Abstrakter Aufbau der Idealtheorie in algebraischen Zahl- und Funktionenkörpern.

Von

Emmy Noether in Göttingen.

Im folgenden wird eine abstrakte Charakterisierung all derjenigen Ringe gegeben, deren Idealtheorie übereinstimmt mit der Idealtheorie aller ganzen Größen des algebraischen Zahlkörpers — deren Ideale sich also eindeutig als Potenzprodukte von Primidealen darstellen lassen. Zu diesen Ringen gehören als bekannteste Beispiele noch der Ring aller ganzen Größen eines algebraischen Funktionenkörpers von einer Unbestimmten — allgemeiner von mehr Unbestimmten, sobald man sich mit Kronecker auf Ideale höchster Dimension beschränkt, also den Übergang zu einem gewissen Quotientenring, dem Funktionalbereich, macht.

Die Axiome, die dieser Idealtheorie vollständig äquivalent sind, sind für den zugrunde gelegten kommutativen Ring die folgenden[1]):

I. Teilerkettensatz: Jede Kette von Idealen, bei der jedes Ideal ein echter Teiler des vorangehenden ist, bricht im Endlichen ab — m. a. W.: zu jeder Teilerkette von Idealen gibt es einen Index, von dem an alle Ideale gleich werden.

II. Vielfachen-Kettensatz modulo jedem vom Nullideal verschiedenen Ideal: Jede Kette von Idealen — die sämtlich Teiler eines festen, vom Nullideal verschiedenen Ideals sind —, bei der jedes Ideal ein echtes Vielfaches des vorangehenden ist, bricht im Endlichen ab.

III. Existenz des Einheitselementes der Multiplikation.

IV. Ring ohne Nullteiler.

[1]) Für die Definition der Grundbegriffe der Idealtheorie vgl. etwa E. Noether, Idealtheorie in Ringbereichen, Math. Ann. **83** (1921), S. 24—66 (zitiert Idealtheorie). Übrigens werden die wesentlichsten Begriffe auch in der vorliegenden Arbeit, besonders in §§ 1, 4 und 5, kurz formuliert. Der Vollständigkeit halber ist dabei manches aufgenommen, was für die unmittelbaren Zwecke dieser Arbeit nicht erforderlich ist

V. Ganze Abgeschlossenheit im Quotientenkörper: Jedes Element des Quotientenkörpers, das ganz in bezug auf den Ring ist, gehört dem Ring an.

Aus diesen Axiomen entwickle ich schrittweise eine immer stärker eingeschränkte Idealtheorie bis hin zu der gesuchten; und zeige umgekehrt, daß hier auch alle Axiome tatsächlich erfüllt sind.

Aus dem Teilerkettensatz I folgt, wie ich (Idealtheorie § 4) gezeigt habe, die Darstellung eines Ideals als kleinstes gemeinsames Vielfaches von endlich vielen, zu verschiedenen Primidealen gehörigen Primäridealen. Ich wiederhole hier kurz diesen Beweis (§ 6), weil er sich unter Verwendung des Begriffs des Idealquotienten vereinfachen läßt, und weil ich ein Versehen berichtigen will; der ursprüngliche Beweis benutzt nämlich an einer Stelle die nicht vorausgesetzte Existenz des Einheitselementes der Multiplikation[2]).

Die Voraussetzung des Vielfachen-Kettensatzes bewirkt (§ 7), daß im Restklassenring nach jedem vom Nullideal verschiedenen Ideal ein Primideal keinen echten Teiler besitzen kann, mit Ausnahme des alle Elemente umfassenden Einheitsideales. Damit aber werden die Primärkomponenten dieser Ideale eindeutig bestimmt, mit Ausnahme der zum Einheitsideal gehörigen. In etwas weniger scharfer Fassung findet sich dies Resultat schon bei Masazo Sono[3]); seine Voraussetzung der Existenz einer Kompositionsreihe im Restklassenring ist dem „Doppelkettensatz“ in diesem Ring gleichwertig, wie ich zum Schluß (§ 10) kurz zeige. Dabei verstehe ich unter Doppelkettensatz die Gültigkeit von Teilerketten- und Vielfachenkettensatz ohne Beschränkung auf vom Nullideal verschiedene Ideale.

Ist noch Axiom III — Existenz des Einheitselementes — erfüllt, so tritt das Einheitsideal nicht als zugehöriges Primideal auf; die Primärkomponenten sind also eindeutig bestimmt; sie werden paarweise teilerfremd und ihr kleinstes gemeinsames Vielfaches gleich dem Produkt. Die Axiome I, II, III sind für alle endlichen Ordnungen eines algebraischen Zahlkörpers erfüllt; hier hat schon Dedekind (Dirichlet-Dedekind, Zahlentheorie, 3. Aufl., 11. Suppl., § 172) ohne vollständig ausgeführten Beweis die eindeutige Darstellung eines Ideals als Produkt von paarweise teilerfremden einartigen Idealen (Primärkomponenten) ausgesprochen.

[2]) Auf dieses Versehen machte mich P. Urysohn aufmerksam; meine Abänderung des Beweises war aber etwas umständlicher als die hier mitgeteilte, die von E. Artin stammt. Dieser hatte schon früher für sich die Lücke ausgefüllt und sich auch unabhängig von mir die Vereinfachung mit dem Idealquotienten überlegt. — Eine weitere Vereinfachung, die die Einführung der „reduzierten Darstellung“ vermeidet, entnehme ich einer verwandten Fragestellung bei W. Krull: Algebraische Theorie der Ringe III, Math. Ann. 92 (1924), S. 181—213, Satz I.

[3]) On the Reduction of Ideals. Memoirs of the College of Science, Kyoto University, Series A, 7 (1924), S. 191—204.

Aus Voraussetzung IV — Nichtauftreten von Nullteilern — folgt, daß die verschiedenen Potenzen eines von Null- und Einheitsideal verschiedenen Ideals alle verschieden sind, und daß der Quotientenkörper existiert.

Ist schließlich noch Axiom V der ganzen Abgeschlossenheit im Quotientenkörper erfüllt, so werden die Primärideale — wegen IV eindeutig bestimmte — Potenzen von Primidealen, womit der übliche Zerlegungssatz gewonnen ist (§ 8). Dieser letztere Nachweis beruht auf einer, im Fall des Zahlkörpers schon von Dedekind (3. Aufl., § 172) gezogenen Folgerung aus der ganzen Abgeschlossenheit: Man kann ein echt gebrochenes Element so als Quotient ganzer darstellen, daß auch das Quadrat des Zählers nicht durch den Nenner teilbar wird. An Stelle dieser Folgerung tritt in den späteren Darstellungen — auch als Folge der ganzen Abgeschlossenheit — der viel weniger durchsichtige verallgemeinerte Gaußsche Satz oder entsprechende, etwas mehr aussagende Modulsätze; alles Sätze, die zur Anwendung Basiselemente voraussetzen, während hier mit den Idealen selbst gearbeitet wird.

In der Umkehrung (§ 9) ergeben sich die von Axiom V verschiedenen Axiome fast direkt; letzteres aus dem Nachweis, daß ein echt gebrochenes Element sich stets so darstellen läßt, daß keine Potenz des Zählers durch den Nenner teilbar wird, was also noch eine Verschärfung der ursprünglich aus V gezogenen Folgerung bedeutet. Dieser Nachweis gelingt aber erst, indem aus der Idealdarstellung die üblichen Schlüsse gezogen werden, Hauptidealdarstellung modulo einem festen Ideal und Theorie der gebrochenen Ideale, also der Idealquotienten im Körper. Auch die Tatsache, daß aus der Darstellung durch Primidealpotenzen die ganze Abgeschlossenheit folgt, war schon Dedekind bekannt, wie eine Bemerkung (3. Aufl., § 172, S. 522 unten) zeigt.

Die Axiome I bis V ergeben, daß die vier im allgemeinen getrennten Zerlegungen in kleinste paarweise teilerfremde Ideale, gegenseitig prime Ideale, größte Primärkomponenten und irreduzible Ideale zusammenfallen; und umgekehrt ergibt sich aus diesem Zusammenfallen und den Axiomen I—IV die ganze Abgeschlossenheit. Für Ringe mit Nullteilern folgt aus dem Erfülltsein der übrigen Axiome — wobei V als ganze Abgeschlossenheit im Quotientenring zu definieren ist — nicht notwendig das Zusammenfallen der Zerlegungen, wie das Beispiel des Restklassenringes nach gewissen Idealen einer endlichen Ordnung zeigt (§ 9).

In § 1 skizziere ich die Theorie der in bezug auf einen Ring ganzen Größen, bis hin zu der Dedekindschen Folgerung aus der ganzen Abgeschlossenheit. In § 2 zeige ich, wie die Kettensätze sich vom Ring übertragen auf Moduln aus Linearformen, mit diesem Ring als Koeffizienten-

und Multiplikatorenbereich [4]). Hieraus ziehe ich (§ 3) die Folgerung, daß beim Übergang zu den ganzen Größen eines algebraischen Erweiterungskörpers (erster Art) die Axiome I bis IV für jede Ordnung erhalten bleiben, während für die aus allen ganzen Größen bestehende Ordnung auch V gilt. Diese — für den algebraischen Zahlkörper natürlich bekannte — Tatsache erlaubt die Unterordnung der am Anfang erwähnten Funktionenkörper; insbesondere ist durch den einfachen Nachweis, daß der aus den ganzzahligen Polynomen mehrerer Unbestimmter abgeleitete Funktionalbereich den Axiomen genügt, auch die Kroneckersche Idealtheorie voll eingeordnet [5]).

Die dann entwickelte Idealtheorie setzt diese nur der Einordnung dienenden §§ 2 und 3 nicht voraus. In § 4 und § 5 werden die von den Axiomen I bis V unabhängigen Grundlagen gegeben; dadurch tritt schärfer als in der ursprünglichen Begründung hervor, welche Teile der Theorie von Endlichkeitsvoraussetzungen unabhängig sind.

§ 1.

Theorie der ganzen Größen.

Zugrunde gelegt sei ein kommutativer Ring [6]) $\mathfrak{T}$ *ohne Nullteiler*, mit *Einheitselement e der Multiplikation* (Axiom III und IV); in $\mathfrak{T}$ sei ein

---

[4]) Diese Fassung der Modulsätze rührt von Prüfer her (Neue Begründung der algebraischen Zahlentheorie, § 2, Math. Ann. **94** (1924), S. 198—243) und ist durchsichtiger als die übliche Übertragung der Basissätze.

[5]) Die Verschiedenheit tritt also erst bei den Diskriminantensätzen auf, dadurch bedingt, daß der Restklassenring des Funktionalbereiches nach einer Primzahl ein unvollkommener Körper wird, und somit Erweiterungen zweiter Art auftreten können.

[6]) Ein Ring ist bekanntlich definiert, wenn in einer Menge eine Gleichheitsrelation gegeben ist, und außerdem zwei Verknüpfungen, Addition und Multiplikation, die den üblichen Gesetzen genügen: die Addition ist assoziativ, kommutativ und eindeutig umkehrbar, die Multiplikation ist assoziativ — kommutativ, wenn es sich um einen kommutativen Ring handelt — und gegenüber der Addition distributiv.

Ist dabei die zugrunde gelegte Gleichheitsdefinition nicht die mengentheoretische Identität, so muß — damit in jedem Untersystem dieselbe Gleichheitsdefinition erhalten bleibt — ein solches Untersystem (Unterring, Modul, Ideal) neben irgendeinem Element auch alle ihm gleichen enthalten. Ebenso muß bei jeder Erweiterung vorausgesetzt werden, daß die neue Gleichheitsdefinition die alte umfaßt.

Alle Begriffe wie „endlich viele Elemente“, „eindeutige Zuordnung“, ... sind im Sinne der Gleichheitsdefinition gemeint; es gibt „ein und nur ein Element“ heißt also beispielsweise, es gibt bis auf gleiche nur ein Element. Übrigens kann man von der Gleichheit immer zu einer mengentheoretischen Identität übergehen, indem man gleiche Elemente in eine Klasse zusammenfaßt und diese Klassen als neue Elemente einführt.

Die hier gegebenen Bemerkungen zur Gleichheitsdefinition stammen von R. Hölzer.

fester, das Einheitselement enthaltender *Unterring* $\mathfrak{R}$ ausgezeichnet. Die Begriffe Modul, Ordnung, ganz sollen sich durchweg auf diesen festen Ring $\mathfrak{R}$ beziehen, was der Kürze halber später in der Bezeichnung weggelassen wird [7]). (Die Elemente aus $\mathfrak{R}$ seien mit lateinischen, die aus $\mathfrak{T}$ allgemein mit griechischen Buchstaben bezeichnet.)

1. Ein System $\mathfrak{M}$ von Elementen aus $\mathfrak{T}$ heißt wie üblich $\mathfrak{R}$-*Modul* — kurz *Modul* —, wenn es neben zwei Elementen α und β auch die Differenz, neben α auch $r\alpha$ enthält, unter r ein beliebiges Element aus $\mathfrak{R}$ verstanden. $\mathfrak{M}$ heißt durch $\mathfrak{N}$ teilbar, $\mathfrak{M} \equiv 0\,(\mathfrak{N})$ und $\mathfrak{M}$ ein Vielfaches, $\mathfrak{N}$ ein Teiler, wenn jedes Element von $\mathfrak{M}$ auch in $\mathfrak{N}$ enthalten ist. $\mathfrak{R}$-Moduln, deren Elemente alle zu $\mathfrak{R}$ gehören, heißen *Ideale* in $\mathfrak{R}$.

Offenbar ist der Durchschnitt — das kleinste gemeinsame Vielfache $[\ldots \mathfrak{M}_i \ldots]$ — beliebig vieler Moduln aus $\mathfrak{T}$ wieder ein Modul; ebenso ist $\mathfrak{T}$ Modul. Somit existiert eindeutig der aus einem beliebigen System Σ von Elementen aus $\mathfrak{T}$ *abgeleitete Modul* als Durchschnitt aller Moduln, die Σ umfassen. Die Summe — der größte gemeinsame Teiler $(\ldots \mathfrak{M}_i \ldots)$ — eines beliebigen Systems von Moduln ist der aus der Vereinigungsmenge abgeleitete Modul. Das Produkt $\mathfrak{M}\mathfrak{N}$ zweier Moduln ist definiert als der aus den Elementen $\mu\nu$ abgeleitete Modul, wo μ alle Elemente aus $\mathfrak{M}$, ν alle aus $\mathfrak{N}$ durchläuft. Das Produkt genügt also dem assoziativen und kommutativen Gesetz, da dies für die Ringelemente gilt. Aus dem distributiven Gesetz in $\mathfrak{T}$ folgt weiter für Moduln das distributive Gesetz $(\ldots \mathfrak{M}_i \ldots)\,\mathfrak{A} = (\ldots \mathfrak{M}_i \mathfrak{A} \ldots)$, da es sich nach eben diesem Gesetz in $\mathfrak{T}$ rechts und links um den aus allen Elementen $\mu_i \alpha$ abgeleiteten Modul handelt.

Da $\mathfrak{R}$ selbst Modul ist, läßt sich die Bedingung, daß $\mathfrak{R}$ Multiplikatorenbereich ist, ausdrücken durch $\mathfrak{R}\mathfrak{M} \equiv 0\,(\mathfrak{M})$. Da $\mathfrak{R}$ nach Voraussetzung das Einheitselement enthält, gilt auch $\mathfrak{M} \equiv 0\,(\mathfrak{R}\mathfrak{M})$ und damit $\mathfrak{M} = \mathfrak{R}\mathfrak{M}$.

Ein Modul $\mathfrak{M}$ heißt *endlich*, wenn es mindestens ein aus *endlich* vielen Elementen bestehendes System Σ gibt, aus dem $\mathfrak{M}$ abgeleitet ist; die Elemente $\mu_1, \ldots, \mu_r$ von Σ heißen eine Modulbasis von $\mathfrak{M} = (\mu_1, \ldots, \mu_r)$.

---

[7]) Die Theorie der ganzen Größen bleibt bestehen, wenn Nullteiler zugelassen werden, und wenn dafür in $\mathfrak{R}$ der Teilerkettensatz vorausgesetzt wird, was nach § 2 auch den Beweis des Hilfssatzes ermöglicht. Da diese Fassung der ganzen Größen aber später nicht benutzt wird, soll nur in Fußnoten darauf hingewiesen werden. Alle in Rede stehenden Definitionen bleiben bei Existenz von Nullteilern erhalten; die meisten benötigen — wie bekannt und leicht ersichtlich — noch geringere Voraussetzungen. Nicht erhalten bleibt die Dedekindsche Fassung: „Eine Zahl ist ganz, wenn sie eine Hülle besitzt." Denn beim Auftreten von Nullteilern braucht der Quotient zweier endlicher Moduln nicht endlich zu bleiben; deshalb ist hier auch die Ordnung direkt und nicht als Modulquotient definiert.

Summe und Produkt von zwei — und damit von endlich vielen — endlichen Moduln sind wieder endlich, da sie aus der Vereinigungsmenge bzw. den Produkten der Basiselemente abgeleitet sind. Letzteres folgt aus der Darstellung $r_1\mu_1 + \ldots + r_k\mu_k$ aller Elemente μ aus $\mathfrak{M}$ durch die Basis[8]) und aus dem kommutativen Gesetz der Multiplikation in $\mathfrak{T}$, was beides an dieser Stelle zum erstenmal benutzt wird.

2. Ein in $\mathfrak{T}$ gelegener Erweiterungsring von $\mathfrak{R}$ — der also alle Elemente von $\mathfrak{R}$ umfaßt — heißt eine $\mathfrak{R}$-*Ordnung*, kurz *Ordnung*. Der Durchschnitt beliebig vieler Ordnungen aus $\mathfrak{T}$ ist wieder eine Ordnung, ebenso ist $\mathfrak{T}$ Ordnung; es existiert also eindeutig die aus einem beliebigen System Σ von Elementen aus $\mathfrak{T}$ abgeleitete Ordnung. Summe und Produkt von Ordnungen lassen sich entsprechend wie für Moduln definieren; insbesondere wird $\mathfrak{O}^2 = \mathfrak{O}$ für jede Ordnung.

Jede Ordnung ist zugleich $\mathfrak{R}$-Modul; eine Ordnung heißt endlich, wenn sie endlicher Modul ist. Da Summe und Produkt durch Bildung von Modulsumme bzw. Produkt entstehen, werden nach 1. Summe und Produkt endlicher Ordnungen wieder endliche Ordnungen; weiter gilt das *transitive Gesetz*: Ist $\mathfrak{A}$ endliche $\mathfrak{R}$-Ordnung, $\mathfrak{B}$ endliche $\mathfrak{A}$-Ordnung, so ist $\mathfrak{B}$ auch endliche $\mathfrak{R}$-Ordnung. Denn $\mathfrak{B}$ wird zugleich $\mathfrak{R}$-Ordnung, also $\mathfrak{R}$-Modul. Bildet aber $\alpha_1, \ldots, \alpha_r$ eine Modulbasis von $\mathfrak{A}$ in bezug auf $\mathfrak{R}$, und $\beta_1, \ldots, \beta_s$ eine solche von $\mathfrak{B}$ in bezug auf $\mathfrak{A}$, so bilden ersichtlich die Produkte $\alpha_i\beta_k$ eine Modulbasis von $\mathfrak{B}$ in bezug auf $\mathfrak{R}$.

3. Ein Element α aus $\mathfrak{T}$ heißt *ganz in bezug auf* $\mathfrak{R}$, kurz *ganz*, wenn die *aus* α *abgeleitetete Ordnung* $\mathfrak{R}_\alpha$ *endlich* ist — anders ausgedrückt, wenn die Teilerkette der Moduln $\mathfrak{A}_\mu = (\alpha^0, \alpha, \ldots, \alpha^{\mu-1})$ im Endlichen abbricht, $\mathfrak{A}_n = \mathfrak{A}_{n+1} = \ldots = \mathfrak{A}_{n+\nu} = \ldots$. Die Definition läßt auch die in 4. zu benutzende *zweite Fassung* zu: Ein Element α aus $\mathfrak{T}$ heißt *ganz*, wenn es mindestens einen vom Nullmodul verschiedenen Hauptmodul $\mathfrak{C}$ — d. h. $\mathfrak{C}$ ist aus *einem* Element $\gamma \neq 0$ abgeleitet — gibt, so daß das Produkt der Ordnung $\mathfrak{R}_\alpha$ mit $\mathfrak{C}$ ein endlicher Modul ist; anders ausgedrückt, daß die Kette der Moduln $\mathfrak{C}\mathfrak{A}_\mu$ im Endlichen abbricht[9]).

