Mathematisch-
Naturwissenschaftliche
Bibliothek

10

LUGOWSKI-WEINERT

GRUNDZÜGE DER ALGEBRA

TEIL II

MATHEMATISCH-NATURWISSENSCHAFTLICHE
BIBLIOTHEK

10

GRUNDZÜGE DER ALGEBRA

TEIL II

ALLGEMEINE RING- UND KÖRPERTHEORIE

von

Dr. Herbert Lugowski und Dr. Hanns Joachim Weinert

Pädagogische Hochschule Potsdam

B.G.TEUBNER VERLAGSGESELLSCHAFT · LEIPZIG

1 9 5 8

Lizenz-Nr. 294/375/47/58

Printed in Germany

Satz und Druck: (III/18/154) B.G.Teubner, Leipzig C1, Querstr.17 · 512

INHALTSVERZEICHNIS

V. GRUNDBEGRIFFE DER RING- UND KÖRPERTHEORIE

Wie wir schon im ersten Teil allgemein ausgeführt haben, sind die Strukturbegriffe der modernen Algebra das Ergebnis einer langen Entwicklung. Sie ist durch das Bestreben gekennzeichnet, aus den verschiedensten mathematischen Gebieten gemeinsame Gesetzmäßigkeiten herauszuarbeiten und zusammengefaßt zu untersuchen, was neben einer systematischen Durchdringung vor allem auf ein tieferes Verständnis und auf neue, wegweisende Gesichtspunkte abzielt.

Als grundlegendes Beispiel für ein solches Vorgehen haben wir im ersten Teil die Gruppentheorie kennengelernt. Sie ist dadurch charakterisiert, daß sie jeweils nur eine zwischen den Elementen einer Menge erklärte Verknüpfung behandelt. Es kommt aber oft darauf an, zwei Verknüpfungen gleichzeitig und in ihrem gegenseitigen Zusammenhang zu betrachten, wie etwa die Addition und Multiplikation von Zahlen, von Matrizen oder von Restklassen ganzer Zahlen. Solchen algebraischen Strukturen mit zwei aufeinander bezogenen Verknüpfungen wollen wir uns nunmehr zuwenden.

Dabei wird man natürlich nach Möglichkeit auf Ergebnisse zurückgreifen, die man schon aus der Untersuchung einer dieser beiden Verknüpfungen kennt. So liegen etwa bei den oben genannten Beispielen hinsichtlich der Addition jeweils Gruppen vor, während bezüglich der Multiplikation nur ein Teil der Gruppenaxiome erfüllt ist (vgl. B(2.1), B(2.4) und B(2.8)). Letzteres veranlaßt uns, in einem vorbereitenden Paragraphen auch auf solche Verknüpfungen etwas näher einzugehen, wobei für unsere Zwecke eine Betrachtung sogenannter Halbgruppen ausreicht.

§ 24. Halbgruppen

Betrachten wir etwa die Multiplikation in der Menge der ganzen Zahlen, in der Menge der Matrizen vom Typ (n, n) oder in der Menge der Restklassen ganzer Zahlen mod m, so stellen wir fest, daß sie stets zwei Elementen ein eindeutig bestimmtes Element der gleichen Menge zuordnet und daß sie assoziativ ist. Dagegen ist die Multiplikation in den genannten Mengen nicht immer umkehrbar. Mit der in D(1.1) eingeführten Bezeichnungsweise sind also stets die Axiome *M I* und *M II*, nicht aber *M III* bzw. die zu ihm äquivalenten Axiome erfüllt. Dies führt uns zur

Definition **D (24.1)**

Eine nichtleere Menge von Elementen $a, b, c, \ldots$ heißt eine multiplikative Halbgruppe $\mathfrak{H}$, wenn in ihr eine als Multiplikation geschriebene Verknüpfung erklärt ist, die folgenden Axiomen genügt:

M I: Die Multiplikation ordnet je zwei in bestimmter Reihenfolge gegebenen Elementen $a \in \mathfrak{H}$ und $b \in \mathfrak{H}$ ein Element $c \in \mathfrak{H}$ eindeutig zu:

$$a \cdot b = c.$$

M II: Die Multiplikation ist assoziativ:

$$(a \cdot b) \cdot c = a \cdot (b \cdot c).$$

Insbesondere heißt eine Halbgruppe abelsch, wenn darüber hinaus gilt:

M IV: Die Multiplikation ist kommutativ:

$$a \cdot b = b \cdot a.$$

Die Begriffe endlich und unendlich übertragen sich aus der Mengenlehre auf beliebige algebraische Strukturen, also auch auf Halbgruppen.

Obgleich wir im folgenden nur multiplikative Halbgruppen benötigen, vermerken wir, daß der abstrakte Begriff der Halbgruppe von der gewählten Schreibweise der Verknüpfung unabhängig ist. So bilden z. B. die natürlichen Zahlen sowohl hinsichtlich der Addition als auch der Multiplikation eine Halbgruppe.

Die in F(1.2) bzw. F(1.3) formulierten Verallgemeinerungen des Assoziativgesetzes *M II* bzw. des Kommutativgesetzes *M IV* auf Produkte mit mehr als 3 bzw. 2 Faktoren sind unabhängig von *M III* und gelten also in beliebigen Halbgruppen bzw. abelschen Halbgruppen. Dagegen beruhen die weiteren Ausführungen in § 1 wesentlich auf der Gültigkeit von *M III*.

