Die Grundlehren der Mathematischen Wissenschaften

B. L. van der Waerden

Moderne Algebra

DIE GRUNDLEHREN DER

MATHEMATISCHEN WISSENSCHAFTEN

IN EINZELDARSTELLUNGEN MIT BESONDERER BERÜCKSICHTIGUNG DER ANWENDUNGSGEBIETE

GEMEINSAM MIT

W. BLASCHKE
HAMBURG

M. BORN
GÖTTINGEN

C. RUNGE†
GÖTTINGEN

HERAUSGEGEBEN VON

R. COURANT
GÖTTINGEN

BAND XXXIV

MODERNE ALGEBRA II

VON

B. L. VAN DER WAERDEN

Springer-Verlag Berlin Heidelberg GmbH

1931

MODERNE ALGEBRA

VON

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

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

ZWEITER TEIL

Springer-Verlag Berlin Heidelberg GmbH
1931

ISBN 978-3-662-41958-8 ISBN 978-3-662-42016-4 (eBook)
DOI 10.1007/978-3-662-42016-4

URSPRÜNGLICH ERSCHIENEN BEI JULIUS SPRINGER IN BERLIN 1931.
SOFTCOVER REPRINT OF THE HARDCOVER 1ST EDITION 1931

Inhaltsverzeichnis.

Elftes Kapitel.

Eliminationstheorie.

Zwölftes Kapitel.

Allgemeine Idealtheorie der kommutativen Ringe.

Dreizehntes Kapitel.

Theorie der Polynomideale.

Vierzehntes Kapitel.

Ganze algebraische Größen.

Fünfzehntes Kapitel.

Lineare Algebra.

Sechzehntes Kapitel.

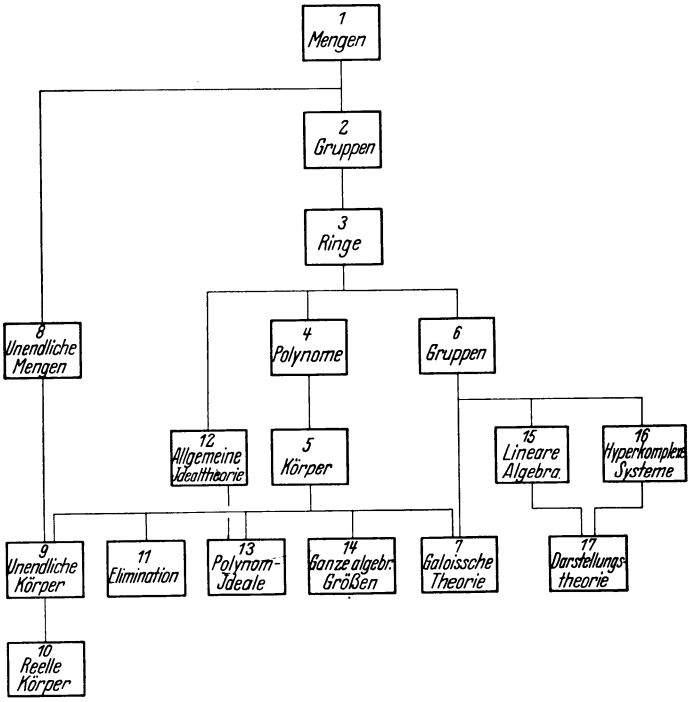
Theorie der hyperkomplexen Größen.

Siebzehntes Kapitel.

Darstellungstheorie der Gruppen und hyperkomplexen Systeme.

Leitfaden.

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



Elftes Kapitel.

Eliminationstheorie.

Die Eliminationstheorie untersucht Systeme von algebraischen Gleichungen in mehreren Unbekannten und sucht Bedingungen für ihre Lösbarkeit sowie Formeln zur Berechnung der Lösungen in verschiedenen Fällen aufzustellen. Dabei wird die entsprechende Theorie für lineare Gleichungen, d. h. die Determinantentheorie, als bekannt vorausgesetzt. Weiter wird als bekannt vorausgesetzt, daß man *eine* Gleichung höheren Grades in *einer* Unbekannten lösen kann, oder genauer, daß man, wenn die Gleichung in einem vorgegebenen Körper noch nicht lösbar ist, einen Erweiterungskörper konstruieren kann, in dem sie lösbar wird, und sogar einen, in dem sie vollständig zerfällt (Kap. 5). Wenn im folgenden von „Lösungen einer Gleichung" oder „Nullstellen eines Polynoms" die Rede ist, sind immer solche Lösungen in einem passend gewählten Erweiterungskörper des festen kommutativen Grundkörpers K gemeint.

§ 71. Die Resultante zweier Polynome.

Es seien

$$f(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_n,$$
$$g(x) = b_0 x^m + b_1 x^{m-1} + \cdots + b_m$$

zwei Polynome in $\mathsf{K}[x]$. Da es bei späteren Anwendungen vorkommen wird, daß die a_ν und b_ν noch von anderen Variablen abhängen und für spezielle Werte dieser Variablen gelegentlich verschwinden, so schließen wir von vornherein die Möglichkeit nicht aus, daß $a_0 = 0$ oder $b_0 = 0$ sein kann. Wenn das Polynom $f(x)$ in der angegebenen Gestalt hingeschrieben wird, anfangend mit einem (eventuell verschwindenden) Glied $a_0 x^n$, so nennen wir n den *formalen Grad* des Polynoms und a_0 den *formalen Anfangskoeffizienten*. Wir nehmen vorläufig an, daß mindestens einer der beiden Anfangskoeffizienten a_0, b_0 nicht verschwindet.

Die Bedingung für die Existenz einer gemeinsamen Lösung der Gleichungen $f = 0$, $g = 0$ ist die, daß die beiden Polynome f, g einen nicht konstanten Faktor $\varphi(x)$ gemein haben. Wir zeigen zunächst, daß

dies dann und nur dann der Fall ist, wenn eine Gleichung der Gestalt

$$h(x)f(x) = k(x)g(x) \tag{1}$$

besteht, wo $h(x)$ höchstens vom Grade $m-1$, $k(x)$ höchstens vom Grade $n-1$ ist und nicht beide Polynome h, k identisch verschwinden.

Ist nämlich (1) erfüllt und zerlegt man die beiden Seiten der Gleichung (1) in Primfaktoren, so muß links und rechts dasselbe herauskommen. Wir können annehmen, daß etwa $f(x)$ wirklich den Grad n hat ($a_0 \neq 0$); denn andernfalls brauchen wir nur die Rollen von $f(x)$ und $g(x)$ zu vertauschen. Alle Primfaktoren von $f(x)$ müssen auch in der rechten Seite von (1) mindestens gleich oft wie in $f(x)$ aufgehen. In $k(x)$ allein können nicht alle so oft vorkommen; denn $k(x)$ hat höchstens den Grad $n-1$ und verschwindet nicht identisch. Also kommt ein Primfaktor von $f(x)$ auch in $g(x)$ vor, was wir beweisen wollten.

Ist umgekehrt $\varphi(x)$ ein nicht konstanter gemeinsamer Faktor von $f(x)$ und $g(x)$, so hat man nur zu setzen

$$f(x) = \varphi(x)k(x),$$
$$g(x) = \varphi(x)h(x),$$

und die Gleichung (1) ist erfüllt.

Um nun die Gleichung (1) weiter zu untersuchen, setzen wir

$$h(x) = c_0x^{m-1} + c_1x^{m-2} + \cdots + c_{m-1},$$
$$k(x) = d_0x^{n-1} + d_1x^{n-2} + \cdots + d_{n-1}.$$

Auswertung der Gleichung (1) und Vergleichung der Koeffizienten der Potenzen x^{n+m-1}, x^{n+m-2}, ..., x, 1 links und rechts ergibt das folgende lineare Gleichungssystem für die Koeffizienten c_i und d_j:

$$\left\{\begin{array}{rl}
c_0a_0 & = d_0b_0,\\
c_0a_1 + c_1a_0 & = d_0b_1 + d_1b_0,\\
c_0a_2 + c_1a_1 + c_2a_0 & = d_0b_2 + d_1b_1 + d_2b_0,\\
\multicolumn{2}{c}{\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots}\\
c_{m-2}a_n + c_{m-1}a_{n-1} & = d_{n-2}b_m + d_{n-1}b_{m-1},\\
c_{m-1}a_n & = d_{n-1}b_m.
\end{array}\right. \tag{2}$$

Das sind $n+m$ homogene lineare Gleichungen für die $n+m$ Größen c_i, d_j. Von diesen Größen wird verlangt, daß sie nicht sämtlich verschwinden. Die Bedingung dafür ist das Verschwinden der Determinante. Um Minuszeichen in der Determinante zu vermeiden, kann man, nachdem man die rechten Seiten von (2) nach links gebracht hat, die Größen c_i und $-d_j$ als Unbekannte auffassen. Vertauscht man dann noch Zeilen und Spalten der Determinante (Spiegelung an der Hauptdiagonale), so

nimmt sie die Gestalt

$$(3) \qquad R = \begin{vmatrix} a_0 & a_1 & \dots & a_n & & & \\ & a_0 & a_1 & \dots & a_n & & \\ & & \dots & \dots & \dots & & \\ & & & a_0 & a_1 & \dots & a_n \\ b_0 & b_1 & \dots & b_m & & & \\ & b_0 & b_1 & \dots & b_m & & \\ & & \dots & \dots & \dots & & \\ & & & b_0 & b_1 & \dots & b_m \end{vmatrix} \begin{matrix} \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} m \text{ Zeilen} \\ \left.\vphantom{\begin{matrix}a\\a\\a\\a\end{matrix}}\right\} n \text{ Zeilen} \end{matrix}$$

an. (Überall, wo nichts hingeschrieben ist, sind Nullen zu denken.)

Die angeschriebene Determinante nennt man die *Resultante* der Polynome $f(x)$, $g(x)$. Zu bemerken ist, daß sie homogen vom Grade m in den a_i und homogen vom Grade n in den b_j ist; weiter, daß sie das „Hauptglied" $a_0^m b_m^n$ (Hauptdiagonale) enthält, und schließlich, daß sie nicht nur verschwindet, wenn die Polynome f, g einen gemeinsamen Faktor haben, sondern auch dann, wenn (entgegen der zu Anfang gemachten Voraussetzung) $a_0 = b_0 = 0$ ist.

Fassen wir zusammen:

Die Resultante zweier Polynome $f(x)$, $g(x)$ ist eine ganze rationale Form in den Koeffizienten von der Gestalt (3). *Verschwindet die Resultante, so haben die Polynome f, g entweder einen gemeinsamen nicht konstanten Faktor oder in beiden verschwindet der Anfangskoeffizient, und umgekehrt.*

Die hier befolgte Eliminationsmethode stammt von EULER; die Gestalt (3) der Resultante wird meist nach SYLVESTER benannt.

Der Ausnahmefall $a_0 = b_0 = 0$ in der Formulierung des Satzes läßt sich vermeiden, entweder indem man von vornherein $a_0 = 1$ setzt, was wir im folgenden bisweilen tun werden, oder in einer mehr symmetrischen Weise, indem man von zwei homogenen Formen in zwei Variablen statt von Polynomen in einer Variablen ausgeht:

$$F(x) = a_0 x_1^n + a_1 x_1^{n-1} x_2 + \dots + a_n x_2^n,$$
$$G(x) = b_0 x_1^m + b_1 x_1^{m-1} x_2 + \dots + b_m x_2^m.$$

Die ursprünglichen Polynome f, g und die Zahlen n, m bestimmen die Formen F, G eindeutig, und umgekehrt. Jeder Faktorzerlegung von f:

$$f(x) = a_0 x^n + a_1 x^{n-1} + \dots + a_n$$
$$= (p_0 x^r + \dots + p_r)(q_0 x^s + \dots + q_s),$$

entspricht eine Zerlegung von F:

$$F(x) = a_0 x_1^n + \dots + a_n x_2^n$$
$$= (p_0 x_1^r + \dots + p_r x_2^r)(q_0 x_1^s + \dots + q_s x_2^s),$$

und entsprechendes gilt für g und G. Ebenso entspricht jedem gemeinsamen Faktor von f und g ein gemeinsamer Faktor von F und G. Wird aber $a_0 = b_0 = 0$, so haben F und G den gemeinsamen Faktor x_2; also lassen sich die beiden im obigen Satz formulierten Fälle, in denen die Resultante verschwindet, zu einer einzigen Aussage: „F und G haben einen gemeinsamen Faktor", zusammenfassen. Aus einer Lösung $\{\xi_1, \xi_2\}$ der Gleichungen $F = 0$, $G = 0$ erhält man, falls $\xi_2 \neq 0$ ist, eine Lösung $\xi = \xi_1 : \xi_2$ der ursprünglichen Gleichungen $f = 0$, $g = 0$. Ist aber $\xi_2 = 0$ und $\xi_1 \neq 0$, so hat man $a_0 = b_0 = 0$. Die immer vorhandene Lösung $\xi_1 = \xi_2 = 0$ ist trivial und zählt nicht mit.

Wir kehren wieder zu den inhomogenen Polynomen f und g zurück, deren Koeffizienten a_μ, b_ν wir jetzt als Unbestimmte auffassen, und setzen

$$\begin{aligned}
x^{m-1}f(x) &= a_0x^{n+m-1} + a_1x^{n+m-2} + \cdots + a_nx^{m-1},\\
x^{m-2}f(x) &= \qquad a_0x^{n+m-2} + \cdots\cdots + a_nx^{m-2},\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
f(x) &= \qquad\qquad a_0x^n + \cdots\cdots\cdots\cdots + a_n;\\
x^{n-1}g(x) &= b_0x^{n+m-1} + b_1x^{n+m-2} + \cdots + b_mx^{n-1},\\
x^{n-2}g(x) &= \qquad b_0x^{n+m-2} + \cdots\cdots + b_mx^{n-2},\\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\
g(x) &= \qquad\qquad b_0x^m + \cdots\cdots\cdots\cdots + b_m.
\end{aligned}$$

Die Determinante der rechten Seite dieses Gleichungssystems ist genau R. Eliminiert man rechts $x^{n+m-1}, \ldots, x$, indem man mit den Unterdeterminanten der letzten Spalte multipliziert und addiert, so kommt links ein Polynom der Gestalt

$$Af + Bg,$$

wo A und B Polynome in x und den a_μ, b_ν sind, und rechts kommt R. *Mithin ist*

$$R \equiv 0\,(f, g)\ ^*$$

im ganzzahligen Polynombereich der x, a_μ, b_ν **.

§ 72. Die Resultante als symmetrische Funktion der Wurzeln.

Klammert man aus R zunächst den Faktor $a_0^m b_0^n$ aus, so bleibt ein Polynom R^* in $\frac{a_1}{a_0}, \ldots, \frac{a_n}{a_0}, \frac{b_1}{b_0}, \ldots, \frac{b_m}{b_0}$ übrig. Diese Quotienten haben die Werte $-s_1, s_2, \ldots, (-1)^n s_n$; $-\sigma_1, \sigma_2, \ldots, (-1)^m \sigma_m$, wo die s bzw. σ die elementarsymmetrischen Funktionen der Wurzeln $\xi_1, \ldots, \xi_n$ von f und $\eta_1, \ldots, \eta_m$ von g bedeuten. Die Funktion R^*, als Funktion

* Das ist eine kurze Schreibweise für $R \equiv 0 \pmod{(f, g)}$. Ähnlich in Zukunft.

** Für die Formen F, G würde die entsprechende Relation lauten: $x_2^{n+m-1} R \equiv 0\ (F, G)$.

der ξ und η aufgefaßt, verschwindet für $\xi_i = \eta_k$ und ist daher durch $\xi_i - \eta_k$ teilbar (§ 19), also auch durch das Produkt

$$\prod_i \prod_k (\xi_i - \eta_k).$$

R selbst ist also durch

$$S = a_0^m b_0^n \prod_i \prod_k (\xi_i - \eta_k) \tag{1}$$

teilbar. Dieses Produkt kann man nun in zweierlei Weisen umformen. Erstens folgt aus

$$g(x) = b_0 \prod_k (x - \eta_k)$$

durch die Substitution $x = \xi_i$ und Produktbildung

$$\prod_i g(\xi_i) = b_0^n \prod_i \prod_k (\xi_i - \eta_k),$$

mithin

$$S = a_0^m \prod_i g(\xi_i). \tag{2}$$

Zweitens folgt aus

$$f(x) = a_0 \prod_i (x - \xi_i) = (-1)^n a_0 \prod_i (\xi_i - x)$$

in derselben Weise

$$S = (-1)^{n\,m} b_0^n \prod_k f(\eta_k). \tag{3}$$

Aus (2) sieht man, daß S ganz und homogen vom Grade n in den b ist, und aus (3), daß S ganz und homogen vom Grade m in den a ist. R hat aber dieselben Gradzahlen und ist durch S teilbar; also muß R mit S bis auf einen ganzen Zahlenfaktor übereinstimmen. Der Vergleich derjenigen Glieder links und rechts, die die höchste Potenz von b_m enthalten, ergibt sowohl in R wie in S ein Glied $+ a_0^m b_m^n$, und das ergibt für den Zahlenfaktor den Wert 1; mithin ist

$$R = S.$$

Damit sind für R die drei Darstellungen (1), (2), (3) gefunden.

Hieraus ergibt sich leicht auch die *Unzerlegbarkeit der Resultante* als Polynom in den Unbestimmten $a_0, \ldots, b_m$, und zwar nicht nur die Unzerlegbarkeit im ganzzahligen Polynombereich, sondern auch die *absolute Irreduzibilität*, d. h. die Unzerlegbarkeit im Polynombereich derselben Unbestimmten mit einem beliebigen Körper als Koeffizientenbereich. Wäre nämlich R zerlegbar in zwei (natürlich homogene) Faktoren A, B, so könnte man wieder A und B als symmetrische Funktionen der Wurzeln schreiben. Da R durch $\xi_1 - \eta_1$ teilbar ist, so muß A oder B, etwa A, es auch sein. Als symmetrische Funktion muß dann aber A auch durch alle anderen $\xi_i - \eta_k$, also durch ihr Produkt

$$\prod_i \prod_k (\xi_i - \eta_k)$$

teilbar sein. Wegen

$$R = a_0^m b_0^n \prod\prod (\xi_i - \eta_k)$$

bleibt für den anderen Faktor B nur die Möglichkeit $B = \text{konst.}\, a_0^p b_0^q$. Aber R ist als Polynom in den a und b weder durch a_0 noch durch b_0 teilbar; also bleibt nur $B = \text{konst.}$ übrig. Damit ist die Irreduzibilität von R bewiesen.

Ein anderer Beweis findet sich bei F. S. MACAULAY: Algebraic Theory of Modular Systems. § 3. Cambridge 1916.

Aufgaben. 1. Man gebe ein Determinantenkriterium dafür, daß $f(x)$ und $g(x)$ einen Faktor von mindestens dem Grade k gemein haben.

2. Für zwei Polynome zweiten Grades ist

$$4R = (2a_0b_2 - a_1b_1 + 2a_2b_0)^2 - (4a_0a_2 - a_1^2)(4b_0b_2 - b_1^2).$$

3. Die Resultante eines Polynoms $f(x) = x^n + \cdots$ und seiner Ableitung $f'(x)$ ist die Diskriminante von $f(x)$ (§ 24).

4. Die Resultante ist in den a und b zusammen isobar vom Gewichte mn (vgl. § 24).

§ 73. Das Resultantensystem für mehrere Polynome in einer Veränderlichen.

Satz. *Für r Polynome $f_1, \ldots, f_r$ in einer Veränderlichen von gegebenen Gradzahlen mit unbestimmten Koeffizienten existiert ein System $D_1, \ldots, D_h$ von ganzzahligen Polynomen in den Koeffizienten, mit der Eigenschaft, daß für spezielle Werte der Koeffizienten aus einem Körper* K *die Bedingungen $D_1 = 0, \ldots, D_h = 0$ notwendig und hinreichend sind dafür, daß entweder die Gleichungen $f_1 = 0, \ldots, f_r = 0$ in einem passenden Erweiterungskörper lösbar sind oder die formalen Anfangskoeffizienten aller Polynome $f_1, \ldots, f_r$ verschwinden.*

Der Beweis wird nach der *Kroneckerschen Eliminationsmethode* geführt.

Wir verwandeln die Polynome $f_1, \ldots, f_r$ zunächst in Polynome gleichen Grades, indem wir, wenn n die höchste ihrer (formalen) Gradzahlen ist, jedes Polynom f_i von kleinerem Grad n_i mit x^{n-n_i} und mit $(x-1)^{n-n_i}$ multiplizieren; dadurch entstehen aus f_i zwei Polynome vom formalen Grad n, deren gemeinsame Nullstellen bei irgendeiner Spezialisierung der Koeffizienten mit den Nullstellen von f_i und deren Anfangskoeffizienten mit dem von f_i übereinstimmen. Das so entstehende System von Polynomen gleichen Grades, welches eventuell einige Polynome mehr enthält als das System $f_1, \ldots, f_r$, aber genau dieselben gemeinsamen Nullstellen hat, bezeichnen wir mit $g_1, \ldots, g_s$.

Wir bilden nun aus $g_1, \ldots, g_s$ die Linearkombinationen

$$g_u = u_1 g_1 + \cdots + u_s g_s;\ g_v = v_1 g_1 + \cdots + v_s g_s$$

mit unbestimmten u, v, die dem Körper K adjungiert werden. Wenn g_u und g_v für spezielle Werte der Koeffizienten von $g_1, \ldots, g_s$ einen Faktor gemein haben, so ist dieser Faktor rational in den u und v bestimmbar (§ 16). Ein von den v wirklich abhängiger rationaler Faktor kann aber bei der Zerlegung von g_u nicht auftreten, da g_u von den v nicht abhängt. Also muß jeder gemeinsame Faktor von g_u und g_v von den v und ebenso von den u unabhängig sein und daher in $g_1, g_2, \ldots, g_s$ aufgehen. Umgekehrt, wenn $g_1, \ldots, g_s$ einen Faktor gemein haben, so geht dieser auch in g_u und g_v auf.

Notwendig und hinreichend dafür, daß g_u und g_v einen Faktor gemein haben oder daß in ihnen die Anfangskoeffizienten verschwinden, ist aber das Verschwinden ihrer Resultante R

(1) $$R = 0 \quad \text{identisch in den } u \text{ und } v.$$

Ordnet man R nach Potenzprodukten der u und v und nennt die Koeffizienten $D_1, \ldots, D_h$, so ist (1) äquivalent mit

$$D_1 = 0, \; D_2 = 0, \; \ldots, \; D_h = 0.$$

Die D_i sind aber ganzzahlige Polynome in den unbestimmten Koeffizienten von $f_1, f_2, \ldots, f_r$. Damit ist der Satz völlig bewiesen.

Das System $D_1, \ldots, D_h$ heißt das *Resultantensystem* der Polynome $f_1, \ldots, f_r$.

Aus § 71 folgt

$$\begin{aligned} R &\equiv 0\,(g_u, g_v) \\ &\equiv 0\,(g_1, \ldots, g_s) \\ &\equiv 0\,(f_1, f_2, \ldots, f_r), \end{aligned}$$

und daraus, wenn man auf beiden Seiten nach Potenzprodukten der u_i und v_i ordnet,

(2) $$(D_1, \ldots, D_h) \equiv 0\,(f_1, \ldots, f_r).$$

Bemerkungen. 1. Wenn man von einem der Polynome f_ν, etwa von f_1 von vornherein weiß, daß sein formaler Anfangskoeffizient nicht verschwindet, so kann die ganze vorbereitende Operation, wodurch die Polynome f_ν in solche gleichen Grades verwandelt werden, unterbleiben. Außerdem kann man dann die Rechnung vereinfachen, indem man, statt von g_u und g_v, von f_1 und $v_2 f_2 + \cdots + v_r f_r$ die Resultante bildet.

2. Man kann natürlich, wie im § 71, den Ausnahmefall des Verschwindens aller Anfangskoeffizienten formal aufheben durch Übergang zu homogenen Formen in x_1 und x_2. Die Bildung der g_i aus den f_i kann dann geschehen durch Multiplikation mit $x_1^{n-n_i}$ und $x_2^{n-n_i}$ (statt x^{n-n_i} und $(x-1)^{n-n_i}$).

3. Im Fall eines einzigen Polynoms ergibt die Anwendung des beschriebenen Verfahrens ein Resultantensystem, das nur aus der Null besteht.

§ 74. Allgemeine Eliminationstheorie.

Im folgenden bedeutet $\{\xi_1, \ldots, \xi_n\}$ immer eine Reihe von n mit Nummern versehenen Elementen eines passend gewählten Erweiterungskörpers des festen Grundkörpers K. Hat ein Polynom f die Eigenschaft $f(\xi_1, \ldots, \xi_n) = 0$, so heißt die Reihe $\{\xi_1, \ldots, \xi_n\}$ oder kurz ξ eine *Nullstelle* von f. Die allgemeine Eliminationstheorie behandelt nun die Aufgabe, alle Lösungen eines beliebigen algebraischen Gleichungssystems

$$f_1(\xi) = 0, \; f_2(\xi) = 0, \; \ldots, \; f_r(\xi) = 0,$$

d. h. alle gemeinsamen Nullstellen der Polynome $f_1, \ldots, f_r$ aus $\mathsf{K}[x_1, \ldots, x_n]$ wenigstens theoretisch zu bestimmen[1].

Die Methode dazu ist die „sukzessive Elimination" aller Unbekannten mit Hilfe des Resultantensystems des vorigen Paragraphen. Dabei ist es zweckmäßig, anzunehmen, daß im System $f_1, \ldots, f_r$ ein Polynom etwa vom Grade α vorkommt, in dem der Koeffizient von x_1^α eine von Null verschiedene Konstante ist. Diese Forderung kann unter Umständen von vornherein erfüllt sein; wenn nicht, so verfahren wir folgendermaßen: *Entweder* verschwinden alle Polynome $f_1, \ldots, f_r$ identisch; dann sind alle Wertsysteme $\{\xi_1, \ldots, \xi_n\}$ Lösungen. Dieser Fall braucht uns also nicht weiter zu interessieren. *Oder* es gibt ein f_i, etwa f_1, das nicht identisch verschwindet. Dann führen wir neue Veränderliche $x_1', \ldots, x_n'$ ein durch die Substitution

$$(1) \qquad \left| \begin{array}{l} x_1 = u_1 x_1', \\ x_2 = x_2' + u_2 x_1', \\ \cdots\cdots\cdots\cdots \\ x_n = x_n' + u_n x_1', \end{array} \right.$$

wo $u_1, \ldots, u_n$ Unbestimmte sind, die dem Körper K adjungiert werden. Setzt man (1) in $f_1, \ldots, f_r$ ein, so entstehen neue Polynome $f_1', \ldots, f_r'$ * in $x_1', \ldots, x_n'$, in denen jetzt der Koeffizient der höchsten Potenz von x_1' ein nichtverschwindendes Polynom in $u_1, \ldots, u_n$ ist. Bedeutet nämlich α den Grad des Polynoms f_1, so ist

$$f_1' = f_1(u_1 x_1', \; x_2' + u_2 x_1', \; \ldots, \; x_n' + u_n x_1')$$

und der Koeffizient von $x_1'^\alpha$ in diesem Ausdruck ist $f_1^*(u_1, \ldots, u_n)$, wo f_1^* den Bestandteil höchsten (α-ten) Grades in f_1 darstellt[2].

---

[1] Praktisch sind die damit verbundenen Rechnungen sehr oft zu kompliziert, um sie wirklich durchführen zu können.

* Der Strich soll natürlich diesmal nicht die Ableitung bedeuten.

[2] Bemerkung: Statt unbestimmter u_ν kann man natürlich auch spezielle Werte der u_ν im Grundkörper oder (falls dieser endlich sein sollte) in einem passend gewählten Erweiterungskörper benutzen, die so gewählt werden, daß $f_1^*(u_1, \ldots, u_n)$ für sie nicht verschwindet.

Nunmehr kann man x_1' eliminieren und findet ein Resultantensystem

$$d_1, \ldots, d_l,$$

das nur noch von $x_2', \ldots, x_n'$ abhängt. Jede Nullstelle $\{\xi_2', \ldots, \xi_n'\}$ dieses Resultantensystems führt (da für das Nichtverschwinden eines Anfangskoeffizienten gesorgt ist) zu mindestens einer Nullstelle $\{\xi_1', \ldots, \xi_n'\}$ der Polynome $f_1', \ldots, f_n'$, und so erhält man auch alle. Die fehlende Unbekannte ξ_1' kann jeweils aus einem System von Gleichungen bestimmt werden, deren größter gemeinsamer Teiler keine Konstante ist; d. h. man hat für ξ_1' jeweils eine algebraische Gleichung von mindestens dem ersten Grad. Wenn nun $d_1, \ldots, d_l$ noch nicht identisch verschwinden, so kann man in derselben Weise fortfahren mit Transformation (Einführung von $x_2'', \ldots, x_n''$ statt $x_2', \ldots, x_n'$) und Elimination, und so weiter. Das Verfahren bricht beim s-ten Schritt ab, wenn man nach Elimination von $x_1', x_2'', \ldots, x_s^{(s)}$ ein identisch verschwindendes Polynomsystem in $x_{s+1}^{(s)}, \ldots, x_n^{(s)}$ findet. Geschieht das nicht, so geht das Verfahren weiter bis zur Elimination aller Unbestimmten, und wenn die dann erhaltenen (konstanten) Resultanten immer noch nicht verschwinden, so ist das vorgelegte Gleichungssystem offenbar *unlösbar*. Im erstgenannten Fall aber, wo die Resultanten nach s Schritten Null werden, kann man für $x_{s+1}^{(s)}, \ldots, x_n^{(s)}$ beliebige Werte $\xi_{s+1}^{(s)}, \ldots, \xi_n^{(s)}$ einsetzen und daraus sukzessiv $\xi_1', \xi_2'', \ldots, \xi_s^{(s)}$ (in umgekehrter Reihenfolge) bestimmen. Zu jedem Wertsystem $\{\xi_{s+1}^{(s)}, \ldots, \xi_n^{(s)}\}$ findet man eine endliche Anzahl von Wertsystemen $\{\xi_1', \xi_2'', \ldots, \xi_s^{(s)}\}$, aus denen sich durch die Substitution (1) rückwärts Wertsysteme $\{\xi_1, \xi_2, \ldots, \xi_n\}$ ergeben, welche die ursprünglichen Gleichungen befriedigen.

Man kann für $\xi_{s+1}^{(s)}, \ldots, \xi_n^{(s)}$ auch Unbestimmte einsetzen und findet dann $\xi_1', \ldots, \xi_s^{(s)}$ in Gestalt eines oder mehrerer Systeme von algebraischen Funktionen dieser Unbestimmten; indessen ist zu beachten, daß es für spezielle $\xi_{s+1}^{(s)}, \ldots, \xi_n^{(s)}$ außerdem Lösungen geben kann, die in keiner Weise durch Spezialisierung aus der Lösung für unbestimmte $\xi_{s+1}^{(s)}, \ldots, \xi_n^{(s)}$ zu gewinnen sind, wie das folgende Beispiel zeigt.

Es sei

$$f_1 = x_1^2 + x_1 x_2,$$
$$f_2 = x_1 x_2 + x_2^2 + x_1 + x_2.$$

Die vorbereitende Transformation (1) ist, da in f_1 schon das Glied x_1^2 vorkommt, hier nicht nötig. Die Resultante nach x_1 muß identisch verschwinden; denn für jeden Wert von x_2 haben f_1 und f_2 den gemeinsamen Faktor $x_1 + x_2$. Für unbestimmte ξ_2 findet man dementsprechend $\xi_1 = -\xi_2$. Wählt man aber speziell $\xi_2 = -1$, so verschwindet f_2, und man findet für ξ_1 außer dem Wert $+1$ auch noch den Wert 0. Das Wertsystem $\{0, -1\}$ ist aber aus der allgemeinen Lösung $\xi_1 = -\xi_2$ durch keinerlei Spezialisierung zu erhalten.

Wie in diesem Beispiel, so zerfällt auch im allgemeinen Fall die „algebraische Mannigfaltigkeit" der gemeinsamen Nullstellen von $f_1, \ldots, f_r$ in verschiedene „unzerlegbare Mannigfaltigkeiten" verschiedener „Dimension", die je eine „Parameterdarstellung" durch algebraische Funktionen zulassen. Hinsichtlich des Beweises (unabhängig von der Eliminationstheorie) siehe Kap. 13. Die explizite Berechnung dieser Mannigfaltigkeiten und Parameterdarstellungen kann mit den Hilfsmitteln der Eliminationstheorie geschehen, worauf wir aber nicht näher eingehen[1].

Aus der Kongruenz (2) des vorigen Paragraphen folgt die im Polynombereich $\mathsf{K}(u)[x_1', \ldots, x_n']$ gültige Kongruenz

$$(d_1, \ldots, d_l) \equiv 0 \ (f_1', \ldots, f_r'). \tag{2}$$

Daraus erhält man ein interessantes Resultat für den Fall, daß die Elimination schließlich auf nichtverschwindende Konstanten als Resultanten führt, nämlich die Kongruenz

$$1 \equiv 0 \ (f_1, \ldots, f_r).$$

Ausführlich formuliert: *Wenn die Polynome* $f_1, \ldots, f_r$ *aus* $\mathsf{K}[x_1, \ldots, x_n]$ *in keinem algebraischen Körper über* K *eine gemeinsame Nullstelle haben, so gilt in* $\mathsf{K}[x_1, \ldots, x_n]$ *eine Relation*

$$1 = A_1 f_1 + \cdots + A_r f_r.$$

Beweis durch vollständige Induktion nach der Variablenzahl. Für konstante f_i oder auch für Polynome in einer Variablen ist alles klar. Die Behauptung werde für Polynome in $n-1$ Variablen als richtig angesehen. Bei n Variablen sind die zuerst auftretenden Resultanten $d_1, \ldots, d_l$ Polynome in $n-1$ Variablen, wieder ohne gemeinsame Nullstellen; also ist in $\mathsf{K}(u)[x_2', \ldots, x_n']$

$$1 = B_1 d_1 + \cdots + B_l d_l.$$

Nach (2) folgt daraus

$$1 = A_1' f_1' + \cdots + A_r' f_r'.$$

Hier setzen wir für die x_i' ihre Werte aus (1) ein; dann gehen die f_i' in die f_i über. Die Ausdrücke rechts sind rational in den u; multipliziert man mit dem Nenner $g(u)$ herauf, so kommt:

$$g(u) = A_1(u) \cdot f_1 + \cdots + A_r(u) \cdot f_r.$$

Vergleicht man die Koeffizienten irgend eines Potenzproduktes der u, dessen Koeffizient links nicht verschwindet, so folgt die Behauptung

$$1 = A_1 f_1 + \cdots + A_r f_r.$$

Aufgabe. Die Gradzahlen der Polynome $A_1, \ldots, A_r$ sind beschränkt, sobald die der f_i beschränkt sind.

---

[1] Vgl. etwa das Büchlein von F. S. Macaulay: Algebraic Theory of Modular Systems, Cambridge Tracts Nr. 19. Cambridge 1916.

§ 75. Der Hilbertsche Nullstellensatz.

Eine Verallgemeinerung des im vorigen Paragraphen zuletzt bewiesenen Satzes ist der *Hilbertsche Nullstellensatz*:

Ist f ein Polynom in $\mathsf{K}[x_1, \ldots, x_n]$, das in allen gemeinsamen Nullstellen der Polynome $f_1, \ldots, f_r$ verschwindet, so gilt eine Kongruenz

$$f^\varrho \equiv 0 \ (f_1, \ \ldots, f_r)$$

für eine natürliche Zahl ϱ (und umgekehrt).

Beweis[1]: Für $f = 0$ ist die Behauptung klar. Im Fall $f \neq 0$ nehmen wir eine neue Veränderliche z hinzu. Dann haben die Polynome

$$f_1, \ \ldots, f_r, \ 1 - zf$$

aus $\mathsf{K}[x_1, \ldots, x_n, z]$ keine gemeinsame Nullstelle; denn jede gemeinsame Nullstelle von $f_1, \ldots, f_r$ ist Nullstelle von f, also nicht von $1 - zf$. Daher ist nach dem Satz des vorigen Paragraphen

$$1 = A_1 f_1 + \cdots + A_r f_r + A\,(1 - zf).$$

In dieser Identität mache man die Substitution $z = \frac{1}{f}$ und schaffe die dadurch entstehenden Brüche durch Multiplikation mit einer Potenz f^ϱ fort. Dann kommt:

$$f^\varrho = B_1 f_1 + \cdots + B_r f_r, \qquad \text{q.e.d.}$$

Die Umkehrung ist klar.

Aus diesem Beweis und der Aufgabe von § 74 folgt, daß für den Exponenten ϱ eine Schranke angegeben werden kann, sobald die Gradzahlen von $f_1, \ldots, f_r$ und f gegeben sind. Tatsächlich aber gibt es eine Schranke für ϱ, die *nur* von $f_1, \ldots, f_r$ abhängt, wie wir im § 91 sehen werden.

Erweiterung des Nullstellensatzes. *Wenn die Polynome $h_1, \ldots, h_k$ in allen gemeinsamen Nullstellen von $f_1, \ldots, f_r$ den Wert Null annehmen, so gilt eine Kongruenz*

$$(h_1, \ \ldots, h_k)^\sigma \equiv 0 \ (f_1, \ \ldots, f_r),$$

oder: Jedes Potenzprodukt der h_i mit der Exponentensumme σ gehört dem Ideal $(f_1, \ldots, f_r)$ an (und umgekehrt).

Beweis: Es gilt

$$h_i^{\varrho_i} \equiv 0 \ (f_1, \ \ldots, f_r).$$

Man setze

$$\sigma = (\varrho_1 - 1) + (\varrho_2 - 1) + \cdots + (\varrho_k - 1) + 1.$$

Dann enthält jedes Potenzprodukt $h_1^{l_1} \ldots h_k^{l_k}$ mit $l_1 + \cdots + l_k = \sigma$ mindestens einen Faktor $h_i^{\varrho_i}$, da sonst $l_1 + \cdots + l_k$ höchstens gleich $(\varrho_1 - 1) + \cdots + (\varrho_k - 1) = \sigma - 1$ sein könnte. Daraus folgt die Behauptung.

Die Umkehrung ist klar.

---

[1] Vgl. A. Rabinowitsch: Math. Ann. Bd. 102, S. 518. 1929.

§ 76. Kriterium für die Lösbarkeit eines homogenen Gleichungssystems.

Wir haben in § 74 eine Methode kennengelernt, von jedem algebraischen Gleichungssystem zu entscheiden, ob es Lösungen besitzt oder nicht. Das ist aber etwas anderes als ein „*algebraisches Kriterium*" für Lösbarkeit, worunter wir ein System von ganzen rationalen Funktionen der Koeffizienten verstehen, deren Verschwinden notwendig und hinreichend für die Lösbarkeit ist (wie die Resultante von § 71 und das Resultantensystem von § 73 im Falle einer einzigen Unbekannten oder die Determinante eines linearen *homogenen* Gleichungssystems). Ein solches Kriterium gibt es im allgemeinen nicht[1], wohl aber im Spezialfall der homogenen Gleichungen, zu dem wir uns jetzt wenden.

Sind $f_1, \ldots, f_r$ homogene nichtkonstante Polynome in $x_1, \ldots, x_n$ $(n > 1)$, so haben sie zunächst immer die „triviale" Nullstelle $\{0, \ldots, 0\}$. Es soll sich nun darum handeln, ein Kriterium dafür zu finden, daß noch eine davon verschiedene, also nichttriviale Nullstelle $\{\eta_1, \ldots, \eta_n\}$, und damit notwendig wegen der Homogenität ein ganzer „*Strahl*" von Nullstellen $\{\lambda\eta_1, \ldots, \lambda\eta_n\}$ existiert[2].

Die folgende Herleitung stammt von H. KAPFERER[3]. Sie geht aus von der Kroneckerschen Methode der sukzessiven Elimination, indem sie aus den Formen $f_1, \ldots, f_r$, als Polynome in x_1 betrachtet, nach § 73 das Resultantensystem $D_1, \ldots, D_h$ bildet (aber ohne die vorbereitende Transformation (1) von § 74). Nun wird behauptet: Wenn $f_1, \ldots, f_r$ eine nichttriviale gemeinsame Nullstelle haben, so haben auch $D_1, \ldots, D_h$ als Polynome in $x_2, \ldots, x_n$ eine nichttriviale gemeinsame Nullstelle und umgekehrt.

Beim Beweis sind 2 Fälle zu unterscheiden.

1. Fall. Die Koeffizienten der reinen Potenzen von x_1 in $f_1, \ldots, f_r$ verschwinden nicht alle. In diesem Fall ergibt jede nichttriviale Null-

---

[1] Das sieht man wohl am bequemsten an folgendem Beispiel: Die Gleichungen

$$\left.\begin{aligned} a_1 x_1 + a_2 x_2 + a_3 &= 0, \\ b_1 x_1 + b_2 x_2 + b_3 &= 0 \end{aligned}\right\}$$

sind „im allgemeinen", d. h. für $a_1 b_2 - a_2 b_1 \neq 0$, lösbar. Wäre also

$$D_1(a, b) = 0, \ \ldots, \ D_h(a, b) = 0$$

notwendig und hinreichend für Lösbarkeit, so müßten die D für unbestimmte a, b verschwinden, also identisch verschwinden. Demnach wären die Gleichungen *stets* lösbar, was nicht zutrifft. (Auch die Ungleichung $a_1 b_2 - a_2 b_1 \neq 0$ ist nicht notwendig und hinreichend.)

[2] Die Nullstellen $\{\lambda\eta_1, \ldots, \lambda\eta_n\}$ bilden bei festem η und variablem λ eine Gerade des Raumes R_n, die vom Anfangspunkt $\{0, \ldots, 0\}$ ausgeht und deshalb „Strahl" genannt wird. Die Strahlen werden auch als „Punkte" des „projektiven Raumes" P_{n-1} aufgefaßt, deren „homogene Koordinaten" dann die η sind; vgl. § 87.

[3] KAPFERER, H.: Über Resultanten und Resultantensysteme. Sitzungsber. Bayer. Ak. München 1929, S. 179—200.

stelle $\{\xi_2, \ldots, \xi_n\}$ von $D_1, \ldots, D_h$ auf Grund der Bedeutung des Resultantensystems mindestens eine Nullstelle $\{\xi_1, \xi_2, \ldots, \xi_n\}$ von $f_1, \ldots, f_r$, die selbstverständlich nicht trivial sein kann, und umgekehrt ergibt jede solche Nullstelle $\{\xi_1, \ldots, \xi_n\}$ der f_ν eine Nullstelle $\{\xi_2, \ldots, \xi_n\}$ der D_ν, die auch nicht trivial sein kann, weil aus dem Verschwinden von $\xi_2, \ldots, \xi_n$ wegen $f_\lambda = c\,\xi_1^m + \cdots = 0$ sofort das Verschwinden von ξ_1 folgen würde.

2. Fall. Die Koeffizienten der reinen Potenzen von x_1 in $f_1, \ldots, f_r$ verschwinden alle. Nach § 73 verschwinden dann $D_1, \ldots, D_h$ identisch; also gibt es auch eine nichttriviale Nullstelle, etwa $\{1, 1, \ldots, 1\}$, von $D_1, \ldots, D_h$. Es gibt aber in diesem Fall für $f_1, \ldots, f_r$ sicher auch eine nichttriviale Nullstelle, nämlich $\{1, 0, \ldots, 0\}$, weil ja die Glieder mit der höchsten Potenz von x_1 überall fehlen.

Damit ist die obige Behauptung bewiesen. Da die $D_1, \ldots, D_h$ homogen in $x_2, \ldots, x_n$ sind, so kann man mit der Elimination fortfahren und x_2 eliminieren usw., bis man schließlich ein System von Formen in x_n allein übrig behält:

$$b_1 x_n^{s_1},\ b_2 x_n^{s_2},\ \ldots,\ b_k x_n^{s_k}.$$

Für die Existenz einer nichttrivialen Nullstelle dieser Formen ist notwendig und hinreichend das Verschwinden aller Koeffizienten $b_1, \ldots, b_k$.

Die Größen $b_1, \ldots, b_k$ sind durch feste, nur von den Gradzahlen der Urformen abhängige ganze rationale Prozesse aus deren Koeffizienten erhalten worden; sie sind also ganzzahlige Polynome der Koeffizienten von $f_1, \ldots, f_r$.

Das System der Polynome $b_1, \ldots, b_k$ (oder jedes andere System, dessen Verschwinden die Existenz einer Nullstelle anzeigt) heißt wieder ein *Resultantensystem* der Formen $f_1, \ldots, f_r$.

Wenn man die früher bewiesene Relation

$$(D_1, \ldots, D_h) \equiv 0\ (f_1, \ldots, f_r)$$

für jeden Schritt der sukzessiven Eliminationen anschreibt, so ergibt sich aus allen diesen Relationen zusammen:

$$x_n^{s_\nu} b_\nu \equiv 0\ (f_1, \ldots, f_r) \qquad (\nu = 1, \ldots, k). \tag{3}$$

Weiter folgt aus der Bildungsweise der $b_1, \ldots, b_k$ leicht, daß sie homogene Formen in den Koeffizienten jeder einzelnen Form f_i sind. Die $D_1, \ldots, D_h$ sind nämlich aus einer Resultante R entstanden, welche die Koeffizienten a_ν von f_i nur in den Kombinationen $a_\nu u_i$ und $a_\nu v_i$ enthielt. Also hat jedes Glied von R denselben Grad in den a_ν wie in u_i und v_i zusammen, und wenn dann R nach Potenzprodukten der u und v geordnet wird, so ist der Koeffizient D_j eines solchen Potenzproduktes homogen von einem bestimmten Grad in den a_ν. Wendet man dieselbe Betrachtungsweise auf den zweiten, dritten usw. Eliminationsschritt an, so ergibt sich die Behauptung.

Zusammenfassend haben wir:

r Formen $f_1, \ldots, f_r$ mit unbestimmten Koeffizienten besitzen ein Resultantensystem aus ganzzahligen Polynomen b_ν in diesen Koeffizienten, so daß für spezielle Werte der Koeffizienten in irgend einem Körper K *das Nullwerden aller Resultanten notwendig und hinreichend ist für die Existenz einer von der Nullösung verschiedenen Lösung der Gleichungen $f_1 = 0, \ldots, f_r = 0$. Die b_ν sind homogen in den Koeffizienten jeder einzelnen Form f_i und genügen einer Kongruenz* (3).

Aufgaben. 1. Wie kann das Resultantensystem für ein System von Linearformen lauten?

2. Sind $\varphi_1(t_1, t_2), \ldots, \varphi_n(t_1, t_2)$ n homogene Formen ohne gemeinsamen Faktor und betrachtet man die Gesamtheit aller Punkte ξ des projektiven Raumes, deren Koordinatenverhältnisse durch die Parametergleichung

$$(4) \qquad \xi_1 : \xi_2 : \ldots : \xi_n = \varphi_1(\tau_1, \tau_2) : \varphi_2(\tau_1, \tau_2) : \ldots : \varphi_n(\tau_1, \tau_2)$$

für nicht triviale τ-Werte geliefert werden, so läßt sich diese Gesamtheit, vermehrt um das Wertsystem $\{0, \ldots, 0\}$, auch durch homogene Gleichungen $F(\xi_1, \ldots, \xi_n) = 0$ charakterisieren. [Man drücke die Proportionen (4) zunächst durch homogene Gleichungen in den ξ und τ aus.]

3. Ist ein homogenes Gleichungssystem $f_1(x_1, \ldots, x_n) = 0, \ldots,$ in dem außer den x noch unbestimmte Parameter rational vorkommen, für unbestimmt gelassene Parameter lösbar, so bleibt es lösbar bei jeder Spezialisierung der Parameter.

4. Es gibt ein algebraisches Kriterium für die Lösbarkeit eines Systems von Gleichungen in mehreren Reihen von Unbekannten $x_1, \ldots, x_n$; $y_1, \ldots, y_m; \ldots,$ welche in jeder einzelnen dieser Reihen homogen sind.

Über die Bestimmung der Lösungen homogener Gleichungen siehe auch F. MERTENS: Sitzgsber. Wiener Akad. Wiss. Bd. 108 (1889), S. 1174, sowie § 79 dieses Buches.

§ 77. Über Trägheitsformen.

Während wir für eine beliebige Anzahl von homogenen Formen im vorigen Paragraphen ein Resultantensystem aus meist sehr vielen Formen kennengelernt haben, wird sich jetzt zeigen, daß man für n Formen in n Variablen mit einer einzigen Resultante auskommt, während für weniger als n Formen überhaupt keine Bedingung für Lösbarkeit notwendig ist. Um zu diesem Ergebnis zu gelangen, haben wir zunächst eine Reihe von Sätzen über die sogenannten „Trägheitsformen" zu beweisen.

Es seien

$$\begin{aligned} f_1 &= a_1 x_1^\alpha + a_2 x_1^{\alpha-1} x_2 + \cdots + a_\omega x_n^\alpha, \\ f_2 &= b_1 x_1^\beta + b_2 x_1^{\beta-1} x_2 + \cdots + b_\omega x_n^\beta, \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ f_r &= e_1 x_1^\varepsilon + e_2 x_1^{\varepsilon-1} x_2 + \cdots + e_\omega x_n^\varepsilon \end{aligned}$$

r Formen der Gradzahlen $l_1 = \alpha, l_2 = \beta, \ldots, l_r = \varepsilon$, in denen alle überhaupt möglichen Glieder von diesen Gradzahlen mit unbestimmten Koeffizienten vorkommen. Die letzten Koeffizienten (also die von $x_n^\alpha, x_n^\beta, \ldots, x_n^\varepsilon$) bezeichnen wir, wie angegeben, mit $a_\omega, b_\omega, \ldots, e_\omega$. Alle folgenden Betrachtungen beziehen sich auf ganzzahlige Polynome in den Unbestimmten $x_1, \ldots, x_n, a_1, \ldots, e_\omega$.

In § 76 begegneten uns schon Polynome T in den $a_1, \ldots, e_\omega$ allein mit der Eigenschaft

$$x_i^\tau T \equiv 0 \,(f_1, \ldots, f_r) \tag{1}$$

für ein i und ein τ. Solche Polynome T nennt man nach HURWITZ *Trägheitsformen*. Das ganze Resultantensystem von § 76 besteht aus Trägheitsformen.

Wir können die Trägheitsformen noch anders charakterisieren. Setzen wir nämlich

$$\begin{aligned} f_1 &= f_1^* + a_\omega x_n^\alpha, \\ &\cdots\cdots\cdots \\ f_r &= f_r^* + e_\omega x_n^\varepsilon, \end{aligned}$$

so können wir durch die Substitution

$$\left\{\begin{aligned} a_\omega &= -\frac{f_1^*}{x_n^\alpha}, \\ &\cdots\cdots\cdots \\ e_\omega &= -\frac{f_r^*}{x_n^\varepsilon} \end{aligned}\right. \tag{2}$$

in (1) erreichen, daß $f_1, \ldots, f_r$ verschwinden. In der Kongruenz (1) verschwindet dann die linke Seite; da aber x_i von der Substitution (2) unberührt bleibt, so muß T nach der Substitution verschwinden:

$$T\left(a_1, \ldots, -\frac{f_1^*}{x_n^\alpha}; \ldots; e_1, \ldots, -\frac{f_r^*}{x_n^\varepsilon}\right) = 0. \tag{3}$$

Der Schluß gilt schon, wenn die Kongruenz (1) nur für *ein* x_i vorausgesetzt wird.

Ist umgekehrt für irgend ein Polynom $T(a_1, \ldots, a_\omega, \ldots, e_1, \ldots, e_\omega)$ die Relation (3) erfüllt, so können wir T nach Potenzen von $a_\omega + \frac{f_1^*}{x_n^\alpha}, \ldots, e_\omega + \frac{f_r^*}{x_n^\varepsilon}$ ordnen und wissen dann aus (3), daß das von diesen Größen unabhängige Glied verschwindet; also folgt

$$T \equiv 0\left(a_\omega + \frac{f_1^*}{x_n^\alpha}, \ldots, e_\omega + \frac{f_r^*}{x_n^\varepsilon}\right)$$

im Bereich der Brüche mit Nennern x_n^λ. Multipliziert man mit dem höchsten vorkommenden Nenner auf, so wird alles ganz, und man erhält

$$x_n^\tau T \equiv 0 \,(f_1, \ldots, f_r).$$

Also: Wenn (1) mit irgend einem x_i gilt, so gilt (3), und wenn (3) gilt, so gilt (1) mit x_n statt x_i. Daraus schließt man zunächst, daß aus der

Gültigkeit von (1) mit irgend einem x_i die Gültigkeit von (1) mit x_n folgt, mithin, da der Index n keine Sonderrolle spielen kann, daß aus der Gültigkeit von (1) mit irgend einem x_i die von (1) mit jedem anderen x_j folgt, und weiter, daß (1) mit (3) gleichbedeutend ist: *Die Gleichung* (3) *ist für die Trägheitsformen ebenso charakteristisch wie* (1).

Die Summe oder die Differenz von zwei Trägheitsformen ist offenbar wieder eine Trägheitsform, und ein Vielfaches einer Trägheitsform auch. Daher bilden die Trägheitsformen T ein *Ideal* $\mathfrak{T}$.

Das Ideal $\mathfrak{T}$ ist ein Primideal. Hat nämlich ein Produkt $T_1 T_2$ die Eigenschaft (3), so muß einer der Faktoren sie haben.

Die Trägheitsformen können die Rolle des Resultantensystems von § 76 vollständig übernehmen. Haben nämlich die Formen $f_1, \ldots, f_r$ eine (nichttriviale) gemeinsame Nullstelle und setzt man diese in (1) ein, so verschwindet die rechte Seite, und da nicht alle x_i Null werden, folgt $T = 0$ für jede Trägheitsform. Verschwinden umgekehrt für ein spezielles System $f_1, \ldots, f_r$ *alle* Trägheitsformen, so verschwindet insbesondere das Resultantensystem; mithin gibt es eine gemeinsame Nullstelle. Daraus folgt: Wenn man irgend eine Basis des Ideals $\mathfrak{T}$ der Trägheitsformen gefunden hat, so kann man diese Basis auch als Resultantensystem verwenden. Das werden wir im nächsten Paragraphen benutzen.

Wir wollen nun beweisen:

Ist die Anzahl r der Formen f_i kleiner als die Variablenzahl n, so gibt es keine von Null verschiedene Trägheitsform. Ist $r = n$, so gibt es keine von e_ω unabhängige und von Null verschiedene Trägheitsform.

Aus der ersten Hälfte dieses Satzes folgt schon, daß das Resultantensystem von weniger als n Formen identisch verschwindet, daß also in diesem Falle immer eine gemeinsame Nullstelle existiert.

Beweis: Es sei erstens $r < n$. Wäre T eine von Null verschiedene Trägheitsform, so würde aus (3) folgen, daß die Größen

$$-\frac{f_1^*}{x_n^\alpha}, \ldots, -\frac{f_r^*}{x_n^\varepsilon}$$

algebraisch-abhängig in bezug auf den Polynombereich der Größen $a_1, \ldots, a_{\omega-1}, \ldots, e_1, \ldots, e_{\omega-1}$ wären. Man kann hier $x_n = 1$ setzen, ohne daß diese Tatsache ihre Gültigkeit verliert.

Ebenso würde im Falle $r = n$, wenn die Behauptung falsch wäre, folgen, daß die Größen

$$-\frac{f_1^*}{x_n^\alpha}, \ldots, -\frac{f_{n-1}^*}{x_n^\delta}$$

(wo δ den Grad der Form f_{n-1} bedeutet) algebraisch-abhängig wären (f_n^* kommt nicht vor, da T von e_ω unabhängig sein sollte). Man kann auch jetzt $x_n = 1$ setzen.

Auf jeden Fall würde also eine Reihe von Polynomen

$$[-f_1^*]_{x_n=1}, \ldots, [-f_s^*]_{x_n=1} \qquad (s < n)$$

algebraisch-abhängig in bezug auf den Polynombereich der $a_1, \ldots, a_{\omega-1}, \ldots, e_1, \ldots, e_{\omega-1}$ sein. Nun gilt der folgende

Hilfssatz. *Wenn eine Reihe von Polynomen $f_1, \ldots, f_s$ in den Unbestimmten $a_1, \ldots, a_p, x_1, \ldots, x_q$ algebraisch-abhängig ist in bezug auf den Polynombereich $\mathsf{K}[a_1, \ldots, a_p]$, wo K ein Integritätsbereich, so bleibt diese Abhängigkeit auch bei jeder Spezialisierung $a_p = \alpha (\alpha \in \mathsf{K})$ bestehen.*

Beweis des Hilfssatzes. Nach Voraussetzung besteht eine Relation

$$F(a_1, \ldots, a_p, f_1, \ldots, f_s) = 0, \tag{4}$$

wobei F ein Polynom ist und für unbestimmte $z_1, \ldots, z_s$

$$F(a_1, \ldots, a_p, z_1, \ldots, z_s) \neq 0 \tag{5}$$

ist.

Wir können annehmen, daß das Polynom $F(a, z)$ nicht den Faktor $a_p - \alpha$ enthält; denn sonst könnte man in (4) und (5) durch diesen Faktor kürzen. Unter dieser Annahme verschwindet F auch nicht bei der Substitution $a_p = \alpha$:

$$F(a_1, \ldots, a_{p-1}, \alpha, z_1, \ldots, z_s) \neq 0.$$

Aber die Gültigkeit von (4) bleibt bei der Substitution $a_p = \alpha$ bestehen. Damit ist die Behauptung bewiesen.

Wendet man den Hilfssatz mehrere Male an, so folgt, daß man von den Unbestimmten $a_1, \ldots, a_{\omega-1}, \ldots, e_1, \ldots, e_{\omega-1}$ mehrere oder alle spezialisieren darf, ohne daß die algebraische Abhängigkeit verlorengeht.

Der unterbrochene Beweis ist nun leicht zu Ende zu führen. Man spezialisiere die Größen $a_1, \ldots, a_{\omega-1}, \ldots, e_{\omega-1}$ so, daß die Formen $f_1^*, \ldots, f_s^*$ in $x_1^\alpha, \ldots, x_s^\delta$ übergehen. Wegen $s < n$ sind diese Ausdrücke von der vorhergehenden Substitution $x_n = 1$ unberührt geblieben. Da bei der Spezialisierung jede algebraische Abhängigkeit bestehen bleibt, so müssen die Ausdrücke $x_1^\alpha, \ldots, x_s^\delta$ algebraisch-abhängig sein. Da sie es offenbar nicht sind, so war unsere Annahme falsch, und der Satz ist bewiesen.

Was nach dem eben bewiesenen Satz für $r < n$ gilt, gilt aber nicht mehr für $r = n$. Im Gegenteil:

Für $r = n$ gibt es eine nichtverschwindende Trägheitsform D_e. Sie ist homogen in den $a_1, \ldots, a_\omega$, in den $b_1, \ldots, b_\omega$ usw., und vom Grade $L_n = l_1 l_2 \ldots l_{n-1}$ in den $e_1, \ldots, e_\omega$.

Beweis. Wir setzen

$$\sum_1^n (l_i - 1) = l - 1.$$

Die Gesamtheit aller Potenzprodukte der x_i vom Grade l läßt sich folgendermaßen anordnen:

Zuerst alle Potenzprodukte, die $x_1^{l_1}$ enthalten;
sodann alle, die $x_2^{l_2}$, aber nicht $x_1^{l_1}$ enthalten, usw.;
schließlich alle, die $x_n^{l_n}$, aber nicht $x_1^{l_1}$, nicht $x_2^{l_2}$ usw. enthalten.

Dieses Verfahren liefert alle Potenzprodukte vom Grade l; denn fehlen könnten doch nur die, welche x_1 höchstens in der $(l_1 - 1)$-ten usw., schließlich x_n höchstens in der $(l_n - 1)$-ten Potenz enthalten, und diese Potenzprodukte haben höchstens den Grad $\Sigma(l_i - 1)$, also nicht den Grad l. Nun bezeichnen wir die erhaltenen Potenzprodukte mit

$$H^{(\nu)}_{l-l_1} x_1^{l_1},\ H^{(\nu)}_{l-l_2} x_2^{l_2},\ \ldots,\ H^{(\nu)}_{l-l_n} x_n^{l_n}; \tag{6}$$

dabei bedeuten also die $H^{(\nu)}_{l-l_i}$ Potenzprodukte vom Grade $l - l_i$. Insbesondere kommen in der letzten Kategorie H_{l-l_n} nur Potenzprodukte von einem Grade $< l_1$ in x_1, $\ldots$, $< l_{n-1}$ in x_{n-1} vor, während der Grad in x_n jeweils durch die Bedingung festgelegt ist, daß der Gesamtgrad $l - l_n$ sein soll. Die letzte Kategorie umfaßt also genau $l_1 l_2 \ldots l_{n-1}$ Potenzprodukte.

Wir bilden nun alle Formen

$$H^{(\nu)}_{l-l_i} f_i, \tag{7}$$

deren es offensichtlich genau so viele gibt wie Potenzprodukte (6) vom Grade l. Die Koeffizientenmatrix der Formen (7) ist also eine quadratische; ihre Determinante D_e erhält bei der Spezialisierung $f_i = x_i^{l_i}$ den Wert 1, kann also nicht identisch verschwinden. Weiter ist D_e eine Trägheitsform, denn wenn man die Gleichungen

$$H^{(\nu)}_{l-l_i} f_i = \sum a_{\nu\mu} H^{(\mu)}_l$$

mit den Unterdeterminanten einer Spalte von D_e multipliziert und addiert, kommt links eine Linearkombination der f_i und rechts $D_e \cdot H^{(\mu)}_l$. Wählt man speziell $H^{(\mu)}_l = x_i^l$, so folgt

$$D_e x_i^l \equiv 0\,(f_1,\ \ldots,\ f_r).$$

Schließlich ist D_e homogen in den Koeffizienten jeder einzelnen Form f_i, und zwar hat sie in den Koeffizienten von f_n den Grad $L_n = l_1 l_2 \ldots l_{n-1}$. Damit ist die Behauptung bewiesen.

Für weitere Eigenschaften der Trägheitsformen siehe A. Hurwitz: Über die Trägheitsformen eines algebraischen Moduls, Annali di Matematica (3a) 20 (1913).

§ 78. Die Resultante von n Formen in n Variablen.

Wir gehen nun aus von n allgemeinen Formen (d. h. Formen mit unbestimmten Koeffizienten) $f_1, \ldots, f_n$ in $x_1, \ldots, x_n$, bilden das Ideal $\mathfrak{T}$ der Trägheitsformen und suchen in $\mathfrak{T}$ ein Polynom von möglichst niedrigem Grad in e_ω. Ein solches gibt es, und sein Grad in e_ω ist nicht Null, da es keine von e_ω unabhängige Trägheitsform außer der Null gibt. Zerlegen wir es in unzerlegbare Faktoren, so muß mindestens ein Faktor schon zu $\mathfrak{T}$ gehören, da $\mathfrak{T}$ Primideal ist. Dieser Faktor hat immer noch denselben Grad in e_ω, da ein niedrigerer Grad innerhalb $\mathfrak{T}$ ja gar nicht möglich ist. Wir nennen diesen Faktor R und beweisen den Satz:

Jedes Polynom aus dem Ideal $\mathfrak{T}$ ist durch R teilbar.

Beweis: Wir ordnen R nach absteigenden Potenzen von e_ω:

$$R = S e_\omega^\lambda + \cdots \qquad (\lambda > 0\,,\ S \neq 0)\,.$$

Nun sei T ein Polynom aus $\mathfrak{T}$. Da der Grad von T in e_ω mindestens gleich λ ist, so können wir T mit S multiplizieren und dann durch Subtraktion eines Vielfachen von R den Grad in e_ω erniedrigen. Indem wir diesen Prozeß fortsetzen, bis dieser Grad kleiner als λ geworden ist, kommen wir auf eine Gleichung von der Gestalt

$$S^j T - Q R = T'\,.$$

T' gehört wieder zu $\mathfrak{T}$ und hat in e_ω einen Grad $< \lambda$, muß also verschwinden. Also ist $S^j T$ durch R teilbar. R ist aber unzerlegbar und S nicht durch R teilbar (schon weil S von e_ω unabhängig ist); daher ist T durch R teilbar, q. e. d.

$\mathfrak{T}$ ist also Hauptideal mit der Basis R. Dadurch ist R bis auf einen konstanten Faktor eindeutig festgelegt. Wir nennen R die *Resultante* der Formen $f_1, \ldots, f_n$. Die Berechtigung dieser Bezeichnung ergibt sich sofort. Wenn nämlich R für spezielle Werte der Koeffizienten der Formen $f_1, \ldots, f_n$ verschwindet, so verschwinden alle Formen des Ideals $\mathfrak{T}$, insbesondere also alle Formen des Resultantensystems von $f_1, \ldots, f_n$; also haben $f_1, \ldots, f_n$ eine nichttriviale gemeinsame Nullstelle. Und wenn umgekehrt $f_1, \ldots, f_n$ eine nichttriviale gemeinsame Nullstelle haben, so verschwindet, wenn man diese Nullstelle in die Identität

$$x_i^\tau R = A_1 f_1 + \cdots + A_n f_n$$

einsetzt, die rechte Seite, also auch die linke; mindestens ein x_i verschwindet aber nicht, also verschwindet R. Nach dem im vorigen Paragraphen Bemerkten können wir R also wirklich als *Resultante* der Formen $f_1, \ldots, f_n$ bezeichnen: $R = 0$ *ist notwendig und hinreichend für die Existenz einer nichttrivialen Lösung.*

Jetzt sollen noch einige formale Sätze über die Resultante bewiesen werden, die uns insbesondere die Gradbestimmung erlauben werden.

Spezialisiert man f_1 zu $g \cdot h$, wo g und h allgemeine Formen von den Gradzahlen μ, ν sind ($\mu + \nu = l_1$), so wird R teilbar durch das Produkt

$$R_g \cdot R_h = R(g, f_2, \ldots, f_n) \cdot R(h, f_2, \ldots, f_n)\,.$$

Beweis: Aus

$$x_n^j R = A_1 f_1 + \cdots + A_n f_n$$

folgt durch Spezialisierung:

$$x_n^j \cdot R(g h, f_2, \ldots, f_n) = A_1 g h + A_2 f_2 + \cdots + A_n f_n\,;$$

also gehört $R(gh, f_2, \ldots, f_n)$ sowohl dem aus den Formen $g, f_2, \ldots, f_n$ gebildeten Ideal $\mathfrak{T}_g$ als auch dem entsprechend gebildeten Ideal $\mathfrak{T}_h$ an. $R(gh, f_2, \ldots, f_n)$ ist also sowohl durch R_g als durch R_h teilbar, also (da diese beiden unzerlegbar und verschieden sind) durch $R_g \cdot R_h$, q. e. d.

Spezialisiert man nun $f_1, \ldots, f_{n-1}$ zu Produkten von Linearformen, so erkennt man durch sukzessive Anwendung des vorigen Satzes, daß R durch ein Produkt von $L_n = l_1 l_2 \ldots l_{n-1}$ Teilresultanten teilbar ist, deren jede nach einem früheren Satze die e_i wirklich enthält; also hat das Produkt mindestens den Grad L_n in den e_i. Da wir andererseits sahen, daß R in den e_i auch höchstens den Grad L_n hat, so folgt, daß der Grad genau L_n ist.

Genau entsprechend wie D_e (§ 77) können wir auch D_a, D_b, ... bilden, indem wir die Formen $f_1, \ldots, f_n$ so anordnen, daß f_1 bzw. f_2 usf. jeweils zuletzt kommt. Dann hat D_a den Grad $L_1 = l_2 l_3 \ldots l_n$ in den a_i, D_b den Grad $L_2 = l_1 l_3 \ldots l_n$ in den b_i, usw.; alle $D_a, D_b, \ldots, D_e$ sind durch R teilbar, und R hat in den a_i den Grad L_1, in den b_i den Grad L_2, usw. Die Definition von R als Basiselement des Ideals $\mathfrak{T}$ hängt ja nicht von der Reihenfolge der Formen $f_1, \ldots, f_n$ ab. Zugleich sieht man, daß R die höchsten Gradzahlen hat, die ein gemeinsamer Teiler von $D_a, D_b, \ldots, D_e$ überhaupt haben kann; mithin:

R ist der größte gemeinsame Teiler der Polynome $D_a, D_b, \ldots, D_e$.

D_e erhält bei der Spezialisierung $f_i = x_i^{l_i}$ $(i = 1, \ldots, n)$ den Wert 1, und R ist Teiler von D_e; also erhält R bei dieser Spezialisierung den Wert ± 1, d. h. R enthält ein Glied

$$\pm a_1^{L_1} \ldots e_\omega^{L_n}.$$

Wir normieren R so, daß dieses „Hauptglied" mit dem Pluszeichen vorkommt.

Die frühere Aussage: R ist teilbar durch $R_g R_h$ für $f_1 = g \cdot h$, läßt sich also jetzt durch Vergleichung der Gradzahlen und Hauptglieder verschärfen zu:

$$R_{gh} = R_g R_h.$$

Wir fassen zusammen:

n allgemeine Formen in n Variablen haben eine Resultante R, die ein unzerlegbares ganzzahliges Polynom in ihren (unbestimmten) Koeffizienten ist und als Basis des Ideals der Trägheitsformen definiert werden kann. Das Verschwinden der Resultante für spezielle $f_1, \ldots, f_n$ mit Koeffizienten aus einem Körper ist notwendig und hinreichend für die Existenz einer von der Nullösung verschiedenen Lösung des Gleichungssystems $f_1 = 0, \ldots, f_n = 0$. Die Resultante ist homogen in den Koeffizienten von f_1 vom Grade $L_1 = l_2 \ldots l_n$, usw. Sie enthält ein Hauptglied $a_1^{L_1} \ldots e_\omega^{L_n}$ und nimmt somit bei der Spezialisierung $f_i = x_i^{l_i}$ den Wert 1 an. Bei der Spezialisierung $f_1 = g \cdot h$ geht R in das Produkt $R_g \cdot R_h$ über. Schließlich ist R der größte gemeinsame Teiler von n explizit bekannten Determinanten $D_a, D_b, \ldots, D_e$.

Aufgaben. 1. Für zwei Formen in zwei Variablen stimmt die Resultante mit der Sylvesterschen Resultante (§ 71) überein.

2. Für eine Form f vom Grade l und $n - 1$ Linearformen

$$\sum b_i x_i, \ \ldots, \ \sum e_i x_i$$

hat die Resultante den Wert

$$f(X_1, \ldots, X_n),$$

wo $X_1, \ldots, X_n$ die $(n-1)$-reihigen Unterdeterminanten der Matrix

$$\begin{pmatrix} b_1 \ldots b_n \\ \cdots\cdots \\ e_1 \ldots e_n \end{pmatrix}$$

sind.

3. Die Resultante ist absolut-unzerlegbar.

4. Führt man in den Formen $f_1, \ldots, f_n$ neue Veränderliche ein durch eine lineare Substitution mit nichtverschwindender Determinante:

$$x_i = \sum a_{ik} x'_k,$$

so ist die Resultante der transformierten Formen in $x'_1, \ldots, x'_n$ bis auf einen von den a_{ik} abhängigen Faktor gleich der Resultante von $f_1, \ldots, f_n$.

Weitere Eigenschaften der Resultante findet man in dem schon früher (§ 72 und § 74) zitierten Büchlein von F. S. MACAULAY: Modular Systems, sowie bei E. FISCHER: Über die Cayleysche Eliminationsmethode, Math. Zeitschr. Bd. 26, S. 497—550. 1927.

§ 79. Die u-Resultante und der Satz von BÉZOUT.

Unter einem *Lösungsstrahl* (vgl. § 76) eines homogenen Gleichungssystems möge verstanden werden die Gesamtheit aller Lösungen $\{\lambda\xi_1, \ldots, \lambda\xi_n\}$, die zu einer festen nichttrivialen Lösung $\{\xi_1, \ldots, \xi_n\}$ proportional sind. Wir nehmen nun an, das Gleichungssystem

$$f_1 = 0, \ldots, f_r = 0 \tag{1}$$

habe nur endlich viele Lösungsstrahlen $\{\xi_1^{(\alpha)}, \ldots, \xi_n^{(\alpha)}\}$ $(\alpha = 1, \ldots, q)$, und suchen diese Strahlen zu bestimmen.

Zu den Polynomen $f_1, \ldots, f_r$ nehmen wir eine Linearform mit unbestimmten Koeffizienten

$$l = u_1 x_1 + \cdots + u_n x_n$$

hinzu und bilden das Resultantensystem $b_1(u), \ldots, b_t(u)$ der Formen $f_1, \ldots, f_r, l$. Dieses Resultantensystem verschwindet für spezielle $u_1, \ldots, u_n$ dann und nur dann, wenn eine Lösung $\{\xi^{(\alpha)}\}$ von (1) zugleich der Bedingung

$$l_\alpha = u_1 \xi_1^{(\alpha)} + \cdots + u_n \xi_n^{(\alpha)} = 0$$

genügt. Mit anderen Worten: die gemeinsamen Nullstellen der Formen $b_1(u), \ldots, b_t(u)$ (als Formen in den u) sind genau die Nullstellen des Produkts $\prod_\alpha l_\alpha$.

Daraus folgt nach dem Hilbertschen Nullstellensatz (§ 75) einerseits

$$(b_i(u))^{\tau_i} \equiv 0 \quad \left(\prod_\alpha l_\alpha\right) \qquad (i = 1, \ldots, t), \tag{2}$$

andererseits

$$(3) \qquad (\prod_{\alpha} l_\alpha)^r \equiv 0 \quad (b_1(u), \ldots, b_t(u)).$$

Die l_α sind Linearformen in den u, also unzerlegbar. Nach (2) sind die $b_i(u)$, also auch ihr größter gemeinsamer Teiler $D(u)$, teilbar durch alle Linearfaktoren l_α. Aus (3) folgt aber

$$(\prod_{\alpha} l_\alpha)^r \equiv 0 \quad (D(u));$$

also kann $D(u)$ auch keine anderen Linearfaktoren als diese l_α enthalten. Daher muß sein

$$(4) \qquad D(u) = \prod l_\alpha^{\varrho_\alpha}, \qquad \varrho_\alpha > 0;$$

in Worten: *Die Linearformen l_α, welche die Lösungsstrahlen von* (1) *bestimmen, werden durch Faktorzerlegung der Form $D(u)$ gefunden.* Die Form $D(u)$, der größte gemeinsame Teiler des Resultantensystems von $f_1, \ldots, f_r$ und l, heißt die *u-Resultante* von $f_1, \ldots, f_r$.

Wir betrachten nun insbesondere den Fall von $n-1$ homogenen Gleichungen in n Veränderlichen, welche endlichviele Lösungstrahlen besitzen. Nimmt man die Linearform l hinzu, so erhält man n Formen, welche eine einzige Resultante $R(u)$ haben; diese ist natürlich zugleich die u-Resultante und zerfällt gemäß (4). Die Lösungen erscheinen mit gewissen *Vielfachheiten* ϱ_α behaftet. Die Summe der ϱ_α ist der Grad von $R(u)$, also das Produkt der Gradzahlen der Formen $f_1, \ldots, f_{n-1}$ (vgl. § 78). Damit ist der *Satz von* BÉZOUT bewiesen:

Wenn $n-1$ homogene Gleichungen in n Veränderlichen nur endlich viele Lösungsstrahlen haben, so ist die Summe der durch (4) *definierten Vielfachheiten dieser Lösungsstrahlen gleich dem Produkt der Gradzahlen der Gleichungen.*

Für $n = 3$ und $n = 4$ stecken darin die geometrischen Sätze: Die Summe der Vielfachheiten der Schnittpunkte zweier algebraischen Kurven in der projektiven Ebene bzw. dreier algebraischen Flächen im projektiven Raum ist gleich dem Produkt der Gradzahlen dieser Kurven bzw. Flächen. Die Vielfachheiten sind positive ganze Zahlen, die durch die Exponenten der Linearfaktoren von $R(u)$ definiert werden.

Aufgabe: Wie lautet das erste Ergebnis dieses Paragraphen für homogene Gleichungen in zwei Variablenreihen $(x_1, \ldots, x_n)$, $(y_1, \ldots, y_m)$, wenn man die Linearform l durch $\sum\sum u_{ik} x_i y_k$ ersetzt?

Siehe weiter: B. L. v. D. WAERDEN: Der Multiplizitätsbegriff der algebraischen Geometrie, Math. Ann. Bd. 97, S. 756. 1927. KAPFERER, H.: Axiomatische Begründung des Bézoutschen Satzes. Sitzungsber. Heidelberger Akademie 1927, 8. Abhandlung, S. 33—59.

Zwölftes Kapitel.

Allgemeine Idealtheorie der kommutativen Ringe.

§ 80. Basissatz und Teilerkettensatz.

Wir wollen in diesem Kapitel die Teilbarkeitseigenschaften der Ideale kommutativer Ringe untersuchen und zusehen, inwieweit die einfachen Gesetze, die etwa im Bereich der ganzen Zahlen gelten, sich auf allgemeinere Ringe übertragen lassen. Um dabei nicht auf zu komplizierte Verhältnisse zu stoßen, ist es zweckmäßig, daß man sich auf solche Ringe beschränkt, in denen jedes Ideal eine endliche Basis besitzt, was tatsächlich, wie wir sehen werden, in sehr vielen wichtigen Fällen zutrifft.

Wir sagen, daß in einem Ring $\mathfrak{o}$ *der Basissatz gilt,* wenn jedes Ideal in $\mathfrak{o}$ eine endliche Basis hat.

Der Basissatz gilt für jeden Körper, weil da nur die Ideale (0) und (1) existieren. Auch gilt er für den Ring der ganzen Zahlen, allgemeiner für jeden Hauptidealring. Sodann gilt er für jeden endlichen Ring. Wie wir später sehen werden, gilt er für jeden Restklassenring $\mathfrak{o}/\mathfrak{a}$, falls er für $\mathfrak{o}$ gilt. Schließlich besteht aber der im wesentlichen auf HILBERT zurückgehende Satz:

Wenn der Basissatz für den Ring $\mathfrak{o}$ *gilt und in* $\mathfrak{o}$ *ein Einselement existiert, so gilt er auch für den Polynombereich* $\mathfrak{o}[x]$.

Beweis: Es sei $\mathfrak{A}$ ein Ideal in $\mathfrak{o}[x]$. Die Koeffizienten der höchsten Potenzen von x in den Polynomen von $\mathfrak{A}$ bilden, zusammen mit der Null, ein Ideal in $\mathfrak{o}$; denn wenn α und β die höchsten Koeffizienten der Polynome a, b sind:

$$a = \alpha x^n + \cdots,$$
$$b = \beta x^m + \cdots,$$

so ist, wenn etwa $n \geqq m$ vorausgesetzt wird,

$$a - b x^{n-m} = (\alpha x^n + \cdots) - (\beta x^n + \cdots)$$
$$= (\alpha - \beta) x^n + \cdots$$

wieder ein Polynom von $\mathfrak{A}$ und $\alpha - \beta$ sein höchster Koeffizient oder Null; ebenso ist, wenn α der höchste Koeffizient von a ist, $\lambda\alpha$ der höchste Koeffizient von λa oder Null.

Dieses Ideal $\mathfrak{a}$ der höchsten Koeffizienten hat nach Voraussetzung eine Basis $(\alpha_1, \ldots, \alpha_r)$; α_i sei etwa der höchste Koeffizient des Polynoms

$$a_i = \alpha_i x^{n_i} + \cdots$$

vom Grad n_i, und es sei n die größte der endlich vielen Zahlen n_i.

Die Polynome a_i nehmen wir in die zu bildende Basis für $\mathfrak{A}$ auf. Wir werden zusehen, welche weiteren Polynome für eine Basis nötig sind.

Ist

$$f = \alpha x^N + \cdots$$

ein Polynom aus $\mathfrak{A}$ von einem Grad $N \geqq n$, so muß α dem Ideal $\mathfrak{a}$ angehören:

$$\alpha = \sum \lambda_i \alpha_i .$$

Man bilde nun das Polynom

$$f_1 = f - \sum (\lambda_i x^{N-n_i}) a_i .$$

Der Koeffizient von x^N in diesem Polynom ist

$$\alpha - \sum \lambda_i \alpha_i = 0;$$

f_1 hat also einen Grad $< N$. Wir können also das Polynom f modulo $(a_1, \ldots, a_r)$ ersetzen durch ein Polynom niedrigeren Grades. In derselben Weise können wir weitergehen, bis der Grad kleiner als n geworden ist. Es genügt also, sich weiterhin auf Polynome von beschränkten Gradzahlen ($< n$) zu beschränken.

Die Koeffizienten von x^{n-1} in den Polynomen vom Grade $\leqq n-1$ aus $\mathfrak{A}$ bilden, eventuell zusammen mit der Null, ein Ideal $\mathfrak{a}_{n-1}$; eine Basis dieses Ideals sei

$$(\alpha_{r+1}, \ldots, \alpha_s) .$$

α_{r+i} sei wiederum der höchste Koeffizient des Polynoms

$$a_{r+i} = \alpha_{r+i} x^{n-1} + \cdots .$$

Wir nehmen nun auch noch die Polynome $a_{r+1}, \ldots, a_s$ in die Basis auf. Jedes Polynom vom Grade $\leqq n-1$ kann nun modulo $(a_{r+1}, \ldots, a_s)$ ersetzt werden durch ein Polynom vom Grade $\leqq n-2$; man hat nur wie vorhin eine passend gewählte Linearkombination

$$\sum \lambda_{r+i} a_{r+i}$$

zu subtrahieren.

So fahren wir fort. Die Koeffizienten von x^{n-2} in den Polynomen vom Grad $\leqq n-2$ bilden mit der Null ein Ideal $\mathfrak{a}_{n-2}$, dessen Basiselemente $\alpha_{s+1}, \ldots, \alpha_t$ den Polynomen $a_{s+1}, \ldots, a_t$ angehören. Diese Polynome nehmen wir wiederum in die Basis auf. So gelangen wir schließlich zum Ideal $\mathfrak{a}_0$ der in $\mathfrak{A}$ liegenden Konstanten; seine Basis $(\alpha_{v+1}, \ldots, \alpha_w)$ führt zu den Polynomen $a_{v+1}, \ldots, a_w$. Jedes Polynom aus $\mathfrak{A}$ muß sich modulo

$$(a_1, \ldots, a_r, a_{r+1}, \ldots, a_s, \ldots, a_{v+1}, \ldots, a_w)$$

schließlich auf Null reduzieren. Also bilden die Polynome $a_1, \ldots, a_w$ eine Basis für das Ideal $\mathfrak{A}$, womit der Basissatz bewiesen ist.

Aus diesem Satz folgt durch n-malige Anwendung unmittelbar die Verallgemeinerung:

Wenn für einen Ring $\mathfrak{o}$ *mit Einselement der Basissatz gilt, so gilt er auch für den Polynombereich* $\mathfrak{o}[x_1, \ldots, x_n]$ *der endlichvielen Unbestimmten* $x_1, \ldots, x_n$.

Die wichtigsten Spezialfälle sind: der ganzzahlige Polynombereich $C[x_1, \ldots, x_n]$ und jeder Polynombereich $\mathsf{K}[x_1, \ldots, x_n]$ mit Koeffizienten aus einem Körper K. In allen diesen Bereichen hat jedes Ideal eine endliche Basis.

HILBERT hat seinen Satz nur für diese Fälle ausgesprochen, in einer scheinbar etwas allgemeineren Fassung, nämlich der folgenden:

In jeder Untermenge $\mathfrak{M}$ *von* $\mathfrak{o}$ *(nicht nur in jedem Ideal) gibt es endlich viele Elemente* $m_1, \ldots, m_r$ *so, daß jedes Element* m *von* $\mathfrak{M}$ *sich in der Gestalt*

$$\lambda_1 m_1 + \cdots + \lambda_r m_r \qquad (\lambda_i \text{ in } \mathfrak{o})$$

schreiben läßt.

Dieser Satz ist aber eine unmittelbare Folge des Basissatzes für Ideale. Denn wenn $\mathfrak{A}$ das von $\mathfrak{M}$ erzeugte Ideal ist, so hat zunächst $\mathfrak{A}$ eine Basis:

$$\mathfrak{A} = (a_1, \ldots, a_s).$$

Jedes Element a_i hängt (als Element des von $\mathfrak{M}$ erzeugten Ideals) von endlich vielen Größen von $\mathfrak{M}$ ab:

$$a_i = \sum_k \lambda_{ik} m_{ik}.$$

Also hängen alle Elemente von $\mathfrak{A}$ von den endlichvielen m_{ik} linear ab; das gilt nun insbesondere für die Elemente von $\mathfrak{M}$.

Wichtiger ist, daß der Basissatz auch mit dem folgenden „Teilerkettensatz“[1] äquivalent ist:

Teilerkettensatz, 1. Fassung.

Ist eine Kette von Idealen $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3, \ldots$ *in* $\mathfrak{o}$ *gegeben und ist jedes* $\mathfrak{a}_{i+1}$ *ein echter Teiler von* $\mathfrak{a}_i$:

$$\mathfrak{a}_i \subset \mathfrak{a}_{i+1},$$

so bricht die Kette nach endlichvielen Gliedern ab.

Oder, was auf dasselbe hinauskommt:

Teilerkettensatz, 2. Fassung.

Ist eine unendliche Kette von Teilern $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3, \ldots$ *gegeben*:

$$\mathfrak{a}_i \subseteq \mathfrak{a}_{i+1},$$

so müssen von einem gewissen n *ab alle Glieder gleich sein*:

$$\mathfrak{a}_n = \mathfrak{a}_{n+1} = \cdots.$$

[1] Man könnte vielleicht besser sagen: Teilerkettenforderung oder Teilerkettenbedingung.

Daß der Teilerkettensatz aus dem Basissatz folgt, sieht man so: Es sei $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3, \ldots$ eine unendliche Kette und stets $\mathfrak{a}_i \leqq \mathfrak{a}_{i+1}$. Die Vereinigung $\mathfrak{v}$ aller Ideale $\mathfrak{a}_i$ ist ein Ideal. Denn wenn a und b in $\mathfrak{v}$ liegen, etwa a in $\mathfrak{a}_n$ und b in $\mathfrak{a}_m$, so liegen a und b beide in $\mathfrak{a}_N$, wo N die größte der Zahlen n und m ist; also liegt $a - b$ auch in $\mathfrak{a}_N$, also in $\mathfrak{v}$. Und wenn a in $\mathfrak{v}$ liegt, etwa in $\mathfrak{a}_n$, so liegt auch λa in $\mathfrak{a}_n$, also in $\mathfrak{v}$.

Dieses Ideal $\mathfrak{v}$ hat nach Voraussetzung eine Basis $(a_1, \ldots, a_r)$. Jedes a_i liegt in einem Ideal $\mathfrak{a}_{n_i}$. Ist n die größte der Zahlen n_i, so liegen $a_1, \ldots, a_r$ sämtlich in $\mathfrak{a}_n$. Da alle Elemente von $\mathfrak{v}$ linear von $a_1, \ldots, a_r$ abhängen, so liegen alle Elemente von $\mathfrak{v}$ in $\mathfrak{a}_n$, und daraus folgt

$$\mathfrak{v} = \mathfrak{a}_n = \mathfrak{a}_{n+1} = \mathfrak{a}_{n+2} = \cdots.$$

Umgekehrt folgt der Basissatz aus dem Teilerkettensatz (Auswahlpostulat vorausgesetzt). Nämlich: Auf Grund des Auswahlpostulats (§ 58) denke man sich in jeder nichtleeren Untermenge von $\mathfrak{o}$ ein Element ausgezeichnet. Es sei nun $\mathfrak{a}$ ein Ideal, a_1 das ausgezeichnete Element von $\mathfrak{a}$. Wenn a_1 noch nicht das ganze Ideal erzeugt, so gibt es in $\mathfrak{a}$ noch Elemente, die nicht in (a_1) liegen; in der Menge dieser Elemente sei a_2 das ausgezeichnete Element. Dann folgt:

$$(a_1) \subset (a_1, a_2).$$

Wenn a_1 und a_2 noch nicht das ganze Ideal $\mathfrak{a}$ erzeugen, so findet man in derselben Weise ein drittes ausgezeichnetes Element a_3 in $\mathfrak{a}$, das nicht in (a_1, a_2) liegt, usw. So erhält man eine Teilerkette

$$(a_1) \subset (a_1, a_2) \subset (a_1, a_2, a_3) \subset \cdots,$$

die im Endlichen (etwa nach r Schritten) abbrechen muß. Dann folgt:

$$(a_1, a_2, \ldots, a_r) = \mathfrak{a};$$

demnach hat $\mathfrak{a}$ eine endliche Basis.

Wenn der Teilerkettensatz in einem Ring $\mathfrak{o}$ gilt, so gilt er auch in jedem Restklassenbereich $\mathfrak{o}/\mathfrak{a}$.

Beweis: Ein Ideal $\bar{\mathfrak{b}}$ in $\mathfrak{o}/\mathfrak{a}$ ist eine Menge von Restklassen. Bildet man die Vereinigungsmenge aller dieser Restklassen, so erhält man ein Ideal $\mathfrak{b}$ in $\mathfrak{o}$. Umgekehrt ist $\bar{\mathfrak{b}}$ durch $\mathfrak{b}$ eindeutig bestimmt vermöge

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

Eine Kette von Idealen $\bar{\mathfrak{b}}_1 \subset \bar{\mathfrak{b}}_2 \subset \bar{\mathfrak{b}}_3 \subset \cdots$ in $\mathfrak{o}/\mathfrak{a}$ ergibt in dieser Weise eine Kette von Idealen $\mathfrak{b}_1 \subset \mathfrak{b}_2 \subset \mathfrak{b}_3 \subset \cdots$ in $\mathfrak{o}$, und da die letztere im Endlichen abbricht, so muß die erstere es auch tun.

Damit ist auch die zu Anfang dieses Paragraphen aufgestellte Behauptung, daß aus dem Basissatz für $\mathfrak{o}$ der Basissatz für $\mathfrak{o}/\mathfrak{a}$ folgt, bewiesen.

Der Teilerkettensatz läßt noch zwei andere Fassungen zu, die für Anwendungen oft bequemer sind:

Teilerkettensatz, 3. Fassung: Maximalbedingung.

Wenn in $\mathfrak{o}$ *der Teilerkettensatz gilt, so gibt es in jeder nichtleeren Menge von Idealen ein maximales Ideal, d. h. ein solches, das nicht von einem anderen Ideal der Menge umfaßt wird.*

Beweis: Aus jeder nichtleeren Menge von Idealen sei eins ausgezeichnet. Gesetzt nun, es gäbe in einer Menge $\mathfrak{M}$ von Idealen kein maximales Ideal, so würde jedes Ideal der Menge noch von einem anderen der Menge umfaßt werden. Suchen wir nun aus $\mathfrak{M}$ das ausgezeichnete Ideal $\mathfrak{a}_1$, weiter aus der Menge derjenigen Ideale von $\mathfrak{M}$, die $\mathfrak{a}_1$ umfassen und $\neq \mathfrak{a}_1$ sind, das ausgezeichnete Ideal $\mathfrak{a}_2$ usw., so kommen wir zu einer unendlichen Kette

$$\mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \mathfrak{a}_3 \subset \cdots,$$

die nach Voraussetzung nicht möglich ist.

Teilerkettensatz, 4. Fassung: Prinzip der Teilerinduktion.

Wenn in $\mathfrak{o}$ *der Teilerkettensatz gilt und eine Eigenschaft E für jedes Ideal* $\mathfrak{a}$ *(insbesondere auch für das Einheitsideal) bewiesen werden kann unter der Voraussetzung, daß sie für alle echten Teiler von* $\mathfrak{a}$ *erfüllt ist, so kommt die Eigenschaft E allen Idealen zu.*

Beweis: Gesetzt, die Eigenschaft E käme einem Ideal nicht zu. Dann gäbe es nach der 3. Fassung des Teilerkettensatzes auch ein maximales Ideal $\mathfrak{a}$, welches die Eigenschaft E nicht hätte. Wegen der Maximalität müßten alle echten Teiler von $\mathfrak{a}$ die Eigenschaft E haben, also $\mathfrak{a}$ auch, was einen Widerspruch bedeutet.

§ 81. Produkte und Quotienten von Idealen.

Ähnlich wie in § 15 verstehen wir unter dem *größten gemeinsamen Teiler* (G. G. T.) oder der *Summe* der Ideale $\mathfrak{a}, \mathfrak{b}, \ldots$ das von ihrer Vereinigungsmenge erzeugte Ideal $(\mathfrak{a}, \mathfrak{b}, \ldots)$ und ebenso unter dem *kleinsten gemeinsamen Vielfachen* (K. G. V.) den Durchschnitt $[\mathfrak{a}, \mathfrak{b}, \ldots] = \mathfrak{a} \cap \mathfrak{b} \cap \ldots$. Dieselbe Bezeichnung wie für die Idealsumme verwendet man für ein Erzeugnis aus einigen Elementen und einigen Idealen, etwa:

$$(a, b) = (a, (b)).$$

Selbstverständlich ist $(\mathfrak{a}, \mathfrak{b}) = (\mathfrak{b}, \mathfrak{a})$, $((\mathfrak{a}, \mathfrak{b}), \mathfrak{c}) = (\mathfrak{a}, (\mathfrak{b}, \mathfrak{c})) = (\mathfrak{a}, \mathfrak{b}, \mathfrak{c})$, usw. Weiter:

$$((a_1, a_2, \ldots), \quad (b_1, b_2, \ldots)) = (a_1, a_2, \ldots, b_1, b_2, \ldots);$$

in Worten: *Man erhält eine Basis für den größten gemeinsamen Teiler, indem man die Basen der einzelnen Ideale nebeneinander schreibt.*

Multipliziert man die Elemente eines Ideals $\mathfrak{a}$ mit denen eines Ideals $\mathfrak{b}$, so bilden die Produkte $a\,b$ (im Gegensatz zu den Summen)

im allgemeinen kein Ideal[1]. Das von diesen Produkten $a\,b$ erzeugte Ideal aber nennt man das *Produkt* der Ideale $\mathfrak{a}$, $\mathfrak{b}$ und bezeichnet es mit $\mathfrak{a}\cdot\mathfrak{b}$ oder $\mathfrak{a}\mathfrak{b}$. Es besteht aus allen Summen $\sum a_i b_i$ (a_i in $\mathfrak{a}$, b_i in $\mathfrak{b}$).

Offenbar ist

$$\mathfrak{a}\cdot\mathfrak{b} = \mathfrak{b}\cdot\mathfrak{a},$$
$$(\mathfrak{a}\cdot\mathfrak{b})\cdot\mathfrak{c} = \mathfrak{a}\cdot(\mathfrak{b}\cdot\mathfrak{c});$$

man kann also mit Produkten von Idealen wie mit gewöhnlichen Produkten rechnen. Insbesondere hat es Sinn, von *Potenzen* $\mathfrak{a}^\varrho$ eines Ideals zu reden; sie sind definiert durch

$$\mathfrak{a}^1 = \mathfrak{a}; \qquad \mathfrak{a}^{\varrho+1} = \mathfrak{a}\cdot\mathfrak{a}^\varrho.$$

Ist $\mathfrak{a} = (a_1, \ldots, a_n)$ und $\mathfrak{b} = (b_1, \ldots, b_m)$, so wird ersichtlich das Produkt $\mathfrak{a}\mathfrak{b}$ von den Produkten $a_i b_k$ erzeugt. *Man erhält also eine Basis für das Produkt durch Multiplikation aller Basiselemente des einen Faktors mit allen Basiselementen des anderen.*

Insbesondere ist für Hauptideale

$$(a)\cdot(b) = (a\,b);$$

im Bereich der Elemente von $\mathfrak{o}$ stimmt also die Produktdefinition mit der gewöhnlichen überein.

Das Produkt $\mathfrak{a}\cdot(b)$ aus einem beliebigen Ideal und einem Hauptideal besteht aus allen Produkten ab, wo a in $\mathfrak{a}$ liegt. Man schreibt daher einfach $\mathfrak{a}b$ oder $b\mathfrak{a}$.

Eine weitere Rechenregel ist das „Distributivgesetz der Ideale“:

$$\mathfrak{a}\cdot(\mathfrak{b},\mathfrak{c}) = (\mathfrak{a}\cdot\mathfrak{b},\ \mathfrak{a}\cdot\mathfrak{c}). \tag{1}$$

Denn $\mathfrak{a}\cdot(\mathfrak{b},\mathfrak{c})$ wird erzeugt von den Produkten $a(b+c)$, welche wegen

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

alle in $(\mathfrak{a}\cdot\mathfrak{b},\ \mathfrak{a}\cdot\mathfrak{c})$ liegen; umgekehrt wird $(\mathfrak{a}\cdot\mathfrak{b},\ \mathfrak{a}\cdot\mathfrak{c})$ erzeugt von den Produkten ab und den Produkten ac, welche alle in $\mathfrak{a}\cdot(\mathfrak{b},\mathfrak{c})$ liegen.

Dieselbe Regel (1) gilt auch, wenn in der Klammer statt $\mathfrak{b}$, $\mathfrak{c}$ mehrere oder sogar unendlichviele Ideale stehen.

Da alle Produkte ab in $\mathfrak{a}$ liegen, so ist

$$\mathfrak{a}\cdot\mathfrak{b} \subseteq \mathfrak{a}$$

und ebenso

$$\mathfrak{a}\cdot\mathfrak{b} \subseteq \mathfrak{b}.$$

Daraus folgt:

$$\mathfrak{a}\cdot\mathfrak{b} \subseteq [\mathfrak{a},\mathfrak{b}]$$

oder: *Das Produkt ist durch das kleinste gemeinsame Vielfache teilbar.*

[1] Beispiel: Ist in einem Polynombereich $\mathfrak{a} = (x, y)$ und $\mathfrak{b} = (x^2, y)$, so sind x^3 und y^2 Produkte von der Gestalt $a\cdot b$, nicht aber $x^3 - y^2$.

Im Ring der ganzen Zahlen ist das Produkt aus kleinstem gemeinsamen Vielfachen und größtem gemeinsamen Teiler zweier Ideale $\mathfrak{a}, \mathfrak{b}$ gleich dem Produkt $\mathfrak{a}\mathfrak{b}$. Das gilt nicht in beliebigen Ringen; wohl aber gilt:

$$(2) \qquad [\mathfrak{a} \cap \mathfrak{b}] \cdot (\mathfrak{a}, \mathfrak{b}) \equiv 0\,(\mathfrak{a} \cdot \mathfrak{b}).$$

Beweis:

$$[\mathfrak{a} \cap \mathfrak{b}] \cdot (\mathfrak{a}, \mathfrak{b}) = ([\mathfrak{a} \cap \mathfrak{b}] \cdot \mathfrak{a}, [\mathfrak{a} \cap \mathfrak{b}] \cdot \mathfrak{b}) \subseteq (\mathfrak{b} \cdot \mathfrak{a}, \mathfrak{a} \cdot \mathfrak{b}) = \mathfrak{a} \cdot \mathfrak{b}.$$

Das Ideal $\mathfrak{o}$, das aus *allen* Elementen des betrachteten Ringes besteht, heißt nach § 14 *Einheitsideal*. Es ist natürlich

$$\mathfrak{a} \cdot \mathfrak{o} \subseteq \mathfrak{a}.$$

Enthält aber $\mathfrak{o}$ ein Einselement e, so ist auch umgekehrt

$$\mathfrak{a} = \mathfrak{a} \cdot e \subseteq \mathfrak{a} \cdot \mathfrak{o},$$

also

$$\mathfrak{a} \cdot \mathfrak{o} = \mathfrak{a}.$$

Das Ideal $\mathfrak{o}$ spielt demnach in diesem Fall die Rolle eines Einselements der Multiplikation. Es wird dann vom Einselement erzeugt.

Man hat immer

$$(\mathfrak{a}, \mathfrak{o}) = \mathfrak{o}; \qquad \mathfrak{a} \cap \mathfrak{o} = \mathfrak{a}.$$

Unter dem *Idealquotienten* $\mathfrak{a}:\mathfrak{b}$, wo $\mathfrak{a}$ ein Ideal ist, verstehen wir die Gesamtheit der Elemente γ von $\mathfrak{o}$, für die

$$(3) \qquad \gamma\, b \equiv 0\,(\mathfrak{a}) \text{ für alle } b \text{ aus } \mathfrak{b}.$$

Diese Gesamtheit ist ein Ideal; denn wenn γ und δ die Eigenschaft (3) haben, so hat $\gamma - \delta$ sie auch, und wenn γ sie hat, so hat $r\gamma$ sie auch. Dabei ist vorausgesetzt, daß $\mathfrak{a}$ ein Ideal ist; $\mathfrak{b}$ braucht es nicht zu sein, sondern kann irgend eine Menge oder auch ein einzelnes Element sein.

Zufolge der Definition ist, wenn $\mathfrak{a}$ und $\mathfrak{b}$ Ideale sind,

$$\mathfrak{b} \cdot (\mathfrak{a} : \mathfrak{b}) \equiv 0\,(\mathfrak{a}).$$

Im Ring der ganzen Zahlen wird die Quotientenbildung zweier Hauptideale $(a), (b) \neq (0)$ so ausgeführt, daß man aus der Faktorzerlegung der Zahl a die Faktoren, die auch in b vorkommen, wegläßt; z. B.:

$$(12) : (2) = (6),$$
$$(12) : (4) = (3),$$
$$(12) : (8) = (3),$$
$$(12) : (5) = (12).$$

Anders ausgedrückt: Man dividiert a im gewöhnlichen Sinn durch den größten gemeinsamen Teiler (a, b).

In allgemeinen Ringen gilt eine entsprechende Regel:

$$\mathfrak{a} : \mathfrak{b} = \mathfrak{a} : (\mathfrak{a}, \mathfrak{b}),$$

die leicht zu beweisen und übrigens nicht sehr wichtig ist.

