatrix} 1 & \xi_1 & \xi_1^2 & \cdots & \xi_1^{n-1} \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ 1 & \xi_n & \xi_n^2 & \cdots & \xi_n^{n-1} \end{vmatrix}$$

zu K_n gewonnen, das Wurzel eines reinen Polynoms $x^2 - d$ vom zweiten Grade aus K_n ist[1]).

Beweis: Daß $V_n = K_n(\delta)$ der $\mathfrak{A}_n$ zugeordnete Körper zwischen K_n und W_n ist, folgt gemäß Satz 112, 129 [110, 152] daraus, daß δ bei den geraden Permutationen von $\xi_1, \ldots, \xi_n$ invariant ist, bei den ungeraden dagegen sein Vorzeichen ändert (**1**, Satz 65 [116]), und daß $\delta \neq 0$ (siehe **3**, Teil **1**, § 19, Aufg. 4), also nach der Annahme über die Charakteristik $\delta \neq -\delta$ ist. Hiernach ist ferner $\delta^2 = d$ bei allen Permutationen von $\xi_1, \ldots, \xi_n$ invariant, also Element aus K_n (Satz 112, Zusatz [111]).

Das Element $d = \delta^2$, das natürlich sogar zu $K[\xi_1, \ldots, \xi_n]$ gehört, also eine ganze rationale Funktion über K der Wurzeln $\xi_1, \ldots, \xi_n$ ist, heißt die **Diskriminante von $f_n(x)$.**

Nun beweist man in der Gruppentheorie, daß für $n \neq 4$ die alternierende Gruppe $\mathfrak{A}_n$ keinen echten Normalteiler besitzt[2]), und daß $\mathfrak{A}_n$ der einzige Normal-

[1]) Hinsichtlich des Falles, daß K die Charakteristik 2 hat, siehe **3**, § 23, Aufg. 20.

[2]) Speiser, l. c. (**1**, Lit.-Verz. 16), Satz 94. Siehe auch **3**, § 23, Aufg. 13, 14.

teiler von $\mathfrak{S}_n$ ist [1]). Da $\frac{n!}{2}$ für $n \geqq 4$ keine Primzahl ist, kann also für $n > 4$ keine Untergruppenkette von $\mathfrak{S}_n$ der in Def. 41 [143] genannten Art existieren, so daß dann $\mathfrak{S}_n$ nicht metazyklisch ist. Nach Satz 127 [144] ergibt sich so das

Resultat von Abel. Das allgemeine Polynom n-ten Grades über einem Körper K der Charakteristik 0 ist für $n > 4$ nicht durch Wurzelzeichen auflösbar.

Durch diesen Satz ist die Existenz nicht durch Wurzelzeichen auflösbarer Gleichungen zunächst nur für die besonderen Grundkörper K_n von Def. 42 [148] sichergestellt. Eine weitere Frage ist dann, ob es in einem gegebenen Grundkörper K spezielle, d. h. in K selbst gelegene nicht durch Wurzelzeichen auflösbare Gleichungen jeden Grades $n > 4$ gibt. Diese Frage beantwortet sich für den Spezialfall des rationalen Grundkörpers P bejahend durch den

Irreduzibilitätssatz von Hilbert[2]**).** Ist $g(x; x_1, \ldots, x_n)$ eine ganze rationale Funktion der Unbestimmten $x; x_1, \ldots, x_n$ über P, die ein in $\mathsf{P}_n = \mathsf{P}(x_1, \ldots, x_n)$ irreduzibles Polynom von x ist, so gibt es unendlich viele Elementsysteme $a_1, \ldots, a_n$ aus P, so daß $g(x; a_1, \ldots, a_n)$ in P irreduzibel ist.

Aus diesem Satz ergibt sich die Lösung der zuvor aufgeworfenen Frage für den Grundkörper P folgendermaßen: Sind $\xi_1, \ldots, \xi_n$ die Wurzeln des allgemeinen Polynoms n-ten Grades $f_n(x) = x^n + x_1 x^{n-1} + \cdots + x_n$ über P, so ist nach Satz 112, Zusatz [111] und Satz 129 [152]

$$\vartheta = c_1 \xi_1 + \cdots + c_n \xi_n$$

primitives Element des Wurzelkörpers $\mathsf{W}_n = \mathsf{P}_n(\xi_1, \ldots, \xi_n)$

---

[1]) Das folgt dann aus dem sog. Jordanschen Satz (Speiser, ebenda Satz 27) in Verbindung mit der evidenten Nichtexistenz von Normalteilern von $\mathfrak{S}_n$ der Ordnung 2. Siehe auch **3**, § 23, Aufg. 16.

[2]) D. Hilbert, Über die Irreduzibilität ganzer rationaler Funktionen mit ganzzahligen Koeffizienten, Journ. f. d. reine u. angew. Math. **110**, 1892.

bzgl. $\mathsf{P}_n = \mathsf{P}(x_1, \ldots, x_n)$, wenn die Koeffizienten c_ν aus P_n so gewählt werden, daß alle Permutationen $\binom{\nu}{i_\nu}$ der ξ_ν verschiedene konjugierte

$$\vartheta_i = c_1 \xi_{i_n} + \cdots + c_n \xi_{i_n}$$

ergeben. Wir denken uns die c_ν in dieser Weise gewählt, und zwar, was nach Satz 49 [41] möglich ist, sogar als Elemente aus dem Integritätsbereich $\Gamma_n = \mathsf{P}[x_1, \ldots, x_n]$. Dann ist

$$g(x; x_1, \ldots, x_n) \equiv \prod_{i=1}^{n!} (x - \vartheta_i)$$

eine Galoissche Resolvente von W_n bzgl. P_n und genügt den Voraussetzungen des Hilbertschen Irreduzibilitätssatzes. Es gibt also unendlich viele Elementsysteme $a_1, \ldots, a_n$ aus P derart, daß $g(x; a_1, \ldots, a_n)$ irreduzibel in P ist. Die Wurzelkörper W über P der diesen Systemen $a_1, \ldots, a_n$ entsprechenden speziellen $f(x)$ haben dann, weil es in ihnen je ein Element ϑ des Grades $n!$ gibt, den höchstmöglichen Grad $n!$ über P (Satz 108 [100]) und somit eine zu $\mathfrak{S}_n$ selbst isomorphe Galoisgruppe (Satz 107 [98]). Nach den Ausführungen dieses Paragraphen sind also diese $f(x)$ für $n > 4$ nicht durch Wurzelzeichen auflösbar. Wir haben daher:

Korollar. Es gibt in P für jeden Grad n unendlich viele algebraische Gleichungen, deren Galoisgruppe zu $\mathfrak{S}_n$ isomorph ist (sog. Gleichungen ohne **Affekt**), insbesondere also für jeden Grad $n > 4$ unendlich viele nicht durch Wurzelzeichen auflösbare algebraische Gleichungen.

Ob dies Resultat auch für allgemeine Grundkörper K, sowie für irgendwelche Untergruppen von $\mathfrak{S}_n$ als vorgeschriebene Galoisgruppen gilt, ist bis heute, abgesehen von einfachen Fällen, unentschieden.

Namen- und Sachverzeichnis.

SAMMLUNG GÖSCHEN

GESAMTVERZEICHNIS

Jeder Band DM 3,60 · Doppelband DM 5,80
Dreifachband DM 7,80

Herbst 1966

WALTER DE GRUYTER & CO · BERLIN 30

Inhaltsübersicht

Geisteswissenschaften

Philosophie

Einführung in die Philosophie von *H. Leisegang †*. 6. Auflage. 146 Seiten. 1966. (281)

Hauptprobleme der Philosophie von *G. Simmel †*. 8., unveränderte Auflage. 177 Seiten. 1964. (500)

Geschichte der Philosophie

I: Die griechische Philosophie von *W. Capelle*. 1. Teil. Von Thales bis Leukippos. 3., erweiterte Auflage. Etwa 135 Seiten. 1966. (857)

II: Die griechische Philosophie von *W. Capelle*. 2. Teil. Von der Sophistik bis zum Tode Platons. 3., stark erweiterte Auflage. Etwa 144 Seiten. 1966. In Vorbereitung (858)

III: Die griechische Philosophie von *W. Capelle*. 3. Teil. Vom Tode Platons bis zur Alten Stoa. 2., stark erweiterte Auflage. 132 Seiten. 1954. (859)

IV: Die griechische Philosophie von *W. Capelle*. 4. Teil. Von der Alten Stoa bis zum Eklektizismus im 1. Jh. v. Chr. 2., stark erweiterte Auflage. 132 Seiten. 1954. (863)

V: Die Philosophie des Mittelalters von *J. Koch*. In Vorbereitung. (826)

VI: Von der Renaissance bis Kant von *K. Schilling*. 234 Seiten. 1954. (394/394a)

VII: Immanuel Kant von *G. Lehmann*. In Vorbereitung. (536)

VIII: Die Philosophie des 19. Jahrhunderts von *G. Lehmann*. 1. Teil. 151 Seiten. 1953. (571)

IX: Die Philosophie des 19. Jahrhunderts von *G. Lehmann*. 2. Teil. 168 Seiten. 1953. (709)

X: Die Philosophie im ersten Drittel des 20. Jahrhunderts 1. Teil von *G. Lehmann*. 128 Seiten. 1957. (845)

XI: Die Philosophie im ersten Drittel des 20. Jahrhunderts 2. Teil von *G. Lehmann*. 114 Seiten. 1960. (850)

Die geistige Situation der Zeit (1931) von *K. Jaspers*. 6. Abdruck der im Sommer 1932 bearbeiteten 5. Auflage. 211 Seiten. 1965. (1000)

Erkenntnistheorie von *G. Kropp*.
1. Teil: Allgemeine Grundlegung. 143 Seiten. 1950. (807)

Formale Logik von *P. Lorenzen*. 3., durchgesehene und erweiterte Auflage. 184 Seiten. 1966. (1176/1176a)

Philosophisches Wörterbuch von *M. Apel †*. 5., völlig neu bearbeitete Auflage von *P. Ludz*. 315 Seiten. 1958. (1031/1031a)

Philosophische Anthropologie. Menschliche Selbstdeutung in Geschichte und Gegenwart von *M. Landmann*. 2., durchgesehene Auflage. 223 Seiten. 1964. (156/156a)

Pädagogik, Psychologie, Soziologie

Geschichte der Pädagogik von *Herm. Weimer* 17. Auflage von *Heinz Weimer*. 184 Seiten. 1967. (145/145a)

Therapeutische Psychologie. Ihr Weg durch die Psychoanalyse von *W. M. Kranefeldt*. Mit einer Einführung von *C. G. Jung*. 3. Auflage. 152 Seiten. 1956. (1034)

Allgemeine Psychologie von *Th. Erismann* †. 4 Bände.
I: Grundprobleme. 3. Auflage. 146 Seiten. 1965. (831)
II: Grundarten des psychischen Geschehens. 2., neubearbeitete Auflage. 248 Seiten. 1959. (832/832a)
III: Experimentelle Psychologie und ihre Grundlagen. 1. Teil. 2., neubearbeitete Auflage. 112 Seiten, 7 Abbildungen. 1962. (833)
IV: Experimentelle Psychologie und ihre Grundlagen. 2. Teil. 2., neubearbeitete Auflage. 199 Seiten, 20 Abbildungen. 1962. (834/834a)

Soziologie. Geschichte und Hauptprobleme von *L. von Wiese*. 7. Auflage. 176 Seiten. 1964. (101)
Ideengeschichte der sozialen Bewegung des 19. und 20. Jh. von *W. Hofmann*. 243 Seiten. 1962. (1205/1205a)
Sozialpsychologie von *P. R. Hofstätter*. 2. Auflage. 191 Seiten, 18 Abbildungen. 1964. (104/104a)
Psychologie des Berufs- und Wirtschaftslebens von *W. Moede* †. 190 Seiten, 48 Abbildungen. 1958. (851/851a)
Industrie- und Betriebssoziologie von *R. Dahrendorf*. 3. Auflage. 142 Seiten. 3 Figuren. 1965. (103)
Wirtschaftssoziologie von *F. Fürstenberg*. 122 Seiten. 1961. (1193)
Einführung in die Sozialethik von *H.-D. Wendland*. 144 S. 1963. (1203)