So gibt es z. B. Halbgruppen, in denen kein Einselement existiert, wie etwa in der multiplikativen Halbgruppe der geraden Zahlen. Weiterhin hatten wir am Ende von B(2.4) das multiplikative System der Matrizen

$$\begin{pmatrix} a_{11} & a_{12} \\ 0 & 0 \end{pmatrix}$$

betrachtet. Dieses bildet eine multiplikative Halbgruppe, in der es unendlich viele Linkseinselemente, dagegen kein Rechtseinselement gibt. Schließlich besitzen die am Anfang des Paragraphen genannten Halbgruppen ein eindeutig bestimmtes Einselement. Wir ersehen daraus, daß man allein aus *M I* und *M II* weder die Existenz noch die Eindeutigkeit eventuell vorhandener Einselemente folgern kann. Um diesbezügliche Aussagen machen zu können, bedarf es also zusätzlicher Voraussetzungen.

Satz **S (24.2)**

Wenn in einer Halbgruppe $\mathfrak{H}$ *wenigstens ein Linkseinselement* e_L *und wenigstens ein Rechtseinselement* e_R *existieren, so ist* $e_L = e_R = e$ *eindeutig bestimmtes Einselement von* $\mathfrak{H}$. *Außer e gibt es kein weiteres Links- oder Rechtseinselement in* $\mathfrak{H}$.

Der Beweis verläuft wie der Teil 3) des Beweises von S(1.4), während die dort unter 1) und 2) nachgewiesene Existenz von e_L und e_R hier vorausgesetzt werden muß.

Damit ergeben sich für eine Halbgruppe $\mathfrak{H}$ genau folgende vier einander ausschließende Möglichkeiten:

Die Halbgruppe $\mathfrak{H}$ besitzt

a) weder ein Links- noch ein Rechtseinselement;

b) wenigstens ein Linkseinselement, aber kein Rechtseinselement;

c) wenigstens ein Rechtseinselement, aber kein Linkseinselement;

d) ein eindeutig bestimmtes Einselement.

Da bei kommutativer Verknüpfung jedes Linkseinselement zugleich Rechtseinselement ist und umgekehrt, kommen dann nach S(24.2) nur die Fälle a) und d) in Frage:

Folgerung **F (24.3)**

Eine abelsche Halbgruppe hat entweder kein oder ein eindeutig bestimmtes Einselement.

Entsprechende Betrachtungen über inverse Elemente stellt man im allgemeinen nur dann an, wenn eine Halbgruppe mit eindeutig bestimmtem Einselement vorliegt. Auch hier müssen über *M I* und *M II* hinausgehende Voraussetzungen gemacht werden.

Satz **S (24.4)**

Es sei $\mathfrak{H}$ eine Halbgruppe mit eindeutig bestimmtem Einselement e. Wenn zu einem Element $a \in \mathfrak{H}$ wenigstens ein Linksinverses a_L^{-1} und wenigstens ein Rechtsinverses a_R^{-1} existieren, so ist $a_L^{-1} = a_R^{-1} = a^{-1}$ eindeutig bestimmtes Inverses zu a. Außer a^{-1} gibt es zu a kein weiteres Links- oder Rechtsinverses.

Der Beweis verläuft ebenfalls wie der Teil 3) des Beweises von S(1.5), wobei wieder die dort unter 1) und 2) nachgewiesene Existenz von a_L^{-1} und a_R^{-1} unseren Voraussetzungen entspricht.

Für eine Halbgruppe $\mathfrak{H}$ mit eindeutig bestimmten Einselement können somit für jedes ihrer Elemente unabhängig voneinander die folgenden sich gegenseitig ausschließenden Möglichkeiten eintreten:

Ein Element $a \in \mathfrak{H}$ besitzt

a) weder ein Links- noch ein Rechtsinverses;

b) wenigstens ein Linksinverses, aber kein Rechtsinverses;

c) wenigstens ein Rechtsinverses, aber kein Linksinverses;

d) ein eindeutig bestimmtes Inverses.

Bei kommutativer Verknüpfung entfallen wiederum b) und c):

Folgerung **F (24.5)**

In einer abelschen Halbgruppe mit Einselement hat ein Element entweder kein Inverses oder ein eindeutig bestimmtes Inverses.

Schließlich untersuchen wir, ob und wann die in einer Halbgruppe $\mathfrak{H}$ erklärte Verknüpfung umkehrbar ist. Der Fall, daß die beiden Gleichungen $ax = b$ und $ya = b$ mit beliebigen $a \in \mathfrak{H}$ und $b \in \mathfrak{H}$ in $\mathfrak{H}$ lösbar sind, entspricht der Gültigkeit von *M III* und kennzeichnet die Halbgruppe $\mathfrak{H}$ als Gruppe. Wenn also tatsächlich nur eine Halbgruppe vorliegt, ist wenigstens eine solche Gleichung in $\mathfrak{H}$ unlösbar. Damit ergeben sich wieder verschiedene Möglichkeiten. So können nämlich beide Gleichungen je nach Wahl von a und b unabhängig voneinander lösbar oder unlösbar sein, und es kann sogar der Fall eintreten, daß $ya = b$ mehrere Lösungen, dagegen $ax = b$ keine Lösung besitzt und umgekehrt (vgl. Aufg. 3). Wie das Beispiel der natürlichen Zahlen zeigt, gibt es aber Halbgruppen, in denen jede ausführbare Division eindeutig ist:

Definition **D (24.6)**

Eine Halbgruppe $\mathfrak{H}$ heißt regulär, wenn über M I und M II hinaus das folgende Axiom gilt:

M III: Sind $x_1 \in \mathfrak{H}$ und $x_2 \in \mathfrak{H}$ Lösungen der Gleichung $ax = b$ mit $a \in \mathfrak{H}$ und $b \in \mathfrak{H}$, so folgt $x_1 = x_2$.*

Entsprechend:

Sind $y_1 \in \mathfrak{H}$ und $y_2 \in \mathfrak{H}$ Lösungen der Gleichung $ya = b$ mit $a \in \mathfrak{H}$ und $b \in \mathfrak{H}$, so folgt $y_1 = y_2$.