Schließlich ist die Definition auch identisch mit der *üblichen Fassung*: Ein Element α aus $\mathfrak{T}$ heißt ganz, wenn es mindestens einer Gleichung genügt: $\alpha^n + r_1\alpha^{n-1} + \ldots + r_n = 0$, wo die r Elemente aus $\mathfrak{R}$ sind.

Die verschiedenen Definitionen sind tatsächlich identisch. Denn da

[8]) Enthält $\mathfrak{R}$ kein Einheitselement, so wird die Basisdarstellung von der Form $r_1\mu_1 + \ldots + r_k\mu_k + n_1\mu_1 + \ldots + n_k\mu_k$, wo die ganzen Zahlen n nicht Ringelemente, sondern Symbole für die wiederholte Addition bzw. Subtraktion bedeuten.

[9]) Sind in $\mathfrak{R}$ Nullteiler zugelassen, so muß die Existenz eines regulären Hauptmoduls gefordert werden; d. h. γ muß als Nicht-Nullteiler, als reguläres Element vorausgesetzt werden, was für Ringe ohne Nullteiler auf $\gamma \neq 0$ zurückkommt.

$\mathfrak{R}_\alpha$ übereinstimmt mit dem aus allen Potenzen von α abgeleiteten Modul, läßt sich für endliches $\mathfrak{R}_\alpha$ immer eine Modulbasis aus diesen Potenzen wählen. Ist eine solche etwa gegeben durch $e = \alpha^0, \alpha, \ldots, \alpha^{n-1}$, so bedeutet das, daß die Kette der $\mathfrak{A}_\mu$ mit $\mathfrak{A}_n$ abbricht, und umgekehrt ergibt sich aus $\mathfrak{A}_n = \mathfrak{A}_{n+\nu} \ldots$ diese Basis. Das Abbrechen der Kette der $\mathfrak{A}_\mu$ ist aber auch identisch mit dem Bestehen der Gleichung $\alpha^n + r_1 \alpha^{n+1} + \ldots + r_n = 0$. Mit $\mathfrak{R}_\alpha$ ist auch $\mathfrak{C}\mathfrak{R}_\alpha$ endlich, also bricht die Kette der $\mathfrak{C}\mathfrak{A}_\mu$ ab; anderseits folgt aus der Endlichkeit von $\mathfrak{C}\mathfrak{R}_\alpha$, also dem Abbrechen der $\mathfrak{C}\mathfrak{A}_\mu$, auch das Abbrechen der $\mathfrak{A}_\mu$ und damit die Endlichkeit von $\mathfrak{R}_\alpha$. Denn da $\mathfrak{C}$ als vom Nullmodul verschiedener Hauptmodul vorausgesetzt, ergibt $\mathfrak{C}\mathfrak{A}_n = \mathfrak{C}\mathfrak{A}_{n+\nu}$ stets $\mathfrak{A}_n = \mathfrak{A}_{n+\nu}$.

Die Ringeigenschaft der ganzen Größen und das transitive Gesetz der ganzen Abhängigkeit beruhen auf dem

Hilfssatz. *Ist $\mathfrak{S}$ eine endliche Ordnung aus $\mathfrak{T}$, α ein beliebiges Element aus $\mathfrak{S}$, so ist die aus α abgeleitete Ordnung $\mathfrak{R}_\alpha$ endlich — m. a. W.: alle Elemente einer endlichen Ordnung sind ganz.*

Der Beweis ergibt sich nach den üblichen Schlüssen. Ist $\sigma_1, \ldots, \sigma_n$ eine Modulbasis von $\mathfrak{S}$, so gehört wegen der Ringeigenschaft auch $\alpha\sigma_i$ zu $\mathfrak{S}$. Also kommt $\alpha\sigma_i = r_{i1}\sigma_1 + \ldots + r_{in}\sigma_n$ und daraus $|r_{ik} - \alpha e_{ik}| = 0$, mit $e_{ik} = 0$ für $i \neq k$; $e_{ii} = e$, womit α als ganz nachgewiesen ist. Für das Verschwinden der Determinante wird benutzt, daß $\mathfrak{T}$ und damit $\mathfrak{S}$ ohne Nullteiler vorausgesetzt ist [10]).

Das System $\mathfrak{S}$ aller ganzen Größen aus $\mathfrak{T}$ bildet eine Ordnung. $\mathfrak{S}$ umfaßt $\mathfrak{R}$; denn die Elemente aus $\mathfrak{R}$ sind ganz, da $\mathfrak{R}$ einen endlichen $\mathfrak{R}$-Modul mit dem Einheitselement als Basis bildet. $\mathfrak{S}$ hat aber auch Ringeigenschaft; denn die aus zwei beliebigen ganzen Größen α, β abgeleitete Ordnung $\mathfrak{R}_{\alpha,\beta}$ wird gleich dem Produkt $\mathfrak{R}_\alpha \cdot \mathfrak{R}_\beta$, also endlich. Somit sind nach dem Hilfssatz $\alpha \pm \beta$ und $\alpha\beta$ als Elemente einer endlichen Ordnung ganz.

Transitives Gesetz der ganzen Abhängigkeit: Ist $\mathfrak{S}$ eine aus ganzen Größen bestehende Ordnung, so ist jedes *in bezug auf $\mathfrak{S}$ ganze Element aus $\mathfrak{T}$* auch *ganz in bezug auf* $\mathfrak{R}$. Nach Definition genügt α einer Gleichung: $\alpha^m + \sigma_1\alpha^{m-1} + \ldots + \sigma_m = 0$, ist also auch ganz in bezug auf die aus $\sigma_1, \ldots, \sigma_m$ abgeleitete Ordnung $\overline{\mathfrak{S}} = \mathfrak{R}_{\sigma_1, \ldots, \sigma_m}$, die als

[10]) Ist in $\mathfrak{R}$ der Teilerkettensatz vorausgesetzt, sind aber Nullteiler zugelassen, so wird der Hilfssatz eine unmittelbare Folge des Modulsatzes in § 2, demzufolge sich der Kettensatz auf die Moduln aus $\mathfrak{S}$ überträgt. Auch dieser Beweis stammt für den Zahlkörper von Dedekind (4. Aufl., § 173, III) und stellt die erste Anwendung von Kettensätzen in der Literatur dar. In den unter 4. zu gebenden Folgerungen benutzt Dedekind statt dessen noch die speziellere Tatsache, daß die Anzahl der Restklassen nach einem Ideal im algebraischen Zahlkörper endlich ist.

Produkt $\mathfrak{R}_{\sigma_1} \cdot \mathfrak{R}_{\sigma_2} \cdot \ldots \cdot \mathfrak{R}_{\sigma_m}$ endlich wird. Nach dem unter 2. gegebenen transitiven Gesetz wird somit die aus α abgeleitete endliche $\overline{\mathfrak{S}}$-Ordnung $\overline{\mathfrak{S}}_\alpha$ auch eine endliche $\mathfrak{R}$-Ordnung, und α wird nach dem Hilfssatz ganz als Element einer endlichen Ordnung.

4. Der Ring $\mathfrak{R}$ heißt *ganz-abgeschlossen in* $\mathfrak{T}$, wenn jedes in bezug auf $\mathfrak{R}$ ganze Element aus $\mathfrak{T}$ zu $\mathfrak{R}$ gehört. Nach der zweiten Fassung der Definition der ganzen Größen in 3. gehört also ein Element α aus $\mathfrak{T}$ dann und nur dann zu $\mathfrak{R}$, wenn es mindestens einen vom Nullmodul verschiedenen Hauptmodul $\mathfrak{C}$ gibt, so daß $\mathfrak{C} \cdot \mathfrak{R}_\alpha$ einen endlichen Modul bildet [11]).

Aus dem Begriff des ganz-abgeschlossenen Ringes hat Dedekind (3. Aufl., § 172) zwei wichtige Folgerungen gezogen, die es ermöglichen, diesen Begriff für die Idealtheorie zu verwerten:

Dedekindsche Folgerung I. *$\mathfrak{R}$ sei ganz-abgeschlossen in $\mathfrak{T}$, und außerdem sei als weitere Voraussetzung in $\mathfrak{R}$ der Teilerkettensatz für Ideale (Axiom* I*) erfüllt. Ist β ein nichtganzes Element aus $\mathfrak{T}$, $c \neq 0$ ein Element aus $\mathfrak{R}$, so gibt es einen Exponenten $\sigma \geqq 0$ derart, daß in der Reihe der Elemente $c, c\beta, \ldots, c\beta^\tau, \ldots$ die Elemente $c, \ldots, c\beta^\sigma$ ganz, alle übrigen nichtganz sind.*

Wären alle Elemente $c\beta^\tau$ ganz, so gehörten sie wegen der ganzen Abgeschlossenheit von $\mathfrak{R}$ zu $\mathfrak{R}$. Damit aber ginge die Kette der Moduln $\mathfrak{C}\mathfrak{B}_1, \mathfrak{C}\mathfrak{B}_2, \ldots, \mathfrak{C}\mathfrak{B}_r, \ldots$ — wo $\mathfrak{C}$ den aus c, $\mathfrak{B}_r$ den aus $\beta^0, \ldots, \beta^{r-1}$ abgeleiteten Modul bezeichnet — über in eine Kette von Idealen $\mathfrak{c}_1, \ldots, \mathfrak{c}_r, \ldots$, mit $\mathfrak{c}_r = (c, c\beta, \ldots, c\beta^{r-1})$, die nach Voraussetzung im Endlichen abbricht. Damit aber wäre gegen die Voraussetzung $\mathfrak{R}_\beta$ endlich und β ganz; es gibt somit nichtganze unter den Elementen $c\beta^\tau$. Weiter sind mit irgendeinem nichtganzen Element auch alle folgenden nichtganz; denn ist $c\beta^\tau$ ganz, also in $\mathfrak{R}$, so genügt $c\beta^\varrho$ für $\varrho < \tau$ der Gleichung $(c\beta^\varrho)^\tau - c^{\tau-\varrho}(c\beta^\tau)^\varrho = 0$ und ist also auch ganz. Ist somit $c\beta^{\sigma+1}$ das erste nichtganze Element, so wird — da c ganz — $\sigma \geqq 0$ und ist der gesuchte Exponent.

Spezialisiert man den Erweiterungsring $\mathfrak{T}$ zu dem Quotientenkörper von $\mathfrak{R}$ — d. h. zu dem durch Adjunktion aller Elementenpaare entstehenden Körper [12]) —, so folgt daraus die

[11]) Sind in $\mathfrak{R}$ Nullteiler zugelassen, so muß $\mathfrak{C}$ wieder als regulärer Hauptmodul vorausgesetzt werden; ebenso muß das Element c in Folgerung I als regulär vorausgesetzt werden.

[12]) In bekannter Steinitzscher Fassung, J. f. M. **137**. Sind in $\mathfrak{R}$ Nullteiler zugelassen, so muß an Stelle des Quotientenkörpers der Quotientenring treten, durch Adjunktion aller Quotientenpaare, bei denen der Nenner ein reguläres Element aus $\mathfrak{R}$ ist. Hier ist die *Dedekindsche Folgerung II nicht mehr erfüllt*; denn n wird im allgemeinen kein reguläres Element sein.

Dedekindsche Folgerung II. *$\mathfrak{R}$ sei ganz abgeschlossen in seinem Quotientenkörper $\mathfrak{K}$, und in $\mathfrak{R}$ sei der Teilerkettensatz für Ideale erfüllt. Ist β ein nichtganzes Element aus $\mathfrak{K}$, so läßt β eine Darstellung als Quotient von Elementen aus $\mathfrak{R}$ zu: $\beta = m/n$ derart, daß auch m^2/n nichtganz ist.*

Setzt man $\beta = b/c$ mit $c \neq 0$, so werden in der Reihe $c, c\beta = b, c\beta^2 \ldots$ die beiden ersten Elemente sicher ganz, also $\sigma \geqq 1$, wo σ den Exponenten aus Folgerung I bedeutet. Setzt man $m = c\beta^\sigma$, $n = c\beta^{\sigma-1}$ — wegen $\sigma \geqq 1$ sind das ganze Größen der Reihe —, so werden $m/n = \beta$ und $m^2/n = c\beta^{\sigma+1}$ nichtganz.

Das *transitive Gesetz der ganzen Abgeschlossenheit* besteht in der Form: Ist $\mathfrak{R}$ ein beliebiger Ring aus $\mathfrak{T}$, bezeichnet $\mathfrak{S}$ das System aller in bezug auf $\mathfrak{R}$ ganzen Größen aus $\mathfrak{T}$, so besteht $\mathfrak{S}$ auch aus allen in bezug auf $\mathfrak{S}$ ganzen Größen aus $\mathfrak{T}$. — Denn jede in bezug auf $\mathfrak{S}$ ganze Größe ist auch ganz in bezug auf $\mathfrak{R}$, nach dem transitiven Gesetz in 3., gehört also zu $\mathfrak{S}$.

§ 2.

Kettensätze in endlichen Modulbereichen.

Der Modulsatz, demzufolge sich die Kettensätze übertragen, tritt in der hier zu gebenden Anwendung nur für Moduln eines Erweiterungsringes auf. Da der Beweis aber im Fall eines allgemeinen Modulbereichs derselbe bleibt, soll ein solcher zugrunde gelegt werden.

Ein System M von Elementen $\alpha, \beta \ldots$ heißt *Modulbereich in bezug auf einen Ring* $\mathfrak{R}$, wenn in M zwei Operationen gegeben sind, die eindeutig zu Elementen aus M führen: eine additive Verknüpfung der Elemente und eine Multiplikation der Elemente mit den Elementen aus $\mathfrak{R}$; wenn M gegenüber der Addition eine Abelsche Gruppe bildet, während für die Multiplikation das assoziative Gesetz erfüllt ist, und wenn das distributive Gesetz in beiden Fassungen gilt[13]).

Für einen Modulbereich bleiben offenbar alle unter § 1, 1. gegebenen Moduldefinitionen erhalten, die sich nicht auf die Multiplikation beziehen. Insbesondere heißt M ein *endlicher Modulbereich*, wenn es endlich viele Elemente $\xi_1, \ldots, \xi_k$ aus M gibt derart, daß M gleich dem aus $\xi_1, \ldots, \xi_k$ abgeleiteten Modul wird, also gleich dem System aller Linearformen $r_1\xi_1 + \ldots + r_k\xi_k$, wenn in $\mathfrak{R}$ ein Einheitselement existiert, während sonst noch Zusatzglieder $n_\lambda \xi_\lambda$ hinzukommen (vgl. Anm. [8])).

Modulsatz. *Ist M ein endlicher Modulbereich in bezug auf einen kommutativen Ring $\mathfrak{R}$ mit Einheitselement, und gilt in $\mathfrak{R}$ der Teiler-*

[13]) Vgl. Idealtheorie, § 9.

bzw. Vielfachenkettensatz der Ideale, so gilt in M *Teiler- bzw. Vielfachenkettensatz der Moduln.*

Der Beweis beruht darauf, daß jedem Modul aus M eindeutig ein System von endlich vielen Idealen aus $\mathfrak{R}$ zugeordnet wird derart, daß einem echten Teiler bzw. Vielfachen des Moduls jeweils mindestens ein echtes Teiler- bzw. Vielfachenideal entspricht.

Ein Element aus M heißt *von der Länge* i, wenn es sich auf mindestens eine Art als Linearform in $\xi_1, \ldots, \xi_i$ darstellen läßt, während es keine Darstellung als Linearform in $\xi_1, \ldots, \xi_{i-1}$ zuläßt. Einem beliebigen Modul $\mathfrak{A}$ aus M seien jetzt k Ideale $\mathfrak{a}_1, \ldots, \mathfrak{a}_k$ aus $\mathfrak{R}$ zugeordnet: unter $\mathfrak{A}_i$ sei der Modul aller Elemente aus $\mathfrak{A}$ verstanden von der Länge $\leqq i$, und $\mathfrak{a}_i$ bezeichne das System aller Koeffizienten von ξ_i in $\mathfrak{A}_i$. Dann folgt vorerst: Ist $\mathfrak{B}$ ein *echter Teiler* von $\mathfrak{A}$, sind $\mathfrak{b}_1 \ldots, \mathfrak{b}_k$ die $\mathfrak{B}$ zugeordneten Ideale, so ist unter den $\mathfrak{b}$ mindestens ein *echter Teiler* des entsprechenden $\mathfrak{a}$. Aus $\mathfrak{A} \equiv 0\,(\mathfrak{B})$ folgt nämlich $\mathfrak{A}_\lambda \equiv 0\,(\mathfrak{B}_\lambda)$ und damit $\mathfrak{a}_\lambda \equiv 0\,(\mathfrak{b}_\lambda)$ für $\lambda = 1, 2, \ldots, k$. Nach Voraussetzung muß es in $\mathfrak{B}$ nicht in $\mathfrak{A}$ enthaltene Elemente geben, also auch solche kleinster Länge i. Dann aber wird $\mathfrak{b}_i$ ein echter Teiler von $\mathfrak{a}_i$; denn es wird $b_i \equiv 0\,(\mathfrak{b}_i)$, $\not\equiv 0\,(\mathfrak{a}_i)$, wenn $\beta = b_1 \xi_1 + \ldots + b_i \xi_i$ ein solches Element kleinster Länge aus $\mathfrak{B}$ ist. Aus $b_i \equiv 0\,(\mathfrak{a}_i)$ folgt nämlich die Existenz eines Elementes $\alpha = a_1 \xi_1 + \ldots + b_i \xi_i \equiv 0\,(\mathfrak{A})$, und damit die Existenz eines Elementes $\beta - \alpha \equiv 0\,(\mathfrak{B})$, $\not\equiv 0\,(\mathfrak{A})$ von kleinerer Länge als β.

Sei jetzt eine Teiler- bzw. Vielfachenkette $\mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_r, \ldots$ vorgelegt; sei in $\mathfrak{R}$ der Teiler- bzw. Vielfachenkettensatz erfüllt. Bezeichnen $\mathfrak{a}_{r1}, \ldots, \mathfrak{a}_{rk}$ die $\mathfrak{A}_r$ zugeordneten Ideale, so bilden die Reihen $\mathfrak{a}_{1\lambda}, \mathfrak{a}_{2\lambda}, \ldots, \mathfrak{a}_{r\lambda}, \ldots$ Teiler- bzw. Vielfachenketten für $\lambda = 1, \ldots, k$; es gibt also nach Voraussetzung einen Index μ derart, daß das Ideal $\mathfrak{a}_{\mu\lambda}$ gleich allen folgenden wird für jedes λ. Dann aber wird der Modul $\mathfrak{A}_\mu$ nach dem oben Bewiesenen gleich allen folgenden, womit die *Kettensätze übertragen* sind.

Unmittelbar ergibt sich jetzt die

Folgerung des Modulsatzes. *Gilt in* $\mathfrak{R}$ *der Vielfachenkettensatz modulo jedem vom Nullideal verschiedenen Ideal, so gilt in* M *der Vielfachenkettensatz modulo jedem Modul* $\mathfrak{C}$, *dessen zugeordnete Ideale* $\mathfrak{c}_1, \ldots, \mathfrak{c}_k$ *sämtlich vom Nullideal verschieden sind.*

Denn unter diesen Annahmen brechen die Vielfachenketten $\mathfrak{a}_{1\lambda}, \ldots, \mathfrak{a}_{r\lambda}, \ldots$ im Endlichen ab.

Zusatzbemerkung. Ist $\mathfrak{R}$ ein Ring ohne Einheitselement, so überträgt sich noch der Teilerkettensatz und der Vielfachenkettensatz modulo den vom Nullideal verschiedenen Idealen. Man betrachte nämlich an Stelle von $\mathfrak{A}$ das System $\overline{\mathfrak{A}}$ aller Elemente der Form $a_1 \xi_1 + \ldots + a_k \xi_k + n_1 \xi_{k+1}$

$+ \ldots + n_k \xi_{2k}$, das wieder in $\mathfrak{A}$ übergeht, wenn man $\xi_{k+\lambda}$ durch ξ_λ ersetzt. Diesem $\overline{\mathfrak{A}}$ lassen sich entsprechend wie oben $2k$ Ideale $\mathfrak{a}_1, \ldots, \mathfrak{a}_k, \mathfrak{n}_1, \ldots, \mathfrak{n}_k$ zuordnen, wobei die $\mathfrak{a}_\lambda$ Ideale aus $\mathfrak{R}$, die $\mathfrak{n}_\lambda$ Ideale aus ganzen Zahlen bedeuten. Da für die $\mathfrak{n}_\lambda$ Teilerkettensatz und Vielfachenkettensatz modulo jedem vom Nullideal verschiedenen Ideal erfüllt ist, bleibt für $\overline{\mathfrak{A}}$ und damit für $\mathfrak{A}$ der Beweis für den Teilerkettensatz erhalten, während man beim Vielfachenkettensatz fordern muß, daß die $\mathfrak{C}$ bzw. $\overline{\mathfrak{C}}$ zugeordneten $2k$ Ideale alle vom Nullideal verschieden sind.