Offensichtlich ist $\mathfrak{a} \equiv 0\,(\mathfrak{a}:\mathfrak{b})$, denn jedes Element von $\mathfrak{a}$ hat die Eigenschaft (3). Es gibt also zwei Extremfälle:

$$\mathfrak{a} : \mathfrak{b} = \mathfrak{o} \quad \text{und} \quad \mathfrak{a} : \mathfrak{b} = \mathfrak{a}.$$

Der erste Fall tritt u. a. dann ein, wenn $\mathfrak{b} \subseteq \mathfrak{a}$; denn dann ist für jedes γ

$$\gamma\,\mathfrak{b} \equiv 0\,(\mathfrak{b}) \equiv 0\,(\mathfrak{a}).$$

Der zweite Fall bedeutet, daß aus $\gamma\mathfrak{b} \equiv 0\,(\mathfrak{a})$ folgt $\gamma \equiv 0\,(\mathfrak{a})$. Man kann also die Kongruenz $\gamma\mathfrak{b} \equiv 0\,(\mathfrak{a})$ durch $\mathfrak{b}$ kürzen. Man nennt in diesem Fall $\mathfrak{b}$ *relativ-prim zu* $\mathfrak{a}$ oder prim zu $\mathfrak{a}$; doch werden wir diesen leicht mißzuverstehenden Ausdruck selten verwenden und meist die Gleichung $\mathfrak{a}:\mathfrak{b} = \mathfrak{a}$ direkt hinschreiben. Im Falle ganzer Zahlen a und b, beide $\neq 0$, ist offensichtlich das Kriterium:

$$\text{aus} \quad \gamma\, b \equiv 0\,(a) \quad \text{folgt} \quad \gamma \equiv 0\,(a)$$

nur dann erfüllt, wenn a und b keinen gemeinsamen Primfaktor besitzen. In allgemeineren Fällen ist aber das Prädikat „relativ-prim" *nicht symmetrisch;* wenn z. B. $\mathfrak{a}$ ein Primideal und $\mathfrak{b}$ ein von $\mathfrak{o}$ verschiedener echter Primidealteiler von $\mathfrak{a}$ ist, so ist

$$\mathfrak{a} : \mathfrak{b} = \mathfrak{a}, \text{ also } \mathfrak{b} \text{ relativ-prim zu } \mathfrak{a},$$

aber

$$\mathfrak{b} : \mathfrak{a} = \mathfrak{o}, \text{ also } \mathfrak{a} \text{ nicht relativ-prim zu } \mathfrak{b}.$$

Z. B. ist

$$(0) : (2) = (0),$$
$$(2) : (0) = (1).$$

Wichtig ist die folgende Rechenregel:

(4) $$[\mathfrak{a}_1, \ldots, \mathfrak{a}_r] : \mathfrak{b} = [\mathfrak{a}_1 : \mathfrak{b}, \ldots, \mathfrak{a}_r : \mathfrak{b}].$$

Beweis: Aus

$$\gamma\,\mathfrak{b} \subseteq [\mathfrak{a}_1, \ldots, \mathfrak{a}_r]$$

folgt

$$\gamma\,\mathfrak{b} \subseteq \mathfrak{a}_i \quad \text{für jedes } i$$

und umgekehrt.

Aufgaben. 1. Man beweise die Rechenregeln:

$$(\mathfrak{a}:\mathfrak{b}):\mathfrak{c} = \mathfrak{a}:\mathfrak{b}\,\mathfrak{c} = (\mathfrak{a}:\mathfrak{c}):\mathfrak{b},$$
$$\mathfrak{a}:(\mathfrak{b},\mathfrak{c}) = (\mathfrak{a}:\mathfrak{b}) \cap (\mathfrak{a}:\mathfrak{c}).$$

2. Man zeige die Äquivalenz der drei Behauptungen:

a) $\mathfrak{a}:\mathfrak{b}_1 = \mathfrak{a}$ und $\mathfrak{a}:\mathfrak{b}_2 = \mathfrak{a}$;

b) $\mathfrak{a}:[\mathfrak{b}_1 \cap \mathfrak{b}_2] = \mathfrak{a}$;

c) $\mathfrak{a}:\mathfrak{b}_1\,\mathfrak{b}_2 = \mathfrak{a}$.

§ 82. Primideale und Primärideale.

Schon früher haben wir Primideale definiert als solche Ideale, deren Restklassenring keine Nullteiler hat.

Im Bereich der ganzen Zahlen ist jede ganze Zahl $a > 0$ Produkt von Potenzen verschiedener Primzahlen

$$a = \mathfrak{p}_1^{\varrho_1} \cdots \mathfrak{p}_r^{\varrho_r}, \tag{1}$$

und demnach jedes Ideal (a) Produkt von Primidealpotenzen:

$$(a) = (\mathfrak{p}_1)^{\varrho_1} \cdots (\mathfrak{p}_r)^{\varrho_r}.$$

In allgemeineren Ringen kann man nicht erwarten, daß die Zerlegungsgesetze der Ideale so einfach sind. Zum Beispiel hat im ganzzahligen Polynombereich einer Unbestimmten x das Ideal $(4, x)$, das nicht prim ist, außer $\mathfrak{o}$ nur einen Primteiler $(2, x)$; aber keine Potenz von $(2, x)$ stellt das Ideal $(4, x)$ dar. Man kann also im allgemeinen keine Produktdarstellung der Ideale erwarten, sondern höchstens eine Darstellung als K. G. V. (Durchschnitt) von möglichst einfachen Bestandteilen[1], entsprechend der aus (1) folgenden Darstellung von (a) als K. G. V.:

$$(a) = [(\mathfrak{p}_1^{\varrho_1}), \ldots, (\mathfrak{p}_r^{\varrho_r})].$$

Die Ideale $(\mathfrak{p}_k^{\varrho_k})$ haben nun die folgende charakteristische Eigenschaft: Wenn ein Produkt $a\,b$ durch $\mathfrak{p}_k^{\varrho_k}$ teilbar ist und der eine Faktor a es nicht ist, so muß der andere Faktor b zumindest einen Faktor von $\mathfrak{p}_k^{\varrho_k}$ enthalten. Das drückt sich darin aus, daß eine Potenz b^ϱ durch $\mathfrak{p}_k^{\varrho_k}$ teilbar sein muß. Also:

Aus

$$a\,b \equiv 0\,(\mathfrak{p}_k^{\varrho_k}),$$
$$a \not\equiv 0\,(\mathfrak{p}_k^{\varrho_k})$$

folgt

$$b^\varrho \equiv 0\,(\mathfrak{p}_k^{\varrho_k}).$$

Ideale mit dieser Eigenschaft werden *Primärideale* genannt.

Ein Ideal $\mathfrak{q}$ *heißt primär, wenn aus*

$$a\,b \equiv 0\,(\mathfrak{q}), \quad a \not\equiv 0\,(\mathfrak{q})$$

folgt, daß es ein ϱ *gibt so, daß*

$$b^\varrho \equiv 0\,(\mathfrak{q}).$$

Man kann die Definition auch so fassen:

Wenn im Restklassenring nach $\mathfrak{q}$ $\bar{a}\bar{b} = 0$ *und* $\bar{a} \neq 0$ *ist, so soll eine Potenz* $\bar{b}^\varrho$ *verschwinden.*

---

[1] Eine K.G.V.-Darstellung ist in gewissen Fällen auch nützlicher als eine Produktdarstellung, nämlich dann, wenn es sich darum handelt, zu entscheiden, ob ein Element b durch ein Ideal $\mathfrak{m}$ teilbar ist, d. h. zu $\mathfrak{m}$ gehört. Ist $\mathfrak{m} = [\mathfrak{a}_1, \ldots, \mathfrak{a}_r]$, so gehört b zu $\mathfrak{m}$, sobald b allen $\mathfrak{a}_\nu$ angehört, und nur dann.

Ist $\bar{a}\bar{b} = 0$ und $\bar{a} \neq 0$, so heißt das nichts anderes, als daß $\bar{b}$ ein Nullteiler ist. Wenn ein Ringelement $\bar{b}$ die Eigenschaft hat, daß eine Potenz $\bar{b}^\varrho$ verschwindet, so heißt das Element *nilpotent*. Also kann man auch sagen:

Ein Ideal heißt primär, wenn in seinem Restklassenring jeder Nullteiler nilpotent ist.

Wie man sieht, ist die Definition eine leichte Modifikation der Primidealdefinition; im Restklassenring nach einem Primideal muß jeder Nullteiler nicht nur nilpotent sein, sondern selbst verschwinden.

Wir werden sehen, daß die Primärideale in allgemeinen Ringen dieselbe Rolle spielen wie die Primzahlpotenzen im Bereich der ganzen Zahlen, daß nämlich unter sehr allgemeinen Voraussetzungen jedes Ideal sich als Durchschnitt von Primäridealen darstellen läßt und daß in dieser Darstellung die wesentlichsten Struktureigenschaften der Ideale zum Ausdruck kommen.

Die Primärideale sind nicht notwendig Primidealpotenzen; das zeigt schon das zu Anfang angeführte Ideal $(4, x)$, welches man leicht als primär erkennt. Das Umgekehrte gilt aber ebensowenig; denn im Ring derjenigen ganzzahligen Polynome $a_0 + a_1 x + \cdots + a_n x^n$, bei denen a_1 durch 3 teilbar ist, ist $\mathfrak{p} = (3x, x^2)$ ein Primideal, aber $\mathfrak{p}^2 = (9x^2, 3x^3, x^4)$ nicht primär, denn es ist

$$9 \cdot x^2 \equiv 0 \,(\mathfrak{p}^2),$$
$$x^2 \not\equiv 0 \,(\mathfrak{p}^2),$$
$$9^\varrho \not\equiv 0 \,(\mathfrak{p}^2)$$

für jedes ϱ.

Eigenschaften der Primärideale unabhängig vom Teilerkettensatz.

I. *Zu jedem Primärideal* $\mathfrak{q}$ *gehört ein Primidealteiler* $\mathfrak{p}$, *der folgendermaßen definiert wird:* $\mathfrak{p}$ *ist die Gesamtheit der Elemente* b, *von denen eine Potenz* b^ϱ *in* $\mathfrak{q}$ *liegt.*

Beweis: Erstens: $\mathfrak{p}$ ist ein Ideal; denn aus $b^\varrho \equiv 0 \,(\mathfrak{q})$ folgt $(rb)^\varrho \equiv 0 (\mathfrak{q})$ und aus $b^\varrho \equiv 0 \,(\mathfrak{q})$ und $c^\sigma \equiv 0 \,(\mathfrak{q})$ folgt, da in der Entwicklung von $(b - c)^{\varrho+\sigma-1}$ in jedem Summanden entweder b^ϱ oder c^σ vorkommt,

$$(b - c)^{\varrho+\sigma-1} \equiv 0 \,(\mathfrak{q}).$$

Zweitens: $\mathfrak{p}$ ist prim; denn aus

$$ab \equiv 0 \,(\mathfrak{p}),$$
$$a \not\equiv 0 \,(\mathfrak{p})$$

folgt, daß es ein ϱ gibt so, daß

$$a^\varrho b^\varrho \equiv 0 \,(\mathfrak{q})$$

und weiter

$$a^\varrho \not\equiv 0 \,(\mathfrak{q})$$

ist. Es muß also ein σ geben so, daß

$$b^{\varrho\sigma} \equiv 0 \,(\mathfrak{q})$$

ist; daraus folgt

$$b \equiv 0 \,(\mathfrak{p}).$$

Drittens: $\mathfrak{p}$ ist Teiler von $\mathfrak{q}$:

$$\mathfrak{q} \equiv 0 \,(\mathfrak{p});$$

denn die Elemente von $\mathfrak{q}$ haben sicher die Eigenschaft, daß eine Potenz in $\mathfrak{q}$ liegt.

$\mathfrak{p}$ heißt *das zu* $\mathfrak{q}$ *gehörige Primideal,* $\mathfrak{q}$ ein zu $\mathfrak{p}$ gehöriges Primärideal. Zufolge der Definition des Primärideals gilt:

II. *Aus* $ab \equiv 0 \,(\mathfrak{q})$ *und* $a \not\equiv 0 \,(\mathfrak{q})$ *folgt* $b \equiv 0 \,(\mathfrak{p})$.

Gewissermaßen die Umkehrung dieses Satzes ist der folgende:

III. *Wenn* $\mathfrak{p}$ *und* $\mathfrak{q}$ *Ideale sind und die Eigenschaft haben, daß*

1. *aus* $ab \equiv 0 \,(\mathfrak{q})$ *und* $a \not\equiv 0 \,(\mathfrak{q})$ *folgt* $b \equiv 0 \,(\mathfrak{p})$,
2. $\mathfrak{q} \equiv 0 \,(\mathfrak{p})$,
3. *aus* $b \equiv 0 \,(\mathfrak{p})$ *folgt* $b^\varrho \equiv 0 \,(\mathfrak{q})$,

so ist $\mathfrak{q}$ *primär und* $\mathfrak{p}$ *das zugehörige Primideal.*

Beweis: Aus $ab \equiv 0 \,(\mathfrak{q})$ und $a \not\equiv 0 \,(\mathfrak{q})$ folgt (wegen 1. und 3.) $b^\varrho \equiv 0 \,(\mathfrak{q})$. Also ist $\mathfrak{q}$ primär. Zu zeigen ist nur noch, daß $\mathfrak{p}$ aus den Elementen b besteht, von denen eine Potenz b^ϱ in $\mathfrak{q}$ liegt. Die eine Hälfte dieser Behauptung ist gerade 3. Zu zeigen bleibt, daß aus $b^\varrho \equiv 0 \,(\mathfrak{q})$ folgt $b \equiv 0 \,(\mathfrak{p})$. Es sei ϱ die kleinste natürliche Zahl, für die $b^\varrho \equiv 0 \,(\mathfrak{q})$ gilt. Für $\varrho = 1$ sind wir fertig nach 2. Für $\varrho > 1$ hat man $b \cdot b^{\varrho-1} \equiv 0 \,(\mathfrak{q})$, aber $b^{\varrho-1} \not\equiv 0 \,(\mathfrak{q})$, mithin (nach 1.) $b \equiv 0 \,(\mathfrak{p})$.

Dieser Satz erleichtert den Nachweis der Primäreigenschaft und die Auffindung des zugehörigen Primideals in speziellen Fällen und zeigt, durch welche Eigenschaften das zugehörige Primideal eindeutig bestimmt ist.

Die Eigenschaft II gilt auch dann noch, wenn man a und b durch Ideale $\mathfrak{a}$ und $\mathfrak{b}$ ersetzt:

IV. *Aus* $\mathfrak{a}\mathfrak{b} \equiv 0 \,(\mathfrak{q})$ *und* $\mathfrak{a} \not\equiv 0 \,(\mathfrak{q})$ *folgt* $\mathfrak{b} \equiv 0 \,(\mathfrak{p})$.

Denn wäre $\mathfrak{b} \not\equiv 0 \,(\mathfrak{v})$, so würde es ein Element b in $\mathfrak{b}$ geben, das nicht in $\mathfrak{p}$ liegt, und ebenso ein Element a in $\mathfrak{a}$, das nicht in $\mathfrak{q}$ liegt. Das Produkt ab müßte aber in $\mathfrak{a}\mathfrak{b}$, also in $\mathfrak{q}$ liegen im Widerspruch zum früher Bewiesenen.

Genau so beweist man den entsprechenden Satz für Primideale:

Aus $\mathfrak{a}\mathfrak{b} \equiv 0 \,(\mathfrak{p})$ *und* $\mathfrak{a} \not\equiv 0 \,(\mathfrak{p})$ *folgt* $\mathfrak{b} \equiv 0 \,(\mathfrak{p})$.

Eine Folge davon [durch $(h-1)$-malige Anwendung zu beweisen] ist:

Aus $\mathfrak{a}^h \equiv 0\,(\mathfrak{p})$ *folgt* $\mathfrak{a} \equiv 0\,(\mathfrak{p})$.

Eine andere Fassung von Satz IV ist:

IV'. *Aus* $\mathfrak{b} \not\equiv 0\,(\mathfrak{p})$ *folgt* $\mathfrak{q} : \mathfrak{b} = \mathfrak{q}$.

Im Restklassenring $\mathfrak{o}/\mathfrak{q}$ liegt (wegen $\mathfrak{p} \supseteq \mathfrak{q}$) das Ideal $\mathfrak{p}/\mathfrak{q}$. Es besteht aus allen nilpotenten Elementen, im Falle $\mathfrak{q} \neq \mathfrak{o}$ also aus allen Nullteilern.

Eigenschaften der Primärideale unter Voraussetzung des Teilerkettensatzes.

Ist $\mathfrak{p}$ das zu $\mathfrak{q}$ gehörige Primideal, so liegt eine Potenz eines jeden Elements von $\mathfrak{p}$ in $\mathfrak{q}$. Die dazu mindestens nötigen Exponenten hängen vom gewählten Element ab und können unbeschränkt wachsen. Setzt man aber im Ring $\mathfrak{o}$ den Teilerkettensatz voraus, so wachsen die Exponenten nicht mehr unbeschränkt, vermöge des folgenden Satzes:

V. *Eine Potenz* $\mathfrak{p}^\varrho$ *ist durch* $\mathfrak{q}$ *teilbar*:

$$\mathfrak{p}^\varrho \equiv 0\,(\mathfrak{q}).$$

Beweis: Es sei $(p_1, \ldots, p_r)$ eine Basis für $\mathfrak{p}$. Es mögen $p_1^{\varrho_1}, \ldots, p_r^{\varrho_r}$ in $\mathfrak{q}$ liegen. Setzt man dann

$$\varrho = \sum_1^r (\varrho_i - 1) + 1,$$

so wird $\mathfrak{p}^\varrho$ erzeugt von allen Produkten der p_i zu je ϱ; in jedem solchen Produkt muß mindestens ein Faktor p_i mehr als $(\varrho_i - 1)$ mal, also mindestens ϱ_i mal vorkommen; alle Erzeugenden von $\mathfrak{p}^\varrho$ liegen also in $\mathfrak{q}$, woraus der Satz folgt.

Zwischen einem Primärideal $\mathfrak{q}$ und seinem zugehörigen Primideal $\mathfrak{p}$ bestehen demnach die folgenden Relationen:

$$\text{(2)} \qquad \begin{cases} \mathfrak{q} \equiv 0\,(\mathfrak{p}), \\ \mathfrak{p}^\varrho \equiv 0\,(\mathfrak{q}). \end{cases}$$

Die kleinste Zahl ϱ, für die diese Relationen gelten, heißt der *Exponent* von $\mathfrak{q}$. Der Exponent gibt insbesondere eine obere Schranke für die Exponenten der Potenzen, in die man die Elemente von $\mathfrak{p}$ (mindestens) zu erheben hat, um Elemente von $\mathfrak{q}$ zu erhalten.

Ist $\mathfrak{q}$ primär, so sind die Gleichungen (2) für das zugehörige Primideal $\mathfrak{p}$ charakteristisch. Denn gesetzt, ein zweites Primideal $\mathfrak{p}'$ erfüllte mit einem Exponenten ϱ' ebenfalls (2), so würde folgen

$$\begin{cases} \mathfrak{p}^\varrho \subseteq \mathfrak{q} \subseteq \mathfrak{p}', & \text{also} \quad \mathfrak{p} \subseteq \mathfrak{p}', \\ \mathfrak{p}'^{\varrho'} \subseteq \mathfrak{q} \subseteq \mathfrak{p}, & \text{also} \quad \mathfrak{p}' \subseteq \mathfrak{p}, \end{cases}$$

mithin $\mathfrak{p}' = \mathfrak{p}$. Die Relationen (2) sind aber nicht charakteristisch für die Primärideale: es kann sehr gut sein, daß (2) für ein nicht primäres $\mathfrak{q}$ gilt (vgl. die nachstehende Aufgabe 1).

VI. *Aus* $\mathfrak{a}\mathfrak{b} \equiv 0\,(\mathfrak{q})$ *und* $\mathfrak{a} \not\equiv 0\,(\mathfrak{q})$ *folgt, daß eine Potenz* $\mathfrak{b}^\sigma \equiv 0\,(\mathfrak{q})$ *ist.*

Beweis: Es genügt, $\sigma = \varrho$ zu wählen. Aus $\mathfrak{a}\mathfrak{b} \equiv 0\,(\mathfrak{q})$ und $\mathfrak{a} \not\equiv 0\,(\mathfrak{q})$ folgt nämlich, wie früher bewiesen, $\mathfrak{b} \equiv 0\,(\mathfrak{p})$ und daraus

$$\mathfrak{b}^\varrho \equiv 0\,(\mathfrak{p}^\varrho) \equiv 0\,(\mathfrak{q}).$$

Ein Ideal $\mathfrak{q}$ mit der zuletzt ausgesprochenen Eigenschaft heißt *stark primär*, im Gegensatz zu den früher definierten *schwach primären* Idealen oder Primäridealen schlechthin. Gilt der Teilerkettensatz, so fallen die beiden Begriffe zusammen; denn wir sahen schon, daß die primären Ideale in diesem Fall auch stark primär sind, und das Umgekehrte folgt einfach durch Spezialisierung der Ideale $\mathfrak{a}$, $\mathfrak{b}$ zu Hauptidealen (a), (b). Gilt der Teilerkettensatz nicht, so ist zwar jedes stark primäre Ideal auch schwach primär; aber die Umkehrung braucht nicht zu gelten.

Beispiel: Im Polynombereich von unendlich vielen Unbestimmten $x_1, x_2, x_3, \ldots$ ist das Ideal

$$\mathfrak{q} = (x_1, x_2^2, x_3^3, \ldots)$$

primär, und das zugehörige Primideal ist

$$\mathfrak{p} = (x_1, x_2, x_3, \ldots).$$

Diese beiden Behauptungen ergeben sich am leichtesten aus Satz III. $\mathfrak{q}$ besteht aus allen Polynomen, in denen das konstante Glied fehlt und in jedem Glied mindestens ein darin vorkommendes x_ν mindestens den Exponenten ν hat, während $\mathfrak{p}$ aus allen Polynomen ohne konstantes Glied besteht. Ist nun $a \not\equiv 0\,(\mathfrak{q})$ und $b \not\equiv 0\,(\mathfrak{p})$, so enthält b ein konstantes Glied $b_0 \neq 0$ und a ein Glied, in welchem jedes x_ν einen Exponenten $< \nu$ hat. Wir suchen nun unter diesen Gliedern von a ein Glied niedrigsten Grades aus; das ergibt, mit der Konstanten b_0 multipliziert, ein in ab wirklich vorkommendes Glied niedrigsten Grades, in welchem wieder jedes x_ν einen Exponenten $< \nu$ hat. Also folgt $ab \not\equiv 0\,(\mathfrak{q})$. Damit ist die Voraussetzung 1 von Satz III bewiesen. Ist weiter $b \equiv 0\,(\mathfrak{p})$, so fehlt in b das konstante Glied; ist x_ω die letzte der Unbestimmten $x_1, x_2, \ldots$, die im Polynom b wirklich vorkommt (in b können ja nur endlich viele x_ν vorkommen), so haben in b^{ω^2} alle Glieder mindestens den Grad ω^2. In jedem Glied kommt also mindestens ein x_ν in der ω-ten Potenz vor; demnach liegt b^{ω^2} in $\mathfrak{q}$. Da schließlich $\mathfrak{q} \equiv 0\,(\mathfrak{p})$ ist, so sind alle Voraussetzungen von Satz III erfüllt.

Trotzdem ist $\mathfrak{p}^\varrho \not\equiv 0\,(\mathfrak{q})$, wie groß man ϱ auch nehmen mag; denn $\mathfrak{p}^\varrho$ enthält das Element $x_{\varrho+1}^\varrho$, welches nicht in $\mathfrak{q}$ liegt.

Aufgaben. 1. Das Ideal $\mathfrak{a} = (x^2, 2x)$ im ganzzahligen Polynombereich einer Veränderlichen x ist nicht primär. Trotzdem ist $(x)^2 \equiv 0\,(\mathfrak{a}) \equiv 0\,(x)$ und (x) ein Primideal.

2. Ist $\mathfrak{p}$ ein teilerloses Primideal (§ 15) und $\mathfrak{p}^\varrho \equiv 0\,(\mathfrak{a}) \equiv 0\,(\mathfrak{o})$, so ist $\mathfrak{a}$ ein Primärideal zum Primideal $\mathfrak{p}$.

3. Hat $\mathfrak{o}$ ein Einselement, so ist $\mathfrak{o}$ selbst das einzige Primärideal zum Primideal $\mathfrak{o}$.

4. Ist $\mathfrak{o}^*$ ein Unterring von $\mathfrak{o}$ und $\mathfrak{q}$ ein Primärideal in $\mathfrak{o}$ zum Primideal $\mathfrak{p}$, so ist $\mathfrak{q} \cap \mathfrak{o}^*$ ein Primärideal in $\mathfrak{o}^*$ zum Primideal $\mathfrak{p} \cap \mathfrak{o}^*$.

§ 83. Der allgemeine Zerlegungssatz.

Im Ring $\mathfrak{o}$ sei der Teilerkettensatz vorausgesetzt: Jede Teilerkette von Idealen bricht im Endlichen ab. Daraus folgt also (unter Zugrundelegung des Auswahlpostulats) das „Prinzip der Teilerinduktion".

Reduzibel heißt ein Ideal $\mathfrak{m}$, wenn es als Durchschnitt zweier echter Teiler darstellbar ist:

$$\mathfrak{m} = \mathfrak{a} \cap \mathfrak{b}, \qquad \mathfrak{a} \supset \mathfrak{m}, \quad \mathfrak{b} \supset \mathfrak{m}.$$

Ist eine solche Darstellung nicht möglich, so heißt das Ideal *irreduzibel.*

Beispiele irreduzibler Ideale sind die Primideale; denn wäre für ein Primideal $\mathfrak{p}$ eine Darstellung

$$\mathfrak{p} = \mathfrak{a} \cap \mathfrak{b}, \qquad \mathfrak{a} \supset \mathfrak{p}, \quad \mathfrak{b} \supset \mathfrak{p}$$

möglich, so wäre

$$\mathfrak{a}\mathfrak{b} \equiv 0\,(\mathfrak{a} \cap \mathfrak{b}) \equiv 0\,(\mathfrak{p}), \qquad \mathfrak{a} \not\equiv 0\,(\mathfrak{p}), \quad \mathfrak{b} \not\equiv 0\,(\mathfrak{p}),$$

entgegen der Primeigenschaft.

Auf Grund des Teilerkettensatzes gilt nun der *erste Zerlegungssatz*: *Jedes Ideal ist Durchschnitt von endlichvielen irreduziblen.*

Beweis: Für irreduzible Ideale ist der Satz richtig. Es sei also $\mathfrak{m}$ reduzibel:

$$\mathfrak{m} = \mathfrak{a} \cap \mathfrak{b}, \qquad \mathfrak{a} \supset \mathfrak{m}, \quad \mathfrak{b} \supset \mathfrak{m}.$$

Setzt man den Satz für alle echten Teiler von $\mathfrak{m}$ als bewiesen voraus, so gilt er insbesondere für $\mathfrak{a}$ und $\mathfrak{b}$; also ist etwa

$$\mathfrak{a} = [\mathfrak{i}_1, \ldots, \mathfrak{i}_s],$$
$$\mathfrak{b} = [\mathfrak{i}_{s+1}, \ldots, \mathfrak{i}_r].$$

Daraus folgt aber

$$\mathfrak{m} = [\mathfrak{i}_1, \ldots, \mathfrak{i}_s, \mathfrak{i}_{s+1}, \ldots, \mathfrak{i}_r];$$

also gilt der Satz auch für $\mathfrak{m}$. Da er für das (stets irreduzible) Einheitsideal auch gilt, ist er nach dem „Prinzip der Teilerinduktion" allgemein richtig.

Von der Darstellung durch irreduzible Ideale kommt man nun zu einer Darstellung durch Primärideale, vermöge des Satzes:

Jedes irreduzible Ideal ist primär.

Beweis: $\mathfrak{m}$ sei nichtprimär. Es soll gezeigt werden, daß $\mathfrak{m}$ reduzibel ist.

Da $\mathfrak{m}$ nichtprimär ist, so gibt es zwei Elemente a, b mit den Eigenschaften

$$a\,b \equiv 0\,(\mathfrak{m}),$$
$$a \not\equiv 0\,(\mathfrak{m}),$$
$$b^{\varrho} \not\equiv 0\,(\mathfrak{m}) \text{ für jedes } \varrho.$$

Nach dem Teilerkettensatz muß die Reihe der Idealquotienten

$$\mathfrak{m}:b, \subset \mathfrak{m}:b^2, \ldots$$

einmal abbrechen, d. h. für ein gewisses k ist:

$$\mathfrak{m}:b^k = \mathfrak{m}:b^{k+1}.$$

Wir behaupten nun:

$$\mathfrak{m} = (\mathfrak{m}, a) \cap (\mathfrak{m}, \mathfrak{o}\, b^k). \tag{1}$$

Die beiden Ideale rechter Hand sind Teiler von $\mathfrak{m}$, und zwar echte Teiler, denn das erstere enthält a, das zweite enthält b^{k+1}. Wir haben zu zeigen, daß jedes gemeinsame Element von beiden notwendig zu $\mathfrak{m}$ gehört. Ein solches Element c hat, als Element von $(\mathfrak{m}, \mathfrak{o}\, b^k)$, die Gestalt

$$c = m + r\, b^k;$$

zweitens hat es aber, als Element von $(\mathfrak{m}, a)$, die Eigenschaft

$$c\, b \equiv 0\ (\mathfrak{m}\, b,\ a\, b) \equiv 0\ (\mathfrak{m}).$$

Daraus folgt

$$m\, b + r\, b^{k+1} = c\, b \equiv 0\ (\mathfrak{m}),$$

$$r\, b^{k+1} \equiv 0\ (\mathfrak{m})$$

und daraus wegen $\mathfrak{m} : b^{k+1} = \mathfrak{m} : b^k$:

$$r\, b^k \equiv 0\ (\mathfrak{m}),$$

$$c = m + r\, b^k \equiv 0\ (\mathfrak{m}).$$

Damit ist (1) bewiesen; $\mathfrak{m}$ ist also in der Tat reduzibel.

Da jedes Ideal als Durchschnitt von endlichvielen irreduziblen darstellbar und jedes irreduzible Ideal primär ist, so folgt:

Jedes Ideal ist als Durchschnitt von endlichvielen Primäridealen darstellbar.

Dieser Satz läßt sich noch verschärfen. Zunächst nämlich kann man aus einer Darstellung

$$\mathfrak{m} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_r]$$

alle überflüssigen Ideale $\mathfrak{q}_i$, d. h. alle diejenigen, die den Durchschnitt der übrigen umfassen, sukzessive streichen. Man kommt so zu einer *unverkürzbaren* Darstellung, d. h. zu einer solchen, in der keine Komponente $\mathfrak{q}_i$ den Durchschnitt der übrigen umfaßt. In einer solchen Darstellung kann es noch vorkommen, daß einige Primärkomponenten sich zu einem Primärideal zusammenfassen lassen, d. h. daß ihr Durchschnitt wieder primär ist. Wann das der Fall ist, ergibt sich aus folgenden Sätzen:

1. *Ein Durchschnitt von endlichvielen Primäridealen, die zum selben Primideal gehören, ist wieder primär und hat dasselbe zugehörige Primideal.*

2. *Ein unverkürzbarer Durchschnitt von endlichvielen Primäridealen, die nicht alle zum selben Primideal gehören, ist nicht primär.*

Diese Sätze gelten unabhängig vom Teilerkettensatz.

Beweis von 1: Es sei

$$\mathfrak{m} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_r],$$

wo $\mathfrak{q}_1, \ldots, \mathfrak{q}_r$ alle zu $\mathfrak{p}$ gehören. Wir stützen uns auf Satz III (§ 82). Aus

$$a\,b \equiv 0\,(\mathfrak{m}), \quad a \not\equiv 0\,(\mathfrak{m})$$

folgt

$$a\,b \equiv 0\,(\mathfrak{q}_\nu)$$

für alle ν und

$$a \not\equiv 0\,(\mathfrak{q}_\nu)$$

für mindestens ein ν, und daraus wieder $b \equiv 0\,(\mathfrak{p})$.

Zweitens ist offenbar

$$\mathfrak{m} \equiv 0\,(\mathfrak{q}_\nu) \equiv 0\,(\mathfrak{p}).$$

Ist schließlich $b \equiv 0\,(\mathfrak{p})$, so folgt

$$b^{\varrho_\nu} \equiv 0\,(\mathfrak{q}_\nu) \text{ für alle } \nu,$$

also, wenn $\varrho = \max \varrho_\nu$ gesetzt wird:

$$b^{\varrho} \equiv 0\,(\mathfrak{q}_\nu) \text{ für alle } \nu,$$

$$b^{\varrho} \equiv 0\,(\mathfrak{m}).$$

Damit sind alle drei in Satz III genannten Eigenschaften nachgewiesen. Also ist $\mathfrak{m}$ primär und $\mathfrak{p}$ das zugehörige Primideal.

Beweis von 2: Gegeben sei eine unverkürzbare Darstellung

$$\mathfrak{m} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_r] \qquad (r \geqq 2),$$

bei welcher mindestens zwei der zugehörigen Primideale $\mathfrak{p}_\nu$ verschieden sind. Wir denken uns von vornherein jede Gruppe von Primäridealen, die zum selben Primideal gehören, zu einem Primärideal zusammengefaßt. Die Darstellung bleibt dann unverkürzbar.

Unter den endlichvielen Primidealen $\mathfrak{p}_\nu$ gibt es ein minimales, d. h. ein solches, das keins der übrigen umfaßt. Dieses sei etwa $\mathfrak{p}_1$. Da $\mathfrak{p}_1$ die Ideale $\mathfrak{p}_2, \ldots, \mathfrak{p}_r$ nicht umfaßt, so gibt es Elemente a_ν so, daß

$$\left.\begin{aligned} a_\nu &\not\equiv 0\,(\mathfrak{p}_1), \\ a_\nu &\equiv 0\,(\mathfrak{p}_\nu) \end{aligned}\right\} \qquad (\nu = 2, 3, \ldots, r),$$

also für ein genügend hohes ϱ

$$a_\nu^{\varrho} \equiv 0\,(\mathfrak{q}_\nu).$$

Wäre $\mathfrak{q}_1 = \mathfrak{m}$, so wäre die Darstellung $\mathfrak{m} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_r]$ verkürzbar (nämlich $\mathfrak{q}_2, \ldots, \mathfrak{q}_r$ überflüssig). Also gibt es in $\mathfrak{q}_1$ ein Element q_1 mit

$$q_1 \not\equiv 0\,(\mathfrak{m}).$$

Das Produkt

$$q_1\,(a_2 \cdot \cdots a_r)^{\varrho}$$

liegt nun sowohl in $\mathfrak{q}_1$ als in $\mathfrak{q}_2, \ldots, \mathfrak{q}_r$, also in $\mathfrak{m}$. q_1 liegt aber nicht in $\mathfrak{m}$. Wäre $\mathfrak{m}$ primär, so würde daraus folgen:

$$(a_2 \cdot \cdots a_r)^{\varrho\,\sigma} \equiv 0\,(\mathfrak{m}),$$

$$(a_2 \cdot \cdots a_r)^{\varrho\,\sigma} \equiv 0\,(\mathfrak{p}_1),$$

also, da $\mathfrak{p}_1$ prim ist,

$$a_\nu \equiv 0 \,(\mathfrak{p}_1)$$

für mindestens ein ν, entgegen dem Früheren.

Wenn in einer unverkürzbaren Darstellung

$$\mathfrak{m} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_r]$$

alle zugehörigen Primideale $\mathfrak{p}_\nu$ verschieden sind, so daß sich auf keine Weise zwei oder mehr Ideale der Darstellung zu einem Primärideal zusammenfassen lassen, so nennt man die Darstellung eine *Darstellung durch größte Primärideale*. Diese größten Primärideale heißen auch *Primärkomponenten* von $\mathfrak{m}$.

Jede unverkürzbare Darstellung $\mathfrak{m} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_r]$ läßt sich durch Zusammenfassung der zum selben Primideal gehörigen Primärideale in eine Darstellung durch größte Primärideale verwandeln. Damit ist der *zweite Zerlegungssatz* bewiesen:

Jedes Ideal läßt eine unverkürzbare Darstellung als Durchschnitt von endlichvielen größten Primärkomponenten zu. Diese Primärkomponenten gehören zu lauter verschiedenen Primidealen.

Dieser „zweite Zerlegungssatz", für Polynombereiche von E. LASKER, allgemein von E. NOETHER bewiesen, ist das wichtigste Ergebnis der allgemeinen Idealtheorie. Anwendungen des Satzes werden wir vor allem im dreizehnten Kapitel kennenlernen. Wir wollen in den nächstfolgenden Paragraphen untersuchen, wie es mit der Eindeutigkeit der Primärkomponenten bestellt ist.

Aufgaben. 1. Man zerlege das Ideal $(9, 3x + 3)$ im ganzzahligen Polynombereich einer Unbestimmten in Primärkomponenten.

2. Zu jedem Ideal $\mathfrak{a}$ gibt es ein Produkt von Primidealpotenzen $\mathfrak{p}_1^{\varrho_1} \cdot \mathfrak{p}_2^{\varrho_2} \cdots \mathfrak{p}_h^{\varrho_h}$, welches durch $\mathfrak{a}$ teilbar ist, derart, daß jedes $\mathfrak{p}_\nu$ ein Teiler von $\mathfrak{a}$ ist.

3. Wenn der Ring $\mathfrak{o}$ ein Einselement besitzt, so ist jedes von $\mathfrak{o}$ verschiedene Ideal $\mathfrak{a}$ durch mindestens ein von $\mathfrak{o}$ verschiedenes Primideal teilbar.

4. Das Ideal $(4, 2x, x^2)$ im ganzzahligen Polynombereich einer Unbestimmten ist primär, aber reduzibel. [Zerlegung: $(4, 2x, x^2) = (4, x) \cap (2, x^2)$.]

§ 84. Die Eindeutigkeitssätze.

Die Zerlegung eines Ideals in größte Primärkomponenten ist nicht eindeutig.

Beispiel: Das Ideal

$$\mathfrak{m} = (x^2, xy)$$

im Polynombereich $\mathsf{K}[x, y]$ besteht aus allen Polynomen, die durch x teilbar sind und in denen außerdem die linearen Glieder fehlen. Die

Menge aller durch x teilbaren Polynome ist das Primideal

$$\mathfrak{q}_1 = (x);$$

die Menge aller Polynome, in denen die linearen und konstanten Glieder fehlen, ist das Primärideal

$$\mathfrak{q}_2 = (x^2, xy, y^2).$$

Es ist also

$$\mathfrak{m} = [\mathfrak{q}_1, \mathfrak{q}_2].$$

Das ist eine unverkürzbare Darstellung, und da die zugehörigen Primideale von $\mathfrak{q}_1$ und $\mathfrak{q}_2$ verschieden sind, nämlich gleich (x) bzw. (x, y), so ist es auch eine Darstellung durch größte Primärideale.

Aber neben dieser Darstellung gibt es noch die andere:

$$\mathfrak{m} = [\mathfrak{q}_1, \mathfrak{q}_3],$$

wo

$$\mathfrak{q}_3 = (x^2, y)$$

ist; denn damit ein Polynom in $\mathfrak{m}$ liegt, genügt es, zu fordern, daß das Polynom durch x teilbar ist und daß in ihm das Glied mit x fehlt. Von dieser Art gibt es sogar, wenn der Körper K unendlich ist, unendlich viele Darstellungen:

$$\mathfrak{m} = [\mathfrak{q}_1, \mathfrak{q}^{(\lambda)}], \qquad \mathfrak{q}^{(\lambda)} = (x^2, y + \lambda x).$$

Allen angeführten Zerlegungen von $\mathfrak{m}$ ist gemeinsam, daß die *Anzahl* der Primärkomponenten und die zugehörigen Primideale:

$$(x), (x, y),$$

übereinstimmen. Das gilt nun allgemein:

Erster Eindeutigkeitssatz: Bei zwei unverkürzbaren Darstellungen eines Ideals $\mathfrak{m}$ *durch größte Primärkomponenten stimmen die Anzahlen der Komponenten und (zwar nicht notwendig die Komponenten selbst, aber) die zugehörigen Primideale überein.*

Beweis: Für ein Primärideal ist die Behauptung trivial. Wir können also eine Induktion nach der Anzahl der Primärkomponenten ansetzen, die in mindestens einer Darstellung des betreffenden Ideals auftritt.

Es sei

$$\mathfrak{m} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_l] = [\mathfrak{q}'_1, \ldots, \mathfrak{q}'_{l'}]. \tag{1}$$

Aus allen zugehörigen Primidealen $\mathfrak{p}_1, \ldots, \mathfrak{p}_l, \mathfrak{p}'_1, \ldots, \mathfrak{p}'_{l'}$ wähle man ein maximales aus, d. h. ein solches, das von keinem anderen mehr umfaßt (geteilt) wird. Dieses komme etwa auf der linken Seite vor und sei $\mathfrak{p}_1$. Behauptung: Es kommt auch rechts vor. Denn sonst könnte man in (1) Quotienten nach $\mathfrak{q}_1$ bilden:

$$[\mathfrak{q}_1 : \mathfrak{q}_1, \ldots, \mathfrak{q}_l : \mathfrak{q}_1] = [\mathfrak{q}'_1 : \mathfrak{q}_1, \ldots, \mathfrak{q}'_{l'} : \mathfrak{q}_1].$$

Nun ist (für alle $\nu > 1$) $\mathfrak{q}_1 \not\equiv 0 (\mathfrak{p}_\nu)$, weil sonst $\mathfrak{p}_1 \equiv 0 (\mathfrak{p}_\nu)$ wäre, entgegen der vorausgesetzten Maximaleigenschaft von $\mathfrak{p}_1$. Ebenso folgt

für alle ν, daß $\mathfrak{q}_1 \not\equiv 0 (\mathfrak{p}'_\nu)$ ist. Nach Satz IV' (§ 82) ist also

$$\mathfrak{q}_\nu : \mathfrak{q}_1 = \mathfrak{q}_\nu \quad (\nu = 2, \ldots, l),$$
$$\mathfrak{q}'_\nu : \mathfrak{q}_1 = \mathfrak{q}'_\nu \quad (\nu = 1, \ldots, l').$$

Da weiter $\mathfrak{q}_1 : \mathfrak{q}_1 = \mathfrak{o}$ ist, so ergibt sich

$$[\mathfrak{o}, \mathfrak{q}_2, \ldots, \mathfrak{q}_l] = [\mathfrak{q}'_1, \ldots, \mathfrak{q}'_{l'}].$$

Rechts steht $\mathfrak{m}$; also muß auch links $\mathfrak{m}$ stehen. $\mathfrak{o}$ kann weggelassen werden; es ist also

$$\mathfrak{m} = [\mathfrak{q}_2, \ldots, \mathfrak{q}_l].$$

Demnach wäre die erste der beiden Darstellungen (1) verkürzbar, entgegen der Voraussetzung.

Jedes maximale Primideal kommt also auf *beiden* Seiten vor.

Es sei jetzt etwa $l \leqq l'$. Zu beweisen ist: $l = l'$ und (bei passender Anordnung) $\mathfrak{p}'_\nu = \mathfrak{p}_\nu$. Für Ideale, die sich durch weniger als l Primärideale darstellen lassen, sei alles bewiesen. Wir ordnen die $\mathfrak{q}$ und $\mathfrak{q}'$ so an, daß $\mathfrak{p}_1 = \mathfrak{p}'_1$ ein maximales zugehöriges Primideal (zu $\mathfrak{q}_1$ und zu $\mathfrak{q}'_1$ gehörig) ist.

Bildet man auf beiden Seiten von (1) Quotienten nach dem Produkt $\mathfrak{q}_1 \mathfrak{q}'_1$:

$$[\mathfrak{q}_1 : \mathfrak{q}_1 \mathfrak{q}'_1, \ldots, \mathfrak{q}_l : \mathfrak{q}_1 \mathfrak{q}'_1] = [\mathfrak{q}'_1 : \mathfrak{q}_1 \mathfrak{q}'_1, \ldots, \mathfrak{q}'_{l'} : \mathfrak{q}_1 \mathfrak{q}'_1],$$

so ergibt sich aus den gleichen Schlüssen wie vorhin:

$$\left.\begin{aligned} \mathfrak{q}_\nu : \mathfrak{q}_1 \mathfrak{q}'_1 &= \mathfrak{q}_\nu \\ \mathfrak{q}'_\nu : \mathfrak{q}_1 \mathfrak{q}'_1 &= \mathfrak{q}'_\nu \end{aligned}\right\} (\nu > 1).$$

Weiter ist, da $\mathfrak{q}_1 \mathfrak{q}'_1$ durch $\mathfrak{q}_1$ und durch $\mathfrak{q}'_1$ teilbar ist,

$$\mathfrak{q}_1 : \mathfrak{q}_1 \mathfrak{q}'_1 = \mathfrak{o},$$
$$\mathfrak{q}'_1 : \mathfrak{q}_1 \mathfrak{q}'_1 = \mathfrak{o};$$

also kommt:

$$[\mathfrak{q}_2, \ldots, \mathfrak{q}_l] = [\mathfrak{q}'_2, \ldots, \mathfrak{q}'_{l'}].$$

Nach Induktionsvoraussetzung muß, da jetzt links und rechts eine unverkürzbare Darstellung durch größte Primärkomponenten steht, $l' - 1 = l - 1$, also $l' = l$ sein. Weiter muß bei passender Anordnung $\mathfrak{p}_\nu = \mathfrak{p}'_\nu$ für alle $\nu > 1$ gelten. Da außerdem $\mathfrak{p}_1 = \mathfrak{p}'_1$ ist, so ist alles bewiesen.

Die nach dem eben bewiesenen Satz eindeutig bestimmten Ideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_l$, die bei einer unverkürzbaren Darstellung $\mathfrak{a} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_l]$ als zugehörige Primideale auftreten, heißen *die zugehörigen Primideale des Ideals* $\mathfrak{a}$. Ihre wichtigste Eigenschaft ist die folgende:

Wenn ein Ideal $\mathfrak{a}$ *durch kein zugehöriges Primideal eines Ideals* $\mathfrak{b}$ *teilbar ist, so ist* $\mathfrak{b} : \mathfrak{a} = \mathfrak{b}$ *und umgekehrt.*

Beweis: Es sei $\mathfrak{b} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_l]$ eine unverkürzbare Darstellung. Zunächst sei $\mathfrak{a} \not\equiv 0 \,(\mathfrak{p}_i)$ für $i = 1, \ldots, l$, wo $\mathfrak{p}_i$ zu $\mathfrak{q}_i$ gehört. Daraus folgt

$$\begin{aligned} \mathfrak{q}_i : \mathfrak{a} &= \mathfrak{q}_i\,, \\ \mathfrak{b} : \mathfrak{a} &= [\mathfrak{q}_1, \ldots, \mathfrak{q}_l] : \mathfrak{a} \\ &= [\mathfrak{q}_1 : \mathfrak{a}, \ldots, \mathfrak{q}_l : \mathfrak{a}] \\ &= [\mathfrak{q}_1, \ldots, \mathfrak{q}_l] = \mathfrak{b}\,. \end{aligned}$$

Umgekehrt sei $\mathfrak{b} : \mathfrak{a} = \mathfrak{b}$. Wäre $\mathfrak{a} \equiv 0 \,(\mathfrak{p}_i)$ für ein i, etwa $\mathfrak{a} \equiv 0 \,(\mathfrak{p}_1)$, so würde folgen $\mathfrak{a}^\varrho \equiv 0 \,(\mathfrak{q}_1)$, mithin

$$\mathfrak{a}^\varrho \cdot [\mathfrak{q}_2, \ldots, \mathfrak{q}_l] \equiv 0 \,([\mathfrak{q}_1, \mathfrak{q}_2, \ldots, \mathfrak{q}_l]) \equiv 0 \,(\mathfrak{b})\,,$$

mithin, da man in jeder Kongruenz (mod $\mathfrak{b}$) durch $\mathfrak{a}$ und somit auch durch $\mathfrak{a}^\varrho$ kürzen darf,

$$[\mathfrak{q}_2, \ldots, \mathfrak{q}_l] \equiv 0 \,(\mathfrak{b})\,,$$

entgegen der Unverkürzbarkeit der Darstellung.

Ein wichtiger Spezialfall entsteht, wenn man $\mathfrak{a}$ zu einem Hauptideal (a) spezialisiert:

Wenn ein Element a durch kein zugehöriges Primideal eines Ideals $\mathfrak{b}$ teilbar ist, so ist $\mathfrak{b} : a = \mathfrak{b}$; d. h. aus $ac \equiv 0 \,(\mathfrak{b})$ folgt stets $c \equiv 0 \,(\mathfrak{b})$.

Man kann den allgemeinen Satz noch anders fassen, indem man auch $\mathfrak{a}$ als Durchschnitt von Primäridealen $[\mathfrak{q}'_1, \ldots, \mathfrak{q}'_{l'}]$ darstellt. $\mathfrak{a}$ ist dann und nur dann durch $\mathfrak{p}_i$ teilbar, wenn ein $\mathfrak{q}'_j$ es ist[1] oder, was dasselbe ist, wenn ein $\mathfrak{p}'_j$ es ist. Also folgt:

Wenn kein zugehöriges Primideal von $\mathfrak{a}$ durch ein zugehöriges Primideal von $\mathfrak{b}$ teilbar ist, so ist $\mathfrak{b} : \mathfrak{a} = \mathfrak{b}$, und umgekehrt.

In dieser Fassung wird der Satz gebraucht, um den zweiten Eindeutigkeitssatz, die Eindeutigkeit der „isolierten Komponentenideale", zu beweisen.

Unter einem *Komponentenideal* eines Ideals $\mathfrak{a}$ wird jeder Durchschnitt von Primäridealen verstanden, die in irgend einer unverkürzbaren Darstellung des Ideals $\mathfrak{a}$ durch größte Primärideale auftreten.

Es sei also

$$\mathfrak{a} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_l]$$

eine unverkürzbare Darstellung und

$$\begin{aligned} \mathfrak{a}_1 &= [\mathfrak{q}_1, \ldots, \mathfrak{q}_k], \quad \text{bzw.} = \mathfrak{o}, \text{ falls } k = 0\,, \\ \mathfrak{a}_2 &= [\mathfrak{q}_{k+1}, \ldots, \mathfrak{q}_l], \quad \text{bzw.} = \mathfrak{o}, \text{ falls } k = l\,. \end{aligned}$$

Dann ist

$$\mathfrak{a} = \mathfrak{a}_1 \cap \mathfrak{a}_2\,,$$

und $\mathfrak{a}_1$ ist ein Komponentenideal von $\mathfrak{a}$.

---

[1] Denn daß mit $\mathfrak{q}'_j$ auch $\mathfrak{a}$ durch $\mathfrak{p}_i$ teilbar ist, ist klar, und aus $\mathfrak{a} \equiv 0 \,(\mathfrak{p}_i)$ folgt $\mathfrak{q}'_1 \cdots \mathfrak{q}'_{l'} \equiv 0 \,([\mathfrak{q}'_1, \ldots, \mathfrak{q}'_{l'}]) \equiv 0 \,(\mathfrak{p}_i)$, so daß ein $\mathfrak{q}'_j$ durch $\mathfrak{p}_i$ teilbar ist.

Das Komponentenideal $\mathfrak{a}_1$ heißt *isoliert*, wenn kein zu $\mathfrak{a}_2$ gehöriges Primideal $\mathfrak{p}_{k+j}$ durch ein zu $\mathfrak{a}_1$ gehöriges $\mathfrak{p}_i$ teilbar ist.

Nennt man ein zugehöriges Primideal von $\mathfrak{a}$ *eingebettet*, wenn es ein Teiler eines anderen zugehörigen Primideals von $\mathfrak{a}$ ist, so kann man ein isoliertes Komponentenideal von $\mathfrak{a}$ auch definieren als ein solches, dessen Menge von zugehörigen Primidealen entweder überhaupt keine eingebetteten Primideale enthält, oder wenigstens zu jedem eingebetteten Primideal auch alle die Primideale enthält, in denen es eingebettet ist.

Zweiter Eindeutigkeitssatz: Jedes isolierte Komponentenideal eines Ideals $\mathfrak{a}$ ist durch Angabe der zugehörigen Primideale (also einer Teilmenge aller zu $\mathfrak{a}$ gehörigen Primideale) eindeutig bestimmt.

Beweis: Gegeben seien zwei Darstellungen

$$\mathfrak{a} = \mathfrak{a}_1 \cap \mathfrak{a}_2 = \mathfrak{a}_1' \cap \mathfrak{a}_2', \tag{2}$$

wobei $\mathfrak{a}_1'$ dieselben zugehörigen Primideale hat wie $\mathfrak{a}_1$. Außerdem seien $\mathfrak{a}_1$ und $\mathfrak{a}_1'$ isolierte Komponenten. Dann folgt aus dem eben bewiesenen Satz:

$$\mathfrak{a}_1 : \mathfrak{a}_2 = \mathfrak{a}_1,$$
$$\mathfrak{a}_1' : \mathfrak{a}_2 = \mathfrak{a}_1',$$

also aus (2) durch Quotientenbildung nach $\mathfrak{a}_2$:

$$\mathfrak{a} : \mathfrak{a}_2 = \mathfrak{a}_1 = \mathfrak{a}_1' \cap (\mathfrak{a}_2' : \mathfrak{a}_2),$$
$$\mathfrak{a}_1 \subseteq \mathfrak{a}_1'.$$

Ebenso folgt

$$\mathfrak{a}_1' \subseteq \mathfrak{a}_1,$$

also

$$\mathfrak{a}_1 = \mathfrak{a}_1', \qquad \text{q. e. d.}$$

Insbesondere sind die *isolierten Primärkomponenten* (d. h. also die zu nicht-eingebetteten Primidealen gehörigen Primärkomponenten) eines Ideals eindeutig bestimmt.

§ 85. Theorie der teilerfremden Ideale.

Im folgenden wird die Existenz des Einselements im Ring $\mathfrak{o}$ vorausgesetzt. Dieses Einselement erzeugt dann das Einheitsideal $\mathfrak{o}$:

$$\mathfrak{o} = (1).^1$$

Zwei Ideale $\mathfrak{a}, \mathfrak{b}$ heißen *teilerfremd*, wenn sie keinen gemeinsamen Teiler außer $\mathfrak{o}$ haben oder wenn ihr größter gemeinsamer Teiler $\mathfrak{o}$ ist:

$$(\mathfrak{a}, \mathfrak{b}) = \mathfrak{o}.$$

---

[1] Aus dieser Darstellung folgt

$$\mathfrak{o}^2 = (1) \cdot (1) = (1),$$

also $\mathfrak{o}^2 = \mathfrak{o}$, was in Ringen ohne Einselement nicht zu gelten braucht.

Das bedeutet, daß jedes Element von $\mathfrak{o}$ sich als Summe eines Elements von $\mathfrak{a}$ und eines von $\mathfrak{b}$ darstellen läßt.

Notwendig und hinreichend dafür ist, daß die Eins (das erzeugende Element von $\mathfrak{o}$) sich als Summe

$$1 = a + b \tag{1}$$

(a in $\mathfrak{a}$, b in $\mathfrak{b}$) darstellen läßt. Man hat dann:

$$\begin{cases} a \equiv 1\,(\mathfrak{b}), & b \equiv 0\,(\mathfrak{b}), \\ a \equiv 0\,(\mathfrak{a}), & b \equiv 1\,(\mathfrak{a}). \end{cases} \tag{2}$$

Wenn zwei Primärideale $\mathfrak{q}_1, \mathfrak{q}_2$ teilerfremd sind, so sind die zugehörigen Primideale $\mathfrak{p}_1, \mathfrak{p}_2$ es um so mehr (jeder gemeinsame Teiler von $\mathfrak{p}_1$ und $\mathfrak{p}_2$ ist ja auch ein gemeinsamer Teiler von $\mathfrak{q}_1$ und $\mathfrak{q}_2$). Aber auch die Umkehrung gilt: *Aus der Teilerfremdheit von* $\mathfrak{p}_1, \mathfrak{p}_2$ *folgt die von* $\mathfrak{q}_1, \mathfrak{q}_2$. Denn aus

$$1 = p_1 + p_2$$

folgt durch Erhebung in die $(\varrho + \sigma - 1)$-te Potenz:

$$1 = p_1^{\varrho+\sigma-1} + \cdots + p_2^{\varrho+\sigma-1};$$

wählt man nun ϱ und σ so groß, daß p_1^ϱ in $\mathfrak{q}_1$ und p_2^σ in $\mathfrak{q}_2$ liegt, so liegt von der Summe rechts jedes Glied in $\mathfrak{q}_1$ oder in $\mathfrak{q}_2$, und es folgt

$$1 = q_1 + q_2.$$

Wenn zwei Ideale teilerfremd sind, so sind sie in beiden Richtungen relativ-prim.

Beweis: Es sei $(\mathfrak{a}, \mathfrak{b}) = \mathfrak{o}$, also etwa $a + b = 1$. Es genügt, zu zeigen, daß $\mathfrak{a}:\mathfrak{b} \subseteq \mathfrak{a}$ ist. Wenn x zu $\mathfrak{a}:\mathfrak{b}$ gehört, so ist $x\mathfrak{b} \subseteq \mathfrak{a}$, also $xb \equiv 0\,(\mathfrak{a})$, also auch

$$\begin{aligned} x(a + b) &\equiv 0\,(\mathfrak{a}), \\ x \cdot 1 &\equiv 0\,(\mathfrak{a}); \end{aligned}$$

demnach gehört x zu $\mathfrak{a}$, q. e. d.

Die Umkehrung gilt nicht; Beispiel im Polynombereich $\mathsf{K}[x, y]$: die Ideale (x) und (y) sind gegenseitig relativ-prim, aber nicht teilerfremd:

$$\begin{aligned} &(x, y) \neq \mathfrak{o}, \\ &\begin{cases} (x):(y) = (x), \\ (y):(x) = (y). \end{cases} \end{aligned}$$

Wenn $\mathfrak{a}$ und $\mathfrak{b}$ teilerfremd sind, so kann man wie in der Zahlentheorie Kongruenzen simultan lösen. Es seien zwei Kongruenzen

$$\begin{aligned} f(\xi) &\equiv 0\,(\mathfrak{a}), \\ g(\xi) &\equiv 0\,(\mathfrak{b}) \qquad\qquad (f(x), g(x) \in \mathfrak{o}[x]) \end{aligned}$$

vorgelegt. Angenommen werde, jede einzelne Kongruenz sei lösbar. Ist etwa $\xi \equiv \alpha$ eine Lösung der ersten, $\xi \equiv \beta$ eine Lösung der zweiten

Kongruenz, so verschafft man sich ein Element ξ, welches beide Kongruenzen löst, in der folgenden Weise: Mit Hilfe der früher konstruierten Größen a und b, die den Gleichungen (1) und (2) genügen, bilde man

$$\xi = b\alpha + a\beta .$$

Dann ist $\xi \equiv \alpha(\mathfrak{a})$ und $\xi \equiv \beta(\mathfrak{b})$, also ξ eine Lösung der beiden vorgelegten Kongruenzen.

Für zwei teilerfremde Ideale ist das kleinste gemeinsame Vielfache gleich dem Produkt.

Beweis: In § 81 wurde bewiesen:

$$\mathfrak{a}\mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b} ,$$

$$[\mathfrak{a} \cap \mathfrak{b}] \cdot (\mathfrak{a}, \mathfrak{b}) \subseteq \mathfrak{a}\mathfrak{b} .$$

Ist nun $(\mathfrak{a}, \mathfrak{b}) = \mathfrak{o}$ und ein Einselement vorhanden, so vereinfacht sich die zweite Gleichung zu

$$\mathfrak{a} \cap \mathfrak{b} \subseteq \mathfrak{a}\mathfrak{b} ;$$

also folgt

$$\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a}\mathfrak{b} , \qquad \text{q. e. d.}$$

Um diesen Satz auch für mehr als zwei paarweise teilerfremde Ideale aussprechen zu können, müssen wir einen Hilfssatz vorausschicken:

Wenn $\mathfrak{a}$ *zu* $\mathfrak{b}$ *und zu* $\mathfrak{c}$ *teilerfremd ist, so ist* $\mathfrak{a}$ *auch zum Produkt* $\mathfrak{b}\mathfrak{c}$ *und zum Durchschnitt* $\mathfrak{b} \cap \mathfrak{c}$ *teilerfremd.*

Beweis: Aus

$$a + b = 1 ,$$

$$a' + c = 1$$

folgt:

$$(a + b)(a' + c) = 1 ,$$

$$a a' + a c + a' b + b c = 1 ,$$

$$a'' + b c = 1 ,$$

wo $a'' = a a' + a c + a' b$ wieder ein Element von $\mathfrak{a}$ ist. Hieraus folgt

$$(\mathfrak{a}, \mathfrak{b}\mathfrak{c}) = \mathfrak{o}$$

und um so mehr

$$(\mathfrak{a}, \mathfrak{b} \cap \mathfrak{c}) = \mathfrak{o} .$$

Damit sind beide Behauptungen bewiesen.

Sind nun $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_n$ paarweise teilerfremd und ist

$$[\mathfrak{a}_1, \ldots, \mathfrak{a}_{n-1}] = \mathfrak{a}_1 \cdot \cdots \mathfrak{a}_{n-1}$$

schon bewiesen, so hat man:

$$\begin{aligned} [\mathfrak{a}_1, \ldots, \mathfrak{a}_n] &= [\mathfrak{a}_1, \ldots, \mathfrak{a}_{n-1}] \cap \mathfrak{a}_n \\ &= (\mathfrak{a}_1 \cdot \cdots \mathfrak{a}_{n-1}) \cap \mathfrak{a}_n \\ &= \mathfrak{a}_1 \cdot \cdots \mathfrak{a}_{n-1} \cdot \mathfrak{a}_n , \end{aligned}$$

also durch Induktion den Satz:

Das kleinste gemeinsame Vielfache endlichvieler paarweise teilerfremder Ideale ist gleich ihrem Produkt.

Die frühere Bemerkung über die Lösung von Kongruenzen nach teilerfremden Idealen gilt auch für mehrere paarweise teilerfremde Ideale:

Es ist immer möglich, ξ aus den Kongruenzen

$$\xi \equiv \alpha_i \,(\mathfrak{a}_i) \qquad (i = 1, 2, \ldots, r)$$

zu bestimmen, falls $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_r$ paarweise teilerfremde Ideale sind.

Beweis durch Induktion: Man habe η schon so bestimmt, daß

$$\eta \equiv \alpha_i \,(\mathfrak{a}_i) \qquad (i = 1, 2, \ldots, r-1)$$

ist, und bestimme ξ aus

$$\begin{cases} \xi \equiv \eta \,([\mathfrak{a}_1, \ldots, \mathfrak{a}_{r-1}]), \\ \xi \equiv \alpha_r \,(\mathfrak{a}_r), \end{cases}$$

was immer möglich ist, weil $\mathfrak{a}_r$ zu $[\mathfrak{a}_1, \ldots, \mathfrak{a}_{r-1}]$ teilerfremd ist.

Gilt in $\mathfrak{o}$ der Teilerkettensatz, so kann man jedes Ideal als Durchschnitt von paarweise teilerfremden Idealen darstellen, die selbst nicht mehr als Durchschnitt von paarweise teilerfremden echten Teilern darstellbar sind.

Zu dem Zweck suche man in einer unverkürzbaren Darstellung des gegebenen Ideals $\mathfrak{a}$ durch Primärideale

$$\mathfrak{a} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_r]$$

alle die Primärideale, die mit irgend einem festen unter ihnen durch eine Kette von paarweise nicht teilerfremden Primäridealen verbunden sind, und bilde deren Durchschnitt $\mathfrak{a}_1$. Aus den verbleibenden Idealen bilde man in derselben Weise sukzessive die Ideale $\mathfrak{a}_2, \ldots, \mathfrak{a}_s$. Die Darstellung

$$\mathfrak{a} = [\mathfrak{a}_1, \ldots, \mathfrak{a}_s] \tag{3}$$

hat die gewünschten Eigenschaften. Denn erstens sind $\mathfrak{a}_i$ und $\mathfrak{a}_k$ für $i \neq k$ in der Tat teilerfremd, da die Komponenten von $\mathfrak{a}_i$ zu denen von $\mathfrak{a}_k$ teilerfremd sind. Zweitens ist es unmöglich, etwa $\mathfrak{a}_1$ noch als Durchschnitt zweier paarweise teilerfremden echten Teiler darzustellen. Wäre nämlich eine solche Darstellung gegeben:

$$\mathfrak{a}_1 = \mathfrak{b} \cap \mathfrak{c} = \mathfrak{b}\mathfrak{c},$$
$$(\mathfrak{b}, \mathfrak{c}) = \mathfrak{o},$$

so müßte jedes zu $\mathfrak{a}_1$ gehörige Primideal ein Teiler von $\mathfrak{b}\mathfrak{c}$, also von $\mathfrak{b}$ oder von $\mathfrak{c}$ sein; da nun alle diese Primideale mit einem unter ihnen durch eine Kette von paarweise nicht teilerfremden Primidealen verbunden sind, so müssen, wenn eins dieser Primideale etwa $\mathfrak{b}$ teilt, alle diese Primideale $\mathfrak{b}$ teilen und keines $\mathfrak{c}$. Die zugehörigen Primärkompo-

nenten teilen $\mathfrak{b}\mathfrak{c}$; also teilen sie $\mathfrak{b}$ (da ihre Primideale $\mathfrak{c}$ nicht teilen). Daraus folgt, daß auch der Durchschnitt $\mathfrak{a}_1$ ein Teiler von $\mathfrak{b}$ ist:

$$\mathfrak{b} \leqq \mathfrak{a}_1;$$

entgegen der Voraussetzung, daß $\mathfrak{b}$ ein echter Teiler von $\mathfrak{a}_1$ sein sollte.

Statt der Darstellung (3) kann man nach unseren Sätzen eine Produktdarstellung schreiben:

$$\mathfrak{a} = \mathfrak{a}_1 \mathfrak{a}_2 \cdots \mathfrak{a}_s.$$

Aufgaben. 1. Man beweise den *„dritten Eindeutigkeitssatz"*, der die eindeutige Bestimmtheit der Ideale $\mathfrak{a}_1, \ldots, \mathfrak{a}_s$, welche in einer Darstellung (3) mit den angegebenen Eigenschaften auftreten, aussagt. [Man führe diesen dritten Eindeutigkeitssatz auf den zweiten zurück.]

Mit der multiplikativen Zerlegung des Ideals $\mathfrak{a}$ geht eine additive Zerlegung des Ringes $\mathfrak{o}$ und des Restklassenringes $\mathfrak{o}/\mathfrak{a}$ einher. Wir beweisen zunächst:

Sind $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ *paarweise teilerfremde Ideale und ist*

$$\mathfrak{a} = \mathfrak{a}_1 \cdots \mathfrak{a}_r = [\mathfrak{a}_1, \ldots, \mathfrak{a}_r],$$

$$\mathfrak{b}_\nu = \mathfrak{a}_1 \cdots \mathfrak{a}_{\nu-1}\, \mathfrak{a}_{\nu+1} \cdots \mathfrak{a}_r = [\mathfrak{a}_1, \ldots, \mathfrak{a}_{\nu-1}, \mathfrak{a}_{\nu+1}, \ldots, \mathfrak{a}_r],$$

so ist

$$\mathfrak{o} = (\mathfrak{b}_1, \ldots, \mathfrak{b}_r),$$

und zwar ist die additive Darstellung eines jeden Elements von $\mathfrak{o}$ *als Summe von Elementen von* $\mathfrak{b}_1, \ldots, \mathfrak{b}_r$ *eindeutig modulo* $\mathfrak{a}$.

Beweis. Aus den Definitionen von $\mathfrak{a}$ und $\mathfrak{b}_\nu$ folgt $\mathfrak{a} = \mathfrak{a}_\nu \cap \mathfrak{b}_\nu = \mathfrak{a}_\nu \cdot \mathfrak{b}_\nu$.

Es sei nun b ein beliebiges Element von $\mathfrak{o}$. Wir bestimmen $b_1, \ldots, b_{r-1}$ aus den Kongruenzen

$$b_\nu \equiv b \ (\mathfrak{a}_\nu); \qquad b_\nu \equiv 0 \ (\mathfrak{b}_\nu).$$

Dann ist für $\nu = 1, 2, \ldots, r-1$:

$$b \equiv \sum_1^{r-1} b_\lambda \ (\mathfrak{a}_\nu).$$

Setzen wir also $b - \sum_1^{r-1} b_\lambda = b_r$, so wird $b_r \equiv 0 \ (\mathfrak{a}_\nu)$ für $\nu = 1, 2, \ldots, r-1$, mithin $b_r \equiv 0 \ (\mathfrak{b}_r)$. Damit ist die behauptete Darstellung

$$b = \sum_1^r b_\nu$$

gefunden. — Sind nun zwei solche Darstellungen

$$b = \sum_1^r b_\nu = \sum_1^r b'_\nu$$

gegeben, so folgt, da modulo $\mathfrak{a}_\mu$ alle $\mathfrak{b}_\nu$ mit $\nu \neq \mu$ kongruent Null sind:

$$b_\mu \equiv b'_\mu \ (\mathfrak{a}_\mu).$$

Die Differenz $b_\mu - b'_\mu$ gehört also zu $\mathfrak{a}_\mu$ und zu $\mathfrak{b}_\mu$, mithin zu $\mathfrak{a} = \mathfrak{a}_\mu \cap \mathfrak{b}_\mu$. Also ist $b_\mu \equiv b'_\mu \ (\mathfrak{a})$, womit alles bewiesen ist.

Gehen wir nun zum Restklassenring $\bar{\mathfrak{o}} = \mathfrak{o}/\mathfrak{a}$ über, indem wir alle Elemente b durch die zugehörigen Restklassen $\bar{b}$ ersetzen und ebenso $\bar{\mathfrak{b}}_\nu = \mathfrak{b}_\nu/\mathfrak{a}$, $\bar{\mathfrak{a}}_\nu = \mathfrak{a}_\nu/\mathfrak{a}$ setzen, so folgt eine eindeutige Darstellung aller Elemente $\bar{b}$ von $\bar{\mathfrak{o}}$ in der Form

$$\bar{b} = \bar{b}_1 + \bar{b}_2 + \cdots + \bar{b}_r; \qquad \bar{b}_\nu \in \bar{\mathfrak{b}}_\nu. \tag{4}$$

Da die Darstellung eindeutig ist, so ist die Summe $\bar{\mathfrak{o}} = (\bar{\mathfrak{b}}_1, \ldots, \bar{\mathfrak{b}}_r)$ *direkt* im Sinne von § 42. Weiter folgt $\bar{\mathfrak{a}}_\nu \cdot \bar{\mathfrak{b}}_\nu = (0)$, mithin, da jedes $\bar{\mathfrak{b}}_\mu$ $(\mu \neq \nu)$ eine Untermenge von $\bar{\mathfrak{a}}_\nu$ ist,

$$\bar{\mathfrak{b}}_\mu \cdot \bar{\mathfrak{b}}_\nu = 0 .$$

Der Ring $\bar{\mathfrak{o}} = \mathfrak{o}/\mathfrak{a}$ erscheint also als direkte Summe von Ringen $\bar{\mathfrak{b}}_1, \ldots, \bar{\mathfrak{b}}_r$, die sich gegenseitig annullieren.

Jedem b von $\mathfrak{o}$ ist ein $\bar{b}$ zugeordnet und jedem $\bar{b}$ wieder ein $\bar{b}_1$. Beide Zuordnungen sind Ringhomomorphismen; also ist auch die Zuordnung $b \to \bar{b}_1$ ein Ringhomomorphismus. Ist $\bar{b}_1 = 0$, so muß $\bar{b} \in \bar{\mathfrak{a}}_1$ und daher $b \in \mathfrak{a}_1$ sein, und umgekehrt. Daraus folgt nach dem Homomorphiesatz:

$$\bar{\mathfrak{b}}_1 \cong \mathfrak{o}/\mathfrak{a}_1 .$$

Ebenso gilt natürlich für jedes ν: $\bar{\mathfrak{b}}_\nu \cong \mathfrak{o}/\mathfrak{a}_\nu$.

Aufgaben. 2. Wendet man die Zerlegung (4) auf das Einselement 1 von $\bar{\mathfrak{o}}$ an, so findet man:

$$1 = \bar{e}_1 + \bar{e}_2 + \cdots + \bar{e}_r; \qquad \bar{e}_\nu^2 = \bar{e}_\nu; \qquad \bar{e}_\mu \bar{e}_\nu = 0 \text{ für } \mu \neq \nu .$$

Die $\bar{e}_\nu$ sind die Einselemente der Ringe $\bar{\mathfrak{b}}_\nu$.

§ 86. Einartige Ideale.

Es sei wieder $\mathfrak{o}$ ein Ring mit Einselement.

Das Einheitsideal $\mathfrak{o}$ ist stets Primideal. Welche Primärideale können zu ihm gehören? Die Antwort lautet: Nur $\mathfrak{o}$ selbst; denn wenn $\mathfrak{q}$ ein zu $\mathfrak{o}$ gehöriges Primärideal ist, so ist $1 \in \mathfrak{o}$, also $1^e \in \mathfrak{q}$, mithin $\mathfrak{q} = \mathfrak{o}$.

Wenn nun bei der Darstellung eines Ideals $\mathfrak{a} \neq \mathfrak{o}$ als Durchschnitt von Primäridealen $[\mathfrak{q}_1, \ldots, \mathfrak{q}_r]$ unter den zugehörigen Primidealen $\mathfrak{p}_i$ das Einheitsideal vorkommt, so ist das zugehörige $\mathfrak{q}_i$ ebenfalls gleich $\mathfrak{o}$ und daher in der Durchschnittsdarstellung überflüssig. Mithin: *Ist die Darstellung $\mathfrak{a} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_r]$ unverkürzbar und $\mathfrak{a} \neq \mathfrak{o}$, so kommt das Einheitsideal nicht unter den zugehörigen Primidealen vor.*

Daraus folgt sofort, wenn in $\mathfrak{o}$ der Teilerkettensatz gilt und daher jedes Ideal $\mathfrak{a}$ als Durchschnitt von Primäridealen darstellbar ist:

Jedes Ideal $\mathfrak{a} \neq \mathfrak{o}$ besitzt mindestens einen Primidealteiler $\mathfrak{p} \neq \mathfrak{o}$. Ist das Ideal $\mathfrak{a}$ nicht primär, so besitzt es sogar mindestens zwei Primidealteiler $\neq \mathfrak{o}$.

Ein Ideal, das nicht mehr als einen Primidealteiler außer $\mathfrak{o}$ besitzt, heißt nach DEDEKIND *einartig*. Nach dem vorigen Satz ist jedes einartige Ideal $\mathfrak{q}$ primär. Außerdem muß das zugehörige Primideal $\mathfrak{p}$ teilerlos sein, denn wäre $\mathfrak{a}' \neq \mathfrak{o}$ ein echter Teiler von $\mathfrak{p}$, so hätte $\mathfrak{a}'$ wieder einen Primteiler $\mathfrak{p}' \neq \mathfrak{o}$, der echter Teiler von $\mathfrak{p}$ wäre, also hätte $\mathfrak{q}$ zwei voneinander und von $\mathfrak{o}$ verschiedene Primidealteiler $\mathfrak{p}$ und $\mathfrak{p}'$, entgegen der vorausgesetzten Einartigkeit von $\mathfrak{q}$.

Es gilt

$$\mathfrak{p}^e \equiv 0 \,(\mathfrak{q}) . \tag{1}$$

Aus der Relation (1) folgt, wenn $\mathfrak{p}$ teilerlos ist, auch umgekehrt die Einartigkeit von $\mathfrak{q}$. Denn wenn $\mathfrak{p}'$ ein beliebiger Primidealteiler von $\mathfrak{q}$

ist, so folgt aus (1):

$$\mathfrak{p}^{\varrho} \equiv 0\,(\mathfrak{p}'),$$

mithin

$$\mathfrak{p} \equiv 0\,(\mathfrak{p}'),$$

also entweder $\mathfrak{p}' = \mathfrak{p}$ oder $\mathfrak{p}' = \mathfrak{o}$; mithin hat $\mathfrak{q}$ keine anderen Primidealteiler als $\mathfrak{p}$ und $\mathfrak{o}$.

Die Begriffe:

1. einartiges Ideal,
2. Primärideal zu einem teilerlosen Primideal $\mathfrak{p}$,
3. Teiler einer Potenz $\mathfrak{p}^{\varrho}$ eines teilerlosen Primideals $\mathfrak{p}$,

sind also gleichbedeutend. Weiter gilt:

Wenn das Ideal $\mathfrak{m}$ *eine isolierte einartige Primärkomponente* $\mathfrak{q}$ *besitzt, deren zugehöriges Primideal* $\mathfrak{p}$ *und deren Exponent* ϱ *ist, so ist für jede ganze Zahl* $\sigma \geqq \varrho$:

(2) $$\mathfrak{q} = (\mathfrak{m}, \mathfrak{p}^{\sigma}).$$

Beweis: Aus

$$\mathfrak{m} \equiv 0\,(\mathfrak{q})$$

und

$$\mathfrak{p}^{\sigma} \equiv 0\,(\mathfrak{q})$$

schließt man

(3) $$(\mathfrak{m}, \mathfrak{p}^{\sigma}) \equiv 0\,(\mathfrak{q}).$$

Andererseits sei

$$\mathfrak{m} = [\mathfrak{q}, \mathfrak{q}_2, \ldots, \mathfrak{q}_s]$$

eine Darstellung von $\mathfrak{m}$ durch Primärkomponenten. Das Ideal $(\mathfrak{m}, \mathfrak{p}^{\sigma})$ ist einartig, also primär; das zugehörige Primideal ist $\mathfrak{p}$. Das Produkt $\mathfrak{q}\mathfrak{q}_2 \cdots \mathfrak{q}_s$ ist durch $(\mathfrak{m}, \mathfrak{p}^{\sigma})$ teilbar; aber $\mathfrak{q}_2 \cdots \mathfrak{q}_s$ ist, da $\mathfrak{q}$ als *isoliert* angenommen war, nicht durch $\mathfrak{p}$ teilbar; also muß $\mathfrak{q}$ durch $(\mathfrak{m}, \mathfrak{p}^{\sigma})$ teilbar sein:

(4) $$\mathfrak{q} \equiv 0\,(\mathfrak{m}, \mathfrak{p}^{\sigma}).$$

Aus (3) und (4) folgt (2).

Folgerung: Für $\sigma \geqq \varrho$ ist

$$\mathfrak{p}^{\sigma} \equiv 0\,(\mathfrak{q}) \equiv 0\,(\mathfrak{m}, \mathfrak{p}^{\sigma+1}).$$

also

(5) $$\mathfrak{p}^{\sigma} \equiv 0\,(\mathfrak{m}, \mathfrak{p}^{\sigma+1}).$$

Für $\sigma < \varrho$ gilt die Relation (5) nicht mehr. Denn wäre

$$\mathfrak{p}^{\sigma} \equiv 0\,(\mathfrak{m}, \mathfrak{p}^{\sigma+1})$$

für ein $\sigma < \varrho$, so würde man durch Multiplikation mit $\mathfrak{p}^{\varrho-\sigma-1}$ erhalten:

$$\mathfrak{p}^{\varrho-1} \equiv 0\,(\mathfrak{m}\,\mathfrak{p}^{\varrho-\sigma-1}, \mathfrak{p}^{\varrho}) \equiv 0\,(\mathfrak{m}, \mathfrak{q}) \equiv 0\,(\mathfrak{q})$$

entgegen der Definition des Exponenten ϱ.

Der Exponent ϱ *von* $\mathfrak{q}$ *ist also die kleinste Zahl* σ, *für die* (5) *gilt.*

Es gibt Integritätsbereiche $\mathfrak{o}$ mit Einselement, in denen (der Teilerkettensatz gilt und) jedes vom Nullideal verschiedene Primideal teilerlos

ist. Z. B. gehören dazu die Hauptidealringe (vgl. § 17), ebenso gewisse später zu definierende „Ordnungen" in Zahl- und Funktionenkörpern, für die der Ring $C[\sqrt{-3}]$ ein typisches Beispiel ist. In diesen Ringen sind nun ersichtlich *alle Primärideale außer dem Nullideal einartig.* Weiter sind hier je zwei untereinander und von (0) verschiedene Primideale auch teilerfremd. Daraus folgt, daß je zwei zu verschiedenen Primidealen $\neq (0)$ gehörige Primärideale auch teilerfremd sind. Schließlich sind alle Primärkomponenten eines Ideals isoliert und somit eindeutig bestimmt. Mithin: *Jedes vom Nullideal verschiedene Ideal läßt sich eindeutig als Durchschnitt von teilerfremden einartigen Primäridealen darstellen.* Nach § 85 ist dieser Durchschnitt zugleich Produkt:

$$\mathfrak{a} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_r] = \mathfrak{q}_1 \cdot \mathfrak{q}_2 \cdots \mathfrak{q}_r .$$

Nach den Sätzen von § 85, Schluß, ist der Restklassenring $\mathfrak{o}/\mathfrak{a}$ eine direkte Summe von Ringen, die sich gegenseitig annullieren und isomorph den Restklassenringen $\mathfrak{o}/\mathfrak{q}_\nu$ sind. Die letzteren Restklassenringe sind *primär*, d. h. in ihnen ist jeder Nullteiler nilpotent.

In Hauptidealringen sind die Primärideale $\mathfrak{q}_i$ zugleich Primidealpotenzen. Ob das in allgemeineren Ringen auch der Fall ist, hängt ab von einer Bedingung, die wir später noch kennenlernen werden, nämlich der Bedingung der „ganzen Abgeschlossenheit" (§ 98).

Die Idealtheorie der zuletzt besprochenen Integritätsbereiche, in denen jedes Primideal außer (0) teilerlos ist, ist nach W. KRULL wesentlich einfacher herzuleiten als die allgemeine Idealtheorie der §§ 82 bis 84. Zunächst nämlich kann man aus dem Teilerkettensatz allein sehr leicht herleiten, daß es zu jedem Ideal $\mathfrak{a}$ ein Potenzprodukt von Primidealen, Teilern von $\mathfrak{a}$ gibt, welches durch $\mathfrak{a}$ teilbar ist (vgl. § 100, Hilfssatz 1):

$$\mathfrak{p}_1^{\varrho_1} \cdot \mathfrak{p}_2^{\varrho_2} \cdots \mathfrak{p}_r^{\varrho_r} \equiv 0 \ (\mathfrak{a})$$
$$\mathfrak{a} \equiv 0 \ (\mathfrak{p}_i) \qquad (i = 1, \ldots, r)$$

Ist $\mathfrak{a} = \mathfrak{q}$ einartig, so kann es außer 0 höchstens ein $\mathfrak{p}_i = \mathfrak{p}$ geben und man erhält $\mathfrak{p}^\varrho \equiv 0 \ (\mathfrak{q})$, womit die oben gegebene Charakterisierung der einartigen Ideale als Teiler von Primidealpotenzen neu hergeleitet ist. Ist $\mathfrak{a} \neq (0)$ nicht einartig, so sind die Primideale $\mathfrak{p}_i$ und daher auch ihre Potenzen $\mathfrak{p}_i^{\varrho_i}$ untereinander teilerfremd, mithin sind auch die Ideale $\mathfrak{q}_i = (\mathfrak{a}, \mathfrak{p}_i^{\varrho_i})$ teilerfremd und ihr Durchschnitt gleich ihrem Produkt

$$[\mathfrak{q}_1, \ldots, \mathfrak{q}_r] = \mathfrak{q}_1 \mathfrak{q}_2 \cdots \mathfrak{q}_r .$$

$\mathfrak{a}$ ist durch alle $\mathfrak{q}_i$, also auch durch ihren Durchschnitt teilbar. Andererseits ergibt das Produkt

$$\mathfrak{q}_1 \mathfrak{q}_2 \cdots \mathfrak{q}_r = (\mathfrak{a}, \mathfrak{p}_1^{\varrho_1}) \cdot (\mathfrak{a}, \mathfrak{p}_2^{\varrho_2}) \cdots (\mathfrak{a}, \mathfrak{p}_r^{\varrho_r})$$

beim Ausmultiplizieren nach dem Distributivgesetz (§ 81) eine Summe von Idealen, die alle durch $\mathfrak{a}$ teilbar sind. Also ist

$$\mathfrak{a} \equiv 0 \ (\mathfrak{q}_1 \mathfrak{q}_2 \cdots \mathfrak{q}_r) \equiv 0 \ (\mathfrak{a}) ,$$

mithin

$$\mathfrak{a} = [\mathfrak{q}_1, \mathfrak{q}_2, \ldots, \mathfrak{q}_r] = \mathfrak{q}_1 \mathfrak{q}_2 \cdots \mathfrak{q}_r .$$

Die $\mathfrak{q}_i$ sind, als Teiler von $\mathfrak{p}_i^{\varrho_i}$, offenbar durch keine anderen Primideale als $\mathfrak{p}_i$ und $\mathfrak{o}$ teilbar und somit einartig. Die Eindeutigkeit der $\mathfrak{q}_i$ folgt daraus, daß nach dem Obigen bei jeder Zerlegung $\mathfrak{a} = [\mathfrak{q}_1', \mathfrak{q}_2', \ldots, \mathfrak{q}_r']$ notwendig $\mathfrak{q}_i' = (\mathfrak{a}, \mathfrak{p}_i^{\sigma})$ ist.

Dreizehntes Kapitel.

Theorie der Polynomideale.

In diesem Kapitel soll die allgemeine Idealtheorie auf (kommutative) Polynombereiche angewandt werden. Außer der allgemeinen Idealtheorie wird nur die Körpertheorie (Kap. 5) und was ihr vorangeht als bekannt vorausgesetzt.

§ 87. Algebraische Mannigfaltigkeiten.

Es sei K ein kommutativer Körper. Eine Reihe von n Elementen $\{\xi_1, \ldots, \xi_n\}$ eines beliebigen algebraischen Erweiterungskörpers von K heißt ein *Punkt* des n-dimensionalen Raumes R_n. Der Punkt $\{\xi_1, \ldots, \xi_n\}$ wird kurz mit ξ bezeichnet; die ξ_ν heißen seine *Koordinaten*.

Es sei $\mathfrak{o} = \mathsf{K}[x_1, \ldots, x_n]$ der Polynombereich der n Unbestimmten $x_1, \ldots, x_n$. Seine Elemente, die Polynome, werden mit $f = f(x) = f(x_1, \ldots, x_n)$, g, h, ... bezeichnet. Ein Punkt ξ heißt *Nullstelle* des Polynoms $f(x)$, wenn $f(\xi) = f(\xi_1, \ldots, \xi_n) = 0$ ist. Die gemeinsamen Nullstellen irgend welcher Polynome $f_1, \ldots, f_r$, also die Lösungen eines Gleichungssystems

$$f_1(\xi) = 0, \ldots, f_r(\xi) = 0, \tag{1}$$

bilden, wenn ihre Menge nicht leer ist, das, was man eine *algebraische Mannigfaltigkeit* $\mathfrak{M}$ nennt. Bekannt sind z. B. die „algebraischen Kurven" in der Ebene und die „algebraischen Flächen" im Raum, die durch je eine Gleichung $f(\xi_1, \xi_2) = 0$ bzw. $f(\xi_1, \xi_2, \xi_3) = 0$ dargestellt werden, ebenso gewisse „Raumkurven", die durch zwei Gleichungen bestimmt sind, usw. Auch ein einzelner Punkt ξ mit Koordinaten aus K bildet eine algebraische Mannigfaltigkeit, und der ganze Raum R_n ist eine.

Wie man die Lösungen von (1) tatsächlich bestimmt, haben wir im elften Kapitel auseinandergesetzt. Hier interessiert uns eine andere Frage, nämlich die, welche allgemeinen Sätze man über die algebraischen Mannigfaltigkeiten aussagen kann, und insbesondere, wie man sie nach der „Dimension" in Kurven, Flächen usw. einteilen kann.

Bildet man aus den „definierenden Polynomen" $f_1, \ldots, f_r$ einer algebraischen Mannigfaltigkeit $\mathfrak{M}$ das Ideal $\mathfrak{a} = (f_1, \ldots, f_r)$, so sieht man, daß alle Punkte der Mannigfaltigkeit (Nullstellen von $f_1, \ldots, f_r$) zugleich auch Nullstellen aller Polynome $f = g_1 f_1 + \cdots + g_r f_r$ des Ideals sind, daß also $\mathfrak{M}$ auch charakterisiert werden kann als Gesamtheit aller gemeinsamen Nullstellen der Polynome des Ideals $\mathfrak{a}$ oder, wie wir kurz sagen werden, aller *Nullstellen des Ideals* $\mathfrak{a}$. Daß $\mathfrak{a}$ eine endliche Basis $(f_1, \ldots, f_r)$ besitzt, bedeutet für $\mathfrak{a}$ nach dem Hilbertschen Basissatz (§ 80) keine Einschränkung; denn jedes Ideal von $\mathfrak{o}$ besitzt

eine endliche Basis. Also gilt: *Eine algebraische Mannigfaltigkeit* $\mathfrak{M}$ *besteht aus den Punkten* ξ, *die Nullstellen eines Ideals* $\mathfrak{a}$ *in* $\mathsf{K}[x_1, \ldots, x_n]$ *sind.* Man nennt $\mathfrak{M}$ *die Nullstellenmannigfaltigkeit von* $\mathfrak{a}$ oder kurz *die Mannigfaltigkeit von* $\mathfrak{a}$.

Ein $\mathfrak{a}$ umfassendes Ideal (Teiler von $\mathfrak{a}$) definiert eine Teilmannigfaltigkeit von $\mathfrak{M}$. Es kann aber vorkommen, daß verschiedene Ideale dieselbe algebraische Mannigfaltigkeit $\mathfrak{M}$ definieren; z. B. hat mit $\mathfrak{a}$ stets auch $\mathfrak{a}^2$ die Mannigfaltigkeit $\mathfrak{M}$. Unter allen diesen Idealen ist aber eins ausgezeichnet: die Gesamtheit *aller* Polynome f, die in allen Punkten der Mannigfaltigkeit $\mathfrak{M}$ den Wert Null annehmen. Diese Gesamtheit umfaßt alle Ideale, welche die Mannigfaltigkeit $\mathfrak{M}$ definieren; und sie ist ein Ideal, denn wenn f auf $\mathfrak{M}$ überall verschwindet, so gilt dies auch von jedem Vielfachen von f, und wenn f und g es tun, tut es auch $f - g$. Die Mannigfaltigkeit dieses Ideals ist $\mathfrak{M}$. Dieses Ideal heißt das *zugehörige Ideal* der Mannigfaltigkeit.

Nimmt ein Polynom f in allen Punkten einer Mannigfaltigkeit $\mathfrak{M}$ den Wert Null an, so sagt man wohl: das Polynom f *enthält* die Mannigfaltigkeit $\mathfrak{M}$ (weil dann nämlich die Mannigfaltigkeit $f = 0$ die Mannigfaltigkeit $\mathfrak{M}$ in sich enthält). Das zugehörige Ideal einer Mannigfaltigkeit $\mathfrak{M}$ besteht also aus allen Polynomen, die die Mannigfaltigkeit $\mathfrak{M}$ enthalten.

Der *Durchschnitt* $\mathfrak{M} \cap \mathfrak{N}$ zweier algebraischen Mannigfaltigkeiten $\mathfrak{M}$ und $\mathfrak{N}$ ist, wenn er nicht leer ist, wieder eine algebraische Mannigfaltigkeit. Wenn nämlich $\mathfrak{M}$ durch das Ideal $\mathfrak{a} = (f_1, \ldots, f_r)$ und $\mathfrak{N}$ durch das Ideal $\mathfrak{b} = (g_1, \ldots, g_s)$ definiert wird, so ist der Durchschnitt $\mathfrak{M} \cap \mathfrak{N}$ offenbar die durch das Ideal $(\mathfrak{a}, \mathfrak{b}) = (f_1, \ldots, f_r, g_1, \ldots, g_s)$ definierte Mannigfaltigkeit.

Aber auch die *Vereinigungsmenge* zweier algebraischen Mannigfaltigkeiten $\mathfrak{M}$, $\mathfrak{N}$ ist eine algebraische Mannigfaltigkeit; diese wird durch das Durchschnittsideal (K. G. V.) $\mathfrak{a} \cap \mathfrak{b}$ (oder auch durch das Produkt $\mathfrak{a} \cdot \mathfrak{b}$) definiert. Zunächst nämlich ist jeder Punkt der Vereinigung entweder Nullstelle aller Polynome aus $\mathfrak{a}$ oder Nullstelle aller Polynome aus $\mathfrak{b}$, also auf jeden Fall Nullstelle aller Polynome aus $\mathfrak{a} \cap \mathfrak{b}$ (und insbesondere von denen aus $\mathfrak{a} \cdot \mathfrak{b}$). Wenn aber ein Punkt ξ nicht zur Vereinigung $\{\mathfrak{M}, \mathfrak{N}\}$ gehört, so gibt es in $\mathfrak{a}$ ein Polynom f und ebenso in $\mathfrak{b}$ ein Polynom g, welche im Punkt ξ nicht verschwinden; dann verschwindet aber auch das zu $\mathfrak{a} \cap \mathfrak{b}$ (und $\mathfrak{a} \cdot \mathfrak{b}$) gehörige Produkt fg im Punkte ξ nicht, und somit ist ξ nicht Nullstelle von $\mathfrak{a} \cap \mathfrak{b}$ (oder $\mathfrak{a} \cdot \mathfrak{b}$). Nullstellen von $\mathfrak{a} \cap \mathfrak{b}$ (sowie von $\mathfrak{a} \cdot \mathfrak{b}$) sind also die Punkte von $\{\mathfrak{M}, \mathfrak{N}\}$ und nur diese.

Es folgt, daß die Vereinigung endlich vieler algebraischen Mannigfaltigkeiten (z. B. endlich vieler Punkte, Kurven usw.) wieder eine algebraische Mannigfaltigkeit ist.

Eine Mannigfaltigkeit, die als Vereinigung zweier echten Teilmannigfaltigkeiten dargestellt werden kann, heißt *zusammengesetzt* oder *redu-*

zibel. Eine nicht zusammengesetzte Mannigfaltigkeit heißt *unzerlegbar* oder *irreduzibel.*

Die Entscheidung über Reduzibilität einer Mannigfaltigkeit hängt noch vom Grundkörper K ab. Z. B. bildet das Punktepaar $\xi_1 = 0$, $\xi_2 = \pm\sqrt{2}$ eine im rationalen Zahlkörper irreduzible Mannigfaltigkeit, die Nullstellenmannigfaltigkeit des Ideals $(x_1, x_2^2 - 2)$, welche aber bei Adjunktion von $\sqrt{2}$ in zwei Bestandteile (Punkte) zerfällt.

Ein Kriterium für Irreduzibilität ist: *Eine Mannigfaltigkeit* $\mathfrak{M}$ *ist dann und nur dann irreduzibel, wenn das zugehörige Ideal prim ist, d. h. wenn aus „*fg *enthält* $\mathfrak{M}$*" folgt:* f *oder* g *enthält* $\mathfrak{M}$.

Beweis: $\mathfrak{M}$ sei zunächst reduzibel: $\mathfrak{M} = \mathfrak{M}_1 \vee \mathfrak{M}_2$, wo $\mathfrak{M}_1$ und $\mathfrak{M}_2$ echte Teilmannigfaltigkeiten von $\mathfrak{M}$ sind. In dem zugehörigen Ideal von $\mathfrak{M}_1$ gibt es ein Polynom f, welches $\mathfrak{M}$ nicht enthält, weil ja sonst $\mathfrak{M}_1 \geqq \mathfrak{M}$ wäre. Ebenso gibt es in dem zugehörigen Ideal von $\mathfrak{M}_2$ ein Polynom g, welches $\mathfrak{M}$ nicht enthält. Das Produkt fg enthält $\mathfrak{M}_1$ und $\mathfrak{M}_2$, also $\mathfrak{M}$. Das zu $\mathfrak{M}$ gehörige Ideal ist also nicht prim.

Zweitens sei $\mathfrak{M}$ irreduzibel. Wenn nun fg ein Produkt wäre, das $\mathfrak{M}$ enthielte, ohne daß f oder g es täte, so könnte man $\mathfrak{M}$ als Vereinigung zweier echten Teilmannigfaltigkeiten $\mathfrak{M}_1$ und $\mathfrak{M}_2$ darstellen, die sich folgendermaßen definieren lassen: $\mathfrak{M}_1$ besteht aus allen Punkten von $\mathfrak{M}$, welche der Gleichung $f = 0$ genügen, und $\mathfrak{M}_2$ aus allen Punkten von $\mathfrak{M}$, welche der Gleichung $g = 0$ genügen. Jeder Punkt ξ von $\mathfrak{M}$ gehört dann zu $\mathfrak{M}_1$ oder zu $\mathfrak{M}_2$, da aus $f(\xi)\, g(\xi) = 0$ folgt, daß $f(\xi) = 0$ oder $g(\xi) = 0$ ist. Das widerspricht aber der vorausgesetzten Irreduzibilität von $\mathfrak{M}$.

Dadurch, daß man die Primideale mit der Vorstellung der irreduziblen Mannigfaltigkeiten verknüpft, zu denen sie gehören, erhält man eine anschauliche Vorstellung der mannigfachen möglichen Primideale, und davon, wie ein Primideal durch ein anderes teilbar sein kann. In der Ebene z. B. hat man, vom Nullideal ausgehend, das zur ganzen Ebene als Mannigfaltigkeit gehört, als dessen Teiler die Prim-Hauptideale (f), die je zu einer unzerlegbaren Kurve $f = 0$ gehören, dann als deren Teiler solche Primideale, die zu Punkten (oder Systemen konjugierter Punkte, wenn der Körper K nicht algebraisch-abgeschlossen ist) gehören, schließlich als Teiler aller Primideale das Einheitsideal, das keine Nullstelle besitzt.

Daß es tatsächlich keine anderen Primideale gibt als die zu irreduziblen Mannigfaltigkeiten gehörigen Primideale und das Einheitsideal $\mathfrak{o}$, ergibt sich sehr leicht, wenn man den Hilbertschen Nullstellensatz (§ 75) als bekannt annimmt, nämlich so: Es sei $\mathfrak{p}$ ein vom Einheitsideal verschiedenes Primideal, $\mathfrak{M}$ seine Nullstellenmannigfaltigkeit. Wenn ein Polynom f auf $\mathfrak{M}$ überall verschwindet, so folgt aus dem Hilbertschen Nullstellensatz $f^\varrho \equiv 0\,(\mathfrak{p})$, daraus aber, weil $\mathfrak{p}$ prim ist, $f \equiv 0\,(\mathfrak{p})$. Also ist $\mathfrak{p}$ das zugehörige Ideal der Mannigfaltigkeit $\mathfrak{M}$, und $\mathfrak{M}$ muß irreduzibel sein, da sonst $\mathfrak{p}$ nicht prim wäre.

Wir werden aber für den Satz, daß jedes vom Einheitsideal verschiedene Primideal das zugehörige Ideal seiner Mannigfaltigkeit ist, im übernächsten Paragraphen einen anderen Beweis erbringen und daraus dann umgekehrt den Hilbertschen Nullstellensatz von neuem herleiten.

Aufgabe. 1. Man zerlege die Mannigfaltigkeit des Ideals $(x_1^2 + x_2^2 - 1, x_1^2 - x_3^3 - 1)$ in irreduzible

a) über dem rationalen Zahlkörper Γ;

b) über dem Gaußschen Zahlkörper $\Gamma(i)$;

c) über dem Körper aller algebraischen Zahlen.

In der Geometrie macht man sehr häufig den Übergang vom gewöhnlichen „offenen" oder „affinen" n-dimensionalen Raum R_n zum projektiven Raum P_n, dessen Punkte durch $n+1$ homogene Koordinaten $\xi_0, \xi_1, \ldots, \xi_n$ bestimmt werden, die nicht alle Null sind und die mit einem von Null verschiedenen Faktor multipliziert werden dürfen (vgl. S. 12, Fußnote 2). Jedem Punkt $\{\xi_1, \ldots, \xi_n\}$ des R_n ist ein Punkt $\{1, \xi_1, \ldots, \xi_n\}$ des projektiven Raumes P_n zugeordnet; man kann also den R_n als einen Teil des P_n betrachten, der durch die „uneigentliche Hyperebene" $\xi_0 = 0$ zum ganzen P_n ergänzt wird.

Jedem Ideal $\mathfrak{a}$ aus $\mathsf{K}[x_1, \ldots, x_n]$ kann ein Ideal $\mathfrak{a}^*$ aus $\mathsf{K}[x_0, \ldots, x_n]$ zugeordnet werden, das von denjenigen Formen (homogenen Polynomen) $F(x_0, \ldots, x_n)$ erzeugt wird, welche nach der Substitution $x_0 = 1$ Polynome aus $\mathfrak{a}$ ergeben. Ein solches Ideal, das von homogenen Polynomen erzeugt wird, heißt ein *homogenes Ideal* oder H-Ideal. Insbesondere kann man $\mathfrak{a}^*$ als das *zugehörige H-Ideal* zu $\mathfrak{a}$ bezeichnen. Die H-Ideale haben die Eigenschaft, daß, wenn $\{\xi_0, \ldots, \xi_n\}$ eine Nullstelle ist, auch $\{\lambda\xi_0, \ldots, \lambda\xi_n\}$ $(\lambda \neq 0)$ eine ist; wir sagen in diesem Fall: der Punkt ξ des P_n ist Nullstelle des H-Ideals. Diese Nullstellen eines H-Ideals im projektiven Raum bilden die *Mannigfaltigkeit des H-Ideals im projektiven Raum.*

Zu jeder algebraischen Mannigfaltigkeit $\mathfrak{M}$ im R_n können wir eine (kleinste) sie umfassende algebraische Mannigfaltigkeit $\mathfrak{M}^*$ im P_n bilden, indem wir zu $\mathfrak{M}$ das zugehörige Ideal $\mathfrak{a}$, zu $\mathfrak{a}$ das zugehörige H-Ideal $\mathfrak{a}^*$ bilden und dessen Mannigfaltigkeit im P_n mit $\mathfrak{M}^*$ bezeichnen. Der Beweis, daß $\mathfrak{M}^*$ tatsächlich $\mathfrak{M}$ umfaßt und die kleinste derartige Mannigfaltigkeit im P_n ist, möge dem Leser überlassen bleiben, ebenso der Beweis, daß $\mathfrak{M}$ aus denjenigen Punkten von $\mathfrak{M}^*$ besteht, die nicht in der uneigentlichen Hyperebene liegen.