Religion

Jesus von *M. Dibelius* †. 4. Auflage, mit einem Nachtrag von *W. G. Kümmel*. 140 Seiten. 1966. (1130)
Paulus von *M. Dibelius* †. Nach dem Tode des Verfassers herausgegeben und zu Ende geführt von *W. G. Kümmel*. 3., durchgesehene Auflage. 156 Seiten. 1964. (1160)
Luther von *F. Lau*. 2., verbesserte Auflage. 153 Seiten. 1966 (1187)
Melanchthon von *R. Stupperich*. 139 Seiten. 1960. (1190)
Zwingli von *F. Schmidt-Clausing*. 119 Seiten. 1965. (1219)
Sören Kierkegaard. Leben u. Werk von *H. Gerdes*. 134 Seiten. 1966. (1221)
Einführung in die Konfessionskunde der orthodoxen Kirchen von *K. Onasch*. 291 Seiten. 1962. (1197/1197a)
Geschichte des christlichen Gottesdienstes von *W. Nagel*. 215 Seiten. 1962. (1202/1202a)
Geschichte Israels. Von den Anfängen bis zur Zerstörung des Tempels (70 n.Chr.) von *E.L. Ehrlich*. 2. Aufl. 1966. In Vorbereitung. (231/231a)
Römische Religionsgeschichte von *F. Altheim*. 2 Bände. 2., umgearbeitete Auflage.
I: Grundlagen und Grundbegriffe. 116 Seiten. 1956. (1035)
II: Der geschichtliche Ablauf. 164 Seiten. 1956. (1052)
Die Religion des Buddhismus von *D. Schlingloff*. 2 Bände.
I: Der Heilsweg des Mönchstums. 122 Seiten, 11 Abbildungen, 1 Karte. 1962. (174)
II: Der Heilsweg für die Welt. 129 Seiten, 9 Abbildungen, 1 Karte. 1963. (770)

Musik

Musikästhetik von *H. J. Moser.* 180 Seiten. Mit zahlreichen Notenbeispielen. 1953. (344)

Systematische Modulation von *R. Hernried.* 2. Auflage. 136 Seiten. Mit zahlreichen Notenbeispielen. 1950. (1094)

Der polyphone Satz von *E. Pepping.* 2 Bände.
I: Der cantus-firmus-Satz. 2. Auflage. 233 Seiten. Mit zahlreichen Notenbeispielen. 1950. (1148)
II: Übungen im doppelten Kontrapunkt und im Kanon. 137 Seiten. Mit zahlreichen Notenbeispielen. 1957. (1164/1164a)

Allgemeine Musiklehre von *H. J. Moser.* 2., durchgesehene Auflage. 155 Seiten. Mit zahlreichen Notenbeispielen. 1955. (220/220a)

Harmonielehre von *H. J. Moser.* 2 Bände.
I: 109 Seiten. Mit 120 Notenbeispielen. 1954. (809)
II: In Vorbereitung. (810)

Die Musik des 19. Jahrhunderts von *W. Oehlmann.* 180 Seiten. 1953. (170)

Die Musik des 20. Jahrhunderts von *W. Oehlmann.* 312 Seiten. 1961. (171/171a)

Technik der deutschen Gesangskunst von *H. J. Moser.* 3., durchgesehene und verbesserte Auflage. 144 Seiten, 5 Figuren sowie Tabellen und Notenbeispiele. 1954. (576/576a)

Die Kunst des Dirigierens von *H. W. von Waltershausen †.* 2., vermehrte Auflage. 138 Seiten. Mit 19 Notenbeispielen. 1954. (1147)

Die Technik des Klavierspiels aus dem Geiste des musikalischen Kunstwerkes von *K. Schubert †.* 3. Auflage. 110 Seiten. Mit Notenbeispielen. 1954. (1045)

Kunst

Stilkunde von *H. Weigert.* 2 Bände. 3., durchgesehene und ergänzte Auflage.
I: Vorzeit, Antike, Mittelalter. 136 Seiten, 94 Abbildungen. 1958. (80)
II: Spätmittelalter und Neuzeit. 150 Seiten, 88 Abbildungen. 1958. (781)

Archäologie von *A. Rumpf.* 3 Bände.
I: Einleitung, historischer Überblick. 143 Seiten, 6 Abbildungen, 12 Tafeln. 1953. (538)
II: Die Archäologensprache. Die antiken Reproduktionen. 136 Seiten. 7 Abbildungen, 12 Tafeln. 1956. (539)
III: In Vorbereitung. (540)

Geschichte

Einführung in die Geschichtswissenschaft von *P. Kirn.* 4., durchgesehene Auflage. 127 Seiten. 1963. (270)

Einführung in die Zeitgeschichte von *B. Scheurig.* 101 Seiten. 1962. (1204)

Zeitrechnung der römischen Kaiserzeit, des Mittelalters und der Neuzeit für die Jahre 1—2000 n. Chr. von *H. Lietzmann †*. 3. Auflage, durchgesehen von *K. Aland*. 130 Seiten. 1956. (1085)

Kultur der Urzeit von *F. Behn*. 3 Bände. 4. Auflage der Kultur der Urzeit Bd. 1—3 von *M. Hoernes*.

I: Die vormetallischen Kulturen. (Die Steinzeiten Europas. Gleichartige Kulturen in anderen Erdteilen.) 172 Seiten, 48 Abbildungen. 1950. (564)

II: Die älteren Metallkulturen. (Der Beginn der Metallbenutzung, Kupfer- und Bronzezeit in Europa, im Orient und in Amerika.) 160 Seiten, 67 Abbildungen. 1950. (565)

III: Die jüngeren Metallkulturen. (Das Eisen als Kulturmetall, Hallstatt-Latène-Kultur in Europa. Das erste Auftreten des Eisens in den anderen Weltteilen.) 149 Seiten, 60 Abbildungen. 1950. (566)

Vorgeschichte Europas von *F. Behn*. Völlig neue Bearbeitung der 7. Auflage der „Urgeschichte der Menschheit" von *M. Hoernes*. 125 Seiten, 47 Abbildungen. 1949. (42)

Der Eintritt der Germanen in die Geschichte von *J. Haller †*. 3. Auflage, durchgesehen von *H. Dannenbauer*. 120 Seiten, 6 Kartenskizzen. 1957. (1117)

Von den Karolingern zu den Staufern. Die altdeutsche Kaiserzeit (900—1250) von *J. Haller †*. 4., durchgesehene Auflage von *H. Dannenbauer*. 142 Seiten, 4 Karten. 1958. (1065)

Von den Staufern zu den Habsburgern. Auflösung des Reichs und Emporkommen der Landesstaaten (1250 —1519) von *J. Haller †*. 2., durchgesehene Auflage von *H. Dannenbauer*. 118 Seiten, 6 Kartenskizzen. 1960. (1077)

Deutsche Geschichte im Zeitalter der Reformation, der Gegenreformation und des dreißigjährigen Krieges von *F. Hartung*. 2., durchgesehene Auflage. 128 Seiten. 1963. (1105)

Deutsche Geschichte von 1648—1740. Politischer und geistiger Wiederaufbau von *W. Treue*. 120 Seiten. 1956. (35)

Deutsche Geschichte von 1713—1806. Von der Schaffung des europäischen Gleichgewichts bis zu Napoleons Herrschaft von *W. Treue*. 168 Seiten. 1957. (39)

Deutsche Geschichte von 1806—1890. Vom Ende des alten bis zur Höhe des neuen Reiches von *W. Treue*. 128 Seiten. 1961. (893)

Deutsche Geschichte von 1890 bis zur Gegenwart von *W. Treue*. In Vorbereitung. (894)

Quellenkunde der Deutschen Geschichte im Mittelalter (bis zur Mitte des 15. Jahrhunderts) von *K. Jacob †*. 3 Bände.

I: Einleitung. Allgemeiner Teil. Die Zeit der Karolinger. 6. Auflage, bearbeitet von *H. Hohenleutner*. 127 Seiten. 1959. (279)

II: Die Kaiserzeit (911-1250). 5. Auflage, neubearbeitet von *H. Hohenleutner*. 141 Seiten. 1961. (280)

III: Das Spätmittelalter (vom Interregnum bis 1500). Herausgegeben von *F. Weden*. 152 Seiten. 1952. (284)

Geschichte Englands von *H. Preller*. 2 Bände.
I: bis 1815. 4., stark umgearbeitete Auflage. Etwa 135 Seiten, 7 Stammtafeln, 2 Karten. 1966. Im Druck. (375)
II: Von 1815 bis 1910. 2., völlig umgearbeitete Auflage. 118 Seiten, 1 Stammtafel, 7 Karten. 1954. (1088)

Römische Geschichte von *F. Altheim*. 4 Bände. 2., verbesserte Auflage.
I: Bis zur Schlacht bei Pydna (168 v. Chr.). 124 Seiten. 1956. (19)
II: Bis zur Schlacht bei Actium (31 v. Chr.). 129 Seiten, 1956. (677)
III: Bis zur Schlacht an der Milvischen Brücke (312 n. Chr.). 148 Seiten. 1958. (679)
IV: Bis zur Schlacht am Yarmuk (636 n. Chr.). In Vorbereitung. (684)

Geschichte der Vereinigten Staaten von Amerika von *O. Graf zu Stolberg-Wernigerode*. 192 Seiten, 10 Karten. 1956. (1051/1051 a)

Deutsche Sprache und Literatur

Geschichte der Deutschen Sprache von *H. Sperber*. 5., neubearbeitete Auflage von *P. von Polenz*. 136 Seiten. 1966. (915)

Deutsches Rechtschreibungswörterbuch von *M. Gottschald †*. 2., verbesserte Auflage. 269 Seiten. 1953. (200/200a)

Deutsche Wortkunde. Kulturgeschichte des deutschen Wortschatzes von *A. Schirmer*. 5. Auflage von *W. Mitzka*. 125 Seiten. 1965. (929)

Deutsche Sprachlehre von *W. Hofstaetter*. 10. Auflage. Völlige Umarbeitung der 8. Auflage. 150 Seiten. 1960. (20)

Stimmkunde für Beruf, Kunst und Heilzwecke von *H. Biehle*. 111 Seiten. 1955. (60)

Redetechnik. Einführung in die Rhetorik von *H. Biehle*. 2., erweiterte Auflage. 151 Seiten. 1961. (61)

Grundlagen der Sprecherziehung von *J. Jesch* 1966. In Vorbereitung (1122/1122a)

Deutsches Dichten und Denken von der germanischen bis zur staufischen Zeit von *H. Naumann †*. (Deutsche Literaturgeschichte vom 5.—13. Jahrhundert.) 3., verbesserte Auflage. 1966. (1121)

Deutsches Dichten und Denken vom Mittelalter zur Neuzeit von *G. Müller* (1270 bis 1700). 3., durchgesehene Auflage. 159 Seiten. In Vorbereitung. (1086)

Deutsches Dichten und Denken von der Aufklärung bis zum Realismus (Deutsche Literaturgeschichte von 1700—1890) von *K. Viëtor †*. 3., durchgesehene Auflage. 159 Seiten. 1958. (1096)

Deutsche Heldensage von *H. Schneider*. 2. Auflage, bearbeitet von *R. Wisniewski*. 148 Seiten. 1964. (32)

Der Nibelunge Nôt in Auswahl. Mit kurzem Wörterbuch herausgegeben von *K. Langosch*. 11., durchgesehene Auflage. 166 Seiten. 1966. (1)

Kudrun und Dietrich-Epen in Auswahl mit Wörterbuch von *O. L. Jiriczek*. 6. Auflage, bearbeitet von *R. Wisniewski*. 173 Seiten. 1957. (10)

Wolfram von Eschenbach. Parzifal. Eine Auswahl mit Anmerkungen und Wörterbuch von *H. Jantzen*. 3. Auflage, bearbeitet von *H. Kolb*. 128 Seiten. 1966. (921)