§ 3.

Übergang zu endlichen Erweiterungskörpern.

Zur Einordnung der Zahl- und Funktionenkörper ist zu zeigen, wie die in der Einleitung formulierten Axiome I bis V sich beim Übergang zu endlichen Erweiterungskörpern übertragen.

1. *In* $\mathfrak{R}$ *seien alle Axiome* I *bis* V *mit Ausnahme des Axioms* II *— Vielfachenkettensatz — erfüllt. Es bedeute* $\mathfrak{K}$ *den Quotientenkörper von* $\mathfrak{R}$, *und* $\mathfrak{L}$ *einen endlichen Erweiterungskörper erster Art von* $\mathfrak{K}$[14]). *Dann sind in dem System* $\mathfrak{S}$ *aller in bezug auf* $\mathfrak{R}$ *ganzen Größen aus* $\mathfrak{L}$ *dieselben Axiome erfüllt, in jeder Ordnung aus* $\mathfrak{S}$ *noch alle diese Axiome mit Ausnahme der ganzen Abgeschlossenheit.*

Nach § 1, 3. bildet $\mathfrak{S}$ einen Ring, für den die Axiome III und IV — Existenz des Einheitselementes und Ring ohne Nullteiler — erfüllt sind. Nach § 1, 4. Schluß ist $\mathfrak{S}$ ganz abgeschlossen in $\mathfrak{L}$; zugleich wird $\mathfrak{L}$ Quotientenkörper von $\mathfrak{S}$, da jedes Element aus $\mathfrak{L}$ durch Multiplikation mit einem geeigneten Element aus $\mathfrak{R}$ in ein Element aus $\mathfrak{S}$ übergeht; Axiom V ist also erfüllt.

Der Nachweis von I ergibt sich nach bekannten Schlüssen: Als Erweiterung erster Art entsteht $\mathfrak{L}$ durch Adjunktion eines einzigen Elementes α zu $\mathfrak{K}$, das nach dem obigen als ganz in bezug auf $\mathfrak{R}$ angenommen werden darf. Neben α sind auch die im Galoisschen Körper von $\mathfrak{L}$ in bezug auf $\mathfrak{K}$ enthaltenen konjugierten Größen $\alpha', \alpha'', \ldots$ ganz; und somit auch ihr Differenzenprodukt und das Quadrat D dieses Differenzenproduktes. Da $\alpha, \alpha', \ldots$ alle verschieden sind, wird D eine von Null verschiedene Größe aus $\mathfrak{K}$, also wegen der ganzen Abgeschlossenheit von $\mathfrak{R}$ in $\mathfrak{K}$ eine Größe aus $\mathfrak{R}$. Nach den üblichen Schlüssen ist $\mathfrak{S}$ infolge der ganzen Abgeschlossenheit von $\mathfrak{R}$ enthalten in dem durch die Elemente $\xi_i = \alpha^i/D$ erzeugten in bezug auf $\mathfrak{R}$ endlichen Modulbereich M; man hat dazu nur in

[14]) Ein algebraischer Erweiterungskörper heißt nach Steinitz „erster Art“, wenn jedes Element Nullstelle einer Primfunktion ist, die in einem geeigneten Erweiterungskörper in lauter verschiedene Linearfaktoren zerfällt.

der Darstellung eines Elementes aus $\mathfrak{S}$ durch die ξ_i zu den konjugierten Elementen überzugehen und das lineare Gleichungssystem für die Koeffizienten der Darstellung aufzulösen. Nach dem Modulsatz in § 2 gilt für alle $\mathfrak{R}$-Moduln aus M, also insonderheit für alle Ideale aus $\mathfrak{S}$, der Teilerkettensatz. Ebenso gilt der Teilerkettensatz für die Ideale einer beliebigen Ordnung aus $\mathfrak{S}$, da es sich auch hier um $\mathfrak{R}$-Moduln aus M handelt; für jede Ordnung ist aber auch Axiom III und IV erfüllt.

2. *Sind in* $\mathfrak{R}$ *alle Axiome* I *bis* V *erfüllt, so gilt das gleiche für* $\mathfrak{S}$. *In jeder Ordnung aus* $\mathfrak{S}$ *sind noch alle Axiome mit Ausnahme der ganzen Abgeschlossenheit erfüllt.*

Unter Berücksichtigung von 1. ist nur noch das Erfülltsein von Axiom II nachzuweisen. Nach der Folgerung aus dem Modulsatz in § 2 genügt der folgende Nachweis: Wird ein vom Nullideal verschiedenes Ideal aus $\mathfrak{S}$ als $\mathfrak{R}$-Modul $\mathfrak{C}$ in M aufgefaßt, so sind die $\mathfrak{C}$ zugeordneten Ideale $\mathfrak{c}_i$ aus $\mathfrak{R}$ alle vom Nullideal verschieden. Nun ist $\mathfrak{C}$ von gleichem endlichen linearen Rang in bezug auf $\mathfrak{R}$ wie M; denn $\mathfrak{C}$ enthält neben irgendeinem Element γ auch $\gamma\,\alpha^i$. Zu jedem ξ_i gibt es also ein Element $c_i \neq 0$ aus $\mathfrak{R}$, so daß $c_i \xi_i$ zu $\mathfrak{C}$ gehört; wegen der Eindeutigkeit der Darstellung durch die ξ_i — der Index soll nur die Werte kleiner als der Grad des Körpers durchlaufen — gehört c_i zu $\mathfrak{c}_i$, das somit vom Nullideal verschieden wird. Diese Überlegung bleibt erhalten für alle Ordnungen von gleichem Rang wie M; für eine Ordnung von niedrigerem Rang geht man zum Quotientenkörper über, der als Zwischenkörper von $\mathfrak{R}$ und $\mathfrak{L}$ auch erster Art wird und dessen Grad in bezug auf $\mathfrak{R}$ mit dem linearen Rang der Ordnung übereinstimmt; für den somit die Überlegungen erhalten bleiben. Schließlich sei bemerkt, daß eine von $\mathfrak{S}$ verschiedene Ordnung aus $\mathfrak{S}$ nie ganz abgeschlossen ist; denn da jede Ordnung auch $\mathfrak{R}$ umfaßt, muß sie bei ganzer Abgeschlossenheit auch $\mathfrak{S}$ umfassen.

Zur Unterordnung von Zahl- und Funktionenkörpern genügt es somit das Erfülltsein der Axiome I bis V für die Grundbereiche — ganze Zahlen, Polynome einer Unbestimmten, Funktionalbereich der Polynome mehrerer Unbestimmter — nachzuweisen.

3. *Für den Ring* $\mathfrak{R}$ *der ganzen rationalen Zahlen bzw. der Polynome einer Unbestimmten mit Koeffizienten aus einem Körper sind die Axiome* I *bis* V *erfüllt.* Dabei folgt I und II entweder daraus, daß es nach jeder von Null verschiedenen Zahl bzw. nach einem solchen Polynom einer Unbestimmten nur endlich viele bzw. endlich viele linear-unabhängige Restklassen gibt — oder auch aus der Tatsache, daß jedes Ideal Hauptideal wird; denn daraus ergibt sich die eindeutige Zerlegbarkeit der Ideale als Potenzprodukt von Primidealen, demzufolge ein vom Nullideal ver-

schiedenes Ideal nur durch endlich viele teilbar wird. Axiom III und IV ist offenbar erfüllt, letzteres eine Folge der Gleichheitsdefinition; die ganze Abgeschlossenheit V folgt daraus, daß vermöge der bis auf Einheiten — Teiler der Eins — eindeutigen Zerlegbarkeit der Elemente aus $\mathfrak{R}$ in unzerlegbare jedes nicht in $\mathfrak{R}$ enthaltene Element des Quotientenkörpers sich als Quotient zweier teilerfremder Elemente aus $\mathfrak{R}$ darstellen läßt, so daß also keine Potenz des Zählers durch den Nenner teilbar wird. Ein solches Element kann mithin keiner Gleichung genügen, die es als ganz in bezug auf $\mathfrak{R}$ charakterisiert.

4. *Es bedeute jetzt* $\mathfrak{R}$ *den Ring aller Polynome in mehreren Unbestimmten mit Koeffizienten aus einem Körper oder mit ganzen rationalen Zahlkoeffizienten.* Dann sind die Axiome III, IV, V wie unter 3. erfüllt; denn auch hier gilt die bis auf Einheiten eindeutige Zerlegbarkeit der Elemente in unzerlegbare. Daß der Teilerkettensatz I erfüllt ist, ist eine unmittelbare Folge des Hilbertschen Satzes von der Existenz der Idealbasis; während der Vielfachenkettensatz II hier nicht gilt.

Man kann aber durch Übergang zum *Funktionalbereich*, was einer Beschränkung auf Ideale höchster Dimension entspricht, auch noch die Gültigkeit von Axiom II erreichen; die Gültigkeit von I läßt sich dann wie unter 3., ohne Heranziehung des Hilbertschen Satzes, nachweisen. Man adjungiere nämlich zu $\mathfrak{R}$ eine Unbestimmte u, betrachte also den *Ring* $\mathfrak{R}^*$ *aller Polynome in* u *mit Koeffizienten aus* $\mathfrak{R}$, wobei Gleichheit als Koeffizientengleichheit definiert ist. Bezeichnet man wie üblich ein Polynom aus $\mathfrak{R}^*$ als primitiv (in bezug auf $\mathfrak{R}$), wenn der größte gemeinsame Teiler seiner Koeffizienten — Teiler im Sinn von Polynom aus $\mathfrak{R}$, nicht Idealteiler — eine Einheit aus $\mathfrak{R}$ wird, so wird jedes Polynom aus $\mathfrak{R}^*$ Produkt eines Elementes aus $\mathfrak{R}$ mit einem primitiven Polynom aus $\mathfrak{R}^*$, und das Produkt primitiver Polynome aus $\mathfrak{R}^*$ wird wieder primitiv.

Die Gesamtheit der Elemente des Quotientenkörpers von $\mathfrak{R}^*$, *deren Nenner primitive Polynome aus* $\mathfrak{R}^*$ *sind, bildet somit einen Ring, den Funktionalbereich* $\mathfrak{F}$ *von* $\mathfrak{R}$. In diesem Funktionalbereich $\mathfrak{F}$ sind alle und nur die Elemente Einheiten, deren Zähler und Nenner primitive Polynome aus $\mathfrak{R}^*$ sind; jedes Element aus $\mathfrak{F}$ läßt sich somit eindeutig als Produkt eines Elementes aus $\mathfrak{R}$ und einer Einheit aus $\mathfrak{F}$ darstellen. Damit überträgt sich der Zerlegungssatz der Elemente aus $\mathfrak{R}$ auf die Elemente aus $\mathfrak{F}$; für $\mathfrak{F}$ ist somit neben den Axiomen III und IV auch V wie unter 3. erfüllt.

In $\mathfrak{F}$ wird ferner jedes Ideal *Hauptideal.* Ein Ideal enthält nämlich neben irgendeinem Element aus $\mathfrak{F}$ auch das durch Multiplikation mit einer Einheit daraus hervorgehende aus $\mathfrak{R}$; und neben irgend zwei Elementen aus $\mathfrak{R}$ auch ihren größten gemeinsamen Teiler. Denn neben $f(x) = t(x)\bar{f}(x)$ und

$g(x) = t(x)\,\bar{g}(x)$ gehört auch $t(x)(\bar{f}(x) + u\,\bar{g}(x))$ zum Ideal, also auch $t(x)$, wenn $\bar{f}$ und $\bar{g}$ teilerfremd sind und ihre lineare Kombination somit eine Einheit wird. Geht man also von einem beliebigen Element $f(x)$ des Ideals aus, und gibt es im Ideal ein durch dieses nicht teilbares $g(x)$, so gehört auch der größte gemeinsame Teiler $t(x)$ zum Ideal und wird ein echter Teiler von $f(x)$, so daß die endlich oftmalige Wiederholung auf ein Basiselement des Ideals führt, das Ideal also als Hauptideal erkannt ist. Damit gilt aber in $\mathfrak{F}$ die eindeutige Zerlegbarkeit der Ideale als Potenzprodukte von Primidealen, die der Zerlegung der Elemente aus $\mathfrak{R}$ entspricht; und hieraus folgt wie unter 3. das Erfülltsein der Axiome I und II. Bei den in Betracht kommenden Erweiterungskörpern des Quotientenkörpers von $\mathfrak{F}$ handelt es sich dabei nur um solche, die durch Adjunktion eines Elementes aus $\mathfrak{S}$ erzeugt werden können[15]). Damit ist unter Berücksichtigung von 1. und 2. für *Zahl- und Funktionenkörper die Gültigkeit der Axiome* I *bis* V *erkannt.*

§ 4.

Isomorphiesätze. Direkte Summen.

Im folgenden wird nur Ring- bzw. Moduleigenschaft aber kein weiteres Axiom vorausgesetzt.

1. Sind M und $\overline{\mathsf{M}}$ Modulbereiche in bezug auf $\mathfrak{R}$ (§ 2), so heißt M zu $\overline{\mathsf{M}}$ *homomorph* (genauer: *modul-homomorph*), $\mathsf{M} \sim \overline{\mathsf{M}}$, wenn jedem Element aus M ein und nur ein Element aus $\overline{\mathsf{M}}$ entspricht, derart, daß dadurch $\overline{\mathsf{M}}$ erschöpft wird[16]); und wenn bei dieser Zuordnung die Differenz und die Multiplikation mit demselben Element aus $\mathfrak{R}$ sich entsprechen; wenn also aus $\beta \sim \bar{\beta}$ und $\gamma \sim \bar{\gamma}$ stets folgt: $(\beta - \gamma) \sim (\bar{\beta} - \bar{\gamma})$ und $r\,\beta \sim r\,\bar{\beta}$.

Einem $\mathfrak{R}$-Modul $\mathfrak{B}$ aus M entspricht also homomorph ein $\mathfrak{R}$-Modul $\overline{\mathfrak{B}}$ aus $\overline{\mathsf{M}}$; und die *Gesamtheit* $\mathfrak{C}^*$ der Elemente aus M, denen Elemente eines $\mathfrak{R}$-Moduls $\overline{\mathfrak{C}}$ aus $\overline{\mathsf{M}}$ entsprechen, bildet einen durch $\overline{\mathfrak{C}}$ eindeutig bestimmten $\mathfrak{R}$-Modul in M, den $\overline{\mathfrak{C}}$ zugeordneten Modul $\mathfrak{C}^*$ mit $\mathfrak{C}^* \sim \overline{\mathfrak{C}}$. Ist insbesondere $\mathfrak{A}$ der dem Nullelement aus $\overline{\mathsf{M}}$ zugeordnete Modul, so wird $\mathfrak{C}^*$ ein Teiler von $\mathfrak{A}$ und zerfällt in Klassen von modulo $\mathfrak{A}$ kongruenten Elementen aus M, derart daß diese Klassen den Elementen aus $\mathfrak{C}$ ein-eindeutig entsprechen. Geht man von $\mathfrak{B}$ in M über zu $\overline{\mathfrak{B}}$ in $\overline{\mathsf{M}}$, und von da zurück zu $\mathfrak{B}^*$, so wird $\mathfrak{B}^* = (\mathfrak{B}, \mathfrak{A})$; also gleich dem größten

[15]) Das System der in bezug auf $\mathfrak{F}$ ganzen Größen dieser Erweiterungskörper gewinnt man auch, indem man von $\mathfrak{S}$ entsprechend zu einem Funktionalbereich übergeht, wie von $\mathfrak{R}$ zu $\mathfrak{F}$. Vgl. etwa J. König, Algebraische Größen, Leipzig 1903, S. 468/69.

[16]) Alles im Sinne der in $\overline{\mathsf{M}}$ herrschenden Gleichheitsdefinition, vgl. Anmerkung [6]).

gemeinsamen Teiler von $\mathfrak{B}$ und $\mathfrak{A}$; es wird also $\mathfrak{B}^* = \mathfrak{B}$, wenn $\mathfrak{B}$ Teiler von $\mathfrak{A}$.

Ist das Entsprechen der Elemente aus M und $\overline{\mathsf{M}}$ umkehrbar eindeutig, so heißen die Bereiche *isomorph* (genauer *modul-isomorph*) $\mathsf{M} \sim \overline{\mathsf{M}}$.

Ist $\mathfrak{A}$ ein beliebiger $\mathfrak{R}$-Modul aus M, so entsteht ein zu M homomorpher Modulbereich $\overline{\mathsf{M}}$ — der *Restklassenmodul* $\mathsf{M}|\mathfrak{A}$ —, indem man die Kongruenz nach $\mathfrak{A}$ als neue Gleichheitsbeziehung auffaßt. Jedem Element aus M sind dabei alle und nur die ihm gleichen aus $\overline{\mathsf{M}}$ zugeordnet. Geht man in $\overline{\mathsf{M}}$ von der Gleichheitsdefinition zur Identität über, so heißt das, daß man alle in $\overline{\mathsf{M}}$ gleichen Elemente in einer Klasse — *Restklasse* — zusammenfaßt und diese Restklassen als neue Elemente von $\overline{\mathsf{M}}$ auffaßt[17]).

Durch den *Übergang zum Restklassenmodul wird jeder Homomorphismus erzeugt*; denn ist $\mathsf{M} \sim \overline{\mathsf{M}}$, und ist $\mathfrak{A}$ der dem Nullelement aus $\overline{\mathsf{M}}$ zugeordnete Modul, so wird, wie oben gezeigt, $\overline{\mathsf{M}}$ *isomorph dem Restklassenmodul* $\mathsf{M}|\mathfrak{A}$.

2. Erster Isomorphiesatz. *Bedeutet* $\overline{\mathsf{M}}$ *den Restklassenmodul* $\mathsf{M}|\mathfrak{A}$, *und ist* $\mathfrak{C}$ *Teiler von* $\mathfrak{A}$, *so gilt der Isomorphismus*: $\overline{\mathsf{M}}|\overline{\mathfrak{C}} \simeq \mathsf{M}|\mathfrak{C}$. Denn die Kongruenz nach $\mathfrak{A}$ ist zugleich eine Kongruenz nach $\mathfrak{C}$; nach $\mathfrak{A}$ gleiche Elemente bleiben also gleich nach $\mathfrak{C}$, und man kann mithin den Restklassenmodul $\mathsf{M}|\mathfrak{C}$ — also die Gleichheit nach $\mathfrak{C}$ — bilden, indem man zuerst die Elemente nach $\mathfrak{A}$ gleichsetzt, also zu $\overline{\mathsf{M}}$ übergeht, und unter diesen die nach $\mathfrak{C}$ gleichen zusammenfaßt, was in $\overline{\mathsf{M}}$ dem Gleichsetzen nach $\overline{\mathfrak{C}}$, also der Bildung von $\overline{\mathsf{M}}|\overline{\mathfrak{C}}$ entspricht.

Zweiter Isomorphiesatz. *Sind* $\mathfrak{B}$ *und* $\mathfrak{A}$ *Moduln aus* M, *so gilt der Isomorphismus*: $(\mathfrak{B}, \mathfrak{A})|\mathfrak{A} \simeq \mathfrak{B}|[\mathfrak{B}, \mathfrak{A}]$. Denn nach 1. wird $\mathfrak{B}$ homomorph zu $\overline{\mathfrak{B}}$, wenn $(\mathfrak{B}, \mathfrak{A})|\mathfrak{A}$ gleich $\overline{\mathfrak{B}}$ gesetzt wird; und da hierbei allen Elementen aus $[\mathfrak{B}, \mathfrak{A}]$ und nur diesen das Nullelement in $\overline{\mathfrak{B}}$ entspricht, so kommt wieder nach 1. der obige Isomorphismus.

3. Sind $\mathfrak{R}$ und $\overline{\mathfrak{R}}$ (kommutative) Ringe, so heißt $\mathfrak{R}$ *homomorph* zu $\overline{\mathfrak{R}}$ (genauer *ring-homomorph*), $\mathfrak{R} \sim \overline{\mathfrak{R}}$, wenn jedem Element aus $\mathfrak{R}$ ein und nur ein Element aus $\overline{\mathfrak{R}}$ entspricht derart, daß dadurch $\overline{\mathfrak{R}}$ erschöpft wird; und wenn bei dieser Zuordnung Differenz und Produkt sich entsprechen. Ist das Entsprechen der Elemente umkehrbar eindeutig, so heißen die Ringe *isomorph* (genauer *ring-isomorph*), $\mathfrak{R} \simeq \overline{\mathfrak{R}}$.