Ist $\mathfrak{M}$ irreduzibel, so ist offensichtlich $\mathfrak{M}^*$ es auch.

Aufgaben. 2. Man führe die Beweise durch.

3. Wenn ein Polynom f einem H-Ideal angehört, so gehören auch die homogenen Bestandteile verschiedenen Grades, in die f additiv zerlegt werden kann, dem H-Ideal an.

4. Jedes H-Ideal besitzt eine Idealbasis aus endlich vielen Formen.

§ 88. Algebraische Funktionen.

Wir wollen untersuchen, in welcher Weise die Punkte einer algebraischen Mannigfaltigkeit als algebraische Funktionen von Parametern dargestellt werden können. Dazu müssen wir zunächst etwas über algebraische Funktionen im allgemeinen sagen.

Unter einem *rationalen Funktionenkörper* verstehen wir den Körper $\mathsf{K}(t_1, \ldots, t_r)$ der rationalen Funktionen der Unbestimmten $t_1, \ldots, t_r$.

Unter einem *algebraischen Funktionenkörper* verstehen wir irgend eine algebraische Erweiterung des rationalen Funktionenkörpers $\mathsf{K}(t_1, \ldots, t_r)$. Die Elemente eines solchen Körpers heißen *algebraische Funktionen* von $t_1, \ldots, t_r$.

Was man bei einer rationalen Funktion $\varphi = \frac{f(t_1, \ldots, t_r)}{g(t_1, \ldots, t_r)}$ (f und g Polynome) unter dem *Wert* der Funktion für spezielle Werte $\tau_1, \ldots, \tau_r$ aus dem Körper K zu verstehen hat, ist klar: man kann ja in die Definition von φ für die t die τ einsetzen, sofern nur $g(\tau_1, \ldots, \tau_r)$ nicht verschwindet:

$$\varphi(\tau_1, \ldots, \tau_r) = \frac{f(\tau_1, \ldots, \tau_r)}{g(\tau_1, \ldots, \tau_r)}.$$

Die Werte $\tau_1, \ldots, \tau_r$ können auch einem algebraischen Erweiterungskörper Ω von K entnommen werden; dann wird auch der φ-Wert diesem Erweiterungskörper angehören. Da ein passendes Ω beliebig viele Elemente besitzt, so stehen für jedes τ_ν unendlich viele Werte zur Verfügung, mithin gibt es stets $\tau_1, \ldots, \tau_r$ mit $g(\tau_1, \ldots, \tau_r) \neq 0$.

Bei algebraischen Funktionen ist der Begriff des Wertes nicht so unmittelbar klar, da die algebraischen Funktionen zwar als Elemente eines Körpers mit den Unbestimmten $t_1, \ldots, t_r$ durch gewisse Gleichungen verbunden sind, aber nicht direkt durch $t_1, \ldots, t_r$ ausgedrückt werden können. Ist f eine Funktion aus dem Körper, so genügt f einer irreduziblen Gleichung:

$$a_0(t) f^h + a_1(t) f^{h-1} + \cdots + a_h(t) = 0, \tag{1}$$

wo $a_0, \ldots, a_h$ rationale Funktionen von $t_1, \ldots, t_r$ (mit Koeffizienten aus K) sind, die man natürlich auch als ganzrational und teilerfremd annehmen kann. Setzt man nun für $t_1, \ldots, t_r$ irgend welche Werte $\tau_1, \ldots, \tau_r$ aus K oder aus $\Omega \supseteq \mathsf{K}$ ein, so betrachtet man als *Funktionswerte* alle Wurzeln φ der spezialisierten Gleichung (1) in einem passenden algebraischen Erweiterungskörper. Solche Werte gibt es z. B. immer, wenn $a_0(\tau) \neq 0$ ist, oder überhaupt, wenn $a_\nu(\tau)$ für ein $\nu < h$ von Null verschieden ist. Die Funktion f ist also im allgemeinen *mehrdeutig*: zu jedem Argumentwertsystem gehören mehrere Funktionswerte.

Hat man gleichzeitig mit mehreren Funktionen $f_1, \ldots, f_s$ aus einem Funktionenkörper zu tun, so wollen wir als *Funktionswerte* $\varphi_1, \ldots, \varphi_s$ der Funktionen $f_1, \ldots, f_s$ zu gegebenen Argumentwerten $\tau_1, \ldots, \tau_r$ nur solche Wertsysteme $\varphi_1, \ldots, \varphi_s$ (in einem passenden Körper Ω) betrachten, welche die Eigenschaften besitzen, daß alle algebraischen Relationen $F(f_1, \ldots, f_s, t_1, \ldots, t_r) = 0$ (mit Koeffizienten aus K), die im Funktionenkörper bestehen, auch für die Funktionswerte gelten; daß also aus $F(f_1, \ldots, f_s, t_1, \ldots, t_r) = 0$ folgt $F(\varphi_1, \ldots, \varphi_s, \tau_1, \ldots, \tau_r) = 0$[1]. Es ist

[1] Bei nur einer Funktion f ist diese Bedingung von selbst erfüllt, wenn man die Funktionswerte gemäß (1) bestimmt; denn jede Gleichung $F(f, t_1, \ldots, t_r) = 0$ ist eine Folge der irreduziblen Gleichung (1).

also im allgemeinen nicht erlaubt, beliebige Werte der mehrdeutigen Funktion f_1 mit beliebigen Werten von $f_2, \ldots, f_s$ zu verknüpfen, da dann eventuelle Relationen zwischen den f verlorengehen können. Ist z. B. $f_1 = \sqrt{t}$ und $f_2 = -f_1$, also $f_1^2 = t$ und $f_2^2 = t$, so hat man für $\tau = 1$ die Funktionswerte $\varphi_1 = \pm 1$ und $\varphi_2 = \pm 1$ zur Verfügung, darf aber nicht $\varphi_1 = +1$ mit $\varphi_2 = +1$ kombinieren, da sonst die Relation $f_1 + f_2 = 0$ verletzt würde.

Wir wollen nun zeigen, daß es in einem passenden Körper Ω immer (sogar unendlich viele) Wertsysteme $\tau_1, \ldots, \tau_r$ und zugehörige Funktionswerte $\varphi_1, \ldots, \varphi_s$ gibt, welche die obige Bedingung erfüllen. Zu dem Zweck schreiben wir untereinander: die irreduzible Gleichung für f_1 im Körper $\mathsf{K}(t_1, \ldots, t_r)$; die irreduzible Gleichung für f_2 im Körper $\mathsf{K}(f_1, t_1, \ldots, t_r)$; usw., alle dividiert durch ihre Anfangskoeffizienten:

$$(2) \qquad \begin{cases} f_1^h + a_1(t) f_1^{h-1} + \cdots + a_h(t) = 0, \\ f_2^k + b_1(f_1, t) f_2^{k-1} + \cdots + b_k(f_1, t) = 0, \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \end{cases}$$

Die Koeffizienten der zweiten Gleichung sind rational in f_1 und können, da f_1 algebraisch ist, ganzrational in f_1 gewählt werden. Ebenso können die Koeffizienten der dritten Gleichung ganzrational in f_2 und f_1 gewählt werden, usw. Schließlich kommen also in allen Gleichungen als Nenner nur Polynome in $t_1, \ldots, t_r$ allein vor. Ein von Null verschiedenes gemeinsames Vielfaches aller dieser Nenner sei $V(t_1, \ldots, t_r)$. Wir wählen nun $\tau_1, \ldots, \tau_r$ so, daß $V(\tau_1, \ldots, \tau_r) \neq 0$ ist, und bestimmen dann sukzessiv $\varphi_1, \ldots, \varphi_s$ aus den spezialisierten Gleichungen (2):

$$\begin{aligned} &\varphi_1^h + a_1(\tau) \varphi_1^{h-1} + \cdots + a_h(\tau) = 0, \\ &\varphi_2^k + b_1(\varphi_1, \tau) \varphi_2^{k-1} + \cdots + b_k(\varphi_1, \tau) = 0, \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \end{aligned}$$

Wir behaupten nun, daß die so bestimmten $\tau_1, \ldots, \tau_r, \varphi_1, \ldots, \varphi_s$ tatsächlich die gestellte Bedingung erfüllen, daß aus

$$F(f_1, \ldots, f_s, t_1, \ldots, t_r) = 0,$$

wo F ein Polynom in den $r + s$ Unbestimmten $u_1, \ldots, u_s, t_1, \ldots, t_r$ mit Koeffizienten aus K ist,

$$F(\varphi_1, \ldots, \varphi_s, \tau_1, \ldots, \tau_r) = 0$$

folgt.

Für Polynome F, die nur $t_1, \ldots, t_r$ enthalten, ist die Behauptung klar. Wir können also Induktion nach der Nummer q des letzten in F wirklich vorkommenden φ_q vornehmen. Die Behauptung sei für Polynome $F(u_1, \ldots, u_{q-1}, t_1, \ldots, t_r)$ schon bewiesen.

Die q-te Gleichung der Reihe (2) möge lauten:

$$G(f_1, \ldots, f_q, t_1, \ldots, t_r) = f_q^m + d_1(f, t) f_q^{m-1} + \cdots + d_m(f, t) = 0,$$

wo $G(f_1, \ldots, f_{q-1}, u_q, t_1, \ldots, t_r) = G(u_q)$ ein in $\mathsf{K}(f_1, \ldots, f_{q-1}, t_1, \ldots, t_r)$ irreduzibles Polynom der Unbestimmten u_q ist. Aus $F(f_1, \ldots, f_q, t_1, \ldots, t_r) = 0$ folgt nun, daß $F(f_1, \ldots, f_{q-1}, u_q, t_1, \ldots, t_r) = F(u_q)$ durch $G(u_q)$ teilbar ist. Die Division läßt sich so ausführen, daß dabei nur solche Polynome in $t_1, \ldots, t_r$ als Faktoren im Nenner auftreten, die in G selbst schon vorkamen. Diese Faktoren kommen also alle schon in $V(t_1, \ldots, t_r)$ vor. Man erhält etwa:

$$F(u_q) = G(u_q)\, H(u_q)\,. \tag{3}$$

Vergleichung der Koeffizienten der Potenzen von u_q links und rechts in (3) und Multiplikation mit einer passenden Potenz von $V(t_1, \ldots, t_r)$ ergibt eine Reihe von ganzrationalen Gleichungen in $f_1, \ldots, f_{q-1}, t_1, \ldots, t_r$. Diese bleiben nach der Induktionsvoraussetzung bei der Ersetzung der t durch die τ und der f durch die φ bestehen. Dividiert man dann wieder durch die betreffende Potenz von $V(\tau_1, \ldots, \tau_r)$, so ergibt sich, daß auch die Gleichung (3) bei der Ersetzung der t durch die τ und der f durch die φ gültig bleibt. Ersetzt man nun auch noch u_q durch φ_q, so verschwindet der erste Faktor auf der rechten Seite, und man erhält

$$F(\varphi_1, \ldots, \varphi_s, \tau_1, \ldots, \tau_r) = 0\,,$$

was zu beweisen war.

Wir gehen hier nicht auf die verschiedenen Methoden ein, die Bestimmung der $\varphi_1, \ldots, \varphi_s$ auch auf solche $\tau_1, \ldots, \tau_r$ auszudehnen, die nicht der Bedingung $V(\tau_1, \ldots, \tau_r) \neq 0$ genügen. Man kann diese Werte durch Grenzübergang erhalten, auch durch Reihenentwicklungen in der Umgebung der singulären Stellen, usw.; alle diese Methoden genügen dem Kriterium der Erhaltung aller algebraischen Relationen $F(f_1, \ldots, f_s, t_1, \ldots, t_r) = 0$. Auch auf die Einführung des Symbols ∞, durch die man die Fälle noch mitumfaßt, in denen es keine endlichen Werte $\varphi_1, \ldots, \varphi_s$ gibt, gehen wir hier nicht ein, sondern verweisen auf die Theorie der algebraischen Funktionen[1]. Für unseren Zweck genügt es, daß es überhaupt zu jedem Funktionensystem zulässige Argumentwerte und zugehörige Funktionswerte gibt.

Im folgenden wird ein Satz gebraucht, der gewissermaßen eine Umkehrung des vorangehenden ist und so lautet: *Wenn eine Relation* $F(\varphi_1, \ldots, \varphi_s, \tau_1, \ldots, \tau_r) = 0$ *für alle zulässigen Argumentwerte* τ *und zugehörigen Funktionswerte* φ *gilt, so gilt auch die entsprechende Relation* $F(f_1, \ldots, f_s, t_1, \ldots, t_r) = 0$ *im Funktionenkörper.*

Beweis: Wäre $F(f_1, \ldots, f_s, t_1, \ldots, t_r) \neq 0$, so könnte man die Funktion

$$f_{s+1} = \frac{1}{F(f_1, \ldots, f_s, t_1, \ldots, t_r)}$$

[1] Siehe z. B. JORDAN: Cours d'analyse, 3. Aufl., Bd. 2, S. 622—693. 1913. HURWITZ-COURANT: Funktionentheorie, 3. Aufl., S. 480—527, 1929; für mehr Veränderliche: B. L. v. D. WAERDEN: Zur Produktzerlegung der Ideale in ganz-abgeschlossenen Ringen, Math. Ann. Bd. 101, S. 293—308, § 8. 1929.

bilden und für die Funktionen $f_1, \ldots, f_s, f_{s+1}$ ein zulässiges Wertsystem $\varphi_1, \ldots, \varphi_s, \varphi_{s+1}, \tau_1, \ldots, \tau_r$ aufstellen. Die Relation

$$1 = f_{s+1} \cdot F(f_1, \ldots, f_s, t_1, \ldots, t_r)$$

muß bei der Spezialisierung $f_\nu \to \varphi_\nu$, $t_\lambda \to \tau_\lambda$ bestehen bleiben. Nach Voraussetzung wird aber $F(\varphi_1, \ldots, \varphi_s, \tau_1, \ldots, \tau_r) = 0$; also erhält man

$$1 = 0,$$

quod est absurdum.

§ 89. Parameterdarstellung algebraischer Mannigfaltigkeiten.

Sind $\xi_1, \ldots, \xi_n$ algebraische Funktionen von $t_1, \ldots, t_r$, so bestimmen die zu speziellen zulässigen Argumentwerten $\tau_1, \ldots, \tau_r$ gehörigen Funktionswerte $\xi_1', \ldots, \xi_n'$ jeweils einen Punkt ξ' im R_n, und diese Punkte ξ' können eine algebraische Mannigfaltigkeit ganz oder teilweise ausfüllen. Wir reden dann von einer *Parameterdarstellung* der Mannigfaltigkeit durch algebraische Funktionen $\xi_1, \ldots, \xi_n$ der Parameter $t_1, \ldots, t_r$.

Zum Beispiel genügen die durch

$$\xi_1 = \frac{1 - t^2}{1 + t^2}, \qquad \xi_2 = \frac{2t}{1 + t^2} \tag{1}$$

dargestellten Punkte der Ebene R_2 der Gleichung

$$\xi_1^2 + \xi_2^2 = 1. \tag{2}$$

Aber nicht alle Punkte des Kreises (2) werden durch die Gleichungen (1) dargestellt; denn der Punkt $(-1, 0)$ genügt der Gleichung (2), während der Ausdruck $\frac{1 - t^2}{1 + t^2}$ den Wert -1 nicht annimmt.

Wir können also von einer Parameterdarstellung einer Mannigfaltigkeit durch algebraische Funktionen nicht erwarten, daß alle Punkte der Mannigfaltigkeit durch sie dargestellt werden. Wohl aber können wir bei gegebenen Parameterfunktionen die kleinste algebraische Mannigfaltigkeit suchen, die alle durch die Parameterdarstellung erreichbaren Punkte ξ' umfaßt.

Jede algebraische Mannigfaltigkeit, welche die Punkte ξ' alle umfaßt, wird durch Gleichungen $f = 0$ gegeben, welche für alle Punkte ξ' erfüllt sind. Die kleinste unter diesen algebraischen Mannigfaltigkeiten werden wir also erhalten, wenn wir *alle* Gleichungen $f = 0$ nehmen, die in den Punkten ξ' erfüllt sind.

Die Polynome $f(x_1, \ldots, x_n)$, die in allen Punkten ξ' den Wert Null annehmen, können nach § 88 auch dadurch charakterisiert werden, daß für sie im Funktionenkörper $\mathsf{K}(\xi_1, \ldots, \xi_n)$ die Gleichung $f(\xi) = 0$ besteht. Diese Polynome bilden, wie man sofort feststellt, ein Ideal im Polynombereich $\mathfrak{o} = \mathsf{K}[x_1, \ldots, x_n]$. Das Ideal ist sogar ein Primideal; denn aus $f(\xi) \cdot g(\xi) = 0$ folgt im Funktionenkörper, daß $f(\xi) = 0$ oder

$g(\xi) = 0$ ist. Die Nullstellen dieses Primideals $\mathfrak{p}$ bilden nun, wie wir eben sahen, die kleinste algebraische Mannigfaltigkeit, welche alle durch die Parameterdarstellung erreichbaren Punkte umfaßt. Wir nennen diese Mannigfaltigkeit $\mathfrak{M}$ *die durch die Parameterfunktionen* $\xi_1, \ldots, \xi_n$ *bestimmte algebraische Mannigfaltigkeit.*

Durch die Zuordnung

$$f(x) \to f(\xi)$$

oder

$$\sum \alpha_\lambda x_1^{i_1} \cdots x_n^{i_n} \to \sum \alpha_\lambda \xi_1^{i_1} \cdots \xi_n^{i_n}$$

ist eine homomorphe Abbildung von $\mathfrak{o} = \mathsf{K}[x]$ auf den Ring $\mathsf{K}[\xi]$ gegeben. Die Polynome f, die dabei in Null übergehen, bilden gerade das Ideal $\mathfrak{p}$. Nach dem Homomorphiesatz ist also

$$\mathsf{K}[\xi] \cong \mathfrak{o}/\mathfrak{p}\,. \tag{3}$$

Daraus ersieht man von neuem, daß $\mathfrak{p}$ ein Primideal sein muß.

Die Definition des Ideals $\mathfrak{p}$ und daher auch die der Mannigfaltigkeit $\mathfrak{M}$ hängt, wie man sieht, nicht von der Wahl der unabhängigen Variablen $t_1, \ldots, t_r$, von denen die $\xi_1, \ldots, \xi_n$ Funktionen sind, sondern nur von den algebraischen Eigenschaften der Körperelemente ξ ab. Umgekehrt sind nach (3) die algebraischen Eigenschaften der ξ allein durch das Ideal $\mathfrak{p}$ bestimmt. Der Körper, dem die ξ angehören, ist der Quotientenkörper von $\mathsf{K}[\xi]$, also isomorph dem Quotientenkörper von $\mathfrak{o}/\mathfrak{p}$.

Das Primideal $\mathfrak{p}$ *ist das zugehörige Ideal seiner Mannigfaltigkeit* $\mathfrak{M}$. Denn wenn ein Polynom f auf $\mathfrak{M}$ überall verschwindet, so ist insbesondere $f(\xi') = 0$ für alle durch die Parameterfunktionen erreichbaren Punkte ξ', und daraus folgt $f \equiv 0\ (\mathfrak{p})$. Da nun $\mathfrak{p}$ prim ist, so folgt nach § 87 die Irreduzibilität von $\mathfrak{M}$ im Körper K. Also: *Je n algebraische Funktionen* $\xi_1, \ldots, \xi_n$ *bestimmen eine irreduzible algebraische Mannigfaltigkeit in Parameterdarstellung.*

Die Funktionen $\frac{f(\xi_1, \ldots, \xi_n)}{g(\xi_1, \ldots, \xi_n)}$ des Körpers $\mathsf{K}(\xi)$ nehmen in allen Punkten ξ' der Mannigfaltigkeit $\mathfrak{M}$, in denen nicht gerade der Nenner $g(\xi')$ gleich Null wird, bestimmte Werte $\frac{f(\xi')}{g(\xi')}$ an. Zwei Funktionen $\frac{f(\xi)}{g(\xi)}$ und $\frac{f_1(\xi)}{g_1(\xi)}$ sind im Körper $\mathsf{K}(\xi)$ dann und nur dann einander gleich, wenn ihre Werte $\frac{f(\xi')}{g(\xi')}$ und $\frac{f_1(\xi')}{g_1(\xi')}$ für alle diejenigen Punkte ξ', in denen $g(\xi')$ und $g_1(\xi')$ nicht verschwinden, einander gleich sind; denn aus

$$f(\xi) g_1(\xi) = f_1(\xi) g(\xi)$$

folgt

$$f(\xi') g_1(\xi') = f_1(\xi') g(\xi'),$$

für alle ξ', und umgekehrt. Daher können die Funktionen des Körpers $\mathsf{K}(\xi)$ auch als *Funktionen auf der Mannigfaltigkeit* $\mathfrak{M}$ aufgefaßt werden.

Die Größen $\xi_1, \ldots, \xi_n$ können auch als Koordinaten eines „Punktes" ξ *im weiteren Sinne* aufgefaßt werden: eines Punktes nämlich, dessen Koordinaten nicht wie bisher Konstanten aus einem algebraischen,

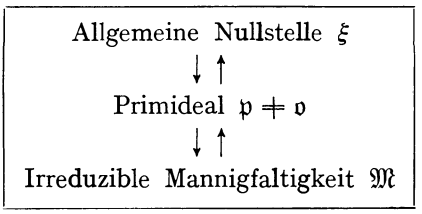
sondern Funktionen aus einem transzendenten Erweiterungskörper des Körpers K sind. Der „Punkt" ξ heißt ein *allgemeiner Punkt* der Mannigfaltigkeit $\mathfrak{M}$, weil die gewöhnlichen Punkte ξ' von $\mathfrak{M}$ aus ihm durch Parameterspezialisierung (wobei alle Relationen $f(\xi) = 0$ erhalten bleiben) hervorgehen. Man nennt ξ auch die *allgemeine Nullstelle* des Ideals $\mathfrak{p}$, nach folgender Definition: *ξ heißt allgemeine Nullstelle von $\mathfrak{p}$, wenn aus $f(\xi) = 0$ folgt $f \equiv 0\,(\mathfrak{p})$ und umgekehrt, für beliebiges f aus $\mathsf{K}[x]$.*

Wie wir sahen, gehört zu jedem Funktionensystem $\xi_1, \ldots, \xi_n$ ein Primideal $\mathfrak{p}$, dessen allgemeine Nullstelle ξ ist. Wir wollen nun sehen, ob es auch zu jedem Primideal $\mathfrak{p}$ eine allgemeine Nullstelle gibt. Dabei müssen wir natürlich den Fall $\mathfrak{p} = \mathfrak{o}$ ausschließen; denn das Einheitsideal $\mathfrak{o}$ hat überhaupt keine Nullstelle. Dagegen behaupten wir, daß *jedes Primideal $\mathfrak{p} \neq \mathfrak{o}$ eine allgemeine Nullstelle hat.*

Zum Beweis bilden wir zunächst den Ring $\bar{\mathfrak{o}} = \mathfrak{o}/\mathfrak{p}$ der Restklassen nach $\mathfrak{p}$. Bei der Homomorphie $\mathfrak{o} \sim \bar{\mathfrak{o}}$ wird jedem Polynom f eine Restklasse $\bar{f}$ zugeordnet, insbesondere jeder Konstanten α eine Restklasse $\bar{\alpha}$. Verschiedenen Konstanten entsprechen aber verschiedene Restklassen; denn wenn $\bar{\alpha} = \bar{\beta}$ und $\alpha \neq \beta$ wäre, so wäre $\alpha \equiv \beta\,(\mathfrak{p})$, mithin $\alpha - \beta = \gamma$ in $\mathfrak{p}$ enthalten, also auch $\gamma\gamma^{-1} = 1$ in $\mathfrak{p}$ enthalten, mithin $\mathfrak{p}$ das Einheitsideal, entgegen der Voraussetzung. Also ist der Körper K der Konstanten α isomorph abgebildet auf einen Körper $\bar{\mathsf{K}}$, bestehend aus den Bildern $\bar{\alpha}$ dieser Konstanten. Nach § 11, Schluß können wir nun einen zu $\bar{\mathfrak{o}}$ isomorphen Ring $\mathfrak{o}^*$ bilden, der K umfaßt, indem wir einfach die Elemente von $\bar{\mathsf{K}}$ durch die ihnen entsprechenden von K ersetzen. $\mathfrak{o}^*$ ist wieder ein homomorphes Bild von $\mathfrak{o}$, und bei der homomorphen Abbildung $\mathfrak{o} \to \mathfrak{o}^*$ entsprechen die Konstanten α sich selbst. Den Variablen $x_1, \ldots, x_n$ entsprechen gewisse Größen von $\mathfrak{o}^*$, die wir mit $\xi_1, \ldots, \xi_n$ bezeichnen. Jedem Polynom $f(x) = \sum \alpha_\lambda x_1^{\lambda_1} \cdots x_n^{\lambda_n}$ entspricht der zugehörige Ausdruck $f(\xi) = \sum \alpha_\lambda \xi_1^{\lambda_1} \cdots \xi_n^{\lambda_n}$. Also ist $\mathfrak{o}^* = \mathsf{K}[\xi_1, \ldots, \xi_n]$, und wir haben die Isomorphie (3) wiedergefunden.

Der Ring $\mathsf{K}[\xi]$ läßt sich in einen Quotientenkörper $\mathsf{K}(\xi_1, \ldots, \xi_n)$ einbetten. Die ξ sind also Elemente eines Funktionenkörpers: algebraische Funktionen von r unter ihnen. Aus $f^* = f(\xi) = 0$ folgt stets $f = f(x) \equiv 0\,(\mathfrak{p})$ und umgekehrt; also bilden die ξ eine allgemeine Nullstelle des Ideals $\mathfrak{p}$, q. e. d.

Das bis jetzt Bewiesene läßt sich in dem folgenden Schema zusammenfassen:



Zu Anfang dieses Paragraphen sind wir von einer beliebigen allgemeinen Nullstelle ξ (System von n algebraischen Funktionen) ausgegangen und haben dazu das Primideal $\mathfrak{p}$ und die Mannigfaltigkeit $\mathfrak{M}$ konstruiert. Das zugehörige Ideal von $\mathfrak{M}$ war wieder $\mathfrak{p}$, und $\mathfrak{p}$ bestimmte die allgemeine Nullstelle ξ bis auf Isomorphie eindeutig; also ließ die Kette sich auch rückwärts verfolgen. Zum Schluß haben wir bewiesen, daß man auch von einem beliebigen $\mathfrak{p} \neq \mathfrak{o}$ ausgehen und dazu stets eine allgemeine Nullstelle ξ finden kann. Da auch zu jeder beliebigen algebraischen Mannigfaltigkeit ein zugehöriges Primideal $\mathfrak{p}$ existiert, so sind alle in unserem Schema durch Pfeile angedeuteten Relationen vollständig *eineindeutig*. Insbesondere schließen wir daraus, daß *jede irreduzible Mannigfaltigkeit eine Parameterdarstellung durch algebraische Funktionen* $\xi_1, \ldots, \xi_n$ *besitzt* (und zwar können, wie wir sahen, stets einige ξ als algebraische Funktionen der übrigen aufgefaßt werden), und weiter schließen wir, daß *jedes Primideal* $\mathfrak{p} \neq \mathfrak{o}$ *das zugehörige Ideal seiner Nullstellenmannigfaltigkeit ist.* Das einzige Primideal ohne Nullstellen ist $\mathfrak{o}$. Auch dieses Primideal ist demnach durch seine Nullstellen bestimmt.

Aufgaben. 1. Das Ideal in $\mathsf{K}[x_1, x_2, x_3]$

$$(x_1 x_3 - x_2^2,\ x_2 x_3 - x_1^3,\ x_3^2 - x_1^2 x_2)$$

ist prim, weil es die allgemeine Nullstelle

$$\{t^3,\ t^4,\ t^5\}$$

hat.

2. Das Ideal in $\mathsf{K}[x_1, x_2, x_3]$

$$(x_1^2 + x_2^2 - x_3^2,\ x_1^2 - x_2^2 + 1)$$

ist prim mit der allgemeinen Nullstelle

$$\left\{\frac{1-t^2}{2t},\ \frac{1+t^2}{2t},\ \frac{\sqrt{2(1+t^2)}}{2t}\right\}.$$

3. Das Ideal in $\mathsf{K}[x_1, x_2, x_3, x_4]$

$$(x_1 x_4 - x_2 x_3,\ x_2^3 - x_1^2 x_3,\ x_3^3 - x_2 x_4^2,\ x_2^2 x_4 - x_1 x_3^2)$$

ist prim mit der allgemeinen Nullstelle

$$\{t_1^4,\ t_1^3 t_2,\ t_1 t_2^3,\ t_2^4\}.$$

4. Ist $\mathfrak{p}$ ein Primideal in $\mathsf{K}[x_1, \ldots, x_n]$ mit der allgemeinen Nullstelle $\{\xi_1, \ldots, \xi_n\}$, so ist das zugehörige H-Ideal $\mathfrak{p}^*$ in $\mathsf{K}[x_0, \ldots, x_n]$ (vgl. § 87, Schluß) prim mit der allgemeinen Nullstelle $\{\lambda, \lambda\xi_1, \ldots, \lambda\xi_n\}$, wo λ eine Unbestimmte ist.

§ 90. Die Dimensionszahl.

Es seien $\xi_1, \ldots, \xi_n$ algebraische Funktionen von $t_1, \ldots, t_r$. Der Transzendenzgrad s des Systems $\{\xi_1, \ldots, \xi_n\}$ (vgl. § 62) ist dann $\leqq r$. Genau gleich r ist der Transzendenzgrad dann, wenn die $t_1, \ldots, t_r$ auch umgekehrt algebraisch von den ξ abhängen, insbesondere, wenn

die t dem Körper $\mathsf{K}(\xi_1, \ldots, \xi_n)$ angehören, und noch spezieller dann, wenn für $t_1, \ldots, t_r$ einfach $r = s$ algebraisch-unabhängige unter den ξ, etwa $\xi_1, \ldots, \xi_s$ gewählt werden. Für die Parameterdarstellung einer algebraischen Mannigfaltigkeit $\mathfrak{M}$ hat es vielfach Vorteile, die Parameter $t_1, \ldots, t_r$ im Körper $\mathsf{K}(\xi_1, \ldots, \xi_n)$ zu wählen, weil die Parameter dann als Funktionen auf der Mannigfaltigkeit $\mathfrak{M}$ gedeutet werden können und nicht etwa fremd hinzukommende sind. Ist die Anzahl r der Parameter größer als der Transzendenzgrad s, so hat man *„überzählige Parameter"*. Die kleinste Anzahl der Parameter, mit der man auskommt, ist genau s. Diese Anzahl heißt die *Dimensionszahl der Mannigfaltigkeit* $\mathfrak{M}$ oder die *Dimensionszahl des zugehörigen Primideals* $\mathfrak{p}$. Demnach ist die Dimensionszahl eines vom Einheitsideal verschiedenen Primideals nichts anderes als der Transzendenzgrad seiner allgemeinen Nullstelle ξ.

Die Dimensionszahl der Primideale $\mathfrak{p} \neq \mathfrak{o}$ variiert offenbar von 0 bis n. Dem Einheitsideal $\mathfrak{o}$, das keine Nullstelle hat, geben wir die Dimensionszahl -1.

Ist ξ die allgemeine Nullstelle eines Primideals $\mathfrak{p}$, ξ' eine beliebige Nullstelle desselben Ideals, so kann man jedem Polynom $f(\xi)$ aus $\mathsf{K}[\xi]$ das Polynom $f(\xi')$ aus $\mathsf{K}[\xi']$ zuordnen. Da aus $f(\xi) = g(\xi)$ folgt $f(x) \equiv g(x)\ (\mathfrak{p})$, und daraus $f(\xi') = g(\xi')$, so ist die Zuordnung $f(\xi) \to f(\xi')$ eindeutig. Da die Zuordnung offenbar Summen in Summen und Produkte in Produkte überführt, so ist sie ein *Homomorphismus*:

$$\mathsf{K}[\xi] \sim \mathsf{K}[\xi']. \tag{1}$$

Wenn die Zuordnung ein Isomorphismus ist, so ist natürlich auch ξ' eine allgemeine Nullstelle von $\mathfrak{p}$, und umgekehrt.

Bei einem nulldimensionalen Ideal $\mathfrak{p}$ sind alle ξ algebraisch über K; mithin sind alle rationalen Funktionen der ξ schon ganzrational: $\mathsf{K}(\xi) = \mathsf{K}[\xi]$. Daher ist $\mathsf{K}[\xi]$ ein *Körper*. Ist dann wieder ξ' eine beliebige Nullstelle, so muß der Homomorphismus (1) notwendig ein Isomorphismus sein; denn ein Körper hat keine anderen Homomorphismen als eineindeutige und solche, die ihn auf den Nullring abbilden. Demnach gilt der Satz:

Bei einem nulldimensionalen Primideal sind alle Nullstellen allgemein und untereinander äquivalent[1].

Die Koordinaten $\xi_1, \ldots, \xi_n$ oder $\xi'_1, \ldots, \xi'_n$ sind in diesem Falle algebraische Größen (der Transzendenzgrad ist ja Null). Denkt man sich alle Nullstellen in einem gemeinsamen (etwa algebraisch-abgeschlossenen) Umfassungskörper Ω, so sind sie nach (1) algebraisch konjugiert. Die Anzahl dieser konjugierten Punkte in einem passenden Körper Ω ist höchstens gleich (und, wenn $\mathsf{K}(\xi)$ separabel ist, genau gleich) dem Körpergrad von $\mathsf{K}(\xi)$ über K. Also:

[1] D. h. sie gehen auseinander durch Isomorphismen hervor, die den Grundkörper K fest lassen.

Eine nulldimensionale irreduzible algebraische Mannigfaltigkeit besteht aus endlichvielen algebraisch konjugierten Punkten.

Ist insbesondere der Körper K schon algebraisch-abgeschlossen, so gibt es nur eine Nullstelle ξ im Körper K selbst, und das zugehörige Ideal ist

$$\mathfrak{p} = (x_1 - \xi_1, \ldots, x_n - \xi_n).$$

Satz. *Die verschiedenen Nullstellen eines r-dimensionalen Primideals haben einen Transzendenzgrad $\leqq r$, und wenn der Transzendenzgrad einer Nullstelle genau r ist, ist die Nullstelle allgemein.*

Beweis: Ist ξ' eine Nullstelle, vom Transzendenzgrad s, so besteht die Homomorphie (1). Sind $\xi'_1, \ldots, \xi'_s$ algebraisch-unabhängig, so sind $\xi_1, \ldots, \xi_s$ es auch; denn jede algebraische Relation zwischen den ξ würde dieselbe zwischen den ξ' nach sich ziehen. Daraus folgt $r \geqq s$. Ist $r = s$, so hängen alle ξ algebraisch von $\xi_1, \ldots, \xi_s$ ab. Ginge bei der Homomorphie (1) ein Polynom $f(\xi)$, das selbst nicht Null ist, in Null über, so könnte man im Körper $\mathsf{K}(\xi)$ das Element $\frac{1}{f}$ in folgender speziellen Form schreiben:

$$\frac{1}{f(\xi_1, \ldots, \xi_n)} = \frac{g(\xi_1, \ldots, \xi_n)}{h(\xi_1, \ldots, \xi_s)}.$$

Daraus würde folgen

$$h(\xi_1, \ldots, \xi_s) = g(\xi_1, \ldots, \xi_n) f(\xi_1, \ldots, \xi_n).$$

Bei der Homomorphie (1) ginge f in 0 über; also müßte auch $h(\xi_1, \ldots, \xi_s)$ in 0 übergehen, d. h. man hätte

$$h(\xi'_1, \ldots, \xi'_s) = 0,$$

entgegen der vorausgesetzten algebraischen Unabhängigkeit von $\xi'_1, \ldots, \xi'_s$. Also geht bei der Homomorphie (1) kein von Null verschiedenes Polynom in Null über; (1) ist also im Falle $r = s$ eine Isomorphie. Daraus folgt die Behauptung, daß ξ' eine allgemeine Nullstelle ist.

Jede Nullstelle ξ' von $\mathfrak{p}$ kann als allgemeine Nullstelle eines Ideals $\mathfrak{p}'$ aufgefaßt werden. Aus $f \equiv 0\,(\mathfrak{p})$ folgt dann $f(\xi') = 0$ oder $f \equiv 0\,(\mathfrak{p}')$; mithin ist $\mathfrak{p}'$ ein Teiler von $\mathfrak{p}$. Umgekehrt kann jeder von $\mathfrak{o}$ verschiedene Primteiler $\mathfrak{p}'$ von $\mathfrak{p}$ in dieser Weise erhalten werden; denn jedes Ideal $\mathfrak{p}' \neq \mathfrak{o}$ besitzt eine allgemeine Nullstelle ξ'. Aus dem eben formulierten Satz folgt nun unmittelbar:

Jeder Teiler $\mathfrak{p}'$ von $\mathfrak{p}$ hat eine Dimension $r' \leqq r$; ist $r' = r$, so muß $\mathfrak{p}' = \mathfrak{p}$ sein.

Unter der Dimensionszahl einer beliebigen algebraischen Mannigfaltigkeit verstehen wir die höchste unter den Dimensionszahlen ihrer irreduziblen Bestandteile. Die rein eindimensionalen algebraischen Mannigfaltigkeiten heißen *Kurven*, die rein zweidimensionalen *Flächen*, die rein $(n-1)$-dimensionalen *Hyperflächen*. Die einzige n-dimensionale

Mannigfaltigkeit im R_n ist der ganze Raum R_n, das zugehörige Ideal ist das Nullideal (denn wenn $\xi_1, \ldots, \xi_n$ algebraisch-unabhängig sind, folgt aus $f(\xi) = 0$, daß $f = 0$ ist).

Aufgaben. 1. Ein Hauptideal (p), wo p ein unzerlegbares nichtkonstantes Polynom ist, ist ein $(n-1)$-dimensionales Primideal.

2. Umgekehrt: jedes $(n-1)$-dimensionale Primideal ist Hauptideal.

3. Jedes d-dimensionale Primideal $\mathfrak{p}$ $(d > 0)$ besitzt (mindestens) einen $(d-1)$-dimensionalen Primidealteiler. [Wenn $\xi_{d+1}, \ldots, \xi_n$ algebraische Funktionen von $\xi_1, \ldots, \xi_d$ sind, so bilde man eine spezielle Nullstelle von $\mathfrak{p}$ durch Spezialisierung von ξ_d nach § 88, während $\xi_1, \ldots, \xi_{d-1}$ unbestimmt bleiben.]

Geht man vom offenen Raum R_n zum projektiven Raum P_n über, so entspricht nach § 87 jeder irreduziblen Mannigfaltigkeit $\mathfrak{M}$ von R_n (mit zugehörigem Primideal $\mathfrak{p}$) eine ebensolche $\mathfrak{M}^*$ in P_n (mit zugehörigem Primideal $\mathfrak{p}^*$). Ist d die Dimensionszahl von $\mathfrak{p}$, so ist die von $\mathfrak{p}^*$ gleich $d+1$, da ein unbestimmter Proportionalitätsfaktor λ den Transzendenzgrad der allgemeinen Nullstelle um Eins erhöht (vgl. § 89, Aufg. 4). Als Dimensionszahl von $\mathfrak{M}^*$ bezeichnet man aber die Zahl d (nicht $d+1$), aus dem geometrisch naheliegenden Grunde, daß $\mathfrak{M}^*$, von den hinzugekommenen uneigentlichen Punkten abgesehen, mit $\mathfrak{M}$ zusammenfällt. Ist etwa $\mathfrak{M}$ eine Kurve, so wird man das Gebilde $\mathfrak{M}^*$, das aus $\mathfrak{M}$ durch Hinzufügung endlichvieler Punkte entsteht, ebenfalls eine Kurve nennen. Unter der Dimensionszahl einer Mannigfaltigkeit im projektiven Raum versteht man also immer die um 1 verringerte Dimensionszahl des zugehörigen Primideals.

§ 91. Die Primärideale.

Das Hauptproblem der Idealtheorie in Polynombereichen lautet: *Zu entscheiden, ob ein Polynom f einem gegebenen Ideal*

$$\mathfrak{m} = (f_1, \ldots, f_r)$$

angehört.

Unter Entscheiden wird aber hier nicht eine rechnerische Entscheidung mit endlichvielen wirklich ausführbaren Rechenoperationen verstanden, obzwar auch eine solche stets möglich ist[1], sondern eine solche Methode, die zugleich einen Einblick in die Struktur des Ideals gibt und die geometrischen Relationen zwischen den Nullstellen des Ideals und seinen Elementen f möglichst klar zum Ausdruck bringt. Eine solche Methode ist von E. LASKER[2] zuerst angegeben; sie operiert mit der Zerlegung der Ideale in Primärkomponenten.

Der Grundgedanke der Laskerschen Methode ist folgender: Nach dem Zerlegungssatz von § 83 ist jedes Ideal $\mathfrak{m}$ als Durchschnitt von

[1] Vgl. J. KÖNIG: Einleitung in die allgemeine Theorie der algebraischen Größen (B. G. Teubner, Leipzig 1903), sowie G. HERMANN: Die Frage der endlichvielen Schritte in der Theorie der Polynomideale, Math. Ann. Bd. 95, S. 736—788.

[2] LASKER, E.: Zur Theorie der Moduln und Ideale, Math. Ann. Bd. 60, S. 20 bis 116. 1905.

Primäridealen darstellbar:

$$\mathfrak{m} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_s].$$

Damit also ein Polynom f dem Ideal $\mathfrak{m}$ angehört, ist notwendig und hinreichend, daß f allen Primäridealen $\mathfrak{q}_\nu$ angehört. Um die obige Aufgabe im Prinzip zu lösen, braucht man also nur die Bedingungen aufzustellen, denen ein Polynom genügen muß, um einem Primärideal anzugehören.

Zu jedem Primärideal $\mathfrak{q}$ gehören nach § 82 ein Primideal $\mathfrak{p}$ und ein „Exponent" ϱ mit folgenden Eigenschaften:

1. $\mathfrak{p}^\varrho \equiv 0(\mathfrak{q}) \equiv 0(\mathfrak{p})$.
2. Aus $fg \equiv 0(\mathfrak{q})$ und $f \not\equiv 0(\mathfrak{p})$ folgt $g \equiv 0(\mathfrak{q})$.

Das Primideal $\mathfrak{p}$ gehört im Falle $\mathfrak{q} \neq \mathfrak{o}$ wiederum zu einer irreduziblen Mannigfaltigkeit $\mathfrak{M}$. Nach 1. sind alle Nullstellen von $\mathfrak{q}$ zugleich Nullstellen von $\mathfrak{p}$ und umgekehrt. *Also ist die Mannigfaltigkeit eines Primärideals $\mathfrak{q} \neq \mathfrak{o}$ irreduzibel und gleich der Mannigfaltigkeit des zugehörigen Primideals.*

Vermöge des Zerlegungssatzes folgt daraus für ein beliebiges Ideal $\mathfrak{m}$, daß seine Mannigfaltigkeit eine Vereinigung irreduzibler Mannigfaltigkeiten, nämlich der Mannigfaltigkeiten seiner Primärkomponenten, ist. Mithin:

Jede algebraische Mannigfaltigkeit ist als Vereinigung endlich vieler irreduzibler Mannigfaltigkeiten darstellbar.

Die irreduziblen Mannigfaltigkeiten der Primärkomponenten von $\mathfrak{m}$ sind schon durch die zugehörigen Primideale bestimmt. Dabei können die „eingebetteten" Primideale (§ 84) weggelassen werden, da ihre Mannigfaltigkeiten in den Mannigfaltigkeiten der nichteingebetteten („*isolierten*") Primideale enthalten sind[1]. Da die zugehörigen Primideale in ihrer Gesamtheit eindeutig bestimmt sind, so folgt, daß auch *die Zerlegung einer algebraischen Mannigfaltigkeit in irreduzible eindeutig bestimmt ist.*

Es sei $\mathfrak{q}$ ein Primärideal zum Primideal $\mathfrak{p}$ und vom Exponenten ϱ, und $\mathfrak{M}$ sei seine Mannigfaltigkeit. Ist nun f ein Polynom, das $\mathfrak{M}$ enthält, so ist $f \equiv 0(\mathfrak{p})$, also $f^\varrho \equiv 0(\mathfrak{q})$. Wenn aber f nicht $\mathfrak{M}$ enthält, so kann man nach der obigen Eigenschaft 2 in jeder Kongruenz modulo $\mathfrak{q}$ den Faktor f wegheben. Das sind schon zwei sehr wichtige Mittel, durch die man häufig eine Kongruenz $f^\varrho \equiv 0(\mathfrak{q})$ bzw. $g \equiv 0(\mathfrak{q})$ erschließen kann. Sie lassen sich mit Hilfe des Zerlegungssatzes sofort auf beliebige Ideale $\mathfrak{m} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_s]$ übertragen. Ist nämlich f ein Polynom, das die Mannigfaltigkeit $\mathfrak{M}$ von $\mathfrak{m}$ enthält, und ist ϱ der größte der Exponenten der Primärideale $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$, so folgt sofort

$$f^\varrho \equiv 0(\mathfrak{q}_i) \qquad (\text{für } i = 1, \ldots, s),$$

mithin

$$f^\varrho \equiv 0(\mathfrak{m}).$$

[1] Von diesem Sachverhalt rührt auch das Wort „eingebettet" her.

Damit ist der *Hilbertsche Nullstellensatz* (§ 75) von neuem bewiesen, und zwar mit der Verschärfung, daß der Exponent ϱ nur vom Ideal $\mathfrak{m}$ abhängt.

Ist andererseits f ein Polynom, das keine der Mannigfaltigkeiten der Primärideale $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$ enthält, so kann man in jeder Kongruenz

$$fg \equiv 0 (\mathfrak{m})$$

durch f kürzen und auf

$$g \equiv 0 (\mathfrak{m})$$

schließen, da das Entsprechende ja für alle Primärideale $\mathfrak{q}_\nu$ gilt. Man kann die Kürzungsmöglichkeit auch kurz und prägnant durch die Gleichung

$$\mathfrak{m} : (f) = \mathfrak{m}$$

zum Ausdruck bringen, die nach § 84 ebenfalls dann und nur dann gilt, wenn f durch keines der zu $\mathfrak{m}$ gehörigen Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ teilbar ist (also keine ihrer irreduziblen Mannigfaltigkeiten enthält). Etwas allgemeiner gilt sogar nach § 84 für ein beliebiges Ideal $\mathfrak{a}$, daß

$$\mathfrak{m} : \mathfrak{a} = \mathfrak{m} \tag{1}$$

dann und nur dann, wenn $\mathfrak{a}$ durch alle $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ unteilbar ist, oder, was wieder dasselbe ist, *wenn die Mannigfaltigkeit von* $\mathfrak{a}$ *keine der Mannigfaltigkeiten der Primideale* $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$ *enthält.* Dieser Satz ist oft nützlich beim Aufsuchen der zu einem gegebenen Ideal $\mathfrak{m}$ gehörigen Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_s$. Wenn man nämlich von irgendeinem Primideal $\mathfrak{p}$ vermutet, daß es sich unter den $\mathfrak{p}_\nu$ befindet, so nimmt man ein durch $\mathfrak{p}$ teilbares Ideal $\mathfrak{a}$, z. B. $\mathfrak{a} = \mathfrak{p}$, und sieht nach, ob man die Relation (1) oder deren Negation beweisen kann, d. h. ob aus $g\mathfrak{a} \equiv 0 (\mathfrak{m})$ folgt $g \equiv 0 (\mathfrak{m})$ oder nicht. Wenn (1) gilt, so ist $\mathfrak{p}$ kein $\mathfrak{p}_\nu$. Mit dieser Methode werden wir z. B. in § 95 beweisen, daß die zugehörigen Primideale eines Ideals mit r Basiselementen, wenn ihre Dimensionen den Wert $n - r$ nicht überschreiten, alle genau die Dimension $n - r$ haben (und daher nicht eingebettet sind).

Unter der *Dimensionszahl* eines Primärideals versteht man die Dimensionszahl des zugehörigen Primideals (oder die Dimensionszahl der Nullstellenmannigfaltigkeit). Unter der Dimensionszahl oder *Höchstdimension* eines beliebigen Ideals $\mathfrak{a} \neq \mathfrak{o}$ versteht man die höchste der Dimensionszahlen der Primärkomponenten (oder der zugehörigen Primideale). Dieselbe Zahl stellt auch die Dimensionszahl der Mannigfaltigkeit von $\mathfrak{a}$ dar.

Sind die Dimensionszahlen der zu $\mathfrak{a}$ gehörigen Primärideale alle gleich, etwa gleich d, so heißt das Ideal $\mathfrak{a}$ *ungemischt d-dimensional.*

Aufgaben. 1. Das Ideal $(x_1^2, x_2 x_3 + 1)$ ist primär, mit dem Exponenten 2 und dem zugehörigen Primideal $(x_1, x_2 x_3 + 1)$.

2. Jede Potenz p^ϱ eines unzerlegbaren nichtkonstanten Polynoms p erzeugt ein $(n-1)$-dimensionales Primärideal. Jedes nichtkonstante Polynom f erzeugt ein ungemischtes $(n-1)$-dimensionales Ideal.

3. Ist $\mathfrak{p}$ das Primideal von § 89, Aufg. 1, so ist $\mathfrak{p}^2$ nicht primär. [Das Polynom $(x_2x_3 - x_1^3)^2 - (x_2^2 - x_1x_3)(x_3^2 - x_1^2x_2)$ spaltet einen Faktor x_1 ab, und der andere Faktor gehört nicht zu $\mathfrak{p}^2$.]

§ 92. Der Noethersche Satz.

Mit den Hilfsmitteln der Primärideal-Zerlegung werden wir das Problem, welche Bedingungen ein Polynom f zu erfüllen hat, um einem Ideal $\mathfrak{m}$ anzugehören, im Falle nulldimensionaler Ideale vollständig lösen. Wir schicken einen *Hilfssatz* voraus, der auch sonst nützlich ist:

Ist Σ ein Erweiterungskörper von K und sind $f, f_1, \ldots, f_r$ Polynome aus $\mathsf{K}[x] = \mathsf{K}[x_1, \ldots, x_n]$, so folgt aus

$$f \equiv 0\,(f_1, \ldots, f_r) \quad \text{in } \Sigma[x],$$

daß

$$f \equiv 0\,(f_1, \ldots, f_r) \quad \text{in } \mathsf{K}[x]$$

ist.

Beweis: Es sei

$$f = \sum g_i f_i, \tag{1}$$

wo die g_i Polynome mit Koeffizienten aus Σ sind. Man drücke diese Koeffizienten durch endlichviele linear-unabhängige Elemente $1, \omega_1, \omega_2, \ldots$ von Σ mit Koeffizienten aus K linear aus. Jeder Term $g_i f_i$ in (1) erhält dann die Form

$$(g_{i0} + g_{i1}\omega_1 + g_{i2}\omega_2 + \cdots) f_i,$$

wo die g_{ik} Polynome mit Koeffizienten aus K sind. Aus (1) folgt also

$$f = \sum g_{i0} f_i + \omega_1 \sum g_{i1} f_i + \omega_2 \sum g_{i2} f_i + \cdots$$

oder, da die Körperelemente $1, \omega_1, \omega_2, \ldots$ linear-unabhängig waren, also die Glieder mit $1, \omega_1, \omega_2, \ldots$ links und rechts einzeln übereinstimmen müssen,

$$f = \sum g_{i0} f_i, \qquad \text{q. e. d.}$$

Auf Grund dieses Hilfssatzes können wir zur Beantwortung der Frage, ob $f \equiv 0\,(f_1, \ldots, f_r)$ ist, den Grundkörper K stets beliebig erweitern, so z. B. durch Adjunktion von Nullstellen des Ideals $(f_1, \ldots, f_r)$. Gilt die fragliche Kongruenz im erweiterten Bereich $\Sigma[x]$, so gilt sie auch vor der Erweiterung.

Eine nulldimensionale algebraische Mannigfaltigkeit zerfällt bei passender Erweiterung des Grundkörpers immer in lauter einzelne Punkte; also können wir, wenn es vorteilhaft ist, immer annehmen, daß alle auftretenden nulldimensionalen Primideale je nur einen Punkt zur

Nullstelle haben (nicht, wie sonst immer, ein System konjugierter Punkte).

Ein nulldimensionales Primideal $\mathfrak{p}$ ist teilerlos; denn der Restklassenring $\mathfrak{o}/\mathfrak{p}$ ist nach § 90 ein Körper. Daraus folgt, daß jedes nulldimensionale Primärideal einartig ist; denn ein Primärideal, dessen zugehöriges Primideal teilerlos ist, ist nach § 86 stets einartig. Weiter folgt aus den Sätzen des § 86, daß jede nulldimensionale isolierte Primärkomponente $\mathfrak{q}$ eines Ideals $\mathfrak{m}$ sich durch

$$\mathfrak{q} = (\mathfrak{m}, \mathfrak{p}^{\varrho}) \tag{2}$$

darstellen läßt. Der Exponent ϱ ist dabei die kleinste Zahl σ mit der Eigenschaft

$$\mathfrak{p}^{\sigma} \equiv 0\,(\mathfrak{m}, \mathfrak{p}^{\sigma+1}). \tag{3}$$

Machen wir uns die Bedeutung der Relation (2) einmal klar im Falle, daß der Grundkörper vorher so erweitert wird, daß die in Betracht kommenden einartigen Ideale $\mathfrak{q}$ je nur eine Nullstelle $a = \{a_1, \ldots, a_n\}$ haben. (2) besagt, daß für $f \equiv 0\,(\mathfrak{q})$ notwendig und hinreichend ist

$$f \equiv 0\,(\mathfrak{m}, \mathfrak{p}^{\varrho}). \tag{4}$$

Ist nun $\mathfrak{m}$ durch eine Basis $(f_1, \ldots, f_r)$ gegeben und setzen wir $y_\nu = x_\nu - a_\nu$, so ist $\mathfrak{p} = (y_1, \ldots, y_n)$. Denken wir uns alle auftretenden Polynome nach aufsteigenden Potenzen der y_ν geordnet, so besteht $\mathfrak{p}^{\varrho}$ aus allen denjenigen Polynomen, die nur Potenzprodukte der y_ν vom Grade $\geqq \varrho$ enthalten. Die Relation (4) bedeutet also, daß f mit einer Linearkombination $\sum g_\nu f_\nu$ übereinstimmt bis auf Glieder vom Grade ϱ und höhere Glieder. Denkt man sich also $f_1, \ldots, f_r$ multipliziert mit 1 und mit allen Potenzprodukten der y_ν vom Grade $< \varrho$ und bezeichnet man die so entstehenden Polynome unter Weglassung aller Glieder vom Grade $\geqq \varrho$ mit $h_1, \ldots, h_k$, so besagt (4), daß f bis auf Glieder vom Grade $\geqq \varrho$ einer Linearkombination von $h_1, \ldots, h_k$ mit konstanten Koeffizienten gleich ist. Das ist ein Sachverhalt, dessen Bestehen oder Nichtbestehen man in jedem vorliegenden Fall (bei gegebenen $\varrho, f_1, \ldots, f_r$ und f) wirklich feststellen kann. Insbesondere besteht er dann, wenn es formale Potenzreihen $P_1(y), \ldots, P_r(y)$ gibt[1] derart, daß

$$f = P_1 f_1 + \cdots + P_r f_r \tag{5}$$

ist[2]. Man kann dann nämlich für jeden Wert von σ diese Potenzreihen bei den Gliedern vom Grade σ abbrechen und die Übereinstimmung der beiden Seiten mod $\mathfrak{p}^{\sigma}$ konstatieren. Das Potenzreihenkriterium (5) verlangt also eigentlich noch zu viel: die beiden Seiten von (5) brauchen

[1] Über deren Konvergenz natürlich nichts vorausgesetzt wird.

[2] Gemeint ist, daß bei formaler Entwicklung nach Potenzprodukten der y_ν die beiden Seiten von (5) übereinstimmen.

nicht genau, sondern nur bis auf Glieder vom Grade $\geqq \varrho$ übereinzustimmen.

Ebenso ist die Gültigkeit oder Nichtgültigkeit der Relation (3) für jedes σ feststellbar: sie bedeutet, daß durch die Polynome $\sum g_\nu f_\nu$ unter Weglassung der Potenzprodukte vom Grade $> \sigma$ alle Potenzprodukte vom Grade σ darstellbar sind. Man kann also bei gegebenen $f_1, \ldots, f_r$ für jede Nullstelle a die Werte $\sigma = 1, 2, 3, \ldots$ der Reihe nach durchprobieren, bis man ein σ gefunden hat, für welches (3) gilt: dieses σ ist dann der Exponent von $\mathfrak{q}$.

Bei einem nulldimensionalen Ideal $\mathfrak{m}$ sind alle Primärkomponenten nulldimensional und isoliert; man kann also für *alle* das obige Kriterium für $f \equiv 0\,(\mathfrak{q})$ anwenden. Ist es für alle Nullstellen erfüllt, so folgt $f \equiv 0\,(\mathfrak{m})$. Demnach gilt folgender Satz:

Bestimmt man für jede Nullstelle $a = \{a_1, \ldots, a_n\}$ *eines nulldimensionalen Ideals* $\mathfrak{m}$ *den Exponenten* ϱ *als die kleinste natürliche Zahl* σ, *für die* (3) *mit* $\mathfrak{p} = (x_1 - a_1, \ldots, x_n - a_n)$ *gilt, und genügt ein Polynom* f *für alle diese* $\mathfrak{p}$ *der Bedingung* (4), *so ist* $f \equiv 0\,(\mathfrak{m})$.

Dieser Satz wurde für den Fall $\mathfrak{m} = (f_1, f_2)$, wo f_1 und f_2 Polynome in zwei Variablen sind, zuerst von MAX NOETHER ausgesprochen[1]: das war der berühmte „*Noethersche Fundamentalsatz*", der die Grundlage für die „geometrische Richtung" in der Theorie der algebraischen Funktionen bildete. NOETHER setzte allerdings statt der schwächeren Relation (4) die Potenzreihenbedingung (5) als in allen Nullstellen erfüllt voraus. Die hier gegebene Fassung, bei der nur die Übereinstimmung der Glieder bis zum Grade $\varrho - 1$ in $y_1, \ldots, y_n$ verlangt wird, stammt von BERTINI[2], der zugleich für den Exponenten ϱ eine Schranke gegeben hat[3]. Die n-dimensionale Verallgemeinerung stammt von LASKER und MACAULAY. Die für $f \equiv 0\,(\mathfrak{q})$ hinreichende Bedingung $f \equiv 0\,(\mathfrak{m}, \mathfrak{p}^\varrho)$ nennen wir nach MACAULAY die *Noethersche Bedingung im Punkte a.*

§ 93. Spezialfälle und Anwendungen des Noetherschen Satzes.

Jedes der Polynome $f_1, \ldots, f_r$, welche die Basis des Ideals $(f_1, \ldots, f_r)$ bilden, bestimmt für sich eine algebraische Mannigfaltigkeit (Hyperfläche) $f_\nu = 0$ im n-dimensionalen Raum. Ebenso bestimmt das Polynom f eine Hyperfläche $f = 0$. Zerfällt f in irreduzible Faktoren: $f = p_1^{\varrho_1} p_2^{\varrho_2} \ldots$, so zerfällt auch die Mannigfaltigkeit $f = 0$ in

[1] NOETHER, M.: Über einen Satz aus der Theorie der algebraischen Funktionen, Math. Ann. Bd. 6, S. 351–359. 1873.

[2] BERTINI, E.: Zum Fundamentalsatz aus der Theorie der algebraischen Funktionen, Math. Ann. Bd. 34, S. 447–449. 1889.

[3] Schärfere Schranken bringt P. DUBREIL: Thèse de Doctorat, Paris 1930. Vgl. auch H. KAPFERER: Notwendige und hinreichende Multiplizitätsbedingungen zum Noetherschen Fundamentalsatz, Sitzungsber. der Heidelberger Akademie 1927, 8. Abhandlung.

irreduzible Teile $p_1 = 0, p_2 = 0, \ldots$, welche wir je so oft zählen wollen, als der betreffende Exponent in der Zerlegung von f angibt.

Wird f für eine Stelle a nach Potenzen der $y_\nu = x_\nu - a_\nu$ entwickelt und fängt die Entwicklung mit den Gliedern s-ter Ordnung ($s \geqq 0$) an:

$$f = c_0 y_1^s + c_1 y_1^{s-1} y_2 + \cdots + c_\omega y_n^s + \cdots,$$

so sagt man, die Hyperfläche $f = 0$ *habe in a einen s-fachen Punkt.* Die Glieder s-ter Ordnung $c_0 y_1^s + \cdots + c_\omega y_n^s$ für sich ergeben, gleich Null gesetzt, eine Hyperfläche, die aus lauter „geraden Linien" durch a besteht: den *Tangentialkegel* der Hyperfläche $f = 0$ im Punkte a.

Der einfachste Fall des Noetherschen Satzes ist der, daß unter den Hyperflächen $f_1 = 0, \ldots, f_r = 0$, die das nulldimensionale Ideal $\mathfrak{m}$ bestimmen, solche $f_1 = 0, \ldots, f_n = 0$ vorkommen, die in a alle einen einfachen Punkt haben und deren Tangentialhyperebenen nur den Punkt a gemein haben:

$$\begin{aligned} f_1 &= c_{11} y_1 + \cdots + c_{1n} y_n + \cdots, \\ f_2 &= c_{21} y_1 + \cdots + c_{2n} y_n + \cdots, \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ f_n &= c_{n1} y_1 + \cdots + c_{nn} y_n + \cdots; \end{aligned}$$

$$\text{Linearformen } \sum_{\mu=1}^{n} c_{\lambda\mu} y_\mu \text{ linear-unabhängig.}$$

In diesem Fall kommen, wenn das Primideal $(x_1 - a_1, \ldots, x_n - a_n)$ mit $\mathfrak{p}$ bezeichnet wird, unter den Linearkombinationen von $f_1, \ldots, f_n$ modulo $\mathfrak{p}^2$ (d. h. unter Vernachlässigung der Glieder zweiten und höheren Grades) auch $y_1, \ldots, y_n$ selber vor; d. h. es ist

$$(y_1, \ldots, y_n) \equiv 0 \,((f_1, \ldots, f_n), \mathfrak{p}^2)$$

und daher auch

$$\mathfrak{p} \equiv 0 \,(\mathfrak{m}, \mathfrak{p}^2).$$

Daraus folgt: Das Ideal $\mathfrak{m}$ hat im Punkte a eine isolierte Primärkomponente $\mathfrak{q}$ vom Exponenten 1, d. h. es ist $\mathfrak{q} = \mathfrak{p}$. Jedes Polynom mit der Nullstelle a ist also durch $\mathfrak{q}$ teilbar. Sind alle Nullstellen a von $\mathfrak{m}$ solche „einfachen Schnittpunkte", so ist für $f \equiv 0 \,(\mathfrak{m})$ hinreichend, daß f alle diese Nullstellen enthält.

Bei der Diskussion komplizierterer Fälle beschränken wir uns auf zwei Veränderliche x_1, x_2 und auf solche Ideale $\mathfrak{m}$, die von zwei teilerfremden Polynomen f_1, f_2 erzeugt werden. Da f_1 und f_2 als Polynome in x_2 teilerfremd sind, besteht eine Relation

$$1 = g_1 f_1 + g_2 f_2,$$

wo g_1 und g_2 rational in x_1, ganzrational in x_2 sind. Macht man beide Seiten durch Multiplikation mit einem von Null verschiedenen Polynom $h(x_1)$ ganzrational in x_1, so folgt

$$h(x_1) \equiv 0 \,(f_1, f_2).$$

Für die Nullstellen von (f_1, f_2) kommen also nur endlich viele Werte von x_1 und ebenso nur endlich viele Werte von x_2 in Frage: es gibt nur endlichviele Nullstellen a.[1] Adjungiert man deren Koordinaten dem Grundkörper, so gehört zu jeder Nullstelle a eine isolierte Primärkomponente $\mathfrak{q}$ von $\mathfrak{m} = (f_1, f_2)$, zum Primideal $\mathfrak{p} = (y_1, y_2) = (x_1 - a_1, x_2 - a_2)$.

Den einfachsten Fall, daß der Punkt a für die beiden Kurven $f_1 = 0$ und $f_2 = 0$ einfach ist und die Tangenten verschieden sind, haben wir oben schon behandelt: es ergab sich $\varrho = 1$ und $\mathfrak{q} = \mathfrak{p}$. Der nächst einfache Fall ist der, daß der Punkt a ein r-facher Punkt für $f_1 = 0$ und ein s-facher Punkt für $f_2 = 0$ ist, aber die r Tangenten von $f_1 = 0$ von den s Tangenten von $f_2 = 0$ verschieden sind. Setzen wir

$$f_1 = c_0 y_1^r + c_1 y_1^{r-1} y_2 + \cdots + c_r y_2^r + \cdots,$$
$$f_2 = d_0 y_1^s + d_1 y_1^{s-1} y_2 + \cdots + d_s y_2^s + \cdots,$$

so werden die Tangenten von f_1 durch die Nullrichtungen der Form $c_0 y_1^r + \cdots + c_r y_2^r$ und die von f_2 durch die der Form $d_0 y_1^s + \cdots + d_s y_2^s$ geliefert. Die Voraussetzung, daß die Nullrichtungen von f_1 von denen von f_2 verschieden sind, drückt sich nach § 71 durch das Nichtverschwinden der Resultante dieser beiden Formen

$$R = \begin{vmatrix} c_0 c_1 \ldots c_r & & \\ & c_0 c_1 \ldots c_r & \\ & \cdots\cdots & \\ d_0 d_1 \ldots d_s & & \\ & d_0 d_1 \ldots d_s & \\ & \cdots\cdots & \end{vmatrix}$$

aus.

Versuchen wir nun, ein σ zu finden, für welches

$$\mathfrak{p}^\sigma \equiv 0 \,((f_1, f_2), \mathfrak{p}^{\sigma+1})$$

ist. Um aus f_1, f_2 und $\mathfrak{p}^{\sigma+1}$ Potenzprodukte der y_ν vom Grade σ zu erhalten, hat man f_1 mit den $\sigma - r + 1$ möglichen Potenzprodukten vom Grade $\sigma - r$ und f_2 mit den $\sigma - s + 1$ möglichen Potenzprodukten vom Grade $\sigma - s$ zu multiplizieren und in den Produkten alle Glieder vom Grade $> \sigma$ zu vernachlässigen. Das ergibt höchstens

$$(\sigma - r + 1) + (\sigma - s + 1) = 2\sigma - r - s + 2$$

linear-unabhängige Ausdrücke. Will man daraus durch Linearkombination alle $\sigma + 1$ Potenzprodukte vom Grade σ erhalten, so muß

$$2\sigma - r - s + 2 \geqq \sigma + 1,$$
$$\sigma \geqq r + s - 1$$

[1] Nach § 79 gibt es sogar höchstens so viele Nullstellen, als das Produkt der Gradzahlen von f_1 und f_2 angibt.

sein. Wählen wir aber $\sigma = r + s - 1$ und schreiben die erhaltenen Ausdrücke hin:

$$\begin{aligned} &c_0 y_1^\sigma + c_1 y_1^{\sigma-1} y_2 + \cdots + c_r y_1^{\sigma-r} y_2^r, \\ &\qquad c_0 y_1^{\sigma-1} y_2 + c_1 y_1^{\sigma-2} y_2^2 + \cdots, \\ &\qquad\qquad \cdots\cdots\cdots\cdots, \\ &d_0 y_1^\sigma + d_1 y_1^{\sigma-1} y_2 + \cdots + d_s y_1^{\sigma-s} y_2^s, \\ &\qquad d_0 y_1^{\sigma-1} y_2 + d_1 y_1^{\sigma-2} y_2^2 + \cdots, \\ &\qquad\qquad \cdots\cdots\cdots\cdots, \end{aligned}$$

so ergibt sich gerade auf Grund der obigen Bedingung $R \neq 0$, daß man genau $\sigma + 1$ linear-unabhängige Ausdrücke erhalten hat, aus denen sich somit alle Potenzprodukte vom Grade σ linear zusammensetzen. Also ist

$$\mathfrak{p}^\sigma \equiv 0\,((f_1, f_2), \mathfrak{p}^{\sigma+1}) \quad \text{mit} \quad \sigma = r + s - 1;$$

mithin: *Der Exponent des Primärideals* $\mathfrak{q}$ *im Falle der getrennten Tangenten ist* $r + s - 1$. Jedes Polynom, das in a von der Ordnung $r + s - 1$ verschwindet, gehört somit zum Ideal $\mathfrak{q}$. Dieses Resultat hat schon M. NOETHER erhalten.

Als nächsten Fall betrachten wir den, daß die Kurve $f_1 = 0$ in a einen einfachen Punkt hat, während $f_2 = 0$ ganz beliebig sein darf. Es sei also

$$f_1 = a_1 y_1 + a_2 y_2 + \cdots$$

und etwa $a_1 \neq 0$. Vernachlässigt man alle diejenigen Potenzprodukte, deren Grad mindestens $\sigma + 1$ beträgt, so ist es klar, daß man jedes Polynom f durch Subtraktion eines Vielfachen des Polynoms f_1 gänzlich von y_1 befreien kann. Man verfährt einfach so: Zuerst entfernt man durch Subtraktion eines Vielfachen des Polynoms f_1 die Glieder mit der ersten Potenz von y_1, sodann durch Subtraktion eines Vielfachen des Polynoms $y_1 f_1$ die Glieder mit y_1^2 usw. bis zu den Gliedern mit y_1^σ. Wendet man das Verfahren einmal auf ein beliebiges Polynom f, das andere Mal auf f_2 an, so findet man etwa

$$(1) \qquad f - g f_1 \equiv c_0 + c_1 y_2 + c_2 y_2^2 + \cdots + c_\sigma y_2^\sigma \ (\mathfrak{p}^{\sigma+1}),$$

$$(2) \qquad f_2 - h f_1 \equiv d_0 + d_1 y_2 + d_2 y_2^2 + \cdots + d_\sigma y_2^\sigma \ (\mathfrak{p}^{\sigma+1}).$$

Die nach diesem Verfahren hergestellten Koeffizienten c_ν und d_ν sind offenbar eindeutig bestimmt. Läßt man den Exponenten σ anwachsen, so wird jede der Reihen immer weiter fortgesetzt; bei unbeschränkter Fortsetzung entsteht eine unendliche sogenannte *Puiseuxsche Reihe*[1].

[1] Vgl. PUISEUX: Mémoire sur la théorie des fonctions algébriques. Journal de Liouville Bd. 1, S. 15. 1854; JORDAN, C.: Cours d'analyse I, 3me éd., S. 346 bis 357. 1909; HENSEL, K. und G. LANDSBERG: Theorie der algebraischen Funktionen einer Veränderlichen. Leipzig 1902.

In derselben Weise findet man für die Potenzprodukte der y vom Grade σ, welche das Ideal $\mathfrak{p}^\sigma$ erzeugen:

$$y_1^\nu y_2^{\sigma-\nu} \equiv b_\nu y_2^\sigma ((f_1), \mathfrak{p}^{\sigma+1}).$$

Das Rechnen im Restklassenring modulo $((f_1), \mathfrak{p}^{\sigma+1})$ ist also dasselbe wie das Rechnen mit Potenzreihen in y_2, die alle nach dem Glied mit y_2^σ abgebrochen werden. Setzt man nun die Relationen

$$\mathfrak{p}^\sigma \equiv 0 ((f_1, f_2), \mathfrak{p}^{\sigma+1}) \tag{3}$$

und

$$f \equiv 0 ((f_1, f_2), \mathfrak{p}^{\sigma+1}) \qquad [\sigma + 1 = \varrho] \tag{4}$$

um in Relationen für abgebrochene Potenzreihen in diesem Restklassenring, so ergibt sich sehr leicht, daß die Relation (3) nur dann erfüllt ist, wenn ein $d_k \neq 0$ ist ($k \leqq \sigma$); also ist das kleinste σ, für welches (3) gilt, zugleich das kleinste k mit $d_k \neq 0$. *Also ist der Exponent ϱ von $\mathfrak{q}$ genau der Exponent des ersten von Null verschiedenen Gliedes der Reihe* (2).

Ebenso leicht findet man, daß (4) nur dann erfüllt ist, wenn $c_0 = c_1 = \cdots = c_\sigma = 0$ ist. D. h.: *In der Entwicklung* (1) *für f dürfen, wenn $f \equiv 0$ ($\mathfrak{q}$) sein soll, nur die Glieder mit y_2^ϱ und höhere vorkommen.*

Man kann beweisen, daß der eben bestimmte Exponent ϱ zugleich die Multiplizität des Punktes a als Schnittpunkt der Kurven $f_1 = 0$ und $f_2 = 0$ (vgl. § 79) angibt.

Bei den geometrischen Anwendungen des Noetherschen Satzes liegt oft der Fall vor, daß die Polynome f, f_1, f_2 durch die Substitution $x_0 = 1$ aus homogenen Polynomen F, F_1, F_2 entstanden sind. Die Frage ist nun: Unter welchen Bedingungen kann man aus

$$f = g_1 f_1 + g_2 f_2 \tag{5}$$

auf

$$F = G_1 F_1 + G_2 F_2 \tag{6}$$

schließen, wo G_1 und G_2 wieder Formen sein sollen?

Bei der Untersuchung dieser Frage nehmen wir an, daß für $x_0 = 0$ die Formen F_1 und F_2 keinen nichtkonstanten gemeinsamen Teiler (also keine gemeinsame Nullstelle außer der trivialen $x_1 = 0$, $x_2 = 0$) haben. Durch eine lineare Transformation der drei Veränderlichen x_0, x_1, x_2, eventuell nach Erweiterung des Koeffizientenkörpers K, ist das ja immer zu erreichen.

Durch die Substitution $x_1 \to \frac{x_1}{x_0}$, $x_2 \to \frac{x_2}{x_0}$ und Multiplikation mit einer passenden Potenz von x_0 entsteht aus (5) eine Gleichung der Gestalt

$$x_0^h \cdot F = H_1 F_1 + H_2 F_2, \tag{7}$$

wo H_1 und H_2 Formen sind.

Wir wollen diese Gleichung so umformen, daß sich ein Faktor x_0 wegkürzt. Setzt man in (7) links und rechts $x_0 = 0$, so kommt:

$$0 = H_{10} F_{10} + H_{20} F_{20}.$$

Da F_{10} und F_{20} nach Voraussetzung teilerfremd sind, so muß H_{10} durch F_{20} und H_{20} durch F_{10} teilbar sein:

$$H_{10} = \quad G_0 F_{20},$$
$$H_{20} = -G_0 F_{10}.$$

Da H_1 bis auf Glieder mit x_0 mit H_{10} übereinstimmt, ebenso H_2 mit H_{20}, F_1 mit F_{10} und F_2 mit F_{20}, so folgt:

$$H_1 = \quad G_0 F_2 + x_0 K_1,$$
$$H_2 = -G_0 F_1 + x_0 K_2,$$

wo K_1 und K_2 Formen sind. In (7) eingesetzt, ergibt das:

$$x_0^h F = x_0 K_1 F_1 + x_0 K_2 F_2.$$

Hier kann man einen Faktor x_0 wegkürzen. Die h-malige Wiederholung desselben Verfahrens ergibt schließlich eine Gleichung der Form (6).

Also:

Für die Gleichung (5) *ist notwendig und hinreichend, daß für alle gemeinsamen Nullstellen der Formen F_1 und F_2 die inhomogen gemachten Polynome F, F_1, F_2 den Noetherschen Bedingungen genügen.*

Deutet man die Größen x_0, x_1, x_2 als homogene Koordinaten eines veränderlichen Punktes der projektiven Ebene, so wird $F = 0$ eine Kurve, welche alle Schnittpunkte der Kurven $F_1 = 0$ und $F_2 = 0$ enthält und außerdem in allen diesen Punkten gewissen „Noetherschen Bedingungen" zu genügen hat, damit die Gleichung (5) gelte. Diese Gleichung ist vor allem wichtig wegen einer darin enthaltenen Folgerung, des „Restsatzes":

Wenn eine Kurve $F_2 = 0$ vom Grade m durch eine Kurve $F = 0$ vom Grade $n + p$ geschnitten wird in $m(n + p)$ Punkten, jeder nach § 79 *mit der richtigen Vielfachheit gezählt, und wenn von diesen $m(n + p)$ Punkten $m \cdot n$ Punkte durch eine Kurve $F_1 = 0$ vom Grade n ausgeschnitten werden, so werden die übrigen $m \cdot p$ Punkte von einer Kurve $G_1 = 0$ vom Grade p ausgeschnitten, vorausgesetzt, daß die Kurve $F = 0$ in allen jenen $m \cdot n$ Punkten die Noetherschen Bedingungen des Ideals (F_1, F_2) erfüllt.*

Denn aus der Formel (6) geht klar hervor, daß die Schnittpunkte von $F = 0$ mit $F_2 = 0$ dieselben sind wie die von $F_1 \cdot G_1 = 0$ mit $F_2 = 0$.

Hinsichtlich weiterer geometrischer Ausführungen, die sich an den Restsatz anschließen, siehe etwa das Lehrbuch von F. Severi: Vorlesungen über algebraische Geometrie (deutsch von E. Löffler), 1921, sowie des Verfassers kurze Note in Math. Ann. Bd. **104**, S. 472. 1931.

Aufgaben. 1. Wenn ein Kegelschnitt eine Kurve 3. Ordnung in 6 verschiedenen Punkten schneidet und man diese Punkte in 3 Paare zerlegt, jedes Paar durch eine Gerade verbindet und diese Geraden wieder mit der Kurve schneidet, so werden die entstehenden 3 Punkte wieder von einer Geraden ausgeschnitten.

2. Als Spezialfall (für eine in 3 Gerade zerfallende Kurve 3. Ordnung) ist aus Aufgabe 1 der Pascalsche Satz für den Kegelschnitt herzuleiten.

3. Die Tangenten in 3 auf einer Geraden liegenden Punkten einer Kurve 3. Ordnung schneiden diese Kurve noch einmal in 3 Punkten, die einer Geraden angehören.

4. Als Spezialfall ist aus Aufgabe 3 zu folgern, daß die Verbindungsgerade zweier Wendepunkte noch einen Wendepunkt trifft.

5. Wenn ein Kreispaar ein anderes Kreispaar außer in den isotropen Punkten der projektiven Ebene noch in 8 Punkten trifft und 4 von diesen 8 Punkten auf einem Kreis liegen, so liegen die 4 übrigen ebenfalls auf einem Kreis.

6. Wählt man auf jeder Seite eines Dreiecks $A_1A_2A_3$ einen von den Ecken verschiedenen Punkt, nämlich B_1 auf der Seite A_2A_3 und von A_2 und A_3 verschieden usw., so gehen die Kreise $A_1B_2B_3$, $A_2B_3B_1$, $A_3B_1B_2$ durch einen Punkt.

§ 94. Zurückführung der mehrdimensionalen Ideale auf nulldimensionale.

In diesem Paragraphen werden wir die Sätze, die in § 92 für nulldimensionale Ideale bewiesen wurden, auf mehrdimensionale Ideale auszudehnen versuchen.

Die Methode dazu ist folgende: Ist $\mathfrak{q}$ ein Primärideal in $\mathsf{K}[x]$ von der Dimension d, $\mathfrak{p}$ das zugehörige Primideal, $\{\xi_1, \ldots, \xi_n\}$ dessen allgemeine Nullstelle und sind (etwa) $\xi_1, \ldots, \xi_d$ algebraisch-unabhängig[1], so reduzieren wir die Ideale $\mathfrak{q}$ und $\mathfrak{p}$ durch die Substitution $x_1 = \xi_1, \ldots, x_d = \xi_d$ zu nulldimensionalen Idealen. Wir nehmen diese Substitution in allen Polynomen q des Ideals $\mathfrak{q}$ vor; dadurch gehen diese Polynome q in Polynome q' aus $\mathsf{K}(\xi_1, \ldots, \xi_d)[x_{d+1}, \ldots, x_n]$ über, die ein Ideal $\mathfrak{q}'$ erzeugen. Es ist klar, daß es genügt, die Substitution $x_1 = \xi_1, \ldots, x_d = \xi_d$ in den Basispolynomen $q_1, \ldots, q_r$ auszuführen; die entstehenden Polynome $q_1', \ldots, q_r'$ erzeugen dann das Ideal $\mathfrak{q}'$:

$$\mathfrak{q}' = (q_1', \ldots, q_r').$$

Das Ideal $\mathfrak{q}'$ besteht offenbar aus den Polynomen q', dividiert durch beliebige von Null verschiedene Polynome φ in $\xi_1, \ldots, \xi_d$; denn die Polynome q' bilden ein Ideal in $\mathsf{K}[\xi_1, \ldots, \xi_d, x_{d+1}, \ldots, x_n]$, und um das dadurch erzeugte Ideal in $\mathsf{K}(\xi_1, \ldots, \xi_d)[x_{d+1}, \ldots, x_n]$ zu erhalten, braucht man nur noch die Nenner φ zuzulassen.

In derselben Weise wie $\mathfrak{q}'$ aus $\mathfrak{q}$, entsteht aus $\mathfrak{p}$ ein Ideal $\mathfrak{p}'$, und überhaupt aus jedem Ideal $\mathfrak{m} = (f_1, \ldots, f_r)$ ein Ideal $\mathfrak{m}' = (f_1', \ldots, f_r')$.

Geometrisch bedeutet die Substitution $x_1 = \xi_1, \ldots, x_d = \xi_d$, daß man alle auftretenden Mannigfaltigkeiten mit dem linearen Raum $x_1 = \xi_1, \ldots, x_d = \xi_d$ schneidet, welcher durch den allgemeinen Punkt der Mannigfaltigkeit von $\mathfrak{q}$ gelegt wird.

Wenn $f(x_1, \ldots, x_n)$ ein Polynom ist und wenn $f(\xi_1, \ldots, \xi_d, x_{d+1}, \ldots, x_n)$ zu $\mathfrak{q}'$ gehört, so ist nach dem Vorigen

$$f(\xi, x) = \frac{q'}{\varphi(\xi_1, \ldots, \xi_d)} = \frac{q(\xi, x)}{\varphi(\xi)}, \qquad q(x) \equiv 0 \,(\mathfrak{q}),$$

also

$$q(\xi, x) = \varphi(\xi) f(\xi, x).$$

Daraus folgt wegen der algebraischen Unabhängigkeit der $\xi_1, \ldots, \xi_d$

$$q(x) = \varphi(x) f(x) \equiv 0 \,(\mathfrak{q}).$$

Aus $\varphi(\xi) \neq 0$ folgt aber $\varphi(x) \not\equiv 0 \,(\mathfrak{p})$, mithin

$$f(x) \equiv 0 \,(\mathfrak{q}).$$

---

[1] Die $\xi_1, \ldots, \xi_d$ können also als Unbestimmte aufgefaßt werden (wir hätten sie auch etwa $t_1, \ldots, t_d$ nennen können), die übrigen ξ als algebraische Funktionen dieser Unbestimmten.

Um also zu entscheiden, ob ein Polynom $f(x)$ zu $\mathfrak{q}$ gehört, braucht man nur zu untersuchen, ob das entsprechende $f' = f(\xi_1, \ldots, \xi_d, x_{d+1}, \ldots, x_n)$ zu $\mathfrak{q}'$ gehört. $\mathfrak{q}'$ bestimmt also $\mathfrak{q}$ eindeutig[1].

Wir behaupten nun: *Das Ideal* $\mathfrak{q}'$ *in* $\mathsf{K}(\xi_1, \ldots, \xi_d)[x_{d+1}, \ldots, x_n]$ *ist primär; das zugehörige Primideal ist* $\mathfrak{p}'$; *der Exponent von* $\mathfrak{q}'$ *ist gleich dem von* $\mathfrak{q}$; *die allgemeine Nullstelle von* $\mathfrak{p}'$ *ist* $\{\xi_{d+1}, \ldots, \xi_n\}$, *und die Dimension von* $\mathfrak{p}'$ *ist Null.*

Beweis: Um zu zeigen, daß $\mathfrak{q}'$ primär und $\mathfrak{p}'$ das zugehörige Primideal ist, genügt es, folgende drei Eigenschaften nachzuweisen:

1. Aus $f(\xi, x)\, g(\xi, x) \equiv 0\,(\mathfrak{q}')$ und $f(\xi, x) \not\equiv 0\,(\mathfrak{p}')$ folgt $g(\xi, x) \equiv 0\,(\mathfrak{q}')$.
2. Aus $f(\xi, x) \equiv 0\,(\mathfrak{q}')$ folgt $f(\xi, x) \equiv 0\,(\mathfrak{p}')$.
3. Aus $f(\xi, x) \equiv 0\,(\mathfrak{p}')$ folgt $f(\xi, x)^\varrho \equiv 0\,(\mathfrak{q}')$.

In allen drei Eigenschaften kann man f und g als ganzrational in $\xi_1, \ldots, \xi_d$ voraussetzen, da man sie andernfalls nur mit einem passenden $\varphi(\xi)$ zu multiplizieren braucht. Dann kann man vermöge der obigen Bemerkung überall die ξ durch die x, $\mathfrak{q}'$ durch $\mathfrak{q}$, $\mathfrak{p}'$ durch $\mathfrak{p}$ ersetzen; denn z. B. $f(\xi, x) \equiv 0\,(\mathfrak{q}')$ ist äquivalent mit $f(x) \equiv 0\,(\mathfrak{q})$, usw. Nach dieser Ersetzung besagen aber 1., 2., 3. nichts anderes als, daß $\mathfrak{q}$ primär und $\mathfrak{p}$ das zugehörige Primideal ist, was wir schon wissen. Zugleich ist gezeigt, daß die Exponenten von $\mathfrak{q}'$ und $\mathfrak{q}$ übereinstimmen.

Um zu zeigen, daß $\{\xi_{d+1}, \ldots, \xi_n\}$ die allgemeine Nullstelle von $\mathfrak{p}'$ ist, haben wir nur zu beweisen, daß aus

$$f(\xi_1, \ldots, \xi_d, \xi_{d+1}, \ldots, \xi_n) = 0,$$

wo f rational in $\xi_1, \ldots, \xi_d$, ganzrational in $\xi_{d+1}, \ldots, \xi_n$ ist, folgt

$$f(\xi, x) \equiv 0\,(\mathfrak{p}')$$

und umgekehrt. Wiederum kann f ganzrational in $\xi_1, \ldots, \xi_d$ vorausgesetzt werden. Dann ist aber $f(\xi, x) \equiv 0\,(\mathfrak{p}')$ äquivalent mit $f(x) \equiv 0\,(\mathfrak{p})$; also erledigt sich dieser Teil der Behauptung durch die Bemerkung, daß $\{\xi_1, \ldots, \xi_n\}$ die allgemeine Nullstelle von $\mathfrak{p}$ ist.

Die Nulldimensionalität von $\mathfrak{p}'$ folgt schließlich aus der Tatsache, daß $\xi_{d+1}, \ldots, \xi_n$ algebraisch in bezug auf $\mathsf{K}(\xi_1, \ldots, \xi_d)$ sind. Damit sind alle Behauptungen bewiesen.

In derselben Weise kann man auch zeigen, daß, *wenn* $\mathfrak{q}$ *eine Primärkomponente eines Ideals* $\mathfrak{m} = (f_1, \ldots, f_r)$ *ist, auch* $\mathfrak{q}'$ *eine Primärkomponente des entsprechenden Ideals* $\mathfrak{m}' = (f_1', \ldots, f_r')$ *ist.*

---

[1] Dasselbe gilt, wie der Beweis zeigt, von jedem anderen Primärideal $\mathfrak{r}$ mit der Eigenschaft, daß $x_1, \ldots, x_d$ modulo dem zugehörigen Primideal $\mathfrak{s}$ unabhängig sind, d. h. daß aus $\varphi(x_1, \ldots, x_d) \not\equiv 0$ folgt $\varphi \not\equiv 0\,(\mathfrak{s})$. Gibt es dagegen ein $\varphi(x_1, \ldots, x_d) \not\equiv 0$ in $\mathfrak{s}$, so ist $\varphi(x)^\varrho \equiv 0\,(\mathfrak{r})$, mithin

$$1 = \varphi(\xi)^{-\varrho}\, \varphi(\xi)^\varrho \equiv 0\,(\mathfrak{r}'),$$

mithin wird $\mathfrak{r}'$ das Einheitsideal.

Denn wenn $\mathfrak{m} = [\mathfrak{q}, \mathfrak{q}_2, \ldots, \mathfrak{q}_s]$ eine unverkürzbare Darstellung von $\mathfrak{m}$ durch größte Primärkomponenten ist, so folgt $\mathfrak{m}' = [\mathfrak{q}', \mathfrak{q}'_2, \ldots, \mathfrak{q}'_s]$, weil man die Polynome $f(\xi, x)$ von $\mathfrak{m}'$ und von $[\mathfrak{q}', \mathfrak{q}'_2, \ldots]$ durch Multiplikation mit passenden Polynomen $\varphi(\xi_1, \ldots, \xi_d) \neq 0$ in solche Ausdrücke $g(\xi, x)$ verwandeln kann, daß $g(x_1, \ldots, x_d, x_{d+1}, \ldots, x_n)$ zu $\mathfrak{m}$ bzw. zu $\mathfrak{q}$ und $\mathfrak{q}_2, \ldots, \mathfrak{q}_s$ gehört. Wäre nun in der Darstellung $\mathfrak{m}' = [\mathfrak{q}', \mathfrak{q}'_2, \ldots, \mathfrak{q}'_s]$ das $\mathfrak{q}'$ überflüssig, so wäre $[\mathfrak{q}'_2, \ldots, \mathfrak{q}'_s] \equiv 0\,(\mathfrak{q}')$. Wenn man $\mathfrak{m}_1 = [\mathfrak{q}_2, \ldots, \mathfrak{q}_s]$ setzt, so würde folgen $\mathfrak{m}'_1 = [\mathfrak{q}'_2, \ldots, \mathfrak{q}'_s] \equiv 0\,(\mathfrak{q}')$. Ist f ein beliebiges Element von $\mathfrak{m}_1$, so wäre $f' \equiv 0\,(\mathfrak{m}'_1) \equiv 0\,(\mathfrak{q}')$, mithin $f \equiv 0\,(\mathfrak{q})$. Also würde folgen $\mathfrak{m}_1 \equiv 0\,(\mathfrak{q})$; d. h. $\mathfrak{q}$ wäre in der Darstellung von $\mathfrak{m}$ überflüssig, entgegen der Annahme, daß die Darstellung von $\mathfrak{m}$ unverkürzbar ist. In der Darstellung $\mathfrak{m}' = [\mathfrak{q}', \mathfrak{q}'_2, \ldots, \mathfrak{q}'_s]$ ist also $\mathfrak{q}'$ nicht überflüssig. Läßt man die eventuell überflüssigen $\mathfrak{q}'_\nu$ weg, so bleibt eine unverkürzbare Darstellung, in der $\mathfrak{q}'$ vorkommt. Ist weiter $\mathfrak{p}_\nu$ das zu $\mathfrak{q}_\nu$ gehörige und somit $\mathfrak{p}'_\nu$ das zu $\mathfrak{q}'_\nu$ gehörige Primideal, so ist $\mathfrak{p} \neq \mathfrak{p}_\nu$ und daher auf Grund der früher (Fußnote S. 76) bemerkten Eindeutigkeit $\mathfrak{p}' \neq \mathfrak{p}'_\nu$. Im Fall $\mathfrak{p}'_\nu = \mathfrak{o}$, wo die Eindeutigkeit nicht mehr gilt, ist ebenfalls $\mathfrak{p}' \neq \mathfrak{p}'_\nu$. Also ist in der Darstellung von $\mathfrak{m}'$ das Primärideal $\mathfrak{q}'$ das einzige zu $\mathfrak{p}'$ gehörige. Das heißt aber, $\mathfrak{q}'$ ist eine Primärkomponente von $\mathfrak{m}'$.

Ist $\mathfrak{q}$ sogar eine *isolierte* Komponente von $\mathfrak{m}$, so ist *auch* $\mathfrak{q}'$ *eine isolierte Komponente von* $\mathfrak{m}'$, was man in ähnlicher Weise leicht einsieht.

Die entwickelte Methode der Reduktion aller Primärideale auf nulldimensionale gibt uns die Mittel in die Hand, von einem gegebenen Polynom f zu entscheiden, ob es einem gegebenen Ideal $\mathfrak{m} = (f_1, \ldots, f_r)$ angehört, vorausgesetzt, daß einmal die Zerlegung von $\mathfrak{m}$ in Primärkomponenten

$$\mathfrak{m} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_s]$$

gegeben ist. Wir suchen nämlich zu jeder Primärkomponente $\mathfrak{q}$ das zugehörige nulldimensionale $\mathfrak{q}'$, erweitern dann den Körper $\mathsf{K}(\xi_1, \ldots, \xi_d)$ so, daß $\mathfrak{q}'$ in lauter Primärideale $\mathfrak{q}'_\nu$ mit je nur einer Nullstelle $a^{(\nu)}$ zerfällt, und untersuchen nach der Methode von § 92 mittels der „Noetherschen Bedingungen“

$$(1) \qquad f' \equiv 0\,(\mathfrak{q}', \mathfrak{p}'^{\varrho}_\nu),\ \mathfrak{p}'_\nu = (x_{d+1} - a^{(\nu)}_{d+1}, \ldots, x_n - a^{(\nu)}_n),$$

ob das Polynom f' den Idealen $\mathfrak{q}'_\nu = (\mathfrak{q}', \mathfrak{p}'^{\varrho}_\nu)$ und demnach auch dem Ideal $\mathfrak{q}'$ angehört. Da die Nullstellen der $\mathfrak{p}'_\nu$ konjugiert in bezug auf $\mathsf{K}(\xi_1, \ldots, \xi_d)$ sind, so sind auch die $\mathfrak{p}'_\nu$ und somit die $\mathfrak{q}'_\nu$ konjugiert in bezug auf $\mathsf{K}(\xi_1, \ldots, \xi_d)$; es genügt also, zu jedem $\mathfrak{q}'$ *ein* $\mathfrak{q}'_\nu$ zu untersuchen. Man braucht also auch nur eine Nullstelle eines jeden $\mathfrak{q}'$ zu adjungieren. Nun ist $\{\xi_{d+1}, \ldots, \xi_n\}$ eine solche Nullstelle. An die Stelle von $\mathfrak{p}'_\nu$ tritt also das Primideal

$$\mathfrak{p}_\xi = (x_{d+1} - \xi_{d+1}, \ldots, x_n - \xi_n);$$

statt der Bedingung (1) können wir die bequemere

$$f' \equiv 0 \,(\mathfrak{m}', \mathfrak{p}_\xi^\varrho) \tag{2}$$

benutzen, denn (2) ist auch notwendig für $f \equiv 0\,(\mathfrak{m})$, und aus (2) folgt (1) sofort. Die Bedingung (2), die für jede Primärkomponente $\mathfrak{q}$ von $\mathfrak{m}$ erfüllt sein muß, ist unter dem Namen *Kriterium von* HENTZELT oder *Hentzeltscher Nullstellensatz* bekannt.

Ist speziell $\mathfrak{q}$ eine isolierte Komponente von $\mathfrak{m}$, also $\mathfrak{q}'$ eine isolierte Komponente von $\mathfrak{m}'$, so kann man wie in § 86 den Exponenten ϱ aus der Bedingung

$$\mathfrak{p}_\xi^\varrho \equiv 0 \,(\mathfrak{m}', \mathfrak{p}_\xi^{\varrho+1})$$

bestimmen.

Aus den Bedingungen (1) für $f \equiv 0\,(\mathfrak{q})$ erhellt am klarsten die eigentliche geometrische Bedeutung der Primärideale: Die Zugehörigkeit zu einem Primärideal stellt gewisse Anforderungen an die Anfangsglieder der Entwicklung des Polynoms f nach Potenzen von $x_1 - \xi_1, \ldots, x_n - \xi_n$ für einen allgemeinen Punkt ξ einer irreduziblen Mannigfaltigkeit, z. B. die Anforderung, daß f in diesem allgemeinen Punkt verschwinden soll, oder die, daß die Hyperfläche $f = 0$ in diesem allgemeinen Punkt eine andere Hyperfläche berühren soll, usw.

Aufgaben. 1. Mit der Methode der Reduktion auf nulldimensionale Ideale beweise man, daß jedes $(n-1)$-dimensionale Primärideal in $\mathsf{K}[x_1, \ldots, x_n]$ ein Hauptideal ist.

2. Jedes ungemischte $(n-1)$-dimensionale Ideal in $\mathsf{K}[x_1, \ldots, x_n]$ ist ein Hauptideal und umgekehrt.

§ 95. Ungemischte Ideale.

Bei ungemischten Idealen, bei denen alle Primärkomponenten dieselbe Dimension d haben, sind alle diese Primärkomponenten automatisch isoliert; ihre Mannigfaltigkeiten und deren allgemeine Punkte erhält man sofort mittels der Eliminationstheorie (§ 74), und die Kriterien für $f \equiv 0\,(\mathfrak{m})$ sind aus dem vorigen Paragraphen in einfacher Form zu entnehmen. Es ist also sehr wichtig, für gewisse Ideale die Ungemischtheit von vornherein feststellen zu können. Wir werden zunächst einige Kriterien aufstellen, mit denen man entscheiden kann, ob ein Ideal nulldimensionale Komponenten besitzt.

Ist $\mathfrak{m} = (f_1, \ldots, f_r)$ ein Ideal in $\mathfrak{o} = \mathsf{K}[x]$ und $\mathfrak{M}$ das von $\mathfrak{m}$ erzeugte Ideal (mit derselben Basis) in $\mathfrak{O} = \Omega[x]$, wo Ω ein passender (am bequemsten algebraisch-abgeschlossener) algebraischer Erweiterungskörper von K ist, so ist nach dem Hilfssatz von § 92 der Durchschnitt $\mathfrak{M} \cap \mathfrak{o}$ gleich $\mathfrak{m}$. Ist $\mathfrak{M}$ in Primärkomponenten zerlegt:

$$\mathfrak{M} = [\mathfrak{Q}_1, \mathfrak{Q}_2, \ldots, \mathfrak{Q}_s], \tag{1}$$

so ist

$$\begin{aligned} \mathfrak{m} = \mathfrak{M} \cap \mathfrak{o} &= [\mathfrak{Q}_1, \mathfrak{Q}_2, \ldots, \mathfrak{Q}_s, \mathfrak{o}] \\ &= [\mathfrak{Q}_1 \cap \mathfrak{o}, \mathfrak{Q}_2 \cap \mathfrak{o}, \ldots, \mathfrak{Q}_s \cap \mathfrak{o}]. \end{aligned} \tag{2}$$

[1] Von den Idealen $\mathfrak{Q}_\nu \cap \mathfrak{o}$ werden im allgemeinen einige miteinander identisch werden. Zwei (in bezug auf K) konjugierte $\mathfrak{Q}_\nu$ haben nämlich denselben Durchschnitt mit $\mathfrak{o}$.

Es gilt nun:

Wenn $\mathfrak{Q}$ *primär ist zum Primideal* $\mathfrak{P}$, *so ist* $\mathfrak{Q} \cap \mathfrak{o}$ *primär im Ring* $\mathfrak{o}$ *zum Primideal* $\mathfrak{P} \cap \mathfrak{o}$.[1]

Den Beweis führt man mühelos auf Grund der bekannten drei Kriterien:

1. aus $fg \equiv 0(\mathfrak{Q} \cap \mathfrak{o})$, $f \not\equiv 0(\mathfrak{P} \cap \mathfrak{o})$ folgt $g \equiv 0(\mathfrak{Q} \cap \mathfrak{o})$;
2. aus $f \equiv 0(\mathfrak{Q} \cap \mathfrak{o})$ folgt $f \equiv 0(\mathfrak{P} \cap \mathfrak{o})$;
3. aus $f \equiv 0(\mathfrak{P} \cap \mathfrak{o})$ folgt $f^{\varrho} \equiv 0(\mathfrak{Q} \cap \mathfrak{o})$

für f und g aus $\mathfrak{o}$.

Weiter: *Ist* ξ *die allgemeine Nullstelle von* $\mathfrak{P}$ (*in einem Erweiterungskörper von* Ω), *so ist* ξ *zugleich die allgemeine Nullstelle von* $\mathfrak{P} \cap \mathfrak{o}$. Denn wenn $\mathfrak{P}$ aus allen Polynomen von $\mathfrak{O}$ mit der Nullstelle ξ besteht, so besteht $\mathfrak{P} \cap \mathfrak{o}$ aus allen Polynomen von $\mathfrak{o}$ mit der Nullstelle ξ.

Folgerung. Die Dimension von $\mathfrak{P}$ ist gleich der von $\mathfrak{P} \cap \mathfrak{o}$.

Wenn also $\mathfrak{M}$ nach (1) ein Durchschnitt von Primäridealen bestimmter Dimensionen ist, so ist $\mathfrak{m}$ nach (2) ein Durchschnitt von Primäridealen derselben Dimensionen. Insbesondere: Hat $\mathfrak{M}$ keine nulldimensionale Komponente, so hat auch $\mathfrak{m}$ keine, und ist $\mathfrak{M}$ ungemischt, so gilt dasselbe von $\mathfrak{m}$. (Die Umkehrung gilt auch, ist aber nicht so leicht zu beweisen und für uns ohne Wichtigkeit.)