Aus S(1.10) ergibt sich unmittelbar:

Folgerung **F (24.7)**

Eine endliche reguläre Halbgruppe ist Gruppe.

Aufgaben zu § 24

1. Man gebe einige Beispiele von multiplikativen Halbgruppen an und charakterisiere ihre Eigenschaften.
2. Die zu Halbgruppen führenden Verknüpfungen brauchen nicht die üblicherweise als Multiplikation oder Addition bezeichneten Operationen zu sein. Als Beispiel zeige man, daß die Untermengen einer beliebigen Menge $\mathfrak{M}$ sowohl mit der Durchschnittsbildung als auch mit der Vereinigungsbildung als Verknüpfung abelsche Halbgruppen mit Einselement sind.
3. Man bilde in der Halbgruppe $\mathfrak{H}$ der Matrizen vom Typ (n, n) mit reellen Zahlen als Elementen Beispiele dafür, daß die Gleichung $YA = B$ unendlich viele Lösungen, aber die Gleichung $AX = B$ keine Lösung in $\mathfrak{H}$ besitzt.

§ 25. Ringe

Gemäß unseren allgemeinen Vorbetrachtungen legen wir unsere Untersuchungsobjekte in Anlehnung an die Addition und Multiplikation der Zahlenrechnung fest. Die so zu erklärenden algebraischen Strukturen mit zwei Verknüpfungen nennt man allgemein Ringe und unterscheidet je nach der Auswahl der geforderten Eigenschaften Schiefringe, kommutative Ringe, Schiefkörper und kommutative Körper.

Definition **D (25.1)**

Eine nichtleere Menge von Elementen $a, b, c, \ldots$ heißt ein Schiefring $\mathfrak{R}$, wenn in ihr zwei Verknüpfungen (geschrieben als Addition und Multiplikation) erklärt sind, die den folgenden Axiomen genügen:

A I: *Die Addition ordnet je zwei Elementen $a \in \mathfrak{R}$ und $b \in \mathfrak{R}$ ein Element $c \in \mathfrak{R}$ eindeutig zu:*

$$a + b = c.$$

A II: *Die Addition ist assoziativ:*

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

A III: *Die Addition ist in $\mathfrak{R}$ in dem Sinne umkehrbar, daß zu beliebigen $a \in \mathfrak{R}$ und $b \in \mathfrak{R}$ die Gleichung*

$$a + x = b$$

mit $x \in \mathfrak{R}$ lösbar ist (Möglichkeit der Subtraktion).

A IV: *Die Addition ist kommutativ:*

$$a + b = b + a.$$

M I: *Die Multiplikation ordnet je zwei in bestimmter Reihenfolge gegebenen Elementen $a \in \mathfrak{R}$ und $b \in \mathfrak{R}$ ein Element $c \in \mathfrak{R}$ eindeutig zu:*

$$a \cdot b = c.$$

M II: *Die Multiplikation ist assoziativ:*

$$(a \cdot b) \cdot c = a \cdot (b \cdot c).$$

D: *Addition und Multiplikation sind distributiv verbunden:*

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

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

Insbesondere nennt man den Schiefring $\mathfrak{R}$ *einen* Schiefkörper, *wenn darüber hinaus erfüllt ist:*

M III: Die Multiplikation ist in $\mathfrak{R}$ *in dem Sinne umkehrbar, daß zu beliebigen* $a \in \mathfrak{R}$ *und* $b \in \mathfrak{R}$ *mit* $a \neq o$[1] *die Gleichungen*

$$a \cdot x = b, \quad y \cdot a = b$$

mit $x \in \mathfrak{R}$ *und* $y \in \mathfrak{R}$ *lösbar sind (Möglichkeit der beiderseitigen Division durch vom Nullelement verschiedene Elemente).*

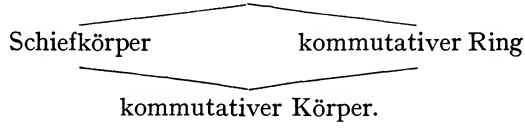
Hingegen heißt ein Schiefring $\mathfrak{R}$ *insbesondere ein* kommutativer Ring[2], *wenn außer den Schiefringaxiomen noch gilt:*

M IV: Die Multiplikation ist kommutativ:

$$a \cdot b = b \cdot a.$$

Sind sowohl M III als auch M IV zusätzlich erfüllt, so nennt man den Schiefring $\mathfrak{R}$ *einen* kommutativen Körper[2].

Die gegenseitigen Beziehungen dieser vier Begriffe veranschaulicht das Schema:



Ein kommutativer Körper ist also sowohl Schiefkörper als auch kommutativer Ring und erst recht Schiefring.

---

1) o bedeutet dabei das nach S(1.13) in $\mathfrak{R}$ eindeutig bestimmte Nullelement der additiven Verknüpfung. *M III* ist nur sinnvoll, wenn in $\mathfrak{R}$ wenigstens ein Element $a \neq o$ existiert, also $\mathfrak{R}$ aus mindestens zwei Elementen besteht.

2) Die der Verwendung bei Gruppen entsprechende Bezeichnung „abelsch" ist nicht möglich, da sie schon für andere Zusammenhänge vergeben ist.