Alle Überlegungen unter 1. und 2. bleiben erhalten, wenn man die Moduln durch Ideale in $\mathfrak{R}$ ersetzt[18]), und wenn der Begriff des Modul-Homomorphismus und Modul-Isomorphismus durch Ring-Homomorphismus

[17]) Vgl. dazu Anmerkung [6]).

[18]) Bei nichtkommutativen Ringen müssen zweiseitige Ideale zugrunde gelegt werden.

und Ring-Isomorphismus ersetzt wird. Insbesondere entsteht, wenn $\mathfrak{c}$ ein Teiler von $\mathfrak{a}$ ist, der *Restklassenring* $\mathfrak{c}|\mathfrak{a}$, indem die Kongruenz nach $\mathfrak{a}$ als neue Gleichheitsbeziehung eingeführt wird, wobei zu beachten ist, daß jetzt noch die Produkte von Restklassen definiert sind.

Es wird $\mathfrak{c}$ homomorph zu $\mathfrak{c}|\mathfrak{a}$; jeder Homomorphismus ist auf diese Art erzeugt, und es gelten wie unter 2. die Isomorphiesätze:

Erster Isomorphiesatz. Bedeutet $\overline{\mathfrak{R}}$ den Restklassenring $\mathfrak{R}|\mathfrak{a}$, und ist $\mathfrak{c}$ Teiler von $\mathfrak{a}$, so wird $\overline{\mathfrak{R}}|\overline{\mathfrak{c}} \simeq \mathfrak{R}|\mathfrak{c}$ im Sinne des Ring-Isomorphismus.

Zweiter Isomorphiesatz. Sind $\mathfrak{b}$ und $\mathfrak{a}$ Ideale aus $\mathfrak{R}$, so gilt der Ring-Isomorphismus: $(\mathfrak{b}, \mathfrak{a})|\mathfrak{a} \simeq \mathfrak{b}|[\mathfrak{b}, \mathfrak{a}]$ [19]).

4. Im folgenden sollen die Rechenregeln über *teilerfremde Ideale* zusammengestellt werden [20]), aus denen sich in 5. die Sätze über direkte Summen ergeben werden. In dem kommutativen Ring $\mathfrak{R}$ werde die *Existenz des Einheitselementes* e der Multiplikation vorausgesetzt. Es wird also $\mathfrak{a} = \mathfrak{o}\,\mathfrak{a}$ für jedes Ideal aus $\mathfrak{R}$, unter $\mathfrak{o}$ das Einheitsideal verstanden. Zwei Ideale $\mathfrak{a}, \mathfrak{b}$ heißen teilerfremd, wenn ihr größter gemeinsamer Teiler $(\mathfrak{a}, \mathfrak{b})$ gleich $\mathfrak{o}$ wird.

4α. *Ist* $(\mathfrak{a}, \mathfrak{b}) = \mathfrak{o}$, *so wird* $(\mathfrak{a}, \mathfrak{b}\,\mathfrak{c}) = (\mathfrak{a}, \mathfrak{c})$. Denn $(\mathfrak{a}, \mathfrak{c}) = (\mathfrak{a}, \mathfrak{b}) \cdot (\mathfrak{a}, \mathfrak{c}) = (\mathfrak{a}^2, \mathfrak{a}\,\mathfrak{b}, \mathfrak{a}\,\mathfrak{c}, \mathfrak{b}\,\mathfrak{c})$ wird durch $(\mathfrak{a}, \mathfrak{b}\,\mathfrak{c})$ teilbar und umgekehrt. Daraus folgt:

4β. *Aus* $\mathfrak{c}\,\mathfrak{b} \equiv 0\,(\mathfrak{a})$ *und* $(\mathfrak{a}, \mathfrak{b}) = \mathfrak{o}$ *folgt* $\mathfrak{c} \equiv 0\,(\mathfrak{a})$. Denn $\mathfrak{c}\,\mathfrak{b} \equiv 0\,(\mathfrak{a})$ ist gleichbedeutend mit $(\mathfrak{a}, \mathfrak{b}\,\mathfrak{c}) = \mathfrak{a}$; also wird wegen $(\mathfrak{a}, \mathfrak{b}) = \mathfrak{o}$ auch $(\mathfrak{a}, \mathfrak{c}) = \mathfrak{a}$ oder $\mathfrak{c} \equiv 0\,(\mathfrak{a})$. Es folgt weiter:

4γ. *Ist jedes der Ideale* $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ *teilerfremd zu jedem der Ideale* $\mathfrak{b}_1, \ldots, \mathfrak{b}_s$, *so wird das Produkt der* $\mathfrak{a}_i$ *teilerfremd zu dem Produkt der* $\mathfrak{b}_i$. Denn aus $(\mathfrak{a}, \mathfrak{b}) = \mathfrak{o}$ und $(\mathfrak{a}, \mathfrak{c}) = \mathfrak{o}$ kommt $(\mathfrak{a}, \mathfrak{b}\,\mathfrak{c}) = \mathfrak{o}$, woraus durch endlich oftmalige Wiederholung die Behauptung folgt.

Aus 4α und 4γ ergibt sich:

4δ. *Sind die Ideale* $\mathfrak{b}_1, \ldots, \mathfrak{b}_r$ *paarweise teilerfremd, also* $(\mathfrak{b}_i, \mathfrak{b}_k) = \mathfrak{o}$ *für* $i \neq k$, *so wird ihr kleinstes gemeinsames Vielfaches gleich ihrem Produkt.* Sei $(\mathfrak{a}, \mathfrak{b}) = \mathfrak{o}$, $\mathfrak{v} = [\mathfrak{a}, \mathfrak{b}]$; dann wird $\mathfrak{v} = \mathfrak{o}\,\mathfrak{v} = (\mathfrak{a}\,\mathfrak{v}, \mathfrak{b}\,\mathfrak{v})$

---

[19]) Diese aus der Gruppentheorie bekannten Isomorphiesätze finden sich für Moduln in etwas speziellerer Fassung zuerst bei Dedekind (vgl. 3. Aufl., S. 484). Die obige Fassung für Ideale findet sich bei Masazo Sono: On Congruences. I., II., III., IV. Memoirs of the College of Science, Kyoto Imperial University, 2 (1917), 3 (1918, 1919). Vgl. 2, S. 215. Explizit ausgesprochen ist jeweils nur der zweite Isomorphiesatz.

[20]) Und zwar in der auf Dedekind zurückgehenden Form (4. Aufl., § 178, III bis VIII). Das in neueren Darstellungen durchweg auftretende Rechnen mit dem Einheitselement ist viel umständlicher.

$\equiv 0\,(\mathfrak{a}, \mathfrak{b})$; wegen $\mathfrak{a}\,\mathfrak{b} \equiv 0\,(\mathfrak{v})$ kommt also $\mathfrak{v} = \mathfrak{a}\,\mathfrak{b}$, woraus durch endlich oftmalige Wiederholung unter Beachtung von 4γ die Behauptung folgt.

4ε. *Sind die Ideale* $\mathfrak{b}_1, \ldots, \mathfrak{b}_r$ *paarweise teilerfremd, wird* $\mathfrak{a}_i = [\mathfrak{b}_1, \ldots, \mathfrak{b}_{i-1}, \mathfrak{b}_{i+1}, \ldots, \mathfrak{b}_r] = \mathfrak{b}_1 \ldots \mathfrak{b}_{i-1}\,\mathfrak{b}_{i+1} \ldots \mathfrak{b}_r$ *gesetzt, so wird* $(\mathfrak{a}_1, \ldots, \mathfrak{a}_{i-1}, \mathfrak{a}_{i+1}, \ldots, \mathfrak{a}_r) = \mathfrak{b}_i$ *und also* $(\mathfrak{a}_1, \ldots, \mathfrak{a}_r) = \mathfrak{o}$. Denn nach dem distributiven Gesetz wird $(\mathfrak{a}_1, \mathfrak{a}_2) = \mathfrak{b}_3 \ldots \mathfrak{b}_r\,(\mathfrak{b}_2, \mathfrak{b}_1) = \mathfrak{b}_3 \ldots \mathfrak{b}_r$; und also $(\mathfrak{a}_1, \mathfrak{a}_2, \mathfrak{a}_3) = \mathfrak{b}_4 \ldots \mathfrak{b}_r\,(\mathfrak{b}_3, \mathfrak{b}_1\,\mathfrak{b}_2) = \mathfrak{b}_4 \ldots \mathfrak{b}_r$, woraus durch endlich oftmalige Wiederholung bei passender Numerierung die Behauptung folgt.

Es wird $\mathfrak{a}_i$ als Komplement von $\mathfrak{b}_i$ in der Darstellung $\mathfrak{m} = [\mathfrak{b}_1, \ldots, \mathfrak{b}_r]$ bezeichnet.

5. In dem kommutativen Ring $\mathfrak{R}$ sei wieder die Existenz des Einheitselementes der Multiplikation vorausgesetzt. Der Ring $\mathfrak{R}$ heißt *direkte Summe* der Ideale $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$, — in Zeichen: $\mathfrak{R} = \mathfrak{a}_1 + \mathfrak{a}_2 + \ldots + \mathfrak{a}_r$ — wenn jedes Element c aus $\mathfrak{R}$ sich auf eine und nur eine Art darstellen läßt in der Form: $c = a_1 + a_2 + \ldots + a_r$, wo jeweils a_i Element aus $\mathfrak{a}_i$.

Ist das Nullideal kleinstes gemeinsames Vielfaches der paarweise teilerfremden Ideale $\mathfrak{b}_1, \ldots, \mathfrak{b}_r$, *und ist* $\mathfrak{a}_i$ *das Komplement von* $\mathfrak{b}_i$, *so wird* $\mathfrak{R}$ *direkte Summe der Ideale* $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$. Denn wegen $\mathfrak{o} = (\mathfrak{a}_1, \ldots, \mathfrak{a}_r)$ läßt jedes Element aus $\mathfrak{R}$ mindestens eine additive Darstellung durch die $\mathfrak{a}_i$ zu; wegen $[\mathfrak{a}_i, \mathfrak{b}_i] = (0)$ ist diese Darstellung eindeutig; denn aus $0 = a_1 + a_2 + \ldots + a_r = a_i + b_i$ kommt $a_i = 0$. Nach dem zweiten Isomorphiesatz werden die $\mathfrak{a}_i$ *isomorph dem Restklassenring* $\mathfrak{R}\,|\,\mathfrak{b}_i$. Es gelten die „Orthogonalitätsrelationen“ $\mathfrak{a}_i\,\mathfrak{a}_k = (0)$ für $i \neq k$ und $\mathfrak{a}_i^2 = \mathfrak{a}_i$, letzteres wegen $\mathfrak{a}_i = \mathfrak{o}\,\mathfrak{a}_i$.

Existiert umgekehrt eine Darstellung von $\mathfrak{R}$ *als direkte Summe* — $\mathfrak{R} = \mathfrak{a}_1 + \mathfrak{a}_2 + \ldots + \mathfrak{a}_r$ — *und setzt man* $\mathfrak{b}_i = (\mathfrak{a}_1, \ldots, \mathfrak{a}_{i-1}, \mathfrak{a}_{i+1}, \ldots, \mathfrak{a}_r) = \mathfrak{a}_1 + \ldots + \mathfrak{a}_{i-1} + \mathfrak{a}_{i+1} + \ldots + \mathfrak{a}_r$, *so werden die* $\mathfrak{b}_i$ *paarweise teilerfremd und ihr kleinstes gemeinsames Vielfaches gleich dem Nullideal.* Denn aus $\mathfrak{o} = (\mathfrak{a}_i, \mathfrak{b}_i)$ folgt $\mathfrak{o} = (\mathfrak{b}_k, \mathfrak{b}_i)$ für $k \neq i$, da $\mathfrak{b}_k$ Teiler von $\mathfrak{a}_i$. Sei weiter c teilbar durch alle $\mathfrak{b}_i$, so kommt $c = a_2^{(1)} + \ldots + a_r^{(1)} = a_1^{(2)} + a_3^{(2)} + \ldots + a_r^{(2)} = \ldots = a_1^{(r)} + \ldots + a_{r-1}^{(r)}$, wo jeweils $a_i^{(\lambda)} \equiv 0\,(\mathfrak{a}_i)$. Aus der Eindeutigkeit der Darstellung folgt also, da jeweils eine Komponente zu Null wird: $0 = a_1^{(\lambda)}, \ldots, 0 = a_r^{(\lambda)}$ für jedes λ und damit $c = 0$.[21])

---

[21]) Die unter 5. gegebenen Sätze sind Spezialfälle eines allgemeinen Satzes über den Zusammenhang zwischen direkter Summe und direktem Durchschnitt. Vgl. H. Prüfer, Theorie der Abelschen Gruppen I, Math. Zeitschr. 20 (1924), S. 165—187, § 6. Die dort gegebenen Überlegungen bleiben auch bei so allgemeiner Fassung des Gruppenbegriffs erhalten, daß Moduln und Ideale sich als Spezialfall unterordnen.

§ 5.

Primideale und Primärideale.

Es sei wieder $\mathfrak{R}$ ein kommutativer Ring, für den kein weiteres Axiom — auch nicht Existenz des Einheitselementes — vorausgesetzt werde. Es sollen die Grundtatsachen über Primideale und Primärideale zusammengestellt werden [22]).

1. Ein Ideal $\mathfrak{p}$ aus $\mathfrak{R}$ heißt *schwaches Primideal*, wenn der Restklassenring $\mathfrak{R}|\mathfrak{p}$ ein Ring ohne Nullteiler ist; wenn also aus $a \not\equiv 0 (\mathfrak{p})$ und $b \not\equiv 0 (\mathfrak{p})$ stets folgt $a\,b \not\equiv 0 (\mathfrak{p})$. Ein Ideal $\mathfrak{p}^*$ aus $\mathfrak{R}$ heißt *starkes Primideal*, wenn der Restklassenring $\mathfrak{R}|\mathfrak{p}^*$ ein Ring ohne Nullteiler*ideale* ist; wenn also aus $\mathfrak{a} \not\equiv 0 (\mathfrak{p}^*)$ und $\mathfrak{b} \not\equiv 0 (\mathfrak{p}^*)$ stets folgt $\mathfrak{a}\,\mathfrak{b} \not\equiv 0 (\mathfrak{p}^*)$. *Jedes starke Primideal ist zugleich schwaches Primideal*, wie die Spezialisierung von $\mathfrak{a}, \mathfrak{b}$ zu Hauptidealen zeigt. Umgekehrt ist auch *jedes schwache Primideal zugleich starkes Primideal*; man kann also von *Primidealen* schlechthin sprechen. Denn sei $\mathfrak{p}$ schwaches Primideal; sei $\mathfrak{a} \not\equiv 0 (\mathfrak{p})$ und $\mathfrak{b} \not\equiv 0 (\mathfrak{p})$; seien weiter a und b Elemente aus $\mathfrak{a}$ und $\mathfrak{b}$, so daß $a \not\equiv 0 (\mathfrak{p})$ und $b \not\equiv 0 (\mathfrak{p})$. Dann kommt $a\,b \not\equiv 0 (\mathfrak{p})$ und damit $\mathfrak{a}\,\mathfrak{b} \not\equiv 0 (\mathfrak{p})$; also ist $\mathfrak{p}$ auch starkes Primideal.

2. Ein Ideal $\mathfrak{q}$ aus $\mathfrak{R}$ heißt *schwaches Primärideal*, wenn im Restklassenring $\mathfrak{R}|\mathfrak{q}$ eine Potenz jedes Nullteilers verschwindet; wenn also aus $a \not\equiv 0 (\mathfrak{q})$ und $b^\varkappa \not\equiv 0 (\mathfrak{q})$ für jedes $\varkappa$ stets folgt $a\,b \not\equiv 0 (\mathfrak{q})$. Das System $\mathfrak{p}$ aller Elemente aus $\mathfrak{R}$, die Nullteiler aus $\mathfrak{R}|\mathfrak{q}$ werden, bildet ein Ideal, und zwar ein Primideal, das Teiler von $\mathfrak{q}$ wird, das *zugehörige Primideal*. Denn neben a wird auch $r\,a$ Nullteiler, neben a und b auch $a - b$; letzteres da mit $a^\varkappa$ und b^λ stets $(a-b)^{\varkappa+\lambda}$ durch $\mathfrak{q}$ teilbar wird. Ist ferner a kein Nullteiler, so wird nach Definition auch keine Potenz von a Nullteiler; aus $a \not\equiv 0 (\mathfrak{p})$ und $b \not\equiv 0 (\mathfrak{p})$ folgt also $a^\varkappa b^\varkappa = (a\,b)^\varkappa \not\equiv 0 (\mathfrak{q})$ und damit $a\,b \not\equiv 0 (\mathfrak{p})$.

Ein Ideal $\mathfrak{q}^*$ aus $\mathfrak{R}$ heißt *starkes Primärideal*, wenn im Restklassenring $\mathfrak{R}|\mathfrak{q}^*$ eine Potenz jedes Nullteiler*ideals* verschwindet; wenn also aus $\mathfrak{a} \not\equiv 0 (\mathfrak{q}^*)$ und $\mathfrak{b}^\varkappa \not\equiv 0 (\mathfrak{q}^*)$ für jedes $\varkappa$ stets folgt $\mathfrak{a}\,\mathfrak{b} \not\equiv 0 (\mathfrak{q}^*)$. Wie bei schwachen Primäridealen zeigt man: Der größte gemeinsame Teiler aller Idale aus $\mathfrak{R}$, die Nullteilerideale aus $\mathfrak{R}|\mathfrak{q}^*$ werden, bildet ein Primideal, das Teiler von $\mathfrak{q}^*$ wird, das *zugehörige Primideal*. Umgekehrt sagt man von allen Primäridealen, die dasselbe zugehörige Primideal $\mathfrak{p}$ besitzen, sie „gehören zu $\mathfrak{p}$“.

---

[22]) In Idealtheorie, § 4, ist Axiom I des Teilerkettensatzes vorausgesetzt, und es tritt deshalb nicht scharf hervor, welche Eigenschaften der Prim- und Primärideale von diesem Axiom unabhängig sind.

Jedes starke Primärideal ist zugleich schwaches Primärideal, wie die Spezialisierung von $\mathfrak{a}, \mathfrak{b}$ zu Hauptidealen zeigt. Im allgemeinen *gilt aber nicht die Umkehrung*[23]. *Wird jedoch in* $\mathfrak{R}$ *das Axiom* I *des Teilerkettensatzes vorausgesetzt, so wird jedes schwache Primärideal zugleich starkes Primärideal*; man kann also von *Primäridealen* schlechthin sprechen. Dann sei $\mathfrak{q}$ schwaches Primärideal; sei $\mathfrak{a} \not\equiv 0 (\mathfrak{q})$ und $\mathfrak{b}^\varkappa \not\equiv 0 (\mathfrak{q})$ für jedes $\varkappa$. Dann *gibt es Elemente* a aus $\mathfrak{a}$ und b aus $\mathfrak{b}$, so daß $a \not\equiv 0 (\mathfrak{q})$ und $b^\varkappa \not\equiv 0 (\mathfrak{q})$ für jedes $\varkappa$; mithin kommt $ab \not\equiv 0 (\mathfrak{q})$ und damit $\mathfrak{a}\mathfrak{b} \not\equiv 0 (\mathfrak{q})$. Denn wenn zu jedem b aus $\mathfrak{b}$ ein Exponent λ existiert, so daß $b^\lambda \equiv 0 (\mathfrak{q})$ wird, so wird $\mathfrak{b}^{\lambda_1 + \ldots + \lambda_r} \equiv 0 (\mathfrak{q})$ unter $\lambda_1, \ldots, \lambda_r$ die Exponenten der endlich vielen Basiselemente verstanden[24]. Diese letztere Überlegung zeigt noch: Es gibt einen (kleinsten) Exponenten ϱ derart, daß $\mathfrak{p}^\varrho \equiv 0 (\mathfrak{q})$ wird, wo $\mathfrak{p}$ das zugehörige Primideal bedeutet; ϱ heißt der *Exponent von* $\mathfrak{q}$.

3. Im folgenden sei der Teilerkettensatz wieder *nicht vorausgesetzt*. Das kleinste gemeinsame Vielfache $[\mathfrak{a}_1, \ldots, \mathfrak{a}_r]$ von endlich vielen Idealen heißt eine *kürzeste Darstellung*, wenn kein $\mathfrak{a}_i$ im kleinsten gemeinsamen Vielfachen der übrigen aufgeht, wenn also kein $\mathfrak{a}_i$ weggelassen werden kann.