Die Entscheidung, ob $\mathfrak{M}$ eine k-dimensionale Komponente besitzt, kann nach der Methode von § 94 auf die Entscheidung über nulldimensionale Komponenten zurückgeführt werden. Bei passender Wahl des Körpers Ω haben die nulldimensionalen Komponenten von $\mathfrak{M}$ je nur eine Nullstelle a; ihr zugehöriges Primideal ist $\mathfrak{p} = (x_1 - a_1, \ldots, x_n - a_n)$, und die Entscheidung, ob eine zu $\mathfrak{p}$ gehörige Primärkomponente vorhanden ist, hängt davon ab, ob

$$\mathfrak{M} : \mathfrak{p} = \mathfrak{M}$$

ist, d. h. ob aus

$$f\mathfrak{p} \equiv 0(\mathfrak{M})$$

folgt

$$f \equiv 0(\mathfrak{M}).$$

Ist l eine beliebige Linearkombination von $x_1 - a_1, \ldots, x_n - a_n$, so folgt aus $f\mathfrak{p} \subseteq \mathfrak{M}$, daß insbesondere $fl \equiv 0(\mathfrak{M})$ ist; wenn man also beweisen kann, daß (für ein passend gewähltes l) aus $fl \equiv 0(\mathfrak{M})$ folgt $f \equiv 0(\mathfrak{M})$, so besitzt das Ideal $\mathfrak{M}$ und daher auch $\mathfrak{m}$ sicher keine nulldimensionale Primärkomponente mit der Nullstelle a. Die Beweismethode dabei ist häufig dieselbe, die im § 93 (Kleindruck) schon angewandt wurde, um aus $x_0^h F = H_1F_1 + H_2F_2$ auf $F = G_1F_1 + G_2F_2$ zu schließen. Der allgemeine Satz, den man mit dieser Beweismethode erhalten kann, lautet:

Wenn das von $\mathfrak{o}$ *verschiedene Ideal* $(f_1, \ldots, f_r)$ *mit* r *Basiselementen eine Dimension* $d \leqq n - r$ *hat, so ist es ungemischt* $(n - r)$*-dimensional.*

Für $r = 1$ ist dieser Satz aus § 91 (Aufgabe 2) bekannt; wir nehmen also vollständige Induktion nach r vor und nehmen an, für den Fall von $r - 1$ Basispolynomen sei der Satz bei jeder Variablenzahl n richtig.

Wir haben zu zeigen, daß das Ideal $(f_1, \ldots, f_r)$ für $k < n - r$ keine k-dimensionale Primärkomponente besitzt. Gesetzt, es wäre $\mathfrak{q}$ eine solche. Nach der Methode des § 94 können wir dann die Dimension von $\mathfrak{q}$ zu Null erniedrigen; dabei erniedrigen sich die Variablenzahl n und die Höchstdimension d von $(f_1, \ldots, f_r)$ genau um k,

---

[1] Um Mißverständnissen vorzubeugen, weise ich darauf hin, daß die Umkehrung nicht gilt: wenn $\mathfrak{Q} \cap \mathfrak{o}$ primär ist, braucht $\mathfrak{Q}$ es nicht zu sein. Es gibt ja (vgl. § 87) *Beispiele von* Primidealen $\mathfrak{m}$ in $\mathfrak{o}$, die bei Erweiterung des Grundkörpers K zu Ω in verschiedene Primärkomponenten zerfallen.

und somit bleibt die Voraussetzung $d \leqq n - r$ erhalten. Wir haben also nur noch zu beweisen, daß ein solches Ideal $(f_1, \ldots, f_r)$ im Falle $n - r > 0$ keine nulldimensionale Primärkomponente besitzt, und können dabei außerdem nach den früheren Bemerkungen annehmen, daß die fragliche nulldimensionale Primärkomponente nur eine Nullstelle a im (eventuell erweiterten) Grundkörper besitzt.

Wir zeigen zunächst, daß unter der Voraussetzung $d \leqq n - r$ die Basispolynome $f_1, \ldots, f_r$ so gewählt werden können, daß jedes der Ideale $(f_1, \ldots, f_i)$ höchstens die Dimension $n - i$ hat. Für $i = 1$ und $f_1 \neq 0$ ist diese Bedingung von selbst erfüllt. Gesetzt, man habe schon erreicht, daß $(f_1, \ldots, f_{i-1})$ eine Dimension $\leqq n - i + 1$ hat. In jeder der irreduziblen $(n - i + 1)$-dimensionalen Mannigfaltigkeiten des Ideals $(f_1, \ldots, f_{i-1})$ (falls es solche gibt) wählen wir einen Punkt, der nicht zur Mannigfaltigkeit von $(f_1, \ldots, f_r)$ gehört. In jedem dieser Punkte verschwindet mindestens eins der Polynome $f_i, f_{i+1}, \ldots, f_r$ nicht; also wird eine passend gewählte Linearkombination $f_i^* = f_i + \mu_{i+1} f_{i+1} + \cdots + \mu_r^i f_r$ in keinem dieser Punkte verschwinden. Diese Linearkombination wähle man als i-tes Basiselement statt f_i; dann hat das Ideal $(f_1, \ldots, f_{i-1}, f_i^*)$ höchstens noch die Dimension $n - i$, während das Ideal $(f_1, \ldots, f_r)$ bei der Ersetzung ungeändert bleibt.

Zum eigentlichen Beweis dafür, daß $(f_1, \ldots, f_r)$ in a keine nulldimensionale Komponente besitzt, wählen wir ein lineares Polynom

$$l = (x_1 - a_1) + c_2(x_2 - a_2) + \cdots + c_n(x_n - a_n),$$

wo die c so bestimmt sind, daß l in keiner der allgemeinen Nullstellen der $(n - r)$-dimensionalen zugehörigen Primideale von $(f_1, \ldots, f_r)$ und der $(n - r + 1)$-dimensionalen zugehörigen Primideale von $(f_1, \ldots, f_{r-1})$ den Wert Null annimmt. Wenn wir zeigen können, daß aus

$$lf \equiv 0 (f_1, \ldots, f_r)$$

folgt

$$f \equiv 0 (f_1, \ldots, f_r),$$

so sind wir fertig.

Durch die Substitution

$$x_1 = a_1 - \sum_{\nu=2}^{n} c_\nu (x_\nu - a_\nu)$$

geht l in 0 und jedes Polynom f in ein Polynom $f_0 \equiv f \pmod{l}$ über. Aus der Voraussetzung

$$lf = g_1 f_1 + \cdots + g_r f_r \tag{3}$$

folgt durch diese Substitution

$$0 = g_{10} f_{10} + \cdots + g_{r0} f_{r0}. \tag{4}$$

Das Ideal $(f_{10}, \ldots, f_{r-1,0})$ in $\mathsf{K}[x_2, \ldots, x_n]$ ist zufolge der Wahl von l höchstens $(n - r)$-dimensional, also nach der Induktionsvoraussetzung ungemischt $(n - r)$ dimensional, und f_{r0} enthält keine $(n - r)$-dimensionale Mannigfaltigkeit dieses Ideals; also folgt aus (4)

$$g_{r0} \equiv 0 (f_{10}, \ldots, f_{r-1,0})$$

und daraus

$$g_r \equiv h_r l (f_1, \ldots, f_{r-1}).$$

In (3) eingesetzt, ergibt dies

$$lf \equiv h_r l f_r (f_1, \ldots, f_{r-1}),$$
$$l(f - h_r f_r) \equiv 0 (f_1, \ldots, f_{r-1}).$$

Da das Ideal $(f_1, \ldots, f_{r-1})$ ungemischt ist und l in den allgemeinen Nullstellen seiner zugehörigen Primärideale von 0 verschieden ist, so folgt

$$f - h_r f_r \equiv 0 (f_1, \ldots, f_{r-1}),$$
$$f \equiv 0 (f_1, \ldots, f_r).$$

Damit ist der Beweis erbracht.

Aufgaben. 1. Wenn f_1 und f_2 keinen nichtkonstanten gemeinsamen Teiler haben und $(f_1, f_2) \neq \mathfrak{o}$ ist, so ist das Ideal (f_1, f_2) ungemischt $(n-2)$-dimensional.

2. Sind unter den Voraussetzungen von Aufgabe 1 in den allgemeinen Punkten der irreduziblen Bestandteile der Mannigfaltigkeit des Ideals (f_1, f_2) die „Tangentialräume" der Hyperflächen $f_1 = 0$ und $f_2 = 0$ (hinsichtlich deren Definition vgl. § 93) verschieden, so ist für $f \equiv 0$ (f_1, f_2) notwendig und hinreichend, daß f diese Mannigfaltigkeit enthält.

3. Welche Bedingungen muß ein Polynom f erfüllen, damit es dem Ideal

$$(x_1^2 + x_2^2 - x_3^2,\ x_1 + x_4,\ x_2 + x_4)$$

angehört?

Weitere Sätze über ungemischte Ideale findet man in dem Büchlein von F. S. MACAULAY: Algebraic Theory of Modular Systems, Cambridge Tracts in Mathematics 19, Cambridge 1916.

§ 96. Der Grad einer Mannigfaltigkeit und die Schnittpunkte mit linearen Räumen.

Wir fragen nach den Schnittpunkten einer irreduziblen algebraischen Mannigfaltigkeit $\mathfrak{M}$ mit einer linearen Mannigfaltigkeit L_{n-r}, bestehend aus den Nullstellen von r linearen Polynomen

$$(1) \qquad \begin{cases} l_1 = l_1' - t_1 = \sum_{k=1}^{n} s_{1k} x_k - t_1, \\ \cdots\cdots\cdots\cdots\cdots \\ l_r = l_r' - t_r = \sum_{k=1}^{n} s_{rk} x_k - t_r. \end{cases}$$

Wir betrachten zunächst den Fall, daß alle s_{ik} und t_i Unbestimmte sind. Man nennt den Raum L_{n-r} dann einen *allgemeinen linearen Unterraum* von der Dimension $n - r$.

Wir adjungieren zunächst die Größen s_{ik} an K und bilden neben $l_1', \ldots, l_r'$ weitere Linearkombinationen $l_{r+1}', \ldots, l_n'$, so daß insgesamt n linear-unabhängige Formen entstehen, welche wir als neue Veränderliche statt $x_1, \ldots, x_n$ benutzen können. In den Nullstellen ξ von $\mathfrak{M}$ nehmen diese neuen Veränderlichen $l_1', \ldots, l_n'$ Werte $\lambda_1, \ldots, \lambda_n$ an, und es ist insbesondere

$$(2) \qquad \lambda_i = \sum_{k=1}^{n} s_{ik} \xi_k \qquad (i = 1, \ldots, r).$$

Unter diesen λ_i gibt es, wenn d die Dimension von $\mathfrak{M}$ ist, höchstens d algebraisch-unabhängige Größen. Daraus folgt, daß unter ihnen höchstens d gleich neuen Unbestimmten t_i gesetzt werden können; *mithin muß, wenn überhaupt Schnittpunkte von $\mathfrak{M}$ mit L_{n-r} vorhanden sein sollen, $r \leqq d$ gewählt werden.* Im Fall $r = d$ muß jeder Schnittpunkt genau den Transzendenzgrad d haben, mithin einen allgemeinen Punkt von $\mathfrak{M}$ darstellen.

Wir werden nun zeigen, daß für $r = d$ wirklich Schnittpunkte, und zwar endlichviele vorhanden sind. Für $r < d$ gibt es dann, wie leicht ersichtlich, unendlichviele Schnittpunkte.

Wir bemerken zunächst, daß die $r = d$ Größen (2) algebraisch-unabhängig sind, wenn man für ξ eine allgemeine Nullstelle wählt. Wären sie nämlich abhängig, so würden sie es nach dem Hilfssatz von § 77 bei jeder Spezialisierung der s_{ik} bleiben; man kann aber die s_{ik} so spezialisieren, daß die λ_i in $\xi_1, \ldots, \xi_d$ oder in irgend d vorgegebene der $\xi_1, \ldots, \xi_n$ übergehen, und diese sind algebraisch-unabhängig. Die somit als unabhängig erkannten $\lambda_1, \ldots, \lambda_d$ können wir wegen

$$\mathsf{K}(s_{ik}, \lambda_1, \ldots, \lambda_d) \cong \mathsf{K}(s_{ik}, t_1, \ldots, t_r)$$

mit den Unbestimmten $t_1, \ldots, t_d$ identifizieren. Die übrigen λ und daher auch die ξ sind dann algebraische Funktionen dieser Unbestimmten; d. h. der Körper

$$\mathsf{K}(s_{ik}, \lambda_1, \ldots, \lambda_n) = \mathsf{K}(s_{ik}, \xi_1, \ldots, \xi_n)$$

ist algebraisch über $\mathsf{K}(s_{ik}, t_j)$.[1] Die Gleichungen (2) besagen nunmehr, daß der Punkt ξ dem Raum L_{n-r} angehört; die Existenz von Schnittpunkten ist also bewiesen. Da alle Nullstellenkörper

$$\mathsf{K}(s_{ik}, \xi_1, \ldots, \xi_n) = \mathsf{K}(s_{ik}, \lambda_1, \ldots, \lambda_n)$$

äquivalent sind, so kommen für $\lambda_1, \ldots, \lambda_n$ oder $\xi_1, \ldots, \xi_n$ in jedem passenden Erweiterungskörper von $\mathsf{K}(s, t)$ nur endlichviele konjugierte Wertsysteme in Betracht. *Es gibt also endlichviele Schnittpunkte von* $\mathfrak{M}$ *und* L_{n-d}, *und diese sind untereinander konjugiert in bezug auf* $\mathsf{K}(s, t)$. Die Anzahl dieser Schnittpunkte heißt der *Grad* der Mannigfaltigkeit $\mathfrak{M}$.

Wir wollen nun untersuchen, was mit diesen Schnittpunkten geschieht, wenn wir die Unbestimmten s, t durch Größen aus K ersetzen. Um da ausnahmslose Regeln zu erhalten, ist es notwendig, zunächst vom Raum R_n zum projektiven Raum P_n und von der Mannigfaltigkeit $\mathfrak{M}$ zur entsprechenden Mannigfaltigkeit $\mathfrak{M}^*$ in P_n überzugehen. Wir machen dementsprechend die l_ν durch Einführung eines x_0 homogen, setzen $t_1 = -s_{10}$, $t_2 = -s_{20}$ usw. und erhalten an Stelle von (1) die Formen

$$\begin{aligned} l_1^* &= \sum_{k=0}^{n} s_{1k} x_k, \\ &\cdots\cdots\cdots \\ l_d^* &= \sum_{k=0}^{n} s_{dk} x_k. \end{aligned}$$

Da der Durchschnitt von $\mathfrak{M}^*$ mit der „uneigentlichen Ebene" $\xi_0 = 0$ eine kleinere Dimension als $\mathfrak{M}^*$ hat, so hat er mit dem allgemeinen $(n-d)$-dimensionalen Raum L_{n-d} keinen Punkt gemein. Als Schnittpunkte kommen also nur die Punkte von $\mathfrak{M}$, d. h. die endlichvielen konjugierten Punkte von vorhin in Betracht.

Ist $(f_1^*, \ldots, f_s^*)$ das zugehörige Ideal von $\mathfrak{M}^*$, wobei die f_ν^* nach § 87, Aufgabe 4 homogen gewählt werden können, so sind die Schnittpunkte von $\mathfrak{M}^*$ mit L_{n-d}^* die gemeinsamen Nullstellen der Formen

$$f_1^*, \ldots, f_s^*, l_1^*, \ldots, l_d^*. \tag{3}$$

Diese Formen ergeben, gleich Null gesetzt, ein homogenes Gleichungssystem, auf das man die Theorie von Kap. 11 (§ 76 und § 79) anwenden kann. Die nun folgenden Betrachtungen, in denen untersucht wird, was mit den Lösungen $\xi^{(\nu)}$ $(\nu = 1, \ldots, g)$

---

[1] Genauer: Der Isomorphismus

$$\mathsf{K}(s_{ik}, \lambda_1, \ldots, \lambda_d) \cong \mathsf{K}(s_{ik}, t_1, \ldots, t_r)$$

läßt sich zu einem Isomorphismus

$$\mathsf{K}(s_{ik}, \lambda_1, \ldots, \lambda_d, \xi_1, \ldots, \xi_n) \cong \mathsf{K}(s_{ik}, t_1, \ldots, t_r, \xi_1^*, \ldots, \xi_n^*)$$

erweitern, und die ξ^* können nachher wieder mit ξ bezeichnet werden.

dieses Gleichungssystems bei Ersetzung der Unbestimmten s_{ik} durch andere Größen σ_{ik} (aus K oder aus einem Erweiterungskörper von K) geschieht, beruhen ausschließlich auf den allgemeinen Eigenschaften homogener Gleichungssysteme und gelten demnach nicht nur für das System (3), sondern auch für jedes andere System von Formen, in denen außer den „Unbekannten" x oder ξ noch unbestimmte Parameter s_{ik} vorkommen.

Wir wollen versuchen, für jede Spezialisierung $s_{ik} \to \sigma_{ik}$ solche Punkte $\eta^{(1)}, \ldots, \eta^{(g)}$ zu finden, daß *alle algebraischen Relationen, die zwischen den Größen s_{ik} und $\xi_i^{(\nu)}$ bestehen und in jeder Größenreihe $\{\xi_0^{(\nu)}, \ldots, \xi_n^{(\nu)}\}$ homogen sind, auch für die Größen σ_{ik} und $\eta_i^{(\nu)}$ gelten.* Mit anderen Worten: Wenn ein Polynom $F(s_{ik}, x_i^{(\nu)})$, homogen in jeder Variablenreihe $\{x_0^{(\nu)}, \ldots, x_n^{(\nu)}\}$, die Eigenschaft

$$F(s_{ik}, \xi_i^{(\nu)}) = 0 \tag{4}$$

besitzt, so verlangen wir, daß auch

$$F(\sigma_{ik}, \eta_i^{(\nu)}) = 0 \tag{5}$$

ist. Insbesondere soll das natürlich für die Formen (3) gelten; somit müssen alle $\eta^{(\nu)}$ auch Nullstellen der spezialisierten Formen (3) sein.

Daß es tatsächlich immer möglich ist, die η dieser Forderung gemäß zu bestimmen, sieht man folgendermaßen ein: Unter den Formen F mit der obigen Eigenschaft (4) können wir nach § 80 endlichviele auswählen, von denen alle übrigen linear (mit Formen als Koeffizienten) abhängen. Das Gleichungssystem (4) läßt sich also durch ein endliches System ersetzen. Eliminiert man nun aus diesem Gleichungssystem sukzessiv die Größenreihen $\xi^{(g)}, \xi^{(g-1)}, \ldots, \xi^{(1)}$ nach der Methode des Resultantensystems (§ 76), wobei man immer wieder homogene Gleichungen erhält, so bleiben schließlich Gleichungen in den s_{ik} allein übrig, welche identisch erfüllt sein müssen. Also sind die Gleichungen auch bei der Spezialisierung $s_{ik} \to \sigma_{ik}$ erfüllt, und das bedeutet, daß das Gleichungssystem (5) sich nach den η auflösen läßt.

Noch eine Bemerkung: Eliminiert man aus (4) nicht alle ξ, sondern nur die $\xi^{(g)}, \xi^{(g-1)}, \ldots, \xi^{(2)}$, so bleiben neben den s_{ik} die $\xi_i^{(1)}$ übrig. Sind nun solche Größen $\eta_i^{(1)}$ gegeben, von denen man weiß, daß alle algebraischen Relationen, die zwischen den s_{ik} und den $\xi_i^{(1)}$ bestehen und homogen in den $\xi_i^{(1)}$ sind, auch für die σ_{ik} und die $\eta_i^{(1)}$ gelten, so kann man wie oben erschließen, daß man die $\eta^{(2)}, \ldots, \eta^{(g)}$ so hinzubestimmen kann, daß wieder alle Gleichungen (5) gelten und damit die oben gestellte Forderung erfüllt ist. Diese Bemerkung werden wir nachher noch benutzen.

Die obige Methode gibt nun zwar die Existenz der Größen η, legt aber diese Größen noch nicht eindeutig fest. Um sie festzulegen, bilden wir nach § 79 die u-Resultante R_u des Formensystems (3), d. h. den G.G.T. des Resultantensystems des aus den Formen (3) und einer allgemeinen Linearform $u_x = u_0 x_0 + \cdots + u_n x_n$ bestehenden Formensystems. Da die Formen (3) nur endlichviele gemeinsame Nullstellen haben, so zerfällt ihre u-Resultante R_u nach § 79 in Linearfaktoren, die diesen Nullstellen $\xi^{(\nu)}$ entsprechen:

$$R_u(s_{ik}, u_k) = c \prod_{\nu=1}^{g} (u_0 \xi_0^{(\nu)} + \cdots + u_n \xi_n^{(\nu)})^{\varrho_\nu} \qquad (c = \text{konst.}). \tag{6}$$

Um nun von (6) auf die entsprechende Relation für die η zu schließen, müssen wir zunächst die Konstante c eliminieren und die Gleichung homogen machen. Das gelingt folgendermaßen: Es seien $a_1(s), \ldots, a_h(s)$ die Koeffizienten der Potenzprodukte der u_k auf der linken Seite von (6) und $c\,b_1(\xi), \ldots, c\,b_h(\xi)$ die entsprechenden Koeffizienten rechts. Für $i = 1, \ldots, h$ muß dann $a_i(s) = c\,b_i(\xi)$ sein, und das kommt auf

$$a_i(s)\, b_k(\xi) - a_k(s)\, b_i(\xi) = 0 \qquad (i, k = 1, \ldots, h)$$

hinaus. Diese homogenen Gleichungen müssen bei der Spezialisierung $s_{ik} \to \sigma_{ik}$, $\xi_i^{(\nu)} \to \eta_i^{(\nu)}$ erhalten bleiben. Das ergibt:

$$a_i(\sigma)\, b_k(\eta) - a_k(\sigma)\, b_i(\eta) = 0,$$

mithin, da die $b_i(\eta)$ nicht alle $= 0$ sind,

$$a_i(\sigma) = \gamma\, b_i(\eta),$$

$$R_u(\sigma_{ik}, u_k) = \gamma \prod_{\nu=1}^{g} (u_0 \eta_0^{(\nu)} + \cdots + u_n \eta_n^{(\nu)})^{\varrho_\nu}. \tag{7}$$

Wenn $R_u(\sigma, u)$ nicht identisch verschwindet, muß $\gamma \neq 0$ sein. Dann gibt die Gleichung (7) das Mittel zur wirklichen Berechnung der η: sie ergeben sich aus der Faktorzerlegung des spezialisierten Polynoms $R_u(\sigma_{ik}, u_k)$. Zugleich folgt, daß die η bis auf die Reihenfolge eindeutig bestimmt sind, alles unter der Voraussetzung, daß R_u nicht identisch verschwindet. Das ist aber immer der Fall, wenn die spezialisierten Polynome (3) nur endlichviele gemeinsame Nullstellen im P_n haben. Da nämlich $R_u(s_{ik}, u_k)$ ein gemeinsamer Teiler des Resultantensystems der Formen (3) und u_x ist, so ist $R_u(\sigma_{ik}, u_k)$ ein gemeinsamer Teiler des Resultantensystems der spezialisierten Formen (3) und u_x, und dieses Resultantensystem verschwindet im Falle endlichvieler gemeinsamer Nullstellen der Formen (3) nicht.

Wir müssen also den Fall, daß der spezielle lineare Raum L_{n-r}^* unendlichviele Punkte mit $\mathfrak{M}^*$ gemein hat, ausschließen. Sind nur endlichviele gemeinsame Punkte vorhanden, so können wir nach der obigen Methode *eindeutig bis auf die Reihenfolge die g Schnittpunkte* $\eta^{(1)}, \ldots, \eta^{(g)}$ *bestimmen, „in die"*, wie wir sagen werden, *„die* ξ *bei der Spezialisierung der allgemeinen* L_{n-r}^* *zur speziellen übergehen"*.

Ein und derselbe Schnittpunkt η kann unter den $\eta^{(\nu)}$ mehrmals vorkommen: es sind dann bei der Spezialisierung verschiedene Punkte „zusammengerückt". Die Zahl, die angibt, wie oft ein η unter den $\eta^{(1)}, \ldots, \eta^{(g)}$ vorkommt, heißt die *Multiplizität* oder *Vielfachheit* des Punktes η als Schnittpunkt von $\mathfrak{M}^*$ mit L_{n-r}^*. *Die Summe der Multiplizitäten aller Schnittpunkte ist gleich dem Grad g*, wie sofort ersichtlich.

Es drängt sich jetzt auch die Frage auf: Gibt es Schnittpunkte mit der Multiplizität Null, also solche, die unter den $\eta^{(1)}, \ldots, \eta^{(g)}$ nicht vorkommen? Bei ganz beliebigen Gleichungssystemen kommen solche „Lösungen mit der Multiplizität Null" bei passenden Spezialisierungen gelegentlich vor[1]. Wir werden aber zeigen, daß dies bei unserm Problem (Schnitt von L_{n-r}^* und $\mathfrak{M}^*$) nicht vorkommen kann, sondern daß jeder vorgegebene Schnittpunkt η als $\eta^{(1)}$ gewählt werden kann.

Nach der oben (S. 83) gemachten Bemerkung genügt es dazu, zu beweisen, daß alle in den $\xi_i^{(1)}$ homogenen algebraischen Relationen $F(s_{ik}, \xi_i^{(1)}) = 0$ bei der Spezialisierung $s_{ik} \to \sigma_{ik}$, $\xi^{(1)} \to \eta$ ihre Geltung behalten. Wir nehmen an, daß $\eta_0 \neq 0$ ist, was ja, nötigenfalls durch Umnumerierung der Koordinaten, stets zu erreichen ist, und können dann immer $\xi_0^{(1)} = \eta_0 = 1$ voraussetzen. Weiter können die s_{i0} auf Grund der Beziehung

$$s_{i0} + \sum_{k=1}^{n} s_{ik}\, \xi_k^{(1)} = 0,$$

die auch nach der Spezialisierung bestehen bleibt, aus $F(s_{ik}, \xi_i^{(1)})$ eliminiert werden, indem man s_{i0} durch $-\sum_{k=1}^{n} s_{ik}\, \xi_k^{(1)}$ ersetzt. Denkt man sich wieder die s_{ik} $(k \neq 0)$ zum Grundkörper K adjungiert, so ist $\xi^{(1)}$ ein allgemeiner Punkt von $\mathfrak{M}$ (vgl. den Anfang dieses Paragraphen), und jede Relation $F(\xi_i^{(1)}) = 0$, die für den allgemeinen Punkt $\xi^{(1)}$ gilt, gilt auch für jeden speziellen Punkt η von $\mathfrak{M}$. Also folgt $F(s_{ik}, \eta_i) = 0$ und daraus $F(\sigma_{ik}, \eta_i) = 0$, q. e. d.

---

[1] Vgl. B. L. v. d. Waerden: Der Multiplizitätsbegriff der algebraischen Geometrie, Math. Ann. Bd. 97, S. 756—774, § 5.

Jeder Schnittpunkt von $\mathfrak{M}^*$ und L^*_{n-d} hat also eine nichtverschwindende Schnittpunktsmultiplizität, und die Summe dieser Multiplizitäten ist, wie schon bemerkt, gleich dem Grad von $\mathfrak{M}^*$.

Man kann dasselbe Problem auch in ganz anderer Weise angreifen, nämlich mit Hilfe der Hilbertschen „charakteristischen Funktion". Siehe etwa B. L. v. D. WAERDEN: On Hilbert's function, Proc. Kon. Ak. Amsterdam Bd. 31, S. 749. 1928.

Aufgaben. 1. Der Durchschnitt einer d-dimensionalen Mannigfaltigkeit $\mathfrak{M}$ mit einer allgemeinen L_{n-r} ist für $r < d$ eine $(d-r)$-dimensionale Mannigfaltigkeit von demselben Grade wie $\mathfrak{M}$.

2. Wenn der Durchschnitt einer d-dimensionalen Mannigfaltigkeit $\mathfrak{M}^*$ des projektiven Raumes P_n mit einer speziellen L_{n-r} $(r < d)$ nicht mehr als $d-r$ Dimensionen hat, so kann man den irreduziblen Bestandteilen, in die dieser Durchschnitt zerfällt, solche Vielfachheiten erteilen, daß die Summe der mit den Vielfachheiten multiplizierten Grade gleich dem Grad von $\mathfrak{M}^*$ ist. [Man schneide alles mit einer allgemeinen L_{n-d+r}.]

Vierzehntes Kapitel.

Ganze algebraische Größen.

Die Entwicklung der Idealtheorie hat historisch zwei Ausgangspunkte: die Theorie der ganzen algebraischen Zahlen und die Theorie der Polynomideale. Diese beiden Theorien haben sich aber aus ganz verschiedenen Problemstellungen entwickelt. Während bei den Polynomidealen die Bestimmung der Nullstellen und die Aufstellung der notwendigen und hinreichenden Bedingungen für Zugehörigkeit eines Polynoms zu einem Ideal die zentralen Probleme sind, geht die Theorie der ganzen algebraischen Zahlen von der Frage der Faktorzerlegung aus. Zu dieser Frage kommt man z. B. durch die folgende Betrachtung.

Im Ring der Größen $a + b\sqrt{-5}$, wo a und b ganze rationale Zahlen sind, gilt der Satz von der eindeutigen Faktorzerlegung der Elemente nicht. Die Zahl 9 z. B. läßt die beiden wesentlich verschiedenen Zerlegungen in unzerlegbare[1] Faktoren

$$9 = 3 \cdot 3 = (2 + \sqrt{-5})\,(2 - \sqrt{-5})$$

[1] Daß die Zahlen 3 und $2 \pm \sqrt{-5}$ unzerlegbar sind, folgt leicht daraus, daß ihre Norm 9 ist (§ 35). Wären sie zerlegbar, so müßten entweder beide Faktoren die Norm ± 3 oder ein Faktor die Norm ± 1 haben. Eine Zahl $a + b\sqrt{-5}$ mit der Norm ± 3 gibt es nicht, da dann

$$a^2 + 5b^2 = \pm 3$$

sein müßte, was in ganzen Zahlen unmöglich ist. Eine Zahl mit der Norm ± 1 ist aber notwendig eine der Einheiten ± 1, da

$$a^2 + 5b^2 = \pm 1$$

nur durch $a = \pm 1$, $b = 0$ erfüllbar ist.

zu[1]. Diese Tatsache veranlaßte DEDEKIND (in Nachfolgung von KUMMER, der für Kreisteilungskörper durch Einführung gewisser „idealer Zahlen" die Eindeutigkeit der Faktorzerlegung erzwungen hatte) dazu, den Bereich der Elemente zu dem der (von ihm zuerst so genannten) Ideale zu erweitern. Er konnte zeigen, daß in diesem Bereich jedes Ideal einem eindeutig bestimmten Produkt von Primidealen gleich ist. In der Tat ist im obigen Fall, wenn man die Primideale

$$\mathfrak{p}_1 = (3, 2 + \sqrt{-5}), \quad \mathfrak{p}_2 = (3, 2 - \sqrt{-5})$$

einführt, wie man leicht nachrechnet:

$$(3) = \mathfrak{p}_1 \mathfrak{p}_2; \qquad (2 + \sqrt{-5}) = \mathfrak{p}_1^2; \qquad (2 - \sqrt{-5}) = \mathfrak{p}_2^2,$$

mithin erhält man für das Hauptideal (9) die (einzige) Zerlegung

$$9 = \mathfrak{p}_1^2 \mathfrak{p}_2^2.$$

In diesem Kapitel soll die „klassische" (DEDEKINDsche) Idealtheorie der ganzen Größen eines Körpers in moderner, von E. NOETHER[2] entworfener axiomatischer Gestalt entwickelt werden. Die Darstellung setzt die allgemeine Idealtheorie des zwölften Kapitels nicht voraus, wenn auch auf die gegenseitigen Beziehungen immer hingewiesen werden soll.

§ 97. Endliche $\mathfrak{R}$-Moduln.

Wir betrachten Moduln in bezug auf einen (nicht notwendig kommutativen) Ring $\mathfrak{R}$, d. h. Moduln mit $\mathfrak{R}$ als (Links-) Multiplikatorenbereich. Meist sind die betrachteten Moduln entweder in $\mathfrak{R}$ selbst enthalten (also Linksideale in $\mathfrak{R}$) oder in einem Erweiterungsring $\mathfrak{S}$.

Unter einem *endlichen $\mathfrak{R}$-Modul* versteht man einen Modul $\mathfrak{M}$, der von einer endlichen *Modulbasis* $(a_1, \ldots, a_h)$ erzeugt wird oder dessen Elemente sich durch $a_1, \ldots, a_h$ mit Koeffizienten aus $\mathfrak{R}$ und ganzzahligen Koeffizienten linear ausdrücken lassen:

$$(1) \qquad m = r_1 a_1 + \cdots + r_h a_h + n_1 a_1 + \cdots + n_h a_h$$

($r_\nu \in \mathfrak{R}$, n_ν ganze Zahlen).

---

[1] Ein ähnlicher Sachverhalt ist uns schon früher beim Ring der Zahlen $a + b\sqrt{-3}$ (§ 17, Aufg. 5) begegnet: dort hatte die Zahl 4 zwei verschiedene Zerlegungen. Die eindeutige Faktorzerlegung läßt sich aber in diesem Fall wiederherstellen durch Adjunktion der Größe

$$\varrho = -\tfrac{1}{2} + \tfrac{1}{2}\sqrt{-3}$$

zum Ring (vgl. § 16, Aufg. 5). Eine derartige endliche Erweiterung des Ringes $C[\sqrt{-5}]$ ist aber, wie wir noch sehen werden, unmöglich.

[2] NOETHER, E.: Abstrakter Aufbau der Idealtheorie in algebraischen Zahl- und Funktionenkörpern. Math. Ann. Bd. 96, S. 26—61. 1926.

(Hat $\mathfrak{R}$ ein Einselement, das zugleich Einheitsoperator ist, so sind die Glieder $n_1 a_1, \ldots, n_h a_h$ natürlich überflüssig.) Man schreibt in diesem Fall $\mathfrak{M} = (a_1, \ldots, a_h)$.

Man sagt, daß für einen Modul $\mathfrak{M}$ der *Teilerkettensatz* gilt, wenn jede Kette von Untermoduln $\mathfrak{M}_1, \mathfrak{M}_2, \ldots$ von $\mathfrak{M}$, von denen jeder folgende ein echter Obermodul („Teiler") des vorangehenden ist:

$$\mathfrak{M}_1 \subset \mathfrak{M}_2 \subset \cdots,$$

nach endlichvielen Schritten abbricht.

Satz. *Wenn für $\mathfrak{M}$ der Teilerkettensatz gilt, so hat jeder Untermodul von $\mathfrak{M}$ eine endliche Basis, und umgekehrt.*

Der Satz ist eine Verallgemeinerung des Satzes von § 80 über Idealbasis- und Teilerkettensatz und wird genau so bewiesen. Da wir aber hier Kapitel 12 nicht als bekannt voraussetzen wollen, sei der Beweis noch einmal kurz angegeben:

Um für einen Untermodul $\mathfrak{N}$ eine Basis zu finden, suche man zunächst in $\mathfrak{N}$ ein Element a_1. Ist $(a_1) = \mathfrak{N}$, so ist man fertig; sonst wähle man in $\mathfrak{N}$ ein Element a_2, das nicht in (a_1) enthalten ist. Ist $(a_1, a_2) = \mathfrak{N}$, so ist man fertig; sonst bestimme man ein weiteres a_3, usw. Wenn man nun weiß, daß die Modulkette

$$(a_1) \subset (a_1, a_2) \subset (a_1, a_2, a_3) \subset \cdots$$

nach endlichvielen Gliedern abbrechen muß, so hat $\mathfrak{N}$ eine endliche Basis.

Wenn umgekehrt jeder Untermodul von $\mathfrak{M}$ eine endliche Basis hat und

$$\mathfrak{M}_1 \subset \mathfrak{M}_2 \subset \cdots$$

eine Teilerkette von Untermoduln von $\mathfrak{M}$ ist, so ist die Vereinigungsmenge $\mathfrak{V}$ aller $\mathfrak{M}_\nu$ wieder ein Untermodul, der folglich eine endliche Basis hat:

$$\mathfrak{V} = (a_1, \ldots, a_r).$$

Alle a_ν sind aber schon in einem $\mathfrak{M}_\omega$ der Kette enthalten; also ist $\mathfrak{V} \subseteq \mathfrak{M}_\omega$, mithin $\mathfrak{V} = \mathfrak{M}_\omega$. Die Kette bricht also bei $\mathfrak{M}_\omega$ ab.

Unter welchen Bedingungen nun tatsächlich für $\mathfrak{M}$ der Teilerkettensatz gilt, lehrt der folgende Satz:

Wenn in $\mathfrak{R}$ der Teilerkettensatz für Linksideale gilt und $\mathfrak{M}$ ein endlicher $\mathfrak{R}$-Modul ist, so gilt in $\mathfrak{M}$ der Teilerkettensatz für $\mathfrak{R}$-Moduln.

Gleichbedeutend damit ist (auf Grund des vorigen Satzes):

Wenn in $\mathfrak{R}$ jedes Linksideal eine endliche Idealbasis besitzt und $\mathfrak{M}$ eine endliche $\mathfrak{R}$-Modulbasis hat, so hat auch jeder Untermodul von $\mathfrak{M}$ eine endliche $\mathfrak{R}$-Modulbasis.

Der Beweis ist ganz analog dem Beweis des Hilbertschen Basissatzes (§ 80). Es sei $\mathfrak{M} = (a_1, \ldots, a_h)$, und es sei $\mathfrak{N}$ ein Untermodul

von $\mathfrak{M}$. Jedes Element von $\mathfrak{R}$ läßt sich in der Form (1) schreiben. Sind in dem Ausdruck (1) von den $2h$ Koeffizienten $r_1, \ldots, n_h$ die letzten $2h - l$, also die vom $(l+1)$-ten bis zum $(2h)$-ten, alle Null, so sprechen wir von einem *Ausdruck der Länge* $\leqq l$. Wir betrachten nun alle in $\mathfrak{R}$ vorkommenden Ausdrücke der Länge $\leqq l$. Deren l-te Koeffizienten (r_l oder n_{l-h}) bilden, wie man sofort sieht, ein Linksideal in $\mathfrak{R}$ oder im Ring C der ganzen Zahlen. Dieses Ideal hat eine endliche Basis

$$(b_{l1}, \ldots, b_{ls_l}).$$

Jedes $b_{l\nu}$ ist letzter (l-ter) Koeffizient (r_l oder n_{l-h}) eines gewissen Ausdrucks (1), den wir mit $B_{l\nu}$ bezeichnen:

$$B_{l\nu} = r_1 a_1 + \cdots + b_{l\nu} a_l \quad \text{oder} \quad = r_1 a_1 + \cdots + b_{l\nu} a_{1-h}.$$

Wir behaupten, daß alle diese $B_{l\nu} (l = 1, \ldots, 2h;\ \nu = 1, \ldots, s_l)$ zusammen eine Basis für $\mathfrak{R}$ bilden. In der Tat: Jedes Element (1) von $\mathfrak{R}$, von der Länge l, kann durch Subtraktion einer Linearkombination der $B_{l1}, \ldots, B_{ls_l}$ (mit Koeffizienten aus $\mathfrak{R}$ oder C, je nach dem Wert von l) von seinem letzten (l-ten) Koeffizienten befreit, d. h. auf einen Ausdruck kleinerer Länge zurückgeführt werden; dieser kann in derselben Weise weiter in seiner Länge reduziert werden, bis man schließlich nach wiederholten Subtraktionen von Linearkombinationen der $B_{\lambda\nu}$ Null übrig behält. Jedes Element von $\mathfrak{R}$ läßt sich somit als Linearkombination der $B_{l\nu}$ schreiben, q. e. d. Ist etwa eins der Ideale $(b_{l1}, \ldots, b_{ls_l})$ das Nullideal, so sind die entsprechenden $B_{l\nu}$ sogar in der Basis ganz entbehrlich.

Bemerkungen. Hat $\mathfrak{R}$ ein Einselement, welches Einheitsoperator ist, so kann man in (1) wiederum die Glieder $n_1 a_1, \ldots, n_h a_h$ weglassen und den Beweis entsprechend vereinfachen.

Ist $\mathfrak{R}$ insbesondere ein Hauptidealring, so hat jedes Ideal in $\mathfrak{R}$ eine Basis aus nur einem Element; man erhält also für jedes l nur ein b_l und nur ein B_l. Man findet also in diesem Fall eine Basis $(B_1, \ldots, B_h)$ von ebenso vielen Basiselementen, wie die ursprüngliche Basis von $\mathfrak{M}$ enthielt. War die Basis $(a_1, \ldots, a_h)$ von $\mathfrak{M}$ linear-unabhängig, so zeigt man sehr leicht, daß die Basis $(B_1, \ldots, B_h)$ nach Weglassung derjenigen B_l, die einem $b_l = 0$ entsprechen, wieder linear-unabhängig ist (vgl. § 106).

§ 98. Ganze Größen in bezug auf einen Ring.

Es sei $\mathfrak{R}$ ein Unterring eines Ringes $\mathfrak{T}$.

Ein Element t von $\mathfrak{T}$ heißt *ganz in bezug auf* $\mathfrak{R}$, wenn alle Potenzen[1] von t einem endlichen $\mathfrak{R}$-Modul $(a_1, \ldots, a_m)$ angehören, oder: wenn alle Potenzen von t sich durch endlichviele Größen $a_1, \ldots, a_m$ aus $\mathfrak{T}$

[1] Unter Potenzen werden in diesem Paragraphen nur solche mit positivem Exponenten verstanden.

linear in der Gestalt

$$t^{\varrho} = r_1 a_1 + \cdots + r_m a_m + n_1 a_1 + \cdots + n_m a_m \tag{1}$$

($r_\nu \in \mathfrak{R}$, n_ν ganze Zahlen)

ausdrücken lassen.

Insbesondere ist jedes Element r von $\mathfrak{R}$ ganz in bezug auf $\mathfrak{R}$, da $r, r^2, r^3, \ldots$ dem $\mathfrak{R}$-Modul (r) angehören. Auch das Einselement von $\mathfrak{T}$, wenn vorhanden, ist stets ganz in bezug auf $\mathfrak{R}$.

Ist $\mathfrak{T}$ ein Körper, der also den Quotientenkörper P von $\mathfrak{R}$ umfaßt, so hängen alle Potenzen einer ganzen Größe t linear von endlichvielen Größen $a_1, \ldots, a_m$ mit Koeffizienten aus P ab; denn P enthält nicht nur den Ring $\mathfrak{R}$, sondern auch das Einselement. Mithin gibt es unter den Potenzen von t nur endlichviele in bezug auf P linear-unabhängige; t ist also algebraisch in bezug auf P. Statt „ganze Größe" sagt man daher auch *ganze algebraische Größe*. Nicht jede algebraische Größe ist eine ganze algebraische Größe; denn beispielsweise ist die Zahl $\frac{1}{2}$ oder $\sqrt{\frac{1}{2}}$ zwar algebraisch in bezug auf den Körper der rationalen Zahlen, aber nicht ganz in bezug auf den Ring der ganzen Zahlen.

Ist $\mathfrak{R}$ ein Ring, in dem der Teilerkettensatz für Linksideale gilt, so gilt nach § 97 auch für die Untermoduln des endlichen $\mathfrak{R}$-Moduls $(a_1, \ldots, a_m)$ der Teilerkettensatz. Insbesondere kann also die Modulkette

$$(t) \leqq (t, t^2) \leqq \cdots$$

nicht aus lauter verschiedenen Moduln bestehen; d. h. eine Potenz von t ist durch niedrigere Potenzen linear ausdrückbar:

$$t^h = r_1 t + \cdots + r_{h-1} t^{h-1} + n_1 t + \cdots + n_{h-1} t^{h-1}. \tag{2}$$

Ist umgekehrt t ein Element von $\mathfrak{T}$, welches bei passendem h eine Darstellung in der Gestalt (2) mit Koeffizienten aus $\mathfrak{R}$ bzw. C gestattet, so kann man vermöge (2) sukzessiv auch alle höheren Potenzen von t linear durch die endlichvielen $t, t^2, \ldots, t^{h-1}$ ausdrücken, und somit ist t nach unserer Definition ganz. Damit ist bewiesen:

Gilt in dem Ring $\mathfrak{R}$ der Teilerkettensatz für Linksideale, so ist das Bestehen einer Gleichung von der Gestalt (2) *notwendig und hinreichend für die Ganzheit von t in bezug auf $\mathfrak{R}$.*

Die Gleichung (2) bringt, wenn $\mathfrak{T}$ ein Körper ist, auch das Algebraischsein von t von neuem zum Ausdruck. Hat $\mathfrak{R}$ ein Einselement, so kann man zu den Potenzen von t auch noch $t^0 = 1$ hinzunehmen und außerdem in (2) den Schwanz $n_1 t + \cdots + n_{h-1} t^{h-1}$ weglassen; statt (2) erhält man also die einfachere Gleichung

$$t^h - r_{h-1} t^{h-1} - \cdots - r_0 = 0,$$

deren charakteristisches Merkmal darin besteht, daß der Koeffizient der höchsten Potenz von t Eins ist.

Beispiele: *Ganze algebraische Zahlen* sind diejenigen algebraischen Zahlen, die in bezug auf den Ring C der gewöhnlichen ganzen Zahlen ganz sind, also einer ganzzahligen Gleichung mit dem höchsten Koeffizienten 1 genügen. *Ganze algebraische Funktionen* von $x_1, \ldots, x_n$ sind diejenigen Funktionen aus einem algebraischen Erweiterungskörper von $\mathsf{K}(x_1, \ldots, x_n)$, die ganz in bezug auf den Polynombereich $\mathsf{K}[x_1, \ldots, x_n]$ sind; K ist dabei ein fester Grundkörper. *Absolut-ganze algebraische Funktionen* von $x_1, \ldots, x_n$ sind solche Funktionen, die ganz in bezug auf den ganzzahligen Polynombereich $C[x_1, \ldots, x_n]$ sind.

In einem kommutativen Ring $\mathfrak{T}$ sind Summe, Differenz und Produkt zweier in bezug auf $\mathfrak{R}$ ganzen Größen wieder ganz. Oder: *Die in bezug auf $\mathfrak{R}$ ganzen Größen in $\mathfrak{T}$ bilden einen Ring $\mathfrak{S}$.*

Beweis: Sind alle Potenzen von s durch $a_1, \ldots, a_m$ und alle Potenzen von t durch $b_1, \ldots, b_n$ linear ausdrückbar, so sind alle Potenzen von $s + t$, $s - t$ oder $s \cdot t$ durch $a_1, \ldots, a_m, b_1, \ldots, b_n, a_1 b_1, a_1 b_2, \ldots, a_m b_n$ linear ausdrückbar.

Setzen wir nun den Teilerkettensatz für die Ideale des Ringes $\mathfrak{S}$ voraus, so können wir den *Satz von der Transitivität der Ganzheit* beweisen:

Ist $\mathfrak{S}$ der Ring der ganzen Größen im kommutativen Ring $\mathfrak{T}$ (in bezug auf den Unterring $\mathfrak{R}$) und ist das Element t von $\mathfrak{T}$ ganz in bezug auf $\mathfrak{S}$, so ist t auch ganz in bezug auf $\mathfrak{R}$ (d. h. in $\mathfrak{S}$ enthalten). Oder anders ausgedrückt: *Genügt t einer Gleichung von der Gestalt (2), deren Koeffizienten r_ν ganz in bezug auf $\mathfrak{R}$ sind, so ist t selbst ganz in bezug auf $\mathfrak{R}$.*

Beweis: Durch wiederholte Anwendung der Gleichung (2) kann man alle Potenzen $t^{h+\lambda}$ linear durch $t, t^2, \ldots, t^{h-1}$ ausdrücken mit Koeffizienten, die entweder ganze Zahlen sind oder sich aus Potenzprodukten der r_ν ganzrational zusammensetzen. Zu jedem r_ν gibt es endlichviele Größen aus $\mathfrak{T}$, durch die sich alle Potenzen von r_ν linear mit Koeffizienten aus $\mathfrak{R}$ und ganzzahligen Koeffizienten ausdrücken lassen; alle Potenzprodukte der r_ν sind also durch endlichviele Produkte aus diesen endlichvielen Größen linear ausdrückbar. Multipliziert man diese endlichvielen Produkte mit $t, t^2, \ldots, t^{h-1}$ und nimmt schließlich noch $t, t^2, \ldots, t^{h-1}$ selber hinzu, so erhält man wieder endlichviele Größen, durch die sich nunmehr alle Potenzen von t linear mit Koeffizienten aus $\mathfrak{R}$ und ganzzahligen Koeffizienten ausdrücken lassen.

Ein Ring $\mathfrak{S}$ heißt *ganz-abgeschlossen in einem Oberring $\mathfrak{T}$*, wenn jede in bezug auf $\mathfrak{S}$ ganze Größe von $\mathfrak{T}$ zu $\mathfrak{S}$ gehört. Insbesondere heißt ein Integritätsbereich $\mathfrak{S}$ *ganz-abgeschlossen* schlechthin, wenn er ganz-abgeschlossen in seinem Quotientenkörper Σ ist. Das bedeutet, wie leicht ersichtlich, daß jedes Element t von Σ, dessen sämtliche Potenzen t^ϱ sich als Brüche mit einem festen Nenner aus $\mathfrak{S}$ darstellen lassen, selbst zu $\mathfrak{S}$ gehört. Die endlichvielen Größen, durch die sich alle Potenzen eines ganzen t ausdrücken lassen, können nämlich stets auf einen gemein-

samen Nenner gebracht werden, und wenn umgekehrt alle Potenzen von t sich als Brüche mit Nenner s darstellen lassen, so sind sie alle linear durch die eine Größe s^{-1} ausdrückbar.

Aus dem vorigen Satz folgt nun, daß unter der Voraussetzung der Kommutativität von $\mathfrak{T}$ *der Ring* $\mathfrak{S}$ *aller in bezug auf* $\mathfrak{R}$ *ganzen Größen von* $\mathfrak{T}$ *stets ganz-abgeschlossen in* $\mathfrak{T}$ *ist*[1]*, sobald für die Ideale von* $\mathfrak{S}$ *der Teilerkettensatz gilt.*

Ein hinreichendes, aber keineswegs notwendiges Kriterium für ganze Abgeschlossenheit eines Integritätsbereichs gibt der folgende Satz:

Ein Integritätsbereich mit Einselement, in dem der Satz von der eindeutigen Primfaktorzerlegung der Elemente gilt, ist ganz-abgeschlossen in seinem Quotientenkörper.

Beweis: Jedes Element des Quotientenkörpers läßt sich als Bruch $\frac{a}{b}$ so darstellen, daß a und b keinen Primfaktor gemein haben. Werden dann alle Potenzen von $\frac{a}{b}$ nach Multiplikation mit einer einzigen Größe c von ihrem Nenner befreit, so muß ca^n und daher auch c durch b^n teilbar sein für jedes n, was nur dann möglich ist, wenn b eine Einheit ist und daher $\frac{a}{b} = ab^{-1}$ zum Integritätsbereich gehört.

Aus dem Satz folgt, daß alle Hauptidealringe (insbesondere der Ring C der ganzen Zahlen) sowie jeder ganzzahlige Polynombereich und jeder Polynombereich über einem kommutativen Körper K ganz-abgeschlossen sind.

Aufgaben. 1. Die Einheitswurzeln eines Körpers sind stets ganz in bezug auf jeden Unterring.

2. Welche Zahlen des Gaußschen Zahlkörpers $\Gamma(i)$ sind ganz in bezug auf C? Welche Zahlen des Körpers $\Gamma(\varrho)$ der dritten Einheitswurzeln $(\varrho = -\frac{1}{2} + \frac{1}{2}\sqrt{-3})$?

3. Ist der Integritätsbereich $\mathfrak{R}$ ganz-abgeschlossen, so ist auch der Polynombereich $\mathfrak{R}[x]$ ganz-abgeschlossen.

§ 99. Die ganzen Größen eines Körpers.

Es sei $\mathfrak{R}$ ein Integritätsbereich, P sein Quotientenkörper, Σ ein kommutativer endlicher Erweiterungskörper von P und $\mathfrak{S}$ der Ring

[1] Derselbe Satz kann auch ohne die Voraussetzung des Teilerkettensatzes bewiesen werden, wenn man statt dessen voraussetzt, daß $\mathfrak{R}$ ganz-abgeschlossen in seinem Quotientenkörper P und $\mathfrak{T}$ ein endlicher Erweiterungskörper von P ist. Zum Beweis wird $\mathfrak{T}$ zu einem über P Galoisschen Körper $\mathfrak{T}'$ und $\mathfrak{S}$ zum Ring $\mathfrak{S}'$ der ganzen Größen von $\mathfrak{T}'$ erweitert. Wenn ein Element t ganz in bezug auf $\mathfrak{S}$, also in bezug auf $\mathfrak{S}'$ ist, so sind es auch die konjugierten Größen von t (in bezug auf P) und somit auch die elementarsymmetrischen Funktionen dieser konjugierten Größen, d. h. die Koeffizienten der definierenden Gleichung von t. Auf Grund der ganzen Abgeschlossenheit von $\mathfrak{R}$ gehören dann diese Koeffizienten zu $\mathfrak{R}$, mithin ist t ganz in bezug auf $\mathfrak{R}$ und somit $t \in \mathfrak{S}$.

der in bezug auf $\mathfrak{R}$ ganzen Größen von Σ. Offenbar ist $\mathfrak{S}$ Erweiterungsring von $\mathfrak{R}$. Wir können die Beziehungen zwischen den Ringen $\mathfrak{R}$, $\mathfrak{S}$ und den Körpern P, Σ schematisch so darstellen:

$$\begin{array}{ccc} \mathfrak{R} & \subset & \mathfrak{S} \\ \cap & & \cap \\ \mathsf{P} & \subset & \Sigma \end{array}$$

Diese Bezeichnungen werden für diesen Paragraphen festgehalten. Mit „ganz" ist immer gemeint: ganz in bezug auf $\mathfrak{R}$.

Beispiele. Ist $\mathfrak{R}$ der Ring der gewöhnlichen ganzen Zahlen, so ist P der Körper der rationalen Zahlen, Σ ein Zahlkörper (endlich in bezug auf P) und $\mathfrak{S}$ der Ring der ganzen algebraischen Zahlen des Körpers Σ.

Ist $\mathfrak{R}$ ein Polynombereich: $\mathfrak{R} = \mathsf{K}[x_1, \ldots, x_n]$, so ist P der Körper der rationalen Funktionen; Σ entsteht durch Adjunktion von endlichvielen algebraischen Funktionen, und $\mathfrak{S}$ besteht aus den ganzen algebraischen Funktionen des Körpers Σ. Usw.

Ziel ist die Untersuchung der Idealtheorie in $\mathfrak{S}$. Dazu muß, wie wir wissen, allererst untersucht werden, wie es sich mit dem Teilerkettensatz für die Ideale von $\mathfrak{S}$ verhält. Genauer werden wir fragen, ob sich der Teilerkettensatz, falls er für $\mathfrak{R}$ gilt, auf $\mathfrak{S}$ überträgt. Nach den Sätzen des § 97 gelingt diese Übertragung, sobald eine $\mathfrak{R}$-Modulbasis für $\mathfrak{S}$ gefunden ist. Das wird also unser erstes Ziel sein.

Zunächst ein vorbereitender Satz:

Ist σ ein Element von Σ, so ist $\sigma = \frac{s}{r}$, wo $s \in \mathfrak{S}$, $r \in \mathfrak{R}$.

Beweis: Das Element σ genügt einer Gleichung mit Koeffizienten aus P. Diese Koeffizienten sind gebrochen in bezug auf $\mathfrak{R}$. Durch Multiplikation mit dem Produkt der Nenner verwandelt man sie in Größen aus $\mathfrak{R}$:

$$r_0 \sigma^m + r_1 \sigma^{m-1} + \cdots + r_m = 0.$$

Setzt man $r_0 = r$ und multipliziert mit r^{m-1}, so kommt:

$$(r\sigma)^m + r_1 (r\sigma)^{m-1} + r_2 r (r\sigma)^{m-2} + \cdots + r_m r^{m-1} = 0.$$

Also ist $r\sigma$ ganz in bezug auf $\mathfrak{R}$. Setzt man $r\sigma = s$, so folgt die Behauptung.

Aus diesem Satz folgt, daß Σ der Quotientenkörper von $\mathfrak{S}$ ist.

Ist ein Element ξ ganz, so sind auch alle Konjugierten von ξ (in einem über P Galoisschen Erweiterungskörper von Σ) ganz.

Beweis: Die endlichvielen Größen von Σ, durch die sich alle Potenzen von ξ nach Voraussetzung linear ausdrücken lassen, gehen bei einem Isomorphismus von Σ über in endlichviele Größen, durch die sich alle Potenzen einer beliebigen Konjugierten von ξ linear ausdrücken lassen.

Da Summen und Produkte ganzer Größen wieder ganz sind, so sind auch die elementarsymmetrischen Funktionen von ξ und seinen Konjugierten ganz. Daraus folgt:

Wenn in der über P *irreduziblen Gleichung, der eine ganze Größe* ξ *genügt, der höchste Koeffizient gleich* 1 *gewählt wird, so sind alle übrigen Koeffizienten ganz in bezug auf* $\mathfrak{R}$. *Ist insbesondere* $\mathfrak{R}$ *ganz-abgeschlossen in* P, *so liegen alle diese Koeffizienten in* $\mathfrak{R}$.

Dieser Satz gibt bei ganz-abgeschlossenem $\mathfrak{R}$ das bequemste Mittel, zu untersuchen, ob eine Größe ξ ganz ist: man braucht nicht mehr alle Gleichungen zu bilden, denen ξ genügt, und nachzusehen, ob es darunter eine Gleichung mit ganzen Koeffizienten gibt; sondern es genügt, die eine irreduzible Gleichung mit höchstem Koeffizienten 1 zu nehmen. Sind ihre Koeffizienten ganz, so ist ξ es auch; sonst nicht.

Wir machen nun die folgenden einschränkenden Annahmen:

I. $\mathfrak{R}$ *sei ganz-abgeschlossen in seinem Quotientenkörper* P.

II. *In* $\mathfrak{R}$ *gelte der Teilerkettensatz für Ideale.*

III. Σ *sei eine separable Erweiterung von* P.

Aus III folgt nach § 34, daß Σ von einem „primitiven Element" σ erzeugt wird: $\Sigma = \mathsf{P}(\sigma)$. Nach dem obigen Satz ist $\sigma = \frac{s}{r}$ $(s \in \mathfrak{S}, r \in \mathfrak{R})$; also erzeugt auch die ganze Größe s den Körper. s genügt einer Gleichung n-ten Grades, wo n der Körpergrad (Σ/P) ist. Jedes Element ξ von Σ läßt sich darstellen in der Gestalt:

$$\xi = \sum_0^{n-1} \varrho_k s^k \qquad (\varrho_k \in \mathsf{P}). \tag{1}$$

Ersetzt man in (1) s durch seine Konjugierten s_ν (in einem Σ umfassenden Galoisschen Erweiterungskörper von P), von denen es nach § 34 genau n gibt, so erhält man für die Konjugierten ξ_ν von ξ die Gleichungen

$$\xi_\nu = \sum_0^{n-1} \varrho_k s_\nu^k \qquad (\nu = 1, 2, \ldots, n). \tag{2}$$

Die Determinante dieses Gleichungssystems ist:

$$D = |s_\nu^k| = \prod_{\lambda < \mu} (s_\lambda - s_\mu),$$

nach dem Vandermondeschen Determinantensatz. Ihr Quadrat ist eine symmetrische Funktion der s_ν und daher in P enthalten. Da weiter die Konjugierten s_ν alle verschieden sind, ist $D \neq 0$. Man kann also das Gleichungssystem (2) auflösen:

$$\varrho_k = \frac{\sum S_{k\nu} \xi_\nu}{D},$$

wo die $S_{k\nu}$ und D Polynome in den s_ν, also ganz in bezug auf $\mathfrak{R}$ sind. Multiplikation dieser Gleichung mit D^2 ergibt:

$$D^2 \varrho_k = \sum_\nu D S_{k\nu} \xi_\nu. \tag{3}$$

Nehmen wir nun an, ξ sei Element von $\mathfrak{S}$, also ganz, so sind auch die ξ_ν und damit die rechte Seite von (3) ganz. Die linke Seite aber ist ein Element von P. Wegen der ganzen Abgeschlossenheit von $\mathfrak{R}$ in P muß also $D^2\varrho_k$ in $\mathfrak{R}$ liegen. Setzt man $D^2\varrho_k = r_k$, so wird $\varrho_k = r_k D^{-2}$ und daher nach (1)

$$\xi = \sum_0^{n-1} r_k D^{-2} s^k .$$

Jedes Element ξ von $\mathfrak{S}$ läßt sich also durch $D^{-2}s^0, D^{-2}s^1, \ldots, D^{-2}s^{n-1}$ linear mit Koeffizienten aus $\mathfrak{R}$ ausdrücken. Mit anderen Worten: $\mathfrak{S}$ ist enthalten in dem endlichen $\mathfrak{R}$-Modul

$$\mathfrak{M} = (D^{-2}s^0, D^{-2}s^1, \ldots, D^{-2}s^{n-1}) .$$

Daraus folgt nach den Sätzen von § 97, *daß* $\mathfrak{S}$, *sowie jeder Untermodul von* $\mathfrak{S}$ *und insbesondere jedes Ideal in* $\mathfrak{S}$ *eine endliche Modulbasis in bezug auf* $\mathfrak{R}$ *besitzt, oder,* was damit gleichbedeutend ist, *daß für die* $\mathfrak{R}$*-Moduln und insbesondere für die Ideale in* $\mathfrak{S}$ *der Teilerkettensatz gilt.* Ist speziell $\mathfrak{R}$ ein Hauptidealring, so besitzen sogar $\mathfrak{S}$ und jeder Untermodul von $\mathfrak{S}$ eine linear-unabhängige $\mathfrak{R}$-Modulbasis.

Dasselbe Ergebnis gilt auch dann noch, wenn III nicht erfüllt ist, also Σ eine Erweiterung zweiter Art (von der Charakteristik p) ist, vorausgesetzt, daß der Wurzelring $\mathfrak{R}^{\frac{1}{p}}$, der (ähnlich wie im § 33 der Wurzelkörper) aus den p-ten Wurzeln der Elemente von $\mathfrak{R}$ besteht, endlich in bezug auf $\mathfrak{R}$ ist. Dies trifft in allen praktisch interessanten Fällen zu. Ist z. B. $\mathfrak{R}$ ein Polynombereich: $\mathfrak{R} = \mathsf{K}[x_1, \ldots, x_n]$, und K aus dem Primkörper Π entstanden durch Adjunktion von endlichvielen algebraischen oder transzendenten Größen $\vartheta_1, \ldots, \vartheta_r$:

$$\mathsf{K} = \Pi(\vartheta_1, \ldots, \vartheta_r) .$$

so ist

$$\begin{aligned}\mathfrak{R}^{\frac{1}{p}} &= \mathsf{K}^{\frac{1}{p}}[x_1^{\frac{1}{p}}, \ldots, x_n^{\frac{1}{p}}] \\ &= \Pi(\vartheta_1^{\frac{1}{p}}, \ldots, \vartheta_r^{\frac{1}{p}})[x_1^{\frac{1}{p}}, \ldots, x_n^{\frac{1}{p}}];\end{aligned}$$

also hat $\mathfrak{R}^{\frac{1}{p}}$ eine endliche $\mathfrak{R}$-Modulbasis, bestehend aus den Elementen

$$\vartheta_1^{\alpha_1 : p}, \ldots, \vartheta_r^{\alpha_r : p}, x_1^{\beta_1 : p}, \ldots, x_n^{\beta_n : p} \begin{pmatrix} 0 \leqq \alpha_i < p , \\ 0 \leqq \beta_k < p \end{pmatrix}.$$

Ist diese Endlichkeitsbedingung an Stelle von III erfüllt, so beweist man die Endlichkeit von $\mathfrak{S}$ folgendermaßen:

Zunächst folgt aus der Endlichkeit von $\mathfrak{R}^{1:p}$ in bezug auf $\mathfrak{R}$ vermöge der Isomorphie $\mathfrak{R} \simeq \mathfrak{R}^{1:p}$ (vgl. § 33) auch die Endlichkeit von $\mathfrak{R}^{1:p^2}$ in bezug auf $\mathfrak{R}^{1:p}$, usw. So fortfahrend, erschließt man schließlich die Endlichkeit von $\mathfrak{R}^{1:p^e}$ in bezug auf $\mathfrak{R}$.

Es sei nun Δ die größte separable Erweiterung von P, die in Σ enthalten ist. Es sei e der Exponent von Σ. Dann liegt Σ zwischen Δ und $\Delta^{1:p^e}$.

Ist $\mathfrak{D}$ der Ring der ganzen Größen in Δ, so ist $\mathfrak{D}^{1:p^e}$ der Ring der ganzen Größen in $\Delta^{1:p^e}$; denn ein Element von $\Delta^{1:p^e}$ ist dann und nur dann ganz, wenn seine p^e-te Potenz es ist. Der Ring $\mathfrak{S}$ liegt somit zwischen $\mathfrak{D}$ und $\mathfrak{D}^{1:p^e}$. $\mathfrak{D}$ ist endlich in bezug

auf $\mathfrak{R}$ nach dem obigen Beweis, da es sich hier noch um eine Erweiterung erster Art handelt. Wegen der Isomorphie

$$\mathfrak{D} \simeq \mathfrak{D}^{1:p^e}$$

ist somit $\mathfrak{D}^{1:p^e}$ endlich in bezug auf $\mathfrak{R}^{1:p^e}$. Aber $\mathfrak{R}^{1:p^e}$ ist nach Voraussetzung endlich in bezug auf $\mathfrak{R}$; daher ist auch $\mathfrak{D}^{1:p^e}$ endlich in bezug auf $\mathfrak{R}$. Wie vorhin ist also $\mathfrak{S}$ in einen endlichen $\mathfrak{R}$-Modul eingebettet. Von hier an gelten alle unsere früheren Schlüsse.

Unter einer $\mathfrak{R}$-*Ordnung* in Σ versteht man einen Unterring von Σ, der $\mathfrak{R}$ umfaßt und endlicher $\mathfrak{R}$-Modul ist. Nach dem Obigen ist $\mathfrak{S}$ eine $\mathfrak{R}$-Ordnung und jeder Ring zwischen $\mathfrak{R}$ und $\mathfrak{S}$ auch. Umgekehrt folgt aus der Ganzheitsdefinition sofort, daß jede $\mathfrak{R}$-Ordnung $\mathfrak{T}$ in Σ aus lauter ganzen Größen besteht, d. h. in $\mathfrak{S}$ enthalten ist. Mithin kann man $\mathfrak{S}$ charakterisieren als die umfassendste $\mathfrak{R}$-Ordnung in Σ. Man nennt $\mathfrak{S}$ auch die *Hauptordnung* des Körpers Σ. Wenn von „Idealen des Körpers", „Einheiten des Körpers" usw. die Rede ist, so sind damit immer die Ideale von $\mathfrak{S}$, die Einheiten von $\mathfrak{S}$ usw. gemeint. Nach § 98 ist $\mathfrak{S}$ ganz-abgeschlossen in Σ.

Die Ergebnisse dieses Paragraphen gelten größtenteils ungeändert, wenn Σ nicht ein Körper, sondern ein kommutatives hyperkomplexes System über P ist, welches dargestellt werden kann als eine Summe von Körpern, die sich gegenseitig annullieren. Sie gelten aber nicht mehr für nichtkommutative hyperkomplexe Systeme über P, und zwar scheitert die Sache hauptsächlich daran, daß die Summe zweier ganzen Größen nicht mehr ganz zu sein braucht. Die Gesamtheit der ganzen Größen ist daher keine Ordnung. Wohl besteht jede Ordnung aus lauter ganzen Größen, aber es gibt nicht eine alle Ordnungen umfassende Hauptordnung. Unter passenden Voraussetzungen über Σ gibt es verschiedene maximale $\mathfrak{R}$-Ordnungen, so daß jede $\mathfrak{R}$-Ordnung und auch jedes ganze Element in mindestens einer maximalen $\mathfrak{R}$-Ordnung enthalten ist. Über die Idealtheorie dieser maximalen $\mathfrak{R}$-Ordnungen siehe L. E. Dickson: Algebras and their Arithmetics, Chicago 1923; E. Artin: Zur Arithmetik der hyperkomplexen Systeme, Abh. Math. Sem. Hamburg, Bd. 5, S. 261—289. 1927; H. Brandt: Zur Idealtheorie Dedekindscher Algebren, Commentarii Mathematici Helvetici, Bd. 2, S. 13—17. 1930.

In allen $\mathfrak{R}$-Ordnungen von Σ gilt nach dem soeben Bewiesenen der Teilerkettensatz. Daher gelten für diese Ordnungen auch die Zerlegungs- und Eindeutigkeitssätze der §§ 83 und 84 (Darstellung aller Ideale als Durchschnitte von Primäridealen).

Eine große Vereinfachung dieser Idealtheorie tritt nach § 86, Schluß, dann ein, wenn jedes vom Nullideal verschiedene Primideal der Ordnung $\mathfrak{o}$ teilerlos ist. Der folgende Satz gibt an, wann das der Fall ist:

Ist in $\mathfrak{R}$ *jedes Primideal* $\neq (0)$ *teilerlos, so ist auch in jeder* $\mathfrak{R}$*-Ordnung* $\mathfrak{o}$ *jedes Primideal* $\neq (0)$ *teilerlos.*

Beweis: Es sei $\mathfrak{p}$ ein Primideal in $\mathfrak{o}$, welches ein von Null verschiedenes Element t enthält. t genügt einer Gleichung niedrigsten Grades mit Koeffizienten aus $\mathfrak{R}$ und höchstem Koeffizienten Eins:

$$t^h + a_1 t^{h-1} + \cdots + a_h = 0,$$

in der $a_h \neq 0$ sein muß, da sonst die ganze Gleichung durch t gekürzt werden könnte. Es folgt $a_h \equiv 0\,(t) \equiv 0\,(\mathfrak{p})$, also gehört a_h dem Durchschnitt $\mathfrak{p} \cap \mathfrak{R}$ an. Dieser Durchschnitt ist ein Primideal in $\mathfrak{R}$, denn wenn ein Produkt zweier Elemente von $\mathfrak{R}$ zu $\mathfrak{R} \cap \mathfrak{p}$, also zu $\mathfrak{p}$ gehört, so muß ein Faktor zu $\mathfrak{p}$, also zu $\mathfrak{R} \cap \mathfrak{p}$ gehören. Da a_h zum Primideal $\mathfrak{R} \cap \mathfrak{p}$ gehört, ist dieses Primideal vom Nullideal verschieden, also teilerlos.

Ist nun $\mathfrak{a}$ ein echter Teiler von $\mathfrak{p}$, u ein Element von $\mathfrak{a}$, das nicht zu $\mathfrak{p}$ gehört, so genügt u wieder einer Gleichung

$$u^l + b_1 u^{l-1} + \cdots + b_l = 0,$$

also auch einer Kongruenz niedrigsten Grades

$$u^k + c_1 u^{k-1} + \cdots + c_k \equiv 0\,(\mathfrak{p}),$$

in der wiederum $c_k \not\equiv 0\,(\mathfrak{p})$ sein muß, da sonst Kürzung durch u möglich wäre. Es folgt nun $c_k \equiv 0\,(u) \equiv 0\,(\mathfrak{a})$, also gehört c_k dem Durchschnitt $\mathfrak{a} \cap \mathfrak{R}$ an, ohne zu $\mathfrak{p} \cap \mathfrak{R}$ zu gehören. Dieser Durchschnitt $\mathfrak{a} \cap \mathfrak{R}$ ist also ein echter Teiler von $\mathfrak{p} \cap \mathfrak{R}$, mithin gleich dem Einheitsideal $\mathfrak{R}$. Also enthält $\mathfrak{a}$ das Einselement, mithin ist $\mathfrak{a} = \mathfrak{o}$, q. e. d.

Die Voraussetzungen dieses Satzes sind insbesondere dann erfüllt, wenn $\mathfrak{R}$ ein Hauptidealring (Ring der ganzen Zahlen, Polynombereich einer Variablen) ist. Dann gilt also für $\mathfrak{o}$ der Satz, daß jedes von Null- und Einheitsideal verschiedene Ideal sich eindeutig als Produkt von teilerfremden und von $\mathfrak{o}$ verschiedenen Primäridealen darstellen läßt.

Für die Hauptordnung $\mathfrak{S}$ gilt aber, wie wir sehen werden, noch mehr: die Primärideale sind Primidealpotenzen, also *jedes Ideal Produkt von Primidealpotenzen.* Wir werden für dieses Hauptresultat der „klassischen" Dedekindschen Idealtheorie wegen seiner Bedeutung für die Theorie der Zahlen- und Funktionenkörper eine direkte Begründung geben, ohne auf den Begriff des Primärideals und auf die allgemeine Idealtheorie Bezug zu nehmen. Das soll im nächsten Paragraphen nach einer von W. KRULL[1] angegebenen Methode geschehen.

Aufgaben. 1. Ist $\mathfrak{R}$ ein Hauptidealring, $(\omega_1, \ldots, \omega_n)$ die in diesem Fall stets existierende linear-unabhängige Basis einer Ordnung $\mathfrak{o}$ und sind $(\omega_1^{(i)}, \ldots, \omega_n^{(i)})$ die konjugierten Basen in einem Galoisschen Erweiterungskörper von P, so ist die „Körperdiskriminante"

$$D = \begin{vmatrix} \omega_1^{(1)} \ldots \omega_n^{(1)} \\ \cdots\cdots\cdots \\ \omega_1^{(n)} \ldots \omega_n^{(n)} \end{vmatrix}^2$$

ganz, rational und von Null verschieden.

---

[1] KRULL, W.: Zur Theorie der allgemeinen Zahlringe. Math. Ann. Bd. 99 S. 51—70. 1928.

2. Es sei $\Sigma = \mathsf{P}(\sqrt{d})$ und $\mathfrak{R}$ ganz-abgeschlossen in P. Zu beweisen: Alle und nur die Zahlen $\xi = a + b\sqrt{d}$ sind ganz in bezug auf $\mathfrak{R}$, deren Spur und Norm:

$$S(\xi) = \xi + \xi' = (a + b\sqrt{d}) + (a - b\sqrt{d}) = 2a,$$
$$N(\xi) = \xi \cdot \xi' = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - b^2 d$$

beide zu $\mathfrak{R}$ gehören.

3. Ist, in Aufgabe 2, $\mathfrak{R} = \mathsf{K}[x]$ ein Polynombereich einer Unbestimmten und d ein Polynom, das keine mehrfachen Faktoren enthält, so ist $\xi = a + b\sqrt{d}$ nur dann ganz, wenn a und b zu $\mathfrak{R}$ gehören.

4. Ist, in Aufgabe 2, $\mathfrak{R} = C$ der Ring der ganzen Zahlen und d eine quadratfreie ganze Zahl, so besteht eine Basis der Hauptordnung im Fall $d \not\equiv 1\,(4)$ aus den Zahlen 1, $\sqrt{d}$; im Fall $d \equiv 1\,(4)$ aus den Zahlen 1, $\frac{1 + \sqrt{d}}{2}$.

§ 100. Axiomatische Begründung der klassischen Idealtheorie.

Es sei $\mathfrak{o}$ ein Integritätsbereich (kommutativer Ring ohne Nullteiler), in dem folgende drei Axiome erfüllt sind:

I. Der Teilerkettensatz für Ideale.

II. Alle vom Nullideal verschiedenen Primideale sind teilerlos.

III. $\mathfrak{o}$ ist ganz-abgeschlossen im Quotientenkörper Σ.

Beispiele von solchen Ringen sind: 1. die Hauptidealringe; 2. die Hauptordnungen, die bei endlicher Erweiterung des Quotientenkörpers nach dem Schema von § 99 aus Hauptidealringen hervorgehen (insbesondere also die Hauptordnungen in Zahlkörpern und Funktionenkörpern einer Veränderlichen).

Elemente von Σ, die ganz in bezug auf $\mathfrak{o}$ sind, also nach III in $\mathfrak{o}$ liegen, werden einfach *ganz* genannt. Insbesondere ist das Einselement von Σ stets ganz, mithin ist $\mathfrak{o}$ ein Integritätsbereich mit Einselement.

Wir betrachten nun neben den Idealen von $\mathfrak{o}$ (oder $\mathfrak{o}$-Moduln in $\mathfrak{o}$) noch $\mathfrak{o}$-*Moduln in* Σ, d. h. Untermengen von Σ, die mit a und b auch $a - b$, mit a auch ra (wo r ganz ist) enthalten. Falls ein solcher $\mathfrak{o}$-Modul eine endliche Modulbasis hat, nennt man ihn auch *gebrochenes Ideal*. Besteht ein $\mathfrak{o}$-Modul $\mathfrak{a}$ aus lauter ganzen Größen ($\mathfrak{a} \subseteq \mathfrak{o}$), so ist er ein Ideal im gewöhnlichen Sinn oder, wie wir jetzt sagen, ein *ganzes Ideal*.

Unter der *Summe* oder dem *G. G. T.* $(\mathfrak{a}, \mathfrak{b})$ zweier $\mathfrak{o}$-Moduln $\mathfrak{a}$ und $\mathfrak{b}$ verstehen wir (wie bei Idealen) den Modul aller Summen $a + b$ mit $a \in \mathfrak{a}$, $b \in \mathfrak{b}$; ebenso unter dem Produkt $\mathfrak{a}\mathfrak{b}$ den von allen Produkten ab erzeugten Modul oder die Gesamtheit aller Summen $\sum a_\nu b_\nu$.

Summen und Produkte von $\mathfrak{o}$-Moduln mit endlicher Basis haben wieder endliche Basis.

In den folgenden Sätzen bezeichnen die deutschen Buchstaben ausschließlich *ganze, vom Nullideal verschiedene* Ideale in $\mathfrak{o}$, während der Buchstabe $\mathfrak{p}$ immer ein *Primideal* $\neq (0)$ angibt.

Hilfssatz 1. *Zu jedem Ideal* $\mathfrak{a}$ *gibt es ein Produkt von Primidealen* $\mathfrak{p}_i$, *Teilern von* $\mathfrak{a}$, *welches durch* $\mathfrak{a}$ *teilbar ist*:

$$\mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_r \equiv 0(\mathfrak{a}).^1$$

Erster Beweis: Setzt man den allgemeinen Zerlegungssatz (§ 83) als bekannt voraus, so hat man:

$$\mathfrak{a} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_s],$$
$$\mathfrak{p}_i^{e_i} \equiv 0(\mathfrak{q}_i),$$
$$\prod_1^s \mathfrak{p}_i^{e_i} \equiv 0([\mathfrak{q}_1, \ldots, \mathfrak{q}_s]) \equiv 0(\mathfrak{a}).$$

Zweiter Beweis: Ohne Benutzung von Primäridealen kann man folgendermaßen schließen.

Ist $\mathfrak{a}$ prim, so ist der Satz richtig. Ist $\mathfrak{a}$ nicht prim, so gibt es ein Produkt zweier Hauptideale $\mathfrak{b}\,\mathfrak{c}$ so, daß

$$\mathfrak{b}\,\mathfrak{c} \equiv 0(\mathfrak{a}), \qquad \mathfrak{b} \not\equiv 0(\mathfrak{a}), \qquad \mathfrak{c} \not\equiv 0(\mathfrak{a}).$$

Die Ideale $\mathfrak{b}' = (\mathfrak{b}, \mathfrak{a})$, $\mathfrak{c}' = (\mathfrak{c}, \mathfrak{a})$ sind echte Teiler von $\mathfrak{a}$, und es ist

$$\mathfrak{b}'\mathfrak{c}' = (\mathfrak{b}, \mathfrak{a}) \cdot (\mathfrak{c}, \mathfrak{a}) = (\mathfrak{b}\,\mathfrak{c}, \mathfrak{b}\,\mathfrak{a}, \mathfrak{a}\,\mathfrak{c}, \mathfrak{a}^2) \equiv 0(\mathfrak{a}, \mathfrak{a}, \mathfrak{a}, \mathfrak{a}) \equiv 0(\mathfrak{a}).$$

Setzt man nun den Satz für die Ideale $\mathfrak{b}'$ und $\mathfrak{c}'$ als richtig voraus, so gibt es ein Produkt $\mathfrak{p}_1 \cdots \mathfrak{p}_s \equiv 0(\mathfrak{b}')$ und ein anderes $\mathfrak{p}_{s+1} \cdots \mathfrak{p}_r \equiv 0(\mathfrak{c}')$. Das Produkt $\mathfrak{p}_1 \cdots \mathfrak{p}_s \mathfrak{p}_{s+1} \cdots \mathfrak{p}_r$ ist dann $\equiv 0(\mathfrak{b}'\cdot\mathfrak{c}') \equiv 0(\mathfrak{a})$ und somit gilt der Satz auch für $\mathfrak{a}$. Wäre der Satz also für ein Ideal $\mathfrak{a}$ nicht gültig, so würde er für einen der beiden echten Teiler $\mathfrak{b}'$ oder $\mathfrak{c}'$ auch nicht gelten; dieser hätte in derselben Weise wieder einen echten Teiler, für den der Satz nicht gälte, usw.; so erhielte man eine unendliche Kette von echten Teilern, was nach Axiom I unmöglich ist. Also gilt der Satz für jedes Ideal $\mathfrak{a}$.

Hilfssatz 2. *Ist* $\mathfrak{p}$ *prim, so folgt aus* $\mathfrak{a}\mathfrak{b} \equiv 0(\mathfrak{p})$, *daß* $\mathfrak{a} \equiv 0(\mathfrak{p})$ *oder* $\mathfrak{b} \equiv 0(\mathfrak{p})$ *ist*[2].

Beweis: Wäre $\mathfrak{a} \not\equiv 0(\mathfrak{p})$ und $\mathfrak{b} \not\equiv 0(\mathfrak{p})$, so gäbe es ein Element a von $\mathfrak{a}$ und ein Element b von $\mathfrak{b}$, die beide nicht zu $\mathfrak{p}$ gehörten. Das Produkt $a\,b$ würde in $\mathfrak{a}\mathfrak{b}$, also in $\mathfrak{p}$ liegen, im Widerspruch zu der Primidealeigenschaft von $\mathfrak{p}$.

Mit $\mathfrak{p}^{-1}$ bezeichnen wir die Gesamtheit der (ganzen oder gebrochenen) Größen a, für die $a\mathfrak{p}$ ganz ist[3]. Offensichtlich ist $\mathfrak{p}^{-1}$ ein $\mathfrak{o}$-Modul.

---

[1] Der Satz beruht ausschließlich auf dem Teilerkettensatz. [2] Vgl. § 82.

[3] Mit $a\mathfrak{p}$ ist die Gesamtheit aller Produkte ac mit $c \in \mathfrak{p}$ gemeint.

Hilfssatz 3. *Ist* $\mathfrak{p} \neq \mathfrak{o}$, *so liegt in* $\mathfrak{p}^{-1}$ *ein nichtganzes Element.*

Beweis: Es sei c ein beliebiges von Null verschiedenes Element von $\mathfrak{p}$. Nach Hilfssatz 1 gibt es ein Produkt von Primidealen

$$\mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_r \equiv 0 (c).$$

Wir können annehmen, daß dieses Produkt unverkürzbar sei, d. h. daß kein Teilprodukt wie $\mathfrak{p}_2 \cdots \mathfrak{p}_r \equiv 0 (c)$ ist. Da das Produkt $\mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_r$ durch $\mathfrak{p}$ teilbar ist, so muß ein Faktor, etwa $\mathfrak{p}_1$, durch $\mathfrak{p}$ teilbar und daher gleich $\mathfrak{p}$ sein.

Mithin ist

$$\mathfrak{p}\, \mathfrak{p}_2 \cdots \mathfrak{p}_r \equiv 0 (c),$$
$$\mathfrak{p}_2 \cdots \mathfrak{p}_r \not\equiv 0 (c).$$

Es gibt also ein nicht zu (c) gehöriges Element b in $\mathfrak{p}_2 \cdots \mathfrak{p}_r$. Für dieses gilt

$$\mathfrak{p}\, b \equiv 0 (\mathfrak{p}\, \mathfrak{p}_2 \cdots \mathfrak{p}_r) \equiv 0 (c).^1$$

Also ist $\mathfrak{p} \frac{b}{c}$ ganz; daher liegt $\frac{b}{c}$ in $\mathfrak{p}^{-1}$. Aber wegen $b \not\equiv 0 (c)$ ist $\frac{b}{c}$ nicht ganz, q. e. d.

Satz 1. *Ist* $\mathfrak{p} \neq \mathfrak{o}$, *so ist*

$$\mathfrak{p} \cdot \mathfrak{p}^{-1} = \mathfrak{o}.$$

Beweis: Nach Definition von $\mathfrak{p}^{-1}$ ist $\mathfrak{o} \subseteq \mathfrak{p}^{-1}$, mithin $\mathfrak{p} = \mathfrak{o}\mathfrak{p} \subseteq \mathfrak{p}^{-1}\mathfrak{p}$. Das ganze Ideal $\mathfrak{p}\mathfrak{p}^{-1}$ ist also Teiler von $\mathfrak{p}$, mithin entweder $= \mathfrak{p}$ oder $= \mathfrak{o}$. Angenommen, es wäre

$$\mathfrak{p} \cdot \mathfrak{p}^{-1} = \mathfrak{p}.$$

Daraus würde folgen: $\mathfrak{p} \cdot (\mathfrak{p}^{-1})^2 = (\mathfrak{p}\mathfrak{p}^{-1})\mathfrak{p}^{-1} = \mathfrak{p}\mathfrak{p}^{-1} = \mathfrak{p}$ und ebenso $\mathfrak{p}(\mathfrak{p}^{-1})^3 = \mathfrak{p}$, usw. Ist also $a \neq 0$ ein beliebiges Element von $\mathfrak{p}$ und b eins von $\mathfrak{p}^{-1}$, so ist $ab^e \in \mathfrak{p}(\mathfrak{p}^{-1})^e$ ganz, mithin sind alle Potenzen von b als Brüche mit dem festen Nenner a darstellbar. Also ist b ganz. Das gilt von jedem b aus $\mathfrak{p}^{-1}$, entgegen Hilfssatz 3.

Jetzt sind wir imstande, den Hauptsatz über die Faktorzerlegung zu beweisen:

Satz 2. *Jedes Ideal* $\mathfrak{a}$ *ist Produkt von Primidealen.*

Beweis: Wir können $\mathfrak{a} \neq \mathfrak{o}$ voraussetzen. Es sei nach Hilfssatz 1

$$\mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_r \equiv 0 (\mathfrak{a}) \equiv 0 (\mathfrak{p}_1) \tag{1}$$

und die Anzahl r sei möglichst klein gewählt, so daß kein kürzeres Produkt $\equiv 0 (\mathfrak{a})$ ist. Multipliziert man (1) mit $\mathfrak{p}_1^{-1}$, so kommt

$$\mathfrak{p}_2 \cdots \mathfrak{p}_r \equiv 0 (\mathfrak{p}_1^{-1} \mathfrak{a}) \equiv 0 (\mathfrak{o});$$

---

[1] Auch diese Schlußweise kann abgekürzt werden, wenn man die allgemeine Idealtheorie als bekannt voraussetzt. Ist nämlich $c \equiv 0 (\mathfrak{p})$, so kommt $\mathfrak{p}$ unter den *zugehörigen Primidealen* von (c) vor, also ist nach § 84 $(c) : \mathfrak{p} \neq (c)$, d. h. es gibt ein nicht zu (c) gehöriges Element b, so daß $\mathfrak{p}\, b \equiv 0 (c)$ ist.

also ist $\mathfrak{p}_1^{-1}\mathfrak{a}$ ein ganzes Ideal, welches schon in einem Produkt von weniger als r Primidealen aufgeht. Machen wir nun eine Induktion nach r, d. h. nehmen wir an, daß für Ideale, die in einem Produkt von weniger als r Primidealen $\neq (0)$ aufgehen, der Satz schon bewiesen sei (für Ideale, die in *einem* Primideal $\neq (0)$ aufgehen, ist ja alles klar), so gilt der Satz insbesondere für $\mathfrak{p}_1^{-1}\mathfrak{a}$, d. h. es ist

$$\mathfrak{p}_1^{-1}\mathfrak{a} = \mathfrak{p}_2' \cdots \mathfrak{p}_s'.$$

Beiderseitige Multiplikation mit $\mathfrak{p}_1$ ergibt die gesuchte Darstellung für $\mathfrak{a}$.

Die Eindeutigkeit dieser Darstellung folgt aus

Satz 3. *Ist* $\mathfrak{a} \equiv 0\,(\mathfrak{b})$ *und* $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$, $\mathfrak{b} = \mathfrak{p}_1' \cdots \mathfrak{p}_s'$, *so kommt jedes von* $\mathfrak{o}$ *verschiedene Primideal, das in der Darstellung von* $\mathfrak{b}$ *vorkommt, auch in der Darstellung von* $\mathfrak{a}$, *und zwar mindestens ebenso oft vor.*

Beweis: Es sei $\mathfrak{p}_1' \neq \mathfrak{o}$. Da $\mathfrak{p}_1'$ Teiler von $\mathfrak{a}$ ist, so muß $\mathfrak{p}_1'$ unter den $\mathfrak{p}_\nu$ vorkommen (Hilfssatz 2). Es sei etwa $\mathfrak{p}_1 = \mathfrak{p}_1'$. Man hat

$$\mathfrak{p}_1^{-1}\mathfrak{a} \equiv 0\,(\mathfrak{p}_1^{-1}\mathfrak{b}),$$
$$\mathfrak{p}_1^{-1}\mathfrak{a} = \mathfrak{p}_2 \cdots \mathfrak{p}_r,$$
$$\mathfrak{p}_1^{-1}\mathfrak{b} = \mathfrak{p}_2' \cdots \mathfrak{p}_s'.$$

Nehmen wir die Behauptung für kleinere Werte von s als bewiesen an (für $s = 0$, $\mathfrak{b} = \mathfrak{o}$ ist sie trivial), so folgt, daß jedes von $\mathfrak{o}$ verschiedene der Ideale $\mathfrak{p}_2', \ldots, \mathfrak{p}_s'$ mindestens gleich oft unter $\mathfrak{p}_2, \ldots, \mathfrak{p}_r$ vorkommt, und daraus die Behauptung.

Folgerungen. 1. *Die Darstellung eines Ideals* $\mathfrak{a}$ *als Produkt von Primidealen ist bis auf die Reihenfolge der Faktoren und bis auf Faktoren* $\mathfrak{o}$ *eindeutig.*

2. *Aus Teilbarkeit folgt Produktdarstellung: Ist* $\mathfrak{a} \equiv 0\,(\mathfrak{b})$, *so ist* $\mathfrak{a} = \mathfrak{b}\mathfrak{c}$ *mit ganzem* $\mathfrak{c}$.

Man hat nämlich für $\mathfrak{c}$ nur das Produkt derjenigen Primfaktoren von $\mathfrak{a}$ zu nehmen, die übrigbleiben, wenn man diejenigen von $\mathfrak{b}$ (jeden so oft, wie er in $\mathfrak{b}$ vorkommt) aus der Darstellung von $\mathfrak{a}$ streicht.

Ist $\mathfrak{o}$ ein kommutativer Ring *mit* Nullteilern, so gilt die ganze Theorie dieses Paragraphen ohne wesentliche Modifikationen, wenn man sich nur auf solche Ideale beschränkt, die nicht aus lauter Nullteilern bestehen. Die Axiome I und II müssen für die Nicht-Nullteilerideale als gültig vorausgesetzt werden, während man in Axiom III den Quotientenkörper durch den *Quotientenring* zu ersetzen hat, d. h. durch den Ring aller Brüche $\frac{a}{b}$, wo b kein Nullteiler ist. Als Ergebnis erhält man die Sätze 1, 2, 3 für Nicht-Nullteilerideale.

§ 101. Umkehrung und Ergänzung der Ergebnisse.

Wir sahen, daß aus den Axiomen I bis III (§ 100) die Sätze 2 und 3 folgen, welche zusammen die eindeutige Primfaktorzerlegung der Ideale besagen. Dieser Sachverhalt läßt sich nun umkehren:

Es sei $\mathfrak{o}$ *ein Integritätsbereich mit Einselement. In* $\mathfrak{o}$ *sei jedes Ideal* $\mathfrak{a}$ *darstellbar als Produkt von Primidealen:* $\mathfrak{a} = \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r$, *und wenn* $\mathfrak{a}$ *durch* $\mathfrak{b}$ *teilbar ist, so möge in jeder Zerlegung von* $\mathfrak{a}$ *jeder von* $\mathfrak{o}$ *verschiedene Faktor einer Zerlegung von* $\mathfrak{b}$ *mindestens so oft vorkommen. Dann gelten in* $\mathfrak{o}$ *die Axiome I bis III.*

Beweis: Der Kettensatz (Axiom I) folgt unmittelbar daraus, daß jedes Ideal $\mathfrak{a} = \mathfrak{p}_1^{\varrho_1} \cdots \mathfrak{p}_r^{\varrho_r}$ nur endlichviele Teiler $\mathfrak{b} = \mathfrak{p}_1^{\sigma_1} \cdots \mathfrak{p}_r^{\sigma_r}$ $(\sigma_i \leqq \varrho_i)$ hat. Insbesondere hat ein Primideal $\mathfrak{p}$ nur die Teiler $\mathfrak{p}$ und $\mathfrak{o}$, also ist auch Axiom II erfüllt.

Um schließlich Axiom III (die ganze Abgeschlossenheit von $\mathfrak{o}$ im Quotientenkörper Σ) zu beweisen, nehmen wir an, λ sei ein Element von Σ, das ganz in bezug auf $\mathfrak{o}$ ist, so daß etwa λ^m sich durch $\lambda^0, \ldots, \lambda^{m-1}$ linear ausdrückt oder, was auf dasselbe hinauskommt, im $\mathfrak{o}$-Modul $\mathfrak{l} = (\lambda^0, \lambda^1, \ldots, \lambda^{m-1})$ liegt. Ist $\lambda = \frac{a}{b}$, so läßt $\mathfrak{l}$ sich durch Multiplikation mit $\mathfrak{b} = (b^{m-1})$ in ein ganzes Ideal verwandeln. Weiter genügt $\mathfrak{l}$ offenbar der Gleichung $\mathfrak{l}^2 = \mathfrak{l}$. Multiplikation mit $\mathfrak{b}^2$ ergibt:

$$(\mathfrak{l}\mathfrak{b})^2 = (\mathfrak{l}\mathfrak{b})\mathfrak{b}.$$

Daraus folgt wegen der Eindeutigkeit:

$$\mathfrak{l}\mathfrak{b} = \mathfrak{b},$$

also, wenn man noch beide Seiten mit $b^{-(m-1)}$ multipliziert:

$$\mathfrak{l} = \mathfrak{o}.$$

λ ist also Element von $\mathfrak{o}$, q. e. d.

Wir werden jetzt einige Ergänzungen der Sätze 2 und 3 erörtern, welche ebenfalls zur klassischen Idealtheorie gehören.

Die Tatsache, daß aus Teilbarkeit Produktdarstellung folgt, gestattet es, größte gemeinsame Teiler und kleinste gemeinsame Vielfache von Idealen in gleicher Weise zu berechnen, wie man es bei ganzen Zahlen mit Hilfe der Primfaktorzerlegung macht.

Es seien $\mathfrak{a}$ und $\mathfrak{b}$ zwei beliebige Ideale:

$$\mathfrak{a} = \mathfrak{p}_1^{\varrho_1} \cdots \mathfrak{p}_r^{\varrho_r},$$
$$\mathfrak{b} = \mathfrak{p}_1^{\sigma_1} \cdots \mathfrak{p}_r^{\sigma_r}$$

(wobei beide Male alle Primfaktoren angeschrieben werden, die in $\mathfrak{a}$ oder $\mathfrak{b}$ vorkommen, eventuell mit Exponenten Null). Jeder gemeinsame Teiler enthält nur Primfaktoren $\mathfrak{p}_i$ der angeschriebenen Reihe, und zwar mit Exponenten $\leqq \tau_i$, wo τ_i die kleinste der Zahlen ϱ_i, σ_i ist. Der größte gemeinsame Teiler $(\mathfrak{a}, \mathfrak{b})$ muß durch jeden gemeinsamen Teiler, insbesondere durch $\mathfrak{p}^{\tau_i}$, teilbar sein. Also kann er nur

$$\mathfrak{p}_1^{\tau_1} \cdots \mathfrak{p}_r^{\tau_r}$$

sein.

* Deutsche Buchstaben stellen wiederum ganze Ideale $\neq (0)$ dar.

Ebenso ist das kleinste gemeinsame Vielfache (der Durchschnitt) $\mathfrak{a} \cap \mathfrak{b}$ von $\mathfrak{a}$ und $\mathfrak{b}$ das Ideal

$$\mathfrak{p}_1^{\mu_1} \cdots \mathfrak{p}_r^{\mu_r},$$

wo μ_i die größte der Zahlen ϱ_i, σ_i ist.

Satz 4. *Ist* $\mathfrak{a} \equiv 0 (\mathfrak{d})$, *so gibt es in* $\mathfrak{d}$ *ein Element* d, *so daß*

$$(\mathfrak{a}, d) = \mathfrak{d}.$$

Beweis: Es sei

$$\mathfrak{a} = \mathfrak{p}_1^{\varrho_1} \cdots \mathfrak{p}_r^{\varrho_r},$$

$$\mathfrak{d} = \mathfrak{p}_1^{\sigma_1} \cdots \mathfrak{p}_r^{\sigma_r}. \qquad (0 \leqq \sigma_i \leqq \varrho_i)$$

Wir haben d so zu wählen, daß d durch $\mathfrak{d}$ teilbar ist, aber keine weiteren Teiler mit $\mathfrak{a}$ gemein hat. Wir setzen

$$\mathfrak{c} = \mathfrak{p}_1^{\sigma_1+1} \cdots \mathfrak{p}_r^{\sigma_r+1},$$

$$\mathfrak{c}_i = \mathfrak{c} : \mathfrak{p}_i = \mathfrak{p}_1^{\sigma_1+1} \cdots \mathfrak{p}_i^{\sigma_i} \cdots \mathfrak{p}_r^{\sigma_r+1}.$$

Dann ist $\mathfrak{c}_i \not\equiv 0 (\mathfrak{c})$. Es gibt also ein Element d_i, das in $\mathfrak{c}_i$, aber nicht in $\mathfrak{c}$ liegt. Es ist dann

$$d_i \equiv 0 (\mathfrak{p}_j^{\sigma_j+1}) \quad \text{für} \quad j \neq i,$$

$$d_i \not\equiv 0 (\mathfrak{p}_i^{\sigma_i+1}).$$

Die Summe

$$d = d_1 + \cdots + d_r$$

ist durch $\mathfrak{d}$ teilbar (weil alle d_i es sind). Aber es ist

$$d \equiv d_i \not\equiv 0 (\mathfrak{p}_i^{\sigma_i+1});$$

also hat d in der Tat mit $\mathfrak{a}$ keine weiteren Faktoren gemein als die Faktoren von $\mathfrak{d}$.

Folgerungen.

1. *Im Restklassenring* $\mathfrak{o}/\mathfrak{a}$ *ist jedes Ideal* $\mathfrak{d}/\mathfrak{a}$ *Hauptideal.* $\mathfrak{d}/\mathfrak{a}$ wird nämlich von der Restklasse $\mathfrak{a} + d$ erzeugt.

2. *Jedes Ideal* $\mathfrak{d}$ *besitzt eine zweigliedrige Basis* (a, d), *wo* $a \neq 0$ *beliebig in* $\mathfrak{d}$ *gewählt werden kann.*

Es sei nämlich a irgendein von Null verschiedenes Element von $\mathfrak{d}$ und $\mathfrak{a} = (a)$. Der obige Satz ergibt $(a, d) = \mathfrak{d}$.

3. *Jedes Ideal* $\mathfrak{d}$ *läßt sich durch Multiplikation mit einem zu einem gegebenen Ideal* $\mathfrak{c}$ *teilerfremden Ideal* $\mathfrak{b}$ *in ein Hauptideal verwandeln.*

Beweis: Wir setzen $\mathfrak{a} = \mathfrak{c}\mathfrak{d}$. Der obige Satz ergibt

$$(\mathfrak{a}, d) = \mathfrak{d}. \tag{1}$$

Da d durch $\mathfrak{d}$ teilbar ist, so können wir setzen

$$(d) = \mathfrak{b}\mathfrak{d}$$

und haben nach (1):

$$(\mathfrak{c}\mathfrak{d}, \mathfrak{b}\mathfrak{d}) = \mathfrak{d}.$$

$\mathfrak{c}$ und $\mathfrak{b}$ müssen also teilerfremd sein.

Aufgabe. Es sei $\mathfrak{O}$ der Ring aller Quotienten $\frac{a}{b}$, wo a und b ganz und b durch gewisse Primideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ nicht teilbar ist. Dann entspricht jedem Ideal $\mathfrak{a}$ von $\mathfrak{o}$ ein Ideal $\mathfrak{A}$ von $\mathfrak{O}$, bestehend aus den Brüchen $\frac{a}{b}$ mit $a \in \mathfrak{a}$. Den Idealen $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ entsprechen Primideale $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$, allen übrigen Primidealen von $\mathfrak{o}$ das Einheitsideal $\mathfrak{O}$. Jedes Ideal in $\mathfrak{O}$ ist eindeutig als Potenzprodukt der Ideale $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ darstellbar. Außerdem ist in $\mathfrak{O}$ jedes Ideal Hauptideal.

§ 102. Gebrochene Ideale.