Hartmann von Aue. Der arme Heinrich nebst einer Auswahl aus der „Klage" dem „Gregorius" und den Liedern (mit einem Worterverzeichnis) herausgegeben von *F. Maurer.* 96 Seiten. 1958. (18)
Gottfried von Straßburg. Tristan und Isolde in Auswahl herausgegeben von *F. Maurer.* 2. Auflage. 142 Seiten. 1965. (22)
Die deutschen Personennamen von *M. Gottschald †.* 2., verbesserte Auflage. 151 Seiten. 1955. (422)
Althochdeutsches Elementarbuch. Grammatik und Texte von *H. Naumann †* und *W. Betz.* 4., verbesserte und vermehrte Auflage. 183 Seiten. 1966. (1111/1111a)
Mittelhochdeutsche Grammatik von *H. de Boor* und *R. Wisniewski.* 4., verbesserte und ergänzte Auflage. 150 Seiten. 1965. (1108)

Indogermanisch, Germanisch

Indogermanische Sprachwissenschaft von *H. Krahe.* 2 Bände.
I: Einleitung und Lautlehre. 5. Auflage. 110 Seiten. 1966. (59)
II: Formenlehre. 4., neubearbeitete Auflage. 100 Seiten. 1963. (64)
Sanskrit-Grammatik mit sprachvergleichenden Erläuterungen von *M. Mayrhofer.* 2., völlig neu bearbeitete Auflage. 110 Seiten. 1965. (1158/1158a)
Altirische Grammatik von *J. Pokorny.* 2. Auflage. In Vorbereitung. (896
Gotisches Elementarbuch. Grammatik. Texte mit Übersetzung und Erläuterungen von *H. Hempel.* 4., neubearbeitete Auflage. 169 Seiten. 1966. (79/79a)
Altnordisches Elementarbuch. Einführung, Grammatik, Texte (zum Teil mit Übersetzung) und Wörterbuch von *F. Ranke.* 3., vollig umgearb. Auflage vo n*D. Hofmann.* Etwa 180 Seiten. 1967. Im Druck. (1115/1115a)
Germanische Sprachwissenschaft von *H. Krahe.* 3 Bände.
I: Einleitung und Lautlehre. 6. Auflage. 147 Seiten. 1966. (238)
II: Formenlehre. 5., verbesserte Auflage. 149 Seiten. 1965. (780)
III: Wortbildungslehre von *W. Meid.* Etwa 240 Seiten. 1966. (1218/1218a/1218b)

Englisch, Romanisch

Altenglisches Elementarbuch. Einführung, Grammatik, Texte mit Übersetzung und Wörterbuch von *M. Lehnert.* 6., verbesserte Auflage. 178 Seiten. 1965. (1125)
Mittelenglisches Elementarbuch von *H. Weinstock.* 1967. In Vorbereitung (1226/1226a)
Historische neuenglische Laut- und Formenlehre von *E. Ekwall.* 4., verbesserte Auflage. 150 Seiten. 1965. (735)
Englische Phonetik von *H. Mutschmann †.* 2. Auflage, bearbeitet von *G. Scherer.* 127 Seiten. 1963. (601)
Englische Literaturgeschichte von *F. Schubel.* 4 Bände.
I: Die alt- und mittelenglische Periode. 163 Seiten. 1954. (1114)
II: Von der Renaissance bis zur Aufklärung. 160 Seiten. 1956. (1116)
III: Romantik und Viktorianismus. 160 Seiten. 1960. (1124)

Beowulf von *M. Lehnert*. Eine Auswahl mit Einführung, teilweiser Übersetzung, Anmerkungen und etymologischem Wörterbuch. 4., verbesserte Auflage. 135 Seiten. 1966. (1135)

Shakespeare von *P. Meißner †*. 2. Auflage, neubearbeitet von *M. Lehnert*. 136 Seiten. 1954. (1142)

Romanische Sprachwissenschaft von *H. Lausberg*. 4 Bände.
I: Einleitung und Vokalismus. 2., durchgesehene Auflage. 211 Seiten. 1963. (128/128a)
II: Konsonantismus. 2. Auflage. 1966. Im Druck. (250)
III: Formenlehre. 1. Teil. 99 Seiten. 1962. (1199)
III: Formenlehre. 2. Teil. S. 99—260. 1962. (1200/1200a)
IV: Wortlehre. In Vorbereitung. (1208)

Griechisch, Lateinisch

Griechische Sprachwissenschaft von *W. Brandenstein*. 3 Bände.
I: Einleitung, Lautsystem, Etymologie. 160 Seiten. 1954. (117)
II: Wortbildung und Formenlehre. 192 Seiten. 1959. (118/118a)
III: Syntax I. Einleitung. Die Flexibilien. 145 Seiten. 1966. (924/924a)

Geschichte der griechischen Sprache. 2 Bände
I: Bis zum Ausgang der klassischen Zeit von *O. Hoffmann †*. 3. Auflage, bearbeitet von *A. Debrunner †*. 156 Seiten. 1953. (111)
II: Grundfragen und Grundzüge des nachklassischen Griechisch von *A. Debrunner †*. 144 Seiten. 1954. (114)

Geschichte der griechischen Literatur von *W. Nestle*. 2 Bände. 3. Auflage, bearbeitet von *W. Liebich*.
I: 144 Seiten. 1961. (70)
II: 149 Seiten. 1963. (557)

Grammatik der neugriechischen Volkssprache von *J. Kalitsunakis*. 3., wesentlich erweiterte und verbesserte Auflage. 196 Seiten. 1963. (756/756a)

Neugriechisch-deutsches Gesprächsbuch von *J. Kalitsunakis*. 2. Auflage, bearbeitet von *A. Steinmetz*. 99 Seiten. 1960. (587)

Geschichte der lateinischen Sprache von *F. Stolz* und *A. Debrunner †*. 4., stark umgearbeitete Auflage von *W. P. Schmid*. 145 Seiten. 1966. (492/492a)

Geschichte der römischen Literatur von *L. Bieler*. 2., verbesserte Auflage. 2 Bände.
I: Die Literatur der Republik. 160 Seiten. 1965. (52)
II: Die Literatur der Kaiserzeit. 133 Seiten. 1965. (866)

Orientalistik, Slavistik

Die Keilschrift von *B. Meissner*. 3. Auflage, neubearbeitet von *K. Oberhuber*. Etwa 150 Seiten. 1966. (708/708a/708b)

Die Hieroglyphen von *A. Erman*. 3. Auflage, neu bearbeitet von *O. Krückmann*. 1966. In Vorbereitung. (608 608a/608b)

Hebräische Grammatik von *R. Meyer.* 3 Bände.
I: Einleitung, Schrift- und Lautlehre. 3., neubearbeitete Auflage. 120 Seiten. 1966. (763/763a/763b)
II: Formenlehre und Flexionstabellen. 3. Auflage. In Vorbereitung. (764/764a/764b)
III: Satzlehre. In Vorbereitung (765/765a/765b)
Hebräisches Textbuch zu *G. Beer-R. Meyer,* Hebräische Grammatik von *R. Meyer.* 170 Seiten. 1960. (769/769a)
Slavische Sprachwissenschaft von *H. Bräuer.* 2 Bände.
I: Einleitung, Lautlehre. 221 Seiten. 1961. (1191/1191a)
Vergleichende Geschichte der slavischen Literaturen von *D. Tschižewskij.* 2 Bände. 1966. In Vorbereitung.
I: Einführung. Anfänge des slavischen Schrifttums bis zum Klassizismus. (1222/1222a)
II: Romantik bis zur Moderne. (1223/1223a)
Russische Grammatik von *E. Berneker †.* 6., verbesserte Auflage von *M. Vasmer †.* 155 Seiten. 1961. (66)
Polnische Grammatik von *N. Damerau.* Etwa 140 Seiten. 1967. (942/942a)

Erd- und Länderkunde, Kartographie

Afrika von *F. Jaeger.* Ein geographischer Überblick. 2 Bände. 3. Auflage.
I: Der Lebensraum. 179 Seiten, 18 Abbildungen. In Vorbereitung. (910)
II: Mensch und Kultur. 155 Seiten, 6 Abbildungen. In Vorbereitung. (911)
Australien und Ozeanien von *H. J. Krug.* 176 Seiten, 46 Skizzen. 1953. (319)
Kartographie von *V. Heissler.* 2. Auflage. 213 Seiten, 125 Abb., 8 Anlagen. 1966. (30/30a)

Volkswirtschaft, Statistik, Publizistik

Allgemeine Betriebswirtschaftslehre von *K. Mellerowicz.* 4 Bände. 11. und 12., durchgesehene Auflage.
I: 224 Seiten. 1964. (1008/1008a)
II: 188 Seiten. 1966. (1153/1153a)
III: 260 Seiten. 1963. (1154/1154a)
IV: 209 Seiten. 1963. (1186/1186a)
Allgemeine Volkswirtschaftslehre von *A. Paulsen.* 4 Bände.
I: Grundlegung, Wirtschaftskreislauf. 7. Auflage. 159 Seiten, 11 Abbildungen. 1966. (1169)
II: Haushalte, Unternehmungen, Marktformen. 7. Auflage. 172 Seiten, 31 Abbildungen. 1966. (1170)
III: Produktionsfaktoren. 5. Auflage. 198 Seiten, 24 Abbildungen. 1966. (1171)
IV: Gesamtbeschäftigung, Konjunkturen, Wachstum. 4., neubearbeitete und ergänzte Auflage. 188 Seiten. 1966. (1172)
Übungsaufgaben mit Lösungen zur Allgemeinen Volkswirtschaftslehre I/II von *A. Paulsen* von *W. Wedig.* Etwa 160 Seiten. 1966. (1227/1227a)

Geschichte der Volkswirtschaftslehre von *S. Wendt.* 182 S. 1961. (1194)

Allgemeine Volkswirtschaftspolitik von *H. Ohm.* 2 Bände.
- I: Systematisch-Theoretische Grundlegung. 2., verbesserte und ergänzte Auflage. 137 Seiten, 6 Abbildungen. 1965. (1195)
- II: Der volkswirtschaftliche Gesamtorganismus als Objekt der Wirtschaftspolitik. In Vorbereitung. (1196)

Finanzwissenschaft von *H. Kolms.* 4 Bände.
- I: Grundlegung, Öffentliche Ausgaben. 3., verbesserte Auflage. 165 Seiten. 1966. (148)
- II: Erwerbseinkünfte, Gebühren und Beiträge, Allgemeine Steuerlehre. 3., verbesserte Auflage. 154 Seiten. 1966. (391)
- III: Besondere Steuerlehre. 2., verbesserte und ergänzte Auflage. 178 Seiten. 1966. (776/776a)
- IV: Öffentlicher Kredit. Öffentlicher Haushalt. Finanzausgleich. 191 Seiten. 1964. (782/782a)

Finanzmathematik von *M. Nicolas.* 192 Seiten, 11 Tafeln, 8 Tabellen und 72 Beispiele. 1959. (1183/1183a)

Programmierung von Datenverarbeitungsanlagen von *H. J. Schneider, D. Jurksch.* Etwa 128 Seiten, 8 Tabellen, 11 Abbildungen. 1967. (1225/1225a)

Lineare Programmierung von *H. Langen.* Etwa 200 Seiten. (1206/1206a)

Buchhaltung und Bilanz von *E. Kosiol.* 170 Seiten. 1964. (1213/1213a)

Industrie- und Betriebssoziologie von *R. Dahrendorf.* 3. Auflage. 142 Seiten, 3 Figuren. 1965. (103)

Wirtschaftssoziologie von *F. Fürstenberg.* 122 Seiten. 1961. (1193)

Psychologie des Berufs- und Wirtschaftslebens von *W. Moede†.* 190 Seiten, 48 Abbildungen. 1958. (851/851a)

Einführung in die Arbeitswissenschaft von *H. H. Hilf.* 169 Seiten, 57 Abbildungen. 1964. (1212/1212a)