Das kleinste gemeinsame Vielfache von endlich vielen, zu demselben Primideal $\mathfrak{p}$ *gehörigen schwachen bzw. starken Primäridealen ist wieder schwaches Primärideal mit* $\mathfrak{p}$ *als zugehörigem Primideal. Eine kürzeste Darstellung durch endlich viele, zu verschiedenen Primidealen gehörigen schwache bzw. starke Primärideale ist kein schwaches bzw. starkes Primärideal.* Sei $\mathfrak{f} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_r]$ und $\mathfrak{p}$ zugehöriges Primideal der schwachen Primärideale $\mathfrak{q}_i$; dann besteht $\mathfrak{p}$ auch aus der Gesamtheit der Elemente, von denen eine Potenz durch $\mathfrak{f}$ teilbar wird. Aus $a \not\equiv 0 (\mathfrak{f})$ und $b^\varkappa \not\equiv 0 (\mathfrak{f})$ für jedes $\varkappa$ folgt also $b \not\equiv 0 (\mathfrak{p})$ und $a \not\equiv 0 (\mathfrak{q}_i)$ für mindestens einen Index i; also $ab \not\equiv 0 (\mathfrak{q}_i)$ und damit $ab \not\equiv 0 (\mathfrak{f})$. Ersetzt man durchweg die Elemente durch Ideale, so läßt sich nicht mehr $\mathfrak{b} \not\equiv 0 (\mathfrak{p})$ schließen.

Sei jetzt $\mathfrak{m} = [\mathfrak{q}_1, \ldots, \mathfrak{q}_r]$ mit $\mathfrak{p}_i \neq \mathfrak{p}_k$ für $i \neq k$ eine kürzeste Darstellung durch schwache Primärideale und sei $r \geqq 2$. Dann gibt es mindestens ein zugehöriges Primideal, etwa $\mathfrak{p}_1$, das in keinem der übrigen

[23]) Das zeigt das folgende, mir von R. Hölzer mitgeteilte Beispiel. Sei $\mathfrak{R}$ der Polynombereich von abzählbar vielen Unbestimmten x_i mit Koeffizienten aus einem Körper; sei $\mathfrak{q} = (x_1^2, x_2^3, \ldots, x_\nu^{\nu+1}, \ldots, x_i x_k [i \neq k] \ldots)$. Nullteiler im Restklassenring sind alle und nur die durch $\mathfrak{p} = (x_1, x_2, \ldots, x_\nu, \ldots)$ teilbaren Polynome, und es wird jeweils eine Potenz dieser Nullteiler durch $\mathfrak{q}$ teilbar; $\mathfrak{q}$ ist also *schwaches Primärideal* mit $\mathfrak{p}$ als zugehörigem Primideal. Dagegen ist $\mathfrak{q}$ *kein starkes Primärideal*; denn setzt man $\mathfrak{a} = (x_1, x_3, x_5, \ldots, x_{2\nu+1}, \ldots)$ und $\mathfrak{b} = (x_2, x_4, \ldots, x_{2\nu}, \ldots)$, so wird $\mathfrak{a}\mathfrak{b} \equiv 0 (\mathfrak{q})$, aber keine Potenz von $\mathfrak{a}$ oder $\mathfrak{b}$ durch $\mathfrak{q}$ teilbar.

[24]) Um von Axiom I auf die endliche Idealbasis schließen zu können, muß eine feste Wohlordnung in $\mathfrak{R}$ zugrunde gelegt werden (vgl. § 6).

aufgeht; denn jede echte Vielfachenkette der $\mathfrak{p}$ muß nach höchstens r Schritten abbrechen. Somit gibt es Elemente a_i aus $\mathfrak{p}_i$, derart, daß $a_i^{\varrho_i} \equiv 0 (\mathfrak{q}_i)$ und $a_2 \not\equiv 0 (\mathfrak{p}_1)$; $\ldots a_r \not\equiv 0 (\mathfrak{p}_1)$ wird. Ist weiter $q_1 \not\equiv 0 (\mathfrak{m})$ ein Element aus $\mathfrak{q}_1$, so wird $q_1 a_2^{\varrho_2} \ldots a_r^{\varrho_r} \equiv 0 (\mathfrak{m})$, aber keine Potenz von $(a_2^{\varrho_2} \ldots a_r^{\varrho_r})$ durch $\mathfrak{m}$ teilbar, da sonst Teilbarkeit durch $\mathfrak{p}_1$ folgen würde; $\mathfrak{m}$ ist also kein schwaches Primärideal. Ersetzt man durchweg die Elemente durch Ideale, also q_1 durch $\mathfrak{q}_1$ und a_i durch $\mathfrak{a}_i [\not\equiv (\mathfrak{p}_1)$, aber $\mathfrak{a}_i^{\varrho} \equiv 0 (\mathfrak{q}_i)]$, so ergibt sich der Beweis für starke Primärideale[25]).

4. *Modul- und Idealquotient.* Sei $\mathfrak{T}$ ein Erweiterungsring von $\mathfrak{R}$, seien $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \ldots$, $\mathfrak{R}$-Moduln in $\mathfrak{T}$. Der *Quotient* $\mathfrak{C} = \mathfrak{A} : \mathfrak{B}$ ist definiert als ein Modul, der den Bedingungen genügt: $\mathfrak{C}\mathfrak{B} \equiv 0 (\mathfrak{A})$ und aus $\mathfrak{D}\mathfrak{B} \equiv 0 (\mathfrak{A})$ folgt $\mathfrak{D} \equiv 0 (\mathfrak{C})$ — es ist also $\mathfrak{C}$ der „kleinste" Modul, für den $\mathfrak{C}\mathfrak{B} \equiv 0 (\mathfrak{A})$ wird. Dadurch ist der Quotient eindeutig bestimmt als größter gemeinsamer Teiler aller Moduln $\mathfrak{D}$, für die $\mathfrak{D}\mathfrak{B} \equiv 0 (\mathfrak{A})$ gilt; solche $\mathfrak{D}$ existieren, da der Nullmodul sicher ein solcher Modul ist.

Aus der Definition folgt: Ist $\mathfrak{B}$ ein Vielfaches von $\overline{\mathfrak{B}}$, so wird $\mathfrak{A} : \overline{\mathfrak{B}}$ ein Vielfaches von $\mathfrak{A} : \mathfrak{B}$. Ist $\mathfrak{A}$ ein Vielfaches von $\overline{\mathfrak{A}}$, so wird $\mathfrak{A} : \mathfrak{B}$ ein Vielfaches von $\overline{\mathfrak{A}} : \mathfrak{B}$. Es wird $\mathfrak{A} : \mathfrak{B}\,\mathfrak{C} = (\mathfrak{A} : \mathfrak{B}) : \mathfrak{C} = (\mathfrak{A} : \mathfrak{C}) : \mathfrak{B}$.

Fällt der Erweiterungsring $\mathfrak{T}$ mit $\mathfrak{R}$ zusammen, so geht der Modulquotient in den *Idealquotient* $\mathfrak{a} : \mathfrak{b}$ über, für den somit auch die obigen Rechenregeln gelten. Wegen $\mathfrak{a}\,\mathfrak{b} \equiv 0 (\mathfrak{a})$ folgt hier noch $\mathfrak{a} \equiv 0 (\mathfrak{a} : \mathfrak{b})$.

5. *Ist* $\mathfrak{a} : \mathfrak{b} = \mathfrak{a}$, *so heißt* $\mathfrak{b}$ *prim zu* $\mathfrak{a}$. Ein Ideal $\mathfrak{b}$ ist also dann und nur dann prim zu $\mathfrak{a}$, wenn aus $\mathfrak{b}\,\mathfrak{b} \equiv 0 (\mathfrak{a})$ stets folgt $\mathfrak{b} \equiv 0 (\mathfrak{a})$. Aus den Rechenregeln unter 4. folgt: *Sind* $\mathfrak{b}$ *und* $\mathfrak{c}$ *prim zu* $\mathfrak{a}$, *so ist auch ihr Produkt nnd ihr kleinstes gemeinsames Vielfaches prim zu* $\mathfrak{a}$. Ist sowohl $\mathfrak{b}$ prim zu $\mathfrak{a}$, wie $\mathfrak{a}$ prim zu $\mathfrak{b}$, so heißen $\mathfrak{a}$ und $\mathfrak{b}$ gegenseitig prim. Aus § 4, 4β folgt: Sind $\mathfrak{a}$ und $\mathfrak{b}$ teilerfremd, so sind sie auch gegenseitig prim.

§ 6.

Idealtheorie bei Voraussetzung des Teilerkettensatzes.

Zugrunde gelegt sei ein (kommutativer) Ring $\mathfrak{R}$, für den *Axiom* I *des Teilerkettensatzes erfüllt* ist; weiter sei im folgenden stets eine feste *Wohlordnung aller Elemente* aus $\mathfrak{R}$ zugrunde gelegt. Damit ist aber zugleich auch eine *Wohlordnung aller Ideale* aus $\mathfrak{R}$ gegeben. Denn die beiden Voraussetzungen ergeben sofort, daß jedes Ideal aus $\mathfrak{R}$ eine aus endlich vielen Elementen bestehende Idealbasis besitzt. Geht man also von der Wohlordnung der Elemente aus $\mathfrak{R}$ über zu einer quasi-lexikographischen An-

[25]) Diese Modifikation meines ursprünglichen Beweises, durch die der Teilerkettensatz entbehrlich wird, verdanke ich B. L. van der Waerden.

ordnung aller endlichen Untermengen von $\mathfrak{R}$[26]), und ordnet jedem Ideal als ausgezeichnete Basis die unter den verschiedenen möglichen Basen erste in der Wohlordnung der endlichen Untermengen zu, so sind mit den endlichen Untermengen auch die Ideale wohlgeordnet.

Satz I. *Jedes Ideal aus* $\mathfrak{R}$ *läßt — bei Voraussetzung des Teilerkettensatzes — eine Darstellung als kleinstes gemeinsames Vielfaches von endlich vielen irreduziblen Idealen zu, d. h. von Idealen die sich nicht als kleinstes gemeinsames Vielfaches von zwei echten Teilern darstellen lassen.*

Zum Beweis ist zu zeigen: Ist Satz I für ein Ideal $\mathfrak{m}$ nicht erfüllt, so besitzt $\mathfrak{m}$ einen echten Teiler, für den Satz I ebenfalls nicht erfüllt ist; daraus läßt sich entgegen dem vorausgesetzten Teilerkettensatz eine nicht im Endlichen abbrechende Teilerkette konstruieren. In der Tat muß $\mathfrak{m}$ reduzibel sei, da sonst $\mathfrak{m} = [\mathfrak{m}]$ die gewünschte Darstellung liefern würde. Wird $\mathfrak{m} = [\mathfrak{a}, \mathfrak{b}]$, so kann Satz I nicht für $\mathfrak{a}$ und $\mathfrak{b}$ gleichzeitig erfüllt sein, da sonst eine entsprechende Darstellung für $\mathfrak{m}$ folgen würde. Es gibt also echte Teiler von $\mathfrak{m}$, für die Satz I nicht erfüllt ist; sei $\mathfrak{a}_1$ der in der Wohlordnung der Ideale erste. Indem man entsprechend zu $\mathfrak{a}_1$ einen echten Teiler $\mathfrak{a}_2$ konstruiert, und allgemein zu $\mathfrak{a}_i$ einen echten Teiler $\mathfrak{a}_{i+1}$, kommt man zu einer wohlbestimmten, nicht im Endlichen abbrechenden Teilerkette, gegen die Voraussetzung[27]).

---

[26]) Darunter ist folgendes zu verstehen: die Elemente $a_1, \ldots, a_n$ einer endlichen Untermenge $\mathfrak{A}_n$ seien so bezeichnet, daß die Anordnung der Indizes mit der in $\mathfrak{R}$ gegebenen Wohlordnung übereinstimmt. Jede Untermenge $\mathfrak{A}_n$ gehe einer solchen mit $m > n$ Elementen voran. Sind $\mathfrak{A}_n$ und $\mathfrak{B}_n$ Untermengen von gleich vielen Elementen, so heiße $\mathfrak{A}_n$ früher als $\mathfrak{B}_n$, wenn das erste Element a_i, das von dem entsprechenden b_i verschieden ist, in der Wohlordnung von $\mathfrak{R}$ dem b_i vorangeht. Damit ist jedem System endlicher Untermengen ein erstes Element $\mathfrak{A}_n$ zugeordnet.

Bei gegebener Wohlordnung von $\mathfrak{R}$ bedarf es also keines weiteren Auswahlpostulats; ist insbesondere $\mathfrak{R}$ abzählbar — wie etwa im Fall des algebraischen Zahlkörpers —, so liegt überhaupt kein Auswahlpostulat zugrunde.

Auf die Rolle des Auswahlpostulats in der Idealtheorie ist ohne nähere Ausführungen in Idealtheorie, Anmerkung [9]), hingewiesen.

[27]) Satz I gilt offenbar genau so für Modulbereiche, wenn der Teilerkettensatz für das System aller Moduln vorausgesetzt wird. Satz I trägt nämlich rein mengentheoretischen Charakter — er ist zugleich der einzige, bei dessen Beweis die Wohlordnung der Ideale benutzt wird. Es handelt sich, unabhängig von allen Verknüpfungen, um die folgenden mengentheoretischen Begriffe:

In einer Menge $\mathfrak{M}$ sei eine Untermenge Σ der Potenzmenge — also ein System von Untermengen — ausgezeichnet. Σ sei als wohlgeordnet angenommen; die Elemente von Σ seien etwa als Σ-Mengen bezeichnet. In Σ sei der *Kettensatz* vorausgesetzt: Jede Kette von Σ-Mengen, $\mathfrak{A}_1, \mathfrak{A}_2, \ldots, \mathfrak{A}_\nu \ldots$, derart, daß $\mathfrak{A}_\nu$ eine echte Obermenge von $\mathfrak{A}_{\nu-1}$ ist, bricht im Endlichen ab. Eine Σ-Menge $\mathfrak{A}$ heiße *reduzibel*

Wegen des vorausgesetzten Teilerkettensatzes kann nach § 5, 2. von Primäridealen schlechthin gesprochen werden. Den Zusammenhang zwischen primär und irreduzibel ergibt

Satz II. *Bei Voraussetzung des Teilerkettensatzes ist jedes irreduzible Ideal primär, m. a. W. jedes nichtprimäre Ideal ist reduzibel.*

Da beim Übergang zum Restklassenring $\mathfrak{R}|\mathfrak{m}$ wegen der Homomorphie der Teilerkettensatz erhalten bleibt, da der Darstellung von $\mathfrak{m}$ als kleinstem gemeinsamen Vielfachen die Darstellung des Nullideals entspricht und da wegen des ersten Isomorphiesatzes (§ 4, 3.) den primären Teilern von $\mathfrak{m}$ wieder solche in $\mathfrak{R}|\mathfrak{m}$ entsprechen und umgekehrt, kann man sich auf die Zerlegung des Nullideals im Restklassenring beschränken. Da dieser ein Ring gleicher Allgemeinheit ist, kann man von vornherein das zu zerlegende Ideal als Nullideal von $\mathfrak{R}$ voraussetzen.

Sei also das Nullideal von $\mathfrak{R}$ nichtprimär, so daß es mindestens ein Paar von Idealen $\mathfrak{a}, \mathfrak{b}$ gibt — wobei noch $\mathfrak{b}$ als Hauptideal vorausgesetzt werden darf — derart, daß $\mathfrak{a} \neq (0)$, $\mathfrak{b}^\varkappa \neq (0)$ für jedes $\varkappa$, aber $\mathfrak{a}\mathfrak{b} = (0)$. Es sei die — nach Voraussetzung im Endlichen abbrechende — Teilerkette der Idealquotienten gebildet: $\mathfrak{a}, \mathfrak{a}:\mathfrak{b}, \ldots, \mathfrak{a}:\mathfrak{b}^\nu, \ldots$; sei etwa $\mathfrak{t} = \mathfrak{a}:\mathfrak{b}^{m-1} = \mathfrak{a}:\mathfrak{b}^m \ldots$ gleich allen folgenden Idealen der Kette; also $\mathfrak{t} = \mathfrak{t}:\mathfrak{b}$ oder $\mathfrak{b}$ prim zu $\mathfrak{t}$. Weiter ist $\mathfrak{t}$ als Teiler von $\mathfrak{a}$ vom Nullideal verschieden, ebenso $\mathfrak{b}^\varkappa$ für jeden Exponenten $\varkappa$. Zum Beweise von Satz II genügt es also, eine Darstellung $(0) = [\mathfrak{t}, \mathfrak{b}^{m+1}]$ nachzuweisen.

Nach Definition ist:

$$\mathfrak{b}^{m-1}\mathfrak{t} \equiv 0(\mathfrak{a}), \quad \text{also} \quad \mathfrak{b}^m\mathfrak{t} = (0),$$

es ist also nur zu zeigen:

$$\mathfrak{c} = [\mathfrak{t}, \mathfrak{b}^{m+1}] \equiv 0(\mathfrak{b}^m\mathfrak{t}).$$

Dies folgt aus den Voraussetzungen, daß $\mathfrak{b}$ Hauptideal und zu $\mathfrak{t}$ prim ist. Jedes Element c aus $\mathfrak{c}$ läßt wegen der Teilbarkeit durch $\mathfrak{b}^{m+1}$ eine Darstellung zu — unter n Symbol einer ganzen Zahl verstanden —:

$$c = k\,b^{m+1} + n\,b^{m+1} = r\,b^m,$$

wo r jetzt wieder ein Element aus $\mathfrak{R}$ bedeutet. Aus $c \equiv 0(\mathfrak{t})$ folgt also $r\,b^m \equiv 0(\mathfrak{t})$ und damit $r \equiv 0(\mathfrak{t})$ wegen $\mathfrak{t}:\mathfrak{b} = \mathfrak{t}$. Damit ist aber $c \equiv 0(\mathfrak{t}\,\mathfrak{b}^m)$ und Satz II bewiesen.

Satz III. *Bei Voraussetzung des Teilerkettensatzes läßt jedes Ideal eine kürzeste Darstellung als kleinstes gemeinsames Vielfaches von endlich*

wenn sie Durchschnitt von zwei Σ-Mengen ist, die beide echte Obermengen von $\mathfrak{A}$ werden, im entgegengesetzten Fall irreduzibel. Dann ergeben die obigen Überlegungen: *Jede Σ-Menge läßt sich als Durchschnitt von endlich vielen irreduziblen Σ-Mengen darstellen.*

vielen, zu verschiedenen Primidealen gehörigen, also größten Primärkomponenten zu[28]).

Um zu einer solchen Darstellung zu gelangen, hat man nur, was immer möglich, die nach Satz I existierende Darstellung durch irreduzible, also nach Satz II primäre Ideale durch eine kürzeste zu ersetzen. Faßt man die zu gleichen Primidealen gehörigen Primärideale zusammen, so ergibt sich die gesuchte Darstellung nach § 5, 3. Die Primärkompouenten können als größte bezeichnet werden, da das kleinste gemeinsame Vielfache von irgendwelchen unter ihnen nicht mehr primär ist.

§ 7.

Idealtheorie bei Voraussetzung des Doppelkettensatzes.

Die Vereinfachungen gegenüber der bis jetzt entwickelten Theorie beruhen auf den unter 1. und 2. zu gebenden Hilfssätzen.

1. *Ist in einem kommutativen Ring ohne Nullteiler der Vielfachenkettensatz erfüllt, so ist der Ring zugleich Körper.* Es ist zu zeigen, daß für $a \neq 0$ die Gleichung $a x = b$ stets eine Lösung im Ring besitzt; daß sie nicht mehr als eine Lösung besitzen kann, folgt daraus, daß der Ring ohne Nullteiler vorausgesetzt ist.

Sei $\mathfrak{a}$ das aus a abgeleitete Hauptideal; nach Voraussetzung bricht die Reihe der Potenzen im Endlichen ab; sei etwa $\mathfrak{a}^m$ gleich allen folgenden. Bezeichnet $\mathfrak{b}$ das aus b abgeleitete Hauptideal, so kommt also:

$$\mathfrak{a}^m \mathfrak{b} = \mathfrak{a}^{m+1} \mathfrak{b} \quad \text{mit} \quad \mathfrak{a}^{m+1} \mathfrak{b} = (a^{m+1} b).$$

Das ergibt insbesondere für das Element $a^m b$ eine Darstellung — unter n Symbol für eine ganze Zahl verstanden —

$$a^m b = k a^{m+1} b + n a^{m+1} b = a^{m+1} c,$$

wo c wieder Element aus $\mathfrak{R}$. Da nach Voraussetzung keine Nullteiler existieren, kommt daraus $b = a c$, womit die Körpereigenschaft bewiesen ist.