Einen $\mathfrak{o}$-Modul im Quotientenkörper Σ nannten wir in § 100 *gebrochenes Ideal*, falls er eine endliche Basis besaß. Die Ideale in $\mathfrak{o}$ oder „ganzen Ideale" sind also spezielle gebrochene Ideale.

Ist $(\sigma_1, \ldots, \sigma_r)$ eine solche Basis eines gebrochenen Ideals, so können wir durch Multiplikation mit einem passenden Nenner die gesamte Basis, also auch das Ideal ganz machen.

Läßt sich umgekehrt ein $\mathfrak{o}$-Modul $\mathfrak{a}$ durch Multiplikation mit einer ganzen Größe $b \neq 0$ ganz machen, so hat $b\mathfrak{a}$ als ganzes Ideal eine endliche Basis

$$b\mathfrak{a} = (a_1, \ldots, a_r),$$

und hieraus folgt:

$$\mathfrak{a} = \left(\frac{a_1}{b}, \ldots, \frac{a_r}{b}\right).$$

Damit ist bewiesen:

Ein $\mathfrak{o}$-Modul in Σ ist dann und nur dann endlich, also gebrochenes Ideal, wenn er sich durch Multiplikation mit einer ganzen Größe $b \neq 0$ in ein ganzes Ideal verwandeln läßt.

Wir sahen schon, daß mit $\mathfrak{a}$ und $\mathfrak{b}$ auch $\mathfrak{a} \cdot \mathfrak{b}$ und $(\mathfrak{a}, \mathfrak{b})$ eine endliche Basis haben, also gebrochene Ideale sind. Dasselbe gilt nun aber von dem *Modulquotienten* $\mathfrak{a}:\mathfrak{b}$, wo $\mathfrak{a}$ und $\mathfrak{b}$ ganze Ideale sind und $\mathfrak{b} \neq (0)$ ist[1]. Denn ist $b \neq 0$ irgend ein Element von $\mathfrak{b}$, so ist

$$b \cdot (\mathfrak{a}:\mathfrak{b}) \subseteq \mathfrak{b} \cdot (\mathfrak{a}:\mathfrak{b}) \subseteq \mathfrak{a} \subseteq \mathfrak{o};$$

demnach wird $\mathfrak{a}:\mathfrak{b}$ durch Multiplikation mit b in ein ganzes Ideal verwandelt.

Insbesondere ist stets $\mathfrak{o}:\mathfrak{p} = \mathfrak{p}^{-1}$ ein gebrochenes Ideal.

Jedes ganze oder gebrochene Ideal $\neq (0)$ hat ein Inverses.

Beweis: Es sei $\mathfrak{c}$ ein ganzes oder gebrochenes Ideal $\neq (0)$, und $b \neq 0$ werde so gewählt, daß $b\mathfrak{c}$ ganz ist:

$$b\mathfrak{c} = \mathfrak{a}. \tag{1}$$

[1] Unter dem Modulquotienten $\mathfrak{a}:\mathfrak{b}$ (in Σ) verstehen wir die Gesamtheit der Elemente λ von Σ, für die $\lambda\mathfrak{b} \subseteq \mathfrak{a}$.

Ist nun $\mathfrak{a} = \mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_r$, so ergibt Multiplikation von (1) mit $\mathfrak{p}_1^{-1} \mathfrak{p}_2^{-1} \cdots \mathfrak{p}_r^{-1}$ nach Satz 1 (§ 100):

$$(\mathfrak{p}_1^{-1} \mathfrak{p}_2^{-1} \cdots \mathfrak{p}_r^{-1} \mathfrak{b})\, \mathfrak{c} = \mathfrak{o},$$

womit die Existenz des Inversen

$$\mathfrak{c}^{-1} = \mathfrak{p}_1^{-1} \cdots \mathfrak{p}_r^{-1} \mathfrak{b}$$

nachgewiesen ist.

Aus diesem Satz folgt: *Die ganzen und gebrochenen Ideale* $\neq (0)$ *bilden eine Abelsche Gruppe.*

Die Gleichung $\mathfrak{a}\mathfrak{c} = \mathfrak{b}$ ist also eindeutig nach $\mathfrak{c}$ auflösbar. Die Lösung kann mit $\mathfrak{a}^{-1}\mathfrak{b}$ oder $\frac{\mathfrak{b}}{\mathfrak{a}}$ bezeichnet werden.

Aus den früheren Sätzen folgt noch:

Jedes gebrochene Ideal ist als Quotient zweier ganzen Ideale, also in der Gestalt

$$\frac{\mathfrak{p}_1' \cdots \mathfrak{p}_s'}{\mathfrak{p}_1'' \cdots \mathfrak{p}_t''}$$

darstellbar. Man kann dabei durch jedes Ideal, das sowohl im Zähler wie auch im Nenner steht, kürzen.

Jedes gebrochene Hauptideal (λ) *läßt eine Darstellung als Quotient zweier ganzen Hauptideale zu, derart, daß von irgend r vorgegebenen Primidealen keines sowohl im Zähler wie im Nenner vorkommt.*

Beweis: Es sei in gekürzter Darstellung

$$(\lambda) = \frac{\mathfrak{p}_1' \cdots \mathfrak{p}_s'}{\mathfrak{p}_1'' \cdots \mathfrak{p}_t''},$$

und $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ seien die r vorgegebenen Primideale. Verwandelt man den Nenner durch Multiplikation mit einem zum Produkt $\mathfrak{p}_1 \cdots \mathfrak{p}_r$ teilerfremden Ideal $\mathfrak{b}$ in ein Hauptideal (d), so wird

$$(\lambda) = \frac{\mathfrak{b}\mathfrak{p}_1' \cdots \mathfrak{p}_s'}{\mathfrak{b}\mathfrak{p}_1'' \cdots \mathfrak{p}_t''} = \frac{\mathfrak{b}\mathfrak{p}_1' \cdots \mathfrak{p}_s'}{(d)},$$

also

$$\mathfrak{b}\mathfrak{p}_1' \cdots \mathfrak{p}_s' = (\lambda d).$$

Der Zähler wird also ebenfalls Hauptideal. Keines der Ideale $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ kommt sowohl im Zähler wie im Nenner vor.

Aufgabe. Der Idealbruch $\mathfrak{a}^{-1}\mathfrak{b} = \frac{\mathfrak{b}}{\mathfrak{a}}$ ist gleich dem Modulquotienten $\mathfrak{b} : \mathfrak{a}$.

Für die weitere Entwicklung der Idealtheorie in Zahlkörpern verweisen wir auf das Buch von E. HECKE: Vorlesungen über die Theorie der algebraischen Zahlen, Leipzig 1923. Für die Idealtheorie in Funktionenkörpern und ihre Anwendungen verweisen wir auf die grundlegende Arbeit von DEDEKIND und WEBER: Crelles Journal Bd. 92, S. 181—290. 1882, sowie auf den 2. Band des Weberschen Lehrbuchs der Algebra. Siehe auch SCHMIDT, F. K.: Analytische Zahlentheorie in Körpern der Charakteristik p. Math. Zeitschr. Bd. 33, S. 1—32. 1931.

§ 103. Idealtheorie beliebiger ganz-abgeschlossener Integritätsbereiche.

Es gibt viele wichtige Integritätsbereiche, welche zwar den Axiomen I und III von § 100 genügen, nicht aber dem Axiom II. Ich führe nur die Polynombereiche $K[x_1, \ldots, x_n]$ in mehr als einer Veränderlichen, die ganzzahligen Polynombereiche $C[x_1, \ldots, x_n]$ und deren endliche ganz-abgeschlossene Erweiterungen (Hauptordnungen) an. In allen diesen Ringen kommt es vor, daß ein vom Null- und Einheitsideal verschiedenes Primideal ein ebensolches Primideal zum echten Teiler hat. In diesen Ringen kann also die Idealtheorie des § 100 nicht gelten. Wir werden aber zeigen, daß ihre Hauptergebnisse trotzdem bestehen bleiben, wenn man die Gleichheit der Ideale durch eine „Quasigleichheits"relation ersetzt, die wir sofort definieren werden[1].

Es sei also $\mathfrak{o}$ ein Integritätsbereich, der ganz-abgeschlossen in seinem Quotientenkörper Σ ist. Die deutschen Buchstaben bezeichnen im folgenden vom Nullideal verschiedene gebrochene Ideale, d. h. $\mathfrak{o}$-Moduln in Σ, die durch Multiplikation mit einer nichtverschwindenden Größe aus $\mathfrak{o}$ ganz werden. Unter dem inversen Ideal $\mathfrak{a}^{-1}$ wird wieder die Gesamtheit derjenigen Elemente r von Σ verstanden, für die $r\mathfrak{a}$ ganz ist.

Wir definieren: $\mathfrak{a}$ ist *quasigleich* $\mathfrak{b}$, wenn $\mathfrak{a}^{-1} = \mathfrak{b}^{-1}$ ist. Zeichen: $\mathfrak{a} \sim \mathfrak{b}$. Die Relation $\sim$ ist offenbar reflexiv, symmetrisch und transitiv.

Ebenso heißt $\mathfrak{a}$ ein *Quasiteiler* von $\mathfrak{b}$, $\mathfrak{b}$ ein *Quasivielfaches* von $\mathfrak{a}$, wenn $\mathfrak{a}^{-1} \subseteq \mathfrak{b}^{-1}$, oder, was dasselbe ist, wenn $\mathfrak{a}^{-1}\mathfrak{b}$ ganz ist. Zeichen: $\mathfrak{a} \leqq \mathfrak{b}$ oder $\mathfrak{b} \geqq \mathfrak{a}$.

Die einfachsten Eigenschaften der Zeichen $\leqq$ und $\sim$ sind:

1. Aus $\mathfrak{a} \geqq \mathfrak{b}$ folgt $\mathfrak{a} \leqq \mathfrak{b}$ (Beweis klar).

2. Ist $\mathfrak{a}$ Hauptideal: $\mathfrak{a} = (a)$, so folgt aus $\mathfrak{a} \leqq \mathfrak{b}$ auch umgekehrt $\mathfrak{a} \geqq \mathfrak{b}$. Denn dann ist $\mathfrak{a}^{-1} = (a^{-1})$; aus der Voraussetzung, daß $\mathfrak{a}^{-1}\mathfrak{b}$ ganz ist, folgt also, daß $a^{-1}\mathfrak{b}$ ganz ist, d. h. daß alle Elemente von $\mathfrak{b}$ durch a teilbar sind.

3. Ist $\mathfrak{a} \leqq \mathfrak{b}$ und zugleich $\mathfrak{a} \geqq \mathfrak{b}$, so ist $\mathfrak{a} \sim \mathfrak{b}$.

4. Alle Quasivielfachen $\mathfrak{b}$ von $\mathfrak{a}$, insbesondere also alle zu $\mathfrak{a}$ quasigleichen $\mathfrak{b}$, haben die Eigenschaft $\mathfrak{b} \subseteq (\mathfrak{a}^{-1})^{-1}$. (Unmittelbare Folge der Ganzheit von $\mathfrak{b}\mathfrak{a}^{-1}$.)

Insbesondere ist also $\mathfrak{a} \subseteq (\mathfrak{a}^{-1})^{-1}$. Nach 1. folgt daraus $\mathfrak{a} \geqq (\mathfrak{a}^{-1})^{-1}$. Andererseits ist $\mathfrak{a}^{-1}(\mathfrak{a}^{-1})^{-1}$ ganz, also $\mathfrak{a} \leqq (\mathfrak{a}^{-1})^{-1}$, mithin

$$5. \qquad \mathfrak{a} \sim (\mathfrak{a}^{-1})^{-1}.$$

Nach 4. und 5. ist $(\mathfrak{a}^{-1})^{-1}$ das umfassendste zu $\mathfrak{a}$ quasigleiche Ideal. Wir bezeichnen es mit $\mathfrak{a}^*$.

6. Ist $\mathfrak{a} \leqq \mathfrak{b}$, so ist auch $\mathfrak{a}\mathfrak{c} \leqq \mathfrak{b}\mathfrak{c}$. Denn es ist $(\mathfrak{c}\mathfrak{a})^{-1}\mathfrak{c}\mathfrak{a}$ ganz, also $(\mathfrak{c}\mathfrak{a})^{-1}\mathfrak{c} \subseteq \mathfrak{a}^{-1} \subseteq \mathfrak{b}^{-1}$, mithin $(\mathfrak{c}\mathfrak{a})^{-1}\mathfrak{c}\mathfrak{b}$ ganz, oder $\mathfrak{c}\mathfrak{a} \leqq \mathfrak{c}\mathfrak{b}$.

7. Ist $\mathfrak{a} \sim \mathfrak{b}$, so ist $\mathfrak{a}\mathfrak{c} \sim \mathfrak{b}\mathfrak{c}$. (Folge von 6.)

8. Ist $\mathfrak{a} \sim \mathfrak{b}$ und $\mathfrak{c} \sim \mathfrak{d}$, so ist $\mathfrak{a}\mathfrak{c} \sim \mathfrak{b}\mathfrak{d}$. (Denn nach 7. ist $\mathfrak{a}\mathfrak{c} \sim \mathfrak{b}\mathfrak{c} \sim \mathfrak{b}\mathfrak{d}$.)

Vereinigt man alle einem Ideal quasigleichen Ideale zu einer Klasse, so ist die Klasse des Produktes $\mathfrak{a}\mathfrak{c}$ nach 8. nur von der Klasse von $\mathfrak{a}$ und der Klasse von $\mathfrak{c}$ abhängig. Wir können also das *Produkt* der beiden letzteren Klassen als die Klasse des Produktes $\mathfrak{a}\mathfrak{c}$ definieren.

9. Einheitsklasse bei der Klassenmultiplikation ist die Klasse derjenigen Ideale, die dem Einheitsideal $\mathfrak{o}$ quasigleich sind; denn für jedes $\mathfrak{a}$ ist $\mathfrak{a}\mathfrak{o} = \mathfrak{a}$.

10. Alle Quasivielfachen von $\mathfrak{o}$, insbesondere alle Ideale der Einheitsklasse, sind ganz. (Spezialfall von 2.: man setze $a = 1$.) Folge: Alle zu einem ganzen Ideal quasigleichen Ideale sind wieder ganz.

---

[1] Die vom Verfasser in Math. Ann. Bd. 101 (1929) in einer weniger schönen Form aufgestellte Theorie wurde von Herrn E. Artin auf eine schöne Form gebracht und wird in dieser Form hier zum erstenmal publiziert.

Wir beweisen nun die wichtigste Eigenschaft des Inversen:

11. $$\mathfrak{a}\,\mathfrak{a}^{-1} \sim \mathfrak{o}\,.$$

Daß $\mathfrak{a}\mathfrak{a}^{-1} \geqq \mathfrak{o}$ ist, ist klar; denn $\mathfrak{a}\mathfrak{a}^{-1}$ ist ganz. Es bleibt zu beweisen $\mathfrak{a}\mathfrak{a}^{-1} \leqq \mathfrak{o}$, oder $(\mathfrak{a}\mathfrak{a}^{-1})^{-1} \subseteqq \mathfrak{o}$. Wenn λ zu $(\mathfrak{a}\mathfrak{a}^{-1})^{-1}$ gehört, so ist $\lambda\mathfrak{a}\mathfrak{a}^{-1}$ ganz, also $\lambda\mathfrak{a}^{-1} \subseteqq \mathfrak{a}^{-1}$, also $\lambda^2\mathfrak{a}^{-1} \subseteqq \lambda\mathfrak{a}^{-1} \subseteqq \mathfrak{a}^{-1}$, usw., allgemein $\lambda^n\mathfrak{a}^{-1} \subseteqq \mathfrak{a}^{-1}$, also $\lambda^n\mathfrak{a}^{-1}\mathfrak{a}$ ganz. Ist μ ein beliebiges Element von $\mathfrak{a}^{-1}\mathfrak{a}$, so werden also alle Potenzen von λ nach Multiplikation mit μ ganz. Mittels der ganzen Abgeschlossenheit von $\mathfrak{o}$ folgt daraus, genau wie an der entsprechenden Stelle in § 100, daß λ selber ganz ist.

Aus **11.** folgt, daß bei der oben definierten Klassenmultiplikation die Klasse von $\mathfrak{a}^{-1}$ eine Inverse zur Klasse von $\mathfrak{a}$ darstellt: das Produkt der Klassen von $\mathfrak{a}$ und $\mathfrak{a}^{-1}$ ist die Einheitsklasse. Daraus folgt:

Satz 1. *Die Klassen quasigleicher Ideale bilden eine Gruppe.*

12. Aus $\mathfrak{a} \geqq \mathfrak{b}$ folgt $\mathfrak{a} \sim \mathfrak{b}\mathfrak{c}$ mit ganzem $\mathfrak{c}$, wobei $\mathfrak{c}$ außerdem noch so gewählt werden kann, daß $\mathfrak{b}\mathfrak{c} \subseteqq \mathfrak{a}$. Setzt man nämlich $\mathfrak{a}\mathfrak{b}^{-1} = \mathfrak{c}$, so ist $\mathfrak{c}$ ganz, und zugleich folgt durch beiderseitige Multiplikation mit $\mathfrak{b}$, daß $\mathfrak{a} \sim \mathfrak{b}\mathfrak{c}$ sowie $\mathfrak{b}\mathfrak{c} = \mathfrak{b}\mathfrak{b}^{-1}\mathfrak{a} \subseteqq \mathfrak{o}\mathfrak{a} = \mathfrak{a}$ ist.

Von jetzt an sollen alle deutschen Buchstaben *ganze* vom Nullideal verschiedene Ideale darstellen. Ein solches Ideal $\mathfrak{p}$ nennen wir *unzerlegbar*, wenn es nicht quasigleich $\mathfrak{o}$ ist und in jeder Produktdarstellung $\mathfrak{p} \sim \mathfrak{a}\mathfrak{b}$ notwendig ein Faktor der Einheitsklasse angehört, oder, was nach **12.** dasselbe ist, wenn $\mathfrak{p}$, ohne quasigleich $\mathfrak{o}$ zu sein, keine anderen Quasiteiler hat als solche, die quasigleich $\mathfrak{p}$ oder quasigleich $\mathfrak{o}$ sind.

Ersetzt man ein unzerlegbares Ideal $\mathfrak{p}$ durch das umfassendste quasigleiche Ideal $\mathfrak{p}^*$, so ist jeder ganze echte Teiler von $\mathfrak{p}^*$ notwendig nicht-quasigleich $\mathfrak{p}$, also quasigleich $\mathfrak{o}$. Jedes durch $\mathfrak{p}$ oder $\mathfrak{p}^*$ quasiteilbare Ideal ist nach **4.** durch $\mathfrak{p}^*$ teilbar. Daraus folgt nun weiter:

13. $\mathfrak{p}^*$ ist ein Primideal. Ist nämlich ein Produkt $\mathfrak{b}\mathfrak{c}$ zweier Hauptideale $\mathfrak{b}$ und $\mathfrak{c}$ teilbar durch $\mathfrak{p}^*$, aber $\mathfrak{b}$ nicht teilbar durch $\mathfrak{p}^*$, so ist $(\mathfrak{b}, \mathfrak{p}^*)$ ein echter Teiler von $\mathfrak{p}^*$, also quasigleich $\mathfrak{o}$, mithin

$$\mathfrak{c} = \mathfrak{o}\,\mathfrak{c} \sim (\mathfrak{b}, \mathfrak{p}^*)\,\mathfrak{c} = (\mathfrak{b}\,\mathfrak{c}, \mathfrak{p}^*\,\mathfrak{c}) \geqq (\mathfrak{p}^*, \mathfrak{p}^*) = \mathfrak{p}^*,$$

also $\mathfrak{c}$ quasiteilbar durch $\mathfrak{p}^*$, also teilbar durch $\mathfrak{p}^*$.

In derselben Weise folgt:

14. Wenn ein Produkt $\mathfrak{b}\mathfrak{c}$ durch das unzerlegbare Ideal $\mathfrak{p}$ quasiteilbar ist, so ist ein Faktor ($\mathfrak{b}$ oder $\mathfrak{c}$) durch $\mathfrak{p}$ quasiteilbar. Denn aus Quasiteilbarkeit durch $\mathfrak{p}$ folgt Teilbarkeit durch $\mathfrak{p}^*$, und weiter verläuft der Beweis wie bei **13.**

Setzen wir noch in $\mathfrak{o}$ den Teilerkettensatz voraus, so gilt:

15. Jede Kette von ganzen Idealen $\mathfrak{a}_1 > \mathfrak{a}_2 > \cdots$, wo jedes folgende Ideal ein echter Quasiteiler des vorangehenden (d. h. Quasiteiler und nicht quasigleich) ist, bricht nach endlichvielen Schritten ab. Denn wenn wir die Ideale $\mathfrak{a}_1, \mathfrak{a}_2, \ldots$ durch ihre umfassendsten quasigleichen $\mathfrak{a}_1^*, \mathfrak{a}_2^*, \ldots$ ersetzen, so erhalten wir eine Kette von ganzen Idealen $\mathfrak{a}_1^* \subset \mathfrak{a}_2^* \subset \cdots$, die nach dem Teilerkettensatz abbrechen muß.

Aus **14.** und **15.** folgen Eindeutigkeit und Möglichkeit der Zerlegung aller ganzen Ideale in unzerlegbare in genau derselben Weise wie in § 17. Mithin gilt:

Satz 2. *Jedes vom Nullideal verschiedene ganze Ideal ist quasigleich einem bis auf die Reihenfolge und bis auf Quasigleichheit eindeutig bestimmten Produkt von unzerlegbaren Idealen* $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_r$ (die natürlich auch als Primideale $\mathfrak{p}_1^*, \mathfrak{p}_2^*, \ldots, \mathfrak{p}_r^*$ gewählt werden können).

Zwischen zwei Hauptidealen besteht nach **2.** nur dann Quasiteilbarkeit bzw. Quasigleichheit, wenn Teilbarkeit bzw. Gleichheit besteht. Durch Hinzunahme der Klassen von Nicht-Hauptidealen zu den Hauptidealen erhält man einen neuen

Bereich, in dem nach Satz 2 die eindeutige Primfaktorzerlegung gilt, womit also das Ziel der „klassischen Idealtheorie" erreicht ist[1].

Um aber die Beziehung der jetzt gewonnenen Theorie zu der allgemeinen Idealtheorie und zu der speziellen Idealtheorie von § 100 herzustellen, müssen wir untersuchen, welche Primideale unzerlegbar und welche Ideale quasigleich $\mathfrak{o}$ sind.

Wir haben gesehen: Für unzerlegbares $\mathfrak{p}$ ist $\mathfrak{p}^*$ prim. Wir zeigen nun:

16. Kein vom Nullideal verschiedenes echtes Vielfaches eines solchen $\mathfrak{p}^*$ ist prim. Ist nämlich $\mathfrak{a}$ ein solches, so ist $\mathfrak{a} \geqq \mathfrak{p}^*$; nach 12. ist also etwa $\mathfrak{a} \sim \mathfrak{p}^*\mathfrak{q}$ mit $\mathfrak{p}^*\mathfrak{q} \equiv 0\,(\mathfrak{a})$. Da in der Zerlegung von $\mathfrak{q}$ ein Primfaktor weniger vorkommt als in der von $\mathfrak{a}$, so ist $\mathfrak{q} \not\equiv 0\,(\mathfrak{a})$; ebenso ist $\mathfrak{p}^* \not\equiv 0\,(\mathfrak{a})$. Also ist $\mathfrak{a}$ nicht prim.

Wir betrachten nun die Zerlegung eines beliebigen Primideals $\mathfrak{p}$. Entweder ist $\mathfrak{p} \sim \mathfrak{o}$, oder in der Zerlegung $\mathfrak{p} \sim \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r$ kommt ein unzerlegbarer Faktor $\mathfrak{p}_1$ vor. Dann ist $\mathfrak{p} \geqq \mathfrak{p}_1$, also $\mathfrak{p} \subseteq \mathfrak{p}_1^*$; da aber ein echtes Vielfaches von $\mathfrak{p}_1^*$ nicht prim sein kann, so muß $\mathfrak{p} = \mathfrak{p}_1^*$ sein. Es folgt $\mathfrak{p}^* = (\mathfrak{p}_1^*)^* = \mathfrak{p}_1^* = \mathfrak{p}$; mithin gilt:

17. Jedes Primideal $\mathfrak{p}$ ist entweder quasigleich $\mathfrak{o}$ oder unzerlegbar und gleich dem zugehörigen $\mathfrak{p}^*$.

Im zweiten Fall hat $\mathfrak{p}$ kein vom Nullideal verschiedenes echtes Primidealvielfaches. Hingegen zeigen wir, daß es ein solches im ersten Fall gewiß gibt:

18. Ist $\mathfrak{p} \sim \mathfrak{o}$, so gibt es ein unzerlegbares echtes Primidealvielfaches $\mathfrak{p}_\nu^*$ von $\mathfrak{p}$. Ist nämlich $p \neq 0$ ein Element von $\mathfrak{p}$ und $(p) \sim \mathfrak{p}_1\mathfrak{p}_2 \cdots \mathfrak{p}_r \sim \mathfrak{p}_1^*\mathfrak{p}_2^* \cdots \mathfrak{p}_r^*$ dessen Zerlegung, so folgt aus 2., daß $\mathfrak{p}_1^*\mathfrak{p}_2^* \cdots \mathfrak{p}_r^* \equiv 0\,(p) \equiv 0\,(\mathfrak{p})$, also ein $\mathfrak{p}_\nu^* \equiv 0\,(\mathfrak{p})$ ist. Es ist aber $\mathfrak{p}_\nu^* \neq \mathfrak{p}$, da sonst $\mathfrak{p}_\nu^* \sim \mathfrak{o}$ wäre.

Nennen wir ein Primideal ein *höheres*, wenn es kein vom Nullideal verschiedenes echtes Primidealvielfaches hat, dagegen ein *niederes*, wenn es ein solches Primidealvielfaches gibt, so können wir 16., 17. und 18. zusammenfassen zu

Satz 3. *Jedes höhere Primideal $\mathfrak{p}$ ist unzerlegbar und gleich seinem $\mathfrak{p}^*$; jedes niedere Primideal ist quasigleich $\mathfrak{o}$.*

Ein Ideal, das nicht der Einheitsklasse angehört, ist auf Grund des Zerlegungssatzes 2 durch mindestens ein höheres Primideal $\mathfrak{p} = \mathfrak{p}^*$ teilbar. Ein Ideal der Einheitsklasse ist aber durch kein höheres Primideal teilbar. Damit ist die Einheitsklasse rein idealtheoretisch (d. h. im Bereich der ganzen Ideale) gekennzeichnet. Mit Hilfe dieses Ergebnisses können wir nun auch die Quasiteilbarkeit (oder Quasigleichheit) idealtheoretisch kennzeichnen:

19. Ist $\mathfrak{a} \geqq \mathfrak{b}$, so gibt es ein Ideal $\mathfrak{c}$ der Einheitsklasse, so daß $\mathfrak{a}\mathfrak{c} \equiv 0\,(\mathfrak{b})$ ist. Wählt man nämlich $\mathfrak{c} = \mathfrak{b}^{-1}\mathfrak{b}$, so wird $\mathfrak{a}\mathfrak{c} = (\mathfrak{a}\mathfrak{b}^{-1})\mathfrak{b} \subseteq \mathfrak{b}$, da $\mathfrak{a}\mathfrak{b}^{-1}$ ganz ist.

---

[1] Setzt man für $\mathfrak{o}$ nicht den Teilerkettensatz voraus, so gilt Satz 2 nicht. An dessen Stelle tritt nach E. Artin der folgende „Verfeinerungssatz": Wenn zwei Faktorzerlegungen eines Ideals gegeben sind:

$$\mathfrak{a} \sim \mathfrak{b}_1\mathfrak{b}_2 \ldots \mathfrak{b}_m \sim \mathfrak{c}_1\mathfrak{c}_2 \ldots \mathfrak{c}_n\,,$$

so kann man die beiden Produkte derart weiter zerlegen, daß diese Zerlegungen bis auf die Reihenfolge der Faktoren und bis auf Quasigleichheit übereinstimmen:

$$\mathfrak{b}_\lambda \sim \prod_\mu \mathfrak{b}_{\lambda\mu}$$

$$\mathfrak{c}_\nu \sim \prod_\nu \mathfrak{c}_{\nu\omega}$$

$$\mathfrak{b}_{\lambda\mu} \sim \mathfrak{c}_{\nu\omega} \text{ in irgendeiner Anordnung.}$$

Der Beweis beruht auf der folgenden Verallgemeinerung eines Hilfssatzes aus § 85: Aus $(\mathfrak{a}, \mathfrak{b}) \sim \mathfrak{o}$ und $(\mathfrak{a}, \mathfrak{c}) \sim \mathfrak{o}$ folgt $(\mathfrak{a}, \mathfrak{b}\mathfrak{c}) \sim \mathfrak{o}$. Der Hilfssatz ist leicht zu beweisen, und mit seiner Hilfe gelingt auch der Beweis des Verfeinerungssatzes ohne Mühe, indem man setzt: $(\mathfrak{b}_1, \mathfrak{c}_1) = \mathfrak{b}_{11}$; $\mathfrak{b}_1 \sim \mathfrak{b}_{11}\mathfrak{b}_1'$; $(\mathfrak{b}_1', \mathfrak{c}_2) = \mathfrak{b}_{12}$; $\mathfrak{b}_1' \sim \mathfrak{b}_{12}\mathfrak{b}_1''$; $(\mathfrak{b}_1'', \mathfrak{c}_3) = \mathfrak{b}_{13}$; usw.

Ist von zwei Idealen jedes quasiteilbar durch das andere, so sind sie quasigleich. Man kann aber die Quasigleichheit auch noch anders beschreiben:

20. Ist $\mathfrak{a} \sim \mathfrak{b}$, so gibt es ein $\mathfrak{c} \sim \mathfrak{o}$ und ein $\mathfrak{d} \sim \mathfrak{o}$, so daß $\mathfrak{a}\mathfrak{c} = \mathfrak{b}\mathfrak{d}$. Aus $\mathfrak{a}^{-1} = \mathfrak{b}^{-1}$ folgt nämlich $\mathfrak{a}(\mathfrak{b}^{-1}\mathfrak{b}) = (\mathfrak{a}\mathfrak{a}^{-1})\mathfrak{b}$.

In den in § 100 untersuchten Ringen ist wegen des Axioms II ein von (0) verschiedenes Primideal nur durch sich selbst und durch $\mathfrak{o}$ teilbar; also gibt es dort keine niederen Primideale außer $\mathfrak{o}$. Da jedes Ideal $\mathfrak{a} \neq \mathfrak{o}$ durch ein von $\mathfrak{o}$ verschiedenes Primideal teilbar ist (Beweis: man suche unter den von $\mathfrak{o}$ verschiedenen Teilern von $\mathfrak{a}$ einen umfassendsten; dieser ist teilerlos, also prim), so kann $\mathfrak{a}$ nicht quasigleich $\mathfrak{o}$ sein. Somit besteht die Einheitsklasse nur aus dem Einheitsideal $\mathfrak{o}$. Aus 19. folgt dann weiter, daß Quasiteilbarkeit und Teilbarkeit gleichbedeutend sind, und daraus oder aus 20., daß Quasigleichheit und Gleichheit ebenfalls gleichbedeutend sind. Mithin ist die Idealtheorie von § 100 in der jetzt dargestellten Theorie als Spezialfall enthalten.

Auch der Anschluß an die allgemeine Idealtheorie des zwölften Kapitels ist jetzt leicht herzustellen. Zunächst ist leicht zu sehen, daß jedes Primärideal, dessen zugehöriges Primideal ein niederes ist, quasigleich $\mathfrak{o}$ sein muß. Bezeichnen wir diese Primärideale als *niedere*, die übrigen als *höhere Primärideale*! Ein Ideal $\mathfrak{a}$ ist dann und nur dann quasigleich $\mathfrak{o}$, wenn alle seine Primärkomponenten niedere sind. Stimmen zwei Ideale $\mathfrak{a}$ und $\mathfrak{b}$ in allen höheren Primärkomponenten (aber nicht notwendig in den niederen) überein, so sind sie quasigleich. Unter den $\mathfrak{a}$ quasigleichen Idealen befindet sich ein umfassendstes Ideal $\mathfrak{a}^*$; man erhält es durch Weglassung aller niederen Primärkomponenten aus der Zerlegung $\mathfrak{a} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_r]$. Man kann also die Zerlegungs- und Eindeutigkeitssätze dieses Paragraphen so interpretieren, daß dabei konsequent alle niederen Primärkomponenten vernachlässigt werden und nur auf die höheren geachtet wird. Die höheren Primärideale sind je nur durch ein höheres Primideal teilbar, müssen also bei der Faktorzerlegung nach Satz 2 notwendig eine Primidealpotenz ergeben; d. h.: *Jedes höhere Primärideal ist einer Primidealpotenz quasigleich.* Der Grund dieses Sachverhalts liegt natürlich in der ganzen Abgeschlossenheit des Ringes $\mathfrak{o}$.

Beispiel. Der Ring $C[x, \sqrt{2x}]$ ist ganz-abgeschlossen im Quotientenkörper $\Gamma(\sqrt{2x})$ und erfüllt alle Voraussetzungen dieses Paragraphen. Das Hauptideal $(2x)$ gestattet im Bereich der Hauptideale folgende zwei wesentlich verschiedene Zerlegungen:

$$(2x) = (2) \cdot (x) = (\sqrt{2x})^2.$$

Im Bereich der Hauptideale gilt also *keine* eindeutige Faktorzerlegung: dazu ist die Einführung der Ideale notwendig. Die Primideale $\mathfrak{p}_1 = (x, \sqrt{2x})$ und $\mathfrak{p}_2 = (2, \sqrt{2x})$ sind nicht quasigleich $\mathfrak{o}$; denn ihre Inversen $\mathfrak{p}_1^{-1}$ und $\mathfrak{p}_2^{-1}$ enthalten die nichtganzen Elemente $\frac{\sqrt{2x}}{x}$ bzw. $\frac{\sqrt{2x}}{2}$. Das Primideal $\mathfrak{p}_3 = (2, x, \sqrt{2x})$ ist ein echter Teiler von $\mathfrak{p}_1$ und von $\mathfrak{p}_2$, also quasigleich $\mathfrak{o}$. Man hat

$$\begin{aligned}
\mathfrak{p}_1^2 &= (x^2, x\sqrt{2x}, 2x) &&= (x) \cdot (x, \sqrt{2x}, 2) &&= (x) \cdot \mathfrak{p}_3 &&\sim (x), \\
\mathfrak{p}_2^2 &= (2^2, 2\sqrt{2x}, 2x) &&= (2) \cdot (2, \sqrt{2x}, x) &&= (2) \cdot \mathfrak{p}_3 &&\sim (2), \\
\mathfrak{p}_1\mathfrak{p}_2 &= (2x, 2\sqrt{2x}, x\sqrt{2x}) = (\sqrt{2x}) \cdot (\sqrt{2x}, 2, x) &&= (\sqrt{2x}) \cdot \mathfrak{p}_3 &&\sim (\sqrt{2x}).
\end{aligned}$$

Die Hauptideale (x) und (2) sind primär, aber nicht Primidealpotenzen, sondern nur quasigleich Primidealpotenzen. Das Hauptideal $(\sqrt{2x})$ ist das K.G.V. von $\mathfrak{p}_1$ und $\mathfrak{p}_2$, aber nicht gleich, sondern nur quasigleich ihrem Produkt. Das Beispiel zeigt die Notwendigkeit der Einführung der Quasigleichheit statt der Gleichheit, wenn man zu einer Primfaktorzerlegung der Hauptideale kommen will.

Aufgaben. 1. Alle Ergebnisse dieses Paragraphen gelten auch für Ringe mit Nullteilern, wenn man nur den Quotientenkörper durch den Quotientenring ersetzt und sich auf die Nicht-Nullteilerideale beschränkt (vgl. § 100, Schluß).

2. Aus Satz 1 folgt umgekehrt die ganze Abgeschlossenheit des Ringes $\mathfrak{o}$. Ebenso aus Satz 2 zusammen mit der ersten Hälfte von 12. [vgl. § 101].

3. Man beweise die ganze Abgeschlossenheit des Restklassenrings

$$\mathfrak{o} = \mathsf{K}[x, y, z]/(xy - z^2)$$

und zerlege die Hauptideale (x), (y), (z) in $\mathfrak{o}$ in ihre Primfaktoren.

4. Man dehne den Satz 4 des § 101 und die Folgerungen daraus auf allgemeinere ganz-abgeschlossene Ringe aus.

5. Man beweise: $\mathfrak{a} : \mathfrak{b} \sim \mathfrak{a}\mathfrak{b}^{-1}$.

Zusammenfassung der Idealtheorie.

Folgende Zusammenstellung zeigt die Bedeutung der im § 100 formulierten Axiome I (Teilerkettensatz), II (jedes Primideal teilerlos), III (ganze Abgeschlossenheit) für die Idealtheorie der Integritätsbereiche:

Aus I folgt: Jedes Ideal K.G.V. von Primäridealen; zugehörige Primideale eindeutig.

Aus I und II: Jedes Ideal Produkt von einartigen Primäridealen; eindeutig.

Aus I und III: Jedes Ideal quasigleich einem Produkt von Primidealpotenzen; eindeutig bis auf Quasigleichheit.

Aus I, II, III: Jedes Ideal Produkt von Primidealpotenzen; eindeutig.

Fünfzehntes Kapitel.

Lineare Algebra.

Die lineare Algebra handelt von *Linearformen* (mit Koeffizienten aus einem Ring K), von *Moduln* aus solchen Linearformen und von deren Homomorphismen oder *linearen Transformationen*. Die Theorie zerfällt in verschiedene Abschnitte, entsprechend den verschiedenen Voraussetzungen, die man über den zugrunde gelegten Ring oder Körper K machen kann. Ein einleitender Paragraph, gültig für beliebige (auch nichtkommutative) Ringe K, geht voran.

Die hier zu gebende Darstellung der linearen Algebra beruht ganz auf der Theorie der Gruppen mit Operatoren (Kap. 6) und benutzt sonst nur die Grundlagen (Kap. 1 bis 3).

§ 104. Moduln. Linearformen. Vektoren. Matrizes.

Es sei K ein Ring mit Einselement ε, dessen Elemente in diesem Paragraphen mit griechischen Typen bezeichnet und bisweilen „*Skalaren*“ genannt werden.

Es sei $\mathfrak{M}$ ein K-(Rechts-)Modul, d. h. eine additiv geschriebene Abelsche Gruppe, die K als Rechtsmultiplikatorenbereich besitzt und

außer den Gruppenaxiomen die folgenden Rechnungsregeln erfüllt:

$$(a+b)\lambda = a\lambda + b\lambda,$$
$$a(\lambda+\mu) = a\lambda + a\mu,$$
$$a\cdot\lambda\mu = a\lambda\cdot\mu.^{1}$$

Dabei bezeichnen die lateinischen Typen die Elemente von $\mathfrak{M}$. Aus den Distributivgesetzen folgen wie üblich dieselben Gesetze für die Subtraktion, die multiplikativen Eigenschaften des Minuszeichens und die Tatsache, daß ein Produkt Null ist, wenn ein Faktor Null (sei es nun die Null von K oder die von $\mathfrak{M}$) darin vorkommt.

Das Einselement von K braucht nicht Einheitsoperator zu sein: $a\varepsilon$ kann für gewisse a von a verschieden sein. (Beispielsweise erfüllt man alle Rechnungsregeln, wenn man $a\lambda = 0$ setzt für jedes a und jedes λ.) In diesem Fall aber kann man stets setzen

$$a = (a - a\varepsilon) + a\varepsilon. \tag{1}$$

Das erste Glied $a - a\varepsilon$ wird durch den Rechtsfaktor ε annulliert; das zweite reproduziert sich bei der Multiplikation mit ε. Die ersten Glieder bilden einen Untermodul $\mathfrak{M}_0$ von $\mathfrak{M}$, der von ε, und daher auch von jedem Element $\varepsilon\lambda$ von K, annulliert wird; die zweiten Glieder $a\varepsilon$ bilden einen Untermodul $\mathfrak{M}_1$, für den ε Einheitsoperator ist. Die beiden Untermoduln können nur die Null gemein haben; denn für jedes andere Element schließen Annullieren und Reproduzieren sich aus. Die Darstellung (1) zeigt nunmehr, daß $\mathfrak{M}$ die direkte Summe $\mathfrak{M}_0 + \mathfrak{M}_1$ ist. Nachdem also von $\mathfrak{M}$ der uninteressante Teil $\mathfrak{M}_0$ abgespalten ist, behält man einen Modul übrig, für den ε Einheitsoperator ist. *Wir setzen daher im folgenden voraus, daß das Einselement von* K *zugleich Einheitsoperator für* $\mathfrak{M}$ *ist*: $a\varepsilon = a$ für jedes a, und bezeichnen dieses Einselement fortan wieder mit 1.

Der Modul $\mathfrak{M}$ heißt *endlich* (in bezug auf K), wenn seine Elemente linear in der Gestalt

$$u_1\lambda_1 + \cdots + u_n\lambda_n$$

durch endlichviele Elemente $u_1, \ldots, u_n$ dargestellt werden können. Wir schreiben in diesem Fall:

$$\mathfrak{M} = (u_1\mathsf{K}, \ldots, u_n\mathsf{K}) \quad \text{oder} \quad \mathfrak{M} = (u_1, \ldots, u_n)'.$$

---

[1] Daß wir die Multiplikatoren rechts schreiben, ist ganz willkürlich. Alle zu beweisenden Sätze gelten auch, wenn sie links stehen. In der letzten Rechnungsregel kommt dann

$$\lambda\mu\cdot a = \lambda\cdot\mu a$$

zu stehen; das heißt, daß in diesem Fall die Multiplikation mit $\lambda\mu$ hinauskommt auf eine Multiplikation zuerst mit μ, dann mit λ, während es vorher umgekehrt war. Das Rechts- oder Linksschreiben ist also eng damit verknüpft, ob man die Operation: erst Λ, dann M, mit $\Lambda\mathsf{M}$ oder mit $\mathsf{M}\Lambda$ bezeichnen will.

Wir spezialisieren nun die Voraussetzungen noch weiter, indem wir annehmen, daß die u_i *linear-unabhängig* sind, d. h. daß aus $\sum u_i \alpha_i = 0$ folgt $\alpha_i = 0$. Unter dieser Voraussetzung heißt $\mathfrak{M}$ ein *(n-gliedriger) Modul aus Linearformen* oder kurz ein *Linearformenmodul*, K *Koeffizientenbereich*; die u_j bilden ein System von *Basiselementen*. Auf Grund der linearen Unabhängigkeit der u_j ist jedes Element von $\mathfrak{M}$ *eindeutig* als Linearform $\sum u_j \lambda_j$ zu schreiben; denn aus $\sum u_j \lambda_j = \sum u_j \mu_j$ folgt

$$\sum u_j (\lambda_j - \mu_j) = 0\,, \quad \text{also} \quad \lambda_j - \mu_j = 0 \quad \text{oder} \quad \lambda_j = \mu_j\,.$$

Je zwei Linearformenmoduln mit demselben Koeffizientenbereich K *und derselben Anzahl von Basiselementen sind operatorisomorph.* Man kann nämlich jedem Basiselement u_j des einen Moduls ein Basiselement v_j des andern Moduls und der Linearform $\sum u_j \lambda_j$ die Linearform $\sum v_j \lambda_j$ zuordnen.

Dieser Isomorphiesatz bedeutet, daß es für die Modultheorie ganz gleichgültig ist, ob die u_i Unbestimmte oder irgend etwas anderes sind, falls nur alle unsere Voraussetzungen erfüllt sind. Sehr oft gehören die u_i einem Ring an, der K umfaßt (z. B. in der Theorie der algebraischen Zahlenmoduln). Es kann auch vorkommen, daß der Modul $\mathfrak{M}$ zunächst als Modul von *Vektoren* gegeben ist. Dabei wird unter einem *Vektor* eine Reihe von n Elementen $(\lambda_1, \ldots, \lambda_n)$ aus K verstanden. Vektoren werden addiert, indem man ihre Komponenten addiert; sie werden mit Skalaren α aus K multipliziert, indem man alle ihre Komponenten (von rechts) mit α multipliziert. Führt man die linear-unabhängigen Grundvektoren

$$\begin{aligned} e_1 &= (1, 0, \ldots, 0)\,,\\ e_2 &= (0, 1, \ldots, 0)\,,\\ &\cdots\cdots\cdots\cdots\\ e_n &= (0, 0, \ldots, 1) \end{aligned}$$

ein, so wird jeder Vektor $(\lambda_1, \ldots, \lambda_n)$ einer Linearform der Grundvektoren

$$e_1 \lambda_1 + \cdots + e_n \lambda_n$$

gleich; damit sind auch die Vektoren auf Linearformen zurückgeführt. Alles, was im folgenden über Linearformenmoduln ausgesagt wird, gilt demnach auch für den „Vektorenraum" und umgekehrt.

Ein Operatorhomomorphismus, welcher einen Linearformenmodul $\mathfrak{M} = (u_1, \ldots, u_m)$ in einen Linearformenmodul $\mathfrak{N} = (v_1, \ldots, v_n)$ abbildet, heißt eine *lineare Abbildung* oder *lineare Transformation*. Eine solche ist vollständig gegeben, wenn das Bildelement eines jeden Basiselements u_j

$$u'_j = \sum_1^n v_i \alpha_{ij} \qquad (j = 1, \ldots, m) \tag{2}$$

gegeben ist, also wenn die *Matrix*

$$A = (\alpha_{ij}) = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \cdots & \alpha_{1m} \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ \alpha_{n1} & \alpha_{n2} & \cdots & \alpha_{nm} \end{pmatrix}$$

gegeben ist[1]. Dann muß nämlich auch $a = \sum u_j \lambda_j$ auf $a' = \sum u'_j \lambda_j$ abgebildet werden. Bei Änderungen der Basis $(u_1, \ldots, u_m)$ oder $(v_1, \ldots, v_n)$ kann eine und dieselbe lineare Transformation jedesmal durch eine andere Matrix dargestellt werden (vgl. die nachstehende Aufgabe 6). Trotzdem bezeichnet man oft eine lineare Transformation durch dasselbe Symbol A, das die zugehörige Matrix bezeichnet.

Für das Bild eines Elementes a in der durch die Matrix A vermittelten Abbildung schreiben wir Aa, also im Fall (2):

$$A u_j = \sum v_i \alpha_{ij}.$$

Die Matrix A ist im allgemeinen „rechteckig"; quadratisch ist sie nur im Fall $m = n$, z. B. bei einer linearen Abbildung von $\mathfrak{M}$ in sich.

Die Zusammensetzung der zur Matrix A gehörigen Abbildung von $\mathfrak{M} = (u_1, \ldots, u_m)$ in $\mathfrak{N} = (v_1, \ldots, v_n)$ mit einer nachfolgenden, durch eine Matrix B vermittelten Abbildung von $\mathfrak{N}$ in $\mathfrak{P} = (w_1, \ldots, w_p)$ führt zu

$$B(A u_j) = B\left(\sum_i v_i \alpha_{ij}\right) = \sum_i (B v_i)\alpha_{ij} = \sum_h \sum_i w_h \beta_{hi} \alpha_{ij},$$

also zum *Matrixprodukt* $C = BA$, definiert durch

$$\gamma_{hj} = \sum_i \beta_{hi} \alpha_{ij}.$$

Es ist also für $u \in \mathfrak{M}$

$$BA \cdot u = B \cdot A u.$$

Das Produkt AB hat nur dann einen Sinn, wenn die Spaltenzahl von A mit der Zeilenanzahl von B übereinstimmt. Es stellt dann nach dem Vorangehenden genau das Produkt AB der zugehörigen Abbildungen dar.

Die *Summe* zweier linearen Abbildungen von $\mathfrak{M}$ in $\mathfrak{N}$ wird durch

$$(A + B) u = A u + B u$$

definiert; die zugehörige Matrix hat die Elemente $\alpha_{ik} + \beta_{ik}$ und heißt die *Summe der Matrizes* A und B; sie hat einen Sinn, wenn A und B gleich viel Zeilen und Spalten haben.

---

[1] Bei der Bildung der Gleichungen (2) aus der Matrix A ist zu beachten, daß bei unseren Bezeichnungen die m Gleichungen (2) den m Spalten von A entsprechen: die Elemente einer Spalte (von oben nach unten gelesen) sind die Koeffizienten einer Gleichung (2).

Aus den Definitionen von Summe und Produkt folgen die Rechnungsregeln (gültig immer dann, wenn die auftretenden Produkte einen Sinn haben):

$$A \cdot BC = AB \cdot C,$$
$$A + (B + C) = (A + B) + C,$$
$$A(B + C) = AB + AC,$$
$$(B + C)A = BA + CA.$$

Mit Hilfe der aus einer Zeile bestehenden Matrizes $(u_1 \ldots u_m)$, $(v_1 \ldots v_n)$ usw. kann man die Formel (2) in Matrixform schreiben:

$$(u'_1 \ldots u'_m) = (v_1 \ldots v_n) \cdot A.$$

Eine Linearform $\Sigma u_i \lambda_i$ schreibt man zweckmäßig als Produkt einer *Zeile* $(u_1 \ldots u_m)$ mit einer *Spalte* $\begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_m \end{pmatrix}$, die den *Vektor* $(\lambda_1, \ldots, \lambda_m)$ repräsentiert. Die Linearform $\Sigma u_j \lambda_j$ wird durch die lineare Abbildung A in

$$\Sigma A u_j \lambda_j = \Sigma \Sigma v_i \alpha_{ij} \lambda_j$$

transformiert; zu der Linearform rechts gehört wieder ein Vektor, nämlich

$$\begin{pmatrix} \lambda'_1 \\ \vdots \\ \lambda'_n \end{pmatrix} = A \cdot \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_m \end{pmatrix}.$$

Das ist die Formel $a' = Aa$, in die Vektorsprache übersetzt. Die einzelnen λ'_i werden je aus einer *Zeile* von A durch Multiplikation mit $\lambda_1, \ldots, \lambda_m$ und Addition gebildet.

Eine Abbildung von $\mathfrak{M} = (u_1, \ldots, u_n)$ in sich wird gegeben durch eine quadratische Matrix:

$$u'_j = \Sigma u_i \alpha_{ij}. \tag{3}$$

Diese quadratischen Matrizes bilden nach dem Vorigen einen Ring, der außerdem als (Links-)Operatorenbereich für den Vektorraum aufgefaßt werden kann.

Es kann sein, daß die durch (3) definierten u'_j wieder eine Basis für $\mathfrak{M}$ bilden. Dazu ist *erstens* notwendig, daß sie linear-unabhängig sind, d. h. daß aus

$$\Sigma u'_j \mu_j = 0 \quad \text{oder} \quad \sum_i \sum_j u_i \alpha_{ij} \mu_j = 0$$

oder schließlich $\sum_j \alpha_{ij} \mu_j = 0$ immer folgt $\mu_j = 0$, mit anderen Worten, daß zwischen den Spalten

$$\begin{pmatrix} \alpha_{11} \\ \vdots \\ \alpha_{n1} \end{pmatrix}, \quad \begin{pmatrix} \alpha_{12} \\ \vdots \\ \alpha_{n2} \end{pmatrix}, \quad \ldots$$

keine lineare Relation besteht, es sei denn, daß alle Koeffizienten μ_j gleich Null sind. Noch anders ausgedrückt: Die Matrix A soll durch keine von Null verschiedene Spalte $\begin{pmatrix} \mu_1 \\ \vdots \\ \mu_n \end{pmatrix}$ von rechts annulliert werden. Dann wird sie von selbst auch durch keine mehrspaltige Matrix $B \neq 0$ annulliert (d. h. es ist $AB \neq 0$ für $B \neq 0$), und wir können sagen, daß *A kein linker Nullteiler* ist. *Zweitens* ist aber nötig, daß sich umgekehrt alle u_i durch die u'_i ausdrücken:

$$u_k = \sum u'_j \beta_{jk}. \tag{4}$$

Dazu muß also die Formel (3), in (4) eingesetzt, eine Identität ergeben:

$$u_k = \sum u_i \alpha_{ij} \beta_{jk},$$

oder das Produkt $A \cdot B$ muß die *Einheitsmatrix*

$$E = \begin{pmatrix} \varepsilon & & 0 \\ & \varepsilon & \\ & \ddots & \\ 0 & & \varepsilon \end{pmatrix}$$

ergeben: $AB = E$. Wir haben also bewiesen:

Dann und nur dann stellt (3) *eine neue Basis dar, wenn die Matrix A kein linker Nullteiler ist und eine Rechtsinverse B besitzt.*

Sind diese Bedingungen erfüllt, so ist die Beziehung zwischen den Basen u, u' und daher auch die zwischen den Matrizes A, B umkehrbar; d. h. es ist auch

$$BA = E.$$

Weiter folgt noch, daß A auch kein rechter Nullteiler ist; denn wenn für eine Zeile $S \neq 0$ das Produkt SA gleich Null wäre, so würde folgen

$$0 = SAB = SE = S \neq 0.$$

Aus der Tatsache, daß A kein linker Nullteiler ist, folgt schließlich, daß A auch nur *eine* Rechtsinverse besitzen kann.

Mithin können wir die einzige rechts- (und links-) inverse Matrix, die vorhin B hieß, mit A^{-1} bezeichnen. Wir nennen die Matrix A unter den angegebenen Bedingungen *invertierbar in* K und resümieren:

Der Übergang zu einer neuen Basis wird durch eine invertierbare Matrix bewerkstelligt.

Zu einer anderen Auffassung der linearen Transformationen kommt man, wenn man die Größen $u_1, \ldots, u_n$ als Unbestimmte in einem Polynombereich $\mathsf{K}[u_1, \ldots, u_n]$ auffaßt. Die Formeln (3), (4) bedeuten dann eine *lineare Substitution*, durch die man im Polynombereich neue Unbestimmte u' einführt. Durch die Substitution (4) wird jede Form $f(u_1, \ldots, u_n)$ in eine Form $f'(u'_1, \ldots, u'_n)$ übergeführt, insbesondere eine Linearform $\sum u_k \lambda_k$ in eine Linearform:

$$\sum u_k \lambda_k = \sum \sum u'_j \beta_{jk} \lambda_k = \sum u'_j \lambda'_j,$$

wobei also die neuen Koeffizienten durch

$$\lambda_j' = \sum_k \beta_{jk} \lambda_k \tag{5}$$

gegeben werden. Die Formel (5) stellt eine lineare Transformation der Vektoren $(\lambda_1, \ldots, \lambda_n)$ dar, deren Matrix B ist.

Gibt man andererseits den Variablen u_i spezielle Werte μ_i aus dem Körper K und bildet nach (3)

$$\mu_k' = \sum \mu_j \alpha_{jk}, \tag{6}$$

so ist das auch eine lineare Transformation in einem Vektorenraum oder Linearformenmodul (dessen Operatorenbereich diesmal *links* geschrieben werden muß, weil die Transformationskoeffizienten *rechts* von den Vektorkomponenten stehen), deren Matrix die gespiegelte oder transponierte[1] Matrix $\tilde{A}$ von A ist.

Die beiden Transformationen (5), (6) sind miteinander verbunden durch die Forderung, daß die Summe $\sum \mu_k \lambda_k$ invariant bleibt:

$$\sum \mu_k \lambda_k = \sum \mu_k' \lambda_k',$$

und heißen *zueinander kontragredient*. Die Matrix $\tilde{A}$ von (6) ist die transponierte inverse oder die inverse transponierte zur Matrix B von (5):

$$\tilde{A} = \tilde{B}^{-1}.$$

Aufgaben. 1. Besitzt eine quadratische Matrix eine Rechts- und eine Linksinverse, so ist sie invertierbar (mithin die beiden Inversen gleich und einzig).

2. Ist A linker Nullteiler und besitzt eine Rechtsinverse, so besitzt A unendlichviele Rechtsinversen. (Ob die Voraussetzungen für endliche quadratische Matrizes überhaupt zutreffen können, ist dem Verfasser unbekannt; der Satz gilt aber auch für unendliche Matrizes, bei denen man leicht Beispiele bildet. Für endliche Matrizes in einem Körper oder Integritätsbereich sind die Voraussetzungen sicher nicht erfüllbar; vgl. § 105.)

3. Die invertierbaren n-reihigen Matrizes in einem Ring K mit Einselement bilden eine Gruppe: die *lineare homogene Gruppe in* K oder die Automorphismengruppe eines n-gliedrigen Linearformenmoduls.

4. Alle n-reihigen quadratischen Matrizes in K bilden einen Ring, den *vollen Matrizenring* in K oder den Automorphismenring eines n-gliedrigen Linearformenmoduls. Dieser Ring besitzt in bezug auf K eine linear-unabhängige Basis, bestehend aus den Matrizes C_{ij}, die im Schnittpunkt der i-ten Zeile und j-ten Spalte eine 1 und sonst überall Nullen haben.

5. Homomorphismen für Linearformenmoduln in unendlichvielen Veränderlichen (wobei unter Linearformen immer solche in endlichvielen dieser Variablen zu verstehen sind) werden durch solche unendlichen

[1] Transponieren heißt Vertauschen von Zeilen und Spalten oder Spiegeln an der Hauptdiagonale. Das Zeichen für die transponierte Matrix zu A ist $\tilde{A}$. *Warnung*: Dasselbe Zeichen wird bisweilen auch für die transponierte konjugiert komplexe Matrix zu A benutzt.

Matrizes dargestellt, bei denen in jeder Spalte nur endlichviele Elemente von Null verschieden sind. Man übertrage die Theorie der invertierbaren Matrizes auf diesen Fall.

6. Wird eine lineare Abbildung von $\mathfrak{M} = (u_1, \ldots, u_n)$ in $\mathfrak{N} = (v_1, \ldots, v_n)$ durch die Matrix A dargestellt und führt man durch

$$(u'_1 \ldots u'_n) = (u_1 \ldots u_n)\, P,$$
$$(v'_1 \ldots v'_n) = (v_1 \ldots v_n)\, Q$$

neue Basen ein, so wird dieselbe Transformation, auf die neuen Basen bezogen, durch die Matrix

$$A' = Q^{-1} A P$$

dargestellt.

7. Wird eine Matrix A von n Zeilen und m Spalten irgendwie in rechteckige „Kästchen" eingeteilt, etwa so:

$$A = \left(\begin{array}{c|c|c} \alpha_{11} \cdots & \alpha_{1i} \cdots & \alpha_{1j} \cdots \alpha_{1m} \\ \vdots & & \vdots \\ \hline \alpha_{k1} & & \vdots \\ \vdots & & \vdots \\ \alpha_{n1} \cdots & \cdots & \alpha_{nm} \end{array}\right) = \begin{pmatrix} A_{11} & A_{12} & A_{13} \\ A_{21} & A_{22} & A_{23} \end{pmatrix},$$

und wird eine Matrix B von m Zeilen und q Spalten auch eingeteilt, aber so, daß die Stellen der Horizontalschnitte von B mit den Stellen $(1, i, j)$ der Vertikalschnitte von A übereinstimmen:

$$B = \left(\begin{array}{c|c|c} \beta_{11} \cdots & \beta_{1h} \cdots & \cdots \beta_{1q} \\ \vdots & & \vdots \\ \hline \beta_{i1} & & \vdots \\ \vdots & & \vdots \\ \hline \beta_{j1} & & \vdots \\ \vdots & & \vdots \\ \beta_{m1} \cdots & \cdots & \cdots \beta_{mq} \end{array}\right) = \begin{pmatrix} B_{11} & B_{12} & B_{13} \\ B_{21} & B_{22} & B_{23} \\ B_{31} & B_{32} & B_{33} \end{pmatrix},$$

so kann man die Multiplikation von A und B so ausführen, als ob die Kästchen A_{ij}, B_{jk} Elemente wären:

$$A\,B = \begin{pmatrix} \sum A_{1j} B_{j1} & \sum A_{1j} B_{j2} & \sum A_{1j} B_{j3} \\ \sum A_{2j} B_{j1} & \sum A_{2j} B_{j2} & \sum A_{2j} B_{j3} \end{pmatrix}.$$

§ 105. Moduln in bezug auf einen Körper. Lineare Gleichungen.

Wir nehmen jetzt an, K sei ein (nicht notwendig kommutativer) Körper, der Modul $\mathfrak{M}$ sei endlich und das Einselement sei Einheitsoperator. Wenn zwischen den Basiselementen $u_1, \ldots, u_n$ eine lineare

Abhängigkeit $\sum u_i \lambda_i = 0$ besteht, wobei etwa $\lambda_n \neq 0$ sei, so kann man die Gleichungen mit λ_n^{-1} multiplizieren und u_n linear durch die übrigen Basiselemente ausdrücken. Also bilden $u_1, \ldots, u_{n-1}$ auch eine Basis. So weiterschließend, kommt man zuletzt zu einer linear-unabhängigen Basis. Mithin ist jeder endliche Modul der betrachteten Art ein Linearformenmodul.

Ein vom Nullmodul verschiedener Modul heißt (wie eine gewöhnliche Abelsche Gruppe) *einfach*, wenn er keine echten Untermoduln außer dem Nullmodul besitzt. Es gilt der Satz: *Ein einfacher* K*-Modul ist eingliedrig, und ein eingliedriger* K*-Modul ist einfach.*

Beweis. 1. $\mathfrak{M}$ sei einfach. Jedes Element $u \neq 0$ muß dann den ganzen Modul erzeugen; also ist $\mathfrak{M}$ eingliedrig.

2. $\mathfrak{M}$ sei eingliedrig: $\mathfrak{M} = (u)$. Ist $\mathfrak{N} \neq (0)$ ein Untermodul und $u\lambda$ ein von Null verschiedenes Element von $\mathfrak{N}$, so enthält $\mathfrak{N}$ auch $u\lambda\lambda^{-1} = u$; mithin ist $\mathfrak{M} = \mathfrak{N}$. Also ist $\mathfrak{M}$ einfach.

Ein n-gliedriger Modul ist eine direkte Summe von einfachen Moduln $(u_1) = u_1\mathsf{K}, \ldots, (u_n) = u_n\mathsf{K}$. Die Untermoduln $(u_1, \ldots, u_n)$, $(u_1, \ldots, u_{n-1}), \ldots, (u_1), (0)$ bilden eine Reihe mit eingliedrigen, somit einfachen Faktormoduln, also eine *Kompositionsreihe. Mithin ist die Gliederzahl n des Moduls gleich der Länge der Kompositionsreihe, also unabhängig von der Basiswahl.*

Die Gliederzahl eines K-Moduls heißt auch der (*lineare*) *Rang des Moduls in bezug auf* K.

Die Eindeutigkeit des linearen Ranges erhielten wir schon in § 28 auf anderem Wege. Das andere frühere Ergebnis, daß man jede Basis eines Untermoduls zu einer Basis des ganzen Moduls ergänzen kann, ist nichts anderes als der gruppentheoretische Satz, daß man durch jeden Untermodul eine Kompositionsreihe ziehen kann. Die Ergänzung einer Basis eines Untermoduls zu einer Basis von $\mathfrak{M}$ kann so geschehen, daß man die fehlenden Basiselemente aus den u_j (d. h. aus einer vorgegebenen Basis von $\mathfrak{M}$) wählt; das folgt nach § 42 aus der Tatsache, daß der Modul $\mathfrak{M}$ direkte Summe von einfachen eingliedrigen Moduln ist. Diese Aussage ist aber der Austauschsatz von § 28, jetzt gruppentheoretisch hergeleitet.

Ein echter Untermodul von $\mathfrak{M}$ hat eine kleinere Länge der Kompositionsreihe, also eine kleinere Gliederzahl. Daraus folgt: *Irgend n linear-unabhängige Elemente* $v_k = \sum u_i \alpha_{ik}$ *von* $\mathfrak{M}$ *erzeugen* $\mathfrak{M}$ *selbst*; denn sie können keinen echten Untermodul erzeugen. Die Voraussetzung der linearen Unabhängigkeit bedeutet, daß die Matrix A kein linker Nullteiler ist; die Folgerung, daß die v eine neue Basis für $\mathfrak{M}$ bilden, besagt aber die Invertierbarkeit der Matrix. Wir sehen also: *Wenn eine quadratische Matrix in einem Körper* K *kein linker Nullteiler ist, so ist sie invertierbar.* Die Matrix heißt in diesem Fall *regulär*; ist sie aber linker Nullteiler (also nicht invertierbar, also auch rechter Nullteiler), so heißt sie

singulär. Die Bezeichnungen übertragen sich auf Matrizes in einem Integritätsbereich $\mathfrak{R}$, da man einen solchen ja immer in einen Körper einbetten kann. Reguläre Matrizes brauchen im Integritätsbereich $\mathfrak{R}$ noch nicht invertierbar zu sein; im Quotientenkörper K sind sie es aber. Singuläre Matrizes aber sind nicht nur im Körper, sondern auch im Ring Nullteiler; denn man kann eine Spalte, die eine Matrix annulliert, durch Multiplikation mit einem Hauptnenner immer ganz machen.

Auf dem Austauschsatz beruht die *Theorie der linearen Gleichungen*. Ein System von linearen Gleichungen möge lauten

$$l_i(\xi) = \beta_i; \tag{1}$$

die l_i sollen dabei m Linearformen der n Unbekannten ξ_k sein:

$$l_i(\xi) = \sum \alpha_{ik}\xi_k .^1$$

Ersetzen wir hier die ξ_k durch Unbestimmte x_k, so werden die l_i Linearformen dieser Unbestimmten:

$$l_i = \sum \alpha_{ik} x_k. \tag{2}$$

Die Anzahl r der linear-unabhängigen unter diesen Linearformen l_i heißt der *Rang* des Gleichungssystems. Notwendig für die Lösbarkeit des Gleichungssystems ist offenbar, daß alle linearen Relationen $\sum \mu_i l_i = 0$, die (identisch in den Unbestimmten x) zwischen den Linearformen l_i bestehen, auch zwischen den rechten Seiten β_i bestehen. Ist das der Fall und sind alle l_i etwa von $l_1, \ldots, l_r$ abhängig, so sind alle Gleichungen (1) Folgen der ersten r unter ihnen. Es ist $r \leqq n$, da es nicht mehr als n linear-unabhängige Linearformen in $x_1, \ldots, x_n$ geben kann. Nach dem Austauschsatz kann man die $l_1, \ldots, l_r$ mit $n - r$ der Unbestimmten x_i, etwa $x_{r+1}, \ldots, x_n$, zu einer Basis für alle Linearformen der x ergänzen. Das heißt, es gilt

$$x_i = \sum_{r+1}^{n} \gamma_{ij} x_j + \sum_{1}^{r} \delta_{ik} l_k \qquad (i = 1, \ldots, r). \tag{3}$$

Satz. *Man findet genau alle Lösungen der Gleichungen* (1), *indem man in* (3) *die* l_i *durch* β_i *und die* $x_{r+1}, \ldots, x_n$ *durch ganz beliebige Größen* $\xi_{r+1}, \ldots, \xi_n$ *aus* K *ersetzt und die Werte* $\xi_1, \ldots, \xi_r$ *von* $x_1, \ldots, x_r$ *aus* (3) *bestimmt.*

Zum Beweis bemerken wir, daß die $l_1, \ldots, l_r, x_{r+1}, \ldots, x_n$ eine linear-unabhängige Basis für den Modul $(x_1, \ldots, x_n)$ bilden. Setzt man also (3) in (2) ein, so muß eine Identität in den $l_1, \ldots, l_r, x_{r+1}, \ldots, x_n$ herauskommen, die also erhalten bleibt, wenn man die l_i durch β_i und die x_j durch beliebige ξ_j ersetzt. Also sind die gefundenen ξ Lösungen von (1). Setzt man ebenso (2) in (3) ein, so kommt eine Identität in den x heraus, die erhalten bleibt bei Ersetzung der x durch solche ξ,

[1] Die Unbestimmten werden für den Augenblick rechts von den Koeffizienten geschrieben, was für die Anwendung der Modulsätze natürlich nichts ausmacht.

welche (1) erfüllen. Also ergibt die angegebene Regel auch alle Lösungen von (1).

Es folgt, daß das oben genannte Kriterium für Lösbarkeit auch hinreichend ist und daß der Rang des Gleichungssystems zugleich die Anzahl der Unbekannten ergibt, nach denen man auflösen kann, während die Werte der übrigen beliebig wählbar sind.

Um die Untersuchung, welche l_i linear-unabhängig sind, und die Aufstellung der Formeln (3) wirklich durchzuführen, bedient man sich des Verfahrens der *sukzessiven Elimination*: man löst zuerst eine der Beziehungen $l_i = \sum \alpha_{ik} x_k$ nach einem x_j auf, setzt dieses x_j in die anderen Beziehungen ein, wodurch also ein Basiselement x_j durch ein l_i ersetzt ist, und fährt so fort, bis schließlich in den Ausdrücken für die eventuell restierenden l_k die x gar nicht mehr vorkommen, mithin diese l_k nur von (sagen wir) $l_1, \ldots, l_r$ allein abhängen. Man kann dann feststellen, ob diese linearen Beziehungen zwischen den l_i auch für die β_i gelten, oder noch bequemer: man ersetzt von vornherein bei der Rechnung die l_i durch die bekannten β_i. Die Formeln (3), eventuell mit β_k statt l_k, folgen durch Substitution ganz von selbst.

Aus der Möglichkeit dieser rationalen Berechnung folgt: *Wenn die Koeffizienten eines Gleichungssystems einem Unterkörper angehören, so liegen in demselben Unterkörper die Koeffizienten der lösenden Formeln* (3) *sowie die der linearen Abhängigkeiten zwischen den linken Seiten. Die Entscheidung über Lösbarkeit oder Widerspruch ist schon im Unterkörper zu treffen.*

Speziell im Fall eines kommutativen K liefert die *Determinantentheorie* mehr explizite Auflösungsformeln und algebraische Kriterien für Lösbarkeit und lineare Abhängigkeit, für die wir auf die betreffenden Lehrbücher verweisen. Besonders hervorzuheben ist aus dieser Theorie das folgende Kriterium für Regularität einer Matrix: *Eine quadratische Matrix A ist in einem kommutativen Körper oder Integritätsbereich regulär, wenn ihre Determinante $|A|$ von Null verschieden ist.* Ist außerdem die Determinante eine Einheit des Integritätsbereichs, so ist die Matrix auch im Integritätsbereich selbst invertierbar; denn in den Auflösungsformeln kommt nur diese Determinante im Nenner vor.

Die Umkehrung dieses Satzes folgt, indem man den Multiplikationssatz der Determinanten:

$$|AB| = |A| \cdot |B|$$

auf den Fall $AB = E$, $|E| = 1$ anwendet. Daher: *In einem Integritätsbereich sind die und nur die Matrizes invertierbar, deren Determinante eine Einheit ist* (unimodulare Matrizes).

Aufgaben. 1. Ein System von homogenen Gleichungen $\sum \alpha_{ik} \xi_k = 0$ ist in einem Körper stets lösbar, und alle Lösungen $\{\xi_1, \ldots, \xi_n\}$, als Vektoren aufgefaßt, setzen sich aus $n - r$ speziellen, linear-unabhängigen

Lösungen linear zusammen (mit Koeffizienten, die rechts von den Vektoren geschrieben werden). Für $r = n$ existiert nur die Nullösung.

2. Zwischen den Gliederzahlen n, m eines K-Moduls und eines Untermoduls und der Gliederzahl f des Faktor-(Restklassen-)Moduls besteht die Beziehung $f = n - m$.

3. Zwischen den Gliederzahlen n, m zweier Untermoduln eines K-Moduls, der Gliederzahl s ihrer Summe und der Gliederzahl d ihres Durchschnitts besteht die Beziehung

$$s + d = n + m.$$

Der projektive Raum. Die eingliedrigen Untermoduln eines n-gliedrigen Linearformen- oder Vektorenmoduls werden als *Strahlen* des Vektorraumes $R_n(\mathsf{K})$ oder als *Punkte* des projektiven $(n-1)$-dimensionalen Raumes $P_{n-1}(\mathsf{K})$ bezeichnet. Die (bis auf einen Proportionalitätsfaktor bestimmten) Komponenten eines erzeugenden Vektors heißen *homogene Koordinaten* des Punktes. Die Strahlen eines Untermoduls bilden einen *linearen Unterraum* im projektiven Raum. Aus Aufgabe 1 folgt nun, daß r unabhängige lineare homogene Gleichungen in den Koordinaten einen Unterraum von $n - r - 1$ Dimensionen bestimmen. Da weiter ein Durchschnitt von Untermoduln wieder ein Untermodul ist, so folgt, daß ein Durchschnitt von linearen Räumen wieder ein solcher (oder leer) ist. Schließlich folgt aus Aufgabe 3, daß zwischen den Dimensionen l, m zweier linearer Unterräume, der Dimension d ihres Durchschnittes und der Dimension s des kleinsten beide umfassenden linearen Raumes die Beziehung

$$d + s = l + m$$

besteht (mit $d = -1$, falls der Durchschnitt leer ist).

§ 106. Moduln in Hauptidealringen. Elementarteiler.

Wir setzen nun von dem Ring K voraus, daß er keine Nullteiler enthält und daß

entweder (*erster Fall*) für alle Elemente a von K ein ganzzahliger nichtnegativer absoluter Betrag $|a|$ definiert ist und ein Divisionsverfahren links und rechts möglich ist (vgl. § 13):

$$a = bq + r, \qquad |r| < |b|, \qquad a = q'b + r', \qquad |r'| < |b|;$$

oder (*zweiter Fall*) K kommutativ ist und in K jedes Ideal Hauptideal ist. (K heißt dann nach § 16 ein Hauptidealring.)

Der Ring C der ganzen Zahlen fällt unter beide Fälle. Der Polynombereich $\mathsf{P}[x]$, wo P ein Körper ist, fällt unter den ersten Fall, wenn man unter dem „absoluten Betrag" den um Eins vermehrten Grad und für das Polynom Null die Zahl Null versteht.

In beiden Fällen ist in K jedes Links- oder Rechtsideal Hauptideal, und es gibt zu je zwei Elementen a, b einen größten gemeinsamen Rechtsteiler $d = (a, b)$ mit den Eigenschaften:

$$a = \alpha d; \qquad b = \beta d; \qquad d = \lambda a + \mu b = \lambda\alpha d + \mu\beta d,$$

$$1 = \lambda\alpha + \mu\beta. \tag{1}$$

Ebenso gibt es einen Linksteiler d' mit ähnlichen Eigenschaften.

Im zweiten (kommutativen) Fall gilt nach § 17 in K die eindeutige Faktorzerlegung. Aus (1) folgt in diesem Fall die Invertierbarkeit der Matrix

$$\begin{pmatrix} \alpha & -\mu \\ \beta & \lambda \end{pmatrix},$$

die den Vektor $\begin{pmatrix} d \\ 0 \end{pmatrix}$ in $\begin{pmatrix} a \\ b \end{pmatrix}$ überführt. Die inverse Matrix

$$\begin{pmatrix} \lambda & \mu \\ -\beta & \alpha \end{pmatrix}$$

führt natürlich $\begin{pmatrix} a \\ b \end{pmatrix}$ in $\begin{pmatrix} d \\ 0 \end{pmatrix}$ über.

Satz. *Es sei $\mathfrak{M}$ ein Linearformenmodul in bezug auf K mit der linear-unabhängigen Basis $(u_1, \ldots, u_n)$. Dann ist jeder Untermodul $\mathfrak{N}$ von $\mathfrak{M}$ wieder ein Linearformenmodul mit höchstens n Basiselementen.*

Beweis: Für den Nullmodul $\mathfrak{M} = (0)$ ist der Satz trivial. Er sei für $(n-1)$-gliedrige Moduln $\mathfrak{M}$ schon bewiesen.

Wenn $\mathfrak{N}$ aus Linearformen in $u_1, \ldots, u_{n-1}$ allein besteht, so ist nach Induktionsvoraussetzung alles bewiesen. Wenn aber $\mathfrak{N}$ eine Linearform $u_1\lambda_1 + \cdots + u_n\lambda_n$ mit $\lambda_n \neq 0$ enthält, so bilden die vorkommenden λ_n ein Rechtsideal in K, also ein Hauptideal (μ_n) mit $\mu_n \neq 0$. Es kommt also in $\mathfrak{N}$ eine Form $l = u_1\mu_1 + \cdots + u_n\mu_n$ vor, und man kann von jeder anderen Form $u_1\lambda_1 + \cdots + u_n\lambda_n$ ein solches Vielfaches $l\alpha$ von l subtrahieren, daß der letzte Koeffizient λ_n zum Verschwinden gebracht wird. Die dann übrigbleibenden zu $\mathfrak{N}$ gehörigen Linearformen in $u_1, \ldots, u_{n-1}$ bilden einen Untermodul, der nach der Induktionsvoraussetzung eine linear-unabhängige Basis $(l_1, \ldots, l_{m-1})$, $m - 1 \leqq n - 1$, besitzt. Dann erzeugen $l_1, \ldots, l_{m-1}, l$ offenbar $\mathfrak{N}$.

Die $l_1, \ldots, l_{m-1}$ sind schon unabhängig. Gäbe es eine lineare Abhängigkeit

$$l_1\beta_1 + \cdots + l_{m-1}\beta_{m-1} + l\beta = 0$$

mit $\beta \neq 0$, so würde die Vergleichung der Koeffizienten von u_n ergeben $\mu_n\beta = 0$, was nicht geht.

Bemerkung. Die lineare Unabhängigkeit der $l_1, \ldots, l_m$ $(l_m = l)$ beruht offenbar darauf, daß jedes l_i nach Konstruktion ein solches u_j enthält, welches in l_1 bis l_{i-1} noch nicht vorkam.

Aufgaben. 1. Ist $\mathfrak{M}$ ein ganzzahliger Linearformenmodul und ist der Untermodul $\mathfrak{N}$ durch endlichviele erzeugende Linearformen $v_k = \sum u_i\alpha_{ik}$ gegeben, so ist eine Basis $(l_1, \ldots, l_m)$ mit den obigen Eigenschaften in endlichvielen Schritten konstruierbar.

2. Mit Hilfe der nach Aufgabe 1 konstruierten Basis $(l_1, \ldots, l_m)$ gebe man ein Mittel an, zu entscheiden, ob eine vorgelegte Linearform

$\beta_1 u_1 + \ldots + \beta_n u_n$ im Modul $\mathfrak{N}$ enthalten ist, mit anderen Worten: ob das lineare diophantische Gleichungssystem

$$\sum \alpha_{ik} \xi_k = \beta_i$$

in ganzen Zahlen ξ_k lösbar ist.

Elementarteilersatz. *Ist $\mathfrak{N}$ ein Untermodul des Linearformenmoduls $\mathfrak{M}$, so gibt es eine Basis $(u_1, \ldots, u_n)$ von $\mathfrak{M}$ und eine Basis $(v_1, \ldots, v_m)$ von $\mathfrak{N}$ derart, daß*

$$\begin{cases} v_i = u_i \varepsilon_i & (i = 1, \ldots, m) \\ \varepsilon_{i+1} \equiv 0 (\varepsilon_i) \end{cases}$$

ist. (Im nichtkommutativen Fall gilt die letztere Teilbarkeitsrelation sowohl von links als auch von rechts.)

Beweis: Wir gehen zunächst aus von irgend einer Basis $(u_1, \ldots, u_n)$ von $\mathfrak{M}$ und irgend einer Basis $(v_1, \ldots, v_m)$ von $\mathfrak{N}$; es sei

$$v_k = \sum u_i \alpha_{ik} \quad \text{oder} \quad (v_1 \ldots v_m) = (u_1 \ldots u_n) \cdot A.$$

Wir wollen nun durch schrittweises Abändern der Basis die Matrix A in die gewünschte Diagonalform

$$(2) \qquad \begin{pmatrix} \varepsilon_1 & & & 0 \\ & \varepsilon_2 & & \\ 0 & & \ddots & \\ & & & \varepsilon_m \\ 0 & \cdots & \cdots & 0 \end{pmatrix}$$

bringen. Erlaubte Abänderungen sind dabei zunächst:

1. Vertauschungen zweier u oder v, die eine Vertauschung zweier Zeilen oder Spalten von A bewirken.

2. Ersetzung eines u_i durch $u_i + u_j \lambda$ $(j \neq i)$, wodurch von der j-ten Zeile von A die von links mit λ multiplizierte i-te Zeile subtrahiert wird:

$$v_k = \sum u_i \alpha_{ik} = \cdots + (u_i + u_j \lambda) \alpha_{ik} + \cdots + u_j (\alpha_{jk} - \lambda \alpha_{ik}) + \cdots.$$

3. Ersetzung eines v_k durch $v_k - v_j \lambda$ $(j \neq k)$, wodurch von der k-ten Spalte von A die von rechts mit λ multiplizierte j-te Spalte subtrahiert wird:

$$v_k - v_j \lambda = \sum u_i (\alpha_{ik} - \alpha_{ij} \lambda).$$

Im Falle, daß es in K ein Divisionsverfahren gibt, reichen diese Operationen hin. Im anderen Fall hat man noch Transformationen von der Gestalt

4. $$(u_i, u_j) = (u_i', u_j') \begin{pmatrix} \lambda & \mu \\ -\beta & \alpha \end{pmatrix},$$

5. $$(v_i', v_j') = (v_i, v_j) \begin{pmatrix} \lambda & -\beta \\ \mu & \alpha \end{pmatrix}$$

hinzuzunehmen.

Wir behandeln zunächst den *ersten* (leichteren) *Fall.* Wir formen die Matrix A mittels 1., 2., 3. so weit um, daß *das absolut-kleinste von Null verschiedene Element von A einen möglichst kleinen absoluten Wert hat.* Durch Operation 1. können wir erreichen, daß dieses kleinste Element in der Matrix an der Stelle α_{11} steht. Macht man dann die übrigen Elemente der ersten Spalte durch Subtraktion geeigneter Vielfachen der ersten Zeile nach 2. möglichst klein, so werden sie dem Betrage nach kleiner als $|\alpha_{11}|$, also Null. Ebenso macht man mittels 3. die Elemente der ersten Zeile zu Null, ohne die erste Spalte zu ändern. Nach diesen Operationen müssen in der ganzen Matrix alle Elemente durch α_{11} teilbar sein (und zwar sowohl von links wie von rechts). Denn gesetzt, es wäre etwa α_{ik} nicht von links durch α_{11} teilbar, so wäre nach dem Divisionsalgorithmus

$$\alpha_{ik} = \alpha_{11} q + r, \qquad r \neq 0, \qquad |r| < |\alpha_{11}|.$$

Addiert man zuerst nach 2. die erste Zeile zur i-ten und subtrahiert man dann nach 3. die mit q multiplizierte erste Spalte von der k-ten, so erscheint an der Stelle (ik) das Element r mit $|r| < |\alpha_{11}|$, was der Minimalvoraussetzung über α_{11} widerspricht.

(Ist α_{ik} nicht von rechts durch α_{11} teilbar, so werden die Operationen 2., 3. in umgekehrter Reihenfolge angewandt.)

Nunmehr sieht unsere Matrix so aus:

$$\begin{pmatrix} \alpha_{11} & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & A' & \\ 0 & & & \end{pmatrix},$$

wo in A' alle Elemente (sowohl Links- wie Rechts-)Vielfache von α_{11} sind. Bei den weiteren Operationen läßt man nun die erste Zeile und Spalte ungeändert und verfährt mit A' genau so wie vorhin mit A. Ginge bei irgend einer dieser Operationen die Links- und Rechtsteilbarkeit aller Elemente durch α_{11} verloren, so könnte man sich nach dem obigen Beweis ein von Null verschiedenes Element r von kleinerem Absolutwert als $|\alpha_{11}|$ verschaffen, was nicht geht. Also bleiben diese Teilbarkeitsrelationen stets erhalten. A' erhält schließlich die Gestalt

$$\begin{pmatrix} \alpha_{22} & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & A'' & \\ 0 & & & \end{pmatrix},$$

wo alle Elemente von A'' durch α_{22} beiderseits teilbar sind. So fortfahrend, erreicht man nach m Schritten die gewünschte Normalform (2). Der Fall, daß schon vorher eine der Matrizes $A, A', A'', \dots$ aus lauter Nullen bestehen sollte, ist ausgeschlossen, da das heißen würde, daß einige v_k gleich Null wären, während im Gegenteil in jedem Stadium

des Prozesses die v_k eine linear-unabhängige Basis für $\mathfrak{R}$ bilden. Damit ist im ersten Fall der Satz bewiesen.

Im *zweiten Fall* ist der Gedankengang des Beweises ganz derselbe, nur hat man — da keine Beträge $|\alpha|$ zur Verfügung stehen — eine andere Minimalforderung zu stellen, nämlich die, daß *das Element mit den wenigsten Primfaktoren in der Matrix A möglichst wenig Primfaktoren besitzt.* An Stelle der Divisionen mit Rest treten jetzt die Operationen 4., 5.; dadurch werden nach dem zu Anfang dieses Paragraphen Gesagten immer je zwei Elemente a, b derselben Zeile oder Spalte durch d, 0 ersetzt, wobei d ihr größter gemeinsamer Teiler ist. Ist $a = \alpha_{11}$ und b nicht durch α_{11} teilbar, so hat d weniger Primfaktoren als α_{11}, und die Minimalbedingung ist verletzt. Also sind alle Elemente der ersten Zeile und Spalte durch α_{11} teilbar; sie können somit durch Operationen 2. und 3. (Subtraktion eines Vielfachen der ersten Zeile oder Spalte) zu Null gemacht werden. Weiter verläuft der Beweis genau so wie im ersten Fall[1].

Bemerkungen. 1. Die Operationen 1. bis 5. kommen immer darauf hinaus, daß die Matrix A von links oder von rechts mit einer in K invertierbaren Matrix multipliziert wird. Denn wenn $(u'_1 \dots u'_n) = (u_1 \dots u_n) \cdot B$ und $(v'_1 \dots v'_m) = (v_1 \dots v_m) \cdot C$ als neue Basen eingeführt werden, so wird

$$(v'_1 \dots v'_m) = (v_1 \dots v_m)\, C = (u_1 \dots u_n)\, A\, C = (u'_1 \dots u'_n)\, B^{-1} A\, C\,.$$

Der Elementarteilersatz ist also gleichbedeutend mit der Existenz zweier invertierbarer Matrizes B, C, so daß $B^{-1}AC$ eine Matrix von der Gestalt (2) wird.

2. Die Reduktion der Matrix A gelingt nach genau derselben Methode auch dann, wenn die v kein linear-unabhängiges System bilden; nur kann dann eine der Matrizes A, A', A'', ... eine Nullmatrix werden, und wir erhalten statt der Normalform (2) die allgemeinere

$$B^{-1}AC = \begin{pmatrix} \varepsilon_1 & & & 0 \\ & \ddots & & \\ & & \varepsilon_r & \\ 0 & & & 0 \end{pmatrix}, \tag{3}$$

wo r der Rang von A ist. Die Teilbarkeitsrelationen der ε_i bleiben dieselben.

3. Im kommutativen Fall hängen die k-reihigen Unterdeterminanten der transformierten Matrix $D = B^{-1}AC$ linear von denen von A ab,

[1] Die Bemerkung, daß der Elementarteilersatz auch für nichtkommutative Ringe K mit Divisionsverfahren (z. B. für den Polynombereich $\mathsf{P}[x]$, wo P ein nichtkommutativer Körper ist) gilt, scheint in der Literatur noch nicht vorzukommen. Es ist dem Verfasser nicht gelungen, Voraussetzungen zu finden, welche die beiden oben genannten Fälle umfassen.

und ebenso die von $A = BDC^{-1}$ linear von denen von D. Also ist für A der größte gemeinsame Teiler δ_k der k-reihigen Unterdeterminanten bis auf Einheiten derselbe wie für D. Für D berechnet man leicht den Wert

$$\delta_k = \varepsilon_1 \varepsilon_2 \dots \varepsilon_k \qquad (k \leqq r).$$

Mithin ist

$$\delta_k = \delta_{k-1} \varepsilon_k \qquad (1 < k \leqq r). \tag{4}$$

Die δ_k heißen die *Determinantenteiler* der Matrix A, die ε_k die *Elementarteiler* der Matrix A. Aus (4) folgt nun: *Die Elementarteiler sind die Quotienten zweier aufeinanderfolgender Determinantenteiler.*

4. Daß die Elementarteiler ε_k im kommutativen Fall bis auf Einheiten durch die Matrix A eindeutig bestimmt werden, wird sich auf anderem Wege im nächsten Paragraphen ergeben, in dem gezeigt wird, daß die Elementarteiler (soweit sie nicht Einheiten sind) sogar nur vom Faktormodul $\mathfrak{M}/\mathfrak{N}$ abhängen, der seinerseits natürlich durch A bestimmt ist.

Eine Fülle von schönen Sätzen über ganzzahlige Moduln findet man bei A. CHÂTELET: Leçons sur la théorie des Nombres, Paris 1913.

Aufgaben. 3. Man bringe die Matrix

$$A = \begin{pmatrix} 4 & 3 & 6 & 2 \\ 2 & 3 & 6 & 4 \\ 6 & 6 & 13 & 5 \end{pmatrix}$$

in die Diagonalform (3).

4. Jedes lineare diophantische Gleichungssystem

$$\sum_1^n \alpha_{ik} \xi_k = \beta_i \qquad (i = 1, \dots, m) \tag{5}$$

(mit ganzen Zahlen α_{ik} und β_i) ist durch unimodulare Transformation der Unbekannten und der Gleichungen in die Gestalt

$$\begin{cases} \varepsilon_i \eta_i = \gamma_i & (i = 1, \dots, r;\ \varepsilon_i \neq 0) \\ 0 = \delta_j & (j = r+1, \dots, m) \end{cases}$$

transformierbar. Die Bedingungen für Lösbarkeit des Systems in ganzen Zahlen lauten:

$$\gamma_i \equiv 0 \,(\varepsilon_i); \quad \delta_j = 0.$$

Die η_i mit $i \leqq r$ sind bestimmbar, die übrigen η_j willkürlich. Die ξ_k sind lineare ganzzahlige Funktionen der willkürlichen η_j.

5. Ein lineares Gleichungssystem (5) ist in ganzen Zahlen dann und nur dann lösbar, wenn aus

$$\sum_1^m \lambda_i \alpha_{ik} \equiv 0 \,(d) \qquad (k = 1, \dots, n)$$

für beliebige ganzzahlige λ_i und d stets folgt

$$\sum_1^m \lambda_i \beta_i \equiv 0 \,(d).$$

§ 107. Der Hauptsatz über Abelsche Gruppen.

Es sei $\mathfrak{G}$ eine Abelsche Gruppe mit endlichvielen Erzeugenden, additiv geschrieben, also ein Modul. Wenn ein Multiplikatorenbereich K zu $\mathfrak{G}$ gegeben ist, nehmen wir an, daß er von der in § 106 beschriebenen Art sei (Ring ohne Nullteiler mit Divisionsalgorithmus oder Hauptidealring); wenn aber kein Multiplikatorenbereich gegeben ist, nehmen wir als Multiplikatorenbereich den Ring der ganzen Zahlen, der ebenfalls diese Voraussetzungen erfüllt. Wir schreiben diesmal die Operatoren links von den Modulelementen.

Zunächst sei $\mathfrak{G}$ zyklisch: $\mathfrak{G} = (g)$. Die Gesamtheit der μ aus K, welche g annullieren, ist ein Linksideal $\mathfrak{a}$ aus K: aus $\mu_1 g = 0$ und $\mu_2 g = 0$ folgt $(\mu_1 - \mu_2) g = 0$, und aus $\mu g = 0$ folgt $\varkappa \mu g = 0$ für jedes $\varkappa$ in K. Jedem λ aus K ist ein λg zugeordnet, und wegen

$$(\lambda + \mu) g = \lambda g + \mu g ,$$
$$\lambda \mu \cdot g = \lambda \cdot \mu g$$

ist die Zuordnung ein Operatorhomomorphismus in bezug auf K. Daraus folgt nach dem Isomorphiesatz

$$\mathfrak{G} \cong \mathsf{K}/\mathfrak{a} ,$$

oder: *Ein zyklischer* K*-Modul* $\mathfrak{G}$ *ist isomorph dem Restklassenmodul von* K *nach dem annullierenden Linksideal von* $\mathfrak{G}$.

Für den Fall einer gewöhnlichen zyklischen Gruppe $\mathfrak{G}$ erhalten wir daraus von neuem das Ergebnis, daß $\mathfrak{G}$ isomorph der additiven Gruppe der ganzen Zahlen oder der Gruppe der Restklassen nach einer ganzen Zahl ist. Ist $n > 0$ das Basiselement des Ideals $\mathfrak{a}$, so ist n die Ordnung der zyklischen Gruppe (g) oder auch die Ordnung des Elementes g (vgl. § 7).

Der eben bewiesene Satz gilt noch unabhängig von speziellen Voraussetzungen über K. Ist aber K kommutativ und nullteilerfrei und jedes Ideal in K Hauptideal, also insbesondere $\mathfrak{a} = (\alpha)$, und ist weiter $\alpha \neq 0$, so können wir etwas mehr aussagen. Wir zerlegen, wenn möglich, α in zwei teilerfremde Faktoren:

$$\alpha = \varrho \sigma ,$$
$$1 = \lambda \varrho + \mu \sigma ,$$

und bilden die zyklischen Gruppen $\mathfrak{G}_1 = (\varrho g)$, $\mathfrak{G}_2 = (\sigma g)$. Dann wird $\mathfrak{G}_1$ von σ, $\mathfrak{G}_2$ von ϱ annulliert. Wegen

$$g = \lambda \varrho g + \mu \sigma g$$

ist $\mathfrak{G}$ die Summe von $\mathfrak{G}_1$ und $\mathfrak{G}_2$. Der Durchschnitt $\mathfrak{G}_1 \cap \mathfrak{G}_2$ wird von ϱ und von σ, also auch von $1 = \lambda \varrho + \mu \sigma$ annulliert; mithin ist $\mathfrak{G}_1 \cap \mathfrak{G}_2 = (0)$ und die Summe direkt:

$$\mathfrak{G} = \mathfrak{G}_1 + \mathfrak{G}_2 .$$

Wenn σ oder ϱ weiter in teilerfremde Faktoren zerlegbar ist, so läßt sich $\mathfrak{G}_1$ oder $\mathfrak{G}_2$ weiter aufspalten. *Schließlich wird die zyklische Gruppe* $\mathfrak{G}$ *eine direkte Summe von solchen zyklischen Gruppen, die von Primzahlpotenzen*[1] *annulliert werden. Das Produkt dieser Primzahlpotenzen ist* α. Für Gruppen von dieser Beschaffenheit werden wir die Bezeichnung *„Primzahlpotenzgruppen"* verwenden.

Wir gehen nun zum allgemeinen Fall über, wo $\mathfrak{G}$ ein K-Modul mit endlichvielen Erzeugenden $g_1, \ldots, g_n$ ist, also die Elemente von $\mathfrak{G}$ die Gestalt

$$\lambda_1 g_1 + \cdots + \lambda_n g_n$$

haben. Bilden wir mit Unbestimmten $u_1, \ldots, u_n$ den Linearformenmodul

$$\mathfrak{M} = (u_1, \ldots, u_n),$$

so ist jeder Linearform $\sum \lambda_i u_i$ aus $\mathfrak{M}$ ein Element $\sum \lambda_i g_i$ von $\mathfrak{G}$ zugeordnet; die Zuordnung ist wiederum ein Modulhomomorphismus, und es folgt nach dem Homomorphiesatz

$$\mathfrak{G} \simeq \mathfrak{M}/\mathfrak{N},$$

wo $\mathfrak{N}$ der Untermodul derjenigen Linearformen $\sum \lambda_i u_i$ ist, für die $\sum \lambda_i g_i = 0$ wird.

Nach § 106 können wir für $\mathfrak{N}$ und $\mathfrak{M}$ neue Basen $(v_1, \ldots, v_m)$ und $(u'_1, \ldots, u'_n)$ $(n \geqq m)$ einführen, für die gilt:

$$v_i = \varepsilon_i u'_i \qquad \text{für } i = 1, \ldots, m,$$
$$\varepsilon_{i+1} \equiv 0 \,(\varepsilon_i).$$

Zu den u' gehören (vermöge des obigen Homomorphismus) wieder Elemente $h_1, \ldots, h_n$ von $\mathfrak{G}$. Alle Elemente von $\mathfrak{G}$ haben die Gestalt $\mu_1 h_1 + \cdots + \mu_n h_n$, und ein solches Element ist Null dann und nur dann, wenn

$$\mu_1 u'_1 + \cdots + \mu_n u'_n \equiv 0 \,(v_1, \ldots, v_m),$$

d. h. wenn

$$\begin{cases} \mu_1 \equiv 0 \,(\varepsilon_1), \\ \cdots\cdots\cdots \\ \mu_m \equiv 0 \,(\varepsilon_m), \end{cases} \qquad \begin{cases} \mu_{m+1} = 0, \\ \cdots\cdots\cdots \\ \mu_n = 0 \end{cases}$$

ist. Das heißt, eine Summe $\mu_1 h_1 + \cdots + \mu_n h_n$ ist nur dann Null, wenn die einzelnen Glieder es sind, und diese sind es, wenn ihr Koeffizient μ_i durch ε_i teilbar ist für $i = 1, \ldots, m$, dagegen Null ist für $i = m + 1, \ldots, n$.

---

[1] „Primzahl" steht kurz für „Primelement des Ringes K". Im Falle der gewöhnlichen Abelschen Gruppe handelt es sich um gewöhnliche Primzahlen.

Ein anderer Ausdruck dafür ist:

Die Gruppe $\mathfrak{G}$ *ist die direkte Summe von zyklischen Gruppen* $(h_1) + \cdots + (h_n)$, *und das annullierende Ideal von* (h_i) *ist*

$$(\varepsilon_i) \quad \text{für} \quad i = 1, \ldots, m,$$
$$(0) \quad \text{für} \quad i = m+1, \ldots, n.$$

Das ist der *Hauptsatz für Abelsche Gruppen mit endlichvielen Erzeugenden.*

Im Fall der gewöhnlichen Abelschen Gruppen sind die $|\varepsilon_i|$ die Ordnungen der zyklischen Gruppen $(h_1), \ldots, (h_m)$, während die übrigen $(h_{m+1}), \ldots, (h_n)$ unendliche Ordnung haben.

Drei Ergänzungen zum Hauptsatz sind noch nötig:

a) die Ausscheidung der Einheiten unter den ε_i;

b) die weitere Zerlegung der zyklischen Gruppen nach Primzahlpotenzgruppen;

c) die Eindeutigkeit.

Bei b) und c) wird K als *kommutativ* vorausgesetzt.

a) Es sei etwa ε_1 eine Einheit, also (ε_1) das Einheitsideal K, also $\mathsf{K}h_1 = (0)$. Dann kann die zyklische Gruppe $\mathsf{K}h_1$ aus der Summenzerlegung $\mathsf{K}h_1 + \cdots + \mathsf{K}h_n$ weggelassen werden.

Die nach Ausscheidung der Einheiten übrigbleibenden annullierenden Ideale (ε_i), (0) mögen jetzt *in umgekehrter Reihenfolge* $\mathfrak{a}_1, \ldots, \mathfrak{a}_q$ heißen; dann ist

$$\mathfrak{a}_i \equiv 0 \,(\mathfrak{a}_{i+1}).$$

b) Diejenigen Gruppen (h_i), deren annullierendes Ideal (0) ist, sind isomorph zu K. Diejenigen aber, deren annullierendes Ideal $(\varepsilon_i) \neq (0)$ ist, können nach dem zu Anfang Bewiesenen weiter in Primzahlpotenzgruppen aufgespalten werden. Die annullierenden Primzahlpotenzen selbst findet man durch Faktorzerlegung der ε_i. Die Summe aller zu einer Primzahl p gehörigen in der Zerlegung von $\mathfrak{G}$ auftretenden Gruppen ist eine Gruppe $\mathfrak{B}_p$ und besteht aus denjenigen Elementen von $\mathfrak{G}$, die von einer genügend hohen Potenz p^ϱ annulliert werden. Daher: *Die Gruppen* $\mathfrak{B}_p$ *sind eindeutig bestimmt.* Man hat, wenn $\mathfrak{U}$ die Summe der Gruppen mit $\mathfrak{a} = (0)$ bedeutet,

$$\mathfrak{G} = \sum_p \mathfrak{B}_p + \mathfrak{U}.$$

Durch weitere Zerlegung der $\mathfrak{B}_p$ erhält man rückwärts die Primzahlpotenzgruppen, die nicht absolut-eindeutig bestimmt sind, wohl aber eindeutig bis auf Isomorphie, wie wir sehen werden. Es gibt aber in jedem $\mathfrak{B}_p$ noch eine eindeutig bestimmte Reihe von Untergruppen $\mathfrak{B}_{p,\varrho}; \mathfrak{B}_{p,\varrho-1}; \ldots; \mathfrak{B}_{p,0}$; wo $\mathfrak{B}_{p,\nu}$ aus den Elementen von $\mathfrak{B}_p$ besteht, die von p^ν annulliert werden. Die erste Gruppe dieser Reihe ist $\mathfrak{B}_p$; die letzte besteht nur aus der Null.

Die Gruppe $\mathfrak{U}$ ist nicht eindeutig, wohl aber bis auf Isomorphie eindeutig wegen

$$\mathfrak{U} \cong \mathfrak{G}/\sum_p \mathfrak{B}_p .$$

c) Eindeutigkeitssatz: *Die annullierenden Ideale* $\mathfrak{a}_1, \ldots, \mathfrak{a}_q$ *mit* $\mathfrak{a}_i \equiv 0\,(\mathfrak{a}_{i+1})$, *die in einer direkten Summenzerlegung* $\mathfrak{G} = \mathfrak{C}_1 + \cdots + \mathfrak{C}_q$ *auftreten, sind durch den Modul* $\mathfrak{G}$ *allein eindeutig bestimmt.* (Oder, was dasselbe ist: die Gruppen $\mathfrak{C}_i$ sind bis auf Isomorphie eindeutig bestimmt.)