Allgemeine Methodenlehre der Statistik von *J. Pfanzagl.* 2 Bände.
- I: Elementare Methoden unter besonderer Berucksichtigung der Anwendungen in den Wirtschafts- und Sozialwissenschaften. 3., neubearbeitete Auflage. 266 Seiten, 50 Abbildungen. 1966. (746/746a)
- II: Höhere Methoden unter besonderer Berücksichtigung der Anwendungen in Naturwissenschaften, Medizin und Technik. 2., verbesserte Auflage. 315 Seiten, 41 Abbildungen. 1966. (747/747a)

Zeitungslehre von *E. Dovifat.* 2 Bände. 5., neubearbeitete Auflage.
- I: Theoretische und rechtliche Grundlagen — Nachricht und Meinung — Sprache und Form. 149 Seiten. 1966. Im Druck. (1039)
- II: Redaktion — Die Sparten: Verlag und Vertrieb, Wirtschaft und Technik — Sicherung der öffentlichen Aufgabe. 168 Seiten. 1966. Im Druck. (1040)

Naturwissenschaften

Mathematik

Geschichte der Mathematik von *J. E. Hofmann*. 4 Bände.
I: Von den Anfängen bis zum Auftreten von Fermat und Descartes. 2., verbesserte und vermehrte Auflage. 251 Seiten. 1963. (226/226a)
II: Von Fermat und Descartes bis zur Erfindung des Calculus und bis zum Ausbau der neuen Methoden. 109 Seiten. 1957. (875)
III: Von den Auseinandersetzungen um den Calculus bis zur französischen Revolution. 107 Seiten. 1957. (882)
IV: Geschichte der Mathematik der neuesten Zeit von *N. Stuloff*. In Vorbereitung. (883)

Mathematische Formelsammlung von *F.O. Ringleb*. 8., verbesserte Auflage. Etwa 320 Seiten, 40 Figuren. 1967. (51/51a)

Vierstellige Tafeln und Gegentafeln für logarithmisches und trigonometrisches Rechnen in zwei Farben zusammengestellt von *H. Schubert* und *R. Haussner*. 3., neubearbeitete Auflage von *J. Erlebach*. 158 Seiten. 1960. (81)

Fünfstellige Logarithmen mit mehreren graphischen Rechentafeln und häufig vorkommenden Zahlenwerten von *A. Adler*. 4. Auflage, überarbeitet von *J. Erlebach*. 127 Seiten, 1 Tafel. 1962. (423)

Arithmetik von *P. B. Fischer†*. 3. Auflage von *H. Rohrbach*. 152 Seiten, 19 Abbildungen. 1958. (47)

Höhere Algebra von *H. Hasse*. 2 Bände. 5., neubearbeitete Auflage.
I: Lineare Gleichungen. 150 Seiten. 1963. (931)
II: Gleichungen höheren Grades. 158 Seiten, 5 Figuren. 1966. (932)

Aufgabensammlung zur höheren Algebra von *H. Hasse* und *W. Klobe*. 3., verbesserte Auflage. 183 Seiten. 1961. (1082)

Elementare und klassische Algebra vom modernen Standpunkt von *W. Krull*. 2 Bände.
I: 3., erweiterte Auflage. 148 Seiten. 1963. (930)
II: 132 Seiten. 1959. (933)

Lineare Programmierung von *H. Langen*. Etwa 200 Seiten. (1206/1206a)

Algebraische Kurven und Flächen von *W. Burau*. 2 Bande.
I: Algebraische Kurven der Ebene. 153 Seiten, 28 Abbildungen. 1962. (435)
II: Algebraische Flächen 3. Grades und Raumkurven 3. und 4. Grades. 162 Seiten, 17 Abbildungen. 1962. (436/436a)

Einführung in die Zahlentheorie von *A. Scholz†*. Überarbeitet und herausgegeben von *B. Schoeneberg*. 4. Auflage. 128 Seiten. 1966. (1131)

Formale Logik von *P. Lorenzen*. 3., durchgesehene und erweiterte Auflage. 184 Seiten. 1966. (1176/1176a)

Topologie von *W. Franz.* 2 Bände.
I: Allgemeine Topologie. 2., verbesserte Auflage. 144 Seiten, 9 Figuren. 1965. (1181)
II: Algebraische Topologie. 153 Seiten. 1965. (1182/1182a)

Elemente der Funktionentheorie von *K. Knopp†.* 7. Auflage. 144 Seiten, 23 Figuren. 1966. (1109)

Funktionentheorie von *K. Knopp†.* 2 Bände. 11. Auflage.
I: Grundlagen der allgemeinen Theorie der analytischen Funktionen. 144 Seiten, 8 Figuren. 1965. (668)
II: Anwendungen und Weiterführung der allgemeinen Theorie. 130 Seiten, 7 Figuren. 1965. (703)

Aufgabensammlung zur Funktionentheorie von *K. Knopp†.* 2 Bände.
I: Aufgaben zur elementaren Funktionentheorie. 7. Auflage. 135 Seiten. 1965. (877)
II: Aufgaben zur höheren Funktionentheorie. 6. Auflage. 151 Seiten. 1964. (878)

Differential- und Integralrechnung von *M. Barner.* (Früher *Witting*). 4 Bände.
I: Grenzwertbegriff, Differentialrechnung. 2., durchgesehene Auflage. 176 Seiten, 39 Figuren. 1963. (86)

Gewöhnliche Differentialgleichungen von *G. Hoheisel.* 7., neubearbeitete und erweiterte Auflage. 142 Seiten. 1965. (920/920a)

Partielle Differentialgleichungen von *G. Hoheisel.* 4., durchgesehene Auflage. 128 Seiten. 1960. (1003)

Aufgabensammlung zu den gewöhnlichen und partiellen Differentialgleichungen von *G. Hoheisel.* 4., neubearbeitete Auflage. 153 Seiten. 1964. (1059/1059a)

Integralgleichungen von *G. Hoheisel.* 2., neubearbeitete und erweiterte Auflage. 112 Seiten. 1963. (1099)

Mengenlehre von *E. Kamke.* 5. Auflage. 194 Seiten, 6 Figuren. 1965. (999/999a)

Gruppentheorie von *L. Baumgartner.* 4., erweiterte Auflage. 190 Seiten, 3 Tafeln. 1964. (837/837a)

Ebene und sphärische Trigonometrie von *G. Hessenberg†.* 5. Auflage, durchgesehen von *H. Kneser.* 172 Seiten, 60 Figuren. 1957. (99)

Darstellende Geometrie von *W. Haack.* 3 Bände.
I: Die wichtigsten Darstellungsmethoden. Grund- und Aufriß ebenflächiger Körper. 5. Auflage. 113 Seiten, 120 Abbildungen. 1965. (142)
II: Körper mit krummen Begrenzungsflächen. Kotierte Projektionen. 4., durchgesehene Auflage. 129 Seiten, 86 Abbildungen. 1965. (143)
III: Axonometrie und Perspektive. 3. Auflage. 129 Seiten, 100 Abbildungen. 1965. (144)

Analytische Geometrie von *K. P. Grotemeyer.* 3., neubearbeitete Auflage. 218 Seiten, 73 Abbildungen. 1964. (65/65a)

Nichteuklidische Geometrie. Hyperbolische Geometrie der Ebene von *R. Baldus†.* 4. Auflage, bearbeitet und ergänzt von *F. Löbell.* 158 Seiten, 75 Figuren. 1964. (970/970a)

Differentialgeometrie von *K. Strubecker.* 3 Bände.
I: Kurventheorie der Ebene und des Raumes. 2., erweiterte Auflage. 253 Seiten, 45 Figuren. 1964. (1113/1113a)
II: Theorie der Flächenmetrik. 195 Seiten, 14 Figuren. 1958. (1179/1179a)
III: Theorie der Flächenkrümmung. 254 Seiten, 38 Figuren. 1959. (1180/1180a)

Variationsrechnung von *L. Koschmieder.* 2 Bände. 2., neubearbeitete Auflage.
I: Das freie und gebundene Extrem einfacher Grundintegrale. 128 Seiten, 23 Figuren. 1962. (1074)
II: Anwendung klassischer Verfahren auf allgemeine Fragen des Extrems. — Neuere unmittelbare Verfahren. In Vorbereitung. (1075)

Einführung in die konforme Abbildung von *L. Bieberbach.* 6. Auflage. Etwa 180 Seiten, 42 Figuren. 1966. In Vorbereitung. (768/768a)

Vektoren und Matrizen von *S. Valentiner.* 4. Auflage. (11., erweiterte Auflage der „Vektoranalysis"). Mit Anhang: Aufgaben zur Vektorrechnung von *H. König.* 206 Seiten, 35 Figuren. 1967. (354/354a)

Wahrscheinlichkeitstheorie und Grundzüge der Maßtheorie von *H. Bauer.* 2 Bände.
I: 154 Seiten. 1964. (1216/1216a)
II: In Vorbereitung. (1217)

Versicherungsmathematik von *F. Böhm.* 2 Bände.
I: Elemente der Versicherungsrechnung. 3., vermehrte und verbesserte Auflage. Durchgesehener Neudruck. 151 Seiten. 1953. (180)
II: Lebensversicherungsmathematik. Einführung in die technischen Grundlagen der Sozialversicherung. 2., verbesserte und vermehrte Auflage. 205 Seiten. 1953. (917/917a)

Finanzmathematik von *M. Nicolas.* 192 Seiten, 11 Tafeln, 8 Tabellen und 72 Beispiele. 1959. (1183/1183a)

Kinematik von *H. R. Müller.* 171 Seiten, 75 Figuren. 1963. (584/584a)

Physik

Einführung in die theoretische Physik von *W. Döring.* 5 Bände.
I: Mechanik. 3., verbesserte Aufl. 125 Seiten, 23 Abb. 1965. (76)
II: Das elektromagnetische Feld. 2., verbesserte Auflage. 132 Seiten, 15 Abbildungen. 1962. (77)
III: Optik. 2., verbesserte Auflage. 117 Seiten, 32 Abbildungen. 1963. (78)
IV: Thermodynamik. 2., verbesserte Auflage. 107 Seiten, 9 Abbildungen. 1964. (374)
V: Statistische Mechanik. 2., umgearbeitete Auflage. 117 Seiten, 10 Abbildungen. 1966. (1017)

Mechanik deformierbarer Körper von *M. Pasler.* 199 Seiten, 48 Abbildungen. 1960. (1189/1189a)

Atomphysik von *K. Bechert, Ch. Gerthsen*† und *A. Flammersfeld.* 7 Bände. 4., durchgesehene Auflage.
I: Allgemeine Grundlagen. 1. Teil von *A. Flammersfeld.* 124 Seiten, 35 Abbildungen. 1959. (1009)
II: Allgemeine Grundlagen. 2. Teil von *A. Flammersfeld.* 112 Seiten, 47 Abbildungen. 1963. (1033)
III: Theorie des Atombaus. 1. Teil von *K. Bechert.* 148 Seiten, 16 Abbildungen. 1963. (1123/1123a)
IV: Theorie des Atombaus. 2. Teil von *K. Bechert.* 170 Seiten, 14 Abbildungen. 1963. (1165/1165a)

Differentialgleichungen der Physik von *F. Sauter.* 4., durchgesehene und ergänzte Auflage. 147 Seiten, 16 Figuren. 1966. (1070)

Physikalische Formelsammlung von *G. Mahler.* †. Fortgeführt von *K. Mahler.* Neubearbeitet von *H. Graewe.* 11. Auflage. 167 Seiten, 69 Figuren. 1963. (136)

Physikalische Aufgabensammlung mit Ergebnissen von *G. Mahler* †. Fortgeführt von *K. Mahler.* Neubearbeitet von *H. Graewe.* 12. Auflage. 141 Seiten. 1964. (243)

Chemie

Geschichte der Chemie in kurzgefaßter Darstellung von *G. Lockemann.* 2 Bände. 2. Auflage.
I: Vom Altertum bis zur Entdeckung des Sauerstoffs. 142 Seiten, 8 Bildnisse. In Vorbereitung. (264)
II: Von der Entdeckung des Sauerstoffs bis zur Gegenwart. 151 Seiten, 16 Bildnisse. In Vorbereitung (265/265a)