Ohne Zweifel wäre es unserem Sprachempfinden angemessener, für die Oberbegriffe Schiefring und Schiefkörper einfach Ring und Körper zu sagen; kommutativer Ring und kommutativer Körper wären dann auch sprachlich durch den Zusatz „kommutativ" gekennzeichnete Unterbegriffe. Durch die historische Entwicklung hat sich jedoch teilweise sogar die gegenteilige Sprechweise eingebürgert, daß man bei den Unterbegriffen den kennzeichnenden Zusatz „kommutativ" wegläßt. Doch auch diese Bezeichnung „Schiefring — Schiefkörper — Ring — Körper" ist in der Literatur nicht einheitlich durchgeführt; vielmehr wird oft das Wort „Ring" gleichzeitig für den Schiefring verwendet.
Man muß sich daher stets überzeugen, in welcher Bedeutung die Worte Ring und Körper benutzt werden. Auch wir machen von dieser Freiheit der Benennung Gebrauch und verwenden nur in Zweifelsfällen die in D(25.1) festgelegten ausführlichen Bezeichnungen. Beispiele für die eingeführten Begriffe findet man in § 26, dessen Lektüre bereits hier eingeschoben werden kann (unter Übergehung der kurzen Bemerkungen über Nullteiler).

Wir wenden uns zunächst der Behandlung allgemeiner Eigenschaften von Schiefringen und kommutativen Ringen zu. Die darüber gemachten Aussagen gelten selbstverständlich erst recht für Schiefkörper bzw. kommutative Körper, auf deren besondere Eigenschaften wir am Ende dieses Paragraphen eingehen.

Nach D(25.1) *ist jeder Ring* $\mathfrak{R}$ *bezüglich der additiven Verknüpfung ein Modul. Es gelten also für die Addition die aus der Gruppentheorie geläufigen Rechengesetze. Insbesondere besitzt* $\mathfrak{R}$ *ein eindeutig bestimmtes Nullelement o sowie zu jedem Element a ein eindeutig bestimmtes entgegengesetztes Element* $(-a)$*; jede Subtraktion ist in* $\mathfrak{R}$ *eindeutig ausführbar.* Ferner kann in D(25.1) gemäß S(1.18) *A III* durch die Axiome $A\,III_1$ und $A\,III_2$, im endlichen Falle gemäß S(1.19) auch durch *A III** ersetzt werden. In diesem Sinne spricht man auch von der *additiven Gruppe des Ringes* $\mathfrak{R}$ (bezeichnet durch $\mathfrak{R}^+$), wenn man $\mathfrak{R}$ nur hinsichtlich der Addition betrachtet.

Bezüglich der multiplikativen Verknüpfung ist jeder Ring $\mathfrak{R}$ *Halbgruppe, im kommutativen Falle abelsche Halbgruppe. Es gelten also allgemein die von der Multiplikation in Halbgruppen erfüllten Rechengesetze* (vgl. nochmals F(1.2) und F(1.3)). Die verschiedenen Möglichkeiten betreffs Existenz und Eindeutigkeit von Einselement und inversen Elementen haben wir bereits in § 24 ausführlich diskutiert. Insbesondere übertragen sich die Aussagen S(24.2), F(24.3), S(24.4), F(24.5) und die damit im Zusammenhang aufgestellten Fallunterscheidungen.

Es bleibt nun zu untersuchen, welche Aussagen sich aus dem Zusammenhang beider Verknüpfungen ergeben, der durch das Distributivgesetz D vermittelt wird. Wir vermerken nebenbei, daß bei Gültigkeit des Kommutativgesetzes $M\,IV$ die beiden unter D zusammengefaßten Relationen wechselseitig auseinander folgen und damit nur eine von ihnen gefordert zu werden braucht.

Folgerung **F (25.2)**

In seiner allgemeinsten Form lautet das in beliebigen Ringen gültige Distributivgesetz:

$$\left(\sum_{\nu=1}^{n} a_\nu\right) \cdot \left(\sum_{\mu=1}^{m} b_\mu\right) = \sum_{\nu=1}^{n} \sum_{\mu=1}^{m} a_\nu \cdot b_\mu = \sum_{\nu=1,\,\mu=1}^{n,\,m} a_\nu \cdot b_\mu .$$

Die hier festgelegte Reihenfolge der Faktoren darf nur bei zusätzlicher Gültigkeit von $M\,IV$ abgeändert werden (vgl. Aufg. 1).

Für das durch die additive Verknüpfung festgelegte Nullelement eines Ringes $\mathfrak{R}$ gilt bezüglich der multiplikativen Verknüpfung[1]):

Satz **S (25.3)**

Das in einem Ring $\mathfrak{R}$ eindeutig bestimmte Nullelement o erfüllt für alle Elemente $a \in \mathfrak{R}$

$$a \cdot o = o \cdot a = o .$$

Beweis

Aus der ersten Relation des Distributivgesetzes D

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

ergibt sich insbesondere für $c = o$

$$a \cdot b = a \cdot (b + o) = a \cdot b + a \cdot o .$$

Addiert man auf beiden Seiten das zu ab entgegengesetzte Element $-(ab)$, so folgt

$$a \cdot o = o .$$

Entsprechend beweist man aus der anderen Relation von D die Aussage

$$o \cdot a = o .$$

qed.

1) Die umgekehrte Fragestellung, wie sich ein eventuell existierendes, eindeutig bestimmtes Einselement bezüglich der additiven Verknüpfung verhält, ordnet sich allgemeineren Betrachtungen im § 27 unter.

Die additive Verknüpfung bestimmt zu jedem Element eindeutig ein entgegengesetztes Element. Auch über diese Elemente lassen sich bezüglich der Multiplikation Aussagen machen, die den bekannten „Vorzeichenregeln" der Zahlenrechnung entsprechen.