2. Aus 1. folgt unmittelbar der

Hilfssatz: *Ist in einem kommutativen Ring der Vielfachenkettensatz erfüllt, so besitzt ein Primideal keinen von* 0 *verschiedenen echten Teiler.*

Ebenso folgt der Zusatz. *Ist nur Axiom* II *erfüllt — Vielfachenkettensatz modulo jedem vom Nullideal verschiedenen Ideal —, so besitzt jedes*

[28]) Dabei sind die zugehörigen Primideale und die isolierten Komponenten eindeutig bestimmt. Vgl. Idealtheorie oder auch W. Krull, Ein neuer Beweis für die Hauptsätze der allgemeinen Idealtheorie. Math. Ann. 90 (1923), S. 55—64. In § 7 wird ein direkter Beweis der Eindeutigkeit für den dort auftretenden einfachen Spezialfall gegeben werden. Die dort als eindeutig erkannten Primärideale sind isolierte Komponenten.

vom Nullideal verschiedene Primideal keinen von $\mathfrak{o}$ *verschiedenen echten Teiler.*

Denn der Restklassenring nach einem Primideal $\mathfrak{p}$ wird nach Definition ein Ring ohne Nullteiler; und da wegen der Homomorphie auch hier der Vielfachenkettensatz erfüllt ist, nach 1. ein Körper. Wegen des eineindeutigen Entsprechens der Teiler von $\mathfrak{p}$ und der Ideale im Restklassenring besitzt also $\mathfrak{p}$ keinen von $\mathfrak{o}$ verschiedenen echten Teiler[29]).

Satz IV. *Ist in einem kommutativen Ring der Doppelkettensatz erfüllt, so sind in jeder kürzesten Darstellung eines Ideals diejenigen primären Komponenten, die nicht zum Einheitsideal* $\mathfrak{o}$ *gehören, eindeutig bestimmt.*

Zusatz. *Bei Voraussetzung von Axiom* I *und* II *gilt Satz* IV *für jedes vom Nullideal verschiedene Ideal.*

Seien $\mathfrak{m} = [\mathfrak{q}, \mathfrak{q}_1, \ldots, \mathfrak{q}_r] = [\bar{\mathfrak{q}}, \bar{\mathfrak{q}}_1, \ldots, \bar{\mathfrak{q}}_{\bar{r}}]$ kürzeste Darstellungen von $\mathfrak{m}$ durch größte Primärkomponenten, seien $\mathfrak{o}, \mathfrak{p}_1, \ldots, \mathfrak{p}_r$ bzw. $\mathfrak{o}, \bar{\mathfrak{p}}_1, \ldots, \bar{\mathfrak{p}}_r$ die zugehörigen Primideale. Dabei soll $\mathfrak{q}$ bzw. $\bar{\mathfrak{q}}$ fortgelassen werden, wenn kein zu $\mathfrak{o}$ gehöriges Primärideal auftritt. Wegen $\mathfrak{o}^{\varrho}\mathfrak{p}_1^{\varrho_1} \ldots \mathfrak{p}_r^{\varrho_r} \equiv 0\,(\mathfrak{m})$ muß jedes $\bar{\mathfrak{p}}_i$ in einem $\mathfrak{p}_i$ aufgehen, also nach dem Hilfssatz mit diesem identisch sein. Da ebenso jedes $\mathfrak{p}_k$ mit einem $\bar{\mathfrak{p}}_k$ übereinstimmen muß, stimmen also die von $\mathfrak{o}$ verschiedenen Primideale überein, $\mathfrak{p}_\lambda = \bar{\mathfrak{p}}_\lambda$. Es wird weiter $\mathfrak{q}\,\mathfrak{q}_1 \ldots \mathfrak{q}_r \equiv 0\,(\bar{\mathfrak{q}}_\lambda)$ und daraus $\mathfrak{q}_\lambda \equiv 0\,(\bar{\mathfrak{q}}_\lambda)$, da die übrigen Komponenten nicht durch $\mathfrak{p}_\lambda$ teilbar, also prim zu $\bar{\mathfrak{q}}_\lambda$ sind. Da ebenso $\bar{\mathfrak{q}}_\lambda \equiv 0\,(\mathfrak{q}_\lambda)$ folgt, ist also die Eindeutigkeit der nicht zu $\mathfrak{o}$ gehörigen Primärkomponenten gezeigt. Tritt schließlich $\mathfrak{q}$ wirklich auf, so muß wegen der kürzesten Darstellung auch $\bar{\mathfrak{q}}$ wirklich auftreten, womit noch die Eindeutigkeit der zugehörigen Primideale gezeigt ist. Weiter zeigt der Eindeutigkeitsbeweis noch, daß jede Darstellung, die keine zu $\mathfrak{o}$ gehörige Primärkomponente enthält, zugleich kürzeste ist.

3. Fügt man zu der Voraussetzung des Doppelkettensatzes noch die Existenz des Einheitselementes hinzu, so verschärft sich Satz IV zu

Satz V. *Ist in einem kommutativen Ring mit Einheitselement der Doppelkettensatz erfüllt, so läßt sich jedes Ideal eindeutig als Produkt von endlich vielen, paarweise teilerfremden Primäridealen darstellen.*

Zusatz. *Bei Voraussetzung von Axiom* I, II, III *gilt Satz* V *für jedes vom Nullideal verschiedene Ideal.*

---

[29]) Dabei braucht in $\mathfrak{R}$ und damit in $\mathfrak{o}$ — dem aus allen Elementen von $\mathfrak{R}$ bestehenden Einheitsideal — kein Einheitselement zu existieren, obwohl es nach 1. im Restklassenring eine Einheitsklasse gibt. Das einfachste Beispiel dieser Art — wo es sich um den schwächeren Fall des Zusatzes handelt — bildet das System aller geraden Zahlen.

Wegen der Existenz des Einheitselementes wird $\mathfrak{o}^2 = \mathfrak{o}$, und damit wird jedes zu $\mathfrak{o}$ gehörige Primärideal gleich $\mathfrak{o}$, kann also in einer kürzesten Darstellung eines von $\mathfrak{o}$ verschiedenen Ideals nicht auftreten; somit sind nach Satz IV die Primärkomponenten eindeutig bestimmt. Zugleich wird jede Darstellung durch Fortlassen von $\mathfrak{o}$ zu einer kürzesten. Zwei verschiedene Primideale werden ferner nach dem Hilfssatz unter 2. stets teilerfremd; also gilt nach den Rechenregeln aus § 4, 4. dasselbe für die Primärkomponenten; das kleinste gemeinsame Vielfache wird somit zum Produkt.

Aus den Voraussetzungen folgt weiter der

Hilfssatz. *In einem kommutativen Ring mit Einheitselement und Doppelkettensatz sind außer dem Einheitsideal alle und nur die Primideale prim zu einem Ideal* $\mathfrak{m}$, *die nicht in* $\mathfrak{m}$ *aufgehen. Die Begriffe prim und teilerfremd fallen zusammen.*

Zusatz. *Bei Voraussetzung der Axiome* I, II, III *muß* $\mathfrak{m}$ *vom Nullideal verschieden angenommen werden.*

Geht $\mathfrak{p}$ nicht in $\mathfrak{m}$ auf, so ist es von allen zu $\mathfrak{m}$ gehörigen Primidealen verschieden, also nach dem Hilfssatz unter 2. durch keines dieser — von $\mathfrak{o}$ verschiedenen — Primideale teilbar; somit wird $\mathfrak{p}$ prim zu jeder Primärkomponente und damit zu $\mathfrak{m}$. Zugleich wird $\mathfrak{p}$ teilerfremd zu jeder Primärkomponente und damit zu $\mathfrak{m}$.

Geht $\mathfrak{p} \neq \mathfrak{o}$ in $\mathfrak{m}$ auf, so muß es mit einem der zugehörigen Primideale übereinstimmen. Gehört es etwa zur Komponente $\mathfrak{q} = \mathfrak{q}_1$, so wird demnach $\mathfrak{q} : \mathfrak{p}$ ein echter Teiler von $\mathfrak{q}$ — wegen $\mathfrak{p}^{\varrho-1} \equiv 0\,(\mathfrak{q} : \mathfrak{p})$; $\not\equiv 0\,(\mathfrak{q})$. Zugleich wird $\mathfrak{q} : \mathfrak{p}$ als Teiler von $\mathfrak{p}^{\varrho-1}$ nur durch ein Primideal $\neq \mathfrak{o}$ teilbar und also primär. Wegen der eindeutigen Zerlegbarkeit wird daher auch das durch $\mathfrak{m} : \mathfrak{p}$ teilbare Produkt $(\mathfrak{q} : \mathfrak{p}) \cdot \mathfrak{q}_2 \dots \mathfrak{q}_r$ ein echter Teiler von $\mathfrak{m}$; es wird also $\mathfrak{p}$ nicht prim zu $\mathfrak{m}$.

Somit wird ein Ideal $\mathfrak{t} \neq \mathfrak{o}$ dann und nur dann prim zu $\mathfrak{m}$, wenn keines der zu $\mathfrak{t}$ gehörigen Primideale in $\mathfrak{m}$ aufgeht; in diesem Fall wird aber $\mathfrak{t}$ auch teilerfremd zu $\mathfrak{m}$. Da umgekehrt zwei teilerfremde Ideale stets gegenseitig prim sind (§ 5, 5.), so fallen also unter den obigen Voraussetzungen die beiden Begriffe zusammen.

§ 8.

Idealtheorie bei ganzer Abgeschlossenheit im Quotientenkörper.

Die bis hierher entwickelte Idealtheorie soll jetzt durch Hinzunahme der beiden letzten Axiome zu der üblichen verschärft werden.

1. Hilfssatz. *Ist* $\mathfrak{R}$ *ein kommutativer Ring ohne Nullteiler mit Einheitselement, und wird in* $\mathfrak{R}$ *der Teilerkettensatz vorausgesetzt (Axiom*

I, III, IV), *so folgt aus* $\mathfrak{a} = \mathfrak{a}\mathfrak{b}$ *und* $\mathfrak{a} \neq (0)$ *stets* $\mathfrak{b} = \mathfrak{o}$. *Es wird also* $\mathfrak{c}^\varrho \neq \mathfrak{c}^{\varrho+1}$ *für alle von Null- und Einheitsideal verschiedenen Ideale*[30]).

Der Beweis ergibt sich wie bei dem Hilfssatz § 1, 3., da man $\mathfrak{a}\mathfrak{b}$ als endlichen Modul in bezug auf $\mathfrak{b}$ auffassen kann. Bedeutet $\alpha_1, \ldots, \alpha_n$ eine wegen I existierende Idealbasis von $\mathfrak{a}$, so folgt aus $\mathfrak{a} = \mathfrak{a}\mathfrak{b}$ das Gleichungssystem $\alpha_i = b_{i1}\alpha_1 + \ldots + b_{in}\alpha_n$ mit $b_{ik} \equiv 0\,(\mathfrak{b})$ für $i = 1, \ldots, n$.

Da $\mathfrak{R}$ ohne Nullteiler vorausgesetzt, folgt daraus $|b_{ik} - e_{ik}| = 0$; mit $e_{ik} = 0$ für $i \neq k$; $e_{ii} = e$. Aus der Gleichung $e^n + b_1 e^{n-1} + \ldots + b_n = 0$ mit $b_i \equiv 0\,(\mathfrak{b})$ folgt aber $e \equiv 0\,(\mathfrak{b})$ und damit $\mathfrak{b} = \mathfrak{o}$.

2. Es ist jetzt nur noch zu zeigen, daß durch Hinzunahme der Voraussetzung der *ganzen Abgeschlossenheit im Quotientenkörper* (Axiom V) zu den Axiomen I bis IV folgt, daß jedes vom Nullideal verschiedene *Primärideal eine Potenz seines zugehörigen Primideals* wird. Die *Eindeutigkeit* der daraus folgenden Darstellung $\mathfrak{m} = \mathfrak{p}_1^{\varrho_1} \ldots \mathfrak{p}_r^{\varrho_r}$ für alle vom Nullideal verschiedenen Ideale ist schon durch Satz V und den Hilfssatz unter 1. bewiesen; zugleich ist gezeigt, daß diese Primideale keinen vom Einheitsideal verschiedenen echten Teiler besitzen. Der Beweis soll für den Exponenten zwei unter Heranziehung der Dedekindschen Folgerung II (§ 1, 4.) geführt werden, allgemein durch volle Induktion.

Hilfssatz. *Bei Voraussetzung der Axiome* I *bis* V *gibt es keine weiteren Primärideale vom Exponenten zwei als* $\mathfrak{q} = \mathfrak{p}^2$.

Zum Beweis ist zu zeigen, daß aus $\mathfrak{p}^2 \equiv 0\,(\mathfrak{q})$; $\mathfrak{q} \equiv 0\,(\mathfrak{p})$; aber $\mathfrak{q} \not\equiv 0\,(\mathfrak{p}^2)$ notwendig $\mathfrak{q}$ gleich $\mathfrak{p}$ folgt. Sei also

$$c \equiv 0\,(\mathfrak{q}); \quad \text{mithin} \quad c \equiv 0\,(\mathfrak{p}); \quad \text{aber} \quad c \not\equiv 0\,(\mathfrak{p}^2).$$

Dann folgt aus dem Hilfssatz § 7, 3., daß $\mathfrak{o}c : \mathfrak{p}$ echter Teiler von $\mathfrak{o}c$ wird; also gibt es ein Element b, derart, daß

$$b\mathfrak{p} \equiv 0\,(\mathfrak{o}c) \equiv 0\,(\mathfrak{q}); \quad \text{aber} \quad b \not\equiv 0\,(\mathfrak{o}c);$$

mithin $\gamma = b/c$ nicht ganz wird, d. h. zum Quotientenkörper, aber nicht zu $\mathfrak{R}$ gehört.

Es ist $b \not\equiv 0\,(\mathfrak{p})$ nachzuweisen, woraus — da $\mathfrak{q}$ primär und zu $\mathfrak{p}$ gehörig — $\mathfrak{p} \equiv 0\,(\mathfrak{q})$ folgt.

Nach der Dedekindschen Folgerung II gibt es Elemente m, n aus $\mathfrak{R}$ derart, daß $\gamma = b/c = m/n$ wird und auch m^2/n nicht ganz; daß also

$$bn = mc; \quad m \not\equiv 0\,(\mathfrak{o}n); \quad m^2 \equiv 0\,(\mathfrak{o}n)$$

---

[30]) Dagegen kann bei den gleichen Voraussetzungen *nicht* von $\mathfrak{a}\mathfrak{b} = \mathfrak{a}\mathfrak{c}$ auf $\mathfrak{b} = \mathfrak{c}$ geschlossen werden, wie das folgende Beispiel zeigt, wo $\mathfrak{R}$ als Polynombereich in x, y mit Koeffizienten aus einem Körper angenommen ist: $\mathfrak{a} = (x, y)$; $\mathfrak{b} = (x^2, xy, y^2)$; $\mathfrak{c} = (x^2, y^2)$. Tatsächlich wird $\mathfrak{a}\mathfrak{b} = \mathfrak{a}\mathfrak{c} = \mathfrak{a}^3$; aber $\mathfrak{b} \neq \mathfrak{c}$.

wird. Duch Multiplikation von $b\mathfrak{p}$ mit m folgt:

$$mb\mathfrak{p} \equiv 0(\mathfrak{o}mc); \quad \text{also } \equiv 0(\mathfrak{o}nb) \text{ und daraus } m\mathfrak{p} \equiv 0(\mathfrak{o}n),$$

letzteres, da es sich um einen Ring ohne Nullteiler handelt. Hieraus folgt

$$m \not\equiv 0(\mathfrak{p}) \quad \text{wegen} \quad m^2 \not\equiv 0(\mathfrak{o}n) \quad \text{und} \quad n \equiv 0(\mathfrak{p});$$

letzteres nach dem Hilfssatz § 7, 3; da $\mathfrak{o}n:\mathfrak{p}$ echter Teiler von $\mathfrak{o}n$ wegen $m \not\equiv 0(\mathfrak{o}n)$. Die vier Relationen

$$m \not\equiv 0(\mathfrak{p}); \quad n \equiv 0(\mathfrak{p}); \quad c \equiv 0(\mathfrak{p}); \not\equiv 0(\mathfrak{p}^2); \quad bn = mc$$

ergeben aber $b \not\equiv 0(\mathfrak{p})$. Denn da $\mathfrak{p}^2$ primär, kommt vorerst $mc \not\equiv 0(\mathfrak{p}^2)$, und damit folgt $b \not\equiv 0(\mathfrak{p})$ wegen $bn = mc$. Damit ist der Hilfssatz bewiesen.

3. Hilfssatz. *Bei Voraussetzung der Axiome* I *bis* V *gibt es keine weiteren Primärideale vom Exponenten* ϱ *als* $\mathfrak{q} = \mathfrak{p}^\varrho$.

Der Hilfssatz ergibt sich aus dem Hilfssatz unter 2. ohne Anwendung der Axiome[31]). Zum Beweise ist vorerst zu zeigen:

Ist $c \equiv 0(\mathfrak{p}); \not\equiv 0(\mathfrak{p}^2)$, *so wird* $\mathfrak{p}^\sigma = (\mathfrak{o}c^\sigma, \mathfrak{p}^{\sigma+1})$ *für jedes* σ.

Es wird $\mathfrak{p} = (\mathfrak{o}c, \mathfrak{p}^2)$ nach dem Hilfssatz unter 2. Setzt man also voraus $\mathfrak{p}^{\sigma-1} = (\mathfrak{o}c^{\sigma-1}, \mathfrak{p}^\sigma)$, so folgt durch Multiplikation mit $\mathfrak{p}$ nach dem distributiven Gesetz:

$$\mathfrak{p}^\sigma = (\mathfrak{p}c^{\sigma-1}, \mathfrak{p}^{\sigma+1}) = (\mathfrak{o}c^\sigma, \mathfrak{p}^2c^{\sigma-1}, \mathfrak{p}^{\sigma+1}) = (\mathfrak{o}c^\sigma, \mathfrak{p}^{\sigma+1}).$$

Der zu beweisende Hilfssatz kann auf die folgende zweite Fassung gebracht werden:

Ist $\mathfrak{q} \equiv 0(\mathfrak{p}^\sigma); \not\equiv 0(\mathfrak{p}^{\sigma+1})$ *und ist* $\mathfrak{p}^{\sigma+\lambda} \equiv 0(\mathfrak{q})$ *mit* $\lambda \geqq 1$, *so wird auch* $\mathfrak{p}^{\sigma+\lambda-1} \equiv 0(\mathfrak{q})$.

Denn wegen $\mathfrak{q} \equiv 0(\mathfrak{p}); \not\equiv 0(\mathfrak{p}^{\varrho+1})$ existiert für jedes Primärideal ein solcher Exponent $\sigma \geqq 1$; dabei folgt $\mathfrak{q} \not\equiv 0(\mathfrak{p}^{\varrho+1})$ aus $\mathfrak{p}^\varrho \equiv 0(\mathfrak{q})$ und $\mathfrak{p}^\varrho \neq \mathfrak{p}^{\varrho+1}$ nach dem Hilfssatz unter 1. Die endlich oftmalige Anwendung der zweiten Fassung ergibt aber $\mathfrak{p}^\sigma \equiv 0(\mathfrak{q})$ und damit $\mathfrak{q} = \mathfrak{p}^\sigma$.

Aus der Voraussetzung der zweiten Fassung folgt unter Berücksichtigung der Darstellung von $\mathfrak{p}^\sigma$ für jedes Element q aus $\mathfrak{q}$:

$$q \equiv bc^\sigma(\mathfrak{p}^{\sigma+1}) \text{ mit } b \not\equiv 0(\mathfrak{p}) \text{ oder } bc^\sigma \equiv 0(\mathfrak{q}, \mathfrak{p}^{\sigma+1}).$$

Da $(\mathfrak{q}, \mathfrak{p}^{\sigma+1})$ primär, folgt daraus $c^\sigma \equiv 0(\mathfrak{q}, \mathfrak{p}^{\sigma+1})$ oder

$$c^{\sigma+\lambda-1} \equiv 0(\mathfrak{q}, \mathfrak{p}^{\sigma+\lambda}) \quad \text{und damit} \quad \mathfrak{p}^{\sigma+\lambda-1} \equiv 0(\mathfrak{q}).$$

---

[31]) Der Beweis von Hilfssatz 3. unter Voraussetzung der Gültigkeit von Hilfssatz 2. findet sich bei Masazo Sono, On Congruences II, §§ 9 und 10. Vgl. Anm. [19]).

4. Zusammenfassend kommt

Satz VI. *Sind in einem kommutativen Ring die Axiome* I *bis* V *erfüllt, so läßt sich jedes von Null- und Einheitsideal verschiedene Ideal eindeutig darstellen als Potenzprodukt von endlich vielen, von Null- und Einheitsideal verschiedenen Primidealen; diese Primideale besitzen keinen vom Einheitsideal verschiedenen echten Teiler.*

§ 9.