Anorganische Chemie von *W. Klemm.* 13. Auflage. 255 Seiten, 34 Abbildungen. 1964. (37/37a)

Organische Chemie von *W. Schlenk jun.* 10., erweiterte Auflage. 273 Seiten, 16 Abbildungen. 1965. (38/38a)

Physikalische Methoden in der Organischen Chemie von *G. Kresze.* 2 Bände.
I: 119 Seiten, 65 Abbildungen. 1962. (44)
II: 164 Seiten. 1962. (45/45a)

Allgemeine und physikalische Chemie von *W. Schulze.* 2 Bände.
I: 6., verbesserte Auflage. 139 Seiten, 10 Figuren. 1964. (71)
II: 6., verbesserte Auflage. 178 Seiten, 37 Figuren. 1966. (698/698a)

Molekülbau. Theoretische Grundlagen und Methoden der Strukturermittlung von *W. Schulze.* 123 Seiten, 43 Figuren. 1958. (786)

Einfache Versuche zur allgemeinen und physikalischen Chemie von *E. Dehn.* 371 Versuche mit 40 Abbildungen. 272 Seiten. 1962. (1201/1201a)

Physikalisch-chemische Rechenaufgaben von *E. Asmus.* 3., verbesserte Auflage. 96 Seiten. 1958. (445)

Maßanalyse. Theorie und Praxis der klassischen und der elektrochemischen Titrierverfahren von *G. Jander* und *K. F. Jahr.* 11., durchgesehene Auflage, mitbearbeitet von *H. Knoll.* 359 Seiten, 56 Figuren. 1966. (221/221a)

Qualitative Analyse von *H. Hofmann* u. *G. Jander*. 2., durchgesehene und verbesserte Auflage. 308 Seiten, 5 Abbildungen. 1963. (247/247 a)

Stöchiometrische Aufgabensammlung von *W. Bahrdt†* und *R. Scheer*. Mit den Ergebnissen. 8., durchgesehene Auflage. 119 Seiten. 1964. (452)

Elektrochemie von *K. Vetter*. 2 Bände.
I: In Vorbereitung. (252)
II: In Vorbereitung. (253)

Geochemie von *K. H. Wedepohl*. 220 Seiten, 26 Abbildungen, 37 Tabellen. 1966. (1224/1224 a/1224 b)

Kristallchemie von *J. Zemann*. 144 Seiten, 90 Abbildungen. 1966. (1220/1220 a)

Technologie

Die Chemie der Kunststoffe von *K. Hamann*, unter Mitarbeit von *W. Funke* und *H. D. Hermann*. 2. Aufl. 143 Seiten. 1966. In Vorbereitung. (1173/1173a)

Warenkunde von *K. Hassak* und *E. Beutel†*. 2 Bände.
I: Anorganische Waren sowie Kohle und Erdöl. 8. Auflage. Neubearbeitet von *A. Kutzelnigg*. 119 Seiten, 18 Figuren. 1958. (222)
II: Organische Waren. 8. Auflage. Vollständig neu bearbeitet von *A. Kutzelnigg*. 157 Seiten, 32 Figuren. 1959. (223)

Die Fette und Öle von *Th. Klug*. 6., verbesserte Auflage. 143 Seiten. 1961. (335)

Die Seifenfabrikation von *K. Braun* †. 3., neubearbeitete und verbesserte Auflage von *Th. Klug*. 116 Seiten, 18 Abbildungen. 1953. (336)

Thermische Verfahrenstechnik von *H. Bock*. 3 Bände.
I: Eigenschaften und Verhalten der realen Stoffe. 184 Seiten, 28 Abbildungen. 1963. (1209/1209 a)
II: Funktion und Berechnung der elementaren Geräte. 195 Seiten, 54 Abbildungen. 1964. (1210/1210 a)
III: Fließbilder, ihre Funktion und ihr Zusammenbau aus Geräten. 224 Seiten, 67 Abbildungen. 1965. (1211/1211 a)

Textilindustrie von *A. Blümcke*.
I: Spinnerei und Zwirnerei. 111 Seiten, 43 Abbildungen. 1954. (184)

Biologie

Einführung in die allgemeine Biologie und ihre philosophischen Grund- und Grenzfragen von *M. Hartmann*. 2., unveränderte Auflage. 132 Seiten, 2 Abbildungen. 1965. (96)

Hormone von *G. Koller*. 2., neubearbeitete und erweiterte Auflage. 187 Seiten, 60 Abbildungen, 19 Tabellen. 1949. (1141)

Fortpflanzung im Tier- und Pflanzenreich von *J. Hämmerling*. 2., ergänzte Auflage. 135 Seiten, 101 Abbildungen. 1951. (1138)

Geschlecht und Geschlechtsbestimmung im Tier- und Pflanzenreich von *M. Hartmann*. 2., verbesserte Auflage. 116 Seiten, 61 Abbildungen, 7 Tabellen. 1951. (1127)

Symbiose der Tiere mit pflanzlichen Mikroorganismen von *P. Buchner.* 2., verbesserte und vermehrte Auflage. 130 Seiten, 121 Abbildungen. 1949. (1128)

Grundriß der allgemeinen Mikrobiologie von *W.* u. *A. Schwartz.* 2 Bände. 2., verbesserte und ergänzte Auflage.
I: 147 Seiten, 25 Abbildungen. 1960. (1155)
II: 142 Seiten, 29 Abbildungen. 1961. (1157)

Botanik

Entwicklungsgeschichte des Pflanzenreiches von *H. Heil.* 2. Auflage. 138 Seiten, 94 Abbildungen, 1 Tabelle. 1950. (1137)

Morphologie der Pflanzen von *L. Geitler.* 3., umgearbeitete Auflage. 126 Seiten, 114 Abbildungen. 1953. (141)

Pflanzengeographie von *L. Diels†.* 5., völlig neu bearbeitete Auflage von *F. Mattick.* 195 Seiten, 2 Karten. 1958. (389/389a)

Die Laubhölzer. Kurzgefaßte Beschreibung der in Mitteleuropa gedeihenden Laubbäume und Sträucher von *F. W. Neger†* und *E. Münch†.* 3., durchgesehene Auflage, herausgegeben von *B. Huber.* 143 Seiten, 63 Figuren, 7 Tabellen. 1950. (718)

Die Nadelhölzer (Koniferen) und übrigen Gymnospermen von *F. W. Neger†* und *E. Münch†.* 4. Auflage, durchgesehen und ergänzt von *B. Huber.* 140 Seiten, 75 Figuren, 4 Tabellen, 3 Karten. 1952. (355)

Pflanzenzüchtung von *H. Kuckuck.* 2 Bände.
I: Grundzüge der Pflanzenzüchtung. 3., völlig umgearbeitete und erweiterte Auflage. 132 Seiten, 22 Abbildungen. 1952. (1134)
II: Spezielle gartenbauliche Pflanzenzüchtung (Züchtung von Gemüse, Obst und Blumen). 178 Seiten, 27 Abbildungen. 1957. (1178/1178a)

Zoologie

Entwicklungsphysiologie der Tiere von *F. Seidel.* 2 Bände.
I: Ei und Furchung. 2. Auflage. Etwa 160 Seiten, 61 Abbildungen. 1966 (1162)
II: Körpergrundgestalt und Organbildung. 2. Auflage. In Vorbereitung (1163)

Vergleichende Physiologie der Tiere von *K. Herter.* 2 Bände. 4. Auflage der „Tierphysiologie".
I: Stoff- und Energiewechsel. Neu bearbeitet von *K. Urich.* 158 Seiten, 61 Abbildungen. 1966. (972/972a)
II: Bewegung und Reizerscheinungen. Neu bearbeitet von *G. Birukow.* In Vorbereitung. (973)

Das Tierreich
I: Einzeller, Protozoen von *E. Reichenow.* 115 Seiten. 59 Abbildungen. 1956. (444)
II: Schwämme und Hohltiere von *H. J. Hannemann.* 95 Seiten, 80 Abbildungen. 1956. (442)

III: Würmer. Platt-, Hohl-, Schnurwürmer, Kamptozoen, Ringelwürmer, Protracheaten, Bärtierchen, Zungenwurmer von *S. Jaeckel*. 114 Seiten, 36 Abbildungen. 1955. (439)
IV, 1: Krebse von *H. E. Gruner* und *K. Deckert*. 114 Seiten, 43 Abbildungen. 1956. (443)
IV, 2: Spinnentiere (Trilobitomorphen, Fühlerlose) und Tausendfüßler von *A. Kaestner*. 96 Seiten, 55 Abbildungen. 1955. (1161)
IV, 3: Insekten von *H. von Lengerken*. 2., neubearbeitete Auflage. 140 Seiten, 59 Abbildungen. 1966. (594)
V: Weichtiere. Urmollusken, Schnecken, Muscheln und Kopffüßer von *S. Jaeckel*. 92 Seiten. 34 Figuren. 1954. (440)
VI: Stachelhäuter. Tentakulaten, Binnenatmer und Pfeilwürmer von *S. Jaeckel*. 100 Seiten, 46 Abbildungen. 1955. (441)
VII, 1: Manteltiere, Schädellose, Rundmäuler von *H. Fechter*. In Vorbereitung. (448)
VII, 2: Fische von *D. Lüdemann*. 130 Seiten, 65 Abbildungen. 1955. (356)
VII, 3: Lurche (Chordatiere) von *K. Herter*. 143 Seiten, 129 Abbildungen. 1955. (847)
VII, 4: Kriechtiere (Chordatiere) von *K. Herter*. 200 Seiten, 142 Abbildungen. 1960. (447/447a)
VII, 5: Vögel (Chordatiere) von *H.-A. Freye*. 156 Seiten, 69 Figuren. 1960. (869)
VII, 6: Säugetiere (Chordatiere) von *Th. Haltenorth*. In Vorbereitung. (282)

Land- und Forstwirtschaft

Landwirtschaftliche Tierzucht. Die Züchtung und Haltung der landwirtschaftlichen Nutztiere von *H. Vogel*. 139 Seiten, 11 Abbildungen. 1952. (228)

Kulturtechnische Bodenverbesserungen von *O. Fauser*. 2 Bände. 5., verbesserte und vermehrte Auflage.
I: Allgemeines, Entwässerung. 127 Seiten, 49 Abbildungen. 1959. (691)
II: Bewässerung, Ödlandkultur, Flurbereinigung. 159 Seiten, 71 Abbildungen. 1961. (692)

Agrikulturchemie von *K. Scharrer*. 2 Bände.
I: Pflanzenernährung. 143 Seiten. 1953. (329)
II: Futtermittelkunde. 192 Seiten. 1956. (330/330a)

Geologie, Mineralogie, Kristallographie

Geologie von *F. Lotze*. 3., verbesserte Auflage. 179 Seiten, 80 Abbildungen. 1965. (13/13a)

Mineral- und Erzlagerstättenkunde von *H. Huttenlocher †*. 2 Bände. 2., neubearbeitete Auflage von *P. Ramdohr*.
I: 137 Seiten, 40 Abbildungen, 2 Tabellen. 1965. (1014/1014a)
II: 135 Seiten, 41 Abbildungen. 1965. (1015/1015a)

Allgemeine Mineralogie. 11., erweiterte Auflage der „Mineralogie" von *R. Brauns †*, neubearbeitet von *K. F. Chudoba*. 152 Seiten, 143 Textfiguren, 1 Tafel, 3 Tabellen. 1963. (29/29a)

Spezielle Mineralogie. 11., erweiterte Auflage der „Mineralogie" von *R. Brauns †*, bearbeitet von *K. F. Chudoba*. 193 Seiten, 127 Textfiguren, 6 Tabellen. 1964. (31/31a)

Petrographie (Gesteinskunde) von *W. Bruhns †*. Neubearbeitet von *P. Ramdohr*. 6., erweiterte Auflage. 141 Seiten, 21 Figuren. 1966. (173)

Geochemie von *K. H. Wedepohl*. 220 Seiten, 26 Abbildungen, 37 Tabellen. 1966. (1224/1224a/1224b)