Beweis: Die behauptete Eindeutigkeit wird bewiesen sein, sobald gezeigt ist, daß von jeder Primzahlpotenz p^σ aus K eindeutig entschieden werden kann, in wievielen Idealen $\mathfrak{a}_i$ sie aufgeht. Wenn p^σ nämlich in genau k von diesen Idealen aufgeht, so sind dies wegen der Teilbarkeitseigenschaften dieser Ideale von selbst die ersten k unter ihnen, also $\mathfrak{a}_1, \ldots, \mathfrak{a}_k$, und so weiß man dann von jeder Primzahlpotenz p^σ nicht nur, in wievielen, sondern auch, in welchen $\mathfrak{a}_i$ sie aufgeht, und somit von jedem $\mathfrak{a}_i$, welche Primzahlpotenzen darin aufgehen. Diejenigen $\mathfrak{a}_i$, in denen unbeschränkt hohe Potenzen aufgehen, sind Null, und die übrigen durch ihre Primfaktorzerlegung eindeutig bestimmt.

Wenn p^σ im annullierenden Ideal der zyklischen Gruppe $\mathfrak{C}_i$ aufgeht, so ist

$$p^{\sigma-1}\mathfrak{C}_i/p^\sigma\mathfrak{C}_i$$

eine zyklische Gruppe mit dem annullierenden Ideal (p), also eine einfache Gruppe. Geht dagegen p^σ nicht auf, so ist $p^\sigma\mathfrak{C}_i = p^{\sigma-1}\mathfrak{C}_i$, mithin $p^{\sigma-1}\mathfrak{C}_i/p^\sigma\mathfrak{C}_i = (0)$. Daher ist $p^{\sigma-1}\mathfrak{G}/p^\sigma\mathfrak{G}$ eine direkte Summe von so vielen einfachen Gruppen, als die Anzahl k der durch p^σ teilbaren $\mathfrak{a}_i$ angibt. Somit ist k gleich der Länge der Kompositionsreihe für $p^{\sigma-1}\mathfrak{G}/p^\sigma\mathfrak{G}$, mithin eindeutig bestimmt.

Aufgaben. 1. Man führe den letzten, skizzierten Teil des zuletzt gegebenen Beweises vollständig durch.

2. Die unter b) konstruierte Gruppe $\mathfrak{U}$ ist ein Linearformenmodul in bezug auf den Ring C der ganzen Zahlen, und die Anzahl seiner zyklischen Summanden ist zugleich der Rang von $\mathfrak{G}$ (Rang = Maximalzahl von linear-unabhängigen Elementen in bezug auf K).

3. Man gebe einen zweiten Eindeutigkeitsbeweis mit Hilfe der Längen der Kompositionsreihen der unter b) konstruierten eindeutig bestimmten Gruppen und ihrer Faktorgruppen. Auch der Rang des Moduls $\mathfrak{U}$ (Aufg. 2) kann herangezogen werden.

Im Spezialfall der endlichen Abelschen Gruppen (mit dem Ring der ganzen Zahlen als Multiplikatorenbereich) können wir für den Hauptsatz auch folgenden direkten Beweis durch vollständige Induktion nach der Gruppenordnung geben:

Wir suchen ein Element höchster Ordnung z_0, das eine zyklische Gruppe $\mathfrak{Z}_0$ erzeugt. Die Faktorgruppe $\mathfrak{G}/\mathfrak{Z}_0$ ist nach der Induktionsvoraussetzung eine direkte Summe von zyklischen Gruppen:

$$(1) \qquad \mathfrak{G}/\mathfrak{Z}_0 = \bar{\mathfrak{Z}}_1 + \cdots + \bar{\mathfrak{Z}}_r .$$

$\mathfrak{Z}_1$ werde von einer Restklasse $\bar{z}_1$ erzeugt, aus der wir einen Repräsentanten z_1 wählen. Die annullierende Zahl (Ordnung) von $\bar{z}_1$ sei a_1, also $a_1\bar{z}_1 = 0$, $a_1 z_1 \in \mathfrak{Z}_0$, etwa $a_1 z_1 = b z_0$. Ersetzen wir z_1 durch $z_1 - q z_0$ (welches Element in derselben Restklasse $\bar{z}_1$ enthalten ist), so wird $a_1(z_1 - q z_0) = b z_0 - q a_1 z_0 = (b - q a_1) z_0$; also können wir immer b durch seinen kleinsten Rest nach a_1 ersetzen, also $|b| < |a_1|$ voraussetzen. Ist n die Ordnung von z_0, so ist die Ordnung von z_1 gleich $\frac{a_1 n}{(b, n)}$. Das muß dem Betrage nach höchstens gleich $|n|$ sein:

$$\left|\frac{a_1 n}{(b, n)}\right| \leqq |n|$$

$$|a_1| \leqq |(b, n)| \leqq |b| \qquad \text{(falls } b \neq 0\text{)}.$$

Die Relation $|a_1| \leqq |b|$ steht aber in Widerspruch zur Voraussetzung $|b| < |a_1|$. Also muß $b = 0$ sein. Mithin ist $a_1 z_1 = 0$ und die Ordnung von z_1 gleich der von $\bar{z}_1$. Dasselbe gilt von den entsprechend zu definierenden Elementen $z_2, \ldots, z_r$. Wegen (1) ist jedes Element von $\mathfrak{G}$ modulo $\mathfrak{Z}_0$ kongruent einer Linearkombination der $z_1, \ldots, z_r$:

$$g \equiv c_1 z_1 + \cdots + c_r z_r (\mathfrak{Z}_0) \tag{2}$$

und die Koeffizienten c_ν sind modulo den Ordnungen $a_1, \ldots, a_r$ von $\bar{z}_1, \ldots, \bar{z}_r$ oder $z_1, \ldots, z_r$ eindeutig bestimmt. Aus (2) folgt:

$$g - (c_1 z_1 + \cdots + c_r z_r) = c_0 z_0$$

mit eindeutig bestimmtem $c_0 z_0$. Also ist $\mathfrak{G}$ die direkte Summe der von $z_0, \ldots, z_r$ erzeugten zyklischen Gruppen $\mathfrak{Z}_0, \ldots, \mathfrak{Z}_r$.

Diese Gruppen kann man dann noch wie oben in Primzahlpotenzgruppen zerspalten.

Man überzeugt sich leicht, daß dieselben Betrachtungen auch dann gelten, wenn der Multiplikatorenbereich der Polynomring $\mathsf{P}[u]$ ist. Statt mit Beträgen $|a|$ muß man dann mit den Gradzahlen der Polynome arbeiten. Voraussetzung ist, daß die Gruppe $\mathfrak{G}$ einen endlichen Rang in bezug auf den Körper P hat; nach diesem Rang richtet sich auch die vollständige Induktion. Aus der Voraussetzung des endlichen Ranges folgt auch, daß es für jedes Gruppenelement z unter den Größen $z, uz, u^2 z, \ldots$ nur endlich viele linear-unabhängige gibt, oder daß jedes z durch ein Polynom $f(u) \neq 0$ annulliert wird, was beim obigen Beweis benutzt wurde.

Man kann in ähnlicher Weise auch den allgemeinen Fall des Hauptsatzes direkt, d. h. ohne Benutzung der Elementarteilertheorie des § 106 beweisen und aus dem Beweis umgekehrt den Elementarteilersatz des § 106 herleiten[1].

Es ist wohl unnötig, zu erwähnen, daß alles in diesem Paragraphen Bewiesene sich sofort auf multiplikative Abelsche Gruppen überträgt, wenn man Produkt statt Summe schreibt.

Für endliche Abelsche Gruppen ist folgende Notation üblich: Es bezeichnet z. B. $\mathfrak{A}_{2,2,4,3}$ die direkte Summe (das direkte Produkt) von zyklischen Gruppen der Ordnungen 2, 2, 4, 3 [also der annullierenden Ideale (2), (2), (4), (3)]. Es erscheint zweckmäßig, die Notation so zu erweitern, daß sie auch zyklische Summanden von unendlicher Ordnung [also mit dem annullierenden Ideal (0)] umfaßt, und etwa $\mathfrak{A}_{4,0}$ zu schreiben für eine direkte Summe zweier zyklischer Gruppen mit den annullierenden Idealen (4), (0).

[1] Siehe H. Prüfer: Theorie der Abelschen Gruppen, Math. Zeitschr. Bd. 20, S. 165—187, 1924, sowie K. Shoda: Proc. Imp. Acad. Tokio Bd. 6, S. 217 bis 219, 1930.

Aufgaben. 4. Ist eine Abelsche Gruppe von der Ordnung n zyklisch, so ist n die kleinste Zahl, die alle Elemente der Gruppe annulliert; ist dagegen die Gruppe nicht zyklisch, so gibt es schon einen echten Teiler von n, der das tut.

5. Mit Hilfe von 4. beweise man, daß die multiplikative Gruppe derjenigen Restklassen mod p^k, deren Zahlen nicht durch p teilbar sind, eine zyklische Gruppe ist, ausgenommen wenn $p = 2$ und $k \geqq 3$ ist, wo sie den Typus $\mathfrak{A}_{2,2^{k-2}}$ hat. [Man berechne die Ordnungen der Elemente $1 + p$ und g, wo g eine Primitivzahl mod p ist.]

6. Die multiplikative Gruppe derjenigen Restklassen mod n, deren Zahlen zu n teilerfremd sind, ist isomorph dem direkten Produkt der entsprechenden Gruppen modulo den höchsten in n aufgehenden Primzahlpotenzen.

§ 108. Darstellungen und Darstellungsmoduln.

Unter einer *Darstellung eines Ringes* $\mathfrak{o}$ *durch lineare Transformationen oder durch Matrizes in* K versteht man einen Homomorphismus

$$\mathfrak{o} \sim \mathfrak{D},$$

wo $\mathfrak{D}$ ein Ring aus quadratischen Matrizes r-ten Grades in K ist. Ist der Homomorphismus ein Isomorphismus, so hat man eine *treue Darstellung*. Sind $\mathfrak{o}$ und K beide hyperkomplex in bezug auf einen Körper P, so verlangt man meist außer Ringhomomorphismus auch Operatorhomomorphismus in bezug auf P: wenn $a \to A$, so soll $a\varrho \to A\varrho$ sein für $\varrho \in \mathsf{P}$.

Bei den Anwendungen ist K meist ein Körper. Im hyperkomplexen Fall ist P im Zentrum von K enthalten.

Unter einem *Darstellungsmodul* von $\mathfrak{o}$ in bezug auf K versteht man einen „*Doppelmodul*" $\mathfrak{M}$, der $\mathfrak{o}$ als Links- und K als Rechtsmultiplikatorenbereich besitzt, mit folgenden Eigenschaften:

1. $\mathfrak{M}$ kann als Linearformenmodul in bezug auf K aufgefaßt werden:

$$\mathfrak{M} = u_1 \mathsf{K} + \cdots + u_n \mathsf{K}.$$

2. Für $a \in \mathfrak{o}$, $u \in \mathfrak{M}$, $\lambda \in \mathsf{K}$ gilt:

$$a \cdot u\lambda = au \cdot \lambda. \tag{1}$$

Die letztere Forderung besagt, daß die Multiplikation mit a einen Operatorhomomorphismus des K-Moduls $\mathfrak{M}$, d. h. eine lineare Transformation darstellt. Die lineare Transformation wird durch eine quadratische Matrix $A = (\alpha_{ik})$ gegeben:

$$\begin{cases} a \cdot u_k = \sum u_j \alpha_{jk}, \\ a \cdot \sum u_k \lambda_k = \sum\sum u_j \alpha_{jk} \lambda_k. \end{cases} \tag{2}$$

So entspricht jedem a aus $\mathfrak{o}$ eine Matrix A in K. Zufolge der Modulpostulate entsprechen dem Produkt und der Summe zweier Elemente a, b

von $\mathfrak{o}$ auch Produkt und Summe der zugehörigen linearen Transformationen und daher auch ihrer Matrizes. *Also ist die Zuordnung* $a \to A$ *eine Darstellung des Ringes* $\mathfrak{o}$.

Ist umgekehrt eine Darstellung eines Ringes $\mathfrak{o}$ durch lineare Transformationen eines Linearformenmoduls $\mathfrak{M}$ in bezug auf K gegeben, so kann man aus $\mathfrak{M}$ einen Doppelmodul machen, indem man die Produkte $a \cdot u$ ($a \in \mathfrak{o}$, $u \in \mathfrak{M}$) durch (2) definiert. Rückwärts schließt man dann, daß alle Doppelmoduleigenschaften und die Regel (1) erfüllt sind, daß also $\mathfrak{M}$ *ein Darstellungsmodul ist.*

So gehört zu jedem Darstellungsmodul eine Darstellung von $\mathfrak{o}$ *durch lineare Transformationen oder nach Wahl einer* K*-Basis* $(u_1, \ldots, u_n)$ *durch Matrizes in* K*, und umgekehrt zu jeder Darstellung ein Darstellungsmodul.*

Geht man von der Basis $(u_1, \ldots, u_n)$ vermöge

$$(u'_1 \ldots u'_n) = (u_1 \ldots u_n) P$$

zu einer anderen Basis $(u'_1, \ldots, u'_n)$ über, so wird dieselbe lineare Transformation durch die Matrix

$$A' = P^{-1} A P$$

dargestellt. Den Ringelementen a werden also jetzt neue Matrizes A zugeordnet; man spricht von einer *äquivalenten Darstellung*. Da somit der Übergang zu einer äquivalenten Darstellung nichts anderes ist als der Übergang zu einer anderen Basis für denselben (oder einen dazu operatorisomorphen) Darstellungsmodul, so schließt man: *Zu isomorphen Darstellungsmoduln gehören äquivalente Darstellungen und umgekehrt.*

Sind $\mathfrak{o}$ und K beide hyperkomplex in bezug auf einen kommutativen Körper P im Zentrum von K und verlangt man, daß aus $a \to A$ folgen soll $a\varrho \to A\varrho$, so heißt das für den Darstellungsmodul:

$$a\varrho \cdot u (= \varrho\, a \cdot u) = a u \cdot \varrho.$$

Die Skalaren ϱ aus P kann man also in einem Produkt an beliebiger Stelle schreiben: sie sind mit allen auftretenden Größen vertauschbar.

Ein System von linearen Transformationen eines Linearformenmoduls $\mathfrak{M}$, insbesondere eine Darstellung eines Ringes, heißt *reduzibel*, wenn alle Transformationen des Systems einen festen linearen Unterraum $\mathfrak{N}$ ($\neq (0)$, $\neq \mathfrak{M}$) in sich transformieren. $\mathfrak{N}$ heißt dann ein *invarianter Unterraum*. Faßt man, wenn es sich um eine Darstellung eines Ringes $\mathfrak{o}$ handelt, $\mathfrak{M}$ als Doppelmodul in bezug auf $\mathfrak{o}$ und K auf, so wird der invariante Unterraum $\mathfrak{N}$ alle Elemente von $\mathfrak{o}$ als Linksoperatoren gestatten. Daraus folgt: *Eine Darstellung eines Ringes ist dann und nur dann reduzibel, wenn der zugehörige Darstellungsmodul einen (Doppel-) Untermodul* $\mathfrak{N}$ *besitzt.*

Es sei nun K ein Körper. Um zu untersuchen, wie die Matrizes einer reduziblen Darstellung aussehen, gehen wir aus von einer K-Basis

für $\mathfrak{N}$ und ergänzen sie zu einer K-Basis für $\mathfrak{M}$ (vgl. § 105). Es sei also

$$\mathfrak{N} = v_1\mathsf{K} + \cdots + v_r\mathsf{K},$$
$$\mathfrak{M} = v_1\mathsf{K} + \cdots + v_r\mathsf{K} + w_1\mathsf{K} + \cdots + w_t\mathsf{K}.$$

Die Tatsache, daß eine lineare Transformation den Modul $\mathfrak{N}$ in sich transformiert, bedeutet, daß die Transformierten der v sich durch die v allein ausdrücken:

$$\text{(3)} \qquad \begin{cases} v_j' = \sum v_i \varrho_{ij}, \\ w_j' = \sum v_i \sigma_{ij} + \sum w_i \tau_{ij}. \end{cases}$$

Setzt man $R = (\varrho_{ij})$, $S = (\sigma_{ij})$, $T = (\tau_{ij})$, so wird die Transformation durch die Matrix

$$\text{(4)} \qquad A = \begin{pmatrix} R & S \\ 0 & T \end{pmatrix}$$

dargestellt. Es folgt: *Dann und nur dann ist ein System von Matrizes reduzibel, wenn alle Matrizes des Systems gleichzeitig durch eine Transformation $A' = P^{-1}AP$ (Wahl einer neuen Basis) in die Form* (4) *gebracht werden können.*

Aus (3) folgt:

$$\text{(5)} \qquad \begin{aligned} (v_1' \ \ldots \ v_r') &= (v_1 \ \ldots \ v_r)\cdot R, \\ (w_1' \ \ldots \ w_t') &\equiv (w_1 \ \ldots \ w_t)\cdot T \,(\mathrm{mod}\,\mathfrak{N}). \end{aligned}$$

Daraus liest man ab:

Faßt man bei einer reduziblen Darstellung eines Ringes $\mathfrak{o}$ den invarianten Untermodul $\mathfrak{N}$ und den Faktormodul $\mathfrak{M}/\mathfrak{N}$ selbst als Darstellungsmoduln auf, so werden die dadurch vermittelten Darstellungen durch die Bestandteile R und T von (4) *gegeben.*

Nimmt man für $\mathfrak{N}$ einen maximalen invarianten Untermodul $\mathfrak{M}_{l-1}$, in diesem wieder einen maximalen invarianten Untermodul $\mathfrak{M}_{l-2}$ usw., bis man eine Kompositionsreihe

$$\mathfrak{M} = \mathfrak{M}_l, \quad \mathfrak{M}_{l-1}, \quad \ldots, \quad \mathfrak{M}_0 = (0)$$

hat, so sehen die Matrizes der Darstellung bei passender Basiswahl so aus:

$$\text{(6)} \qquad \begin{pmatrix} R_{11} & \cdots & \cdots & R_{1l} \\ 0 & R_{22} & & \vdots \\ \vdots & & \ddots & \vdots \\ 0 & \cdots & 0 & R_{ll} \end{pmatrix}.$$

Die Diagonalkästchen R_{ii} ergeben Darstellungen, die zu den Kompositionsfaktoren $\mathfrak{M}_i/\mathfrak{M}_{i-1}$ gehören; da diese Kompositionsfaktoren einfache Doppelmoduln (d. h. ohne invariante Untermoduln) sind, so sind die zugehörigen Darstellungen *irreduzibel*. Der Prozeß, der zu (6) führt, ist das *„Ausreduzieren"* einer Darstellung. Nach dem Satz von JORDAN

und HÖLDER (§ 41) sind die Kompositionsfaktoren bis auf die Reihenfolge und bis auf Operatorisomorphie eindeutig bestimmt; mithin: *Die irreduziblen Bestandteile R_{ii} der ausreduzierten Darstellung* (6) *sind bis auf die Reihenfolge und bis auf äquivalente Darstellungen eindeutig bestimmt.*

Fehlen in (3) die σ_{ij}, so heißt das, daß nicht nur $(v_1, \ldots, v_r)$, sondern auch $(w_1, \ldots, w_t)$ ein invarianter Untermodul ist, also daß $\mathfrak{M}$ eine *direkte Summe zweier invarianten Untermoduln* $\mathfrak{N}$, $\mathfrak{Q}$ ist. Die Matrix (4) sieht dann so aus:

$$A = \begin{pmatrix} R & 0 \\ 0 & T \end{pmatrix},$$

wo R zu der durch $\mathfrak{N}$ und T zu der durch $\mathfrak{Q}$ vermittelten Darstellung gehört. Man sagt dann, daß die Darstellung $a \to A$ *zerfällt* in die Darstellungen $a \to R$ und $a \to T$.

Ist der Doppelmodul $\mathfrak{M}$ vollständig reduzibel im Sinn von § 42, d. h. direkte Summe von einfachen Doppelmoduln, so wird die durch $\mathfrak{M}$ vermittelte Darstellung gegeben durch die Matrix

$$\begin{pmatrix} R_{11} & & 0 \\ & R_{22} & \\ & & \ddots \\ 0 & & R_{ll} \end{pmatrix}, \tag{7}$$

wo die einzelnen Kästchen irreduzible Darstellungen ergeben, unter denen natürlich auch gleiche vorkommen dürfen. Man nennt eine solche Darstellung *vollständig reduzibel.*

Beispiele zu den Begriffsbildungen dieses Paragraphen liefert die Theorie der einzelnen Matrix im nächsten Paragraphen.

Aufgaben. 1. Jede (gruppenhomomorphe) Darstellung einer (endlichen oder unendlichen) Gruppe durch lineare Substitutionen kann zu einer (ringhomomorphen) Darstellung des „Gruppenrings" (§ 10, Aufgabe 13) ergänzt werden, indem man, wenn den Gruppenelementen g_i die Matrizes G_i zugeordnet sind, einer Linearkombination $\sum g_i \lambda_i$ die Matrix $\sum G_i \lambda_i$ zuordnet.

2. Ist $\mathfrak{o}$ ein Ring mit Einselement und ist in einer Darstellung von $\mathfrak{o}$ dem Einselement die Einheitsmatrix zugeordnet, so bedeutet das für den Darstellungsmodul, daß das Einselement Einheitsoperator ist. Man zeige mit Hilfe eines Satzes aus § 104, daß jede Darstellung von $\mathfrak{o}$ zerfällt in eine solche, in der dem Einselement die Einheitsmatrix entspricht, und eine solche, in der jedem Element die Nullmatrix zugeordnet ist:

$$A = \begin{pmatrix} S & 0 \\ 0 & 0 \end{pmatrix}.$$

3. Eine Darstellung ist dann und nur dann vollständig reduzibel,

wenn zu jedem invarianten Unterraum $\mathfrak{N}$ ein anderer ebensolcher $\mathfrak{Q}$ gefunden werden kann, der zusammen mit $\mathfrak{N}$ den Raum $\mathfrak{M}$ aufspannt:

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

4. Ist $(u'_1 \ldots u'_n) = (u_1 \ldots u_n) P$ ein Homomorphismus des Darstellungsmoduls in sich, so ist die Matrix P mit allen Matrizes der Darstellung vertauschbar:

$$A P = P A,$$

und umgekehrt.

§ 109. Normalformen für eine Matrix in einem kommutativen Körper.

Es sei $\mathfrak{M} = (u_1, \ldots, u_n)$ ein Linearformenmodul in bezug auf den kommutativen Körper K und

$$u_k \to v_k = \sum u_i \alpha_{ik}$$ [1]

eine lineare Transformation von $\mathfrak{M}$ in sich. Wir wollen durch Einführung einer neuen Basis

$$(u'_1 \ldots u'_n) = (u_1 \ldots u_n) P$$

(wo also P eine invertierbare Matrix in K ist) die Matrix $A = (\alpha_{ik})$ auf eine möglichst einfache Normalform

$$A' = P^{-1} A P$$

bringen. Man bemerke den Unterschied gegenüber der Fragestellung von § 106, wo es sich um zwei neue Basen (v') und (u') handelte und $A' = B^{-1} A C$ gesetzt wurde. Es wird jetzt also die Transformationsmöglichkeit eingeschränkt; dementsprechend muß auch von K mehr vorausgesetzt werden, nämlich, daß K ein Körper ist.

Wir fassen nun die Potenzen der Matrix A als eine meromorphe Darstellung der Potenzen einer Unbestimmten x auf und erweitern diese Darstellung zu einer Darstellung des Polynombereichs $\mathsf{K}[x]$, indem wir dem Polynom

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

die Matrix

$$f(A) = \sum \alpha_\nu A^\nu$$

entsprechen lassen. Die Darstellung ist homomorph, weil die Potenzen von A untereinander und mit den Koeffizienten α_ν vertauschbar sind.

Zu dieser Darstellung gehört der Darstellungsmodul $\mathfrak{M}$, wenn das Produkt eines Polynoms aus $\mathsf{K}[x]$ mit einem $u \in \mathfrak{M}$ definiert wird durch

$$\left(\sum \alpha_\nu x^\nu\right) u = \sum \alpha_\nu A^\nu u.$$

---

[1] Da K kommutativ ist, so ist es ganz einerlei, ob wir die Koeffizienten rechts oder links schreiben.

Der Darstellungsmodul $\mathfrak{M}$ ist ein Doppelmodul in bezug auf $\mathsf{K}[x]$ und K; aber da die Größen aus K mit allen anderen und untereinander vertauschbar sind, können wir sie auch links von den Elementen von $\mathfrak{M}$ schreiben:

$$u\lambda = \lambda u,$$

also $\mathfrak{M}$ als $\mathsf{K}[x]$-Modul schlechthin auffassen.

Da der Polynombereich $\mathsf{K}[x]$ alle Bedingungen von § 106 (Integritätsbereich mit Divisionsverfahren, oder auch: jedes Ideal Hauptideal) erfüllt, so ist der Hauptsatz von § 107 anwendbar[1]: der Modul $\mathfrak{M}$ ist direkte Summe von zyklischen $\mathsf{K}[x]$-Moduln $(w_1), \ldots, (w_\varkappa)$, deren annullierende Ideale entweder Null sind oder von je einem Polynom aus $\mathsf{K}[x]$ erzeugt werden. Der Fall des Nullideals ist aber ausgeschlossen. Denn für jedes $w = w_\nu$ können unter den Größen $w, xw, x^2w, \ldots$ höchstens n linear-unabhängige vorkommen; es gibt also ein Polynom $\sum \alpha_\nu x^\nu \neq 0$ mit der Eigenschaft

$$\sum \alpha_\nu x^\nu w = 0.$$

Jedes $w = w_\nu$ hat also ein annullierendes Polynom niedrigsten Grades

$$f_\nu(x) = f(x) = x^k + \alpha_{k-1}x^{k-1} + \cdots + \alpha_0,$$

und es ist

$$f_{\nu+1} \equiv 0 (f_\nu).$$

Die Größen $w, xw, \ldots, x^{k-1}w$ sind linear-unabhängig in bezug auf K und können daher als K-Basis für den zyklischen $\mathsf{K}[x]$-Modul $(w) = (w, xw, x^2w, \ldots)$ benutzt werden. Man hat:

$$\begin{aligned} A\,w &= x\,w, \\ A\,x\,w &= x^2\,w, \\ &\cdots\cdots\cdots \\ A\,x^{k-1}w = x^k w &= -\alpha_0 \cdot w - \alpha_1 \cdot x\,w - \cdots - \alpha_{k-1} \cdot x^{k-1} w. \end{aligned}$$

Mithin wird die Transformation A des Moduls $(w, xw, \ldots)$ in sich in den neuen Basiselementen durch die Matrix

$$A_\nu = \begin{pmatrix} 0 & \cdots & 0 & -\alpha_0 \\ 1 & \ddots & 0 & -\alpha_1 \\ 0 & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 1 & -\alpha_{k-1} \end{pmatrix} \tag{1}$$

dargestellt. Diese Matrizes nennt man *Begleitmatrizes*; zu jedem w_ν gehört eine Begleitmatrix A_ν von diesem Typ. Da $\mathfrak{M}$ die direkte Summe

[1] Das ergibt sich auch aus dem kurzen direkten Beweis am Schluß von § 107.

der (w_ν) ist, so erhält man für die Matrix A die *erste Normalform*:

$$A = \begin{pmatrix} A_1 & & & \\ & A_2 & & \\ & & \ddots & \\ & & & A_r \end{pmatrix}, \tag{2}$$

wo die Kästchen A_ν die Begleitmatrizes vom Typus (1) *sind.*

Aus dem Eindeutigkeitssatz von § 107 folgt, daß die Polynome $f_\nu(x)$, also auch die Begleitmatrizes A_ν, durch den Modul $\mathfrak{M}$ *eindeutig bestimmt* sind.

Die Kästchen A_ν kann man noch weiter „ausreduzieren", indem man die zyklischen Moduln (w_ν) als direkte Summen von solchen zyklischen Untermoduln darstellt, deren annullierende Polynome Potenzen von Primpolynomen sind. Die Gestalt (2) bleibt erhalten, nur gehören die Begleitmatrizes (1) jetzt zu Primpolynompotenzen $(p(x))^\varrho$. (*Zweite Normalform.*) Auch jetzt sind die Begleitmatrizes, bis auf ihre Reihenfolge in (2), eindeutig bestimmt. Die Polynome $(p(x))^\varrho$ heißen bisweilen *Elementarteiler* der Matrix A. Das Wort hat hier also eine andere Bedeutung als in § 106. Die Beziehung zwischen den beiden Begriffen wird sich in § 110 herausstellen.

Mit Hilfe von Kompositionsreihen der zyklischen Moduln (w_ν) kann man die eben aufgestellte Normalform noch weiter ausreduzieren. Wir wollen das hier nur für den Fall ausführen, daß die auftretenden Primpolynome $p(x)$ *linear* sind, was insbesondere für algebraisch-abgeschlossene Körper K stets der Fall ist. Es sei also

$$p(x) = x - \lambda,$$
$$f(x) = (x - \lambda)^\varrho.$$

Als Basiselemente benutzen wir

$$v_1 = (x - \lambda)^{\varrho-1} w,$$
$$v_2 = (x - \lambda)^{\varrho-2} w,$$
$$\cdots\cdots\cdots\cdots$$
$$v_\varrho = w;$$

es wird

$$(x - \lambda) v_1 = 0,$$
$$(x - \lambda) v_\mu = v_{\mu-1} \qquad (1 < \mu \leqq \varrho)$$

oder

$$\begin{cases} A v_1 = x v_1 = \lambda v_1, \\ A v_\mu = x v_\mu = \lambda v_\mu + v_{\mu-1}. \end{cases} \tag{3}$$

Mithin erhält das „Kästchen" A_1 die „ausreduzierte" Gestalt

$$A_1 = \begin{pmatrix} \lambda & 1 & 0 & \dots & 0 \\ 0 & \lambda & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 0 \\ \vdots & & \ddots & \ddots & 1 \\ 0 & \dots & \dots & 0 & \lambda \end{pmatrix},$$

und ebenso wird, da zu jedem w_ν ein λ_ν gehört,

$$A_\nu = \begin{pmatrix} \lambda_\nu & 1 & \dots & 0 \\ \ddots & \ddots & \ddots & \vdots \\ & \ddots & \ddots & 1 \\ 0 & & & \lambda_\nu \end{pmatrix}.$$

Diese Kästchen hat man wieder in (2) einzusetzen, um die *dritte Normalform* zu erhalten. Die *„charakteristischen Wurzeln"*[1] λ_ν und die Grade ϱ_ν der Kästchen sind wiederum *eindeutig bestimmt.*

Alle Vektoren v_μ, die zur selben Wurzel λ gehören, erzeugen einen Modul $\mathfrak{B}_\lambda$, der von einer Potenz von $x - \lambda$ annulliert wird (§ 107); dieser Modul heißt (in der Vektorsprache) der *zur Wurzel λ gehörige Teilraum.* Der ganze Modul $\mathfrak{M}$ ist die direkte Summe dieser Teilräume. In ihnen gibt es weiter die in § 107 erwähnte Reihe von Unterräumen, die von $(x - \lambda)^\varrho$, $(x - \lambda)^{\varrho-1}, \dots, 1$ annulliert werden. Die von $x - \lambda$ annullierten Vektoren w, für die also

$$A w = \lambda w$$

ist, heißen auch *Eigenvektoren* der Matrix A zum *Eigenwert* λ.

Der Typus der Matrix A wird bisweilen durch ein *Schema* folgender Art angegeben: Kommt eine charakteristische Wurzel, etwa λ_1, in verschiedenen Kästchen der Grade $\varrho, \sigma, \dots, \tau$ vor, so schreibt man $\varrho, \sigma, \dots, \tau$ in einer runden Klammer und vereinigt dann alle zu verschiedenen λ_ν gehörigen runden Klammern in einer eckigen Klammer. So bedeutet das Schema [(2 1) 1] den Typus

$$\begin{pmatrix} \boxed{\begin{matrix} \lambda_1 & 1 \\ 0 & \lambda_1 \end{matrix}} & & 0 \\ & \boxed{\lambda_1} & \\ 0 & & \boxed{\lambda_2} \end{pmatrix}.$$

[1] Der Name erklärt sich im nächsten Paragraphen.

Der *vollständig reduzible* Fall (vgl. § 108), in dem die Normalform (2) eine Diagonalform

$$\begin{pmatrix} \lambda_1 & & & 0 \\ & \lambda_2 & & \\ & & \ddots & \\ 0 & & & \lambda_n \end{pmatrix} \tag{4}$$

wird, tritt ein, wenn alle ϱ gleich 1 sind, d. h. wenn die Polynome $f_\nu(x)$, aus denen die $(\phi(x))^\varrho$ durch Primfaktorzerlegung gewonnen werden, frei von mehrfachen Faktoren sind. Wegen

$$f_{\nu+1} \equiv 0 (f_\nu)$$

reicht dazu hin, daß der höchste Elementarteiler $f_r(x)$ keine mehrfachen Faktoren hat.

Methoden zur wirklichen Bestimmung der charakteristischen Wurzeln und Herstellung der Normalformen findet man im nächsten Paragraphen.

Aufgaben. 1. Der höchste Elementarteiler $f_r(x)$ kann charakterisiert werden als das Polynom $f(x)$ niedrigsten Grades mit der Eigenschaft

$$f(x)\,\mathfrak{M} = 0 \quad \text{oder} \quad f(A) = 0.$$

2. Man bestimme für eine beliebige Matrix A in der zweiten oder dritten Normalform die Gesamtheit der mit A vertauschbaren Matrizes. [Vgl. § 108, Aufg. 4.]

§ 110. Elementarteiler und charakteristische Funktion.

Bei der Transformation

$$A' = P^{-1} A P$$

geht die Matrix $xE - A$ in

$$P^{-1}(xE - A)P = xP^{-1}EP - P^{-1}AP = xE - A'$$

über. Wir wollen die Elementarteiler der Matrix $xE - A$ in $\mathsf{K}[x]$ im Sinne von § 106 bestimmen. Da sie gegenüber vorderer und hinterer Multiplikation mit beliebigen invertierbaren Matrizes invariant sind, können wir sie auch für $xE - A'$ bestimmen, wo A' die erste Normalform aus § 109 ist. Nach (1), (2) § 109 besteht $xE - A'$ aus Kästchen von der Gestalt

$$xE_1 - A_1 = \begin{pmatrix} x & 0 & \dots & 0 & \beta_0 \\ -1 & x & & & \vdots \\ 0 & -1 & x & & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & \vdots \\ \vdots & & & x & \beta_{h-2} \\ 0 & \dots & 0 & -1 & x + \beta_{h-1} \end{pmatrix}$$

Zur Bestimmung der Elementarteiler haben wir diese Matrix auf Diagonalform zu bringen. Addiert man die mit $x, x^2, \ldots, x^{h-1}$ multiplizierte zweite bis h-te Zeile zur ersten, so kommt:

$$\begin{pmatrix} 0 & 0 & \ldots & 0 & f(x) \\ -1 & x & \ddots & & \beta_1 \\ 0 & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & x & \beta_{h-2} \\ 0 & \ldots & 0 & -1 & x+\beta_{h-1} \end{pmatrix}.$$

Bringt man nun durch Vertauschung von Zeilen die erste ganz herunter, so stehen unter der Hauptdiagonale lauter Nullen. Es ist sehr leicht, durch Addition von Vielfachen früherstehender Spalten zu späteren alles, was oberhalb der Hauptdiagonale steht, zum Verschwinden zu bringen. Es bleibt also

$$\begin{pmatrix} -1 & & & 0 \\ & -1 & & \\ & & \ddots & \\ & & & -1 \\ 0 & & & f(x) \end{pmatrix}.$$

Reiht man nun alle diese Kästchen aneinander und vertauscht noch Zeilen und Spalten, bis alle -1 in der Hauptdiagonale zuerst kommen, so erhält man die gesuchte Diagonalform

$$\begin{pmatrix} -1 & & & & 0 \\ & -1 & & & \\ & & \ddots & & \\ & & & -1 & \\ & & & & f_1(x) \\ & & & & & \ddots \\ 0 & & & & & & f_r(x) \end{pmatrix}.$$

Mithin sind die Polynome $f_\nu(x)$ (zusammen mit einigen Einsen) die Elementarteiler von $xE - A$. Die Primpolynompotenzen, in die sie zerfallen, sind die Elementarteiler der Matrix A im Sinne von § 109.

Das *charakteristische Polynom* (die *charakteristische Funktion*) *von A*

$$\chi(x) = \prod_1^r f_\nu(x)$$

annulliert den Modul $\mathfrak{M}$, weil schon der Faktor $f_r(x)$ es tut; man hat somit

$$\chi(A) = 0. \tag{1}$$

Das charakteristische Polynom ist der höchste Determinantenteiler

von $xE - A$, also bis auf eine Konstante gleich der Determinante $|xE - A|$. Die Konstante ergibt sich sofort gleich Eins; mithin ist

$$\chi(x) = |xE - A|. \tag{2}$$

Die *charakteristische Gleichung* (1) für die Matrix A läßt sich auch direkt rechnerisch aus (2) ableiten. Es ist nämlich

$$x u_k = \sum u_i \alpha_{ik},$$

und die Elimination aller u aus diesem Gleichungssystem ergibt (da x und seine Potenzen mit den α_{ik} vertauschbar sind):

$$\begin{vmatrix} x - \alpha_{11} & -\alpha_{12} & \cdots & -\alpha_{1n} \\ \vdots & \ddots & & \vdots \\ -\alpha_{n1} & -\alpha_{n2} & \cdots & x - \alpha_{nn} \end{vmatrix} \cdot u_j = 0$$

oder

$$|xE - A|\, u_j = 0;$$

d. h. $\chi(x) = |xE - A|$ annulliert alle u_j, also den ganzen Modul $\mathfrak{M}$, q. e. d.

Die Koeffizienten der charakteristischen Funktion $\chi(x)$ von A sind nach dem Vorigen Invarianten bei der Transformation $A \to P^{-1}AP$. Die wichtigsten sind der erste und der letzte:

die *Spur* von A: der Koeffizient von $-x^{n-1}$:

$$Sp(A) = \sum \alpha_{ii};$$

die *Norm* von A: der Koeffizient von $(-1)^n x^0$:

$$N(A) = |A|.$$

Die Wurzeln der charakteristischen Funktion sind die *charakteristischen Wurzeln* λ_ν, die im vorigen Paragraphen schon [als Wurzeln der Polynome $f_\nu(x)$] eingeführt wurden. Das liefert zugleich ein brauchbares Mittel zur Bestimmung dieser λ_ν und zur Herstellung der Normalformen des vorigen Paragraphen: Man bestimme zunächst die λ_ν als Wurzeln von

$$\chi(x) = |xE - A|,$$

sodann die v_1 aus den linearen Gleichungen [vgl. (3) § 109]

$$A v_1 = \lambda_\nu v_1.$$

Im Fall der mehrfachen Wurzeln ($\varrho > 1$) sind die weiteren $v_2, \ldots, v_\varrho$ aus (3) § 109 meist leicht zu finden; eventuell hat man dabei die zum selben λ_ν gehörigen v_1 noch durch passende Linearkombinationen zu ersetzen.

Die Gleichung $\chi(\lambda) = 0$, deren Wurzeln die λ_ν sind, tritt in vielen Anwendungen immer wieder auf und wird wegen ihres Auftretens in der Theorie der säkularen Störungen auch *Säkulargleichung* genannt.

Aufgaben. 1. Man bestimme die Normalformen der Matrizes

$$\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix},\quad \begin{pmatrix}1 & 1 & 1\\ 0 & 1 & 1\\ 0 & 0 & 1\end{pmatrix},\quad \begin{pmatrix}0 & 1 & 1\\ 0 & 0 & 1\\ 0 & 0 & 1\end{pmatrix},\quad \begin{pmatrix}0 & 0 & 1\\ 0 & 0 & 1\\ 0 & 0 & 1\end{pmatrix},\quad \begin{pmatrix}1 & 1 & 0\\ 0 & 1 & 0\\ 0 & 1 & 1\end{pmatrix}.$$

2. Man gebe eine Klassifikation der projektiven Abbildungen einer projektiven Ebene auf sich:

$$\begin{pmatrix}\xi_1'\\ \xi_2'\\ \xi_3'\end{pmatrix} = A\begin{pmatrix}\xi_1\\ \xi_2\\ \xi_3\end{pmatrix},$$

und bestimme die Lage der invarianten Punkte und Geraden dieser Abbildungen.

§ 111. Quadratische und Hermitesche Formen.

Es sei K ein kommutativer Körper der Charakteristik $\neq 2$. Um die Werte, welche eine quadratische Form

$$f(x_1, \ldots, x_n) = \sum_i \sum_k \beta_{ik} x_i x_k \qquad (\beta_{ik} = \beta_{ki})$$

annimmt, für spezielle Werte $x_i = c_i$ aus K zu studieren, fassen wir die $c_1, \ldots, c_n$ als Komponenten eines Vektors u auf und setzen

$$f(u, u) = f(c_1, \ldots, c_n) = \sum\sum \beta_{ik} c_i c_k .$$

Wir bilden, wenn $v = (d_1, \ldots, d_n)$ ein zweiter Vektor ist, den Ausdruck

$$\begin{aligned} f(u + \lambda v, u + \lambda v) &= \sum\sum \beta_{ik} c_i c_k + 2\lambda \sum\sum \beta_{ik} c_i d_k + \lambda^2 \sum\sum \beta_{ik} d_i d_k \\ &= f(u, u) + 2\lambda f(u, v) + \lambda^2 f(v, v), \end{aligned}$$

wobei also

$$f(u, v) = \sum\sum \beta_{ik} c_i d_k$$

gesetzt ist. Die Bilinearform $f(u, v)$ ist offenbar invariant (d. h. unabhängig von der Wahl der Basisvektoren) mit der Form $f(u, u)$ verbunden und heißt die *Polarform* von $f(u, u)$.

Bezieht man die Vektoren u des Raumes R_n auf eine neue Basis $(u_1', \ldots, u_n')$, wo die u_i' mit den alten Basisvektoren $u_1, \ldots, u_n$ durch die lineare Transformation P verbunden sind:

$$u_j' = \sum u_i \pi_{ij},$$

so werden, wie wir wissen, die Komponenten c_i eines Vektors transformiert nach der Regel

$$c_i = \sum \pi_{ij} c_j',$$

und die quadratische Form f wird daher übergeführt in

$$f = \sum\sum \beta_{ik} c_i c_k = \sum\sum\sum\sum \beta_{ik} \pi_{ij} \pi_{kl} c_j' c_l'$$

mit Koeffizienten

$$\beta_{jl}' = \sum\sum \beta_{ik} \pi_{ij} \pi_{kl} .$$

Diese Gleichung kann in Matrixform geschrieben werden, wenn man die Matrizes $A = (\beta_{ik})$ und $A' = (\beta'_{ik})$ einführt und außerdem zu der Matrix $P = (\pi_{ik})$ die gespiegelte Matrix $\tilde{P}$ bildet. Dann wird

$$A' = \tilde{P} A P. \tag{1}$$

Wie man sieht, wird die Koeffizientenmatrix einer quadratischen Form ganz anders transformiert als die Matrix einer linearen Transformation, deren Ausdruck auf einer neuen Basis ja durch $A' = P^{-1} A P$ gegeben wird.

Um eine gegebene quadratische Form f durch Transformation auf eine möglichst einfache Gestalt zu bringen, wählen wir einen Vektor v_1 so, daß $f(v_1, v_1) \neq 0$ ist, was immer geht, wenn f nicht identisch Null ist. Dann bestimmt die Gleichung $f(v_1, u) = 0$ einen Unterraum R_{n-1} des Vektorraums R_n, der v_1 nicht enthält. Wählen wir nun in diesem Unterraum, wenn möglich, einen Vektor v_2, so daß $f(v_2, v_2) \neq 0$ ist, so bestimmt die Gleichung $f(v_2, u) = 0$ zusammen mit der vorigen einen Unterraum R_{n-2} in R_{n-1}, der v_2 nicht enthält. So fährt man fort, bis man zu einem Unterraum R_{n-r} gelangt, so daß $f(u, u) = 0$ für alle u in R_{n-r} und daher[1] auch $f(u, v) = 0$ für u und v in R_{n-r}. Eventuell ist $r = n$; dann ist R_{n-r} der Nullraum. Andernfalls wählen wir in R_{n-r} beliebig die Basisvektoren $v_{r+1}, \ldots, v_n$. Dann ist

$$\begin{cases} f(v_i, v_k) = 0 & (i \neq k), \\ f(v_i, v_i) = \gamma_i \neq 0 & (i = 1, \ldots, r), \\ f(v_i, v_i) = 0 & (i = r+1, \ldots, n). \end{cases}$$

Bezieht man jeden Vektor v auf die neuen Basisvektoren $v_1, \ldots, v_n$:

$$v = \sum d_i v_i,$$

so wird

$$f(v, v) = \sum\sum d_i d_k f(v_i, v_k) = \sum_1^r d_i^2 \gamma_i. \tag{2}$$

Die Form f ist also, wie man sagt, *auf eine Summe von Quadraten transformiert.*

Die Vektoren w von R_{n-r} haben die Eigenschaft

$$f(w, u) = 0 \quad \text{für jedes } u$$

und sind dadurch gekennzeichnet. Der Raum R_{n-r} und dessen Dimension $n - r$ sind also invariant mit der Form f verbunden. Die Anzahl r der Quadrate in (2) ist also auch invariant: sie heißt der *Rang* der Form f.

Wir nehmen nun an, der Körper K sei angeordnet (§ 63). Die Anzahl der negativen γ_i in (2) möge der *Trägheitsindex* von f heißen. Wir zeigen, daß auch dieser Trägheitsindex invariant ist (*Trägheitsgesetz von* SYLVESTER).

[1] An dieser Stelle wird die Voraussetzung: Charakteristik $\neq 2$ benutzt.

Gesetzt, dieselbe Form f habe, auf andere Basisvektoren v_i' bezogen, die Darstellung

$$f = \sum_1^r d_i'^2 \gamma_i';$$

es seien etwa $\gamma_1, \ldots, \gamma_h$ positiv, $\gamma_{h+1}, \ldots, \gamma_r$ negativ; ebenso $\gamma_1', \ldots, \gamma_k'$ positiv und $\gamma_{k+1}', \ldots, \gamma_r'$ negativ. Wäre nun etwa $k > h$, so würden die linearen Gleichungen

$$d_1 = 0, \ldots, d_h = 0, \qquad d_{k+1}' = 0, \ldots, d_r' = 0$$

einen Raum von mehr als $n - r$ Dimensionen definieren. Für einen Vektor u dieses Raumes wäre $f(u, u) = \sum_{h+1}^r d_i^2 \gamma_i \leqq 0$, andererseits $f(u, u) = \sum_1^k d_i'^2 \gamma_i' \geqq 0$, mithin $f(u, u) = 0$ und alle d_i und $d_i' = 0$, mithin läge u in R_{n-r}. Also wäre ein Raum von mehr als $n - r$ Dimensionen in einem von $n - r$ Dimensionen enthalten, was nicht geht.

Sind alle γ_i in (2) positiv, so heißt die Form f im Fall $r = n$ *positiv-definit*, im allgemeinen Fall *semidefinit*. Die positiv-definiten Formen sind dadurch gekennzeichnet, daß sie für jeden Vektor $u \neq 0$ einen positiven Wert annehmen; die semidefiniten dadurch, daß ihr Wert stets $\geqq 0$ ist.

Eine positiv-definite Form läßt sich, wie aus (2) unmittelbar folgt, nach Adjunktion der Größen $\sqrt{\gamma_i}$ zum Körper K in die *„Einheitsform"*

$$E(u, u) = \sum d_i^2$$

transformieren.

Zu den quadratischen Formen analog sind die *Hermiteschen Formen.* Um zu diesen zu kommen, adjungieren wir zum angeordneten Körper K eine Quadratwurzel θ aus einer negativen Größe α von K, zum Beispiel $\theta = \sqrt{-1}$. Wir werden gelegentlich die Größen aus K, zum Unterschied von denen aus $\mathsf{K}(\theta)$, „reell" nennen, weil bei den Anwendungen meist K der Körper der reellen Zahlen und $\theta = \sqrt{-1}$ ist.

Zu jeder Größe $c = a + b\theta$ ist konjugiert $\bar{c} = a - b\theta$. Das Produkt $\bar{c}c = a^2 - b^2\theta^2$ ist stets reell und $\geqq 0$, mit dem Gleichheitszeichen nur für $c = 0$.

Unter einer *Hermiteschen Form* verstehen wir nun den Ausdruck

$$H(u, u) = \sum\sum h_{ik} \bar{c}_i c_k \qquad (h_{ik} = \bar{h}_{ki}).$$

Der Wert der Form H für einen beliebigen Vektor u ist stets reell.

Bilden wir, wie zu Anfang dieses Paragraphen,

$$H(u + \lambda v, u + \lambda v) = \sum\sum h_{ik} \bar{c}_i c_k + \lambda \sum\sum h_{ik} \bar{c}_i d_k + \bar{\lambda} \sum\sum h_{ik} \bar{d}_i c_k + \lambda \bar{\lambda} \sum\sum h_{ik} \bar{d}_i d_k,$$

so finden wir als Koeffizienten von λ die *Polarform*

$$H(u, v) = \sum\sum h_{ik}\bar{c}_i d_k .$$

Es ist

$$H(v, u) = \overline{H(u, v)} .$$

Die Transformationsformel (1) gilt auch für Hermitesche Formen, wenn man unter $\tilde{P}$ die gespiegelte konjugierte Matrix ($\tilde{\pi}_{ij} = \bar{\pi}_{ji}$) versteht. Auch die früheren Betrachtungen über die Darstellung der quadratischen Formen als Quadratsummen gelten ungeändert für Hermitesche Formen. Man findet als Normalform

$$H(u, u) = \sum_1^r \bar{c}_i c_i \gamma_i \qquad (\gamma_i \text{ reell}). \tag{3}$$

Die Form H heißt wieder *positiv-definit*, wenn ihre Werte $H(u, u)$ stets positiv sind außer für $u = 0$, oder wenn $r = n$ ist und $\gamma_1, \ldots, \gamma_n$ alle positiv sind. Nach Adjunktion der Quadratwurzeln aus diesen γ_i läßt sich jede positiv-definite Form in die *Einheitsform*

$$E(u, u) = \sum \bar{c}_i c_i$$

transformieren.

Die nun folgenden Erörterungen gelten gleichmäßig für Hermitesche und quadratische Formen. Wir werden sie für Hermitesche Formen aussprechen; man braucht dann nur alle vorkommenden Größen in K zu wählen und alle Querstriche wegzulassen, um die entsprechenden Sätze über quadratische Formen zu erhalten.

Wir wählen eine bestimmte, vorzugsweise positiv-definite Hermitesche Form $G(u, u)$ vom Rang n als *Grundform* und bezeichnen ihre Koeffizientenmatrix (g_{ik}) mit G. Ist speziell $G(u, u)$ die Einheitsform, so ist G die Einheitsmatrix E. Zwei Vektoren u, v heißen *senkrecht*, wenn $G(u, v) = 0$ ist. Dann ist auch $G(v, u) = 0$. Die zu einem Vektor $u \neq 0$ senkrechten Vektoren v bilden einen linearen Unterraum: *den zu u senkrechten Raum.* Ist G positiv-definit, so ist stets $G(u, u) \neq 0$, mithin gehört u selbst nicht zum senkrechten Raum R_{n-1}. Ein System von n untereinander senkrechten Basisvektoren $v_1, \ldots, v_n$, wie es bei der Herstellung der Normalform (3) für $G(u, u)$ benutzt wurde, heißt ein *vollständiges Orthogonalsystem* von Vektoren. Das Orthogonalsystem heißt *normiert*, wenn $G(v_j, v_j) = 1$ ist.

Diejenigen linearen Transformationen A, welche die Eigenschaft

$$G(Au, v) = G(u, Av) \qquad \text{(für alle } u \text{ und } v)$$

besitzen, heißen *Hermitesch symmetrisch* oder einfach *symmetrisch.* Die Bedingung dafür lautet, ausgeschrieben:

$$\sum\sum\sum g_{il}\bar{a}_{ij}\bar{c}_j c_l = \sum\sum\sum g_{jk}\bar{c}_j a_{kl} c_l$$

oder

$$\sum_i g_{il}\bar{a}_{ij} = \sum_k g_{jk}a_{kl}$$

oder

$$\tilde{A}G = GA.$$

Ist speziell G die Einheitsform, so lautet die Symmetriebedingung einfach

$$\tilde{A} = A \quad \text{oder} \quad \bar{a}_{ik} = a_{ki},$$

was die Bezeichnung „symmetrisch" erklärt.

Diejenigen linearen Transformationen U, welche die Grundform $G(u, u)$ invariant lassen:

$$G(Au, Au) = G(u, u) \quad \text{oder} \quad \tilde{A}GA = G,$$

heißen *unitär* oder im reellen Fall *orthogonal*. Offenbar ist dann auch $G(Au, Av) = G(u, v)$. Ist speziell $G = E$, was man ja im positiv-definiten Fall immer annehmen kann, so lautet die Bedingung:

$$\tilde{A}A = E \quad \text{oder} \quad \tilde{A} = A^{-1} \quad \text{oder} \quad A\tilde{A} = E.$$

Ausgeschrieben, erhält man die „Orthogonalitätsbedingungen"

$$\sum \bar{a}_{ik}a_{il} = \delta_{kl} = \begin{cases} 0 & \text{für } k \neq l \\ 1 & \text{für } k = l \end{cases}$$

oder die damit gleichwertigen

$$\sum a_{ik}\bar{a}_{jk} = \delta_{ij}.$$

Eine reelle orthogonale Transformation heißt eine *Drehung*.

Wenn eine symmetrische oder unitäre Transformation A einen von Null verschiedenen Vektor u in ein Vielfaches von sich selbst transformiert:

$$Au = \lambda u, \tag{4}$$

d. h. wenn A den durch u erzeugten Strahl invariant läßt, so läßt A auch den zu u senkrechten R_{n-1} invariant.

Beweis: Wenn v zu R_{n-1} gehört, also $G(u, v) = 0$ ist, so ist für symmetrische A:

$$G(u, Av) = G(Au, v) = G(\lambda u, v) = \lambda G(u, v) = 0$$

und für unitäre A:

$$G(u, Av) = G(AA^{-1}u, Av) = G(A^{-1}u, v) = G(\lambda^{-1}u, v) = \lambda^{-1}G(u, v) = 0.$$

Ein Vektor $u \neq 0$ mit der Eigenschaft (4) heißt ein *Eigenvektor* der Transformation A; λ heißt der zugehörige *Eigenwert*.

Wie wir schon im § 110 sahen, werden die Eigenwerte aus der *„Säkulargleichung"*

$$\chi(\lambda) = \begin{vmatrix} \lambda - \alpha_{11} & -\alpha_{12} & \cdots \\ -\alpha_{21} & \lambda - \alpha_{22} & \cdots \\ \cdots & \cdots & \cdots \end{vmatrix} = 0 \tag{5}$$

und die zugehörigen Eigenvektoren aus den mit (4) gleichbedeutenden linearen Gleichungen

$$\sum \alpha_{ik} c_k = \lambda c_i \tag{6}$$

gefunden.

Setzen wir nun voraus, daß der Körper K reell-abgeschlossen (etwa der Körper der reellen Zahlen) und daher $\mathsf{K}(\theta)$ algebraisch-abgeschlossen ist (vgl. § 67), so hat die Säkulargleichung (5) immer eine Wurzel λ_1 in $\mathsf{K}(\theta)$, zu der auch ein Eigenvektor e_1 gehört. Der zu e_1 senkrechte R_{n-1} wird durch A in sich transformiert, und A ist in R_{n-1} wieder symmetrisch oder unitär, wenn A in R_n symmetrisch oder unitär war. Mithin gibt es nach demselben Schluß in R_{n-1} wieder einen Eigenvektor e_2, dessen senkrechter Raum R_{n-2} innerhalb R_{n-1} wieder invariant ist, usw. *So findet man schließlich ein vollständiges System von n linear-unabhängigen untereinander senkrechten Eigenvektoren* $e_1, \ldots, e_n$:

$$A e_\nu = \lambda_\nu e_\nu .$$

Die Matrix A erhält, auf die neue Basis $(e_1, \ldots, e_n)$ bezogen, die Diagonalform:

$$A_1 = P^{-1} A P = \begin{pmatrix} \lambda_1 & & & 0 \\ & \lambda_2 & & \\ & & \ddots & \\ 0 & & & \lambda_n \end{pmatrix}. \tag{7}$$

Normieren wir die e_ν durch die Bedingung $G(e_\nu, e_\nu) = 1$, was bei reell-abgeschlossenem K immer möglich ist, da die Quadratwurzel aus der positiven Größe $G(e_\nu, e_\nu)$ stets in K vorhanden ist, so wird G, auf die e_ν als Basis bezogen, gleich der Einheitsform E. Ist nun die Matrix A symmetrisch, so muß A_1 auch symmetrisch sein, mithin mit $\tilde{A}_1$ identisch, und daraus folgt

$$\lambda_\nu = \bar{\lambda}_\nu \quad \text{oder} \quad \lambda_\nu \in \mathsf{K}.$$

Das charakteristische Polynom der Matrix A oder A_1 ist

$$\chi(x) = \prod_1^n (x - \lambda_n),$$

mithin: *Die Säkulargleichung* $\chi(\lambda) = 0$ *einer symmetrischen Matrix A hat lauter reelle Wurzeln.*

Sind außerdem die Matrizes A und G reell, so sind auch die Eigenvektoren e_ν, als Lösungen der reellen Gleichungen (6), reell, *mithin läßt sich eine reelle symmetrische Matrix A in reeller Weise in die Diagonalform* (7) *transformieren.*

Wir sind bei unserem Beweis dieses Satzes von der Existenz der Wurzeln λ_ν in $\mathsf{K}(\theta)$ ausgegangen und haben erst hinterher bewiesen, daß die λ_ν reell sein müssen. Man kann den Satz im Fall des Körpers der

reellen Zahlen auch im Reellen beweisen; vgl. etwa R. COURANT und D. HILBERT, Methoden der mathematischen Physik, Band I, § 3, 1924.

Mit der symmetrischen Transformation A ist eine Hermitesche Form

$$H(u, u) = G(u, Au) = G(Au, u)$$

invariant verknüpft, deren Matrix offenbar

$$H = GA$$

lautet, und durch die die Matrix A auch umgekehrt bestimmt wird:

$$A = G^{-1}H.$$

Mit der Diagonaltransformation von A und G ist zugleich auch die von $H = GA$ geleistet; die transformierte Form lautet

$$H(u, u) = \sum \bar{c}_\nu c_\nu \lambda_\nu.$$

Damit ist bewiesen:

Jedes Paar von Hermiteschen Formen G, H, von denen eine, etwa G, positiv-definit ist, läßt sich gleichzeitig durch eine einzige Transformation auf die Gestalt

$$\begin{cases} G(u, u) = \sum \bar{c}_\nu c_\nu \\ H(u, u) = \sum \bar{c}_\nu c_\nu \lambda_\nu \end{cases}$$

bringen. Die λ_i sind die charakteristischen Wurzeln der Matrix $A = G^{-1}H$ oder, was dasselbe ist, die Wurzeln der Säkulargleichung

$$|\lambda g_{jk} - h_{jk}| = 0.$$

Insbesondere: *Jedes Paar von reellen quadratischen Formen, von denen die eine positiv-definit ist, läßt sich in reeller Weise gleichzeitig auf Quadratsummen transformieren:*

$$G(u, u) = \sum c_\nu^2,$$
$$H(u, u) = \sum c_\nu^2 \lambda_\nu.$$

Für eine allgemeine Behandlung der Klassifikation der Paare quadratischer Formen siehe DICKSON, L. E.: Modern algebraic Theories, Chicago 1926 (auch deutsch von E. BODEWIG, Leipzig 1929).

Aufgaben. 1. Wenn r Vektoren $v_1, \ldots, v_r$ einen R_r erzeugen, so bilden die zu ihnen senkrechten Vektoren uəuıə R_{n-r}, und der ganze Raum R_n ist die direkte Summe $R_r + R_{n-r}$.

2. Wenn eine symmetrische oder unitäre Transformation A den Raum R_r invariant läßt, so läßt sie auch den dazu senkrechten R_{n-r} invariant.

3. Jedes System von symmetrischen oder unitären Transformationen ist vollständig reduzibel.

4. Die Determinante D einer unitären Transformation hat den Betrag 1, d. h. es ist $D\bar{D} = 1$. Die Determinante einer reellen orthogonalen Transformation ist ± 1.

5. Die unitären und ebenso die reellen orthogonalen Transformationen eines Vektorraumes in sich bilden je eine Gruppe.

Sechzehntes Kapitel.

Theorie der hyperkomplexen Größen.

§ 112. Systeme hyperkomplexer Größen.

Unter einem *hyperkomplexen System* (oder, wie man neuerdings auch sagt, einer *Algebra*) über dem kommutativen Körper P verstehen wir nach § 10 einen Ring, der zugleich endlicher Linearformenmodul in bezug auf P ist:

$$\mathfrak{o} = b_1\mathsf{P} + \cdots + b_n\mathsf{P},$$

und dessen Elemente mit den Elementen von P vertauschbar sind. Die Elemente von $\mathfrak{o}$ haben also die Gestalt

$$a = b_1\lambda_1 + \cdots + b_n\lambda_n = \lambda_1 b_1 + \cdots + \lambda_n b_n. \qquad (\lambda_i \in \mathsf{P})$$

Sind die b_i linear-unabhängig in bezug auf P, so ist die Zahl n der *Rang* des Systems. Durch Angabe der Basiselemente und ihrer Multiplikationstafel ist bei gegebenem P das hyperkomplexe System $\mathfrak{o}$ völlig bestimmt. Wenn über die Wahl von P kein Zweifel besteht, kann man daher kurz $\mathfrak{o} = (b_1, \ldots, b_n)$ schreiben. Die Multiplikationstafel ist der einzigen Bedingung unterworfen, daß für die Basiselemente das Assoziativgesetz gelten soll:

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

Beispiele von hyperkomplexen Systemen sind:

a) Der *volle Matrizenring* über P, vom Rang n^2, dessen Basiselemente c_{ik} (vgl. § 104, Aufg. 4) den Rechnungsregeln

$$c_{ij}c_{jl} = c_{il},$$
$$c_{ij}c_{kl} = 0 \quad \text{für} \quad j \neq k$$

genügen.

b) Der *Gruppenring* einer endlichen Gruppe $\mathfrak{G}$, der dadurch definiert ist, daß seine Basiselemente eben die Elemente von $\mathfrak{G}$ sind (vgl. § 10, Aufg. 13). Der Rang ist gleich der Gruppenordnung.

c) Alle endlichen Erweiterungskörper von P, die P im Zentrum enthalten. Der Rang ist der Körpergrad. Zum Beispiel fallen darunter die im 5. Kapitel untersuchten endlichen kommutativen Erweiterungskörper.

d) Der Quaternionenring $\mathfrak{o} = (1, j, k, l)$ vom Rang 4. der durch die folgenden Rechnungsregeln definiert wird:

$$j^2 = k^2 = l^2 = -1,$$
$$jk = -kj = l,$$
$$kl = -lk = j,$$
$$lj = -jl = k.$$

(Vgl. § 10, Aufg. 12.)

e) Der Restklassenring nach einem nulldimensionalen Ideal $\mathfrak{a}$ in einem Polynombereich $\mathsf{P}[x_1, \ldots, x_n]$ (oder allgemeiner in einer Ordnung eines Funktionenkörpers) ist ein (kommutatives) hyperkomplexes System über P. Der Rang heißt der *Grad* des Ideals $\mathfrak{a}$.

f) Der Restklassenring nach einer rationalen Primzahl p in einer Ordnung eines Zahlkörpers ist ein kommutatives hyperkomplexes System über $\mathsf{P} = C/(p)$, wobei C wie immer den Ring der ganzen rationalen Zahlen bedeutet. Der Rang ist gleich dem Grad des Zahlkörpers.

Aufgaben. 1. Ein hyperkomplexes System ohne Nullteiler ist ein Körper. [Man vergleiche für $a \neq 0$ den Rang des Systems $a\mathfrak{o}$ mit dem des ganzen Systems $\mathfrak{o}$.]

2. Wenn es in einem hyperkomplexen System $\mathfrak{o}$ einen Nichtnullteiler a gibt, so sind die Gleichungen $xa = b$ und $ax = b$ lösbar; es gibt dann ein Einselement, und jeder Nichtnullteiler besitzt in $\mathfrak{o}$ ein Inverses.

3. Der Quaternionenring ist dann und nur dann nullteilerfrei (also ein Körper), wenn der Grundkörper P die Eigenschaft hat, daß eine Summe von 4 Quadraten in ihm nur dann verschwindet, wenn alle 4 Glieder verschwinden. [Man benutze die bei Aufg. 12, § 10 angeführte Identität.]

4. Ein algebraisch-abgeschlossener Körper besitzt keine hyperkomplexe echte Erweiterung ohne Nullteiler.

5. Ist P ein (kommutativer) Körper, dessen Charakteristik von 2 verschieden ist, so gibt es nur die folgenden drei Typen von hyperkomplexen Systemen vom Range 2 mit Einselement (alle kommutativ; warum?):

a) $(1, c)$, wo c^2 in P liegt und dort kein Quadrat ist. Das System ist ein kommutativer Körper über P.

b) $(1, c)$, wo c^2 das Quadrat eines von Null verschiedenen Elementes γ von P ist. Das System ist die direkte Summe zweier Körper $(c - \gamma)\,\mathsf{P} = \mathsf{P}_1$ und $(c + \gamma)\,\mathsf{P} = \mathsf{P}_2$, die beide isomorph zu P sind und sich gegenseitig annullieren: $\mathsf{P}_1\mathsf{P}_2 = (0)$.

c) $(1, c)$, wo $c^2 = 0$ ist („*System der dualen Zahlen*").

6. Der Restklassenring eines hyperkomplexen Systems mit Einselement nach einem zweiseitigen Ideal ist wieder ein hyperkomplexes System zum selben Grundkörper („difference algebra").

§ 113. Hyperkomplexe Systeme als Gruppen mit Operatoren. Verallgemeinerungen.

Ein hyperkomplexes System $\mathfrak{o}$, als Abelsche Gruppe gegenüber der Addition betrachtet, gestattet zweierlei Operatorenbereiche:

Erstens den Körper P. Bei diesem Operatorenbereich sind zulässige Untergruppen alle *linearen Scharen*, d. h. Untermengen von $\mathfrak{o}$, die mit a (bei jedem λ aus P) auch λa, mit a und b auch $a - b$ enthalten. Jede lineare Schar hat einen Rang $\leqq n$, wo n der Rang von $\mathfrak{o}$ selbst ist (§ 28).

Zweitens das System $\mathfrak{o}$ selbst, dessen Elemente man je nach Belieben als Links- oder Rechtsoperatoren auffassen kann. Zulässige Untergruppen sind dabei die *Linksideale, Rechtsideale* und *zweiseitigen Ideale.*

Wir verabreden nun ein für allemal, bei der Betrachtung von (Links-, Rechts- oder zweiseitigen) Idealen in hyperkomplexen Systemen stets den Körper P als Operatorenbereich mit in Betracht zu ziehen. Das heißt: als *zulässige Linksideale* werden nur diejenigen Untergruppen betrachtet, die neben a nicht nur jedes ra (r in $\mathfrak{o}$), sondern auch jedes λa (λ in P) enthalten, und entsprechend für Rechtsideale. Zulässige Ideale sind also immer zugleich lineare Scharen. Ebenso: als *operatorisomorph* gelten zwei Linksideale nur dann, wenn eine Isomorphie existiert, die, wenn sie a in $\bar{a}$ überführt, auch jedes ra in $r\bar{a}$ und jedes λa in $\lambda\bar{a}$ überführt[1]. Ebenso: ein Linksideal heißt *einfach* oder *minimal*, wenn es keine zulässigen Linksideale außer sich selbst und dem Nullideal umfaßt.

Mit dieser Einschränkung des Idealbegriffs ist für die Ideale eines hyperkomplexen Systems die *„Maximal- und Minimalbedingung"* erfüllt:

Jede nicht leere Menge von (Rechts-, Links- oder zweiseitigen) Idealen enthält (mindestens) ein maximales Ideal, d. h. ein solches, das von keinem anderen Ideal der Menge umfaßt wird, und ein minimales, das kein anderes Ideal der Menge umfaßt.

Denn nach der Verabredung ist jedes Ideal zugleich eine lineare Schar, und in jeder nicht leeren Menge von linearen Scharen vom Range $\leqq n$ gibt es eine Schar größten und eine kleinsten Ranges.

Um die Hauptsätze der hyperkomplexen Algebra unter möglichst allgemeinen Voraussetzungen zu entwickeln, werden wir im Verlauf dieses Kapitels gar nicht mehr von hyperkomplexen Systemen reden, sondern von irgend einem Ring $\mathfrak{o}$ ausgehen, der nur die eben formulierte Maximal- und Minimalbedingung, etwa für Linksideale, erfüllen soll. Gelegentlich werden wir sogar nur die Maximal- oder nur die Minimalbedingung voraussetzen[2]. Zum Ring $\mathfrak{o}$ kann eventuell (aber nicht notwendig) noch ein Operatorenbereich Ω gegeben sein (der die Rolle des früheren P übernimmt), dessen Operatoren $\lambda, \mu, \ldots$ die Eigenschaften

$$\lambda(a+b) = \lambda a + \lambda b,$$
$$\lambda(ab) = (\lambda a)b = a(\lambda b)$$

haben sollen. Ist ein solcher Operatorenbereich vorhanden, so wird der Idealbegriff wie oben eingeschränkt durch die Forderung, daß jedes

[1] Man beachte den Unterschied zur Ringisomorphie, wobei ra nicht in $r\bar{a}$, sondern in $\bar{r}\bar{a}$ übergeführt wird, wenn r und a beide dem betrachteten Unterring angehören.

[2] Die Maximalbedingung ist nach § 80 gleichwertig mit dem Teilerkettensatz.

Ideal neben a auch $\lambda a\,(\lambda \text{ in } \Omega)$ enthalten soll. Wenn wir das ausdrücklich hervorheben wollen, so reden wir von *zulässigen* Rechts- bzw. Linksidealen. Nur für sie wird die Maximal- bzw. Minimalbedingung gestellt.

Durch die Heranziehung beliebiger Ringe, welche nur die Maximal- und Minimalbedingung erfüllen, ist tatsächlich das Feld der Untersuchung sehr erweitert; denn es gibt vielerlei Ringe, welche diesen Bedingungen genügen, ohne hyperkomplexe Systeme zu sein. Zum Beispiel erfüllen alle endlichen Ringe (insbesondere die Restklassenringe nach den vom Nullideal verschiedenen Idealen einer Ordnung in einem Zahlkörper und noch spezieller die Restklassenringe nach einer ganzen Zahl im Ring C) offenbar die Maximal- und Minimalbedingung. Welche kommutativen Ringe sonst dieser Bedingung genügen, darüber siehe die nachstehenden Aufgaben **3**, **4** und **5**. Indessen bleiben die hyperkomplexen Systeme doch das Hauptziel der Untersuchung.

Es sei noch erwähnt, daß die Minimalbedingung viel einschränkender ist als die Maximalbedingung. In der Tat sahen wir im § 80 schon, daß es ausgedehnte Klassen von Ringen mit Nullteilern und ohne Nullteiler gibt, für welche die Maximalbedingung gilt (die meisten interessanten Ringe fallen darunter), während die Minimalbedingung z. B. für Ringe ohne Nullteiler, wie wir nachher sehen werden, nur dann gilt, wenn sie Körper sind.

Es muß untersucht werden, welche von den idealtheoretischen Begriffsbildungen: Summe, Produkt usw., für nichtkommutative Ringe mit Operatorenbereichen oder ohne Operatorenbereiche ihren Sinn behalten. Zunächst ist klar, daß (wie ja allgemein bei Gruppen mit Operatoren) der *Durchschnitt* $\mathfrak{a} \cap \mathfrak{b}$ und die *Summe* $(\mathfrak{a}, \mathfrak{b})$ zweier zulässiger Rechts- bzw. Linksideale $\mathfrak{a}$ und $\mathfrak{b}$ stets wieder zulässige Rechts- bzw. Linksideale sind. Ein *Produkt* $\mathfrak{a} \cdot \mathfrak{b}$ (die Menge aller Summen $\sum ab$, $a \in \mathfrak{a}$, $b \in \mathfrak{b}$) ist, wie man unmittelbar sieht, ein zulässiges Rechtsideal, sobald der zweite Faktor ein zulässiges Rechtsideal ist, und ein zulässiges Linksideal, sobald der erste Faktor ein zulässiges Linksideal ist. Der andere Faktor kann eine ganz beliebige Menge oder auch ein einzelnes Element von $\mathfrak{o}$ sein; z. B. ist $p\mathfrak{r}$, die Gesamtheit aller Produkte $pa\,(a \in \mathfrak{r})$, ein Rechtsideal, sobald $\mathfrak{r}$ eines ist.

Es gelten wie immer die Assoziativ- und Distributivgesetze für Moduln und speziell für Ideale in einem Ring $\mathfrak{o}$:

$$\mathfrak{a} \cdot \mathfrak{b}\,\mathfrak{c} = \mathfrak{a}\,\mathfrak{b} \cdot \mathfrak{c},$$
$$\mathfrak{a}\,(\mathfrak{b}, \mathfrak{c}) = (\mathfrak{a}\,\mathfrak{b}, \mathfrak{a}\,\mathfrak{c}),$$
$$(\mathfrak{b}, \mathfrak{c})\,\mathfrak{a} = (\mathfrak{b}\,\mathfrak{a}, \mathfrak{c}\,\mathfrak{a}).$$

In diesen Formeln kann $\mathfrak{a}$ sogar eine beliebige Menge oder auch ein einzelnes Element sein.

Ist in einem Ring $\mathfrak{o}$ die Minimalbedingung etwa für Linksideale erfüllt und $\mathfrak{o}$ nicht der Nullring, so gibt es in der Menge *aller* vom Null-

ideal verschiedenen Linksideale auch minimale Ideale; diese bezeichnen wir als *minimale Linksideale* schlechthin. Sie sind dadurch charakterisiert, daß sie keine vom Nullideal verschiedenen echten Unterideale besitzen, und können daher auch als *einfache Linksideale* bezeichnet werden.

Ist ein (einseitiges oder zweiseitiges) Ideal $\mathfrak{a}$ in $\mathfrak{o}$ direkte Summe von einseitigen bzw. zweiseitigen Idealen:

$$\mathfrak{a} = \mathfrak{a}_1 + \cdots + \mathfrak{a}_n,$$

und ist $n > 1$ und jedes $\mathfrak{a}_\nu \neq (0)$, so heißt das Ideal $\mathfrak{a}$ (einseitig bzw. zweiseitig) *direkt-zerlegbar*. Ist eine solche Zerlegung unmöglich, so heißt $\mathfrak{a}$ *direkt-unzerlegbar*.

Um zu zeigen, wie einschneidend die Minimalbedingung ist, beweisen wir die folgenden Sätze:

Ist $\mathfrak{o}$ ein Ring mit Minimalbedingung für Linksideale, a ein Element von $\mathfrak{o}$ und ist a kein rechter Nullteiler in $\mathfrak{o}$, so ist in $\mathfrak{o}$ die Gleichung $xa = b$ für jedes b lösbar.

Beweis: In der Menge der Linksideale $\mathfrak{o}a^\mu (\mu = 1, 2, \ldots)$ muß es ein minimales geben, etwa $\mathfrak{o}a^m$. Da $\mathfrak{o}a^{m+1} \subseteq \mathfrak{o}a^m$ gilt, aber $\mathfrak{o}a^{m+1} \subset \mathfrak{o}a^m$ ausgeschlossen ist, muß $\mathfrak{o}a^{m+1} = \mathfrak{o}a^m$ sein; mithin muß sich jedes Produkt ba^m auch in der Gestalt ca^{m+1} schreiben lassen:

$$ba^m = ca^{m+1}.$$

Daraus folgt, da man durch m Faktoren a rechts und links kürzen kann:

$$b = ca;$$

mithin ist die Gleichung $xa = b$ lösbar.

Genau ebenso: *Ist $\mathfrak{o}$ ein Ring mit Minimalbedingung für Rechtsideale und ist a kein linker Nullteiler, so ist $ax = b$ lösbar.*

Aus beiden Sätzen zusammen folgt:

Ist $\mathfrak{o}$ ein Ring ohne Nullteiler mit Minimalbedingung für Rechts- und Linksideale, so ist $\mathfrak{o}$ ein Körper.

Aufgaben. 1. Für einen Ring mit Einselement ist die oben erklärte Einschränkung des Idealbegriffs durch Hinzunahme von P oder Ω als Operatorenbereich unwesentlich: Jedes Ideal gestattet die Multiplikation mit P oder Ω.

2. Notwendig und hinreichend für die Gültigkeit der Maximal- *und* Minimalbedingung für die Linksideale eines Bereichs $\mathfrak{o}$ ist die Existenz einer Kompositionsreihe für diese Linksideale.

3. In einem kommutativen Ring mit Minimalbedingung ist der Restklassenring nach einem Primideal stets ein Körper und daher jedes Primideal teilerlos.

4. Jeder direkt-unzerlegbare kommutative Ring mit Minimalbedingung ist primär (d. h. das Nullideal ist primär); jeder primäre kommutative Ring ist direkt-unzerlegbar.

5. Damit im Restklassenring $\mathfrak{o}/\mathfrak{a}$ eines Ideals $\mathfrak{a}$ im kommutativen Ring $\mathfrak{o}$, für den die Maximalbedingung (der Teilerkettensatz) voraus-

gesetzt wird, die Minimalbedingung gilt, ist notwendig und hinreichend, daß jeder Primidealteiler $\mathfrak{p}$ von $\mathfrak{a}$ ein teilerloses Ideal in $\mathfrak{o}$ ist. [Für „notwendig" benutze man Aufgabe 3; für „hinreichend" stelle man nach § 85 und § 86 den Ring $\mathfrak{o}/\mathfrak{a}$ als direkte Summe von primären Ringen dar.]

§ 114. Nilpotente Ideale.

Ein Element a eines Ringes $\mathfrak{o}$ heißt *nilpotent*, wenn eine Potenz $a^\varrho = 0$ ist. Ein (Links- oder Rechts-) Ideal $\mathfrak{a}$ heißt *nilpotent*, wenn eine Potenz $\mathfrak{a}^\varrho$ gleich dem Nullideal (0) ist. Es gelten nun die folgenden Sätze:

1. *Die Summe* $(\mathfrak{l}_1, \mathfrak{l}_2)$ *zweier nilpotenten Linksideale ist ein nilpotentes Linksideal.*

Beweis: Es sei $\mathfrak{l}_1^n = \mathfrak{l}_2^m = (0)$. Man untersuche das Ideal $(\mathfrak{l}_1, \mathfrak{l}_2)^{n+m-1}$. Ausgerechnet, besteht dieses Linksideal aus einer Summe, deren einzelne Glieder Produkte von $n + m - 1$ Faktoren $\mathfrak{l}_1$ oder $\mathfrak{l}_2$ sind. In einem solchen Produkt tritt jedenfalls $\mathfrak{l}_1$ mindestens n-mal oder $\mathfrak{l}_2$ mindestens m-mal als Faktor auf. Ist etwa das erstere der Fall, so hat das betreffende Glied die Form

$$\cdots \mathfrak{l}_1 \cdots \mathfrak{l}_1 \cdots \mathfrak{l}_1 \cdots,$$

wo an Stelle der Punkte eventuell Faktoren $\mathfrak{l}_2$ stehen können und wo $\mathfrak{l}_1$ mindestens n-mal vorkommt. Da nun $\mathfrak{o}\mathfrak{l}_1 \subseteq \mathfrak{l}_1$ ist, so folgt: $\cdots \mathfrak{l}_1 \cdots \mathfrak{l}_1 \cdots \mathfrak{l}_1 \cdots \subseteq \mathfrak{l}_1^n \cdots = (0)$,

$$(\mathfrak{l}_1, \mathfrak{l}_2)^{n+m-1} = (0).$$

2. *Jedes nilpotente Linksideal (bzw. Rechtsideal) ist in einem nilpotenten zweiseitigen Ideal enthalten.*

Beweis: Es sei $\mathfrak{l}$ ein nilpotentes Linksideal: $\mathfrak{l}^\varrho = (0)$. Dann ist auch $\mathfrak{l}\mathfrak{o}$ nilpotent:

$$(\mathfrak{l}\mathfrak{o})^\varrho = \mathfrak{l}(\mathfrak{o}\mathfrak{l})^{\varrho-1}\mathfrak{o} \subseteq \mathfrak{l}\mathfrak{l}^{\varrho-1}\mathfrak{o} = \mathfrak{l}^\varrho\mathfrak{o} = (0).$$

Das von $\mathfrak{l}$ erzeugte Rechtsideal $(\mathfrak{l}, \mathfrak{l}\mathfrak{o})$ ist demnach Summe zweier nilpotenten Linksideale, mithin selbst nilpotentes Linksideal, also nilpotentes zweiseitiges Ideal.

Verstehen wir unter einer *Wurzelgröße* w ein solches Element von $\mathfrak{o}$, das ein nilpotentes zweiseitiges Ideal erzeugt, so gilt:

3. *Alle Elemente eines nilpotenten Links- oder Rechtsideals sind Wurzelgrößen.*

Beweis: Ist w im nilpotenten Linksideal $\mathfrak{l}$ enthalten, so ist w nach 2. auch in einem nilpotenten zweiseitigen Ideal enthalten, also ist das von w erzeugte zweiseitige Ideal auch nilpotent.

Nach 3. hätten wir die Wurzelgrößen auch als solche definieren können, die ein nilpotentes Links- oder Rechtsideal erzeugen.

4. *Die Gesamtheit aller Wurzelgrößen ist ein zweiseitiges Ideal, das alle nilpotenten Rechts- und Linksideale umfaßt.*

Beweis: Sind w_1 und w_2 Wurzelgrößen und $\mathfrak{w}_1$, $\mathfrak{w}_2$ die von ihnen erzeugten zweiseitigen Ideale, so ist $w_1 - w_2$ im Ideal $(\mathfrak{w}_1, \mathfrak{w}_2)$ enthalten,

das nach 1. nilpotent ist; also ist $w_1 - w_2$ wieder Wurzelgröße. Ebenso ist jedes Vielfache cw_1 oder $w_1 c$ wegen seiner Zugehörigkeit zu $\mathfrak{w}_1$ Wurzelgröße. Also ist die Gesamtheit der Wurzelgrößen ein zweiseitiges Ideal. Die übrigen Behauptungen folgen aus 3.

Die Gesamtheit aller Wurzelgrößen heißt das *Radikal* von $\mathfrak{o}$.

Definition. Ein *Ring ohne Radikal* ist ein Ring, dessen Radikal das Nullideal ist, oder auch ein Ring, in dem das Nullideal das einzige nilpotente Ideal ist.

In einem „Ring *mit* Radikal" gibt es also ein nilpotentes Links- oder Rechtsideal und daher nach 2. auch ein nilpotentes zweiseitiges Ideal $\mathfrak{a} \neq (0)$. Wie leicht zu sehen, gibt es dann auch ein zweiseitiges Ideal $\mathfrak{c} \neq (0)$ mit $\mathfrak{c}^2 = (0)$. Ist nämlich ϱ die kleinste Zahl mit der Eigenschaft $\mathfrak{a}^\varrho = (0)$, so genügt es, $\mathfrak{c} = \mathfrak{a}^{\varrho-1}$ zu setzen.

Gilt in $\mathfrak{o}$ die Maximalbedingung für Linksideale, so gibt es ein maximales nilpotentes Linksideal $\mathfrak{l}$. Dieses muß alle Wurzelgrößen w umfassen, denn sonst gäbe es ein umfassenderes nilpotentes Linksideal $(w, \mathfrak{l})$. Also ist $\mathfrak{l}$ gleich dem Radikal, und es folgt, daß *das Radikal selbst nilpotent ist.*

Hieraus folgt weiter:

Der Restklassenring eines Ringes $\mathfrak{o}$, *der die Maximalbedingung erfüllt, nach seinem Radikal* $\mathfrak{w}$ *ist stets ein Ring ohne Radikal.*

Beweis: Ein Linksideal in $\mathfrak{o}/\mathfrak{w}$ kann stets als Restklassengruppe $\mathfrak{l}/\mathfrak{w}$ angenommen werden, wo $\mathfrak{l}$ ein Linksideal in $\mathfrak{o}$ ist. Ist nun $\mathfrak{l}/\mathfrak{w}$ nilpotent, etwa

$$(\mathfrak{l}/\mathfrak{w})^\varrho = (0),$$

so ist jedes Produkt von ϱ Restklassen aus $\mathfrak{l}$ (mod $\mathfrak{w}$) gleich Null, mithin jedes Produkt von ϱ Elementen aus $\mathfrak{l}$ in $\mathfrak{w}$ enthalten:

$$\mathfrak{l}^\varrho \subseteq \mathfrak{w},$$
$$\mathfrak{w}^\sigma = (0),$$
$$\mathfrak{l}^{\varrho\sigma} = (\mathfrak{l}^\varrho)^\sigma \subseteq \mathfrak{w}^\sigma = (0);$$

also ist $\mathfrak{l}$ nilpotent und daher

$$\mathfrak{l} \subseteq \mathfrak{w},$$
$$\mathfrak{l}/\mathfrak{w} = (0).$$

Ein Ring ohne Radikal mit Minimalbedingung für Linksideale heißt auch *halbeinfach.* Der Name ist so zu erklären: Die Halbeinfachheit verlangt, wenn außer der Minimalbedingung noch die Existenz des Einselements als gegeben angenommen wird, etwas weniger als die *Einfachheit,* welche besagt, daß es überhaupt kein zweiseitiges Ideal in $\mathfrak{o}$ außer (0) und $\mathfrak{o}$ selbst gibt. Nimmt man nämlich die Existenz eines Einselements in $\mathfrak{o}$ an, so ist $\mathfrak{o}$ selbst sicher nicht nilpotent: also kann das Radikal eines einfachen Systems mit Einselement nur das Nullideal sein.

Aufgaben. 1. Von den hyperkomplexen Systemen aus § 112, Aufgabe 5 sind die ersten beiden halbeinfach; im letzten dagegen ist die lineare Schar (c) das Radikal.

2. Das hyperkomplexe System vom Range 3 mit der Multiplikationstafel

	e_1	e_2	u
e_1	e_1	0	u
e_2	0	e_1	0
u	0	u	0

besitzt ein Radikal; welches? Der Restklassenring nach dem Radikal ist direkte Summe zweier Körper.

3. Das System aller Matrizes n-ten Grades in einem Körper K ist einfach.

4. Für kommutative Ringe ist eine Wurzelgröße nichts anderes als ein nilpotentes Element. Daraus ist abzuleiten: Der Restklassenring $C/(m)$ nach einer ganzen rationalen Zahl m ist dann und nur dann ohne Radikal, wenn m keinen Primfaktor zum Quadrat enthält.

5. Dasselbe für den Restklassenring nach einem Ideal in der Hauptordnung eines Zahlkörpers.

6. Das Radikal eines kommutativen primären Ringes ist das zum Nullideal gehörige Primideal.

7. Ist $(0) = [\mathfrak{q}_1, \ldots, \mathfrak{q}_r]$ eine Zerlegung des Nullideals eines kommutativen Ringes $\mathfrak{o}$ in Primärkomponenten und sind $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ die zugehörigen Primideale, so ist $[\mathfrak{p}_1, \ldots, \mathfrak{p}_r]$ das Radikal.

§ 115. Die volle Reduzibilität der Ringe ohne Radikal.

Alle in diesem Paragraphen zu verwendenden gruppentheoretischen Termini (direkte Summe, operatorisomorph usw.) beziehen sich auf den Ring $\mathfrak{o}$ und dessen Linksideale als Abelsche Gruppen, mit $\mathfrak{o}$ (und eventuell noch P oder Ω; vgl. § 113) als festen (Links-)Multiplikatorenbereich.

Ziel dieses Paragraphen ist der Beweis des folgenden *Hauptsatzes über die halbeinfachen Ringe*:

Ein Ring $\mathfrak{o}$ ohne Radikal mit Minimalbedingung für Linksideale besitzt ein Einselement und ist direkte Summe von einfachen Linksidealen. Umgekehrt: Ein Ring mit Einselement, der direkte Summe von einfachen Linksidealen ist, ist ein Ring ohne Radikal mit Minimalbedingung für Linksideale.

Die zum Beweis nötigen Hilfssätze sind auch an sich von Interesse.

Hilfssatz 1. *Ist $\mathfrak{l}$ ein Linksideal, a ein Element von $\mathfrak{o}$, so wird $\mathfrak{l}$ auf $\mathfrak{l}a$ operatorhomomorph abgebildet durch die Zuordnung*

$$x \to xa.$$

Beweis:

$$(x+y)a = xa + ya,$$
$$(rx)\cdot a = r\cdot(xa),$$
$$(\lambda x)\cdot a = \lambda\cdot(xa).$$ [1]

Hilfssatz 2. *Ein minimales (= einfaches) Linksideal* $\mathfrak{l}$ *wird durch einen Operatorhomomorphismus entweder auf das Nullideal abgebildet oder der Homomorphismus ist ein Isomorphismus.*

Beweis: Die Gesamtheit der Elemente a von $\mathfrak{l}$, denen die Null zugeordnet wird, ist ein Linksideal $\leqq \mathfrak{l}$, also entweder $= (0)$ oder $= \mathfrak{l}$. Im ersten Fall ist die Zuordnung isomorph.

Definition. Ein Element e von $\mathfrak{o}$ heißt *idempotent*, wenn $e^2 = e$ (und daher auch $e^3 = e$ usw.) ist.

Das Nullelement und das (etwaige) Einselement sind also stets idempotent.

Hilfssatz 3. *Ein minimales Linksideal* $\mathfrak{l}$ *ist entweder nilpotent, und zwar ist dann schon* $\mathfrak{l}^2 = (0)$, *oder* $\mathfrak{l}$ *enthält ein idempotentes Element* e *und wird von diesem erzeugt*:

$$e^2 = e \quad in \quad \mathfrak{l}, \qquad \mathfrak{l} = \mathfrak{o}e.$$

Beweis: Gesetzt, es sei $\mathfrak{l}^2 \neq (0)$. Dann gibt es in $\mathfrak{l}$ ein a mit $\mathfrak{l}a \neq (0)$. Die Zuordnung $x \to xa$ ist nach Hilfssatz 1 ein Homomorphismus und nach Hilfssatz 2 sogar ein Isomorphismus; sie führt $\mathfrak{l}$ in $\mathfrak{l}a$ über, und man hat

$$\mathfrak{l}a \neq (0), \qquad \mathfrak{l}a \leqq \mathfrak{l},$$

mithin

$$\mathfrak{l}a = \mathfrak{l}.$$

Jedes Element von $\mathfrak{l}$ ist demnach in der Gestalt xa (x in $\mathfrak{l}$) darstellbar, insbesondere auch a selbst:

$$a = ea \qquad (e \text{ in } \mathfrak{l}).$$

Daraus folgt erstens $e \neq 0$, zweitens $ea = e^2a$; also ergeben e und e^2 beim Isomorphismus $x \to xa$ dasselbe Element ea, sind also selbst einander gleich:

$$e^2 = e.$$

Das Ideal $\mathfrak{o}e$ ist nicht Null (denn es enthält das Element $e^2 = e$) und ist in $\mathfrak{l}$ enthalten, ist also gleich $\mathfrak{l}$. Damit ist alles bewiesen.

Hilfssatz 4. *Ist* e *idempotent und* $\mathfrak{l} = \mathfrak{o}e$, *so ist* $\mathfrak{o}$ *direkte Summe von* $\mathfrak{l}$ *und einem anderen Linksideal* $\mathfrak{l}'$:

$$\mathfrak{o} = \mathfrak{l} + \mathfrak{l}'.$$

Weiter ist für alle x *in* $\mathfrak{l}$

$$xe = x,$$

für alle x' *in* $\mathfrak{l}'$

$$x'e = 0.$$

[1] Der Beweis gilt auch, wenn a nicht in $\mathfrak{o}$, sondern in einem $\mathfrak{o}$-Modul gewählt wird.

Beweis: Für jedes a aus $\mathfrak{o}$ setzen wir $a = ae + (a - ae)$ (linksseitige Zerlegung von PEIRCE). Die Elemente ae bilden das Linksideal $\mathfrak{o}e = \mathfrak{l}$. Die Elemente $a - ae$ bilden auch ein Linksideal $\mathfrak{l}'$; denn es ist

$$(a - ae) - (b - be) = (a - b) - (a - b)e,$$
$$r(a - ae) = ra - (ra)e,$$
$$\lambda(a - ae) = \lambda a - (\lambda a)e.$$

Die $a - ae$ werden von e annulliert:

$$(a - ae)e = ae - ae^2 = 0,$$

während die ae bei Multiplikation mit e sich reproduzieren:

$$(ae)e = ae^2 = ae.$$

Das einzige Element, das bei Multiplikation mit e sowohl annulliert als auch reproduziert wird, ist die Null. Also haben $\mathfrak{l}$ und $\mathfrak{l}'$ nur die Null gemein; d. h. die Summe $\mathfrak{o} = \mathfrak{l} + \mathfrak{l}'$ ist direkt.

Wir können nun den ersten Teil des Hauptsatzes beweisen:

Satz 1. *Ein Ring ohne Radikal mit Minimalbedingung für Linksideale ist direkte Summe von einfachen Linksidealen.*

Beweis: Für den Nullring ist der Satz klar. Es sei also $\mathfrak{o}$ vom Nullring verschieden, und $\mathfrak{l}_1$ sei ein von Null verschiedenes minimales Linksideal. Nach Hilfssatz 3 und 4 ist

$$\mathfrak{o} = \mathfrak{l}_1 + \mathfrak{l}'.$$

Ist $\mathfrak{l}'$ nicht Null, so suchen wir in $\mathfrak{l}'$ ein vom Nullideal verschiedenes minimales Linksideal $\mathfrak{l}_2$; dann ist nach Hilfssatz 3 und 4

$$\mathfrak{o} = \mathfrak{l}_2 + \mathfrak{l}^*,$$

und wenn man sich bei dieser Summendarstellung der Elemente von $\mathfrak{o}$ insbesondere auf die Elemente von $\mathfrak{l}'$ beschränkt, so folgt:

$$\mathfrak{l}' = \mathfrak{l}_2 + \mathfrak{l}'',$$
$$\mathfrak{o} = \mathfrak{l}_1 + \mathfrak{l}_2 + \mathfrak{l}''.$$

Nun sucht man im Falle $\mathfrak{l}'' \neq (0)$ wieder in $\mathfrak{l}''$ ein minimales Linksideal $\mathfrak{l}_3 \neq (0)$ und findet durch dieselben Schlüsse:

$$\mathfrak{o} = \mathfrak{l}_1 + \mathfrak{l}_2 + \mathfrak{l}_3 + \mathfrak{l}''',$$

usw. Die Reihe $\mathfrak{o} \supset \mathfrak{l}' \supset \mathfrak{l}'' \supset \mathfrak{l}''' \supset \cdots$ muß nach der Minimalbedingung ein minimales Linksideal enthalten. Nennen wir dieses $\mathfrak{l}_n$ und setzen die Zerlegung bis zu $\mathfrak{l}_n$ fort, so erhalten wir:

$$\mathfrak{o} = \mathfrak{l}_1 + \mathfrak{l}_2 + \cdots + \mathfrak{l}_n,$$

womit Satz 1 *bewiesen* ist.

Laut Konstruktion wird jedes der Ideale $\mathfrak{l}_i$ von einem idempotenten Element erzeugt:

$$\mathfrak{l}_i = \mathfrak{o}e_i, \qquad e_i^2 = e_i \in \mathfrak{l}_i.$$

Weiter ist, da $\mathfrak{l}'$ von e_1 annulliert wird:

$$e_2 e_1 = 0, \quad e_3 e_1 = 0, \quad \ldots, \quad e_n e_1 = 0;$$

ebenso, da $\mathfrak{l}''$ von e_2 annulliert wird:

$$e_3 e_2 = 0, \quad \ldots, \quad e_n e_2 = 0;$$

usw.; allgemein

$$e_k e_i = 0 \quad \text{für} \quad k > i.$$

Um nun unter den angegebenen Voraussetzungen die *Existenz der Eins* zu beweisen, verfahren wir so:

Wir bilden

$$e_{12} = e_1 + e_2 - e_1 e_2.$$

Dann ist

$$\begin{aligned} e_1 e_{12} &= e_1^2 + e_1 e_2 - e_1^2 e_2 &&= e_1, \\ e_2 e_{12} &= e_2 e_1 + e_2^2 - e_2 e_1 e_2 &&= e_2, \\ (e_1 e_2) e_{12} &= e_1 (e_2 e_{12}) &&= e_1 e_2 \end{aligned}$$

also

$$\begin{gathered} (e_1 + e_2 - e_1 e_2) e_{12} = e_1 + e_2 - e_1 e_2, \\ e_{12}^2 = e_{12}. \end{gathered}$$

Das Element e_{12} ist also idempotent und in $\mathfrak{l}_1 + \mathfrak{l}_2$ enthalten. Unter seinen Linksvielfachen $x e_{12}$ kommt aber nach der eben ausgeführten Rechnung sowohl e_1 wie e_2, also jede Größe aus $\mathfrak{l}_1 + \mathfrak{l}_2$ vor. Daher ist

$$\mathfrak{l}_1 + \mathfrak{l}_2 = \mathfrak{o}\, e_{12}.$$

Weiter ist

$$e_k e_{12} = 0 \quad \text{für} \quad k > 2.$$

Wir können also fortfahren und setzen

$$e_{123} = e_{12} + e_3 - e_{12} e_3;$$

dann finden wir in derselben Weise:

$$\begin{gathered} e_{123}^2 = e_{123}, \\ \mathfrak{o}\, e_{123} = \mathfrak{o}\, e_{12} + \mathfrak{l}_3 = \mathfrak{l}_1 + \mathfrak{l}_2 + \mathfrak{l}_3. \end{gathered}$$

So weitergehend, erhalten wir schließlich ein idempotentes Element $e = e_{12\ldots n}$ mit der Eigenschaft

$$\mathfrak{o}\, e = \mathfrak{l}_1 + \cdots + \mathfrak{l}_n = \mathfrak{o}.$$

Nach Hilfssatz 4 ist e ein Rechtseinselement für $\mathfrak{o} = \mathfrak{o} e$. Um zu zeigen, daß e auch ein Linkseinselement ist, nehmen wir eine rechtsseitige Peircesche Zerlegung (Hilfssatz 4 mit Vertauschung von Rechts und Links) vor. Es wird

$$\begin{gathered} \mathfrak{o} = e\,\mathfrak{o} + \mathfrak{r}, \\ e\,\mathfrak{r} = (0), \\ \mathfrak{r} = \mathfrak{r} e \quad \text{(weil } e \text{ Rechtseinselement)}, \end{gathered}$$

also

$$\mathfrak{r}^2 = \mathfrak{r}e\mathfrak{r} = (0),$$

mithin, da $\mathfrak{o}$ ein Ring ohne Radikal ist,

$$\mathfrak{r} = (0),$$

$$\mathfrak{o} = e\mathfrak{o}.$$

Also ist e ein Linkseinselement (Hilfssatz 4 mit Vertauschung von Rechts und Links).

Damit ist der erste Teil des Hauptsatzes *bewiesen.*

Zur Umkehrung benötigen wir

Hilfssatz 5. *Ist ein Ring* $\mathfrak{o}$ *mit Einselement direkte Summe von* n *Linksidealen:*

$$\mathfrak{o} = \mathfrak{l}_1 + \cdots + \mathfrak{l}_n,$$

und besteht insbesondere für die Eins die Darstellung

$$1 = e_1 + \cdots + e_n, \qquad (e_i \in \mathfrak{l}_i)$$

so ist

$$\mathfrak{l}_i = \mathfrak{o}e_i,$$

$$e_i^2 = e_i,$$

$$e_i e_k = 0 \quad \textit{für} \quad i \neq k.$$

Beweis: Für jedes a aus $\mathfrak{l}_1$ gilt

$$a = a \cdot 1 = ae_1 + ae_2 + \cdots + ae_n,$$

andererseits

$$a = a + 0 + \cdots + 0,$$

also wegen der direkten Summe

$$ae_1 = a, \quad ae_2 = 0, \quad \ldots, \quad ae_n = 0.$$

Wendet man dies insbesondere auf $a = e_1$ an, so folgt

$$e_1^2 = e_1, \quad e_1 e_2 = 0, \quad \ldots, \quad e_1 e_n = 0.$$

Ebenso beweist man, da kein Index vor dem anderen ausgezeichnet ist,

$$e_i^2 = e_i,$$

$$e_i e_k = 0 \quad \text{für} \quad i \neq k.$$

Weiter zeigt die Gleichung $ae_1 = a$, daß jedes a aus $\mathfrak{l}_1$ in der Gestalt ae_1 geschrieben werden kann; daraus folgt

$$\mathfrak{l}_1 = \mathfrak{o}e_1$$

und ebenso allgemein

$$\mathfrak{l}_i = \mathfrak{o}e_i \qquad \text{(q. e. d.).}$$

Zur Umkehrung des Hauptsatzes bemerken wir das Folgende.

Wenn ein Ring $\mathfrak{o}$ direkte Summe von n *einfachen* Linksidealen ist oder, wie man sagt, *linksseitig voll reduzibel* ist, so folgt zunächst rein gruppentheoretisch die Existenz einer Kompositionsreihe (aus Links-

idealen) von der Länge n (§ 42). Also besitzt auch jedes Linksideal eine Kompositionsreihe, deren Länge höchstens n ist. Es gibt also in jeder nicht leeren Menge von Linksidealen ein Ideal kleinster Länge, mithin ein minimales Linksideal. *Die Minimalbedingung ist also eine Folge der vollständigen Reduzibilität.* (Ebenso könnte man das Erfülltsein der Maximalbedingung beweisen.) Weiter folgt rein gruppentheoretisch, daß jedes Linksideal direkter Summand ist (§ 42).