Die Axiome als Folge der vorausgesetzten Zerlegung.

Um aus der Existenz der üblichen Idealzerlegung — die nach Satz VI aus den Axiomen I bis V folgt — auch umgekehrt diese Axiome erschließen zu können, ist die Zerlegung in der folgenden Fassung vorauszusetzen:

Voraussetzung. *In dem kommutativen Ring $\Re$ ist jedes nicht vom Null- oder Einheitselement abgeleitete Ideal eindeutig als Potenzprodukt von Primidealen darstellbar. Diese Primideale sind nicht vom Einheitselement abgeleitete einfache Ideale — d. h. sie besitzen keinen von $\mathfrak{o}$ verschiedenen echten Teiler; umgekehrt sind alle einfachen Ideale Primideale. Die Eindeutigkeit gilt in der scharfen Fassung, daß $\mathfrak{a}^{\varrho} \neq \mathfrak{a}^{\varrho+1}$ wird für jedes nicht vom Null- oder Einheitselement abgeleitete Ideal.*

Die Existenz des Einheitselementes ist dabei nicht vorausgesetzt; gibt es kein Einheitselement, so stellt die Bedingung „nicht vom Einheitselement abgeleitet“ keine Einschränkung dar.

1. Nachweis von Axiom III (Existenz des Einheitselementes). Sei Axiom III nicht erfüllt; es ist zu zeigen, daß $\mathfrak{o}^2$ einfaches Ideal wird, ohne Primideal zu sein, gegen die Voraussetzung. Nach der Eindeutigkeitsvoraussetzung wird $\mathfrak{o} \neq \mathfrak{o}^2$; es wird also $\mathfrak{o} \not\equiv 0 (\mathfrak{o}^2)$, aber $\mathfrak{o}^2 \equiv 0 (\mathfrak{o}^2)$, und mithin $\mathfrak{o}^2$ kein Primideal. Es wird aber $\mathfrak{o}^2$ einfach; denn $\mathfrak{o}^2$ kann durch kein von $\mathfrak{o}$ verschiedenes Primideal teilbar sein, besitzt also wegen der vorausgesetzten Produktdarstellung keine von $\mathfrak{o}$ oder $\mathfrak{o}^2$ verschiedenen Teiler.

2. Nachweis von Axiom IV (Ring ohne Nullteiler). Ist a Nullteiler, also $ab = 0$, aber $a \neq 0$ und $b \neq 0$, so kommt durch Multiplikation der Darstellungen der aus a und b abgeleiteten Hauptideale: $(0) = \mathfrak{p}_1^{\varrho_1} \dots \mathfrak{p}_k^{\varrho_k}$, wo die $\mathfrak{p}$ von Null- und Einheitsideal verschieden sind — letzteres wegen Existenz des Einheitselementes. Die Darstellung soll als kürzeste vorausgesetzt werden in dem Sinne, daß durch Weglassen irgendeines Faktors ein echter Teiler der Null entsteht — eine Bedingung, die nicht von selbst erfüllt zu sein braucht, da über das Nullideal keine

Voraussetzung über eindeutige Darstellung gemacht ist. Tritt in dieser Darstellung nur ein Primideal auf, so wird $(0) = \mathfrak{p}^\varrho = \mathfrak{p}^{\varrho+1}$, entgegen der scharfen Eindeutigkeitsforderung. Tritt aber mehr als ein Primideal auf, so kommt

$$\mathfrak{p}_1^{\varrho_1+1} = (\mathfrak{p}_1^{\varrho_1+1}, \mathfrak{p}_1^{\varrho_1} \dots \mathfrak{p}_k^{\varrho_k}) = \mathfrak{p}_1^{\varrho_1}(\mathfrak{p}_1, \mathfrak{p}_2^{\varrho_2} \dots \mathfrak{p}_k^{\varrho_k}) = \mathfrak{p}_1^{\varrho_1};$$

denn wegen der Existenz des Einheitselementes wird $\mathfrak{p}_1$ zu allen übrigen Primidealen teilerfremd; also ergibt sich auch hier ein Widerspruch gegen die scharfe Eindeutigkeitsforderung.

3. Nachweis der Axiome I und II (Kettensätze). Die Voraussetzungen ergeben für jedes vom Nullideal verschiedene Ideal: *Aus Teilbarkeit folgt Produktdarstellung*; d. h. aus $\mathfrak{m} \equiv 0\,(\mathfrak{a})$ und $\mathfrak{a} \neq \mathfrak{o}$ folgt $\mathfrak{m} = \mathfrak{a}\mathfrak{b}$ mit $\mathfrak{b} \not\equiv 0\,(\mathfrak{m})$. Sei

$$\mathfrak{m} \equiv 0\,(\mathfrak{a}); \quad \mathfrak{m} = \mathfrak{p}_1^{\varrho_1} \dots \mathfrak{p}_r^{\varrho_r} \quad \text{und} \quad \mathfrak{a} = \bar{\mathfrak{p}}_1^{\sigma_1} \dots \bar{\mathfrak{p}}_{\bar{r}}^{\sigma_{\bar{r}}};$$

dann folgt, daß jedes $\bar{\mathfrak{p}}$ mit einem $\mathfrak{p}$ identisch ist, und daß $\sigma_i \leqq \varrho_i$ wird, also die Behauptung mit $\mathfrak{b} = \mathfrak{p}_1^{\varrho_1-\sigma_1} \dots \mathfrak{p}_r^{\sigma_r-\sigma_r}$, wo natürlich einige der σ_i Null werden können. Es gibt also nur die endlich vielen, den Kombinationen $0 \leqq \sigma_i \leqq \varrho_i$ entsprechenden Teiler von $\mathfrak{m}$; somit gilt im Restklassenring nach $\mathfrak{m}$ der Doppelkettensatz. Damit ist aber Axiom I und II nachgewiesen: der Teilerkettensatz gilt auch in $\mathfrak{R}$ selbst, da jeder echte Teiler des Nullideals vom Nullideal verschieden ist.

Der Nachweis des Axioms V′ *der ganzen Abgeschlossenheit im Quotientenkörper* setzt die üblichen Folgerungen aus der Idealzerlegung voraus, die daher erst abzuleiten sind.

4. *Der Restklassenring nach jedem vom Nullideal verschiedenen Ideal ist Hauptidealring.* Das Ideal darf vom Einheitsideal verschieden angenommen werden, da hier für den nur aus dem Nullelement bestehenden Restklassenring die Bedingung sicher erfüllt ist.

Ist das Ideal vorerst primär, $\mathfrak{q} = \mathfrak{p}^\varrho$, und ist $c \equiv 0\,(\mathfrak{p})$; $\not\equiv 0\,(\mathfrak{p}^2)$, so folgt aus 3., daß $\mathfrak{o}c = \mathfrak{p}\mathfrak{a}$ wird mit $(\mathfrak{a}, \mathfrak{p}) = \mathfrak{o}$. Es kommt also $\mathfrak{p}^\sigma = (\mathfrak{o}c^\sigma, \mathfrak{p}^\varrho)$ für jedes $\sigma \leqq \varrho$; im Restklassenring nach einem Primärideal wird somit jedes Ideal Hauptideal. Sei jetzt allgemein

$$\mathfrak{m} = \mathfrak{q}_1 \cdot \mathfrak{q}_2 \dots \mathfrak{q}_r \text{ mit } \mathfrak{q}_i = \mathfrak{p}_i^{\varrho_i}; \text{ sei } \mathfrak{R} \,|\, \mathfrak{m} = \bar{\mathfrak{a}}_1 + \dots + \bar{\mathfrak{a}}_r$$

die entsprechende Darstellung des Restklassenringes als direkter Summe (§ 4, 5.). Es wird $\bar{\mathfrak{a}}_i$ isomorph zu $\mathfrak{R} \,|\, \mathfrak{q}_i$, und folglich wird jedes Ideal aus $\bar{\mathfrak{a}}_i$ Hauptideal. Ist $\bar{\mathfrak{c}}$ ein beliebiges Ideal des Restklassenringes, so wird also $\bar{\mathfrak{a}}_i\bar{\mathfrak{c}}$ Hauptideal $\bar{\mathfrak{a}}_i\bar{c}_i$; es kommt

$$\bar{\mathfrak{c}} = \bar{\mathfrak{o}}\bar{\mathfrak{c}} = \bar{\mathfrak{a}}_1\bar{\mathfrak{c}} + \dots + \bar{\mathfrak{a}}_r\bar{\mathfrak{c}} = \bar{\mathfrak{a}}_1\bar{c}_1 + \dots + \bar{\mathfrak{a}}_r\bar{c}_r = \bar{\mathfrak{a}}_1\bar{\mathfrak{c}} + \dots + \bar{\mathfrak{a}}_r\bar{\mathfrak{c}} = \bar{\mathfrak{o}}\bar{\mathfrak{c}},$$

wobei $\bar{c} = \bar{c}_1 + \ldots + \bar{c}_r$ gesetzt ist. Denn wegen $\bar{\mathfrak{a}}_i \bar{\mathfrak{a}}_k = (0)$ und wegen $\bar{c}_i \equiv 0\,(\bar{\mathfrak{a}}_i)$ stimmen die Hauptideale $\bar{\mathfrak{a}}_i \bar{c}_i$ und $\bar{\mathfrak{a}}_i \bar{c}$ aus $\bar{\mathfrak{a}}_i$ überein.

Der Satz vom Hauptidealring läßt bekanntlich noch die folgende Fassung zu:

Ist $\mathfrak{c}$ *ein beliebiges Ideal, so läßt es sich in ein Hauptideal verwandeln durch Multiplikation mit einem zu einem gegebenen Ideal* $\mathfrak{b}$ *teilerfremden Ideal.*

Denn setzt man $\mathfrak{m} = \mathfrak{b}\mathfrak{c}$, so wird $\mathfrak{c}$ modulo $\mathfrak{m}$ zum Hauptideal, d. h. es wird $\mathfrak{c} = (\mathfrak{o}c, \mathfrak{m}) = (\mathfrak{c}\mathfrak{a}, \mathfrak{c}\mathfrak{b}) = \mathfrak{c}(\mathfrak{a}, \mathfrak{b})$; somit wird $\mathfrak{o}c = \mathfrak{c}\mathfrak{a}$ und $(\mathfrak{a}, \mathfrak{b}) = \mathfrak{o}$.

5. Theorie der gebrochenen Ideale. Als *gebrochenes Ideal* bezeichnet man jeden endlichen $\mathfrak{R}$-Modul im Quotientenkörper $\mathfrak{K}$.

Satz. *Die vom Nullmodul verschiedenen endlichen* $\mathfrak{R}$*-Moduln aus* $\mathfrak{K}$ *bilden gegenüber der Multiplikation eine Abelsche Gruppe.*

Das Produkt zweier endlicher $\mathfrak{R}$-Moduln ist wieder ein endlicher $\mathfrak{R}$-Modul; die Multiplikation ist assoziativ und kommutativ; wegen $\mathfrak{A} = \mathfrak{o}\mathfrak{A}$ wird das Einheitsideal Einheitselement des Systems. Es ist also nur noch zu zeigen, daß die Gleichung $\mathfrak{A}\mathfrak{X} = \mathfrak{o}$ stets eine Lösung im System der endlichen $\mathfrak{R}$-Moduln besitzt.

Vorbemerkung. Wenn die Gleichung $\mathfrak{A}\mathfrak{T} = \mathfrak{B}$ eine und nur eine Lösung hat, so wird $\mathfrak{T}$ gleich dem Modulquotient $\mathfrak{B} : \mathfrak{A}$ (§ 5, 4.). Denn es wird

$$\mathfrak{T} \equiv 0\,(\mathfrak{B} : \mathfrak{A}); \text{ also } \mathfrak{B} = \mathfrak{A}\mathfrak{T} \equiv 0\,(\mathfrak{A} \cdot (\mathfrak{B} : \mathfrak{A})) \equiv 0\,(\mathfrak{B}) \text{ oder } \mathfrak{A} \cdot (\mathfrak{B} : \mathfrak{A}) = \mathfrak{B}.$$

Sei jetzt vorerst $\mathfrak{A}$ *Hauptmodul,* $\mathfrak{A} = (\alpha)$, so kommt $\mathfrak{X} = (e/\alpha)$ als Lösung von $\mathfrak{A}\mathfrak{X} = \mathfrak{o}$; es ist $\mathfrak{X}$ wieder endlicher $\mathfrak{R}$-Modul. Daraus folgt: *Jeder endliche* $\mathfrak{R}$*-Modul ist Modulquotient zweier Ideale aus* $\mathfrak{R}$, wodurch sich die Bezeichnung gebrochenes Ideal rechtfertigt. Denn sei $\tau_1, \ldots, \tau_r$ eine Modulbasis von $\mathfrak{T}$, sei $\tau_i = t_i/a$ und sei $\mathfrak{t}$ das aus den $\mathfrak{t}_i$ abgeleitete Ideal in $\mathfrak{R}$. Dann wird $\mathfrak{o}a \cdot \mathfrak{T} = \mathfrak{t}$, woraus nach der Vorbemerkung $\mathfrak{T} = (\mathfrak{t} : \mathfrak{o}a)$ folgt, der Quotient in $\mathfrak{K}$ genommen.

Die Lösung von $\mathfrak{A}\mathfrak{X} = \mathfrak{o}$ läßt sich jetzt allgemein angeben. Sei gesetzt: $\mathfrak{A} = \mathfrak{a} : \mathfrak{o}c$ und sei $\mathfrak{b}$ so bestimmt, daß $\mathfrak{a}\mathfrak{b}$ gleich einem Hauptideal $\mathfrak{o}a$ wird. Dann kommt: $\mathfrak{A}c = \mathfrak{a}$ und daraus $\mathfrak{A}\mathfrak{b}c = \mathfrak{o}a$ oder $\mathfrak{A} \cdot (\mathfrak{b}c : \mathfrak{o}a) = \mathfrak{o}$; dabei wird $\mathfrak{X}$ als Quotient eines Ideals durch ein Hauptideal wieder endlicher $\mathfrak{R}$-Modul. Aus der damit *bewiesenen Gruppeneigenschaft* folgt noch, daß der *Modulquotient irgend zweier Ideale* $\mathfrak{a} : \mathfrak{b}$ als Lösung der Gleichung $\mathfrak{b}\mathfrak{X} = \mathfrak{a}$ *endlicher* $\mathfrak{R}$*-Modul* wird.

6. Aus der Gruppeneigenschaft ergeben sich die weiteren Folgerungen:

6α. *Man kann kürzen*, d. h. aus $\mathfrak{T} = \mathfrak{A}\mathfrak{M} : \mathfrak{B}\mathfrak{M}$ folgt $\mathfrak{T} = \mathfrak{A} : \mathfrak{B}$ und umgekehrt. Denn aus $\mathfrak{T}\mathfrak{B}\mathfrak{M} = \mathfrak{T}\mathfrak{A}\mathfrak{M}$ kommt $\mathfrak{T}\mathfrak{B} = \mathfrak{T}\mathfrak{A}$ und umgekehrt.

6β. Jedes *gebrochene Ideal* (endlicher $\mathfrak{R}$-Modul) *läßt eine Darstellung zu*: $\mathfrak{C} = \mathfrak{a} : \mathfrak{b}$, *wo* $\mathfrak{a}$ *und* $\mathfrak{b}$ *teilerfremd*; durch diese Bedingung sind $\mathfrak{a}$ und $\mathfrak{b}$ *eindeutig bestimmt*. Die Möglichkeit der Darstellung ergibt sich aus 5. und 6α; aus $\mathfrak{C} = \mathfrak{a} : \mathfrak{b} = \bar{\mathfrak{a}} : \bar{\mathfrak{b}}$ ergibt sich aber $\mathfrak{a}\bar{\mathfrak{b}} = \mathfrak{b}\bar{\mathfrak{a}}$ und damit Eindeutigkeit, wenn sowohl $\mathfrak{a}, \mathfrak{b}$, wie $\bar{\mathfrak{a}}, \bar{\mathfrak{b}}$ als zueinander teilerfremd vorausgesetzt werden.

6γ. Jeder *aus einem nichtganzen* (d. h. zu $\mathfrak{K}$ und nicht zu $\mathfrak{R}$ gehörigen) *Element abgeleitete Hauptmodul* $\mathfrak{o}\eta$ *läßt eine Darstellung als Quotient von Hauptidealen zu derart, daß keine Potenz des Zählers durch den Nenner teilbar wird.* Sei in gekürzter Darstellung $\mathfrak{o}\eta = \mathfrak{b} : \mathfrak{c}$, wo also $(\mathfrak{b}, \mathfrak{c}) = \mathfrak{o}$; sei (nach 4.) $\mathfrak{o}b = \mathfrak{b}\mathfrak{a}$ und $(\mathfrak{a}, \mathfrak{c}) = \mathfrak{o}$. Dann kommt $\mathfrak{o}\eta = \mathfrak{a}\mathfrak{b} : \mathfrak{a}\mathfrak{c} = \mathfrak{o}b : \mathfrak{a}\mathfrak{c}$, und wegen $\mathfrak{a}\mathfrak{c} = \mathfrak{o}b : \mathfrak{o}\eta$ wird auch $\mathfrak{a}\mathfrak{c}$ Hauptideal, also $\mathfrak{o}\eta = \mathfrak{o}b : \mathfrak{o}c$. Es wird aber keine Potenz von $\mathfrak{a}\mathfrak{b}$ durch $\mathfrak{c}$ teilbar, wegen $(\mathfrak{a}\mathfrak{c}) = \mathfrak{o}$ und $(\mathfrak{b}, \mathfrak{c}) = \mathfrak{o}$.

7. *Nachweis des Axioms* V *der ganzen Abgeschlossenheit im Quotientenkörper.* Aus 6γ folgt, daß jedes *nichtganze Element aus* $\mathfrak{K}$ *eine Quotientendarstellung* zuläßt, $\eta = a/c$ derart, daß in $\mathfrak{R}$ *keine Potenz des Zählers durch den Nenner teilbar* wird. Denn aus $\mathfrak{o}\eta = \mathfrak{o}b : \mathfrak{o}c$ folgt, daß η sich nur bis auf eine Einheit aus $\mathfrak{R}$ von dem Quotienten b/c unterscheidet. Ein solches Element η kann mithin keiner Gleichung genügen, die es als ganz in bezug auf $\mathfrak{R}$ charakterisiert; denn aus $\eta^n + r_1\eta^{n-1} + \ldots + r_n = 0$ folgt $a^n \equiv 0\,(\mathfrak{o}c)$ in $\mathfrak{R}$.

8. Folgerung: *Sind in einem kommutativen Ring* $\mathfrak{R}$ *die Axiome* I *bis* IV *erfüllt, und ist jedes primäre Ideal irreduzibel, so ist auch Axiom* V *der ganzen Abgeschlossenheit im Quotientenkörper erfüllt.* Wegen der Axiome I bis III ist jede Primidealpotenz $\mathfrak{p}^e$ zugleich Primärideal; das gilt insbesondere für $\mathfrak{p}^2$; es wird somit $\mathfrak{p}^2$ nach Voraussetzung ein irreduzibles Ideal. Hieraus ist die Darstellung $\mathfrak{p} = (\mathfrak{o}c, \mathfrak{p}^2)$ nachzuweisen; denn damit folgt nach dem Hilfssatz § 8, 3, daß jedes Primärideal Primidealpotenz wird, was zusammen mit den andern Voraussetzungen nach 7. die ganze Abgeschlossenheit nach sich zieht.

Wegen des Teilerkettensatzes kommt $\mathfrak{p} = (\mathfrak{o}c_1, \ldots, \mathfrak{o}c_k, \mathfrak{p}^2)$, wobei als Multiplikatoren der c nur die Restklassen nach $\mathfrak{p}$ in Betracht kommen, und wobei die c als linear unabhängig in bezug auf den Restklassenkörper nach $\mathfrak{p}$ vorausgesetzt werden dürfen. Aus dieser Linearunabhängigkeit folgt aber für $k > 1$ eine Darstellung: $\mathfrak{p}^2 = [\mathfrak{q}_1, \mathfrak{q}_2]$, wo $\mathfrak{q}_1 = (\mathfrak{o}c_1\mathfrak{p}^2)$ und $\mathfrak{q}_2 = (\mathfrak{o}c_2, \ldots, \mathfrak{o}c_k, \mathfrak{p}^2)$ gesetzt ist; es werden somit $\mathfrak{q}_1$ und $\mathfrak{q}_2$ echte

Teiler von $\mathfrak{p}^2$, und es wird $\mathfrak{p}^2$ gegen Voraussetzung reduzibel. Damit ist $\mathfrak{p} = (\mathfrak{o}\,c, \mathfrak{p}^2)$ mit der sich daraus ergebenden Folgerung bewiesen.