Kristallchemie von *J. Zemann*. 144 Seiten, 90 Abbildungen. 1966. (1220/1220a)

Kristallographie von *W. Bruhns †*. 6. Auflage, neubearbeitet von *P. Ramdohr*. 115 Seiten, 164 Abbildungen. 1965. (210)

Einführung in die Kristalloptik von *E. Buchwald*. 5., verbesserte Auflage. 128 Seiten, 117 Figuren. 1963. (619/619a)

Lötrohrprobierkunde. Mineraldiagnose mit Lötrohr und Tüpfelreaktion von *M. Henglein*. 4., durchgesehene und erweiterte Auflage. 108 Seiten, 12 Figuren. 1962. (483)

Technik

Graphische Darstellung in Wissenschaft und Technik von *M. Pirani.* 3., erweiterte Auflage bearbeitet von *J. Fischer* unter Benutzung der von *I. Runge* besorgten 2. Auflage. 216 Seiten, 104 Abbildungen. 1957. (728/728a)
Technische Tabellen und Formeln von *W. Müller.* 5., verbesserte und erweiterte Auflage von *E. Schulze.* 165 Seiten, 114 Abbildungen, 99 Tafeln. 1962. (579)
Einführung in die Arbeitswissenschaft von *H. H. Hilf.* 164 Seiten, 57 Abbildungen. 1964. (1212/1212a)
Grundlagen der Straßenverkehrstechnik. Theorie der Leistungsfähigkeit von *E. Engel.* 101 Seiten, 55 Abbildungen. 1962. (1198)

Elektrotechnik

Grundlagen der allgemeinen Elektrotechnik von *O. Mohr.* 3. Auflage. 260 Seiten, 136 Bilder, 14 Tafeln. 1965. (196/196a)
Die Gleichstrommaschine von *K. Humburg.* 2 Bände. 2., durchgesehene Auflage.
I: 102 Seiten, 59 Abbildungen. 1956. (257)
II: 101 Seiten, 38 Abbildungen. 1956. (881)
Die Synchronmaschine von *W. Putz.* 92 Seiten, 64 Bilder. 1962. (1146)
Induktionsmaschinen von *F. Unger.* 2., erweiterte Auflage. 142 Seiten, 49 Abbildungen. 1954. (1140)
Die komplexe Berechnung von Wechselstromschaltungen von *H. H. Meinke.* 3., neubearb. Aufl. 185 S., 126 Abb. 1965. (1156/1156a)
Theoretische Grundlagen zur Berechnung der Schaltgeräte von *F. Kesselring.* 4. Auflage. In Vorbereitung. (711/711a)
Einführung in die Technik selbsttätiger Regelungen von *W. zur Megede.* 3., durchgesehene Aufl. 180 S., 86 Abb. 1966. In Vorb. (714/714a)
Elektromotorische Antriebe von *W. Meyer.* In Vorbereitung. (827/827a)
Überspannungen und Überspannungsschutz von *G. Frühauf.* Durchgesehener Neudruck. 122 Seiten, 98 Abbildungen. 1950. (1132)
Elektrische Höchstspannungs-Schaltanlagen. Für Freiluft und Innenanordnung von *G. Meiners* und *K.-H. Wiesenewsky.* 138 Seiten, 58 Abbildungen. 1964. (796/796a)
Transformatoren von *W. Schäfer.* 4., überarbeitete und ergänzte Auflage. 130 Seiten, 73 Abbildungen. 1962. (952)

Maschinenbau

Thermische Verfahrenstechnik von *H. Bock.* 3 Bände.
I: Eigenschaften und Verhalten der realen Stoffe. 184 Seiten, 28 Abbildungen. 1963. (1209/1209a)
II: Funktion und Berechnung der elementaren Geräte. 195 Seiten, 54 Abbildungen. 1964. (1210/1210a)
III: Fließbilder, ihre Funktion und ihr Zusammenbau aus Geräten. 224 Seiten, 67 Abbildungen. 1965. (1211/1211a)
Technische Thermodynamik von *U. Grigull.* 171 Seiten, 74 Abbildungen. 1966. (1084/1084a)

Metallkunde von *H. Borchers*. 3 Bände.
I: Aufbau der Metalle und Legierungen. 6. Auflage. 120 Seiten, 90 Abbildungen, 2 Tabellen. 1964. (432)
II: Eigenschaften, Grundzüge der Form- und Zustandsgebung. 5., ergänzte und durchgesehene Auflage. 182 Seiten, 107 Abbildungen, 10 Tabellen. 1963. (433/433a)
III: Die metallkundlichen Untersuchungsmethoden von *E. Hanke*. In Vorbereitung (434)

Die Werkstoffe des Maschinenbaues von *A. Thum †* und *C. M. v. Meysenbug*. 2 Bände.
I: Einführung in die Werkstoffprüfung. 2., neubearbeitete Auflage. 100 Seiten, 7 Tabellen, 56 Abbildungen. 1956. (476)
II: Die Konstruktionswerkstoffe. 132 Seiten, 40 Abbildungen. 1959. (936)

Dynamik von *W. Müller*. 2 Bände. 2., verbesserte Auflage.
I: Dynamik des Einzelkörpers. 128 Seiten, 48 Figuren. 1952. (902)
II: Systeme von starren Körpern. 102 Seiten, 41 Figuren. 1952. (903)

Technische Schwingungslehre von *L. Zipperer*. 2 Bände. 2., neubearbeitete Auflage.
I: Allgemeine Schwingungsgleichungen, einfache Schwinger. 120 Seiten, 101 Abbildungen. 1953. (953)
II: Torsionsschwingungen in Maschinenanlagen. 102 Seiten, 59 Abbildungen. 1955. (961/961a)

Werkzeugmaschinen für Metallbearbeitung von *K. P. Matthes*. 2 Bände.
I: 100 Seiten, 27 Abbildungen, 11 Zahlentafeln, 1 Tafelanhang. 1954. (561)
II: Fertigungstechnische Grundlagen der neuzeitlichen Metallbearbeitung. 101 Seiten, 30 Abbildungen, 5 Tafeln. 1955. (562)

Das Maschinenzeichnen mit Einführung in das Konstruieren von *W. Tochtermann*. 2 Bände. 4. Auflage.
I: Das Maschinenzeichnen. 156 Seiten, 75 Tafeln. 1950. (589)
II: Ausgeführte Konstruktionsbeispiele. 130 Seiten, 58 Tafeln. 1950. (590)

Die Maschinenelemente von *E. A. vom Ende †*. 4., überarbeitete Auflage. 184 Seiten, 179 Figuren, 11 Tafeln. 1963. (3/3a)

Die Maschinen der Eisenhüttenwerke von *L. Engel*. 156 Seiten, 95 Abbildungen. 1957. (583/583a)

Walzwerke von *H. Sedlaczek †* unter Mitarbeit von *F. Fischer* und *M. Buch*. 232 Seiten, 157 Abbildungen. 1958. (580/580a)

Getriebelehre von *P. Grodzinski †*. 2 Bände. 3., neubearbeitete Auflage von *G. Lechner*.
I: Geometrische Grundlagen. 164 S., 131 Fig. 1960. (1061)
II: Angewandte Getriebelehre. In Vorbereitung. (1062)

Kinematik von *H. R. Müller*. 171 Seiten, 75 Figuren. 1963. (584/584a)

Gießereitechnik von *H. Jungbluth*. 2 Bände.
I: Eisengießerei. 126 Seiten, 44 Abbildungen. 1951. (1159)

Die Dampfkessel einschließlich Feuerungen und Hilfseinrichtungen. Physikalische und chemische Grundlagen, Berechnung und Konstruktion, Vorschriften und Beispiele von *W. Marcard.* 3., neubearbeitete Auflage von *G. Beyer.* 2 Bände.
I: Physikalische und chemische Grundlagen, Wärmelehre, Wärmeübertragung, Verbrennung. 133 Seiten, 35 Bilder, 26 Tabellen. 1964. (9/9a)
II: Berechnung und Konstruktion. Dampfkessel, Hilfseinrichtungen. Feuerungen, Berechnung. 108 Seiten, 45 Bilder. 1966. (521/521a)

Die Dampfturbinen. Ihre Wirkungsweise, Berechnung und Konstruktion von *C. Zietemann.* 3 Bände.
I: Theorie der Dampfturbinen. 4. Auflage. 139 Seiten, 48 Abbildungen. 1966. In Vorbereitung. (274)
II: Die Berechnung der Dampfturbinen und die Konstruktion der Einzelteile. 4., verbesserte Auflage. 132 Seiten, 111 Abbildungen. 1966. In Vorbereitung. (715)
III: Die Regelung der Dampfturbinen, die Bauarten, Turbinen für Sonderzwecke, Kondensationsanlagen. 3., verbesserte Auflage. 126 Seiten, 90 Abbildungen. 1956. (716)

Verbrennungsmotoren von *W. Endres.* 3 Bände.
I: Überblick. Motor-Brennstoffe. Verbrennung im Motor allgemein, im Otto- und Diesel-Motor. 153 Seiten, 57 Abbildungen. 1958. (1076/1076a)
II: Gaswechselvorgang. Aufladen. Leistung, mittl. Druck, Reibung. Wirkungsgrade und Kraftstoffverbrauch. 152 Seiten, 62 Abbildungen. 1966. (1184/1184a)
III: Die Einzelteile des Verbrennungsmotors. In Vorbereitung. (1185/1185a)

Autogenes Schweißen und Schneiden von *H. Niese.* 5. Auflage, neubearbeitet von *A. Küchler.* 136 Seiten, 71 Figuren. 1953. (499)

Die elektrischen Schweißverfahren von *H. Niese.* 2. Auflage, neubearbeitet von *H. Dienst.* 136 Seiten, 58 Abbildungen. 1955. (1020)

Die Hebezeuge. Entwurf von Winden und Kranen von *G. Tafel.* 2., verbesserte Auflage. 176 Seiten, 230 Figuren. 1954. (414/414a)

Vermessungswesen

Vermessungskunde von *W. Großmann.* 3 Bände.
I: Stückvermessung und Nivellieren. 12., verbesserte Auflage. 156 Seiten, 122 Figuren. 1965. (468)
II: Horizontalaufnahmen und ebene Rechnungen. 9., verbesserte Auflage. 136 Seiten, 101 Figuren. 1963. (469)
III: Trigonometrische und barometrische Höhenmessung. Tachymetrie und Absteckungen. 8., verbesserte Auflage. 140 Seiten, 102 Figuren. 1965. (862)

Kartographie von *V. Heissler.* 2. Auflage. 213 Seiten, 125 Abb., 8 Anlagen. 1966. (30/30a)

Photogrammetrie von *G. Lehmann.* 2., neubearbeitete Auflage. 205 Seiten, 136 Abbildungen. 1966. (1188/1188a)

Wasserbau

Wasserkraftanlagen von *A. Ludin* unter Mitarbeit von *W. Borkenstein.* 2 Bände.
I: Planung, Grundlagen und Grundzüge. 124 Seiten, 60 Abbildungen. 1955. (665)
II: Anordnung und Ausbildung der Hauptbauwerke. 184 Seiten, 91 Abbildungen. 1958. (666/666a)

Verkehrswasserbau von *H. Dehnert.* 3 Bände.
I: Entwurfsgrundlagen, Flußregelungen. 103 Seiten, 53 Abbildungen. 1950. (585)
II: Flußkanalisierung und Schiffahrtskanäle. 94 Seiten, 60 Abbildungen. 1950. (597)
III: Schleusen und Hebewerke. 98 Seiten, 70 Abbildungen. 1950. (1152)

Wehr- und Stauanlagen von *H. Dehnert.* 134 Seiten, 90 Abbildungen. 1952. (965)

Talsperren von *F. Tölke.* 122 Seiten, 70 Abbildungen. 1953. (1044)

Hoch- und Tiefbau

Die wichtigsten Baustoffe des Hoch- und Tiefbaus von *O. Graf †.* 4., verbesserte Auflage. 131 Seiten, 63 Abbildungen. 1953. (984)

Baustoffverarbeitung und Baustellenprüfung des Betons von *A. Kleinlogel.* 2., neubearbeitete und erweiterte Auflage. 126 Seiten, 35 Abbildungen. 1951. (978)

Festigkeitslehre. 2 Bände.
I: Elastizität, Plastizität und Festigkeit der Baustoffe und Bauteile von *W. Gehler †* und *W. Herberg.* Durchgesehener und erweiterter Neudruck. 159 Seiten, 118 Abbildungen. 1952. (1144)
II: Formänderung, Platten, Stabilität und Bruchhypothesen von *W. Herberg* und *N. Dimitrov.* 187 Seiten, 94 Abbildungen. 1955. (1145/1145a)

Grundlagen des Stahlbetonbaues von *A. Troche.* 2., neubearbeitete und erweiterte Auflage. 208 Seiten, 75 Abbildungen, 17 Bemessungstafeln, 20 Rechenbeispiele. 1953. (1078)

Statik der Baukonstruktionen von *A. Teichmann.* 3 Bände.
I: Grundlagen. 101 Seiten, 51 Abbildungen, 8 Formeltafeln. 1956. (119)
II: Statisch bestimmte Stabwerke. 107 Seiten, 52 Abbildungen, 7 Tafeln. 1957. (120)
III: Statisch unbestimmte Systeme. 112 Seiten, 34 Abbildungen, 7 Formeltafeln. 1958. (122)

Fenster, Türen, Tore aus Holz und Metall. Eine Anleitung zu ihrer guten Gestaltung, wirtschaftlichen Bemessung und handwerksgerechten Konstruktion von *W. Wickop †.* 5. Auflage geplant. (1092)

TECHNIK

Heizung und Lüftung von *W. Korting.* 2 Bände. 9., neubearbeitete Auflage.