Nimmt man nun noch die Existenz eines Einselements an, so ist ganz leicht nachzuweisen, daß man es mit einem Ring ohne Radikal zu tun hat. Hat man nämlich ein nilpotentes Linksideal $\mathfrak{l}$, etwa mit $\mathfrak{l}^e = (0)$, so hat man

$$\mathfrak{o} = \mathfrak{l} + \mathfrak{l}';$$

nach Hilfssatz 5 gibt es also in $\mathfrak{l}$ ein erzeugendes Element e_1 mit $e_1^2 = e_1$. Es ist dann auch $e_1^e = e_1$. Andererseits ist $e_1^e = 0$ wegen der Nilpotenz von $\mathfrak{l}$; also folgt $e_1 = 0$ und $\mathfrak{l} = (0)$. Somit ist das einzige nilpotente Linksideal das Nullideal.

Damit ist auch der zweite Teil des Hauptsatzes bewiesen.

Aufgaben. 1. Jeder Ring ohne Nullteiler mit Minimalbedingung für Linksideale ist ein Körper.

2. Man zerlege den Ring mit Radikal von § 114, Aufg. 2 in direkt-unzerlegbare Links- bzw. Rechtsideale und verifiziere, daß diese nicht einfach sind.

3. Das System aller Matrizes n-ten Grades in einem Körper K ist (links- und rechtsseitig) vollständig reduzibel.

4. Man beweise die folgende Umkehrung des Hilfssatzes 5:

Ist in einem Ring $\mathfrak{o}$ mit Einselement

$$1 = e_1 + \cdots + e_n,$$
$$e_i^2 = e_i, \quad e_i e_k = 0 \quad \text{für} \quad i \neq k,$$

so ist

$$\mathfrak{o} = \mathfrak{o}\, e_1 + \cdots + \mathfrak{o}\, e_n$$

eine Zerlegung von $\mathfrak{o}$ in Linksideale und ebenso

$$\mathfrak{o} = e_1\, \mathfrak{o} + \cdots + e_n\, \mathfrak{o}$$

eine Zerlegung von $\mathfrak{o}$ in Rechtsideale.

§ 116. Zweiseitige Zerlegungen und Zentrumszerlegung.

In § 115 haben wir die direkten Summenzerlegungen eines Ringes $\mathfrak{o}$ in Linksideale unter gewissen Voraussetzungen untersucht; jetzt wollen wir sehen, was sich über die Zerlegungen in *zweiseitige* Ideale

$$\mathfrak{o} = \mathfrak{a}_1 + \cdots + \mathfrak{a}_n \tag{1}$$

sagen läßt.

Zunächst ist unmittelbar zu sehen, daß bei einer Zerlegung (1) die Summanden $\mathfrak{a}_\nu$ sich gegenseitig annullieren müssen:

$$\mathfrak{a}_i \mathfrak{a}_k = (0) \quad \text{für} \quad i \neq k;$$

denn $\mathfrak{a}_i \mathfrak{a}_k$ ist sowohl in $\mathfrak{a}_i$ wie in $\mathfrak{a}_k$ enthalten.

Die Ideale $\mathfrak{a}_i$ können auch als Ringe betrachtet werden. Die Zerlegung (1) ist also eine Darstellung von $\mathfrak{o}$ als Summe von Ringen, die sich gegenseitig annullieren.

Ist umgekehrt eine solche Darstellung von $\mathfrak{o}$ als Summe von sich gegenseitig annullierenden Ringen $\mathfrak{a}_i$ gegeben, so sind diese Ringe notwendig zweiseitige Ideale in $\mathfrak{o}$; denn es ist

$$\begin{aligned} \mathfrak{o}\,\mathfrak{a}_i &= (\mathfrak{a}_1, \ldots, \mathfrak{a}_n) \cdot \mathfrak{a}_i \\ &= (\mathfrak{a}_1 \mathfrak{a}_i, \ldots, \mathfrak{a}_n \mathfrak{a}_i) = \mathfrak{a}_i^2 \subseteq \mathfrak{a}_i \end{aligned}$$

und ebenso

$$\mathfrak{a}_i \mathfrak{o} \subseteq \mathfrak{a}_i .$$

Weiter zeigt sich: *Jedes (einseitige oder zweiseitige) Ideal im Ring $\mathfrak{a}_i$ ist zugleich ein (ebensolches) Ideal in $\mathfrak{o}$.* Denn ist $\mathfrak{l}$ etwa ein Linksideal in $\mathfrak{a}_1$, so ist

$$\begin{aligned} \mathfrak{o}\,\mathfrak{l} &= (\mathfrak{a}_1, \ldots, \mathfrak{a}_n)\,\mathfrak{l} = (\mathfrak{a}_1 \mathfrak{l}, \mathfrak{a}_2 \mathfrak{l}, \ldots, \mathfrak{a}_n \mathfrak{l}) \\ &= \mathfrak{a}_1 \mathfrak{l} \subseteq \mathfrak{l}. \end{aligned}$$

Sind insbesondere die Ideale $\mathfrak{a}_i$ zweiseitig einfach, so sind sie nach diesem Satz auch als Ringe zweiseitig einfach. Für „zweiseitig einfache Ringe" sagt man meist kurz *einfache Ringe*: das sind also solche Ringe, die keine zweiseitigen Ideale außer sich selbst und dem Einheitsideal besitzen.

Ist ein Ring $\mathfrak{o}$ mit Einselement darstellbar als direkte Summe von direkt-unzerlegbaren, vom Nullideal verschiedenen zweiseitigen Idealen:

$$\mathfrak{o} = \mathfrak{a}_1 + \cdots + \mathfrak{a}_n,$$

so sind die Ideale $\mathfrak{a}_i$ eindeutig bestimmt.

Beweis: Hat man eine zweite Zerlegung

$$\mathfrak{o} = \mathfrak{c}_1 + \cdots + \mathfrak{c}_m,$$

so ist

$$\mathfrak{c}_1 = \mathfrak{o}\,\mathfrak{c}_1 = (\mathfrak{a}_1 \mathfrak{c}_1, \mathfrak{a}_2 \mathfrak{c}_1, \ldots, \mathfrak{a}_n \mathfrak{c}_1).$$

Die Summe rechts ist direkt wegen

$$\mathfrak{a}_1 \mathfrak{c}_1 \subseteq \mathfrak{a}_1, \ldots, \mathfrak{a}_n \mathfrak{c}_1 \subseteq \mathfrak{a}_n.$$

Da aber $\mathfrak{c}_1$ direkt-unzerlegbar ist, müssen alle Produkte rechts $= (0)$ sein mit Ausnahme eines einzigen, etwa außer $\mathfrak{a}_1 \mathfrak{c}_1$. Dann ist also

$$\mathfrak{c}_1 = \mathfrak{a}_1 \mathfrak{c}_1 \subseteq \mathfrak{a}_1.$$

Ebenso zeigt man, daß umgekehrt $\mathfrak{a}_1$ in einem $\mathfrak{c}_i$ enthalten ist, also

$$\mathfrak{c}_1 \subseteq \mathfrak{a}_1 \subseteq \mathfrak{c}_i ;$$

daraus folgt $i = 1$ und $\mathfrak{c}_1 = \mathfrak{a}_1$. So ist jedes $\mathfrak{c}_i$ einem $\mathfrak{a}_i$ gleich.

Bei einseitigen Summenzerlegungen besteht, wie wir sehen werden, diese Eindeutigkeit nicht mehr.

Bei *kommutativen* Ringen fällt der Unterschied zwischen einseitigen und zweiseitigen Idealen fort. Aus dem Hauptsatze von § 115 in Verbindung mit Hilfssatz 5 folgt daher schon eine Darstellung eines jeden halbeinfachen kommutativen Ringes $\mathfrak{o}$ als Summe von einfachen Ringen mit Einselement, die sich gegenseitig annullieren. Aber jeder einfache kommutative Ring mit Einselement ist ein Körper, da die Vielfachen ax eines Elements $a \neq 0$ ein vom Nullideal verschiedenes Ideal, also den ganzen Ring ausmachen. Also (Satz von DEDEKIND):

Jeder kommutative Ring ohne Radikal mit Minimalbedingung ist eine direkte Summe von kommutativen Körpern, die sich gegenseitig annullieren.

Für kommutative Ringe $\mathfrak{o}$ *mit* Radikal und mit Einselement findet man eine ähnliche Summenzerlegung, nämlich als direkte Summe von primären Ringen, indem man unter Voraussetzung der Maximal- und Minimalbedingung das Nullideal nach § 86 in einartige Primärideale zerlegt (vgl. § 113, Aufgabe 3) und daraus nach § 85, Schluß eine Summendarstellung für $\mathfrak{o}$ herleitet.

Unter dem *Zentrum* eines Ringes $\mathfrak{o}$ verstehen wir die Gesamtheit der Elemente a von $\mathfrak{o}$, die mit allen Elementen von $\mathfrak{o}$ vertauschbar sind:

$$ax = xa \quad \text{für alle } x .$$

Das Zentrum ist ein Unterring; denn aus $ax = xa$ und $bx = xb$ folgt

$$(a - b)\,x = ax - bx = xa - xb = x(a - b)$$

und

$$ab \cdot x = axb = x \cdot ab .$$

Wenn $\mathfrak{o}$ noch einen Operatorenbereich im Sinne von § 113 besitzt, so ist das Zentrum $\mathfrak{Z}$ auch ein zulässiger Unterring; denn ist a irgendein Element des Zentrums, so folgt für alle Operatoren λ und alle x

$$(\lambda a)x = \lambda(ax) = \lambda(xa) = x \cdot \lambda a ,$$

so daß auch λa dem Zentrum angehört.

Das Zentrum ist natürlich kommutativ. Das etwaige Einselement eines Ringes gehört stets dem Zentrum an.

Ist $\mathfrak{o}$ ein Ring ohne Radikal, so ist auch $\mathfrak{Z}$ ein Ring ohne Radikal.

Beweis: Gesetzt, das Radikal von $\mathfrak{Z}$ sei vom Nullideal verschieden, so gäbe es im Ring $\mathfrak{Z}$ ein Ideal $\mathfrak{c} \neq (0)$ mit $\mathfrak{c}^2 = (0)$. $\mathfrak{c}$ erzeugt in $\mathfrak{o}$ ein Linksideal $\mathfrak{d} = (\mathfrak{c}, \mathfrak{o}\mathfrak{c})$, und da $\mathfrak{c}$ mit $\mathfrak{o}$ vertauschbar ist, so ist

$$\begin{aligned}\mathfrak{d}^2 &= (\mathfrak{c}, \mathfrak{o}\mathfrak{c})^2 = (\mathfrak{c}^2, \mathfrak{c}\mathfrak{o}\mathfrak{c}, \mathfrak{o}\mathfrak{c}^2, \mathfrak{o}\mathfrak{c}\mathfrak{o}\mathfrak{c}) \\ &= (\mathfrak{c}^2, \mathfrak{o}\mathfrak{c}^2, \mathfrak{o}^2\mathfrak{c}^2) = (0);\end{aligned}$$

also gäbe es in $\mathfrak{o}$ ein nilpotentes Ideal $\mathfrak{d} \neq (0)$, was der Voraussetzung widerspricht.

Ist $\mathfrak{o}$ direkte Summe von zweiseitigen Idealen:

$$\mathfrak{o} = \mathfrak{a}_1 + \cdots + \mathfrak{a}_n, \tag{1}$$

so ist das Zentrum $\mathfrak{Z}$ von $\mathfrak{o}$ direkte Summe der Zentren $\mathfrak{Z}_i$ der Ringe $\mathfrak{a}_i$:

$$\mathfrak{Z} = \mathfrak{Z}_1 + \cdots + \mathfrak{Z}_n.$$

Beweis: Zunächst sind die Zentren $\mathfrak{Z}_i$ der Ringe $\mathfrak{a}_i$ in $\mathfrak{Z}$ enthalten. Denn wenn a_i zu $\mathfrak{Z}_i$ gehört, so ist für ein beliebiges

$$x = x_1 + \cdots + x_n \qquad (x_j \in \mathfrak{a}_j)$$

aus $\mathfrak{o}$:

$$a_i x = a_i x_i = x_i a_i = x a_i;$$

alle Produkte $a_i x_k$ und $x_k a_i$ mit $i \neq k$ sind ja Null.

Sodann gestattet jedes Element a von $\mathfrak{Z}$ nach (1) eine Zerlegung:

$$a = a_1 + \cdots + a_n \qquad (a_j \in \mathfrak{a}_j)$$

und für beliebige x_i aus $\mathfrak{a}_i$ ist

$$a_i x_i = a x_i = x_i a = x_i a_i;$$

mithin ist jedes a_i in $\mathfrak{Z}_i$ enthalten. $\mathfrak{Z}$ ist also die Summe der $\mathfrak{Z}_i$, die sich natürlich gegenseitig annullieren. Aus $0 = a_1 + \cdots + a_n (a_i \in \mathfrak{Z}_i)$ folgt $a_i = 0$, da die Summe (1) direkt ist; die Summe der $\mathfrak{Z}_i$ ist also ebenfalls direkt.

Aufgaben. 1. Ist $\mathfrak{Z} = \mathfrak{Z}_1 + \cdots + \mathfrak{Z}_n$ eine Zerlegung des Zentrums $\mathfrak{Z}$ eines Ringes $\mathfrak{o}$ mit Einselement und setzt man

$$\mathfrak{a}_i = \mathfrak{o}\,\mathfrak{Z}_i,$$

so sind die $\mathfrak{a}_i$ zweiseitige Ideale in $\mathfrak{o}$, und es ist

$$\mathfrak{o} = \mathfrak{a}_1 + \cdots + \mathfrak{a}_n,$$

während $\mathfrak{Z}_i = \mathfrak{a}_i \cap \mathfrak{Z}$ das Zentrum des Ringes $\mathfrak{a}_i$ ist.

2. Sind die $\mathfrak{a}_\nu$ in (1) direkt-unzerlegbar, so gilt dasselbe von den $\mathfrak{Z}_\nu$.

3. Das Zentrum $\mathfrak{Z}$ eines hyperkomplexen Systems $\mathfrak{o}$ ist wieder ein hyperkomplexes System; ist $\mathfrak{o}$ ein System ohne Radikal, so ist $\mathfrak{Z}$ eine direkte Summe von Körpern.

4. Ist $\mathfrak{o} = \mathfrak{a}_1 + \cdots + \mathfrak{a}_n$ eine zweiseitige Zerlegung eines Ringes mit Einselement, so ist jedes minimale Linksideal von $\mathfrak{o}$ in einem der $\mathfrak{a}_\nu$ enthalten.

5. Das Zentrum des Gruppenrings einer Gruppe $\mathfrak{G}$ besteht aus denjenigen Summen

$$\sum \lambda_\nu a_\nu,$$

in denen alle Elemente a_ν aus einer Klasse konjugierter Elemente von $\mathfrak{G}$ denselben Koeffizienten λ_ν haben. Es gibt in $\mathfrak{o}$ so viele linear-unabhängige Zentrumselemente, als es in $\mathfrak{G}$ Klassen gibt.

§ 117. Der Automorphismenring eines vollständig reduziblen Moduls.

Im § 115 haben wir gesehen, daß ein halbeinfacher Ring $\mathfrak{o}$, als $\mathfrak{o}$-Linksmodul betrachtet, vollständig reduzibel ist. Wir wollen nun den Automorphismenring dieses vollständig reduziblen Moduls bestimmen.

Das Problem der Struktur des Automorphismenrings eines voll reduziblen Moduls $\mathfrak{M}$ ist auch an sich und anderer Anwendungen wegen von Wichtigkeit. Wir wollen darum das Problem ganz allgemein lösen und zunächst davon absehen, daß in dem speziellen Fall, von dem wir ausgegangen sind, der Modul $\mathfrak{M}$ ein Ring mit sich selbst als Multiplikatorenbereich ist.

Es sei also $\mathfrak{M}$ ein vollständig reduzibler Modul mit irgendeinem Multiplikatorenbereich. Unter „Automorphismen" von $\mathfrak{M}$ verstehen wir in diesem Paragraphen alle Operatorhomomorphismen von $\mathfrak{M}$ in sich, also nicht nur die 1-Isomorphismen von $\mathfrak{M}$ auf sich. Nach § 38 bilden diese Automorphismen stets einen Ring; es handelt sich nun um die Struktur dieses Automorphismenringes.

Ist der untersuchte Modul $\mathfrak{M}$ speziell ein Linearformenmodul in bezug auf einen Körper K (dessen Elemente als Rechtsoperatoren geschrieben werden) und besitzt $\mathfrak{M}$ außerdem noch gewisse Linksoperatoren $A, B, \ldots$, welche der Bedingung $Am \cdot \varkappa = A \cdot m\varkappa$ genügen und daher lineare Transformationen des Linearformenmoduls induzieren (vgl. § 104), so sind die Automorphismen dieses Doppelmoduls $\mathfrak{M}$ wieder lineare Transformationen Θ, welche mit den Transformationen $A, B, \ldots$ vertauschbar sind:

$$\Theta(Am) = A(\Theta m).$$

Unsere Untersuchung wird also als Spezialfall die Bestimmung der mit einem vollständig reduziblen System von linearen Transformationen vertauschbaren linearen Transformationen enthalten (vgl. Aufg. 1 nachstehend).

Zunächst betrachten wir die homomorphen Abbildungen eines einfachen Moduls $\mathfrak{M}_1$. Der Untermodul derjenigen Elemente, die dabei auf Null abgebildet werden, ist entweder gleich dem ganzen $\mathfrak{M}_1$ oder besteht nur aus dem Nullelement. Im letzteren Fall ist die Abbildung ein 1-Isomorphismus. *Bei jedem Homomorphismus wird also der einfache Modul $\mathfrak{M}_1$ entweder auf Null abgebildet, oder die Abbildung ist ein 1-Isomorphismus.*

Wird $\mathfrak{M}_1$ in sich abgebildet und ist die Abbildung nicht der Nulloperator (der $\mathfrak{M}_1$ auf Null abbildet), so ist sie 1-isomorph und führt $\mathfrak{M}_1$ in einen von Null verschiedenen Untermodul, d. h. in $\mathfrak{M}_1$ selbst über. Ein solcher 1-Automorphismus besitzt immer einen inversen Automorphismus. Also hat im Automorphismenring von $\mathfrak{M}_1$ jeder Automorphismus einen inversen, d. h. *der Automorphismenring eines einfachen Moduls ist ein Körper.*

In derselben Weise ergibt sich: *Wenn $\mathfrak{M}_1$ homomorph in einen anderen einfachen Modul $\mathfrak{M}_2$ abgebildet wird und die Abbildung nicht der Nulloperator ist, so muß sie ein 1-Isomorphismus und daher $\mathfrak{M}_1 \cong \mathfrak{M}_2$ sein.*

Wir können nun die Automorphismen von $\mathfrak{M} = \mathfrak{M}_1 + \cdots + \mathfrak{M}_r$, wo die $\mathfrak{M}_i$ einfach sind, bestimmen. Zunächst bemerken wir: Wenn ein Element m in seine Komponenten zerlegt wird:

$$m = m_1 + \cdots + m_r, \tag{1}$$

so ist jede der Zuordnungen $m \to m_\nu$ ein Homomorphismus. Wir bezeichnen diesen mit H_ν. An Stelle von (1) kann man jetzt schreiben:

$$m = \sum_\nu H_\nu m. \tag{2}$$

Um nun einen beliebigen Automorphismus Θ zu kennen, genügt es, seine Auswirkung auf die Komponenten $m_\nu = H_\nu m$ zu kennen; denn es ist

$$\Theta m = \sum_\nu \Theta m_\nu. \tag{3}$$

Die Elemente Θm_ν zerlegen wir nun in Komponenten:

$$\Theta m_\nu = \sum_\mu H_\mu \Theta m_\nu. \tag{4}$$

Der Operator $H_\mu \Theta$, angewandt auf die Elemente m_ν von $\mathfrak{M}_\nu$, ergibt einen Homomorphismus, der $\mathfrak{M}_\nu$ in $\mathfrak{M}_\mu$ abbildet. Wir bezeichnen diesen Homomorphismus mit $\Theta_{\mu\nu}$. Die r^2 Homomorphismen $\Theta_{\mu\nu}$ lassen sich in einer quadratischen Matrix anordnen. Ist $\mathfrak{M}_\nu$ nicht isomorph zu $\mathfrak{M}_\mu$, so ist $\Theta_{\mu\nu}$ notwendig der Nulloperator. Für (4) schreiben wir jetzt:

$$\Theta m_\nu = \sum_\mu \Theta_{\mu\nu} m_\nu. \tag{5}$$

In (3) eingesetzt, ergibt dies:

$$\Theta m = \sum_\mu \sum_\nu \Theta_{\mu\nu} m_\nu = \sum_\mu \sum_\nu \Theta_{\mu\nu} H_\nu m \tag{6}$$

oder

$$\Theta = \sum_\mu \sum_\nu \Theta_{\mu\nu} H_\nu. \tag{7}$$

Da man aus (6) oder (7) umgekehrt (5) zurückgewinnen kann, indem man m zu m_ν spezialisiert, und da durch (5) die Homomorphismen $\Theta_{\mu\nu}$ eindeutig bestimmt sind, so folgt, daß jeder Homomorphismus Θ eindeutig in der Gestalt (7) darstellbar ist.

Ist η ein zweiter Homomorphismus:

$$\eta = \sum_\mu \sum_\nu \eta_{\mu\nu} H_\nu,$$

so berechnen sich Summe und Produkt von η und Θ folgendermaßen:

$$\eta + \Theta = \sum_\mu \sum_\nu (\eta_{\mu\nu} + \Theta_{\mu\nu}) H_\nu,$$

$$\begin{aligned} \eta\Theta &= \sum_\lambda \sum_\mu \eta_{\lambda\mu} H_\mu \sum_{\mu'} \sum_\nu \Theta_{\mu'\nu} H_\nu \\ &= \sum_\lambda \sum_\mu \eta_{\lambda\mu} \sum_\nu \Theta_{\mu\nu} H_\nu \text{*} \\ &= \sum_\lambda \sum_\nu \Big(\sum_\mu \eta_{\lambda\mu} \Theta_{\mu\nu}\Big) H_\nu. \end{aligned}$$

* Für $\mu \neq \mu'$ ist nämlich $H_\mu \Theta_{\mu'\nu} = 0$, weil jedes Element von $\mathfrak{M}_{\mu'}$ durch H_μ annulliert wird. Für $\mu = \mu'$ dagegen ist $H_\mu \Theta_{\mu'\nu} = \Theta_{\mu\nu}$, weil jedes Element von $\mathfrak{M}_\mu$ durch H_μ reproduziert wird.

Es ist also jedem Θ eine Matrix $(\Theta_{\mu\nu})$ zugeordnet, und der Summe und dem Produkt sind Summe und Produkt der zugeordneten Matrizes zugeordnet. Die Matrixelemente $\Theta_{\mu\nu}$ sind Null, wenn die Indizes μ und ν zu nichtisomorphen Moduln $\mathfrak{M}_\mu$ und $\mathfrak{M}_\nu$ gehören; sie sind beliebige Homomorphismen von $\mathfrak{M}_\nu$ in $\mathfrak{M}_\mu$, wenn $\mathfrak{M}_\mu$ und $\mathfrak{M}_\nu$ isomorph sind.

Teilen wir nun die Moduln $\mathfrak{M}_\lambda$ in Klassen isomorpher ein und numerieren sie so, daß z. B. $\mathfrak{M}_1, \ldots, \mathfrak{M}_h$ untereinander isomorph sind, ferner $\mathfrak{M}_{h+1}, \ldots, \mathfrak{M}_{h+k}$ untereinander isomorph sind usw., so „zerfallen" die Matrizes $(\Theta_{\mu\nu})$ offenbar in quadratische „Kästchen" von $h, k, \ldots$ Zeilen und Spalten so, daß außerhalb der „Kästchen" lauter Nullen stehen:

$$\begin{pmatrix} \Theta_{11} \ldots \Theta_{1h} & 0 \ldots & & \\ \vdots \quad \vdots & \vdots & & \\ \Theta_{h1} \ldots \Theta_{hh} & & & \\ 0 \ldots & \Theta_{h+1,h+1} \ldots \Theta_{h+1,h+k} & & \\ \vdots & \vdots \quad \vdots & & \\ & \Theta_{h+k,h+1} \ldots \Theta_{h+k,h+k} & & \\ & & \ddots & \\ & & & \ddots \end{pmatrix}$$

Schreibt man in das erste Kästchen beliebige Elemente, in alle weiteren überall Null, so erhält man einen Matrizenring $\mathfrak{A}_1$, der ein Unterring des ursprünglichen Matrizenringes $\mathfrak{A}$ ist; schreibt man ebenso überall außer im zweiten Kästchen Null, so erhält man einen Ring $\mathfrak{A}_2 \subseteq \mathfrak{A}$, usw. Es ist klar, daß jedes Element von $\mathfrak{A}$ eindeutig als Summe von Elementen aus $\mathfrak{A}_1, \mathfrak{A}_2, \ldots$ darstellbar ist und daß die Elemente von $\mathfrak{A}_1, \mathfrak{A}_2, \ldots$ sich gegenseitig annullieren. Das heißt also: *Der Ring $\mathfrak{A}$ ist direkte Summe der sich gegenseitig annullierenden Ringe $\mathfrak{A}_1, \mathfrak{A}_2, \ldots$.*

Um die Struktur von $\mathfrak{A}$ zu kennen, haben wir also nur noch die eines einzelnen $\mathfrak{A}_\lambda$, z. B. die von $\mathfrak{A}_1$, zu untersuchen. Den Elementen von $\mathfrak{A}_1$ sind die h-reihigen Matrizes

$$\begin{pmatrix} \Theta_{11} \ldots \Theta_{1h} \\ \vdots \quad \vdots \\ \Theta_{h1} \ldots \Theta_{hh} \end{pmatrix}$$

des ersten „Kästchens" zugeordnet.

Θ_{11} ist ein Element des Automorphismenkörpers K_1 von $\mathfrak{M}_1$. Die übrigen Elemente $\Theta_{\mu\nu}$ gehören diesem Körper nicht an, sondern stellen Homomorphismen von $\mathfrak{M}_\nu$ in $\mathfrak{M}_\mu$ dar. Wir können sie jedoch eindeutig auf die Elemente von K_1 abbilden, indem wir h feste 1-Isomorphismen

$$\Gamma_1, \ldots, \Gamma_h$$

wählen, welche $\mathfrak{M}_1, \ldots, \mathfrak{M}_h$ auf $\mathfrak{M}_1$ abbilden. Für Γ_1 wählen wir dabei den identischen Automorphismus. Ordnen wir nun jedem $\Theta_{\mu\nu}$ das entsprechende Element

$$\Theta'_{\mu\nu} = \Gamma_\mu \Theta_{\mu\nu} \Gamma_\nu^{-1} \tag{8}$$

zu, das zu K_1 gehört (denn Γ_ν^{-1} bildet $\mathfrak{M}_1$ auf $\mathfrak{M}_\nu$ ab, $\Theta_{\mu\nu}$ bildet $\mathfrak{M}_\nu$ in $\mathfrak{M}_\mu$ ab, und Γ_μ bildet $\mathfrak{M}_\mu$ wieder auf $\mathfrak{M}_1$ ab), so ist offensichtlich einer Summe $\eta_{\mu\nu} + \Theta_{\mu\nu}$ wieder die Summe $\eta'_{\mu\nu} + \Theta'_{\mu\nu}$ und einem sinnvollen Produkt $\eta_{\lambda\mu}\Theta_{\mu\nu}$* wieder das Produkt

$$\eta'_{\lambda\mu}\Theta'_{\mu\nu} = \Gamma_\lambda \eta_{\lambda\mu} \Gamma_\mu^{-1} \Gamma_\mu \Theta_{\mu\nu} \Gamma_\nu^{-1} = \Gamma_\lambda (\eta_{\lambda\mu}\Theta_{\mu\nu}) \Gamma_\nu^{-1}$$

zugeordnet. In dieser Weise entspricht also jeder Matrix $(\Theta_{\mu\nu})$ eineindeutig eine Matrix $(\Theta'_{\mu\nu})$ mit Elementen aus K_1, und den durch

$$\begin{cases} \sigma_{\mu\nu} = \eta_{\mu\nu} + \Theta_{\mu\nu}, \\ \pi_{\lambda\nu} = \sum \eta_{\lambda\mu}\Theta_{\mu\nu} \end{cases}$$

definierten Summen- und Produktmatrizen werden wieder Summen- und Produktmatrix zugeordnet. *Jedes* Element von K_1 läßt sich offenbar bei festen μ, ν und festen Γ_μ, Γ_ν in der Gestalt $\Theta'_{\mu\nu}$ im Sinne von (8) schreiben. *Somit ist* $\mathfrak{A}_1$ *isomorph dem Ring aller h-reihigen Matrizes mit Elementen aus dem Körper* K_1, *dem Automorphismenkörper des einfachen Moduls* $\mathfrak{M}_1$.

Aufgaben. 1. Ist ein vollständig reduzibles System von Matrizes

$$A = \begin{pmatrix} \boxed{\begin{matrix} A_1 & & \\ & A_1 & \\ & & \ddots \\ & & & A_1 \end{matrix}} & & \\ & \boxed{\begin{matrix} A_2 & & \\ & A_2 & \\ & & \ddots \\ & & & A_2 \end{matrix}} & \\ & & \ddots \end{pmatrix}$$

gegeben, wo die Matrizes A_1 im ersten Kästchen h untereinander äquivalente irreduzible Systeme durchlaufen, ebenso die A_2 im zweiten Kästchen k äquivalente Systeme, die aber zum System der A_1 nicht äquivalent sind, usw., so haben die mit dem System vertauschbaren

* Ein Produkt $\eta_{\lambda\mu}\Theta_{\mu'\nu}$ hat nämlich nur dann einen Sinn, wenn $\mu' = \mu$ ist; denn $\Theta_{\mu'\nu}$ bildet $\mathfrak{M}_\nu$ auf $\mathfrak{M}_{\mu'}$ ab, und $\eta_{\lambda\mu}$ muß daher $\mathfrak{M}_{\mu'}$ auf irgend etwas abbilden, wenn das Produkt einen Sinn haben soll.

Matrizes die Gestalt

$$T = \begin{pmatrix} \boxed{\begin{matrix} T_{11} & \cdots & T_{1h} \\ \vdots & & \vdots \\ T_{h1} & \cdots & T_{hh} \end{matrix}} & & \\ & \boxed{\begin{matrix} T_{h+1,h+1} & \cdots & T_{h+1,h+k} \\ \vdots & & \\ T_{h+k,h+1} & \cdots & T_{h+k,h+k} \end{matrix}} & \\ & & \ddots \end{pmatrix}$$

wo die T_{ik} im ersten Kästchen mit dem System der A_1 vertauschbar sind, die im zweiten Kästchen mit dem System der A_2, usw. Die Matrizes T_{11}, die mit dem irreduziblen System der A_1 vertauschbar sind, bilden einen Körper von endlichem Grad über dem Grundkörper K.

2. Ist der Grundkörper K algebraisch-abgeschlossen, so sind die Matrizes T_{11} von Aufg. 1, die mit einem irreduziblen Matrixsystem vertauschbar sind, nur die Vielfachen λE der Einheitsmatrix E.

§ 118. Struktur der vollständig reduziblen Ringe mit Einselement.

Es sei $\mathfrak{o}$ ein halbeinfacher Ring oder, was nach § 115 dasselbe ist, ein linksseitig vollständig reduzibler Ring mit Einselement. Als Modul, mit $\mathfrak{o}$ selbst als Linksmultiplikatorenbereich, ist $\mathfrak{o}$ direkte Summe von einfachen Moduln (Linksidealen):

$$\mathfrak{o} = \mathfrak{l}_1 + \mathfrak{l}_2 + \cdots + \mathfrak{l}_r.$$

Wir bilden nun den Automorphismenring dieses Moduls. Ist Γ ein Operatorautomorphismus, der das Einselement in das Element c überführt:

$$\Gamma 1 = c,$$

so führt Γ ein beliebiges Element a über in

$$\Gamma a = \Gamma(a \cdot 1) = a \cdot \Gamma 1 = ac.$$

Andererseits: Wenn man c beliebig wählt und jedes a von $\mathfrak{o}$ in ac überführt, so ist die Zuordnung ein Operatorhomomorphismus wegen

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

In dieser Weise ist eineindeutig jedem Element c ein Automorphismus Γ zugeordnet. Der Summe $c + d$ entspricht wieder die Summe $\Gamma + \Delta$; dem Produkt cd aber entspricht das umgekehrte Produkt $\Delta\Gamma$, denn es ist

$$a \cdot cd = ac \cdot d = \Delta(ac) = \Delta\Gamma a.$$

Zwei Ringe $\mathfrak{o}$ und $\mathfrak{o}'$, die so aufeinander eineindeutig abgebildet sind, daß der Summe $a + b$ die Summe $a' + b'$, dem Produkt $a \cdot b$

aber das umgekehrte Produkt $b' \cdot a'$ zugeordnet ist, nennen wir *invers-isomorph* oder kurz *invers* zueinander. Wir sehen also: Der Ring $\mathfrak{o}$ ist zu seinem Automorphismenring invers-isomorph.

Andererseits ist nach § 117 der Automorphismenring eines vollständig reduziblen Moduls isomorph einer direkten Summe von sich gegenseitig annullierenden Matrizenringen, deren Matrixelemente jeweils einem Körper (dem Automorphismenkörper eines einfachen Moduls) entnommen werden.

Der Ring $\mathfrak{o}$ ist also invers-isomorph einer direkten Summe von Matrizenringen, die sich gegenseitig annullieren.

Zu jedem Ring kann man bis auf Ringisomorphie eindeutig einen inversen Ring konstruieren, indem man jedem Ringelement a ein neues Symbol a' zuordnet und Summe und Produkt durch $a' + b' = (a + b)'$ und $a' \cdot b' = (b \cdot a)'$ definiert. Der inverse Ring eines Körpers ist offenbar wieder ein Körper. Zu einem Matrizenring in einem Körper K konstruiert man den inversen Ring, indem man von K zum inversen Körper K' und außerdem von jeder Matrix $(a'_{\lambda\mu})$ zur gespiegelten Matrix $(a'_{\mu\lambda})$ übergeht. — Schließlich ist der inverse Ring einer direkten Summe von Ringen die direkte Summe der inversen Ringe der Summanden. Mithin:

Der Ring $\mathfrak{o}$ ist eine direkte Summe von Ringen $\mathfrak{a}_\nu$, von denen jeder isomorph einem vollen Matrizenring in bezug auf einen Körper $\mathsf{K}^{(\nu)}$ ist und die sich gegenseitig annullieren. Es gibt so viele $\mathfrak{a}_\nu$, als es nichtisomorphe Linksideale $\mathfrak{l}_\nu$ in der direkten Summenzerlegung gibt.

Damit ist die Struktur der halbeinfachen Ringe vollständig aufgeklärt.

Wenn die $\mathfrak{a}_\nu$ sich gegenseitig annullieren, so sind sie Ideale in $\mathfrak{o}$. Ist also der Ring $\mathfrak{o}$ zweiseitig einfach, so kann es nur ein $\mathfrak{a}_\nu = \mathfrak{a}_1$ geben: *Ein linksseitig vollreduzibler, zweiseitig einfacher Ring mit Einselement ist isomorph einem vollen Matrizenring in bezug auf einen Körper. Alle minimalen Linksideale sind operatorisomorph.*

Umgekehrt gilt:

Der Ring $\mathfrak{o}$ der Matrizes n-ten Grades in bezug auf einen Körper K ist (zweiseitig) einfach und linksseitig vollständig reduzibel, und der Automorphismenring der minimalen Linksideale von $\mathfrak{o}$ ist invers-isomorph zu K.

Beweis: Es seien $c_{11}, \ldots, c_{1n}; \ldots; c_{n1}, \ldots, c_{nn}$ die Basiselemente des Matrizenringes (§ 112, a). Ferner sei $\mathfrak{a}$ ein zweiseitiges Ideal $\neq (0)$ und

$$a = \sum \gamma_{ik} c_{ik}$$

ein von 0 verschiedenes Element von $\mathfrak{a}$. Einer der Koeffizienten γ_{ik} muß von 0 verschieden sein; es sei etwa $\gamma_{23} \neq 0$. Dann gehört zu $\mathfrak{a}$ auch (für alle λ und μ) das Element

$$\begin{aligned} \gamma_{23}^{-1} c_{\lambda 2}\, a\, c_{3\mu} &= \gamma_{23}^{-1} \sum_{i,k} \gamma_{ik}\, c_{\lambda 2}\, c_{ik}\, c_{3\mu} \\ &= \gamma_{23}^{-1} \gamma_{23}\, c_{\lambda 2}\, c_{23}\, c_{3\mu} = c_{\lambda\mu}; \end{aligned}$$

d. h. $\mathfrak{a}$ enthält alle Basiselemente von $\mathfrak{o}$. Mithin ist $\mathfrak{a} = \mathfrak{o}$. Also ist $\mathfrak{o}$ ein einfacher Ring mit Einselement.

Der K-Modul $\mathfrak{l} = (c_{11}, c_{21}, \ldots, c_{n1})$ ist, wie man leicht einsieht, ein minimales Linksideal in $\mathfrak{o}$. Zunächst nämlich ist das Produkt eines beliebigen Basiselements c_{ik} von $\mathfrak{o}$ mit einem beliebigen Basiselement c_{l1} von $\mathfrak{l}$ entweder gleich 0 oder gleich c_{i1}, also stets wieder ein Element von $\mathfrak{l}$. Daß $\mathfrak{l}$ minimal ist, ergibt sich daraus, daß ein beliebiges Element $\alpha \neq 0$ von $\mathfrak{l}$ stets das ganze Ideal $\mathfrak{l}$ erzeugt. Ist nämlich

$$a = \sum \alpha_k c_{k1}$$

und ist etwa $\alpha_2 \neq 0$, so gehört zu den Linksvielfachen von a auch

$$\alpha_2^{-1} c_{j2}\, a = \alpha_2^{-1} \alpha_2 c_{j2} c_{21} = c_{j1} \qquad (j = 1, \ldots, n).$$

Genau so sieht man, daß allgemein $\mathfrak{l}_\nu = (c_{1\nu}, c_{2\nu}, \ldots, c_{n\nu})$ ein einfaches Linksideal in $\mathfrak{o}$ ist. Da $\mathfrak{o} = \mathfrak{l}_1 + \mathfrak{l}_2 + \cdots + \mathfrak{l}_n$ ist, ist $\mathfrak{o}$ links seitig vollständig reduzibel.

Bestimmen wir schließlich den Automorphismenkörper von $\mathfrak{l}$. Ein Operatorautomorphismus, der etwa c_{11} in

$$a = \sum \alpha_k c_{k1} \tag{1}$$

überführt, muß jedes $x \cdot c_{11}$ in $x \cdot a$ überführen, insbesondere also $c_{11}^2\ (= c_{11})$ in

$$c_{11}\, a = \sum \alpha_k c_{11} c_{k1} = \alpha_1 c_{11}.$$

Das muß wieder das Element a sein. In (1) fehlen also alle Glieder außer $\alpha_1 c_{11}$, und der Automorphismus führt $x \cdot c_{11}$ in $x \cdot \alpha_1 c_{11} = x c_{11} \cdot \alpha_1$ über. Der Automorphismus besteht also darin, daß die Elemente von $\mathfrak{l}$ (die ja sämtlich die Gestalt $x c_{11}$ haben) einfach von rechts mit α_1 multipliziert werden. Die Elemente α_1 des Körpers sind auf die zugehörigen Automorphismen invers-isomorph bezogen; also ist der Automorphismenkörper der minimalen Linksideale invers-isomorph zu K.

In derselben Weise kann man natürlich auch beweisen, daß der volle Matrixring über einem Körper K auch rechtsseitig vollreduzibel ist. Der Automorphismenkörper der minimalen Rechtsideale wird direkt-isomorph zu K. In Verbindung mit den Sätzen von § 116 folgt weiter, daß eine direkte Summe von sich gegenseitig annullierenden Matrixringen auch (links und rechts) vollständig reduzibel ist. Die Begriffe:

a) Ring ohne Radikal mit Minimalbedingung für Links- (oder Rechts-) Ideale;

b) linksseitig oder rechtsseitig vollständig reduzibler Ring mit Einselement;

c) direkte Summe von zweiseitig einfachen Idealen, deren jedes ringisomorph einem vollen Matrixring über einem Körper ist.

sind also *völlig gleichbedeutend*.

Den Ring der Matrizes n-ten Grades im Körper K bezeichnen wir fortan mit K_n, die Einheitsmatrix mit E. Wir behaupten: *Ist* Z *das Zentrum von* K, *so ist* $\mathsf{Z} \cdot E$ *das Zentrum von* K_n.

Beweis: Wenn eine Matrix

$$a = (\alpha_{ik}) = \sum \alpha_{ik} c_{ik}$$

zum Zentrum von K_n gehört, so muß sie insbesondere mit $c_{1\mu}$ vertauschbar sein; das ergibt:

$$c_{1\mu} \cdot \sum_{i,k} \alpha_{ik} c_{ik} = \sum_{i,k} \alpha_{ik} c_{ik} \cdot c_{1\mu},$$

$$\sum_{k} \alpha_{\mu k} c_{1k} = \sum_{i} \alpha_{i1} c_{i\mu}.$$

Vergleichung der Koeffizienten links und rechts ergibt:

$$\alpha_{\mu k} = 0 \quad \text{für} \quad \mu \neq k,$$

$$\alpha_{\mu\mu} = \alpha_{11}.$$

Daher wird

$$a = \begin{pmatrix} \alpha_{11} & & 0 \\ & \alpha_{11} & \\ & & \ddots \\ 0 & & \alpha_{11} \end{pmatrix} = \alpha_{11} \cdot E = \alpha \cdot E.$$

Damit weiter $a = \alpha \cdot E$ mit jedem $\beta \cdot E$ vertauschbar sei, muß α zum Zentrum von K gehören, q. e. d.

Bringt man dieses Resultat in Zusammenhang mit den Resultaten von § 116 und beachtet, daß die Zentren zweier invers-isomorpher Ringe offenbar im gewöhnlichen Sinne isomorph sind, so ergibt sich:

Das Zentrum eines halbeinfachen Ringes $\mathfrak{o}$ *ist eine direkte Summe von Körpern, die in den einzelnen zweiseitigen Komponenten von* $\mathfrak{o}$ *enthalten sind und in deren Matrizendarstellungen durch* $\mathsf{Z} \cdot E$ *dargestellt werden, wo* Z *das Zentrum des Automorphismenkörpers ist.*

Aufgaben. 1. Ein halbeinfaches hyperkomplexes System $\mathfrak{o}$ über einem algebraisch-abgeschlossenen Körper Ω ist direkte Summe von Matrizenringen in Ω.

2. Der Quaternionenring $(1, i, k, l)$ über einem Körper P der Charakteristik $\neq 2$ ist stets zweiseitig einfach und daher stets entweder ein Körper oder isomorph dem Ring aller zweireihigen Matrizes in P.

§ 119. Produkte von hyperkomplexen Systemen. Erweiterung des Grundkörpers.

Es seien $\mathfrak{o}_1 = (b_1, \ldots, b_n)$ und $\mathfrak{o}_2 = (c_1, \ldots, c_m)$ zwei hyperkomplexe Systeme über dem Grundkörper P. Unter dem *Produkt* $\mathfrak{o}_1 \times \mathfrak{o}_2$ versteht man das System

$$\mathfrak{o}_1 \times \mathfrak{o}_2 = (b_1 c_1, \ldots, b_\nu c_\mu, \ldots, b_n c_m),$$

wo die b_ν mit den c_μ vertauschbar sein sollen, also die Multiplikation durch

$$b_\lambda c_\mu \cdot b_\varrho c_\sigma = (b_\lambda b_\varrho)(c_\mu c_\sigma)$$

definiert wird.

Elemente des Produktsystems sind also die Summen

$$\sum\sum \alpha_{\lambda\mu} b_\lambda c_\mu .$$

Dafür kann man auch schreiben entweder

$$\sum b'_\mu c_\mu ,$$

wo die b'_μ beliebige Elemente von $\mathfrak{o}_1$ sind, oder

$$\sum b_\lambda c'_\lambda ,$$

wo die c'_λ beliebige Elemente von $\mathfrak{o}_2$ sind. Die erste dieser beiden Schreibarten zeigt, daß die Produktbildung von der Wahl der Basis von $\mathfrak{o}_1$ unabhängig ist; die zweite zeigt die Unabhängigkeit von der Basis von $\mathfrak{o}_2$.

Leicht einzusehen sind die Gleichungen

$$\mathfrak{o}_1 \times \mathfrak{o}_2 = \mathfrak{o}_2 \times \mathfrak{o}_1 ,$$
$$\mathfrak{o}_1 \times (\mathfrak{o}_2 \times \mathfrak{o}_3) = (\mathfrak{o}_1 \times \mathfrak{o}_2) \times \mathfrak{o}_3 .$$

Beachtenswert ist das Produkt aus einem System $\mathfrak{o}$ und einem kommutativen Körper endlichen Grades Λ über P; die Elemente dieses Produkts lassen sich nämlich, wenn $\mathfrak{o} = (b_1, \ldots, b_n)$ ist, in der Form

$$\lambda_1 b_1 + \cdots + \lambda_n b_n = b_1 \lambda_1 + \cdots + b_n \lambda_n \qquad (\lambda_i \in \Lambda)$$

schreiben, d. h. das Produkt $\Lambda \times \mathfrak{o}$ ist ein hyperkomplexes System mit denselben Basiselementen wie $\mathfrak{o}$, aber mit Λ statt P als Grundkörper. Man bezeichnet dieses System $\Lambda \times \mathfrak{o}$ auch mit $\mathfrak{o}_\Lambda$. Dasselbe Symbol $\mathfrak{o}_\Lambda$ wird im Sinne der letzten Auffassung auch im Fall unendlicher Erweiterungskörper Λ von P benutzt. Schließlich werden wir gelegentlich auch dann, wenn Λ ein hyperkomplexes System über P ist, das Symbol $\mathfrak{o}_\Lambda$ als gleichbedeutend mit $\Lambda \times \mathfrak{o}$ verwenden.

Bei einer solchen Erweiterung des Grundkörpers können wesentliche Eigenschaften des Systems $\mathfrak{o}$ verlorengehen; z. B. bleibt der Quaternionenkörper $(1, j, k, l)$ bei Erweiterung des rationalen Zahlkörpers Γ zu $\Gamma(i)$ kein Körper, sondern es kommen Nullteiler hinein:

$$j^2 + 1 = j^2 - i^2 = (j - i)(j + i) = 0 ,$$

und das System der Quaternionen über $\Gamma(i)$ wird isomorph einem Matrixsystem mit den Basiselementen

$$c_{11} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \qquad c_{12} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \qquad c_{21} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \qquad c_{22} = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix},$$

vermöge folgender Zuordnung:

$$1 \to \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = c_{11} + c_{22},$$

$$j \to \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = i(c_{11} - c_{22}),$$

$$k \to \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = c_{12} - c_{21},$$

$$l \to \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = i(c_{12} + c_{21}).$$

Wir wollen nun untersuchen, was sich bei einem einfachen hyperkomplexen System $\mathfrak{S}$ über die Struktur von $\mathfrak{S}_\Sigma$ schließen läßt. Wir beginnen mit dem Fall, daß $\mathfrak{S}$ und Σ beide *kommutative Körper* sind.

Ist $\mathfrak{S}$ ein separabler endlicher kommutativer Erweiterungskörper von P, so hat $\mathfrak{S}_\Sigma$ kein Radikal, wie auch der (kommutative) Erweiterungskörper Σ von P gewählt wird; ist dagegen $\mathfrak{S}$ inseparabel, so hat $\mathfrak{S}_\Sigma$ bei passender Wahl von Σ ein Radikal.

Beweis: Ist $\mathfrak{S}$ separabel, Θ ein primitives Element von $\mathfrak{S}$ (§ 34) und $\varphi(z)$ das irreduzible Polynom, dessen Nullstelle Θ ist, so ist, wenn n den Grad von $\varphi(z)$ bedeutet,

$$\mathfrak{S} = \mathsf{P}(\Theta) = \mathsf{P} + \mathsf{P}\,\Theta + \cdots + \mathsf{P}\,\Theta^{n-1} \cong \mathsf{P}[z]/(\varphi(z))$$

und daher nach Erweiterung des Grundkörpers

$$\mathfrak{S}_\Sigma = \Sigma + \Sigma\,\Theta + \cdots + \Sigma\,\Theta^{n-1} \cong \Sigma[z]/(\varphi(z)).$$

Da nun $\varphi(z)$ auch in $\Sigma[z]$ keinen mehrfachen Faktor hat, so gibt es kein Polynom $f(z)$, von dem eine Potenz $\equiv 0\,(\varphi(z))$ wäre, ohne daß $f(z)$ selbst $\equiv 0\,(\varphi(z))$ ist; d. h. es gibt in $\Sigma[z]/(\varphi(z))$ kein nilpotentes Element außer der Null. $\mathfrak{S}_\Sigma$ ist also ein Ring ohne Radikal[1].

Ist dagegen $\mathfrak{S}$ inseparabel und Θ ein inseparables Element von $\mathfrak{S}$, so hat $\mathfrak{S}$ den Unterkörper $\mathsf{P}(\Theta)$, und $\mathfrak{S}_\Sigma$ hat den Unterring $\Sigma(\Theta) \cong \Sigma[z]/(\varphi(z))$. Bei passender Wahl des Körpers Σ hat $\varphi(z)$ mehrfache Wurzeln in Σ, und es gibt in $\Sigma[z]$ ein Polynom $f(z) \not\equiv 0\,(\varphi(z))$, von dem eine Potenz $\equiv 0\,(\varphi(z))$ ist. Es gibt also ein nichtverschwindendes nilpotentes Element in $\Sigma[z]/(\varphi(z))$, also auch eines in $\Sigma(\Theta)$, und das letztere erzeugt ein nilpotentes Ideal in $\mathfrak{S}_\Sigma$. (In einem kommutativen Ring $\mathfrak{o}$ erzeugt nämlich jedes nilpotente Element r ein nilpotentes Ideal $r\mathfrak{o}$.) Damit ist der Satz bewiesen.

Gehen wir jetzt zu dem Fall über, daß $\mathfrak{S}$ ein nichtkommutativer Körper ist. In diesem Fall gilt der folgende Hilfssatz, aus dem wir nachher die Struktur von $\mathfrak{S}_\Sigma$ entnehmen werden:

Ist $\mathfrak{S}$ ein Körper endlichen Ranges über P mit Zentrum $\mathsf{Z} \supseteq \mathsf{P}$, ist weiter Σ ein hyperkomplexes System mit Einselement über P (speziell ein endlicher Erweiterungskörper von P) und setzt man $\mathfrak{o} = \mathfrak{S}_\Sigma$, $\mathfrak{Z} = \mathsf{Z}_\Sigma$, so wird jedes zweiseitige Ideal $\mathfrak{a}$ in $\mathfrak{o}$ von einem zweiseitigen Ideal in $\mathfrak{Z}$ erzeugt.

---

[1] Genauer ergibt sich die Struktur von $\mathfrak{S}_\Sigma$ aus § 85, Schluß: $\mathfrak{S}_\Sigma$ ist eine direkte Summe von Körpern $\mathfrak{S}_1, \ldots, \mathfrak{S}_r$, die den irreduziblen Faktoren $\varphi_1, \ldots, \varphi_r$ von $\varphi(z)$ in $\Sigma[z]$ entsprechen; es ist nämlich $\mathfrak{S}_\nu \cong \Sigma[z]/(\varphi_\nu(z))$. Ist insbesondere Σ algebraisch-abgeschlossen, so ist die Anzahl der Körper $\mathfrak{S}_\nu$, in die $\mathfrak{S}_\Sigma$ zerfällt, gleich dem Grad von $\varphi(z)$ oder dem Rang von $\mathfrak{S}$, und die Körper $\mathfrak{S}_\nu$ sind $\cong \Sigma$.

Beweis: Es sei

$$\Sigma = z_1 \mathsf{P} + \cdots + z_q \mathsf{P},$$

mithin

$$\mathfrak{o} = \mathfrak{S}_\Sigma = z_1 \mathfrak{S} + \cdots + z_q \mathfrak{S}.$$

Wir wollen nun mit Hilfe der $z_1, \ldots, z_q$ für jeden $\mathfrak{S}$-Modul $\mathfrak{a}$ in $\mathfrak{o}$ eine besonders normierte $\mathfrak{S}$-Basis $(l_1, \ldots, l_r)$ konstruieren.

Ist $\mathfrak{a} = a_1 \mathfrak{S} + \cdots + a_r \mathfrak{S}$ ein $\mathfrak{S}$-Modul vom Range r, so kann man nach § 28 $a_1, \ldots, a_r$ durch Hinzunahme einiger z_ν, etwa $z_{r+1}, \ldots, z_q$, zu einer $\mathfrak{S}$-Basis für $\mathfrak{o}$ ergänzen; jedes Element von $\mathfrak{o}$ ist dann modulo $\mathfrak{a}$ kongruent einer Linearform der $z_{r+1}, \ldots, z_q$ mit Koeffizienten aus $\mathfrak{S}$. Insbesondere ist für $i = 1, \ldots, r$

$$z_i \equiv \sum_{k=r+1}^{q} z_k \gamma_{ik} \pmod{\mathfrak{a}}, \qquad \gamma_{ik} \in \mathfrak{S}.$$

Setzt man

$$l_i = z_i - \sum_{k=r+1}^{q} z_k \gamma_{ik},$$

so sind die l_i linear-unabhängige Elemente von $\mathfrak{a}$ und bilden daher eine $\mathfrak{S}$-Basis für $\mathfrak{a}$:

$$\mathfrak{a} = l_1 \mathfrak{S} + \cdots + l_r \mathfrak{S}.$$

Diese Basis hat die Eigenschaft, daß für $d \in \mathfrak{a}$ aus einer Darstellung

$$d = \sum_{1}^{r} l_i \delta_i$$

folgt

$$d = \sum_{1}^{r} z_i \delta_i + \sum_{r+1}^{q} z_k \varepsilon_k$$

mit denselben Koeffizienten für $z_1, \ldots, z_r$ im letzteren Ausdruck wie für $l_1, \ldots, l_r$ im ersteren. Zwei Elemente von $\mathfrak{a}$, die in diesen ersten r Koeffizienten übereinstimmen, sind gleich.

Ist nun $\mathfrak{a}$ speziell ein zweiseitiges Ideal in $\mathfrak{o}$, so gehören mit l_i auch

$$\varkappa l_i = z_i \varkappa - \sum_{k=r+1}^{q} z_k \varkappa \gamma_{ik}$$

und

$$l_i \varkappa = z_i \varkappa - \sum_{k=r+1}^{q} z_k \gamma_{ik} \varkappa$$

zu $\mathfrak{a}$. Da die Koeffizienten von $z_1, \ldots, z_r$ in diesen beiden Ausdrücken gleich sind, so sind die Elemente $\varkappa l_i$ und $l_i \varkappa$ nach dem oben Bemerkten auch gleich. Vergleicht man nun die Koeffizienten von $z_{r+1}, \ldots, z_q$ in den beiden Ausdrücken, so findet man:

$$\varkappa \gamma_{ik} = \gamma_{ik} \varkappa.$$

Mithin gehören alle γ_{ik} zum Zentrum Z von $\mathfrak{S}$; demnach gehören die l_i zu $\mathsf{Z}_\Sigma = \mathfrak{Z}$. Also wird $\mathfrak{a}$ von dem $\mathfrak{Z}$-Ideal $(l_1, \ldots, l_r)$ erzeugt.

Zusatz. Der Satz gilt auch dann noch, wenn an Stelle von Σ ein unendlicher algebraischer Erweiterungskörper Ω genommen wird. Ist nämlich $\mathfrak{a}$ ein zweiseitiges Ideal in $\mathfrak{o} = \mathfrak{S}_\Omega$, so hat $\mathfrak{a}$ wie $\mathfrak{o}$ nur einen endlichen Rang über Ω, also eine endliche Basis. Die Basiselemente, ausgedrückt in der Form $\Sigma \omega_i \sigma_i (\omega_i \in \Omega, \sigma_i \in \mathfrak{S})$, enthalten je nur endlichviele ω_i, die also einen endlichen Unterkörper Σ von Ω erzeugen. $\mathfrak{a}$ wird also von einem Ideal in $\mathfrak{S}_\Sigma$ erzeugt, und man kann den vorigen Satz anwenden.

Ist das Zentrum Z von $\mathfrak{S}$ ein *separabler* Erweiterungskörper von P und ist Σ *wie vorhin ein (endlicher oder unendlicher) kommutativer algebraischer Erweiterungskörper*, so folgt aus dem Satz zunächst, daß $\mathfrak{S}_\Sigma$ ein *Ring ohne Radikal* ist; denn das

Radikal von $\mathfrak{S}_\Sigma$ muß, als zweiseitiges Ideal, von einem (nilpotenten) Ideal in $\mathfrak{Z}$ erzeugt werden, und $\mathfrak{Z} = \mathsf{Z}_\Sigma$ ist nach dem ersten Satz dieses Paragraphen ohne Radikal. Aber wir können noch genauer die Struktur von $\mathfrak{S}_\Sigma$ angeben. Zunächst ergibt sich leicht, daß $\mathfrak{Z} = \mathsf{Z}_\Sigma$ das Zentrum von $\mathfrak{S}_\Sigma$ ist. Die zweiseitige Zerlegung von $\mathfrak{S}_\Sigma$ ist also durch die Zerlegung von $\mathfrak{Z}$ bestimmt. Da Z_Σ in höchstens n Körper zerfällt, wo n der Rang von Z in bezug auf P ist, so erhält man das Ergebnis:

$\mathfrak{S}_\Sigma$ zerfällt in so viele zweiseitig einfache Komponenten wie das Zentrum Z_Σ, d. h. in höchstens so viele, als der Rang von Z in bezug auf P beträgt. Ist insbesondere Z selbst der Grundkörper ($\mathsf{Z} = \mathsf{P}$), so ist $\mathfrak{S}_\Sigma$ zweiseitig einfach, also isomorph einem vollen Matrizenring in einem Körper $\mathsf{K} \supseteq \mathsf{Z}$.

Wählt man speziell für Σ den algebraisch-abgeschlossenen Körper Ω über P (§ 60), so wird $\mathsf{K} = \Omega$, also $\mathfrak{S}_\Omega$ isomorph einem vollen Matrizenring (etwa von m-reihigen Matrizes) im Körper Ω (§ 118, Aufgabe 1). Der Rang von $\mathfrak{S}_\Omega$ in bezug auf Ω, und daher auch der von $\mathfrak{S}$ in bezug auf P ($= \mathsf{Z}$), ist gleich m^2, und man erhält das Ergebnis:

Ein Körper $\mathfrak{S}$ von endlichem Rang in bezug auf sein Zentrum Z hat als Rang stets ein volles Quadrat m^2 und geht bei Erweiterung von Z zum algebraisch-abgeschlossenen Körper Ω über in einen Matrizenring vom Grade m.

Man nennt m den *Index* des Körpers $\mathfrak{S}$.

Der Satz, daß alle zweiseitigen Ideale von $\mathfrak{S}_\Sigma$ durch die von Z_Σ erzeugt werden, gilt nach dem Obigen auch dann, wenn Σ ein *nicht*kommutativer Körper endlichen Ranges über P ist, dessen Elemente mit denen von P vertauschbar sind. Wir schreiben in diesem Falle lieber $\mathfrak{S} \times \Sigma$ statt $\mathfrak{S}_\Sigma$ und $\mathsf{Z} \times \Sigma$ statt Z_Σ. Ist Z' das Zentrum von Σ, so ergibt eine nochmalige Anwendung desselben Satzes, daß die zweiseitigen Ideale von $\mathsf{Z} \times \Sigma$ durch die von $\mathsf{Z} \times \mathsf{Z}'$ erzeugt werden. Man folgert wie vorhin, daß $\mathfrak{S} \times \Sigma$ (bei separablem Z oder Z') *kein Radikal hat und in genau so viele zweiseitig einfache Ideale zerfällt wie das Produkt $\mathsf{Z} \times \mathsf{Z}'$ der Zentren.*

Gehen wir jetzt von den Körpern zu den *einfachen Systemen $\mathfrak{S}$ mit Einselement* über. Ein solches System $\mathfrak{S}$ ist isomorph dem Ring aller Matrizes r-ten Grades in einem Körper K. Nennen wir diesen Ring kurz K_r. Dann beweisen wir die folgenden Isomorphien:

$$\mathsf{K}_r \simeq \mathsf{K} \times \mathsf{P}_r , \tag{1}$$

$$\mathsf{P}_r \times \mathsf{P}_s \cong \mathsf{P}_{rs} . \tag{2}$$

Formel (1) ergibt sich sofort aus der Darstellung aller Elemente von K_r in der Form $\sum c_{ij}\, \varkappa_{ij} = \sum c_{ij} (e \varkappa_{ij})$ mit $\varkappa_{ij} \in \mathsf{K}$, wo die c_{ij} mit den $\varkappa_{ij}$ vertauschbar sind und e die Einheitsmatrix r-ten Grades ist. Die $e\varkappa$ bilden einen Unterring $e\,\mathsf{K} \cong \mathsf{K}$, und die c_{ij} erzeugen einen Unterring $\cong \mathsf{P}_r$.

Formel (2) ergibt sich so: Wird P_r von den r^2 Größen c'_{ik} und P_s von den s^2 Größen c''_{jl} erzeugt, so wird $\mathsf{P}_r \times \mathsf{P}_s$ von den $r^2 s^2$ Größen

$$c_{ij,kl} = c'_{ik}\, c''_{jl}$$

erzeugt, die den Rechnungsregeln

$$c_{ij,kl} \cdot c_{mn,pq} = \begin{cases} 0, & \text{wenn } k \neq m \text{ oder } l \neq n \text{ ist,} \\ c_{ij,pq}, & \text{wenn } k = m,\ l = n \text{ ist,} \end{cases}$$

genügen. Numeriert man die rs möglichen Indexpaare ij mit einem Index α, der von 1 bis rs läuft, und ebenso die kl mit einem Index β, so gehen diese Rechnungsregeln über in

$$c_{\alpha\beta} \cdot c_{\gamma\delta} = \begin{cases} 0 & \text{für } \beta \neq \gamma, \\ c_{\alpha\delta} & \text{für } \beta = \gamma, \end{cases}$$

und man erkennt die Isomorphie zu P_{rs}.

Aus (1) folgt, wenn Σ ein Körper endlichen Ranges über P ist,

$$\mathfrak{S}_\Sigma \simeq \Sigma \times \mathsf{K}_r \cong \Sigma \times \mathsf{K} \times \mathsf{P}_r \cong \mathsf{K}_\Sigma \times \mathsf{P}_r. \tag{3}$$

Damit ist die Frage der Struktur von $\mathfrak{S}_\Sigma$ vollständig auf die der Struktur von K_Σ zurückgeführt. Ist das Zentrum von Σ separabel über P (oder speziell sogar $= \mathsf{P}$), wie wir jetzt annehmen wollen, so hat, wie wir früher sahen, K_Σ kein Radikal und zerfällt in zweiseitig einfache Ringe, also Matrizenringe, der Grade $r', r'', \ldots$:

$$\begin{aligned}
\mathsf{K}_\Sigma &\simeq \mathsf{K}'_{r'} + \mathsf{K}''_{r''} + \cdots, \\
\mathfrak{S}_\Sigma &\cong (\mathsf{K}'_{r'} + \mathsf{K}''_{r''} + \cdots) \times \mathsf{P}_r \simeq \mathsf{K}'_{r'} \times \mathsf{P}_r + \mathsf{K}''_{r''} \times \mathsf{P}_r + \cdots \\
&\simeq \mathsf{K}' \times \mathsf{P}_{r'} \times \mathsf{P}_r + \mathsf{K}'' \times \mathsf{P}_{r''} \times \mathsf{P}_r + \cdots \\
&\cong \mathsf{K}' \times \mathsf{P}_{r'r} + \mathsf{K}'' \times \mathsf{P}_{r''r} + \cdots \\
&\cong \mathsf{K}'_{r'r} + \mathsf{K}''_{r''r} + \cdots;
\end{aligned}$$

mithin ist auch $\mathfrak{S}_\Sigma$ wieder ein Ring ohne Radikal, der in genau so viele Matrizenringe zerfällt wie K_Σ, nur daß die Grade der Matrizes sich alle mit r multiplizieren.

Der wichtigste Fall ist der, daß als Grundkörper P das Zentrum Z von K genommen wird. In diesem Fall wird K_Σ nach dem Vorigen einfach, also

$$\mathsf{K}_\Sigma \cong \mathsf{K}'_{r'}$$

und daher

$$\mathfrak{S}_\Sigma \simeq \mathsf{K}'_{r'r};$$

mithin: *Ein einfacher Ring $\mathfrak{S} = \mathsf{K}$ bleibt bei algebraischer Erweiterung des Zentrums Z immer einfach. Geht der Körper K bei der Erweiterung über in einen Matrizenring vom Grade r' in einem Körper K', so geht $\mathfrak{S} = \mathsf{K}_r$ über in einen Matrizenring vom Grade $r'r$ im selben Körper K'.*

Wird der Körper Σ noch weiter erweitert, etwa zu $\mathsf{T} \supset \Sigma$, so kann K' eventuell noch weiter „zerfallen", d. h. in einen Matrizenring vom Grade $r'' > 1$ übergehen. Dann wird K_T ein Matrizenring vom Grade $r''r'$, und $\mathfrak{S}_\mathsf{T}$ einer vom Grade $r''r'r$. Bei fortschreitender Erweiterung werden also die Grade der Matrizenringe immer größer, bis man beim algebraisch-abgeschlossenen Körper Ω angelangt ist und einen Matrizenring in Ω selbst erhält. Die *„Zerfällung"* ist dann *vollständig*.

Im allgemeinen wird man, um die vollständige Zerfällung zu erreichen, nicht bis zum algebraisch-abgeschlossenen Körper Ω zu gehen brauchen, sondern es wird schon ein Unterkörper $\mathsf{T} \subset \Omega$ die Eigenschaft haben, daß sich K_T (und ebenso $\mathfrak{S}_\mathsf{T}$) in einen Matrizenring im Körper T selbst verwandelt. Bei der nachfolgenden Erweiterung zu Ω erhöht sich dann der Grad der Matrizes nicht mehr. Ein solcher Körper T heißt, ebenso wie Ω, ein *Zerfällungskörper* der Systeme K und $\mathfrak{S}$. Wir kommen auf die Zerfällungskörper später noch zurück.

Aufgaben. 1. Zur vollständigen Zerfällung eines einfachen Systems K_r reicht stets ein endlicher Erweiterungskörper des Zentrums aus.

2. Ein halbeinfaches hyperkomplexes System über einem vollkommenen Grundkörper P bleibt bei jeder Erweiterung dieses Grundkörpers halbeinfach.

Siebzehntes Kapitel.

Darstellungstheorie der Gruppen und hyperkomplexen Systeme.

§ 120. Problemstellung.

Es sei $\mathfrak{G}$ eine Gruppe. Unter einer *Darstellung von $\mathfrak{G}$ durch lineare Transformationen im Körper* K verstehen wir einen Gruppenhomomorphismus, durch den jedem Gruppenelement a eine lineare Trans-

formation A mit Koeffizienten aus K zugeordnet wird. Die Darstellung heißt *treu* oder *untreu*, je nachdem sie isomorph ist oder nicht.

Ebenso verstehen wir unter einer *Darstellung eines Ringes* $\mathfrak{o}$ *durch lineare Transformationen in* K einen Ringhomomorphismus $a \to A$ (wobei also nicht nur dem Produkt das Produkt, sondern auch der Summe die Summe entspricht). Ist schließlich der Ring $\mathfrak{o}$ ein *hyperkomplexes System* über einem Körper P, so verlangen wir von einer *Darstellung* außerdem, daß der Grundkörper P im Zentrum des Darstellungskörpers K enthalten ist und daß der Ringhomomorphismus außerdem ein Operatorhomomorphismus in bezug auf P ist, d. h. daß aus $a \to A$ folgt $a\varrho \to A\varrho$ für alle Elemente ϱ von P. Für den Darstellungsmodul $\mathfrak{M}$, der nach § 108 die Darstellung vermittelt, heißt das:

$$a\varrho \cdot m = am \cdot \varrho \quad \text{für} \quad m \in \mathfrak{M}.$$

Wir beschränken uns im folgenden meist, was die Darstellungen der Gruppen betrifft, auf endliche Gruppen $\mathfrak{G} = \{a_1, a_2, \ldots, a_h\}$ und, was die Ringe betrifft, auf die hyperkomplexen Systeme. Das Problem ist, alle Darstellungen zu finden und (wenn möglich) in irreduzible Bestandteile zu zerspalten. Wir bemerken nur, daß das Darstellungsproblem für *Gruppen* sofort auf das für *hyperkomplexe Systeme* zurückzuführen ist, indem man aus der Gruppe $\mathfrak{G}$ den „*Gruppenring*"

$$\mathfrak{o} = a_1 \mathsf{K} + \cdots + a_h \mathsf{K}$$

bildet, dessen Basiselemente die Elemente von $\mathfrak{G}$ sind. Ist $a_i \to A_i$ die Darstellung der Gruppe, so ist

$$\sum a_i \varkappa_i \to \sum A_i \varkappa_i$$

eine Darstellung des Systems $\mathfrak{o}$, sofern wenigstens der Darstellungskörper K als kommutativ vorausgesetzt wird. Der Summe entspricht nämlich offensichtlich die Summe, und dem Produkt

$$(\sum_i a_i \varkappa_i)(\sum_k a_k \lambda_k) = \sum_{ik} a_i a_k \varkappa_i \lambda_k$$

entspricht die Matrix

$$\sum\sum A_i A_k \varkappa_i \lambda_k = (\sum A_i \varkappa_i)(\sum A_k \lambda_k),$$

während dem Produkt $(\sum a_i \varkappa_i) \cdot \varrho$ wieder offensichtlich $(\sum A_i \varkappa_i) \cdot \varrho$ entspricht. Umgekehrt ordnet jede Darstellung des Gruppenrings $\mathfrak{o}$ im Körper K insbesondere den Basiselementen $a_1, \ldots, a_h$ gewisse lineare Transformationen zu, die in ihrer Gesamtheit eine Darstellung der Gruppe $\mathfrak{G}$ ergeben. Mithin:

Jede Darstellung einer endlichen Gruppe $\mathfrak{G}$ *in einem kommutativen Körper* K *wird durch eine Darstellung des Gruppenrings* $\mathfrak{o} = a_1 \mathsf{K} + \cdots + a_h \mathsf{K}$ *vermittelt.*

Von den Darstellungen hyperkomplexer Systeme suchen wir hauptsächlich die, bei denen der Darstellungskörper K mit dem Grundkörper P zusammenfällt. Der allgemeine Fall kann (wenigstens bei kommutativem K) darauf zurückgeführt werden, indem man den Grundkörper P

zu K erweitert, also das hyperkomplexe System $\mathfrak{o}$ zu $\mathfrak{o}_{\mathsf{K}}$ erweitert (§ 119). Sind in der ursprünglichen Darstellung den Basiselementen $b_1, \ldots, b_n$ von $\mathfrak{o}$ die Matrizes $B_1, \ldots, B_n$ von K zugeordnet, so kann man einem Element $\sum b_l \varkappa_l (\varkappa_l \in \mathsf{K})$ von $\mathfrak{o}_{\mathsf{K}}$ die Matrix $\sum B_l \varkappa_l$ zuordnen und dadurch die Darstellung von $\mathfrak{o}$ zu einer Darstellung von $\mathfrak{o}_{\mathsf{K}}$ erweitern. *Mithin wird jede Darstellung von* $\mathfrak{o}$ *in einem kommutativen Körper* K *durch eine Darstellung von* $\mathfrak{o}_{\mathsf{K}}$ *vermittelt.*

Eine weitere Einschränkung der Problemstellung ergibt sich, wenn wir voraussetzen, daß der Ring $\mathfrak{o}$ ein Einselement besitzt. Dann können wir immer annehmen, daß dieses Einselement 1 auch Einheitsoperator für den Darstellungsmodul ist, d. h. daß ihm in der Darstellung die Einheitsmatrix zugeordnet ist. Andernfalls nämlich wird nach § 104 der Darstellungsmodul eine direkte Summe $\mathfrak{M}_0 + \mathfrak{M}_1$, worin $\mathfrak{M}_0$ von $\mathfrak{o}$ annulliert wird, während für $\mathfrak{M}_1$ die 1 Einheitsoperator ist. Die Darstellung zerfällt mithin vollständig in zwei Bestandteile, deren erster aus lauter Nullmatrizes besteht, also uninteressant ist, und deren zweiter eine Darstellung liefert, bei der das Einselement Einheitsoperator wird.

Eine besonders wichtige Darstellung eines hyperkomplexen Systems $\mathfrak{o}$ ist die sogenannte *reguläre Darstellung*, die man erhält, indem man $\mathfrak{o}$ selbst als Darstellungsmodul ($\mathfrak{o}$-Links- und P-Rechtsmodul) auffaßt. Die Untermoduln sind die Linksideale, und die ausreduzierte Form der Darstellung wird durch eine Kompositionsreihe der Linksideale vermittelt. Die reguläre Darstellung ist vollständig reduzibel, wenn der Ring $\mathfrak{o}$ selbst vollständig reduzibel ist.

Bei allen Betrachtungen dieses Kapitels muß man den in § 108 erklärten Zusammenhang zwischen Darstellungen und Darstellungsmoduln stets gut im Auge behalten; nur so wird man die Beweise verstehen können.

§ 121. Darstellung hyperkomplexer Systeme.

Die Darstellungstheorie der hyperkomplexen Systeme beruht auf folgenden beiden Sätzen:

Satz 1. *Es sei* $\mathfrak{o}$ *ein (linksseitig) vollreduzibler Ring mit Einselement und* $\mathfrak{M}$ *ein endlicher* $\mathfrak{o}$*-(Links-)Modul. Der Untermodul* $\mathfrak{M}_0$*, der von* $\mathfrak{o}$ *annulliert wird, sei Null oder vollständig reduzibel. Dann ist* $\mathfrak{M}$ *vollständig reduzibel, und die irreduziblen Bestandteile werden entweder von* $\mathfrak{o}$ *annulliert oder sind isomorph minimalen Linksidealen von* $\mathfrak{o}$*. Dasselbe gilt, wenn für* $\mathfrak{M}$ *und* $\mathfrak{o}$ *ein Rechtsmultiplikatorenbereich* Ω *mit den üblichen Eigenschaften*

$$a\,m \cdot \varrho = a \cdot m\,\varrho = a\,\varrho \cdot m \quad \text{für} \quad a \in \mathfrak{o},\ m \in \mathfrak{M},\ \varrho \in \Omega$$

hinzugegeben ist.

Beweis: Daß man sich auf den Fall beschränken kann, wo das Einselement von $\mathfrak{o}$ Einheitsoperator ist, sahen wir schon. Ist nun

$$\mathfrak{o} = \mathfrak{l}_1 + \mathfrak{l}_2 + \cdots + \mathfrak{l}_r, \tag{1}$$

$$\mathfrak{M} = (m_1, \ldots, m_s) = (\mathfrak{o}\,m_1, \ldots, \mathfrak{o}\,m_s), \tag{2}$$

so folgt durch das Einsetzen von (1) in (2):

$$\mathfrak{M} = (\ldots, \mathfrak{l}_i m_k, \ldots). \tag{3}$$

Diejenigen unter den Moduln $\mathfrak{l}_i m_k$, die vom Nullmodul verschieden sind, sind isomorph den zugehörigen $\mathfrak{l}_i$ (vgl. § 115, Hilfssatz 1 und 2), also ebenfalls minimale $\mathfrak{o}$-Moduln. Jeder von ihnen hat also entweder mit der Summe der vorangehenden nur die Null gemein oder ist ganz darin enthalten. Läßt man aus der Summe (3) diejenigen $\mathfrak{l}_i m_k$, die in der Summe der vorangehenden schon enthalten sind, weg, so wird die Summe also direkt.

Bei der *Anwendung auf die Darstellungstheorie* der hyperkomplexen Systeme ist natürlich Ω der Koeffizientenkörper P und zugleich der Darstellungskörper, und $\mathfrak{M}$ ein Darstellungsmodul. Da jeder Darstellungsmodul endlich in Bezug auf P, also, wenn $\mathfrak{o}$ ein Einselement e besitzt, auch endlich in Bezug auf $e\,\mathsf{P} \leqq \mathfrak{o}$ ist[1], so ergibt sich *die vollständige Reduzibilität aller Darstellungen eines vollständig reduziblen hyperkomplexen Systems mit Einselement (oder eines Systems ohne Radikal).*

Die Linksideale $\mathfrak{l}_1, \ldots, \mathfrak{l}_r$ von $\mathfrak{o}$ kann man erhalten, indem man zunächst $\mathfrak{o}$ zweiseitig zerlegt:

$$\mathfrak{o} = \mathfrak{a}_1 + \cdots + \mathfrak{a}_s,$$

und dann die einfachen Ringe $\mathfrak{a}_\nu$ weiter in Linksideale aufspaltet. Die in einem $\mathfrak{a}_\nu$ enthaltenen $\mathfrak{l}_i$ werden von jedem $\mathfrak{a}_\mu$ mit $\mu \neq \nu$ annulliert. Folglich werden in der durch $\mathfrak{l}_i$ vermittelten Darstellung alle $\mathfrak{a}_\mu$ mit Ausnahme des einzigen Ideals $\mathfrak{a}_\nu$ durch Null dargestellt. Das Ideal $\mathfrak{a}_\nu$ besitzt bis auf Äquivalenz nur eine einzige irreduzible Darstellung; denn alle minimalen Linksideale von $\mathfrak{a}_\nu$ sind operatorisomorph. Weiter ist die Darstellung von $\mathfrak{a}_\nu$ sicher *treu*, da $\mathfrak{a}_\nu$ zweiseitig einfach ist. Die Darstellungen selbst werden wir nachher explizite aufstellen.

Die Umkehrung des Satzes 1 ist trivial: Wenn jeder endliche $\mathfrak{o}$-Modul vollständig reduzibel ist, so ist auch $\mathfrak{o}$ selbst vollständig reduzibel; denn $\mathfrak{o}$ ist ein endlicher $\mathfrak{o}$-Modul mit der Basis 1. Man hat also den Satz:

Ist $\mathfrak{o}$ ein hyperkomplexes System mit Einselement und sind alle Darstellungen des Systems $\mathfrak{o}$ vollständig reduzibel, so ist $\mathfrak{o}$ selbst vollständig reduzibel.

Während Satz 1 eine vollständige Übersicht über alle Darstellungen eines Systems ohne Radikal gibt, wird sich Satz 2 auf die *irreduziblen* Darstellungen eines Systems *mit* Radikal beziehen. Was für Matrixelemente bei einer *reduziblen* Darstellung außerhalb der irreduziblen Diagonalkästchen noch vorkommen können, darüber wird nichts ausgesagt.

Satz 2. *Ist $\mathfrak{o}$ ein Ring mit Maximal- und Minimalbedingung für Linksideale und $\mathfrak{c}$ das Radikal von $\mathfrak{o}$, so wird jeder irreduzible $\mathfrak{o}$-Modul $\mathfrak{M}$ entweder von $\mathfrak{o}$ annulliert, oder er wird einem einfachen Linksideal aus*

[1] und da der von $\mathfrak{o}$ annullierte Modul $\mathfrak{M}_0$ als endlicher P-Modul automatisch vollreduzibel ist.

dem Ring ohne Radikal $\mathfrak{o}/\mathfrak{c}$ *isomorph. Dasselbe gilt auch bei Anwesenheit eines Multiplikatorenbereichs* Ω *wie im Satz* 1.

Beweis: Es muß $\mathfrak{c}\mathfrak{M} = (0)$ sein, da sonst $\mathfrak{c}\mathfrak{M} = \mathfrak{M}$, also

$$\mathfrak{M} = \mathfrak{c}\mathfrak{M} = \mathfrak{c}^2\mathfrak{M} = \cdots = (0)$$

folgen würde. Daher kann man $\mathfrak{M}$ als $\mathfrak{o}/\mathfrak{c}$-Modul auffassen; denn alle Elemente einer Restklasse nach $\mathfrak{c}$ ergeben bei Multiplikation mit einem Element von $\mathfrak{M}$ dasselbe Produkt. Als Ring ohne Radikal besitzt $\mathfrak{o}/\mathfrak{c}$ ein Einselement und ist vollständig reduzibel. Nunmehr folgt unsere Behauptung aus Satz 1.

Als Spezialfall des Satzes 2 ergibt sich, daß die einfachen Kompositionsfaktoren von $\mathfrak{o}$ schon in der Kompositionsreihe von $\mathfrak{o}/\mathfrak{c}$ (oder von $\mathfrak{o}$ nach $\mathfrak{c}$) vorkommen.

Auf die Darstellungen angewandt, bedeutet Satz 2, daß *alle irreduziblen Darstellungen eines hyperkomplexen Systems* $\mathfrak{o}$ *schon in der regulären Darstellung (und sogar in der regulären Darstellung von* $\mathfrak{o}/\mathfrak{c}$*) enthalten sind.* Wiederum werden alle zweiseitig einfachen Komponenten von $\mathfrak{o}/\mathfrak{c}$ durch Null dargestellt, bis auf höchstens eine einzige, die treu dargestellt wird. Eine *irreduzible* Darstellung eines ganz beliebigen hyperkomplexen Systems ist also dem Wesen nach stets nur eine Darstellung eines *einfachen* Systems (wenn es nicht gar die Nulldarstellung ist, was wegen der Irreduzibilität nur bei Darstellungen ersten Grades vorkommen kann).

Die in Satz 1 und Satz 2 auftretenden irreduziblen Darstellungen werden durch die Linksideale einfacher Ringe vermittelt. Wir wollen nun für einfache hyperkomplexe Systeme diese irreduziblen Darstellungen explizite aufstellen.

Ein einfaches hyperkomplexes System $\mathfrak{o}$ mit Einselement ist nach § 118 stets einem vollen Matrizenring in einem Körper Λ isomorph, daher

$$\mathfrak{o} = c_{11}\Lambda + c_{12}\Lambda + \cdots + c_{nn}\Lambda.$$

Ein minimales Linksideal $\mathfrak{l}$ wird durch

$$\mathfrak{l} = c_{11}\Lambda + c_{21}\Lambda + \cdots + c_{n1}\Lambda$$

gegeben. Der Grundkörper P, in dem auch die Darstellung stattfinden soll, ist in Λ enthalten, und Λ hat einen endlichen Grad über P. Der Rang von $\mathfrak{o}$ ist nämlich offenbar das n^2-fache des Grades von Λ.

Wir betrachten zunächst den Fall $\Lambda = \mathsf{P}$. Dieser Fall muß z. B. immer dann eintreten, wenn P algebraisch-abgeschlossen ist. Die Basis $(c_{11}, c_{21}, \ldots, c_{n1})$ von $\mathfrak{l}$ kann dann zur expliziten Aufstellung der Matrizes der Darstellung dienen. Ist $a = \sum_{i,k=1}^{n} c_{ik}\alpha_{ik}$ ein Element von $\mathfrak{o}$, so ist

$$a\,c_{k1} = \sum_{i=1}^{n} c_{ik}c_{k1}\,\alpha_{ik} = \sum_{i=1}^{n} c_{i1}\,\alpha_{ik};$$

mithin ist in der durch $\mathfrak{l}$ *vermittelten Darstellung dem Element* a *die Matrix* (α_{ik}) *zugeordnet.* Die Isomorphie von $\mathfrak{o}$ zum vollen Matrixring der Ma-

trizes (α_{ik}) ist also gerade diejenige irreduzible Darstellung, die durch ein minimales Linksideal $\mathfrak{l}$ vermittelt wird. Das ist auch nicht zu verwundern, da wir ja bewiesen haben, daß es bis auf Äquivalenz nur *eine* irreduzible Darstellung geben kann.

Beachtenswert ist, daß in dem untersuchten Fall $\Lambda = \mathsf{P}$ die darstellenden Matrizes stets den *vollen* Matrizenring n-ten Grades bilden.

Ist das darzustellende System $\mathfrak{o}$ nur halbeinfach, mithin eine direkte Summe von einfachen Ringen $\mathfrak{a}_1 + \mathfrak{a}_2 + \cdots + \mathfrak{a}_s$, und das Linksideal $\mathfrak{l}$ etwa ein Linksideal in $\mathfrak{a}_\nu$, so hat man, um die durch $\mathfrak{l}$ vermittelte Darstellung eines Elements a zu finden, zunächst a als Summe $a_1 + a_2 + \cdots + a_s$ zu schreiben und dann das Glied a_ν durch die zugehörige Matrix (α_{ik}), die übrigen durch die Nullmatrix zu ersetzen; denn diese übrigen Glieder $a_1, \ldots, a_{\nu-1}, a_{\nu+1}, \ldots, a_s$ annullieren ja das Ideal $\mathfrak{l}$.

Dasselbe kann man auch noch so ausdrücken: Man führe im Ring $\mathfrak{a}_\nu$ die Matrixeinheiten $c_{ik}^{(\nu)}\,(i, k = 1, \ldots, n_\nu)$ ein und stelle jedes Element a von $\mathfrak{o}$ in der Form

$$a = \sum \alpha_{ik}^{(\nu)}\, c_{ik}^{(\nu)}$$

dar. Dann ist $(\alpha_{ik}^{(\nu)})$ die darstellende Matrix von a in der ν-ten irreduziblen Darstellung (die durch ein Linksideal von $\mathfrak{a}_\nu$ vermittelt wird).

Ist nun zweitens Λ ein echter Oberkörper von P:

$$\Lambda = \lambda_1 \mathsf{P} + \cdots + \lambda_r \mathsf{P},$$

so bilden wir zunächst die reguläre Darstellung von Λ in P, wobei jedem β aus Λ die durch

$$\beta \lambda_j = \sum \lambda_i \beta_{ij}, \qquad B = (\beta_{ij})$$

definierte Matrix B zugeordnet wird. Sodann bilden wir, wenn $\mathfrak{o}$ einfach ist,

$$\mathfrak{l} = c_{11}\Lambda + \cdots + c_{n1}\Lambda$$
$$= (c_{11}\lambda_1 \mathsf{P} + \cdots + c_{11}\lambda_r \mathsf{P}) + \cdots + (c_{n1}\lambda_1 \mathsf{P} + \cdots + c_{n1}\lambda_r \mathsf{P}).$$

Wenn wir mit Hilfe dieser Basis ein Element $\beta \cdot c_{ik}$ von $\mathfrak{o}$ darstellen, so erhalten wir:

$$\beta c_{ik} \to \begin{pmatrix} 0 & \ldots & 0 & \ldots & 0 \\ \vdots & & \vdots & & \vdots \\ 0 & \ldots & B & \ldots & 0 \\ \vdots & & \vdots & & \vdots \\ 0 & \ldots & 0 & \ldots & 0 \end{pmatrix},$$

wo die Nullen r-reihige Nullmatrizen darstellen und die Matrix B die k-te Stelle in der i-ten Matrizeszeile einnimmt. Daraus folgt durch Summation:

$$\sum_{i,k=1}^{n} \alpha_{ik}\, c_{ik} \to \begin{pmatrix} A_{11} & \ldots & A_{1n} \\ \vdots & & \vdots \\ A_{n1} & \ldots & A_{nn} \end{pmatrix},$$

wo die A_{ik} wieder die Matrizes sind, die den α_{ik} in der regulären Darstellung von A entsprechen.

Eine fast unmittelbare Folge unseres Ergebnisses, daß im Fall des algebraisch-abgeschlossenen Körpers der Ring der darstellenden Matrizes stets der volle Matrizenring ist, ist der *Satz von* BURNSIDE. Versteht man unter einem *absolut-irreduziblen* System von Matrizes (im kommutativen Körper K) ein solches System, das bei jeder algebraischen Erweiterung des Körpers K irreduzibel bleibt, so kann man den Burnsideschen Satz so formulieren:

Ein absolut-irreduzibles System $\mathfrak{S}$ von Matrizes n-ten Grades, das mit je zwei Matrizes auch deren Produkt enthält, enthält genau n^2 linear-unabhängige Matrizes.

Beweis: Ist Ω der algebraisch-abgeschlossene algebraische Erweiterungskörper von K, so bleibt das System $\mathfrak{S}$ auch in Ω irreduzibel. Nimmt man zu den Matrizes A_i von $\mathfrak{S}$ noch alle Linearkombinationen $\sum A_i \omega_i$ ($\omega_i \in \Omega$) hinzu, so wird das erweiterte System $\mathfrak{S}'$ ein Ring mit dem Körper Ω als Operatorenbereich. Da es im ganzen höchstens n^2 linear-unabhängige Matrizes geben kann, so hat das erweiterte System endlichen Rang über Ω. Es ist also ein hyperkomplexes System und bildet eine Darstellung von sich selbst ($A \to A$). Eine irreduzible Darstellung eines hyperkomplexen Systems in dessen Grundkörper ist aber nach Satz 2 immer eine Darstellung eines Systems ohne Radikal und nach Satz 1 sogar eines einfachen Systems. In einer solchen Darstellung kommen aber bei algebraisch-abgeschlossenem Grundkörper stets n^2 linear-unabhängige Matrizes vor: das System $\mathfrak{S}'$ ist der volle Matrizenring.

Aufgaben. 1. Man bestimme alle irreduziblen Darstellungen des in § 114, Aufgabe 2 genannten hyperkomplexen Systems.

2. Ist das irreduzible System $\mathfrak{S}$ von Matrizen, das im Burnsideschen Satz vorkommt, ein Ring, so ist es ein Ring ohne Radikal. [Hätte $\mathfrak{S}$ ein Radikal, so hätte $\mathfrak{S}'$ auch eins.]

3. Erfüllt der in Aufgabe 2 vorkommende Ring $\mathfrak{S}$ noch die Minimalbedingung für Linksideale, so ist $\mathfrak{S}$ ein einfacher Ring. [Wäre $\mathfrak{S}$ nicht einfach, so wäre $\mathfrak{S} = \mathfrak{a}_1 + \mathfrak{a}_2$ mit $\mathfrak{a}_1\mathfrak{a}_2 = (0)$, und eine entsprechende Zerlegung würde demnach für $\mathfrak{S}'$ bestehen.]

4. *Verallgemeinerung des Burnsideschen Satzes.* Ein vollständig reduzibles System von Matrizes im algebraisch-abgeschlossenen Körper Ω, welches mit je zwei Matrizes auch deren Produkte enthält und dessen irreduzible Bestandteile, äquivalente nur einmal gezählt, die Grade $n_1, n_2, \ldots, n_s$ haben, enthält genau

$$n_1^2 + n_2^2 + \cdots + n_s^2$$

linear-unabhängige Matrizes.

5. Sind $n_1, \ldots, n_s$ die Grade der Matrizenringe $\mathfrak{a}_1, \ldots, \mathfrak{a}_s$, in die ein System ohne Radikal $\mathfrak{o}$ zerfällt, und sind $r_1, \ldots, r_s$ die Rang-

zahlen der Automorphismenkörper der Linksideale von $\mathfrak{a}_1, \ldots, \mathfrak{a}_s$, schließlich $\mathfrak{D}_1, \ldots, \mathfrak{D}_s$ die durch diese Linksideale vermittelten irreduziblen Darstellungen, so ist

$$h = \sum_{\nu=1}^{s} n_\nu^2 r_\nu$$

der Rang von $\mathfrak{o}$ und

$$g_\nu = n_\nu r_\nu$$

der Grad der Darstellung $\mathfrak{D}_\nu$. Die reguläre Darstellung enthält bei der Reduktion die Darstellung $\mathfrak{D}_\nu$ genau n_ν-mal. Bei algebraisch-abgeschlossenem Grundkörper wird $r_\nu = 1$, mithin

$$h = \sum_{\nu=1}^{s} n_\nu^2, \qquad g_\nu = n_\nu.$$

6. Ist P algebraisch-abgeschlossen und $\mathfrak{o}$ ein System mit Radikal, so enthält die reguläre Darstellung eine jede irreduzible Darstellung mindestens so oft, wie der Grad der Darstellung beträgt. Der Rang von $\mathfrak{o}$ ist größer als die Summe der Quadrate der Grade der Darstellungen. [Diese ist nämlich gleich dem Rang von $\mathfrak{o}/\mathfrak{c}$.]

7. Eine absolut-irreduzible Darstellung eines Ringes bleibt auch dann irreduzibel, wenn man eine transzendente Erweiterung des Grundkörpers vornimmt. [Folgt aus dem Satz von BURNSIDE.]

8. Entsprechen den Basiselementen $a_1, \ldots, a_n$ eines hyperkomplexen Systems $\mathfrak{o}$ in einer Darstellung die Matrizes $A_1, \ldots, A_n$ und bildet man mit Hilfe der Unbestimmten $x_1, \ldots, x_n$ (die dem Grundkörper Ω adjungiert werden) das „allgemeine Element" $x_1 a_1 + \cdots + x_n a_n$ und dessen Darstellung $A_x = x_1 A_1 + \cdots + x_n A_n$, so ist die Determinante der Matrix A_x eine Funktion von $x_1, \ldots, x_n$, welche

a) irreduzibel ist für eine absolut-irreduzible Darstellung,

b) gleich ist für zwei äquivalente irreduzible Darstellungen, ungleich aber für zwei inäquivalente,

c) in irreduzible Faktoren zerfällt, die den irreduziblen Bestandteilen der Darstellung entsprechen.

[Man wähle die c_{ik}, eventuell zusammen mit einer Basis des Radikals, als neue Basiselemente und transformiere A_x entsprechend.]

§ 122. Die Darstellungen des Zentrums.

Das Zentrum eines hyperkomplexen Systems $\mathfrak{o}$ muß bei einer irreduziblen Darstellung durch solche Matrizes abgebildet werden, die mit allen Matrizes der Darstellung vertauschbar sind. Ist der Grundkörper algebraisch-abgeschlossen, also der Ring der darstellenden Matrizes ein voller Matrizenring, so besteht dessen Zentrum nur aus den Vielfachen der Einheitsmatrix: λE_n; das Zentrum von $\mathfrak{o}$ wird also durch

Matrizes von der Form λE_n dargestellt. Dasselbe gilt überhaupt für absolut-irreduzible Darstellungen, da man bei diesen zum algebraisch-abgeschlossenen Grundkörper übergehen kann, ohne die Irreduzibilität zu zerstören. Also: *Bei einer absolut-irreduziblen Darstellung eines hyperkomplexen Systems* $\mathfrak{o}$ *werden die Zentrumselemente durch Vielfache der Einheitsmatrix dargestellt.*

Ist das System $\mathfrak{o}$ selbst kommutativ, also sein eigenes Zentrum, so haben alle darstellenden Matrizes einer absolut-irreduziblen Darstellung die Form λE_n. Aus der Irreduzibilität folgt dann, daß die Darstellungen vom ersten Grad sein müssen. Also: *Die absolut-irreduziblen Darstellungen eines kommutativen hyperkomplexen Systems sind vom ersten Grade.*

Eine Darstellung ersten Grades von $\mathfrak{o}$ ist eine homomorphe Abbildung von $\mathfrak{o}$ im Darstellungskörper K. Ist K kommutativ, so sind zwei äquivalente Darstellungen 1. Grades überhaupt gleich; denn wenn A eine Matrix der Darstellung, λ ein Element von K ist, so ist

$$\lambda^{-1} A \lambda = A .$$

Daraus folgt: *Die Anzahl der inäquivalenten Darstellungen* 1. *Grades eines kommutativen hyperkomplexen Systems* $\mathfrak{o}$ *im kommutativen Körper* K *ist gleich der Anzahl der verschiedenen Homomorphismen von* $\mathfrak{o}$ *in* K.

Kehren wir zu den nichtkommutativen Systemen zurück und setzen $\mathfrak{o}$ als System ohne Radikal voraus. Dann ist $\mathfrak{o}$ direkte Summe von einfachen Systemen:

$$\mathfrak{o} = \mathfrak{a}_1 + \cdots + \mathfrak{a}_s ,$$

und das Zentrum $\mathfrak{Z}$ von $\mathfrak{o}$ ist Summe von genau so vielen Körpern:

$$\mathfrak{Z} = \mathfrak{Z}_1 + \cdots + \mathfrak{Z}_s \quad (\mathfrak{Z}_\nu \text{ Zentrum von } \mathfrak{a}_\nu).$$

Die Anzahl der inäquivalenten irreduziblen Darstellungen von $\mathfrak{o}$ und ebenso von $\mathfrak{Z}$ ist gleich der Anzahl s der zweiseitigen Komponenten von $\mathfrak{o}$ oder $\mathfrak{Z}$; denn jede solche Darstellung $\mathfrak{D}_\nu$ von $\mathfrak{o}$ wird durch ein Linksideal von $\mathfrak{a}_\nu$ vermittelt, und jede solche Darstellung $\mathfrak{D}'_\nu$ von $\mathfrak{Z}$ wird durch ein $\mathfrak{Z}_\nu$ vermittelt. *Daher gibt es genau so viele inäquivalente irreduzible Darstellungen von* $\mathfrak{o}$ *wie von* $\mathfrak{Z}$, *und jeder irreduziblen Darstellung* $\mathfrak{D}_\nu$ *von* $\mathfrak{o}$, *bei der alle* $\mathfrak{a}_1, \ldots, \mathfrak{a}_s$ *mit Ausnahme von* $\mathfrak{a}_\nu$ *durch Null dargestellt werden, kann eine Darstellung* $\mathfrak{D}'_\nu$ *von* $\mathfrak{Z}$ *zugeordnet werden, bei der alle* $\mathfrak{Z}_1, \ldots, \mathfrak{Z}_s$ *mit Ausnahme von* $\mathfrak{Z}_\nu$ *durch Null dargestellt werden.*

Ist insbesondere der Grundkörper P algebraisch-abgeschlossen, so sind die Körper $\mathfrak{Z}_\nu$ vom Rang 1 und isomorph zu P; somit wird in diesem Fall *die Anzahl* s *der irreduziblen Darstellungen von* $\mathfrak{o}$ *gleich dem Rang des Zentrums* $\mathfrak{Z}$. Daraus, daß die $\mathfrak{Z}_\nu$ P-Moduln vom Rang 1 sind, folgt von neuem, daß die irreduziblen Darstellungen von $\mathfrak{Z}$ vom 1. Grade sind.

Die Beziehungen zwischen den irreduziblen Darstellungen $\mathfrak{D}_\nu$ von $\mathfrak{o}$ und den irreduziblen Darstellungen (ersten Grades) von $\mathfrak{Z}$ sind in diesem Fall ganz einfach. Bei der Darstellung $\mathfrak{D}_\nu$ wird nämlich jedes Zentrums-

element a durch eine Matrix von der Form αE_{n_ν} dargestellt, wo E_{n_ν} die Einheitsmatrix n_ν-ten Grades bedeutet. Zu jedem a gehört so (bei gegebenem ν) ein bestimmtes α, und wir können schreiben:

$$\alpha = \Theta_\nu(a).$$

Die Funktion Θ_ν vermittelt einen Homomorphismus des Zentrums, d. h. es ist

$$\Theta_\nu(a+b) = \Theta_\nu(a) + \Theta_\nu(b),$$
$$\Theta_\nu(ab) = \Theta_\nu(a)\,\Theta_\nu(b),$$
$$\Theta_\nu(a\lambda) = \Theta_\nu(a)\,\lambda.$$

Bei diesem Homomorphismus werden alle $\mathfrak{Z}_1, \ldots, \mathfrak{Z}_s$ mit Ausnahme von $\mathfrak{Z}_\nu$ durch Null dargestellt; d. h. der Homomorphismus Θ_ν ist genau die früher mit $\mathfrak{D}'_\nu$ bezeichnete Darstellung ersten Grades des Zentrums.

Die Darstellung Θ_ν ist bekannt, sobald eine P-Basis für den Modul $\mathfrak{Z}_\nu$ bekannt ist, und als solche kann man das Einselement e_ν des Körpers $\mathfrak{Z}_\nu$ wählen. Schreibt man jedes Element a von $\mathfrak{Z}$ in der Form

$$a = \sum_{\nu=1}^{s} e_\nu \lambda_\nu, \tag{1}$$

so wird

$$a e_\nu = e_\nu^2 \lambda_\nu = e_\nu \lambda_\nu;$$

mithin wird $\lambda_\nu E_{n_\nu}$ die darstellende Matrix:

$$\Theta_\nu(a) = \lambda_\nu.$$

Für (1) können wir jetzt auch schreiben:

$$a = \sum_{\nu=1}^{s} e_\nu \Theta_\nu(a); \tag{2}$$

in Worten: *Die Entwicklungskoeffizienten $\Theta_\nu(a)$ eines Zentrumselementes a nach den idempotenten Elementen e_ν des Zentrums ergeben zugleich die Homomorphismen oder Darstellungen ersten Grades des Zentrums.*

Aufgaben. 1. Die Anzahl der Darstellungen ersten Grades eines kommutativen hyperkomplexen Systems $\mathfrak{o}$ im algebraisch-abgeschlossenen Erweiterungskörper Ω von P ist gleich dem Rang von $\mathfrak{o}_\Omega/\mathfrak{c}$, wo $\mathfrak{c}$ das Radikal von $\mathfrak{o}_\Omega$ ist.

2. Ist K ein kommutativer Körper über P, so ist die Anzahl der Darstellungen ersten Grades von K in Ω gleich dem reduzierten Körpergrad von K über P. Es ist $\mathfrak{c} = (0)$ dann und nur dann, wenn K separabel über P ist.