Satz **S (25.4)**

In jedem Ring $\mathfrak{R}$ *gelten die Relationen:*

$$\begin{aligned}(-a)\cdot b &= -(a\cdot b),\\ a\cdot(-b) &= -(a\cdot b),\\ (-a)\cdot(-b) &= a\cdot b.\end{aligned}$$

Beweis

Aus $(-a)+a=o$ folgt durch Multiplikation mit b von rechts wegen der eindeutigen Bestimmtheit des Produktes in $\mathfrak{R}$

$$((-a)+a)\cdot b = o\cdot b.$$

Anwendung von D und S (25.3) ergibt

$$(-a)\cdot b + a\cdot b = o.$$

Andererseits gilt

$$-(a\cdot b)+a\cdot b = o,$$

wobei $-(a\cdot b)$ das eindeutig bestimmte entgegengesetzte Element zu $a\cdot b$ ist. Also folgt

$$(-a)\cdot b = -(a\cdot b).$$

Die entsprechenden Ansätze

$$a\cdot((-b)+b) = a\cdot o$$
$$((-a)+a)\cdot(-b) = o\cdot(-b)$$

ergeben durchgerechnet die beiden anderen Relationen.

qed.

In der schon unter F (1.16) eingeführten Schreibweise

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

gelten dann die üblichen Formeln wie

$$(a-b)\cdot c = ac - bc \text{ usw.}$$

Der Beweis von S (25.4) zeigt natürlich insbesondere die Richtigkeit der „Vorzeichenregeln" der Zahlenrechnung, allerdings unter der Voraussetzung, daß für die betreffenden Zahlenbereiche bereits die Ringaxiome nachgewiesen

sind. Dieser Sachverhalt liegt bei einer Einführung der negativen Zahlen im Schulunterricht gerade nicht vor, sondern mit Hilfe der Vorzeichenregeln kommt man dort erst zu den Rechengesetzen, die in ihrer Gesamtheit den Ringaxiomen äquivalent sind. Bei einem solchen, natürlich methodisch bedingten Vorgehen vertauschen sich die gegenseitigen Beziehungen derart, daß die Vorzeichenregeln den Charakter axiomatischer Festlegungen gewinnen. Sie sind dabei also unbeweisbar und können allenfalls durch Vorgriffe auf erwünschte Rechengesetze (wie etwa das Distributivgesetz) als sinnvoll nahegelegt werden, entsprechend der Tatsache, daß die Vorzeichenregeln eben nach S(25.4) in Ringen notwendig erfüllt sein müssen.

Dagegen kommt man bei der Einführung etwa der ganzen Zahlen als Zahlenpaare natürlicher Zahlen (siehe auch § 31) unmittelbar zum Nachweis der Ringaxiome und kann dann aus S(25.4) auf die Vorzeichenregeln schließen. Freilich ergeben sich diese auch direkt aus den für diese Zahlenpaare definierten Rechenverknüpfungen, wie etwa

$$n \cdot (-m) = (n, o) \cdot (o, m) = (o, nm) = -(n \cdot m).$$

Die bisherigen Aussagen entsprechen geläufigen Rechenregeln der Buchstabenrechnung (gegebenenfalls unter Berücksichtigung der Reihenfolge der Faktoren), die ja ebenso wie die in D(25.1) eingeführten algebraischen Strukturen aus der Zahlenrechnung abstrahiert sind. Das hat den Vorteil, daß einem die Rechentechnik in Ringen im wesentlichen (man beachte aber das Folgende!) bereits aus der Elementarmathematik geläufig ist. Streng genommen liegen die Dinge natürlich umgekehrt: Die formale Technik der Buchstabenrechnung kann nur auf Rechenobjekte (etwa Funktionen, Matrizen usw.) angewendet werden, wenn diese Objekte und ihre Verknüpfungen den entsprechenden Ringaxiomen (oder ihnen äquivalenten Grundgesetzen) genügen.

Allerdings ist die mit D(25.1) festgelegte Rechentechnik noch wesentlich allgemeiner als die übliche Buchstabenrechnung, so daß durchaus nicht alle für Zahlen gültigen Rechenregeln in beliebigen Ringen bestehen bleiben[1]).

So braucht z. B. die Umkehrung von S(25.3), daß ein Produkt nur dann verschwindet, wenn wenigstens ein Faktor gleich o ist, in beliebigen Ringen nicht zu gelten. Wir haben in B(26.2) und B(26.3) Beispiele für $a \cdot b = o$ mit $a \neq o$, $b \neq o$ und erklären daher:

---

1) Vielmehr kann man dies erst durch weitere einschränkende Voraussetzungen über die betrachteten Ringe erreichen, und zwar handelt es sich dabei um die bereits erwähnte Kommutativität der Multiplikation, um die im folgenden behandelte Nullteilerfreiheit und schließlich noch um eine Voraussetzung über das additive Verhalten des Einselementes, auf die wir im § 27 zu sprechen kommen.

Definition **D (25.5)**

Ein Element a aus einem Ring $\mathfrak{R}$ heißt linker (bzw. rechter) Nullteiler, wenn in $\mathfrak{R}$ wenigstens ein Element $b \neq o$ existiert mit $a \cdot b = o$ (bzw. $b \cdot a = o$).

Nach dieser Definition und S (25.3) ist auch das Nullelement o von $\mathfrak{R}$ sowohl linker wie rechter Nullteiler. Die aus der Zahlenrechnung bekannten Ringe sind Beispiele für solche Ringe, in denen das Nullelement auch der einzige auftretende Nullteiler ist. In Verallgemeinerung dieses Sachverhalts kommen wir zur

Definition **D (25.6)**

Ein Ring $\mathfrak{R}$ heißt „nullteilerfrei"[1]), wenn er außer dem Nullelement o weder linke noch rechte Nullteiler enthält.
Ein kommutativer nullteilerfreier Ring heißt Integritätsbereich[2]).