I: Das Wesen und die Berechnung der Heizungs- und Lüftungsanlagen. 171 Seiten, 29 Abbildungen, 36 Zahlentafeln. 1962. (342/342a)

II: Die Ausführung der Heizungs- und Lüftungsanlagen. 1966. In Vorbereitung. (343)

Industrielle Kraft- und Wärmewirtschaft von *F. A. F. Schmidt* und *A. Beckers.* 167 Seiten, 73 Abbildungen. 1957. (318/318a)

Sammlung Göschen / Bandnummernfolge

1 Langosch, Der Nibelunge Nôt
3/3a v. Ende, Maschinenelemente
9/9a Marcard-Beyer, Dampfkessel I
10 Jiriczek-Wisniewski, Kudrun und Dietrich-Epen
13/13a Lotze, Geologie
18 Maurer, Hartmann von Aue, Der arme Heinrich
19 Altheim, Römische Geschichte I
20 Hofstaetter, Dt. Sprachlehre
22 Maurer, Gottfried von Strassburg
29/29a Brauns-Chudoba, Allgemeine Mineralogie
30/30a Heissler, Kartographie
31/31a Brauns-Chudoba, Spezielle Mineralogie
32 Schneider-Wisniewski, Deutsche Heldensage
35 Treue, Dt. Geschichte von 1648—1740
37/37a Klemm, Anorganische Chemie
38/38a Schlenk, Organische Chemie
39 Treue, Dt. Geschichte von 1713—1806
42 Behn-Hoernes, Vorgeschichte Europas
44 Kresze, Physikalische Methoden in der Organischen Chemie I
45/45a Kresze, Physikalische Methoden in der Organischen Chemie II
47 Fischer-Rohrbach, Arithmetik
51/51a Ringleb, Mathem. Formelsammlung
52 Bieler, Röm. Literaturgesch. I
59 Krahe, Indog. Sprachwiss. I
60 Biehle, Stimmkunde
61 Biehle, Redetechnik
64 Krahe, Indog. Sprachwiss. II
65/65a Grotemeyer, Analyt. Geometrie
66 Berneker-Vasmer, Russische Grammatik
70 Nestle-Liebich, Gesch. d. griechischen Literatur I
71 Schulze, Allgemeine und physikalische Chemie I
76 Döring, Einf. i. d. th. Physik I
77 Döring, Einf. i. d. th. Physik II
78 Döring, Einf. i. d. th. Physik III
79/79a Hempel, Got. Elementarbuch
80 Weigert, Stilkunde I
81 Schubert-Haussner-Erlebach Vierstell. Logarithmentafeln
86 Barner, Differential- u. Integralrechnung I
96 Hartmann, Einf. in die allgem. Biologie

99 Hessenberg-Kneser, Ebene und sphär. Trigonometrie
101 v. Wiese, Soziologie
103 Dahrendorf, Industrie- und Betriebssoziologie
104/104a Hofstätter, Sozialpsychologie
111 Hoffmann-Debrunner, Gesch. der griechischen Sprache I
114 Debrunner, Gesch. der griechischen Sprache II
117 Brandenstein, Griechische Sprachwissenschaft I
118/118a Brandenstein, Griechische Sprachwissenschaft II
119 Teichmann, Statik der Baukonstruktionen I
120 Teichmann, Statik der Baukonstruktionen II
122 Teichmann, Statik der Baukonstruktionen III
128/128a Lausberg, Romanische Sprachwissenschaft I
136 Mahler-Graewe, Physikal. Formelsammlung
141 Geitler, Morphologie der Pflanzen
142 Haack, Darst. Geometrie I
143 Haack, Darst. Geometrie II
144 Haack, Darst. Geometrie III
145/145a Weimer, Gesch. der Pädagogik
148 Kolms, Finanzwissenschaft I
156/156a Landmann, Philosophische Anthropologie
170 Oehlmann, Musik des 19. Jhs.
171/171a Oehlmann, Musik des 20. Jhs.
173 Bruhns-Ramdohr, Petrographie
174 Schlingloff, Religion des Buddhismus I
180 Böhm, Versicherungsmathematik I
184 Blümcke, Textilindustrie I
196/196a Mohr, Grundlagen der allgem. Elektrotechnik
200/200a Gottschald, Dt. Rechtschreibungswörterbuch
210 Bruhns-Ramdohr, Kristallographie
220/220a Moser, Allg. Musiklehre
221/221a Jander-Jahr-Knoll, Maßanalyse
222 Hassak-Beutel-Kutzelnigg, Warenkunde I
223 Hassak-Beutel-Kutzelnigg, Warenkunde II
226/226a Hofmann, Gesch. der Mathematik I
228 Vogel, Landw. Tierzucht
231/231a Ehrlich, Gesch. Israels
238 Krahe, Germ. Sprachwiss. I
243 Mahler-Graewe, Physikal. Aufgabensammlung
247/247a Hofmann-Jander, Qualitative Analyse
250 Lausberg, Romanische Sprachwissenschaft II
252 Vetter, Elektrochemie I
253 Vetter, Elektrochemie II
257 Humburg, Gleichstrommaschine I
264 Lockemann, Gesch. der Chemie I
265/265a Lockemann, Geschichte der Chemie II
270 Kirn, Einführung in die Geschichtswissenschaft
274 Zietemann, Dampfturbinen I
279 Jacob-Hohenleutner, Quellenkunde der deutschen Geschichte I
280 Jacob-Hohenleutner, Quellenkunde der deutschen Geschichte II
281 Leisegang, Einführung in die Philosophie
282 Haltenorth, Säugetiere
284 Jacob-Weden, Quellenkunde der deutschen Geschichte III
318/318a Schmidt-Beckers, Industrielle Kraft- u. Wärmewirtschaft
319 Krug, Australien und Ozeanien
329 Scharrer, Agrikulturchemie I
330/330a Scharrer, Agrikulturchemie II
335 Klug, Fette und Öle
336 Braun-Klug, Seifenfabrikation
342/342a Körting, Heizung und Lüftung I

343 Körting, Heizung und Lüftung II
344 Moser, Musikästhetik
354/354a Valentiner-König, Vektoren und Matrizen
355 Neger-Münch-Huber, Nadelhölzer
356 Lüdemann, Fische
374 Döring, Einf. i. d. th. Physik IV
375 Preller, Geschichte Englands I
389/389a Diels-Mattick, Pflanzengeographie
391 Kolms, Finanzwissenschaft II
394/394a Schilling, Von der Renaissance bis Kant
414/414a Tafel, Hebezeuge
422 Gottschald, Dt. Personennamen
423 Adler-Erlebach, Fünfstellige Logarithmen
432 Borchers, Metallkunde I
433/433a Borchers, Metallkunde II
434 Borchers-Hanke, Metallkunde III
435 Burau, Algebr. Kurven u. Flächen I
436/436a Burau, Algebr. Kurven und Flächen II
439 Jaeckel, Würmer
440 Jaeckel, Weichtiere
441 Jaeckel, Stachelhäuter
442 Hannemann, Schwämme und Hohltiere
443 Gruner-Deckert, Krebse
444 Reichenow, Einzeller
445 Asmus, Physikal.-chem. Rechenaufgaben
447/447a Herter, Kriechtiere
448 Fechter, Manteltiere
452 Bahrdt-Scheer, Stöchiometrische Aufgabensammlung
468 Großmann, Vermessungskunde I
469 Großmann, Vermessungskunde II
476 Thum-Meysenbug, Die Werkstoffe des Maschinenbaues I
483 Henglein, Lötrohrprobierkunde
492/492a Stolz-Debrunner-Schmid Geschichte der lateinischen Sprache
499 Niese-Küchler, Autogenes Schweißen
500 Simmel, Hauptprobleme der Philosophie
521/521a Marcard-Beyer, Dampfkessel II
536 Lehmann, Kant
538 Rumpf, Archäologie I
539 Rumpf, Archäologie II
540 Rumpf, Archäologie III
557 Nestle-Liebich, Gesch. der griech. Literatur II
561 Matthes, Werkzeugmaschinen I
562 Matthes, Werkzeugmaschinen II
564 Behn-Hoernes, Kultur der Urzeit I
565 Behn-Hoernes, Kultur der Urzeit II
566 Behn-Hoernes, Kultur der Urzeit III
571 Lehmann, Philosophie des 19. Jahrhunderts I
576/576a Moser, Gesangskunst
579 Müller-Schulze, Techn. Tabellen
580/580a Sedlaczek-Fischer-Buch, Walzwerke
583/583a Engel, Maschinen der Eisenhüttenwerke
584/584a Müller, Kinematik
585 Dehnert, Verkehrswasserbau I
587 Kalitsunakis-Steinmetz, Neugriech.-dt. Gesprächsbuch
589 Tochtermann, Maschinenzeichnen I
590 Tochtermann, Maschinenzeichnen II
594 v. Lengerken, Insekten
597 Dehnert, Verkehrswasserbau II
601 Mutschmann-Scherer, Engl. Phonetik
608/608a/608b Erman-Krückmann, Hieroglyphen
619/619a Buchwald, Kristalloptik
665 Ludin-Borkenstein, Wasserkraftanlagen I
666/666a Ludin-Borkenstein, Wasserkraftanlagen II