3. Der Grad der irreduziblen Darstellung $\mathfrak{D}'_\nu$ von $\mathfrak{Z}$ ist gleich dem Rang von $\mathfrak{Z}_\nu$ über P. In der Darstellung $\mathfrak{D}_\nu$ von $\mathfrak{Z}$ ist die Darstellung $\mathfrak{D}_\nu$ genau $n_\nu t_\nu$-mal enthalten, wobei sich n_ν und t_ν folgendermaßen bestimmen: $\mathfrak{a}_\nu$ ist ein voller Matrizenring n_ν-ten Grades mit Matrixelementen aus einem Körper K_ν, und t_ν ist der Grad von K_ν in bezug auf dessen Zentrum $\mathfrak{Z}_\nu$.

§ 123. Spuren und Charaktere.

Unter der *Spur des Elements a in der Darstellung $\mathfrak{D}$*, geschrieben

$$S_{\mathfrak{D}}(a) \quad \text{oder kurz} \quad S(a),$$

verstehen wir die Spur $S(A)$ der darstellenden Matrix A von a in der Darstellung $\mathfrak{D}$. Die Spur $S_{\mathfrak{D}}$, für feste $\mathfrak{D}$ als Funktion des Elements a betrachtet, heißt auch die *Spur der Darstellung* $\mathfrak{D}$.

Auf Grund der Relation

$$S(P^{-1}AP) = S(A)$$

haben äquivalente Darstellungen dieselben Spuren.

Die Spuren sind *lineare Funktionen*, d. h. es ist

$$S(a+b) = S(a) + S(b),$$
$$S(a\lambda) = S(a)\lambda.$$

Die Spuren der absolut-irreduziblen Darstellungen (oder, was dasselbe ist, die Spuren der irreduziblen Darstellungen im algebraisch-abgeschlossenen Körper Ω) heißen *Charaktere*[1]. Der Charakter eines Elements a in der ν-ten irreduziblen Darstellung $\mathfrak{D}_\nu$ wird mit

$$\chi_\nu(a)$$

bezeichnet. Der Index ν wird, wenn von einer festen Darstellung die Rede ist, gelegentlich auch weggelassen.

Bei einer absolut-irreduziblen Darstellung $\mathfrak{D}_\nu$ vom Grad n_ν werden die Zentrumselemente z nach §122 durch Diagonalmatrizes $E_{n_\nu} \cdot \Theta_\nu(z)$ dargestellt, wo Θ_ν ein Homomorphismus des Zentrums im Körper Ω ist. Die Spur der Matrix $E_{n_\nu} \cdot \Theta_\nu(z)$ ist

$$\chi_\nu(z) = n_\nu \cdot \Theta_\nu(z). \tag{1}$$

Insbesondere wird das Einselement von $\mathfrak{o}$ durch die Einheitsmatrix E_{n_ν} dargestellt, deren Spur gleich n_ν ist:

$$\chi_\nu(1) = n_\nu.$$

Wir setzen im folgenden voraus, daß die Grade n_ν der absolut-irreduziblen Darstellungen nicht durch die Charakteristik des Körpers Ω teilbar sind. Dann kann man (1) durch n_ν dividieren und erhält:

$$\Theta_\nu(z) = \frac{\chi_\nu(z)}{n_\nu}. \tag{2}$$

In dieser Weise drücken sich die Homomorphismen des Zentrums durch die Charaktere aus.

[1] Die meisten neueren Autoren benutzen das Wort Charaktere auch für reduzible Darstellungen und reden dann von „zusammengesetzten Charakteren". Diese Bezeichnung ist hier vermieden, weil sie im Spezialfall der Abelschen Gruppen nicht die von alters her übliche Bedeutung des Wortes „Charakter" (vgl. § 124) ergibt, und weil außerdem das Wort „Spur" (der Darstellung) ebenso deutlich das Gemeinte bezeichnet.

Satz. *Eine vollständig reduzible Darstellung eines hyperkomplexen Systems* $\mathfrak{o}$ *im Körper* Ω *der Charakteristik* 0 *ist bis auf Äquivalenz durch die Spuren der darstellenden Matrizen allein schon eindeutig bestimmt.*

Beweis: Ist $\mathfrak{c}$ das Radikal von $\mathfrak{o}$, so ist jede vollständig reduzible Darstellung von $\mathfrak{o}$ zugleich eine solche von $\mathfrak{o}/\mathfrak{c}$. Nach Annahme sind die Spuren der Matrizes, welche die Elemente von $\mathfrak{o}/\mathfrak{c}$ darstellen, bekannt. Es sei

$$\mathfrak{o}/\mathfrak{c} = \mathfrak{a}_1 + \cdots + \mathfrak{a}_n;$$

die Einselemente von $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ seien $e_1, \ldots, e_n$. Dann wird in der irreduziblen Darstellung $\mathfrak{D}_\nu$ das Element e_ν durch die n_ν-reihige Einheitsmatrix dargestellt; mithin ist die zugehörige Spur

$$S_\nu(e_\nu) = n_\nu,$$

dagegen

$$S_\nu(e_\mu) = 0 \quad \text{für} \quad \mu \neq \nu.$$

Nun ist eine vollständig reduzible Darstellung bekannt, sobald man weiß, wie oft jede irreduzible Darstellung $\mathfrak{D}_\nu$ in ihr vorkommt. Kommt die Darstellung $\mathfrak{D}_\nu$ etwa q_ν-mal vor, so besteht die Darstellung aus q_1 Kästchen $\mathfrak{D}_1$, q_2 Kästchen $\mathfrak{D}_2$ usw. Die Spur von e_ν in dieser Darstellung ist dann

$$S(e_\nu) = q_\nu n_\nu. \tag{3}$$

Aus (3) kann man die q_ν berechnen, sobald alle Spuren $S(e_\nu)$ bekannt sind. Damit ist der Satz bewiesen.

Bemerkung: Die Spuren aller Elemente von $\mathfrak{o}$ sind bekannt, sobald die Spuren der Basiselemente von $\mathfrak{o}$ bekannt sind. Man braucht also z. B., wenn $\mathfrak{o}$ der Gruppenring einer endlichen Gruppe ist, nur die Spuren der Gruppenelemente zu kennen, und die Darstellung ist schon bestimmt. Also:

Eine vollständig reduzible Darstellung einer endlichen Gruppe ist durch die Spuren der Gruppenelemente bis auf Äquivalenz vollständig bestimmt.

Sind $a_1, \ldots, a_n$ die Basiselemente eines Systems $\mathfrak{o}$ und $\chi_\nu(a_i)$ ihre Spuren bei den irreduziblen Darstellungen, so hat man für eine beliebige Darstellung:

$$S(a_i) = \sum_{\nu=1}^{s} q_\nu \chi_\nu(a_i). \tag{4}$$

Durch diese Gleichungen sind nach dem obigen Satz die Zahlen q_ν eindeutig bestimmt. Die Gleichungen (4) ergeben eine rechnerische Methode, durch alleinige Berechnung der Spuren eine gegebene vollreduzible Darstellung in irreduzible Bestandteile zu zerlegen. Allerdings müssen die Charaktere der irreduziblen Bestandteile vorher bekannt sein.

Aufgaben. 1. Bei einer nicht vollreduziblen Darstellung sind zwar nicht die Darstellungen selbst, aber doch die in ihnen vorkommenden

irreduziblen Diagonalkästchen (Kompositionsfaktoren des Darstellungsmoduls) durch die Spuren allein eindeutig bestimmt.

2. Eine vollständig reduzible Darstellung einer unendlichen Gruppe ist durch die Spuren allein bis auf Äquivalenz eindeutig bestimmt.

[Liegen irgend zwei Darstellungen von endlichem Grade mit gleichen Spuren vor, so kann man sie zu einer Darstellung aneinanderreihen und das System der darstellenden Matrizes zu einem Ring erweitern. Dieser Ring ist dann hyperkomplex, und man hat zwei Darstellungen eines hyperkomplexen Systems vor sich.]

§ 124. Darstellungen Abelscher Gruppen.

Ein schönes und einfaches Beispiel für die Darstellungstheorie bilden die endlichen Abelschen Gruppen.

Die Gruppe $\mathfrak{G}$ von der Ordnung h sei ein direktes Produkt von zyklischen Gruppen der Ordnungen $h_1, \ldots, h_r$, so daß jedes Element a von $\mathfrak{G}$ eindeutig in der Gestalt

$$a = c_1^{\lambda_1} c_2^{\lambda_2} \cdots c_r^{\lambda_r} \qquad (0 \leqq \lambda_1 < h_1,\ 0 \leqq \lambda_2 < h_2, \ldots, 0 \leqq \lambda_r < h_r)$$

darstellbar ist. Wir suchen die irreduziblen Darstellungen der Gruppe in einem algebraisch-abgeschlossenen Körper Ω, dessen Charakteristik Null ist oder wenigstens nicht in $h = h_1 h_2 \cdots h_r$ aufgeht.

Zunächst sind die irreduziblen Darstellungen *linear* (d.h. vom Grad 1). Es handelt sich also darum, jedem Gruppenelement a eine Zahl $\chi(a)$ aus Ω zuzuordnen, derart, daß die Homomorphiebedingung

$$\chi(a\,b) = \chi(a)\,\chi(b) \tag{1}$$

erfüllt ist. Eine solche Funktion χ heißt ein *Charakter* der Gruppe. (Diese Definition ist mit der in § 123 gegebenen allgemeineren in Einklang, da die Spur der Matrix (χ) gleich χ ist.)

Wir schließen die Nulldarstellung

$$\chi(a) = 0 \quad \text{für alle } a$$

von vornherein aus. Dann muß aber $\chi(1) = 1$ sein. Weiter ist

$$\chi(c_1^{\lambda_1} \cdots c_r^{\lambda_r}) = \chi(c_1)^{\lambda_1} \cdots \chi(c_r)^{\lambda_r},$$
$$\chi(c_\nu)^{h_\nu} = \chi(c_\nu^{h_\nu}) = \chi(1) = 1;$$

mithin ist $\chi(c_\nu)$ eine h_ν-te Einheitswurzel ζ_ν, und die Darstellung hat die Gestalt

$$\chi(c_1^{\lambda_1} \cdots c_r^{\lambda_r}) = \zeta_1^{\lambda_1} \cdots \zeta_r^{\lambda_r}. \tag{2}$$

Umgekehrt stellt die Gleichung (2) bei beliebiger Wahl der Einheitswurzeln $\zeta_1, \ldots, \zeta_r$ stets einen Homomorphismus der Gruppe $\mathfrak{G}$ dar. Für jede Einheitswurzel ζ_ν stehen h_ν Werte zur Verfügung; *im ganzen gibt es also*

$$h = h_1 h_2 \cdots h_r$$

verschiedene Charaktere, die ebenso viele inäquivalente Darstellungen ersten Grades vermitteln.

Wählt man alle $\zeta_\nu = 1$, so erhält man den „*Hauptcharakter*" χ_0:

$$\chi_0(a) = 1 .$$

Man kann hier sehr schön im einzelnen verfolgen, wie alle Darstellungen durch Ausreduzieren der regulären Darstellung (vgl. § 121) entstehen. Nehmen wir zunächst eine einzige zyklische Gruppe $\mathfrak{G}$ mit erzeugendem Element c; $c^h = 1$. Dann wird die reguläre Darstellung von c gegeben durch die lineare Transformation

$$c \cdot c^\lambda = c^{\lambda+1}, \qquad \text{im Vektorraum } (1, c, c^2, \ldots, c^{h-1}).$$

Um die Darstellung auszureduzieren, führt man die neuen Basiselemente

$$(\zeta, c) = 1 + \zeta c + \zeta^2 c^2 + \cdots + \zeta^{h-1} c^{h-1} \tag{3}$$

ein (vgl. die Lagrangeschen Resolventen in § 50), wo ζ die h h-ten Einheitswurzeln durchläuft. Daß diese tatsächlich eine Basis bilden, folgt daraus, daß die c^λ umgekehrt durch die (ζ, c) ausdrückbar sind. Multipliziert man nämlich (3) mit ζ^{-r} und summiert über alle ζ, so kommt:

$$\sum \zeta^{-r}(\zeta, c) = h\, c^r . \tag{4}$$

Weiter ist, wie man leicht nachrechnet,

$$c \cdot (\zeta, c) = \zeta^{-1} \cdot (\zeta, c); \tag{5}$$

mithin definiert jedes einzelne Basiselement (ζ, c) schon einen invarianten Unterraum: *die Darstellung ist vollständig reduzibel*, und die darstellende Matrix für c in einem einzelnen Unterraum heißt

$$(\chi(c)) = (\zeta^{-1}) .$$

ζ^{-1} durchläuft, wie ζ, alle h-ten Einheitswurzeln.

Bei einem direkten Produkt zyklischer Gruppen führt man an Stelle der Produkte $c_1^{\lambda_1} c_2^{\lambda_2} \cdots c_r^{\lambda_r}$ die neuen Basiselemente

$$(\zeta_1, \ldots, \zeta_r;\ c_1, \ldots, c_r) = (\zeta_1, c_1)\,(\zeta_2, c_2) \cdots (\zeta_r, c_r)$$

ein und findet als vollständig reduzierte Form der Darstellung:

$$c_\mu \cdot (\zeta_1, \ldots, \zeta_r;\ c_1, \ldots, c_r) = \zeta_\mu^{-1} (\zeta_1, \ldots, \zeta_r;\ c_1, \ldots, c_r),$$

mithin als irreduzible Darstellungen:

$$\chi(c_\mu) = \zeta_\mu^{-1},$$

$$\chi(c_1^{\lambda_1} c_2^{\lambda_2} \cdots c_r^{\lambda_r}) = \zeta_1^{-\lambda_1} \zeta_2^{-\lambda_2} \cdots \zeta_r^{-\lambda_r}.$$

Man sieht also:

Der mit Hilfe eines algebraisch-abgeschlossenen Körpers gebildete Gruppenring einer Abelschen Gruppe ist vollständig reduzibel und direkte Summe von h Körpern $\mathfrak{Z}_\nu$, die von den neuen Basisvektoren $(\zeta_1, \ldots, \zeta_r;\ c_1, \ldots, c_r)$ erzeugt werden, alles unter der Voraussetzung, daß die Charakteristik des Körpers nicht in der Gruppenordnung h aufgeht.

Die $(\zeta_1, \ldots, \zeta_r; c_1, \ldots, c_r)$ müssen also bis auf einen Faktor idempotent sein. In der Tat ergibt sich leicht

$$(\zeta_\nu, c_\nu)^2 = h_\nu (\zeta_\nu, c_\nu),$$

mithin

$$(\zeta_1, \ldots, \zeta_r; c_1, \ldots, c_r)^2 = h(\zeta_1, \ldots, \zeta_r; c_1, \ldots, c_r)$$

oder auch: das Element

$$\frac{1}{h}(\zeta_1, \ldots, \zeta_r; c_1, \ldots, c_r)$$

ist idempotent (und Einselement des Körpers $\mathfrak{Z}_\nu$).

Aus dem eben Bewiesenen folgt nach § 121, Satz 1, daß *jede Darstellung der Gruppe* $\mathfrak{G}$ *vollständig reduzibel ist.*

Zwischen den Charakteren besteht eine Reihe von Relationen, die man folgendermaßen findet: Zunächst ist das Produkt zweier Charaktere wieder ein Charakter:

$$\chi(a)\,\chi'(a) = \chi''(a), \tag{6}$$

und ebenso ist das Inverse eines Charakters ein Charakter. Somit *bilden die Charaktere eine Gruppe* $\mathfrak{H}$.

Ist ζ_ν eine primitive h_ν-te Einheitswurzel, so erzeugt der Charakter

$$\chi(c_1^{\lambda_1} \cdots c_r^{\lambda_r}) = \zeta_\nu^{\lambda_\nu}$$

eine zyklische Untergruppe $\mathfrak{H}_\nu$ der Ordnung h_ν in der Gruppe $\mathfrak{H}$. Man sieht leicht ein, daß die ganze Gruppe $\mathfrak{H}$ das direkte Produkt der Untergruppen $\mathfrak{H}_\nu$ ist. Somit ist die Gruppe $\mathfrak{H}$ genau so wie $\mathfrak{G}$ ein direktes Produkt zyklischer Gruppen der Ordnungen $h_1, \ldots, h_r$; *mithin ist die Gruppe* $\mathfrak{H}$ *der Charaktere isomorph zur gegebenen Gruppe* $\mathfrak{G}$.

Die durch die Gleichungen (1), (6) ausgedrückte Reziprozität zwischen den Gruppen $\mathfrak{G}$, $\mathfrak{H}$ ist umkehrbar. Die Zahl $\chi(a)$ hängt nämlich vom Charakter χ und vom Gruppenelement a ab und läßt sich bei festem a als Funktion des Charakters χ auffassen; nach (6) ist diese Funktion ein Homomorphismus der Charakterengruppe $\mathfrak{H}$. Die Anzahl dieser Homomorphismen ist wieder h; also werden alle Homomorphismen der Gruppe $\mathfrak{H}$ durch die Gruppe $\mathfrak{G}$ gegeben.

Aus (2) folgt durch Summation über alle $\lambda_1, \ldots, \lambda_r$:

$$\sum_a \chi(a) = (\sum \zeta_1^{\lambda_1})(\sum \zeta_2^{\lambda_2}) \ldots (\sum \zeta_r^{\lambda_r}) = \begin{cases} h, & \text{wenn alle } \zeta_\nu = 1 \text{ sind,} \\ 0 & \text{sonst.} \end{cases}$$

Daher hat man:

$$\sum_a \chi(a) = \begin{cases} h & \text{für } \chi = \chi_0, \\ 0 & \text{für } \chi \neq \chi_0. \end{cases} \tag{7}$$

Ebenso gilt die reziproke Beziehung

$$\sum_\chi \chi(a) = \begin{cases} h & \text{für } a = 1, \\ 0 & \text{für } a \neq 1. \end{cases} \tag{8}$$

Setzt man in (8) $a = a'a''$, so folgt:

$$\sum_{\chi} \chi(a')\,\chi(a'') = \begin{cases} h & \text{für } a' = a''^{-1}, \\ 0 & \text{für } a' \neq a''^{-1}. \end{cases} \tag{9}$$

Ebenso wieder reziprok:

$$\sum_{a} \chi'(a)\,\chi''(a) = \begin{cases} h & \text{für } \chi' = \chi''^{-1}, \\ 0 & \text{für } \chi' \neq \chi''^{-1}. \end{cases} \tag{10}$$

Der Charakter χ^{-1} heißt zu χ *konjugiert* und wird mit $\bar{\chi}$ bezeichnet. (Im Fall der Zahlkörper ist ζ^{-1} konjugiert-komplex zu ζ, also χ^{-1} konjugiert-komplex zu χ.) Da offenbar $\chi(a^{-1}) = \bar{\chi}(a)$ ist, so kann man statt (9) und (10) schreiben:

$$\sum_{\chi} \chi(a')\,\bar{\chi}(a'') = \begin{cases} h & \text{für } a' = a'', \\ 0 & \text{für } a' \neq a'', \end{cases} \tag{11}$$

$$\sum_{a} \chi'(a)\,\overline{\chi''}(a) = \begin{cases} h & \text{für } \chi' = \chi'', \\ 0 & \text{für } \chi' \neq \chi''. \end{cases} \tag{12}$$

Jede dieser beiden Gleichungen besagt, daß die Matrix der h^2 Zahlen $\chi(a)$ (wo χ Zeilen-, a Spaltenindex ist) invers zur gespiegelten Matrix der Zahlen $\frac{1}{h}\bar{\chi}(a)$ ($\bar{\chi}$ Zeilen-, a Spaltenindex) ist. Man nennt (11) die *Orthogonalitätsrelation der Charaktere.*

Die Charaktere Abelscher Gruppen finden häufig Anwendung in der Zahlentheorie. Es sei n eine natürliche Zahl. Für $\mathfrak{G}$ nehme man die multiplikative Gruppe derjenigen Restklassen mod n, die durch die zu n teilerfremden natürlichen Zahlen $\leqq n$ repräsentiert werden. (h wird also die Eulersche Funktion $\varphi(n)$.) Unter einem *Restcharakter $\chi(m)$ einer zu n teilerfremden Zahl m modulo n* versteht man dann einen Charakter der Restklasse von m in der Restklassengruppe. Weiter setzt man $\chi(m) = 0$, sobald die ganze Zahl m zu n nicht teilerfremd ist. Auf Grund dieser Verabredung kann man die Summation in (7) oder (10) über ein volles Restsystem modulo n erstrecken, während (1), (6), (8) und (9) für alle Zahlen a, b bzw. a', a'' gelten.

Aufgabe. Man schreibe alle Charaktere der Zahlen 1 bis 11 modulo 12 hin; ebenso modulo 11.

§ 125. Darstellungen endlicher Gruppen.

Wir haben in § 120 die Frage der Darstellungen einer endlichen Gruppe $\mathfrak{G}$ auf dieselbe Frage für den Gruppenring $\mathfrak{o} = (a_1, \ldots, a_h)$ zurückgeführt. Die Auffindung aller Darstellungen wird nach Satz 1 des § 121 geleistet sein, sobald wir bewiesen haben, daß dieser Gruppenring vollständig reduzibel ist. Dazu genügt es, den folgenden *Satz von* MASCHKE zu beweisen:

Jede Darstellung einer endlichen Gruppe $\mathfrak{G}$ in einem Körper P, dessen Charakteristik nicht in der Gruppenordnung h aufgeht, ist vollständig reduzibel.

Beweis: Der Darstellungsmodul $\mathfrak{M}$ sei reduzibel, und es sei $\mathfrak{N}$ ein minimaler (oder irreduzibler) Untermodul. Wir werden zeigen, daß $\mathfrak{M}$ sich als direkte Summe $\mathfrak{N} + \mathfrak{N}''$ darstellen läßt, wo $\mathfrak{N}''$ wieder ein Darstellungsmodul ist.

Als Vektorraum zerfällt $\mathfrak{M}$ nach dem Schema $\mathfrak{N} + \mathfrak{N}'$; dabei ist aber $\mathfrak{N}'$ noch nicht notwendig gegenüber $\mathfrak{o}$ invariant, also noch nicht notwendig ein Darstellungsmodul. Ist y ein Element von $\mathfrak{N}'$ und a eins von $\mathfrak{G}$, so ist ay eindeutig darstellbar als Summe eines Elements von $\mathfrak{N}$ und eines Elements y' von $\mathfrak{N}'$, mithin

$$ay \equiv y' \,(\mathrm{mod}\, \mathfrak{N}).$$

Das Element y' ist bei festem a durch y eindeutig bestimmt und hängt von y linear ab: aus $ay \equiv y'$ und $az \equiv z'$ folgt $a(y+z) \equiv y' + z'$ und $ay\lambda \equiv y'\lambda$ für $\lambda \in \mathsf{P}$. Wir können also schreiben

$$y' = A'y; \qquad A'y \equiv ay \,(\mathrm{mod}\, \mathfrak{N}),$$

wo A' ein linearer Operator (d. h. eine lineare Transformation) in $\mathfrak{N}'$ ist[1] und noch von a abhängt. Und zwar bilden die Operatoren A' eine Darstellung der Gruppe $\mathfrak{G}$; denn aus $a \to A'$ und $b \to B'$ folgt $ab \to A'B'$.

Wir setzen nun

$$\frac{1}{h}\sum_a a^{-1}A'y = Qy = y'';$$

dann hängt auch y'' linear von y ab, und somit bilden die y'' einen linearen Unterraum $\mathfrak{N}'' = Q\mathfrak{N}'$. Weiter folgt modulo $\mathfrak{N}$:

$$y'' \equiv \frac{1}{h}\sum_a a^{-1}ay = y.$$

Jedes Element von $\mathfrak{M}$ ist also modulo $\mathfrak{N}$ nicht nur kongruent einem Element y von $\mathfrak{N}'$, sondern auch einem eindeutig bestimmten Element y'' von $\mathfrak{N}''$; d. h. es besteht die direkte Summendarstellung

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

Schließlich ist für jedes Element b von $\mathfrak{G}$

$$\begin{aligned} by'' &= \frac{1}{h}\sum_a ba^{-1}A'y \\ &= \frac{1}{h}\sum_a (ab^{-1})^{-1}(A'B'^{-1})B'y \\ &= QB'y \in Q\mathfrak{N}' = \mathfrak{N}''; \end{aligned}$$

[1] Stellt man alle linearen Transformationen durch Matrizes dar, wie in § 108, Formel (4), so ist A' gerade die rechts unten stehende, dort mit T bezeichnete Matrix.

mithin wird $\mathfrak{N}''$ durch die Operatoren b von $\mathfrak{G}$ in sich transformiert, d. h. $\mathfrak{N}''$ ist ein Darstellungsmodul.

Ist auch $\mathfrak{N}''$ noch reduzibel, so kann man $\mathfrak{N}''$ in derselben Weise behandeln, indem man einen minimalen Untermodul abspaltet, usw. So findet man schließlich die vollständige Zerfällung des Moduls $\mathfrak{M}$ und damit der Darstellung.

Will man alle Darstellungen einer Gruppe aufstellen, so genügt es nach dem eben bewiesenen Satz, die irreduziblen zu finden, und diese findet man mit Hilfe der minimalen Linksideale des Gruppenrings (oder, was dasselbe ist, durch Ausreduzieren der regulären Darstellung). In einer reduziblen Darstellung kann jede irreduzible beliebig oft wiederholt vorkommen.

Die Anzahl der absolut-irreduziblen Darstellungen ist nach § 122 gleich dem Rang des Zentrums, und das Zentrum des Gruppenrings besteht, wie man mühelos sieht, aus allen denjenigen Summen

$$\sum_{\lambda} a_\lambda \varrho_\lambda \qquad (a_\lambda \in \mathfrak{G},\ \varrho_\lambda \in \mathsf{P}), \tag{1}$$

in denen konjugierte Gruppenelemente dieselben Koeffizienten haben. Die zu einem Element a konjugierten Elemente bilden je eine „*Klasse*". Ist k_a die Summe der Elemente dieser Klasse, so ist (1) eine Summe aus solchen Summen k_a mit Koeffizienten aus P. Mithin gilt der Satz: *Das Zentrum des Gruppenrings wird von den Klassensummen k_a erzeugt.* Der Rang des Zentrums ist also gleich der Klassenanzahl, und daraus folgt:

Die Anzahl der inäquivalenten absolut-irreduziblen Darstellungen einer Gruppe ist gleich der Anzahl der Klassen konjugierter Elemente.

Für die Grade $n_1, \ldots, n_s$ der irreduziblen Darstellungen besteht die Relation

$$n_1^2 + n_2^2 + \cdots + n_s^2 = h,$$

denn der Gruppenring vom Rang h ist direkte Summe von Matrizenringen der Ränge $n_1^2, n_2^2, \ldots, n_s^2$.

Eine stets vorhandene Darstellung ersten Grades ist die „identische Darstellung", die jedem Gruppenelement das Element 1 zuordnet.

Soll es noch weitere Darstellungen ersten Grades geben, so muß ein echter Normalteiler mit Abelscher Faktorgruppe vorhanden sein; denn die Transformationen der Darstellungen ersten Grades sind miteinander vertauschbar und bilden eine zur Gruppe homomorphe Abelsche Gruppe. Ist umgekehrt ein echter Normalteiler mit Abelscher Faktorgruppe vorhanden, so ergeben die Charaktere dieser Abelschen Gruppe schon Darstellungen ersten Grades. Alle übrigen Darstellungen sind von höherem Grade.

Beispiele. 1. *Die symmetrische Gruppe* $\mathfrak{S}_3$. Klassenanzahl 3; also 3 Darstellungen. Die alternierende Gruppe hat 2 Nebenklassen $\mathfrak{R}_0$, $\mathfrak{R}_1$: die der geraden und der ungeraden Substitutionen. Die 2 Charaktere dieser Zweiergruppe:

$$\chi(\mathfrak{R}_0) = 1, \qquad \chi(\mathfrak{R}_1) = \pm 1,$$

bestimmen die Darstellungen ersten Grades. Wegen

$$n_1^2 + n_2^2 + n_3^2 = 6$$

muß die dritte Darstellung den Grad 2 haben. Nimmt man drei Vektoren e_1, e_2, e_3 in einer Ebene, deren Summe Null ist, so ergeben die Permutationen dieser drei Vektoren eine treue Darstellung dieser Permutationsgruppe; die Darstellung erweist sich leicht als irreduzibel. Nimmt man e_1 und e_2 als Grundvektoren, so lautet die Darstellung:

$$\begin{cases}(1\ 2)\,e_1 = e_2,\\ (1\ 2)\,e_2 = e_1,\end{cases} \quad \begin{cases}(1\ 3)\,e_1 = -e_1 - e_2,\\ (1\ 3)\,e_2 = e_2,\end{cases} \quad \begin{cases}(2\ 3)\,e_1 = e_1,\\ (2\ 3)\,e_2 = -e_1 - e_2,\end{cases}$$

$$\begin{cases}(1\ 2\ 3)\,e_1 = e_2,\\ (1\ 2\ 3)\,e_2 = -e_1 - e_2,\end{cases} \quad \begin{cases}(1\ 3\ 2)\,e_1 = -e_1 - e_2,\\ (1\ 3\ 2)\,e_2 = e_1.\end{cases}$$

2. *Die Quaternionengruppe* $\mathfrak{Q}_8$:

$$j^4 = 1, \qquad k^2 = j^2, \qquad kj = j^3 k.$$

Klassenanzahl 5; also 5 Darstellungen. Der Normalteiler $\{1, j^2\}$ hat als Faktorgruppe die Kleinsche Vierergruppe, deren 4 Charaktere 4 lineare Darstellungen ergeben. Die übrigbleibende Darstellung muß wegen

$$n_1^2 + n_2^2 + n_3^2 + n_4^2 + n_5^2 = 8$$

den Grad 2 haben. Ordnet man den Gruppenelementen $1, j, j^2, j^3, k, jk, j^2k, j^3k$ die Quaternionen $1, j, -1, -j, k, l, -k, -l$ zu, so erhält man eine homomorphe Abbildung des Gruppenrings $\mathfrak{o}$ auf den Quaternionenkörper; also muß der Quaternionenkörper unter den zweiseitigen Kompositionsfaktoren von $\mathfrak{o}$ vorkommen. Damit ist schon die Zerlegung von $\mathfrak{o}$ im rationalen Grundkörper Γ gefunden: Es ist

$$\mathfrak{o} = \mathfrak{a}_1 + \mathfrak{a}_2 + \mathfrak{a}_3 + \mathfrak{a}_4 + \mathfrak{a}_5,$$

wo $\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3, \mathfrak{a}_4$ isomorph zu Γ sind und $\mathfrak{a}_5$ isomorph dem Quaternionenkörper ist. Geht man zum algebraisch-abgeschlossenen Grundkörper über (es genügt in diesem Fall die Adjunktion von $i = \sqrt{-1}$), so zerfällt der Quaternionenkörper, und man erhält die Matrixdarstellung

$$j \to \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \qquad k \to \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \qquad l \to \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

3. *Die alternierende Gruppe* $\mathfrak{A}_4$ kann nach genau derselben Methode wie die symmetrische $\mathfrak{S}_3$ behandelt werden, was dem Leser überlassen bleiben möge. Man findet 4 Darstellungen der Grade 1, 1, 1, 3.

4. *Die symmetrische Gruppe* $\mathfrak{S}_4$. Klassenanzahl 5; also 5 Darstellungen. Die Kleinsche Vierergruppe $\{1, (1\,2)\,(3\,4), (1\,3)\,(2\,4), (1\,4)\,(2\,3)\}$ hat eine zu $\mathfrak{S}_3$ isomorphe Faktorgruppe, von der wir schon 3 irreduzible Darstellungen der Grade 1, 1, 2 kennen; diese ergeben auch Dar-

stellungen der Grade 1, 1, 2 von $\mathfrak{S}_4$. Werden diese Gradzahlen mit n_1, n_2, n_3 bezeichnet, so folgt aus

$$n_1^2 + n_2^2 + n_3^2 + n_4^2 + n_5^2 = 24,$$

daß

$$n_4^2 + n_5^2 = 18$$

sein muß, und das trifft nur für $n_4 = 3$, $n_5 = 3$ zu. Führt man 4 Vektoren e_1, e_2, e_3, e_4 mit der Summe Null ein, so ergeben die Permutationen dieser 4 Vektoren eine treue Darstellung dritten Grades von $\mathfrak{S}_4$. Wählt man e_1, e_2, e_3 als Grundvektoren, so lautet die Darstellung:

$$\begin{cases} (1\ 2)\, e_1 = e_2, \\ (1\ 2)\, e_2 = e_1, \\ (1\ 2)\, e_3 = e_3, \end{cases} \qquad \begin{cases} (1\ 3)\, e_1 = e_3, \\ (1\ 3)\, e_2 = e_2, \\ (1\ 3)\, e_3 = e_1, \end{cases} \qquad \begin{cases} (1\ 4)\, e_1 = -e_1 - e_2 - e_3, \\ (1\ 4)\, e_2 = e_2, \\ (1\ 4)\, e_3 = e_3, \end{cases}$$

$$\begin{cases} (1\ 2\ 3)\, e_1 = e_2, \\ (1\ 2\ 3)\, e_2 = e_3, \\ (1\ 2\ 3)\, e_3 = e_1, \end{cases} \quad \text{usw.}$$

Da die Darstellung treu ist, kann sie sich nicht auf die Darstellungen ersten und zweiten Grades reduzieren; mithin ist sie irreduzibel. Multipliziert man die darstellenden Matrizes der ungeraden Substitutionen mit -1, so erhält man eine andere, ebenfalls treue und daher wieder irreduzible Darstellung dritten Grades, die sicher mit der vorigen nicht äquivalent ist, da die Spuren verschieden sind. Damit haben wir alle Darstellungen gefunden.

Aufgaben. 1. Das Element $s = \sum_{a \in \mathfrak{G}} a$ des Gruppenrings $\mathfrak{o}$ genügt den Gleichungen

$$bs = s \quad \text{für} \quad b \in \mathfrak{G}.$$

Welches Linksideal wird von s erzeugt? Welche Darstellung gehört zu diesem Ideal? Welches idempotente Element ist in diesem Ideal enthalten?

2. Ist die Anzahl h der Gruppenelemente durch die Charakteristik des Körpers teilbar, so ist das in Aufgabe 1 genannte Ideal nilpotent. Daraus ist abzuleiten, daß die Bedingung, daß die Charakteristik nicht in h aufgeht, für den Satz von MASCHKE auch notwendig ist.

§ 126. Gruppencharaktere.

Die Kroneckersche Produkttransformation.

Es seien zwei lineare Transformationen A', A'' gegeben, die eine im Vektorraum $(u_1, \ldots, u_n)$, die andere im Vektorraum $(v_1, \ldots, v_m)$, wobei die u und v als Unbestimmte aufgefaßt werden. Es sei also etwa

$$A' u_k = \sum_i u_i \alpha'_{ik},$$

$$A'' v_l = \sum_j v_j \alpha''_{jl}.$$

Wenn man nun auf u und v gleichzeitig diese Transformationen anwendet, so transformieren sich die Produkte $u_k v_l$ folgendermaßen[1]:

$$A\, u_k v_l = \sum_i \sum_j u_i v_j \alpha'_{ik} \alpha''_{jl}\,. \tag{1}$$

Die so entstehende Transformation A im Vektorraum der $n \cdot m$ linearunabhängigen Größen $u_k v_l$ heißt die *Kroneckersche Produkttransformation* und wird mit $A' \times A''$ bezeichnet. Die Matrixelemente von A sind nach (1) die Produkte $\alpha'_{ik}\alpha''_{jl}$. Die Spur von A ist

$$\sum_i \sum_j \alpha'_{ii}\alpha''_{jj} = \sum_i \alpha'_{ii} \cdot \sum_j \alpha''_{jj} = S(A') \cdot S(A'');$$

mithin: *Die Spur der Produkttransformation $A' \times A''$ ist das Produkt der Spuren der Transformationen A' und A''.*

Übt man auf die u nacheinander zwei Transformationen B', A' und auf die v nacheinander zwei Transformationen B'', A'' aus, so erleiden die Produkte $u_k v_l$ nacheinander die Transformationen $B' \times B''$ und $A' \times A''$; d. h. es ist

$$(A' \times A'') \cdot (B' \times B'') = A'B' \times A''B''. \tag{2}$$

Bilden die Matrizes $A', B', \ldots$ eine Darstellung $\mathfrak{D}'$ einer Gruppe $\mathfrak{G}$ und die Matrizes $A'', B'', \ldots$ eine andere Darstellung $\mathfrak{D}''$ derselben Gruppe, so folgt aus (2), daß die Produkttransformationen $A = A' \times A''$, $B = B' \times B'', \ldots$ wieder eine Darstellung bilden. Diese *Produktdarstellung* der Darstellungen $\mathfrak{D}', \mathfrak{D}''$ wird mit $\mathfrak{D}' \times \mathfrak{D}''$ bezeichnet.

Schreibt man noch $\mathfrak{D}' + \mathfrak{D}''$ für eine reduzible Darstellung, die in $\mathfrak{D}'$ und $\mathfrak{D}''$ vollständig zerfällt, und betrachtet dabei äquivalente Darstellungen als nichtverschieden, so verifiziert man leicht für die Summen und Produkte von Darstellungen alle üblichen Rechnungsregeln:

$$\mathfrak{D}' + \mathfrak{D}'' = \mathfrak{D}'' + \mathfrak{D}', \qquad \mathfrak{D}' \times \mathfrak{D}'' = \mathfrak{D}'' \times \mathfrak{D}',$$

$$\mathfrak{D}' + (\mathfrak{D}'' + \mathfrak{D}''') = (\mathfrak{D}' + \mathfrak{D}'') + \mathfrak{D}''', \quad \mathfrak{D}' \times (\mathfrak{D}'' \times \mathfrak{D}''') = (\mathfrak{D}' \times \mathfrak{D}'') \times \mathfrak{D}''',$$

$$\mathfrak{D}' \times (\mathfrak{D}'' + \mathfrak{D}''') = \mathfrak{D}' \times \mathfrak{D}'' + \mathfrak{D}' \times \mathfrak{D}''', \quad (\mathfrak{D}'' + \mathfrak{D}''') \times \mathfrak{D}' = \mathfrak{D}'' \times \mathfrak{D}' + \mathfrak{D}''' \times \mathfrak{D}'.$$

Ist insbesondere $\mathfrak{G}$ eine endliche Gruppe, so daß jede Darstellung vollständig in irreduzible Darstellungen $\mathfrak{D}_\nu$ zerfällt, so hat man:

$$\mathfrak{D}_\lambda \times \mathfrak{D}_\mu = \sum_\nu c^\nu_{\lambda\mu}\, \mathfrak{D}_\nu\,, \tag{3}$$

wo die $c^\nu_{\lambda\mu}$ ganze Zahlen $\geqq 0$ sind. Daher kann man die Darstellungen $\mathfrak{D}_\nu$ als Erzeugende eines kommutativen hyperkomplexen Systems $\mathfrak{H}$ deuten.

Für die Spuren folgt aus (3):

$$S_\lambda(a) \cdot S_\mu(a) = \sum_\nu c^\nu_{\lambda\mu}\, S_\nu(a).$$

---

[1] Die Unbestimmten werden als miteinander und mit den Koeffizienten vertauschbar angenommen.

Falls die Darstellungen absolut-irreduzibel sind, die Spuren also Charaktere werden, kann man dafür auch schreiben:

$$\chi_\lambda(a)\cdot\chi_\mu(a)=\sum_\nu c^\nu_{\lambda\mu}\,\chi_\nu(a) \quad (4)$$

(*erste Charakterenrelation*).

Die Charaktere als Klassenfunktionen.

Sind a und a' konjugierte Gruppenelemente:

$$a'=bab^{-1},$$

so folgt für die darstellenden Matrizes:

$$A'=BAB^{-1}.$$

Somit haben A und A' dieselbe Spur; d. h. es ist

$$S(bab^{-1})=S(a),$$

insbesondere

$$\chi(bab^{-1})=\chi(a).$$

Rechnen wir wieder alle zu a konjugierten Gruppenelemente zu einer *Klasse* $\mathfrak{K}_a$, so hat also jeder einzelne Charakter für alle Elemente einer Klasse denselben Wert.

Ist h_a die Anzahl der Elemente der Klasse $\mathfrak{K}_a$ und ist k_a die Summe der Elemente dieser Klasse (im Gruppenring $\mathfrak{o}$), so ist der Charakter von k_a die Summe aus den Charakteren der Elemente der Klasse, also

$$\chi(k_a)=h_a\cdot\chi(a).$$

Wie wir in § 125 sahen, erzeugen die Größen k_a das Zentrum $\mathfrak{Z}$ des Gruppenrings $\mathfrak{o}$. Nach § 123 sind die Homomorphismen Θ_ν von $\mathfrak{Z}$ mit den Charakteren χ_ν durch die Relationen [1]

$$\Theta_\nu(z)=\frac{\chi_\nu(z)}{n_\nu}$$

verbunden, wo $n_\nu=\chi_\nu(1)$ der Grad der absolut-irreduziblen Darstellung $\mathfrak{D}_\nu$ ist; insbesondere ist

$$\Theta_\nu(k_a)=\frac{\chi_\nu(k_a)}{n_\nu}=\frac{h_a}{n_\nu}\chi_\nu(a). \quad (5)$$

Das Produkt k_ak_b ist eine Summe von Gruppenelementen, die wieder zu $\mathfrak{Z}$ gehört und sich daher ganzzahlig durch die Klassensummen k_a ausdrückt:

$$k_a\cdot k_b=\sum_c g^c_{ab}\,k_c. \quad (6)$$

Die Homomorphieeigenschaft der Θ_ν spricht sich nun in der Gleichung

$$\Theta_\nu(k_a)\cdot\Theta_\nu(k_b)=\sum_c g^c_{ab}\,\Theta_\nu(k_c) \quad (7)$$

[1] Wir setzen wieder voraus, daß weder die Gruppenordnung h noch die Grade n_ν der Darstellungen durch die Charakteristik des Körpers teilbar sind.

aus, die sich mit Hilfe von (5) in

$$h_a h_b \chi_\nu(a) \chi_\nu(b) = n_\nu \sum_c g_{ab}^c h_c \chi_\nu(c) \quad \left\{ \begin{array}{c} (\textit{zweite Charakteren-} \\ \textit{relation}) \end{array} \right. \tag{8}$$

umschreiben läßt. In den Summen (6), (7) und (8) durchläuft c je ein Repräsentantensystem aller Klassen. Läßt man c alle Gruppenelemente durchlaufen, so ist in (8) auf der rechten Seite der Faktor h_c wegzulassen. Da die Θ_ν die einzigen Homomorphismen von $\mathfrak{Z}$ sind, so sind die Charaktere χ_ν die einzigen Lösungen der Gleichung (8).

Genau so, wie (7) in Verbindung mit (6) ausdrückt, daß $\Theta_\nu(k_a)$ bei festem ν ein Homomorphismus des Zentrums $\mathfrak{Z}$ ist, so bedeutet (4) in Verbindung mit (3), daß $\chi_\nu(a)$ bei festem a, als Funktion von $\mathfrak{D}_\nu$ betrachtet, ein Homomorphismus des Ringes $\mathfrak{H}$ im Körper Ω ist: dem Produkt zweier Darstellungen entspricht das Produkt der Charaktere, der Summe die Summe. Die beiden kommutativen Ringe $\mathfrak{Z}$, $\mathfrak{H}$ sind also zueinander reziprok: jedes Basiselement k_a von $\mathfrak{Z}$ bestimmt einen Homomorphismus $\chi_\nu(a)$ von $\mathfrak{H}$, und jedes Basiselement $\mathfrak{D}_\nu$ von $\mathfrak{H}$ bestimmt einen Homomorphismus $\Theta_\nu(k_a)$ von $\mathfrak{Z}$. Zwischen den Θ_ν und den χ_ν besteht dabei die einfache Relation (5). Die Anzahl der so gefundenen Homomorphismen von $\mathfrak{H}$ ist gleich der Anzahl der Klassen, also gleich dem Rang von $\mathfrak{H}$. Daraus folgt, daß $\mathfrak{H}$ ein System ohne Radikal ist, denn wenn $\mathfrak{H}$ ein Radikal $\mathfrak{c}$ hätte, so wäre die Anzahl der möglichen Homomorphismen oder Darstellungen 1. Grades von $\mathfrak{H}$ nur gleich dem Rang von $\mathfrak{H}/\mathfrak{c}$. Zugleich ergibt sich, daß die $\chi_\nu(a)$ die *sämtlichen* Homomorphismen von $\mathfrak{H}$ in Ω ergeben.

Die konjugierten Charaktere.

Zu jeder Darstellung $a \to A$ gibt es eine „*konjugierte* (oder *kontragrediente*) *Darstellung*“ $a \to A'^{-1}$, wo A' die gespiegelte Matrix zu A ist. Bei dieser Zuordnung ist nämlich

$$ab \to (AB)'^{-1} = (B'A')^{-1} = A'^{-1} B'^{-1}.$$

Die Konjugierte zur konjugierten Darstellung ist wieder die ursprüngliche. Ist die Darstellung $a \to A$ reduzibel, so ist es auch die konjugierte, und umgekehrt. Die Konjugierte einer irreduziblen Darstellung ist also wieder irreduzibel.

Geht man von A zu einer äquivalenten Darstellung $P^{-1} A P$ über, so geht die konjugierte Darstellung über in

$$(P^{-1} A P)'^{-1} = P' A'^{-1} P'^{-1},$$

also ebenfalls in eine äquivalente.

Bezeichnet man mit $\mathfrak{D}_{\nu'}$ die zu $\mathfrak{D}_\nu$ konjugierte irreduzible Darstellung, und ist $\mathfrak{D}_\nu(a) = A$, so ist

$$\mathfrak{D}_{\nu'}(a^{-1}) = A',$$

und da die Spur von A' gleich der von A ist, so folgt

$$\chi_{\nu'}(a^{-1}) = \chi_\nu(a).$$

Man bezeichnet den zu χ_ν „*konjugierten*" *Charakter* $\chi_{\nu'}$ auch mit $\bar{\chi}_\nu$.

Jeder Charakter ist eine Summe von Einheitswurzeln. Denn jedes Element a von $\mathfrak{G}$ erzeugt eine zyklische Untergruppe $\mathfrak{C}$, deren Ordnung m ein Teiler von h ist, und jede irreduzible Darstellung $\mathfrak{D}_\nu$ von $\mathfrak{G}$ ergibt eine Darstellung von $\mathfrak{C}$; diese zerfällt nach § 124 vollständig in Darstellungen ersten Grades, deren Matrixelemente m-te Einheitswurzeln sind. Die Spur der darstellenden Matrix ist die Summe der Diagonalelemente, also eine Summe von m-ten Einheitswurzeln, etwa

$$\chi(a) = \zeta^{\nu_1} + \zeta^{\nu_2} + \cdots + \zeta^{\nu_n}, \tag{9}$$

wo ζ eine primitive m-te Einheitswurzel ist.

Die gespiegelte Matrix A' ist, wenn A in der eben angegebenen Diagonalform geschrieben wird, gleich A selbst, und A'^{-1} entsteht durch Ersetzung von ζ durch ζ^{-1}. Also ist

$$\bar{\chi}(a) = \zeta^{-\nu_1} + \zeta^{-\nu_2} + \cdots + \zeta^{-\nu_n}.$$

Im Fall der Zahlkörper ist $\bar{\chi}$ konjugiert-komplex zu χ.

Die Ersetzung von ζ durch ζ^{-1} ist ein Automorphismus des Körpers der m-ten Einheitswurzeln, und dieser Automorphismus führt χ in $\bar{\chi}$ über. In analoger Weise erhält man natürlich aus jedem Charakter χ durch einen beliebigen Körperautomorphismus wieder einen algebraisch-konjugierten Charakter χ^*, zu dem auch eine algebraisch-konjugierte Darstellung gehört, da jeder Isomorphismus des Körpers der Charaktere sich zu einem Isomorphismus des Körpers der Darstellung fortsetzen läßt. χ^* ist zu χ konjugiert im weiteren, körpertheoretischen Sinn.

Die weiteren Charakterenrelationen.

Ist $S(c)$ die Spur des Gruppenelements c in der regulären Darstellung, so ist

$$S(c) = \sum_\nu n_\nu \chi_\nu(c),$$

da die reguläre Darstellung ja die irreduzible Darstellung $\mathfrak{D}_\nu$ genau n_ν-mal enthält. Die Spur $S(c)$ läßt sich aber auch direkt ausrechnen: Die Gruppenelemente $a_1, \ldots, a_h$ bilden eine Basis des Vektorraums $\mathfrak{o}$ der regulären Darstellung, und es ist

$$c a_i = a_k.$$

Glieder mit $i = k$ kommen nur dann vor, wenn c gleich dem Einselement 1 der Gruppe ist; in diesem Fall ist jedes i gleich dem zugehörigen k. Es ist also

$$S(1) = h; \qquad S(c) = 0 \quad \text{für} \quad c \neq 1,$$

mithin

$$\sum_\nu n_\nu \chi_\nu(c) = \begin{cases} h & \text{für} \quad c = 1, \\ 0 & \text{für} \quad c \neq 1. \end{cases} \tag{10}$$

Summiert man nun (8) über alle ν und berücksichtigt dabei (10), so ergibt sich

$$h_a h_b \sum_\nu \chi_\nu(a)\,\chi_\nu(b) = g^1_{ab}\cdot h\,. \tag{11}$$

Die Zahl g^1_{ab} gibt an, wie oft es vorkommt, daß ein Produkt $a'b'$, wo a' zur Klasse $\mathfrak{K}_a$ und b' zur Klasse $\mathfrak{K}_b$ gehört, gleich 1 ist. Die Zahl ist also Null, wenn $\mathfrak{K}_a$ und $\mathfrak{K}_b$ keine zwei zueinander inversen Elemente enthalten. Wenn aber ein solches Paar vorhanden, etwa $b = a^{-1}$ ist, so gibt es zu jedem Element $a' = cac^{-1}$ von $\mathfrak{K}_a$ ein dazu inverses Element $b' = a'^{-1} = cbc^{-1}$ von $\mathfrak{K}_b$, und man erhält:

$$g^1_{ab} = h_a = h_b\,.$$

Mithin wird (11) nach Division durch h_b zu

$$h_a \sum_\nu \chi_\nu(a)\,\chi_\nu(b) = \begin{cases} h & \text{für} \quad \mathfrak{K}_b = \mathfrak{K}_{a^{-1}}\,, \\ 0 & \text{für} \quad \mathfrak{K}_b \neq \mathfrak{K}_{a^{-1}} \end{cases} \qquad \text{(dritte Charakterenrelation).} \tag{12}$$

Als Spezialfall $a = 1$ erhält man hieraus (10) zurück.

Nun möge $a_1, \ldots, a_s$ ein Repräsentantensystem aller Klassen sein. Setzt man

$$\chi_{\nu\mu} = \chi_\nu(a_\mu)\,,$$
$$\eta_{\mu\nu} = \frac{h_\mu}{h}\,\bar{\chi}_\nu(a_\mu) = \frac{h_\mu}{h}\,\chi_\nu(a_\mu^{-1})\,,$$

so besagt die Relation (12), daß die Matrizes $\Xi = (\chi_{\mu\nu})$ und $\Upsilon = (\eta_{\mu\nu})$ zueinander invers sind:

$$\Upsilon\Xi = E \quad \text{oder} \quad \Upsilon = \Xi^{-1}\,. \tag{13}$$

Aus (13) folgt:

$$\Xi\Upsilon = E$$

oder ausgeschrieben

$$\frac{1}{h}\sum_{\mathfrak{K}_a} h_a\,\chi_\nu(a)\,\bar{\chi}_\mu(a) = \begin{cases} 1 & \text{für} \quad \nu = \mu\,, \\ 0 & \text{für} \quad \nu \neq \mu\,. \end{cases} \tag{14}$$

Dabei durchläuft a ein Repräsentantensystem aller Klassen. Läßt man a alle Gruppenelemente durchlaufen, so muß man die Faktoren h_a weglassen. Hieraus ergibt sich die *Orthogonalität der Charaktere*:

$$\sum_{a\,\in\,\mathfrak{G}} \bar{\chi}_\mu(a)\,\chi_\nu(a) = \begin{cases} h & \text{für} \quad \nu = \mu\,, \\ 0 & \text{für} \quad \nu \neq \mu \end{cases} \qquad \text{(vierte Charakterenrelation).} \tag{15}$$

Ist speziell $\mu = 0$, d. h. ist χ_μ der Charakter χ_0 der identischen Darstellung, so ergibt sich aus (15)

$$\sum_a \chi_\nu(a) = \begin{cases} h & \text{für} \quad \nu = 0\,, \\ 0 & \text{für} \quad \nu \neq 0\,. \end{cases} \tag{16}$$

Die Relation (15) kann man zur Bestimmung der Koeffizienten $c_{\lambda\mu}^{\nu}$ in (4) benutzen, indem man (4) mit $\bar{\chi}_{\varkappa}(a)$ multipliziert und über alle a summiert. Das ergibt:

$$\sum_a \bar{\chi}_{\varkappa}(a)\,\chi_{\lambda}(a)\,\chi_{\mu}(a) = h\,c_{\lambda\mu}^{\varkappa}\,.$$

Ersetzt man $\varkappa$ durch $\varkappa'$, wo $\mathfrak{D}_{\varkappa'}$ die zu $\mathfrak{D}_{\varkappa}$ konjugierte Darstellung ist, so ergibt sich:

$$\sum_a \chi_{\varkappa}(a)\,\chi_{\lambda}(a)\,\chi_{\mu}(a) = h\,c_{\lambda\mu}^{\varkappa'}\,.$$

Daraus folgt: *Der Koeffizient $c_{\lambda\mu}^{\varkappa'}$, der angibt, wie oft die zu $\mathfrak{D}_{\varkappa}$ konjugierte Darstellung im Produkt $\mathfrak{D}_{\lambda} \times \mathfrak{D}_{\mu}$ enthalten ist, ist in den Indizes $\lambda, \mu, \varkappa$ symmetrisch.*

Man kann die Tatsache, daß die Matrizes Ξ und Υ zueinander invers sind, zur Berechnung der idempotenten Zentrumselemente $e_1, \ldots, e_s$ benutzen, welche die zweiseitig-einfachen Ideale in $\mathfrak{o}$ erzeugen. Nach § 122 hat man nämlich für die Basiselemente k_a des Zentrums $\mathfrak{Z}$ die Ausdrücke

$$k_a = \sum_{\nu} e_{\nu}\,\Theta_{\nu}(k_a) = \sum_{\nu} e_{\nu}\,\frac{h_a}{n_{\nu}}\,\chi_{\nu}(a)\,. \tag{17}$$

Indem man mit $\bar{\chi}_{\mu}(a)$ multipliziert und über alle Klassen $\mathfrak{K}_a$ summiert, ergibt sich

$$\sum_{\mathfrak{K}_a} k_a\,\bar{\chi}_{\mu}(a) = e_{\mu}\cdot\frac{h}{n_{\mu}}$$

oder

$$e_{\nu} = \sum_{\mathfrak{K}_a} k_a\,\frac{n_{\nu}}{h}\,\chi_{\nu}(a^{-1})\,.$$

Satz. *Die Grade der irreduziblen Darstellungen einer endlichen Gruppe im Körper aller algebraischen Zahlen sind Teiler der Gruppenordnung.*

Beweis: Läßt man in (7) das Element b ein Repräsentantensystem aller Klassen durchlaufen und betrachtet auf der linken Seite $\Theta_{\nu}(k_a)$ als bekannt, so erhält man ein homogenes lineares Gleichungssystem für die $\Theta_{\nu}(k_c)$, aus dem sich durch Elimination dieser Größen die Relation

$$\left|\,\delta_b^c\,\Theta_{\nu}(k_a) - g_{ab}^{c}\,\right| = 0$$

(a wird festgehalten, b und c sind Zeilen- bzw. Spaltenindex) mit

$$\delta_b^c = \begin{cases} 1 & \text{für} \quad b = c\,, \\ 0 & \text{für} \quad b \neq c \end{cases}$$

ergibt. Daher ist $\Theta_{\nu}(k_a)$ als Wurzel einer Gleichung mit ganzen rationalen Koeffizienten und dem höchsten Koeffizienten 1 eine ganze algebraische Zahl. In derselben Weise folgt aus (4), daß die Charaktere $\chi_{\nu}(a)$ ganze algebraische Zahlen sind, was man auch aus (9) ersehen kann.

Nun läßt sich die erste Hälfte von (14) folgendermaßen schreiben:

$$\frac{n_\nu}{h} \sum_{\mathfrak{K}_a} \Theta_\nu(k_a)\, \bar{\chi}_\mu(a) = 1 \quad \text{für} \quad \mu = \nu$$

oder

$$\sum_{\mathfrak{K}_a} \Theta_\nu(k_a)\, \chi_\nu(a^{-1}) = \frac{h}{n_\nu}.$$

Links steht eine ganze algebraische Zahl; also ist $\frac{h}{n_\nu}$ ganz und zugleich rational, mithin ganz-rational, q. e. d.

Literatur. Eine von der Theorie der hyperkomplexen Zahlen unabhängige Begründung der Darstellungstheorie endlicher Gruppen findet man bei I. SCHUR, Neue Begründung der Theorie der Gruppencharaktere, Sitzungsber. Berlin 1905, S. 406. Von der reichhaltigen Literatur über Gruppencharaktere sei hier nur noch auf die wichtige Arbeit von G. FROBENIUS, Über Relationen zwischen den Charakteren einer Gruppe und denen ihrer Untergruppen, Sitzungsber. Berlin 1898, hingewiesen. Siehe weiter, WEYL, H., Gruppentheorie und Quantenmechanik, 2. Aufl., Leipzig 1931.

Aufgaben. 1. Man stelle eine Charakterentabelle der symmetrischen Gruppen von 3 und 4 Elementen auf und berechne die idempotenten Zentrumselemente des Gruppenrings.

2. Man zeige, daß die Relation (8) auch folgendermaßen geschrieben werden kann:

$$h\, \chi_\nu(a)\, \chi_\nu(b) = n_\nu \sum_d \chi_\nu(a\, d\, b\, d^{-1}).$$

3. Die Produktdarstellung $\mathfrak{D}_\lambda \times \mathfrak{D}_\mu$ enthält dann und nur dann die identische Darstellung, und zwar genau einmal, wenn die Darstellungen $\mathfrak{D}_\lambda$ und $\mathfrak{D}_\mu$ zueinander konjugiert sind.

4. Im Körper der komplexen Zahlen ist die zu einer Darstellung konjugiert-komplexe Darstellung äquivalent zur konjugierten.

§ 127. Die Darstellungen der symmetrischen Gruppen[1].

Wir betrachten die Gruppe $\mathfrak{S}_n$ der Permutationen von n Ziffern $1, 2, \ldots, n$ und suchen ihre absolut-irreduziblen Darstellungen etwa im Körper Ω aller algebraischen Zahlen. Es wird sich übrigens zeigen, daß diese Darstellungen rational sind, d. h. im Körper Γ der rationalen Zahlen stattfinden.

Wir gehen vom Gruppenring $\mathfrak{o} = s_1\Omega + \cdots + s_{n!}\,\Omega$ aus und betrachten dessen Linksideale. Jedes solche Linksideal ist direkte Summe von minimalen Linksidealen; diese liefern uns die irreduziblen Darstellungen. Da jedes Linksideal von einem idempotenten Element erzeugt wird, so suchen wir zunächst idempotente Elemente auf.

Wir schreiben die Ziffern $1, 2, \ldots, n$ in irgendeiner Anordnung in h Zeilen

[1] Die gegenüber der Frobeniusschen Theorie (Sitzungsber. Berlin 1903, S. 328) vereinfachten Beweise in diesem Paragraphen verdanke ich einer mündlichen Mitteilung von Herrn J. VON NEUMANN.

(h beliebig) untereinander, so daß in der ν-ten Zeile α_ν Ziffern stehen und die Bedingungen

$$(1)\qquad \begin{cases} \alpha_1 \geqq \alpha_2 \geqq \cdots \geqq \alpha_h, \\ \sum_{\nu=1}^{h} \alpha_\nu = n \end{cases}$$

erfüllt sind. Wir schreiben die ersten Elemente der h Zeilen alle untereinander, ebenso die zweiten, usw., etwa wie in dem folgenden Schema, in welchem die Punkte Ziffern darstellen:

$$\begin{array}{l} \cdot\ \cdot\ \cdot \\ \cdot\ \cdot \\ \cdot\ \cdot \end{array} \qquad (\alpha_1, \alpha_2, \alpha_3) = (3, 2, 2); \qquad n = 7.$$

Eine solche Anordnung der Ziffern $1, 2, \ldots, n$ nennen wir ein *Schema* Σ_α. Der Index α bezeichnet die Ziffernfolge $(\alpha_1, \alpha_2, \ldots, \alpha_h)$. Die möglichen Indizes α werden angeordnet durch die Verabredung: Es soll $\alpha > \beta$ sein, wenn die erste nichtverschwindende Differenz $\alpha_\nu - \beta_\nu$ positiv ist. Z. B. ist bei $n = 5$

$$(5) > (4, 1) > (3, 2) > (3, 1, 1) > (2, 2, 1) > (2, 1, 1, 1) > (1, 1, 1, 1, 1).$$

Ist ein Schema Σ_α gegeben, so bezeichnen wir mit p alle diejenigen Permutationen, welche nur die Ziffern innerhalb der Zeilen des Schemas vertauschen, diese Zeilen selbst aber invariant lassen, mit q dagegen diejenigen Permutationen, die nur die Ziffern innerhalb der Spalten des Schemas vertauschen. Für jedes feste q verstehen wir unter σ_q die Zahl $+1$ oder -1, je nachdem q eine gerade oder eine ungerade Permutation ist. Ist s irgendeine Permutation, so bezeichnen wir mit $s\Sigma_\alpha$ das Schema, in das Σ_α durch die Permutation s übergeht. Man sieht leicht: Wenn q die Spalten von Σ_α invariant läßt, so läßt sqs^{-1} die Spalten von $s\Sigma_\alpha$ invariant, und umgekehrt. Schließlich setzen wir (im Gruppenring $\mathfrak{o}$) für jedes feste Σ_α

$$S_\alpha = \sum_p p,$$

$$A_\alpha = \sum_q q\,\sigma_q.$$

Man verifiziert leicht die Regeln:

$$(2)\qquad p\,S_\alpha = S_\alpha\,p = S_\alpha,$$

$$(3)\qquad A_\alpha\,q\,\sigma_q = q\,A_\alpha\,\sigma_q = A_\alpha.$$

Aus (2) und (3) folgt leicht, daß S_α und A_α bis auf einen Faktor f_α idempotent sind. Die weiteren algebraischen Eigenschaften der S_α und A_α fließen aus folgendem *kombinatorischen Hilfssatz*:

Es seien Σ_α und Σ_β zwei Schemata von der obigen Art; es sei $\alpha \geqq \beta$. Wenn dann in Σ_α nirgends zwei Ziffern in einer Zeile vorkommen, die in Σ_β in einer Spalte stehen, so ist $\alpha = \beta$, und das Schema Σ_α geht durch eine Permutation von der Gestalt pq in das Schema Σ_β über:

$$p\,q\,\Sigma_\alpha = \Sigma_\beta.$$

(Die Bezeichnungen p und q beziehen sich auf Σ_α; d. h. p läßt die Zeilen und q die Spalten von Σ_α invariant.)

Beweis: Aus $\alpha \geqq \beta$ folgt $\alpha_1 \geqq \beta_1$. In der ersten Zeile von Σ_α stehen α_1 Ziffern. Wenn dieselben Ziffern in Σ_β alle in verschiedenen Spalten stehen sollen, so muß Σ_β mindestens α_1 Spalten haben, woraus $\alpha_1 \leqq \beta_1$ und somit $\alpha_1 = \beta_1$ folgt. Durch eine Permutation q_1', die die Spalten von Σ_β invariant läßt, lassen sich diese Ziffern alle in die erste Zeile von Σ_β bringen.

Aus $\alpha \geqq \beta$ folgt nunmehr $\alpha_2 \geqq \beta_2$. In der zweiten Zeile von Σ_α stehen α_2 Ziffern. Wenn diese in $q_1'\,\Sigma_\beta$ alle in verschiedenen Spalten stehen sollen, so muß $q_1'\,\Sigma_\beta$, abgesehen von der ersten Zeile, die ja schon besetzt ist, noch mindestens α_2 Spalten

haben. Daraus folgt $\alpha_2 \leqq \beta_2$, somit $\alpha_2 = \beta_2$. Durch eine Permutation q_2', die die Spalten von $q_1' \Sigma_\beta$ und auch die erste Zeile invariant läßt, lassen sich die genannten Ziffern alle in die zweite Zeile von Σ_β bringen.

So weiter schließend, erhält man ein Schema $q' \Sigma_\beta = q_h' \cdots q_2' q_1' \Sigma_\beta$, dessen Zeilen mit denen von Σ_α übereinstimmen. Man kann also Σ_α durch eine Permutation p in $q' \Sigma_\beta$ überführen:

$$q' \Sigma_\beta = p \Sigma_\alpha .$$

Die Permutation $q' = q_h' \cdots q_2' q_1'$ läßt die Spalten von Σ_β und daher auch die von $q' \Sigma_\beta = p \Sigma_\alpha$ invariant. Bei passendem q ist also

$$q' = p q^{-1} p^{-1}$$

und daher

$$p q^{-1} p^{-1} \Sigma_\beta = p \Sigma_\alpha ,$$
$$\Sigma_\beta = p q \Sigma_\alpha , \qquad \text{q. e. d.}$$

Aus dem kombinatorischen Hilfssatz folgt zunächst

$$A_\beta S_\alpha = 0 \quad \text{für} \quad \alpha > \beta . \tag{4}$$

Denn nach dem Hilfssatz muß es im Falle $\alpha > \beta$ ein Ziffernpaar geben, das in Σ_α in einer Zeile und in Σ_β in einer Spalte steht. Ist t die Transposition, die dieses Ziffernpaar vertauscht, so ist nach (2) und (3)

$$A_\beta S_\alpha = A_\beta t t^{-1} S_\alpha = - A_\beta S_\alpha ,$$

woraus (4) folgt.

Ebenso beweist man

$$S_\alpha A_\beta = 0 \quad \text{für} \quad \alpha > \beta .$$

Aber auch alle Transformierten von A_β werden von S_α annulliert:

$$S_\alpha s A_\beta s^{-1} = 0 \quad \text{für} \quad \alpha > \beta ;$$

denn $s A_\beta s^{-1}$ ist wieder ein A_β, nur zum permutierten Schema $s \Sigma_\beta$. Aus diesem Ergebnis folgt durch Multiplikation mit $s \Omega$ und Summation über alle s aus $\mathfrak{G}$

$$S_\alpha (\sum s \Omega) A_\beta = (0)$$

oder

$$S_\alpha \mathfrak{o} A_\beta = (0) \qquad (\alpha > \beta) . \tag{5}$$

Die Linksideale $\mathfrak{o} A_\beta$ mit $\beta < \alpha$ werden also durch S_α annulliert; oder auch: S_α wird in der durch $\mathfrak{o} A_\beta$ vermittelten Darstellung durch Null dargestellt. Dagegen ist $S_\alpha A_\alpha \neq 0$, da der Koeffizient des Einselements im Produkt $S_\alpha A_\alpha$ nicht verschwindet. S_α wird also in der durch $\mathfrak{o} A_\alpha$ vermittelten Darstellung nicht durch Null dargestellt; somit enthält diese Darstellung mindestens einen irreduziblen Bestandteil, der sicher noch in keinem $\mathfrak{o} A_\beta$ mit $\beta < \alpha$ vorkommt. Diesen irreduziblen Bestandteil wollen wir jetzt näher bestimmen.

Das Element $S_\alpha A_\alpha = \sum_p \sum_q p q \sigma_q$ hat nach (2) und (3) die Eigenschaft

$$p S_\alpha A_\alpha q \sigma_q = S_\alpha A_\alpha .$$

Wir beweisen nun, daß $S_\alpha A_\alpha$ bis auf einen Faktor das einzige Element mit dieser Eigenschaft ist; d. h. wir beweisen: *Wenn ein Element a von $\mathfrak{o}$ die Eigenschaft*

$$p a q \sigma_q = a \tag{6}$$

für alle p und q besitzt, muß a die Gestalt $(S_\alpha A_\alpha) \cdot \lambda$ haben.

Beweis: Wir setzen

$$a = \sum_s s \gamma_s \qquad (\gamma_s \in \Omega) . \tag{7}$$

Einsetzung von (7) in (6) ergibt:

$$\sum_s s \gamma_s = \sum_s p s q \sigma_q \gamma_s . \tag{8}$$

Auf der linken Seite kommt nur ein Glied mit pq vor, nämlich $pq\gamma_{pq}$; auf der rechten Seite auch nur eins, nämlich das Glied mit $s = 1$. Vergleichung der Koeffizienten ergibt:

$$\gamma_{pq} = \sigma_q \gamma_1 .$$

Wir greifen nun ein s heraus, welches nicht die Gestalt pq hat. Dann ist $s\Sigma_\alpha$ von allen $pq\Sigma_\alpha$ verschieden, und nach dem kombinatorischen Hilfssatz gibt es zwei Ziffern j, k, die in Σ_α in einer Zeile, in $s\Sigma_\alpha$ in einer Spalte stehen. Ist t die Transposition dieser Ziffern: $t = (jk)$, so vertauscht $t' = s^{-1}ts$ nur die Ziffern $s^{-1}j$ und $s^{-1}k$, die in $s^{-1}s\Sigma_\alpha = \Sigma_\alpha$ in einer Spalte stehen. Daher ist t eine Permutation p und t' eine Permutation q, und in (8) können wir $p = t$ und $q = t'$ setzen; dann wird für unser spezielles s

$$p s q = t s s^{-1} t s = s ,$$
$$\sigma_q = -1;$$

also ergibt die Vergleichung der Glieder mit s links und rechts in (8):

$$\gamma_s = -\gamma_s , \qquad \gamma_s = 0 .$$

In (7) kommen also nur die Glieder mit $s = pq$, $\gamma_s = \sigma_q \gamma_1$ vor, und es wird

$$a = \sum_{p,q} p q \sigma_q \gamma_1 = (S_\alpha A_\alpha)\gamma_1 , \qquad \text{q. e. d.}$$

Aus dem eben Bewiesenen folgt sofort, daß für jedes Element b von $\mathfrak{o}$ das Element $S_\alpha b A_\alpha$ die Gestalt $(S_\alpha A_\alpha)\lambda$ hat; denn für jedes p und jedes q ist

$$p S_\alpha b A_\alpha q \sigma_q = S_\alpha b A_\alpha .$$

Es ist also

$$S_\alpha \mathfrak{o} A_\alpha \leqq (S_\alpha A_\alpha)\Omega .$$

Setzen wir $S_\alpha A_\alpha = I_\alpha$, so folgt

$$I_\alpha \mathfrak{o} I_\alpha \leqq S_\alpha \mathfrak{o} A_\alpha \leqq I_\alpha \Omega . \tag{9}$$

Wir behaupten nun, daß $\mathfrak{o} I_\alpha$ ein minimales Linksideal ist. Ist nämlich $\mathfrak{l}$ ein Unterideal von $\mathfrak{o} I_\alpha$, so folgt aus (9):

$$I_\alpha \mathfrak{l} \leqq I_\alpha \Omega ,$$

also, da $I_\alpha \Omega$ ein eingliedriger, also minimaler Ω-Modul ist, entweder

$$I_\alpha \mathfrak{l} = I_\alpha \Omega \quad \text{oder} \quad I_\alpha \mathfrak{l} = (0) .$$

Im ersten Fall folgt $\mathfrak{o} I_\alpha = \mathfrak{o} I_\alpha \Omega \leqq I_\alpha \mathfrak{l} \leqq \mathfrak{l}$, mithin $\mathfrak{l} = \mathfrak{o} I_\alpha$. Im zweiten Fall folgt $\mathfrak{l}^2 \leqq \mathfrak{o} I_\alpha \mathfrak{l} = (0)$, mithin, da es kein nilpotentes Ideal außer (0) gibt, $\mathfrak{l} = (0)$.

Die minimalen Linksideale $\mathfrak{o} I_\alpha$ und $\mathfrak{o} I_\beta$ sind für $\alpha > \beta$ nicht operatorisomorph. Nach (5) ist nämlich für $\alpha > \beta$

$$S_\alpha \mathfrak{o} I_\beta = S_\alpha \mathfrak{o} S_\beta A_\beta \leqq S_\alpha \mathfrak{o} A_\beta = (0) ,$$

also für jedes a' aus $\mathfrak{o} I_\beta$:

$$S_\alpha a' = 0 .$$

Wäre nun $\mathfrak{o} I_\alpha \cong \mathfrak{o} I_\beta$, so müßte auch für jedes a aus $\mathfrak{o} I_\alpha$

$$S_\alpha a = 0$$

sein; aber das trifft für $a = I_\alpha = S_\alpha A_\alpha$ nicht zu, da $S_\alpha^2 A_\alpha = f_\alpha S_\alpha A_\alpha \neq 0$.

Jedes Linksideal $\mathfrak{o} I_\alpha$ vermittelt eine irreduzible Darstellung $\mathfrak{D}_\alpha$, und diese Darstellungen sind nach dem eben Bemerkten für verschiedene α inäquivalent.

Die Anzahl der so gefundenen Darstellungen $\mathfrak{D}_\alpha$ ist gleich der Anzahl der Lösungen von (1)[1]. Diese Anzahl gibt aber zugleich die Anzahl der Klassen konjugierter Permutationen an; denn jede solche Klasse besteht aus allen Elementen, die in Zyklen bestimmter Längen $\alpha_1, \alpha_2, \ldots, \alpha_h$ zerfallen, und diese Längen können wieder den Bedingungen (1) gemäß angeordnet werden. Da aber die Anzahl *aller* inäquivalenten irreduziblen Darstellungen durch die Anzahl der Klassen konjugierter Permutationen gegeben ist, so zeigt sich, daß *die Darstellungen $\mathfrak{D}_\alpha$ bis auf Äquivalenz alle irreduziblen Darstellungen der symmetrischen Gruppe $\mathfrak{S}_n$ erschöpfen.*

Die minimalen Linksideale $\mathfrak{o} I_\alpha$ sind im vorangehenden rational bestimmt worden. Hieraus folgt die *Rationalität der irreduziblen Darstellungen* (sowie der Charaktere).

Für die explizite Berechnung der Charaktere und Grade der Darstellungen sei auf die Abhandlungen von FROBENIUS[2], WEYL[3] und SCHUR[4] verwiesen.

§ 128. Anwendungen der Darstellungstheorie auf die Theorie der nichtkommutativen Körper[5].

Wir bemerkten schon im § 120, daß jede Darstellung eines hyperkomplexen Systems $\mathfrak{S}$ in einem kommutativen Körper K, der den Grundkörper P umfaßt, durch eine Darstellung des erweiterten Systems $\mathfrak{S}_\mathsf{K}$ vermittelt wird. In der Sprache der Darstellungsmoduln heißt dies, daß jeder Modul, der $\mathfrak{S}$ als Links- und K als Rechtsmultiplikatorenbereich besitzt, auch als $\mathfrak{S}_\mathsf{K}$-Linksmodul aufgefaßt werden kann. Der Beweis kam darauf hinaus, daß man, wenn $\mathfrak{S} = a_1 \mathsf{P} + \cdots + a_n \mathsf{P}$ und daher $\mathfrak{S}_\mathsf{K} = a_1 \mathsf{K} + \cdots + a_n \mathsf{K}$ gesetzt wird, für die Elemente m des Moduls die Linksmultiplikation mit einem Element von $\mathfrak{S}_\mathsf{K}$ erklärt durch

$$(a_1 \varkappa_1 + \cdots + a_n \varkappa_n)\, m = a_1 m \varkappa_1 + \cdots + a_n m \varkappa_n .$$

Die Verifikation der Rechnungsregeln für den $\mathfrak{S}_\mathsf{K}$-Modul bietet keinerlei Schwierigkeiten; nur wird beim Beweis des Assoziativgesetzes

$$(b\,c)\, m = b\,(c\, m)$$

wesentlich die Kommutativität benutzt: Ist etwa $b = a_1 \varkappa_1$, $c = a_2 \varkappa_2$ (es genügt offenbar, diesen Spezialfall zu betrachten), so folgt das Assoziativgesetz aus den Relationen

$$(a_1 \varkappa_1 \cdot a_2 \varkappa_2)\, m = (a_1 a_2 \varkappa_1 \varkappa_2)\, m = (a_1 a_2)\, m\, (\varkappa_1 \varkappa_2),$$

$$a_1 \varkappa_1 (a_2 \varkappa_2 \cdot m) = a_1 \varkappa_1 (a_2 m \varkappa_2) = a_1 (a_2 m \varkappa_2)\, \varkappa_1 = (a_1 a_2)\, m\, (\varkappa_2 \varkappa_1) .$$

Die beiden Ausdrücke sind in der Tat einander gleich, weil $\varkappa_1 \varkappa_2 = \varkappa_2 \varkappa_1$ ist.

Man kann aber auch für nichtkommutative Körper die Situation retten durch Einführung des Begriffs des *inversen Rings* (bzw. *Körpers*) nach § 118. Wir bezeichnen den inversen Ring zu $\mathfrak{R}$ allgemein mit $\mathfrak{R}'$, und bemerken vorher, daß, wenn $\mathfrak{R}$ hyperkomplex über dem kommutativen Körper P ist, $\mathfrak{R}'$ ebenfalls als hyperkomplexes System über P aufgefaßt werden kann.

---

[1] Zu jeder Lösung von (1) gehören zwar noch verschiedene Schemata, die sich nur durch die Anordnung der Ziffern unterscheiden und verschiedene p_α ergeben können; es genügt aber, zu jedem α ein einziges p_α zu wählen.

[2] FROBENIUS: Sitzungsber. Berlin 1900, S. 516.

[3] WEYL, H.: Math. Zeitschr. 23 (1925), S. 271.

[4] SCHUR, I.: Sitzungsber. Berlin 1927, S. 58.

[5] Die in diesem Paragraphen benutzten Schlußweisen entstammen einer Vorlesung von E. NOETHER über nichtkommutative Algebra (Göttingen, Sommer 1928); vgl. eine demnächst in der Math. Zeitschr. erscheinende Arbeit von E. NOETHER.

Jeder Modul, der $\mathfrak{S}$ *als Links- und* K *als Rechtsmultiplikatorenbereich besitzt, wo* $\mathfrak{S}$ *und* K *hyperkomplexe Systeme über demselben Grundkörper* P *sind*[1]*, kann als* $(\mathfrak{S} \times \mathsf{K}')$*-Linksmodul*[2] *[oder als* $(\mathfrak{S}' \times \mathsf{K})$*-Rechtsmodul] aufgefaßt werden.*

Beweis wie oben: Es sei $\mathfrak{S} = a_1 \mathsf{P} + \cdots + a_n \mathsf{P}$ und daher $\mathfrak{S} \times \mathsf{K}' = a_1 \mathsf{K}' + \cdots + a_n \mathsf{K}'$; dann definieren wir

$$(1) \qquad (a_1 \varkappa_1' + \cdots + a_n \varkappa_n') m = a_1 m \varkappa_1 + \cdots + a_n m \varkappa_n .$$

Alle Rechnungsregeln sind jetzt leicht zu verifizieren. Das Assoziativgesetz $(bc)m = b(cm)$ folgt aus

$$(a_1 \varkappa_1' \cdot a_2 \varkappa_2') m = (a_1 a_2 \varkappa_1' \varkappa_2') m = (a_1 a_2) m (\varkappa_2 \varkappa_1),$$
$$a_1 \varkappa_1' (a_2 \varkappa_2' \cdot m) = a_1 \varkappa_1' (a_2 m \varkappa_2) = a_1 (a_2 m \varkappa_2) \varkappa_1 = (a_1 a_2) m (\varkappa_2 \varkappa_1) .$$

In derselben Weise kann man umgekehrt einen $(\mathfrak{S} \times \mathsf{K}')$-Linksmodul auch als einen $\mathfrak{S}$-Links- und K-Rechtsmodul auffassen, vermöge der Definition $m\varkappa = \varkappa' m$. Es handelt sich im Grunde offenbar nur darum, daß die Modulisomorphismen, die durch Multiplikation der Modulelemente mit den Elementen von K' hervorgerufen werden, statt links auch rechts geschrieben werden können, nur daß dann die Reihenfolge der Multiplikationen sich umkehrt: m wird mit $\varkappa_1 \varkappa_2$ von rechts multipliziert, indem man zuerst mit $\varkappa_1$, dann mit $\varkappa_2$ von rechts multipliziert, dagegen mit $\varkappa_1' \varkappa_2'$ von links, indem man erst mit $\varkappa_2'$, dann mit $\varkappa_1'$ von links multipliziert. Isomorphe $(\mathfrak{S} \times \mathsf{K}')$-Moduln ergeben auch isomorphe $\mathfrak{S}$-Links- und K-Rechtsmoduln, und umgekehrt.

Diese Tatsachen gestatten mannigfache Anwendungen, insbesondere auf den Fall, daß K und $\mathfrak{S}$ beide einfache hyperkomplexe Systeme[3] oder speziell Körper endlichen Ranges über P sind. Nehmen wir etwa an, P sei das Zentrum von K (also auch von K'). Dann haben wir in § 119 bewiesen, daß das Produkt $\mathfrak{S} \times \mathsf{K}'$ wieder ein einfaches System ist. Daraus folgt nach § 118 und § 121, daß alle irreduziblen $(\mathfrak{S} \times \mathsf{K}')$-Linksmoduln zueinander und zu den minimalen Linksidealen von $\mathfrak{S} \times \mathsf{K}'$ isomorph sind. Ebenso ist $\mathfrak{S}' \times \mathsf{K}$ einfach, also alle $(\mathfrak{S}' \times \mathsf{K})$-Rechtsmoduln und minimalen Rechtsideale in $\mathfrak{S}' \times \mathsf{K}$ zueinander isomorph. Damit ist bewiesen:

Sind $\mathfrak{S}$ *und* K *einfache hyperkomplexe Systeme über* P *und ist das Zentrum von* K *gleich* P*, so ist jeder minimale* $\mathfrak{S}$*-Links- und* K*-Rechtsmodul* $\mathfrak{M}$ *(insbesondere, falls* K *ein Körper ist, jeder irreduzible Darstellungsmodul von* $\mathfrak{S}$ *in* K*) nach der obigen Vorschrift aus einem minimalen Linksideal in* $\mathfrak{S} \times \mathsf{K}'$ *oder einem minimalen Rechtsideal in* $\mathfrak{S}' \times \mathsf{K}$ *zu gewinnen. Alle diese minimalen Doppelmoduln sind untereinander isomorph.*

Wir betrachten zunächst den einfachsten Fall, daß $\mathfrak{S}$ und K beide Körper sind und es sich um einen Darstellungsmodul $\mathfrak{M}$ vom Rang 1 in bezug auf K handelt. Die zugehörige Darstellung 1. Grades bildet dann $\mathfrak{S}$ isomorph auf einen Unterkörper Σ von K ab. Da die Isomorphie zugleich Operatorisomorphie in bezug auf P ist, so werden die Elemente von P dabei auf sich selbst abgebildet. Mit dieser Einschränkung wird jede Isomorphie $\mathfrak{S} \cong \Sigma \subseteq \mathsf{K}$ durch einen Darstellungsmodul $\mathfrak{M}$ vom Rang 1 vermittelt. Aus dem obigen Satz folgt zunächst, daß alle diese Darstellungen untereinander äquivalent sind. Das heißt: Sind zwei solche Darstellungen

---

[1] K darf auch ein beliebiger Erweiterungsring von P sein, der P in seinem Zentrum enthält.

[2] Das soll heißen, daß die Operatoren aus $\mathfrak{S} \times \mathsf{K}'$ links von den Modulelementen geschrieben werden sollen.

[3] Unter einem „einfachen System" wird im folgenden immer ein einfaches hyperkomplexes System mit Einselement verstanden.

$\mathfrak{S} \cong \Sigma_1$ und $\mathfrak{S} \cong \Sigma_2$ gegeben, so gehen entsprechende Elemente s_1 von Σ_1 und s_2 von Σ_2 durch eine Transformation

$$s_1 = \varkappa\, s_2\, \varkappa^{-1} \tag{2}$$

ineinander über. Wählt man etwa $\mathfrak{S} = \Sigma_1$ und $\Sigma_2 \cong \Sigma_1$, so folgt:

Jeder Isomorphismus zweier Unterkörper Σ_1, Σ_2 von K, der die Elemente des Zentrums P invariant läßt, wird durch eine Transformation mit einem Element $\varkappa$ von K gemäß (2) hervorgebracht.

Insbesondere ist jeder Automorphismus von K, der die Elemente von P invariant läßt, ein innerer.

Genau so beweist man allgemeiner durch Betrachtung irreduzibler Darstellungsmoduln beliebigen Ranges, daß jedes einfache System $\mathfrak{S}$ über P eine und bis auf Äquivalenz (d. h. bis auf innere Transformationen des vollen Matrizenringes) nur eine irreduzible Darstellung durch Matrizes beliebigen Grades in K zuläßt, wenn wieder P das Zentrum des Körpers K ist. Insbesondere ist jeder Automorphismus des Matrizenringes K_r, der die Elemente von P fest läßt, ein innerer.

Untersuchen wir nun, in welcher Weise eine Darstellung 1. Grades $\mathfrak{S} \cong \Sigma$ durch ein Rechtsideal von $\mathfrak{S}' \times \mathsf{K}$ vermittelt werden kann. Da die Darstellung vom ersten Grade ist, so muß das Rechtsideal $\mathfrak{r}$ vom Rang 1 in bezug auf K sein, also etwa

$$\mathfrak{r} = r\,\mathsf{K}.$$

Das Ideal $\mathfrak{r}$ ist nach unserer Vorschrift als $\mathfrak{S}$-Linksmodul aufzufassen, indem man die Multiplikation eines Elements $r\varkappa$ von $\mathfrak{r}$ mit einem Element s von $\mathfrak{S}$ so definiert:

$$s(r\varkappa) = (r\varkappa)s', \quad \text{insbesondere} \quad sr = rs'.$$

Stellt man das Element rs' wieder in der Form $r\sigma\,(\sigma \in \mathsf{K})$ dar, in der ja alle Elemente von $\mathfrak{r}$ eindeutig geschrieben werden können, so hat man

$$sr = rs' = r\sigma, \tag{3}$$

und die Zuordnung $s \to \sigma$ ist die gesuchte Darstellung $\mathfrak{S} \cong \Sigma$.

Es ist nun leicht, die Struktur von $\mathfrak{S}' \times \mathsf{K}$ zu bestimmen. $\mathfrak{S}' \times \mathsf{K}$ ist isomorph einem Matrizenring im Automorphismenkörper von $\mathfrak{r}$. Ein Automorphismus φ ist durch

$$\varphi(r) = r\varkappa_0, \tag{4}$$

$$\varphi(r\varkappa) = r\varkappa_0\varkappa \quad \text{für} \quad \varkappa \in \mathsf{K} \tag{5}$$

gegeben. Soll Operatorisomorphie in bezug auf $\mathfrak{S}' \times \mathsf{K}$ bestehen, so braucht sie nur noch in bezug auf $\mathfrak{S}'$ zu bestehen:

$$\varphi(rs') = \varphi(r)s'.$$

Daraus ergibt sich mit Hilfe von (3), (4), (5):

$$r\varkappa_0\sigma = r\varkappa_0 s' = rs'\varkappa_0 = r\sigma\varkappa_0,$$

also

$$\varkappa_0\sigma = \sigma\varkappa_0;$$

d. h.: das Element $\varkappa_0$, das den Automorphismus vermittelt, muß mit allen Elementen σ von Σ vertauschbar sein. Die mit allen Elementen von Σ vertauschbaren Elemente τ bilden einen Unterkörper T von K. Jedem Automorphismus φ entspricht eineindeutig ein Element $\varkappa_0$ von T; der Summe $\varphi_1 + \varphi_2$ und dem Produkt $\varphi_1\varphi_2$ entsprechen die Summe $\varkappa_1 + \varkappa_2$ und das Produkt $\varkappa_1\varkappa_2$:

$$(\varphi_1 + \varphi_2)(r) = \varphi_1(r) + \varphi_2(r) = r\varkappa_1 + r\varkappa_2 = r(\varkappa_1 + \varkappa_2),$$

$$\varphi_1\varphi_2(r) = \varphi_1(r\varkappa_2) = r\varkappa_1\varkappa_2.$$

Also ist der Automorphismenkörper isomorph zu T, und $\mathfrak{S}' \times \mathsf{K}$ ist isomorph einem Matrizenring im Körper T. Damit ist bewiesen:

Ist $\mathfrak{S}'$ invers-isomorph zu einem Unterkörper Σ von K und ist T die Gesamtheit derjenigen Elemente von K, die mit allen Elementen von Σ vertauschbar sind, so ist $\mathfrak{S}' \times \mathsf{K}$ isomorph einem Matrizenring im Körper T.

Man kann diesen Satz noch kürzer so beweisen: $\mathfrak{S}' \times \mathsf{K}$ ist isomorph einem Matrizenring im Automorphismenkörper eines minimalen Rechtsideals $\mathfrak{r}$. Diesem Rechtsideal ist nach dem Obigen ein $\mathfrak{S}$-Links- und K-Rechtsmodul $\mathfrak{M}$ (vom Rang 1 über K) zugeordnet. Den Operatorautomorphismen von $\mathfrak{r}$ entsprechen Operatorautomorphismen des Doppelmoduls $\mathfrak{M}$. Faßt man nun $\mathfrak{M}$ zunächst nur als K-Modul auf, so ist $\mathfrak{M}$ ein Linearformenmodul vom Rang 1 und seine Automorphismen φ sind lineare Transformationen, die durch eine (einreihige und einspaltige) Matrix (τ) vermittelt werden, wo $\tau \in \mathsf{K}$. Die Multiplikation der Elemente von $\mathfrak{M}$ mit einem Element s von $\mathfrak{S}$ von links ergibt ebenfalls eine lineare Transformation von $\mathfrak{M}$, die durch eine Matrix (σ) vermittelt wird; die Zuordnung $s \to \sigma$ ist dann eben die durch $\mathfrak{M}$ vermittelte Darstellung von $\mathfrak{S}$ in Σ. Soll nun die lineare Transformation φ ein Operatorisomorphismus des Doppelmoduls $\mathfrak{M}$ auch in bezug auf die Multiplikation mit den Elementen s von $\mathfrak{S}$ sein, so muß die Transformation φ mit diesen Multiplikationen vertauschbar sein. Das ist aber dann und nur dann der Fall, wenn die Matrizes (τ), (σ) vertauschbar sind:

$$\tau\sigma = \sigma\tau .$$

Die τ mit dieser Eigenschaft bilden gerade den Körper T. Die Matrizes (τ) und daher auch die Elemente τ entsprechen eineindeutig und isomorph den Automorphismen φ des Doppelmoduls $\mathfrak{M}$ und daher auch den Automorphismen von $\mathfrak{r}$.

Wörtlich ebenso beweist man allgemeiner:

Ist $\mathfrak{S}$ ein einfaches hyperkomplexes System über P, K ein Körper endlichen Grades mit Zentrum P, und ist $\mathfrak{S} \to \Sigma$ eine isomorphe irreduzible Darstellung r-ten Grades von $\mathfrak{S}$ durch Matrizes in K, so ist die Gesamtheit der mit allen Elementen von Σ vertauschbaren Matrizes ein Körper T, und $\mathfrak{S}' \times \mathsf{K}$ ist isomorph einem Matrizenring im Körper T. Ist Σ kommutativ, so ist $\mathsf{T} \supseteq \Sigma$.

Kehren wir nun zu den Darstellungen 1. Grades $\mathfrak{S} \to \Sigma$ zurück und setzen

$$(\Sigma/\mathsf{P}) = \sigma; \qquad (\mathsf{T}/\mathsf{P}) = \tau; \qquad (\mathsf{K}/\mathsf{P}) = m^2,$$

so ist das Ideal $\mathfrak{r}$ vom Rang 1 über K, also vom Rang m^2 über P. Der Rang des ganzen Ringes $\mathfrak{S}' \times \mathsf{K}$ ist gleich σm^2, also die Anzahl der Ideale $\mathfrak{r}$, in die $\mathfrak{S}' \times \mathsf{K}$ zerfällt, gleich σ. Daher ist auch der Grad der Matrizes des Matrizenringes $\mathfrak{S}' \times \mathsf{K}$ gleich σ und der Rang von $\mathfrak{r}$ über T ebenfalls gleich σ. Daraus folgt, daß der Rang von $\mathfrak{r}$ über P gleich $\sigma\tau$ ist, mithin

$$\sigma\tau = m^2 . \tag{6}$$

Wählt man speziell $\Sigma = \mathsf{K}$, so wird $\mathsf{T} = \mathsf{P}$; mithin gilt: *$\mathsf{K} \times \mathsf{K}'$ ist ein voller Matrizenring im Körper P.*

Wählt man für Σ einen maximalen kommutativen Unterkörper von K, so wird $\mathsf{T} = \Sigma$; denn die einzigen mit Σ vertauschbaren Elemente sind die von Σ selbst. Wäre nämlich noch ein nicht in Σ enthaltenes Element Θ mit Σ vertauschbar, so wäre $\Sigma(\Theta)$ auch noch kommutativ, entgegen der Maximalität von Σ. Also wird $\mathfrak{S}' \times \mathsf{K} = \mathfrak{S} \times \mathsf{K}$ ein Matrizenring im Körper Σ oder im Körper $\mathfrak{S}$ selber. $\mathfrak{S}$ ist also das, was wir in § 119 einen *Zerfällungskörper* von K genannt haben. Aus (6) folgt wegen $\tau = \sigma$:

$$\sigma^2 = m^2 ,$$

$$\sigma = m .$$

Also:

Die maximalen kommutativen Unterkörper Σ eines Körpers K sind Zerfällungskörper, und ihr Grad ist gleich dem „Index" m von K.

Es sei noch bemerkt, daß jedes Element $\varkappa$ von K in mindestens einem maximalen kommutativen Unterkörper Σ enthalten ist. $\mathsf{P}(\varkappa)$ ist nämlich sicher kommutativ und kann zu einem maximalen kommutativen Körper ergänzt werden.

Wir wollen nun einige Anwendungen dieser Sätze auf spezielle Probleme behandeln.

1. Bestimmung aller nichtkommutativen Körper endlichen Grades über dem Körper der reellen Zahlen als Grundkörper.

Ist P der Körper der reellen Zahlen, K der gesuchte Erweiterungskörper vom Index m, Z das Zentrum von K und Σ ein maximaler kommutativer Unterkörper, so ist

$$\mathsf{P} \subseteq \mathsf{Z} \subseteq \Sigma \subset \mathsf{K}; \qquad (\Sigma/\mathsf{Z}) = m; \qquad (\mathsf{K}/\mathsf{Z}) = m^2.$$

Da K nichtkommutativ ist, muß $m > 1$ sein. Für die Körper Z und Σ kommen nur P und $\mathsf{P}(i)$, der Körper der komplexen Zahlen, in Betracht; denn andere kommutative endliche Erweiterungen hat P nicht. Wegen $m > 1$ ist $\Sigma \neq \mathsf{Z}$; also muß

$$\Sigma = \mathsf{P}(i), \qquad \mathsf{Z} = \mathsf{P}, \qquad m = 2$$

sein. Der gesuchte Körper K kann also nur den Grad $m^2 = 4$ haben.

Der Isomorphismus von $\mathsf{P}(i)$, der i in $-i$ überführt, muß durch eine Transformation mit einem Element k von K vermittelt werden, d. h. es muß ein k geben mit der Eigenschaft

$$k\,i\,k^{-1} = -i. \tag{7}$$

Da k nicht in $\Sigma = \mathsf{P}(i)$ enthalten ist, muß $\Sigma(k) = \mathsf{K}$ sein; also ist $\mathsf{K} = \mathsf{P}(i, k)$. Aus (7) folgt:

$$k^2\,i\,k^{-2} = i;$$

d.h. k^2 ist mit i vertauschbar. Da k^2 auch mit k vertauschbar ist, so liegt k^2 im Zentrum: $k^2 = a \in \mathsf{P}$.

Wäre $a \geqq 0$, so wäre $a = b^2$,

$$k^2 - b^2 = (k - b)(k + b) = 0,$$

$$k - b = 0 \quad \text{oder} \quad k + b = 0,$$

also $k \in \mathsf{P}$, was nicht geht. Also muß $a < 0$ sein: $a = -b^2 (b \neq 0)$. Durch Multiplikation von k mit dem reellen Faktor b^{-1} erreicht man, daß $k^2 = -1$ wird, ohne daß die bisherigen Eigenschaften von k verlorengehen. Für i und k gelten also die Relationen

$$k\,i = -i\,k,$$

$$i^2 = k^2 = -1.$$

Diese charakterisieren aber den Quaternionenkörper. *Also ist der Quaternionenkörper der einzig mögliche nichtkommutative Körper von endlichem Grade über dem Körper der reellen Zahlen als Grundkörper.*

2. Bestimmung aller endlichen Körper (Körper mit endlichvielen Elementen).

Ist K ein endlicher Körper, Z sein Zentrum, m^2 der Rang von K über Z, so ist jedes Element von K in einem maximalen kommutativen Unterkörper Σ vom Grade m über Z enthalten. Nun sind alle kommutativen Erweiterungen m-ten Grades Σ eines Galoisfeldes Z von p^n Elementen untereinander äquivalent (sie entstehen nämlich durch Adjunktion aller Wurzeln der Gleichung $x^q = x$, $q = p^{nm}$; vgl. § 31). Diese Körper gehen also alle durch Transformation mit Elementen $\varkappa$ von K aus einem unter ihnen, Σ_0, hervor:

$$\Sigma = \varkappa\,\Sigma_0\,\varkappa^{-1}.$$

Läßt man das Nullelement von K weg, so wird K zu einer Gruppe $\mathfrak{G}$, Σ_0 zu einer Untergruppe $\mathfrak{H}$, Σ zu einer konjugierten Untergruppe $\varkappa\mathfrak{H}\varkappa^{-1}$, und diese konjugierten Untergruppen füllen zusammen die ganze Gruppe $\mathfrak{G}$ aus (denn jedes Element von K ist in einem Σ enthalten). Nun gilt aber der folgende gruppentheoretische

Hilfssatz. *Eine echte Untergruppe $\mathfrak{H}$ einer endlichen Gruppe $\mathfrak{G}$ kann unmöglich mit ihren Konjugierten $s\mathfrak{H}s^{-1}$ die ganze Gruppe $\mathfrak{G}$ ausfüllen.*

Beweis: Es seien n und N die Ordnungen von $\mathfrak{H}$ und $\mathfrak{G}$, und j sei der Index von $\mathfrak{H}$, so daß also $N = j \cdot n$ ist. Wenn s und s' zur selben Nebenklasse $s\mathfrak{H}$ gehören, also etwa $s' = sh$ $(h \in \mathfrak{H})$ ist, so folgt:

$$s'\mathfrak{H}s'^{-1} = shh\mathfrak{H}h^{-1}s^{-1} = s\mathfrak{H}s^{-1}.$$

Es gibt also höchstens so viele verschiedene $s\mathfrak{H}s^{-1}$, als es Nebenklassen gibt, d. h. höchstens j. Wenn diese $s\mathfrak{H}s^{-1}$ (zu denen auch $\mathfrak{H}$ gehört) zusammen die Gruppe $\mathfrak{G}$ ausfüllten, so müßten sie elementefremd sein; denn sonst würden sie nicht die erforderlichen $N = j \cdot n$ Elemente aufbringen. Da aber je zwei verschiedene $s\mathfrak{H}s^{-1}$ das Einselement gemein haben, so sind sie niemals elementefremd, und wir haben einen Widerspruch.

Für unseren Fall folgt aus dem Hilfssatz, daß $\mathfrak{H}$ unmöglich eine *echte* Untergruppe von $\mathfrak{G}$ sein kann, daß also $\mathfrak{H} = \mathfrak{G}$ und somit $\mathsf{K} = \Sigma_0$ ist. Folglich ist K kommutativ. Damit ist bewiesen:

Jeder Körper mit endlichvielen Elementen ist kommutativ, also ein Galoisfeld.

Für weitere, tiefergehende Anwendungen der Darstellungstheorie auf die Theorie der hyperkomplexen Größen siehe R. Brauer: Über Systeme hyperkomplexer Zahlen, Math. Zeitschr. Bd. 30, S. 79—107. 1929.

Aufgaben. 1. Es sei K ein Körper von endlichem Rang über einem kommutativen Grundkörper P, Σ ein Zwischenkörper, T der Körper der mit Σ vertauschbaren Elemente. Dann ist der Körper der mit T vertauschbaren Elemente wieder Σ.

2. Ist das Zentrum von Σ in der vorigen Aufgabe gleich P, so ist $\mathsf{K} = \Sigma \times \mathsf{T}$.

3. Ist $\mathfrak{S}$ ein kommutativer Körper endlichen Ranges über P und $\mathfrak{S} \to \Sigma$ eine irreduzible Darstellung r-ten Grades von $\mathfrak{S}$ in K, so ist nach den obigen Sätzen $\mathfrak{S}' \times \mathsf{K}$ isomorph einem Matrizenring in einem Körper $\mathsf{T} \subset \mathsf{K}_r$, der Σ umfaßt und aus den mit Σ elementweise vertauschbaren Elementen von K_r besteht. Man beweise: Dann und nur dann ist $\mathsf{T} = \Sigma$ und $\mathfrak{S}$ Zerfällungskörper von K, wenn Σ ein maximaler kommutativer Unterkörper von K_r ist. Die Zerfällungskörper von K sind also diejenigen Körper, für die es irreduzible Darstellungen als maximale kommutative Unterkörper von K_r gibt. Ihr Rang ist gleich $m \cdot r$, wo m der Index von K ist.

4. Man bestimme alle Körper vom Index 2 über dem rationalen Zahlkörper Γ als Zentrum („verallgemeinerte Quaternionenkörper").

Sachverzeichnis.

Die Zahlen geben die Seiten an, wo die Begriffe zum erstenmal vorkommen.