Ein Ring $\mathfrak{R}$ ist also genau dann nullteilerfrei, wenn für alle Elemente aus $\mathfrak{R}$ gilt:

Aus $ab = o$ und $a \neq o$ (bzw. $b \neq o$) folgt $b = o$ (bzw. $a = o$).

Die dadurch erreichte Angleichung an die Gesetzmäßigkeiten der Zahlenrechnung wird auch durch die folgende Aussage deutlich.

Satz **S (25.7)**

In nullteilerfreien Ringen $\mathfrak{R}$ und nur in diesen ist die Division durch vom Nullelement o verschiedene Elemente eindeutig, d. h., es gilt:

M III: Sind $x_1 \in \mathfrak{R}$ und $x_2 \in \mathfrak{R}$ Lösungen der Gleichung $ax = b$ mit $a \in \mathfrak{R}$, $b \in \mathfrak{R}$ und $a \neq o$, so folgt $x_1 = x_2$.*

Entsprechend:

Sind $y_1 \in \mathfrak{R}$ und $y_2 \in \mathfrak{R}$ Lösungen der Gleichung $ya = b$ mit $a \in \mathfrak{R}$, $b \in \mathfrak{R}$ und $a \neq o$, so folgt $y_1 = y_2$.

Der Beweis ergibt sich sofort aus dem folgenden, allgemeineren Kriterium für die Eindeutigkeit der Division in beliebigen Ringen:

---

1) „Nullteilerfrei" bezieht sich also, sprachlich nicht ganz einwandfrei, nur auf von o verschiedene Nullteiler. D (25.6) ist natürlich nur sinnvoll, wenn $\mathfrak{R}$ außer o wenigstens noch ein weiteres Element enthält.

2) In der Literatur ist es teilweise üblich, für Integritätsbereiche darüber hinaus die Existenz des Einselementes zu fordern.

Satz **S (25.8)**

Es sei a ein fest gewähltes Element eines beliebigen Ringes $\mathfrak{R}$. Dann gilt:

Aus $ax_1 = ax_2$ folgt $x_1 = x_2$ für alle möglichen Ringelemente x_1 und x_2 dann und nur dann, wenn a kein linker Nullteiler ist.

Entsprechend:

Aus $y_1a = y_2a$ folgt $y_1 = y_2$ für alle möglichen Ringelemente y_1 und y_2 dann und nur dann, wenn a kein rechter Nullteiler ist.

Die Division durch Nichtnullteiler und nur durch diese ist also eindeutig, falls sie überhaupt möglich ist.

Beweis

1. Es sei a kein linker Nullteiler. Dann folgt für alle möglichen x_1 und x_2 mit $ax_1 = ax_2$ wegen

$$ax_1 - ax_2 = a(x_1 - x_2) = o,$$

daß $x_1 - x_2 = o$, also $x_1 = x_2$ ist.

2. Folgt umgekehrt aus $ax_1 = ax_2$ stets $x_1 = x_2$, so kann a kein linker Nullteiler sein. Aus

$$ax_1 = o \quad \text{und} \quad ao = o$$

ergibt sich nämlich (mit $x_2 = o$) sofort $x_1 = o$.

Für rechte Nullteiler beweist man den Satz analog.

qed.

In beliebigen Ringen spielen also die Nullteiler bezüglich der Division eine ähnliche Sonderrolle wie die Null in der Zahlenrechnung. Auch der folgende Satz spricht eine aus der Zahlenrechnung bekannte Eigenschaft der Null für alle Nullteiler eines Ringes aus.

Satz **S (25.9)**

Ein linker (bzw. rechter) Nullteiler von $\mathfrak{R}$ besitzt kein Linksinverses (bzw. Rechtsinverses)[1]).

---

1) Selbstverständlich hat dieser Satz nur Sinn, wenn $\mathfrak{R}$ ein Einselement enthält.

Beweis

Es sei a linker Nullteiler; also existiert wenigstens ein $b \neq o$ mit $ab = o$. Gäbe es nun ein Linksinverses a_L^{-1}, so folgte durch Multiplikation dieser Gleichung mit a_L^{-1} von links doch gerade $b = o$ im Widerspruch zur Voraussetzung $b \neq o$. Für rechte Nullteiler verläuft der Beweis entsprechend. qed.

Die Vereinfachungen, die sich bei allen Überlegungen daraus ergeben, daß im kommutativen Fall die Unterscheidung von linken und rechten Nullteilern entfällt, verstehen sich von selbst.

Die letzten Sätze sind auch aus dem Grunde bemerkenswert, als sie gewisse allgemeine Aussagen über die Division in beliebigen Ringen darstellen. Die Division ist ja die einzige der sogenannten vier Grundrechenoperationen, deren Ausführbarkeit bzw. Eindeutigkeit im Falle der Ausführbarkeit nicht aus den Ringaxiomen folgt. Die Vielfalt der hier vorhandenen Möglichkeiten, die wir bereits bei der Untersuchung von Halbgruppen diskutierten, unterscheidet die verschiedenen als Ringe bezeichneten algebraischen Strukturen wesentlich voneinander. So haben wir z. B. die Ringe, in denen die Division im Falle der Ausführbarkeit eindeutig ist (*M III**), als die nullteilerfreien Ringe erkannt, während bereits in D(25.1) die Schiefkörper bzw. kommutativen Körper durch die Ausführbarkeit der Division (*M III*) ausgezeichnet sind.