668 Knopp, Funktionentheorie I
677 Altheim, Rom. Geschichte II
679 Altheim, Rom. Geschichte III
684 Altheim, Rom. Geschichte IV
691 Fauser, Kulturtechn. Bodenverbesserungen I
692 Fauser, Kulturtechn. Bodenverbesserungen II
698/698a Schulze, Allgemeine u. physikalische Chemie II
703 Knopp, Funktionentheorie II
708/708a/708b Meissner-Oberhuber, Keilschrift
709 Lehmann, Philosophie des 19. Jahrhunderts II
711/711a Kesselring, Berechnung der Schaltgerate
714/714a zur Megede, Technik selbsttatiger Regelungen
715 Zietemann, Dampfturbinen II
716 Zietemann, Dampfturbinen III
718 Neger-Münch-Huber, Laubholzer
728/728a Pirani-Fischer-Runge, Graph. Darstellung in Wissenschaft u. Technik
735 Ekwall, Historische neuengl. Laut- und Formenlehre
746/746a Pfanzagl, Allg. Methodenlehre der Statistik I
747/747a Pfanzagl, Allg. Methodenlehre der Statistik II
756/756a Kalitsunakis, Gramm. d. Neugriech. Volksspr.
763/763a/763b Meyer, Hebräische Grammatik I
764/764a/764b Meyer, Hebräische Grammatik II
765/765a/765b Meyer, Hebräische Grammatik III
768/768a Bieberbach, Einführung in die konforme Abbildung
769/769a Beer-Meyer, Hebraisches Textbuch
770 Schlingloff, Religion des Buddhismus II
776/a Kolms, Finanzwissensch. III
780 Krahe, Germ. Sprachwiss. II
781 Weigert, Stilkunde II
782/782a Kolms, Finanzwissenschaft IV
786 Schulze, Molekulbau
796/796a Meiners-Wiesenewsky, Elektr. Hochstspannungs-Schaltanlagen
807 Kropp, Erkenntnistheorie
809 Moser, Harmonielehre I
810 Moser, Harmonielehre II
826 Koch, Philosophie d. Mittelalters
827/827a Meyer, Elektromotorische Antriebe
831 Erismann, Allg. Psychologie I
832/832a Erismann, Allg. Psychologie II
833 Erismann, Allg. Psychologie III
834/834a Erismann, Allg. Psychologie IV
837/837a Baumgartner, Gruppentheorie
845 Lehmann, Philosophie im ersten Drittel des 20. Jhs. I
847 Herter, Lurche
850 Lehmann, Philosophie im ersten Drittel des 20. Jhs. II
851/851a Moede, Psychologie des Berufs- und Wirtschaftslebens
857 Capelle, Griech. Philosophie I
858 Capelle, Griech. Philos. II
859 Capelle, Griech. Philos. III
862 Großmann, Vermessungskunde III
863 Capelle, Griech. Philos. IV
866 Bieler, Röm. Literaturgeschichte II
869 Freye, Vogel
875 Hofmann, Geschichte der Mathematik II
877 Knopp, Aufgabensammlung zur Funktionentheorie I
878 Knopp, Aufgabensammlung zur Funktionentheorie II
881 Humburg, Gleichstrommaschine II
882 Hofmann, Geschichte der Mathematik III
883 Stuloff, Mathematik der neuesten Zeit
893 Treue, Dt. Geschichte von 1806—1890

894 Treue, Dt. Geschichte von 1890 bis zur Gegenwart
896 Pokorny, Altirische Gramm.
902 Müller, Dynamik I
903 Müller, Dynamik II
910 Jaeger, Afrika I
911 Jaeger, Afrika II
915 Sperber-v. Polenz, Gesch. der Deutschen Sprache
917/917a Böhm, Versicherungsmathematik II
920/920a Hoheisel, Gewöhnliche Differentialgleichungen
921 Jantzen-Kolb, W. v. Eschenbach. Parzival
924/924a Brandenstein, Griechische Sprachwissenschaft III
929 Schirmer-Mitzka, Dt. Wortkunde
930 Krull, Elementare und klassische Algebra I
931 Hasse, Höhere Algebra I
932 Hasse, Höhere Algebra II
933 Krull, Elementare und klassische Algebra II
936 Thum-Meysenbug, Werkstoffe d. Maschinenbaues II
942/942a Damerau, Polnische Grammatik
952 Schäfer, Transformatoren
953 Zipperer, Techn. Schwingungslehre I
961/961a Zipperer, Techn. Schwingungslehre II
965 Dehnert, Wehr- und Stauanlagen
970/970a Baldus-Löbell, Nichteuklidische Geometrie
972/972a Herter-Urich, Vergleichende Physiologie der Tiere I
973 Herter-Birukow, Vergleichende Physiologie der Tiere II
978 Kleinlogel, Baustoffverarbeitung und Baustellenprüfung d. Betons
984 Graf, Baustoffe des Hoch- und Tiefbaues
999/999a Kamke, Mengenlehre
1000 Jaspers, Geistige Situat. der Zeit
1003 Hoheisel, Partielle Differentialgleichung
1008/1008a Mellerowicz, Allgem. Betriebswirtschaftslehre I
1009 Bechert-Gerthsen-Flammersfeld, Atomphysik I
1014/1014a Huttenlocher-Ramdohr, Mineral- und Erzlagerstättenkunde I
1015/1015a Huttenlocher-Ramdohr, Mineral- u. Erzlagerstättenkunde II
1017 Döring, Einf. i. d. th. Physik V
1020 Niese-Dienst, Elektrische Schweißverfahren
1031/1031a Apel-Ludz, Philosophisches Wörterbuch
1033 Bechert-Gerthsen-Flammersfeld, Atomphysik II
1034 Kranefeldt-Jung Therapeutische Psychologie
1035 Altheim, Röm. Religionsgeschichte I
1039 Dovifat, Zeitungslehre I
1040 Dovifat, Zeitungslehre II
1044 Tölke, Talsperren
1045 Schubert, Technik des Klavierspiels
1051/1051a Stolberg-Wernigerode, Gesch. d. Vereinigten Staaten
1052 Altheim, Röm. Religionsgeschichte II
1059/1059a Hoheisel, Aufgabenslg. z. d. gew. u. part. Differentialgleichungen
1061 Grodzinski-Lechner, Getriebelehre I
1062 Grodzinski-Lechner, Getriebelehre II
1065 Haller-Dannenbauer, Von d. Karolingern zu den Staufern
1070 Sauter, Differentialgleichungen der Physik
1074 Koschmieder, Variationsrechnung I
1075 Koschmieder, Variationsrechnung II
1076/1076a Endres, Verbrennungsmotoren I

1077 Haller-Dannenbauer, Von den Staufern zu den Habsburgern
1078 Troche, Stahlbetonbau
1082 Hasse-Klobe, Aufgabensammlung zur höheren Algebra
1084/1084a Grigull, Techn. Thermodynamik
1085 Lietzmann-Aland, Zeitrechnung
1086 Müller, Dt. Dichten und Denken
1088 Preller, Gesch. Englands II
1092 Wickop, Fenster, Turen, Tore
1094 Hernried, System, Modulation
1096 Viëtor, Dt. Dichten und Denken
1099 Hoheisel, Integralgleichungen
1105 Hartung, Dt. Geschichte im Zeitalter der Reformation
1108 de Boor-Wisniewski, Mittelhochdeutsche Grammatik
1109 Knopp, Elemente der Funktionentheorie
1111/1111a Naumann-Betz, Althochdt. Elementarbuch
1113/1113a Strubecker, Differentialgeometrie I
1114 Schubel, Engl. Literaturgeschichte I
1115/1115a Ranke-Hofmann, Altnord. Elementarbuch
1116 Schubel, Engl. Literaturgeschichte II
1117 Haller-Dannenbauer, Eintritt der Germanen in die Geschichte
1121 Naumann, Dt. Dichten u. Denken
1122/1122a Jesch, Sprecherziehung
1123/1123a Bechert-Gerthsen-Flammersfeld, Atomphysik III
1124 Schubel, Engl. Literaturgeschichte III
1125 Lehnert, Altengl. Elementarbuch
1127 Hartmann, Geschlecht u. Geschlechtsbestimmung im Tier- und Pflanzenreich
1128 Buchner, Symbiose d. Tiere
1130 Dibelius-Kümmel, Jesus
1131 Scholz-Schoeneberg, Einführung in die Zahlentheorie
1132 Frühauf, Überspannungen
1134 Kuckuck, Pflanzenzüchtung I
1135 Lehnert, Beowulf
1137 Heil, Entwicklungsgesch. d. Pflanzenreiches
1138 Hämmerling, Fortpflanzung im Tier- und Pflanzenreich
1140 Unger, Induktionsmaschine
1141 Koller, Hormone
1142 Meissner-Lehnert, Shakespeare
1144 Gehler-Herberg, Festigkeitslehre I
1145/1145a Herberg-Dimitrov, Festigkeitslehre II
1146 Putz, Synchronmaschine
1147 v. Waltershausen, Kunst d. Dirigierens
1148 Pepping, Der polyphone Satz I
1152 Dehnert, Verkehrswasserbau III
1153/1153a Mellerowicz, Allgem. Betriebswirtschaftslehre II
1154/1154a Mellerowicz, Allgem. Betriebswirtschaftslehre III
1155 Schwartz, Mikrobiologie I
1156/1156a Meinke, Komplexe Berechnungen v. Wechselstromschaltungen
1157 Schwartz, Mikrobiologie II
1158/1158a Mayrhofer, Sanskrit-Grammatik
1159 Jungbluth, Gießereitechnik I
1160 Dibelius-Kümmel, Paulus
1161 Kaestner, Spinnentiere
1162 Seidel, Entwicklungsphysiologie der Tiere I
1163 Seidel, Entwicklungsphysiologie der Tiere II
1164/1164a Pepping, Der polyphone Satz II

1165/1165a Bechert-Gerthsen-Flammersfeld, Atomphysik IV
1169 Paulsen, Allgemeine Volkswirtschaftslehre I
1170 Paulsen, Allgemeine Volkswirtschaftslehre II
1171 Paulsen, Allgemeine Volkswirtschaftslehre III
1172 Paulsen, Allgemeine Volkswirtschaftslehre IV
1173/1173a Hamann-Funke-Hermann, Chemie der Kunststoffe
1176/1176a Lorenzen, Form. Logik
1178/1178a Kuckuck, Pflanzenzüchtung II
1179/1179a Strubecker, Differentialgeometrie II
1180/1180a Strubecker, Differentialgeometrie III
1181 Franz, Topologie I
1182/1182a Franz, Topologie II
1183/1183a Nicolas, Finanzmathematik
1184/1184a Endres, Verbrennungsmotoren II
1185/1185a Endres, Verbrennungsmotoren III
1186/1186a Mellerowicz, Allgem. Betriebswirtschaftslehre IV
1187 Lau, Luther
1188/1188a Lehmann, Photogrammetrie
1189/1189a Päsler, Mechanik
1190 Stupperich, Melanchthon
1191/1191a Bräuer, Slav. Sprachwissenschaft I
1193 Fürstenberg, Wirtschaftssoziologie
1194 Wendt, Gesch. d. Volkswirtschaftslehre
1195 Ohm Allgem. Volkswirtschaftspolitik I
1196 Ohm, Allgem. Volkswirtschaftspolitik II
1197/1197a Onasch, Einf. in die Konfessionskunde der orthodoxen Kirchen
1198 Engel, Straßenverkehrstechnik
1199 Lausberg, Romanische Sprachwissenschaft III, 1. Teil
1200/1200a Lausberg, Romanische Sprachwissenschaft III, 2. Teil
1201/1201a Dehn, Versuche zur allgem. u. phys. Chemie
1202/1202a Nagel, Gesch. des christl. Gottesdienstes
1203 Wendland, Sozialethik
1204 Scheurig, Zeitgeschichte
1205/1205a Hofmann, Ideengeschichte d. soz. Bewegung
1206/1206a Langen, Lineare Programmierung
1208 Lausberg, Romanische Sprachwissenschaft IV
1209/1209a Bock, Therm. Verfahrenstechnik I
1210/1210a Bock. Therm. Verfahrenstechnik II
1211/1211a Bock, Therm. Verfahrenstechnik III
1212/1212a Hilf, Arbeitswissenschaft
1213/1213a Kosiol, Buchhaltung und Bilanz
1216/1216a Bauer, Wahrscheinlichkeitstheorie I
1217 Bauer, Wahrscheinlichkeitstheorie II
1218/1218a/1218b Meid, Germ. Sprachwiss. III
1219 Schmidt-Clausing, Zwingli
1220/1220a Zemann, Kristallchemie
1221 Gerdes, Kierkegaard
1222/1222a Tschižewskij, Slav. Literaturen I
1223/1223a Tschižewskij, Slav. Literaturen II
1224/1224a/1224b Wedepohl, Geochemie
1225/1225a Schneider-Jurksch, Datenverarbeitungsanlagen
1226/1226a Weinstock, Mittelenglisches Elementarbuch
1227/1227a Wedig, Übungsaufgaben zur Allgem. Volkswirtschaftslehre I/II

Autorenregister

Printed in Germany 150. VIII. 66