Daß umgekehrt als Folge der Axiome I bis V jedes Primärideal irreduzibel wird, ist unmittelbar klar, da eine Primidealpotenz $\mathfrak{p}^\varrho$ sich nicht als kleinstes gemeinsames Vielfaches echter Teiler der Form $\mathfrak{p}^\sigma$ und $\mathfrak{p}^\tau$ darstellen lassen kann.

9. *Sind Nullteiler im Ring zugelassen, so folgt aus den Axiomen* I *bis* III *und der ganzen Abgeschlossenheit im Quotientenring nicht, daß jedes Primärideal irreduzibel wird*[32]). Denn es bedeute $\mathfrak{T}$ einen Ring, in dem alle Axiome I bis IV außer der ganzen Abgeschlossenheit erfüllt sind; solche Ringe gibt es, z. B. sind die vom System aller in bezug auf $\mathfrak{R}$ ganzen Größen verschiedenen endlichen Ordnungen eines endlichen Erweiterungskörpers des Quotientenkörpers von $\mathfrak{R}$ solche Ringe, wenn in $\mathfrak{R}$ die Axiome I bis V gelten (§ 3, 2.). Nach der Folgerung 8. gibt es in $\mathfrak{T}$ *reduzible* Primärideale $\mathfrak{q}$; es bedeute $\mathfrak{p}^\sigma$ ein echtes Vielfaches von $\mathfrak{q}$ und $\overline{\mathfrak{R}}$ den Restklassenring $\mathfrak{T} \mid \mathfrak{p}^\sigma$, in dem also das $\mathfrak{q}$ zugeordnete Ideal $\overline{\mathfrak{q}}$ ein vom Nullideal verschiedenes *reduzibles* Primärideal wird. In $\overline{\mathfrak{R}}$ sind die Axiome I bis III erfüllt, aber es gilt auch die ganze Abgeschlossenheit im Quotientenring. Denn da in $\mathfrak{T}$ jedes nicht durch $\mathfrak{p}$ teilbare Element zu $\mathfrak{p}^\sigma$ teilerfremd wird, sind in $\overline{\mathfrak{R}}$ alle regulären Elemente Einheiten; es ist also $\overline{\mathfrak{R}}$ mit seinem Quotientenring identisch.

§ 10.

Doppelkettensatz und Kompositionsreihe.

Im folgenden soll gezeigt werden, daß für beliebige, als wohlgeordnet angenommene Modulbereiche (§ 2) die *Voraussetzung der Gültigkeit des Doppelkettensatzes* — jede Teilerkette und jede Vielfachenkette von Moduln bricht im Endlichen ab — identisch ist mit der *Voraussetzung, daß eine Kompositionsreihe existiert*[33]). Die Spezialisierung des Modulbereichs zu einem kommutativen Ring ergibt dann die entsprechenden Tatsachen für das System aller Ideale des Ringes; dabei ist unter 2. durchweg der Modulisomorphismus durch Ringisomorphismus zu ersetzen.

---

[32]) Vgl. Anm. [12]).

[33]) Die Moduln des Bereichs sind Abelsche Gruppen gegenüber der Addition, und zwar handelt es sich um *verallgemeinerte* Abelsche Gruppen, da der Multiplikatorenbereich aus den Elementen aus $\mathfrak{R}$ besteht. Da es sich um Abelsche Gruppen handelt, fällt der Begriff der Kompositionsreihe mit dem der Hauptreihe zusammen. Die Sätze dieses Paragraphen bleiben bestehen, wenn unter „Moduln" die Gesamtheit der Normalteiler einer beliebigen nicht kommutativen, auch verallgemeinerten Gruppe verstanden wird. An die Gruppentheorie soll die von der früheren etwas abweichende Bezeichnung erinnern.

Ein Modulbereich $\mathfrak{G}$ heißt *einfach*, wenn es in $\mathfrak{G}$ keine weiteren $\mathfrak{R}$-Moduln als $\mathfrak{G}$ selbst und den Nullmodul $\mathfrak{E}$ gibt. Ein Modul $\mathfrak{A}$ heißt *einfach in* $\mathfrak{G}$, wenn $\mathfrak{G}|\mathfrak{A}$ einfach ist (größter Normalteiler).

Eine *Vielfachenkette* $\mathfrak{G}, \mathfrak{A}_1, \ldots, \mathfrak{A}_r, \mathfrak{E}$ *heißt Kompositionsreihe von* $\mathfrak{G}$ *von der Länge* r, wenn alle Moduln der Kette verschieden, und wenn jeder *Modul einfach in dem vorangehenden* ist, wenn also die Restklassenmoduln (die Quotientengruppen) $\mathfrak{A}_{i-1}|\mathfrak{A}_i$ einfache Modulbereiche sind, ebenso $\mathfrak{G}|\mathfrak{A}_1$ und $\mathfrak{A}_r$. Durch Bildung des Restklassenmoduls $\mathfrak{G}|\mathfrak{A}$ läßt sich der Fall, daß eine Kompositionsreihe von $\mathfrak{G}$ bis $\mathfrak{A} \neq \mathfrak{E}$ existiert, auf den Fall der Kompositionsreihe schlechthin zurückführen.

1. *Wird in* $\mathfrak{G}$ *die Gültigkeit des Doppelkettensatzes vorausgesetzt, so existiert in* $\mathfrak{G}$ *eine Kompositionsreihe* — dabei ist $\mathfrak{G} \neq \mathfrak{E}$ vorausgesetzt. Aus der vorausgesetzten Wohlordnung von $\mathfrak{G}$ und aus der Existenz des Teilerkettensatzes ergibt sich, wie in § 6, durch quasi-lexikographische Anordnung eine Wohlordnung des Systems aller Moduln. Vermöge dieser Wohlordnung folgt aus der Voraussetzung des Teilerkettensatzes die Existenz von mindestens einem *in* $\mathfrak{G}$ *einfachen Modul.* Ist nämlich $\mathfrak{C}_1$ der in der Wohlordnung erste echte Teiler von $\mathfrak{E}$, allgemein $\mathfrak{C}_i$ der erste echte Teiler von $\mathfrak{C}_{i-1}$, so bricht die wohlbestimmte Kette $\mathfrak{E}, \mathfrak{C}_1, \ldots, \mathfrak{C}_i, \ldots$ im Endlichen ab, führt also notwendig zu einem in $\mathfrak{G}$ einfachen Modul $\mathfrak{A}_1$. Ist $\mathfrak{A}_1 \neq \mathfrak{E}$, so gibt es nach demselben Verfahren einen in $\mathfrak{A}_1$ einfachen Modul $\mathfrak{A}_2$; ist allgemein $\mathfrak{A}_{i-1} \neq \mathfrak{E}$, so gibt es einen in $\mathfrak{A}_{i-1}$ einfachen Modul $\mathfrak{A}_i$. Man kommt auf diese Art zu einer wohlbestimmten Vielfachenkette $\mathfrak{G}, \mathfrak{A}_1, \ldots, \mathfrak{A}_i, \ldots$, die nach der Voraussetzung des Vielfachenkettensatzes im Endlichen abbricht und somit eine *Kompositionsreihe von* $\mathfrak{G}$ ergibt.

2. *Wird in* $\mathfrak{G}$ *die Existenz einer Kompositionsreihe vorausgesetzt, so gilt in* $\mathfrak{G}$ *der Doppelkettensatz.* Der Beweis erfolgt durch volle Induktion, wobei die Wohlordnung für $\mathfrak{G}$ nicht vorausgesetzt zu werden braucht. Im Laufe des Induktionsschlusses ergibt sich zugleich ein Beweis des Jordan-Hölderschen Satzes unter alleiniger Voraussetzung der Existenz einer Kompositionsreihe [34]).

---

[34]) Vgl. Masazo Sono (Anm. [19])), On Congruences I, § 11—13, für den Fall der Ringe. Es wird dort auch das Analogon zur Kompositionsreihe in nicht kommutativen Gruppen behandelt, nämlich Reihen $\mathfrak{R}, \mathfrak{A}_1, \ldots, \mathfrak{A}_r, \mathfrak{E}$, wo jeweils $\mathfrak{A}_i$ Ideal und einfach in $\mathfrak{A}_{i-1}$ ist, nicht Ideal in $\mathfrak{R}$ zu sein braucht. Tatsächlich bleiben alle obigen Überlegungen für nichtkommutative Gruppen erhalten, wenn man unter Vielfachenkette eine solche $\mathfrak{G}, \mathfrak{A}_1, \ldots, \mathfrak{A}_i, \ldots$ versteht, wo jeweils $\mathfrak{A}_i$ normal in $\mathfrak{A}_{i-1}$, und wenn Teilerketten entsprechend definiert werden. Vgl. ferner Dedekind, Über die von drei Moduln erzeugte Dualgruppe (Math. Ann. **53** (1900), S. 371—403). Hier ist für viel allgemeinere Bereiche (Modulgruppen) ebenfalls nur unter der Existenz-

Sei vorerst $\mathfrak{G}$ einfach, also $r = 0$, so daß nur die einzige Kompositionsreihe $\mathfrak{G}, \mathfrak{E}$ existiert. Es sind hier die Voraussetzungen erfüllt:

α) Durch jeden in $\mathfrak{G}$ einfachen Modul läßt sich eine Kompositionsreihe ziehen.

β) Jordan-Hölderscher Satz: Jede Kompositionsreihe ist von gleicher Länge und das System der Quotientengruppen (Restklassenmoduln) stimmt bis auf die Anordnung überein, d. h. entsprechende Quotientengruppen sind isomorph.

γ) Durch jeden beliebigen, von $\mathfrak{G}$ verschiedenen Modul läßt sich eine Kompositionsreihe ziehen.

δ) Gültigkeit des Vielfachenkettensatzes.

ε) Gültigkeit des Teilerkettensatzes.

Die Voraussetzungen α) bis ε) dürfen also für jeden Modulbereich, der eine Kompositionsreihe von der Länge $\bar{r} < r + 1$ besitzt, als erfüllt angenommen werden. Sie sollen als erfüllt nachgewiesen werden unter der *Annahme, daß in* $\mathfrak{G}$ *eine Kompositionsreihe* $\mathfrak{G}, \mathfrak{A}, \mathfrak{A}_1, \ldots, \mathfrak{A}_r, \mathfrak{E}$ *von der Länge* $r + 1$ *existiert.*

2α. Gibt es keinen von $\mathfrak{A}$ verschiedenen in $\mathfrak{G}$ einfachen Modul, so ist nichts zu beweisen. Sei also $\mathfrak{B}$ ein in $\mathfrak{G}$ einfacher Modul $\neq \mathfrak{A}$; es ist zu zeigen, daß in $\mathfrak{G}$ eine *durch* $\mathfrak{B}$ *laufende Kompositionsreihe* existiert. Da $\mathfrak{A}$ und $\mathfrak{B}$ beide in $\mathfrak{G}$ einfach und voneinander verschieden, so wird notwendig $(\mathfrak{A}, \mathfrak{B}) = \mathfrak{G}$; setzt man noch $\mathfrak{M} = [\mathfrak{A}, \mathfrak{B}]$, so kommt nach dem zweiten Isomorphiesatz (§ 4, 2.):

$$\mathfrak{G} | \mathfrak{B} \simeq \mathfrak{A} | \mathfrak{M} \quad \text{und} \quad \mathfrak{G} | \mathfrak{A} \simeq \mathfrak{B} | \mathfrak{M}:$$

es wird also $\mathfrak{M}$ einfach in $\mathfrak{A}$ und $\mathfrak{B}$. Da $\mathfrak{A}$ eine Kompositionsreihe der Länge $r < r + 1$ besitzt, gibt es somit nach den Voraussetzungen α) und β) in $\mathfrak{A}$ eine durch $\mathfrak{M}$ laufende Kompositionsreihe der Länge r, etwa $\mathfrak{A}, \mathfrak{M}, \mathfrak{M}_1, \ldots, \mathfrak{M}_{r-1}, \mathfrak{E}$; damit wird aber $\mathfrak{G}, \mathfrak{B}, \mathfrak{M}, \mathfrak{M}_1, \ldots, \mathfrak{M}_{r-1}, \mathfrak{E}$ eine durch $\mathfrak{B}$ laufende Kompositionsreihe von $\mathfrak{G}$.

2β. Zum *Nachweis des Jordan-Hölderschen Satzes* seien

(1) $\mathfrak{G}, \mathfrak{A}, \mathfrak{A}_1, \ldots, \mathfrak{A}_r, \mathfrak{E}$ und (2) $\mathfrak{G}, \mathfrak{B}, \mathfrak{B}_1, \ldots, \mathfrak{B}_s, \mathfrak{E}$ mit $s \geqq r$

zwei Kompositionsreihen von $\mathfrak{G}$. Wird hier $\mathfrak{A}$ gleich $\mathfrak{B}$, so ist nach der für $r < r + 1$ geltenden Voraussetzung alles erledigt. Im andern Fall zeigt der Vergleich mit den unter 2α konstruierten Reihen

(3) $\mathfrak{G}, \mathfrak{A}, \mathfrak{M}, \mathfrak{M}_1, \ldots, \mathfrak{M}_{r-1}, \mathfrak{E}$ und (4) $\mathfrak{G}, \mathfrak{B}, \mathfrak{M}, \mathfrak{M}_1, \ldots, \mathfrak{M}_{r-1}, \mathfrak{E}$

voraussetzung der Jordan-Höldersche Satz bewiesen (§ 6, XVI). An Stelle des zweiten Isomorphiesatzes tritt hier eine etwas schwächere Zuordnungsbeziehung, und infolgedessen ist auch die Aussage des Satzes etwas schwächer; der Beweis ist aber im Prinzip mit dem oben gegebenen identisch.

das Folgende: Nach der für $r < r+1$ gemachten Voraussetzung stimmt das System der Quotientengruppen von (1) und (3) überein; ebenso von (2) und (4), da die in (4) durch $\mathfrak{B}$ laufende Kompositionsreihe von der Länge r ist; es wird also s gleich r. Wegen der unter 2α angegebenen Isomorphie besteht weiter Übereinstimmung zwischen (3) und (4), womit die Übereinstimmung zwischen (1) und (2) und damit der *Jordan-Höldersche Satz bewiesen ist.*

2γ. Vorbemerkung. *Seien* $\mathfrak{A}, \mathfrak{B}, \mathfrak{H}$ *Moduln aus* $\mathfrak{G}$; *sei* $\mathfrak{B}$ *einfach in* $\mathfrak{A}$; *dann stimmen die Moduln* $(\mathfrak{B}, \mathfrak{H})$ und $(\mathfrak{A}, \mathfrak{H})$ *entweder überein, oder* $(\mathfrak{B}, \mathfrak{H})$ *ist einfach in* $(\mathfrak{A}, \mathfrak{H})$. Nach dem zweiten Isomorphiesatz (§ 4, 2.) kommt:

$$(\mathfrak{A}, \mathfrak{B}, \mathfrak{H}) \,|\, (\mathfrak{B}, \mathfrak{H}) \simeq \mathfrak{A} \,|\, [\mathfrak{A}, (\mathfrak{B}, \mathfrak{H})] \quad \text{oder} \quad - \text{ wegen } \mathfrak{B} \equiv 0\,(\mathfrak{A}) \; -$$
$$(\mathfrak{A}, \mathfrak{H}) \,|\, (\mathfrak{B}, \mathfrak{H}) \simeq \mathfrak{A} \,|\, \mathfrak{C} \quad \text{für} \quad \mathfrak{C} = [\mathfrak{A}, (\mathfrak{B}, \mathfrak{H})].$$

Dabei wird $\mathfrak{C} \equiv 0\,(\mathfrak{A})$; andererseits wird $\mathfrak{B} \equiv 0\,(\mathfrak{C})$ wegen $\mathfrak{B} \equiv 0\,(\mathfrak{A})$ und $\mathfrak{B} \equiv 0\,((\mathfrak{B}, \mathfrak{H}))$; es liegt also $\mathfrak{C}$ zwischen $\mathfrak{A}$ und $\mathfrak{B}$ und ist somit nach Voraussetzung mit $\mathfrak{A}$ oder $\mathfrak{B}$ identisch, woraus die Vorbemerkung folgt.

Sei jetzt wieder $\mathfrak{G}, \mathfrak{A}, \mathfrak{A}_1, \ldots, \mathfrak{A}_r, \mathfrak{E}$ eine Kompositionsreihe von $\mathfrak{G}$ und $\mathfrak{H}$ ein beliebiger, von $\mathfrak{G}$ verschiedener Modul aus $\mathfrak{G}$. Um zu zeigen, daß *dnrch* $\mathfrak{H}$ *eine Kompositionsreihe* läuft, sei die Reihe der Moduln $\mathfrak{G}, (\mathfrak{A}, \mathfrak{H}), (\mathfrak{A}_1, \mathfrak{H}) \ldots (\mathfrak{A}_r, \mathfrak{H}), \mathfrak{H}$ gebildet. Nach der Vorbemerkung bilden die verschiedenen unter diesen Moduln $\mathfrak{G}, \mathfrak{C}, \mathfrak{C}_1, \ldots, \mathfrak{C}_s, \mathfrak{H}$ eine Kompositionsreihe von $\mathfrak{G}$ nach $\mathfrak{H}$; es wird also $\mathfrak{C}$ — was im Spezialfall 2α mit $\mathfrak{H}$ zusammenfällt — ein in $\mathfrak{G}$ einfacher Modul. Somit existiert nach 2α in $\mathfrak{C}$ eine Kompositionsreihe der Länge $r < r+1$, und folglich läßt sich in $\mathfrak{C}$ nach Voraussetzung eine Kompositionsreihe durch $\mathfrak{H}$ ziehen, was durch Zufügung von $\mathfrak{G}$ *in* $\mathfrak{G}$ *eine Kompositionsreihe durch* $\mathfrak{H}$ ergibt. Die wiederholte Anwendung dieser Überlegung zeigt noch, daß man eine solche Kompositionsreihe insbesondere als Verlängerung der von $\mathfrak{G}$ nach $\mathfrak{H}$ konstruierten annehmen kann.

2δ. Nachweis des Vielfachenkettensatzes. Sei wieder in $\mathfrak{G}$ die Existenz einer Kompositionsreihe der Länge $r+1$ vorausgesetzt, und sei $\mathfrak{G}, \mathfrak{B}, \mathfrak{B}_1, \ldots, \mathfrak{B}_\nu, \ldots$ eine Vielfachenkette; dabei sei jeder Modul als echtes Vielfaches des vorangehenden vorausgesetzt. Daß die Kette mit $\mathfrak{G}$ beginnt, ist keine Beschränkung der Allgemeinheit, da man immer $\mathfrak{G}$ als erstes Glied zufügen kann. Nach 2γ gibt es eine durch $\mathfrak{B}$ laufende Kompositionsreihe in $\mathfrak{G}$, und somit besitzt $\mathfrak{B}$ eine Kompositionsreihe von kürzerer Länge. Also bricht nach Voraussetzung die Kette $\mathfrak{B}, \mathfrak{B}_1, \ldots, \mathfrak{B}_\nu, \ldots$ im Endlichen ab; es gilt also auch das gleiche für die durch Hinzufügung von $\mathfrak{G}$ verlängerte.

2ε. Nachweis des Teilerkettensatzes. Sei wieder in $\mathfrak{G}$ die Existenz einer Kompositionsreihe der Länge $r+1$ vorausgesetzt, und sei $\mathfrak{E}, \mathfrak{C}, \mathfrak{C}_1, \ldots, \mathfrak{C}_\nu, \ldots$ eine Teilerkette; dabei sei jeder Modul als echter Teiler des vorangehenden vorausgesetzt. Daß die Kette mit $\mathfrak{E}$ beginnt, ist wieder keine Beschränkung der Allgemeinheit. Nach 2γ gibt es eine durch $\mathfrak{C}$ laufende Kompositionsreihe in $\mathfrak{G}$, somit gibt es in $\mathfrak{G}|\mathfrak{C}$ eine Kompositionsreihe von kürzerer Länge. Also bricht nach Voraussetzung in $\mathfrak{G}|\mathfrak{C}$ die Teilerkette $\mathfrak{E}|\mathfrak{C}, \mathfrak{C}_1|\mathfrak{C}, \ldots, \mathfrak{C}_\nu|\mathfrak{C}, \ldots$ im endlichen ab. Wegen des eineindeutigen Entsprechens — nach dem ersten Isomorphiesatz (§ 4, 2.) — gilt das gleiche für die ursprüngliche, mit $\mathfrak{C}$ beginnende Kette, und damit auch für die durch Hinzufügung von $\mathfrak{E}$ verlängerte.

Die Äquivalenz der Voraussetzungen — Kompositionsreihe oder Doppelkettensatz — ist damit bewiesen.

(Eingegangen am 13. 8. 1925.)