Dabei stellen wir ausdrücklich fest, daß in *M III* bzw. *M III** die Einschränkung $a \neq o$ notwendig ist. Aus $a \cdot x = b$ bzw. $y \cdot a = b$ mit $a = o$ folgt nämlich nach S(25.3) stets $b = o$, so daß also *M III* im Falle $a = o$ für alle $b \neq o$ unerfüllbar ist. Ferner löst jedes Ringelement x bzw. y die Gleichungen $a \cdot x = b$ bzw. $y \cdot a = b$ mit $a = b = o$, d. h., auch die Eindeutigkeitsaussage *M III** ist mit $a = o$ in keinem Ringe gültig.

Wir werden sehen, daß auch in Ringen aus der uneingeschränkten Ausführbarkeit der Division (*M III*) die Eindeutigkeit der Division (*M III**) folgt. Damit sind die Schiefkörper bzw. kommutativen Körper diejenigen Ringe, in denen hinsichtlich der Division soviel wie überhaupt nur möglich gefordert ist. Man kann also die Gruppeneigenschaft bezüglich der zweiten Verknüpfung, der Multiplikation, nur für die Menge der vom Nullelement verschiedenen

Elemente erreichen. Diese Menge ist auch stets gemeint, wenn man von der *multiplikativen Gruppe eines Körpers* spricht, während einschließlich des Nullelementes immer nur eine — nicht einmal reguläre — multiplikative Halbgruppe vorliegt.

Es verbleibt uns daher abschließend festzustellen, was sich über die für alle Ringe gültigen Aussagen hinaus an besonderen Eigenschaften bzw. Vereinfachungen für Körper ergibt.

Satz **S (25.10)**

In jedem Schiefkörper bzw. kommutativen Körper existiert ein eindeutig bestimmtes Einselement und zu jedem von o verschiedenen Element ein eindeutig bestimmtes Inverses.

Beweis

Für die multiplikative Gruppe des Körpers (also für die Menge der vom Nullelement o verschiedenen Elemente) existiert ein eindeutig bestimmtes Einselement e nach S(1.4). Dieses Element e ist aber auch Einselement für den Körper, denn die einzige noch fehlende Relation

$$e \cdot o = o \cdot e = o$$

ergibt sich unmittelbar aus S(25.3).

Die zweite Behauptung betrifft nur Elemente der multiplikativen Gruppe des Körpers und ist daher mit S(1.5) bereits bewiesen.

qed.

Satz **S (25.11)**

In einem Schiefkörper bzw. kommutativen Körper ist die Division durch vom Nullelement o verschiedene Elemente eindeutig, d. h., es gilt M III[1]).

Dieser Satz ergibt sich nach S(25.7) aus dem

Satz **S (25.12)**

Ein Schiefkörper bzw. kommutativer Körper ist nullteilerfrei.

---

1) Man beachte, daß in *M III** (Formulierung wie in S(25.7)) $b = o$ sein kann, und damit S(25.11) mehr als der sich nur auf die multiplikative Gruppe des Körpers beziehende Satz S(1.8) aussagt.

Beweis

Auftretende linke bzw. rechte Nullteiler $a \neq o$ würden nach S(25.9) kein Linksinverses bzw. Rechtsinverses besitzen im Widerspruch zu S(25.10).

qed.

Kommutative Körper sind also insbesondere Integritätsbereiche; im endlichen Falle gilt die Umkehrung (vgl. Aufg. 4).

Für den Nachweis der Körpereigenschaft eines Ringes ist die Feststellung nützlich, daß ein Ring bereits dann Körper ist, wenn die vom Nullelement verschiedenen Elemente eine multiplikative Gruppe bilden. Daraus folgt nämlich, daß *M III* für alle $b \neq o$ erfüllt ist, während die *M III* für $b = o$ entsprechenden Gleichungen $ax = o$ und $ya = o$ mit $x = y = o$ in jedem Ring lösbar sind.

Damit ergibt sich nach S(1.9) die Möglichkeit, in D(25.1) unter Beibehaltung aller übrigen Axiome *M III* durch $M\,III_1$ (Existenz eines Linkseinselementes) und $M\,III_2$ (Existenz eines Linksinversen zu jedem von o verschiedenen Element) zu ersetzen. Insbesondere sind nach S(1.10) bzw. F(24.7) im endlichen Falle *M III* und *M III** gleichwertig.

Aufgaben zu § 25

1. Man beweise die in F(25.2) ausgesprochene Verallgemeinerung des Distributivgesetzes.
2. In jedem Ring bilden bezüglich der Multiplikation die Nichtnullteiler eine reguläre Halbgruppe.
3. Man zeige S(25.12) direkt ohne Berufung auf S(25.9).
4. Jeder endliche Integritätsbereich ist ein (kommutativer) Körper.

§ 26. Beispiele von Ringen und Körpern

Zahlen **B(26.1)**

a) Die natürlichen Zahlen bilden keinen Ring.

b) *Die Menge der ganzen Zahlen ist ein kommutativer Ring*, den wir fortan mit Γ bezeichnen. Er besitzt ein eindeutig bestimmtes Einselement und ist nullteilerfrei.

c) *Die Menge der rationalen Zahlen ist ein kommutativer Körper.* Für ihn ist im allgemeinen die Bezeichnung P (lies Rho) gebräuchlich. Desgleichen bilden die *reellen Zahlen* sowie die *komplexen Zahlen* jeweils einen kommutativen Körper. Wir bezeichnen diese Körper im folgenden mit Δ bzw. Z (lies Zeta).

Matrizen **B (26.2)**

a) *Die Matrizen vom Typ* (n, n) *mit reellen Zahlen als Matrizenelementen bilden einen Schiefring, den sogenannten vollen Matrizenring* $\mathfrak{M}_n(\Delta)$. Er ist nichtkommutativ und besitzt Nullteiler; die Einheitsmatrix ist eindeutig bestimmtes Einselement.

Beweis

Die Axiome *A I* – *A IV* wurden bereits in B (2.4 b) nachgewiesen. Ebenso entnehmen wir dem Beweis von B (2.4 c) die Gültigkeit von *M I* und *M II* für beliebige Matrizen vom Typ (n, n); für das Nichterfülltsein von *M IV* vgl. etwa Aufg. 4 in § 2. Es bleiben also nur die Relationen

$$A \cdot [B + C] = A \cdot B + A \cdot C$$
$$[B + C] \cdot A = B \cdot A + C \cdot A$$

des distributiven Gesetzes zu zeigen, was wir für die erste durchführen:

$$\begin{aligned}(a_{ik})\,[(b_{ik}) + (c_{ik})] &= (a_{ik})\,[(b_{ik} + c_{ik})] \\ &= \Big(\sum_h a_{ih}(b_{hk} + c_{hk})\Big) \\ &= \Big(\sum_h (a_{ih}b_{hk} + a_{ih}c_{hk})\Big) \\ &= \Big(\sum_h a_{ih}b_{hk} + \sum_h a_{ih}c_{hk}\Big) \\ &= \Big(\sum_h a_{ih}b_{hk}\Big) + \Big(\sum_h a_{ih}c_{hk}\Big) \\ &= (a_{ik})\,(b_{ik}) + (a_{ik})\,(c_{ik}).\end{aligned}$$

Nullteiler sind z. B. für $n = 2$ (vgl. auch Aufg. 1) mit beliebigem $a \neq 0$:

$$\begin{pmatrix}0 & a\\ 0 & 0\end{pmatrix} \text{ und } \begin{pmatrix}a & 0\\ 0 & 0\end{pmatrix} \text{ mit } \begin{pmatrix}0 & a\\ 0 & 0\end{pmatrix}\begin{pmatrix}a & 0\\ 0 & 0\end{pmatrix} = \begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}.$$

qed.

b) Von den verschiedenen Möglichkeiten, Untersysteme des vollen Matrizenringes $\mathfrak{M}_n(\Delta)$ als Ringe auszuwählen, wollen wir hier nur für $n = 2$ die Menge der Matrizen

$$\begin{pmatrix} a_{11} & a_{12} \\ 0 & 0 \end{pmatrix}$$

erwähnen. Diese bildet offensichtlich einen nichtkommutativen Ring, der nach B(2.4) unendlich viele Linkseinselemente, dagegen kein Rechtseinselement enthält.

c) Die Überlegungen können dahingehend ausgedehnt werden, daß man die Matrizenelemente einem beliebigen Schiefring $\mathfrak{R}$ entnimmt. Man überzeugt sich nämlich leicht davon, daß in sämtliche Beweise unter a) von den Eigenschaften der reellen Zahlen nur die Gültigkeit der Schiefringaxiome eingeht. Wir bezeichnen allgemein den Ring aller Matrizen vom Typ (n, n) mit Elementen aus $\mathfrak{R}$ mit $\mathfrak{M}_n(\mathfrak{R})$.

Restklassen ganzer Zahlen **B (26.3)**

a) *Die Restklassen* $[a]$ *mod* m *bilden einen kommutativen Ring* von m Elementen; die Restklasse $[1]$ mod m ist eindeutig bestimmtes Einselement. Aus unseren bisherigen Überlegungen ergibt sich, daß die Kongruenzrechnung mod m der elementaren Zahlentheorie dem repräsentantenweisen Rechnen im Restklassenring mod m entspricht.

Beweis

Die Moduleigenschaft wurde bereits in B(2.8b) gezeigt, desgleichen die Gültigkeit von *M I*, *M II* und *M IV* in B(2.8e). Die Distributivität überträgt sich aus Γ auf das Rechnen mit Restklassen.

qed.

b) Ist m keine Primzahl, so existieren im Restklassenring mod m Nullteiler. Zerlegt man nämlich $m = m_1 \cdot m_2$ mit $1 < m_1 < m$ und $1 < m_2 < m$, so ist mod m:

$$[m_1] \neq [0], [m_2] \neq [0] \text{ und } [m_1] \cdot [m_2] = [m] = [0].$$

c) *Ist* $m = p$ *eine Primzahl, so ist der Restklassenring mod* m *ein Körper.* Wir haben nämlich bereits in B(2.8e) nachgewiesen, daß genau für den Fall $m = p$ alle von $[0]$ verschiedenen Restklassen mod m prim sind und damit eine Gruppe bilden.

Spezielle Ringe aus komplexen Zahlen **B (26.4)**

a) *Die Gesamtheit aller Zahlen* $a + b\sqrt{k}$ *mit beliebigen ganzen Zahlen* a *und* b *bildet für jedes feste ganzzahlige* k *einen kommutativen Ring.* Offensichtlich erhalten wir mit einer Quadratzahl k (und erst recht mit $k = 0$) wieder alle ganzen Zahlen, was im folgenden als trivial ausgeschlossen sei.

Beweis

Die Gültigkeit von *A II*, *A IV*, *M II*, *M IV* und *D* ist für komplexe Zahlen selbstverständlich. Aus

$$(a_1 + b_1\sqrt{k}) \pm (a_2 + b_2\sqrt{k}) = (a_1 \pm a_2) + (b_1 \pm b_2)\sqrt{k}$$

folgen *A I* und *A III*. Entsprechend ergibt sich *M I* aus

$$(a_1 + b_1\sqrt{k}) \cdot (a_2 + b_2\sqrt{k}) = (a_1a_2 + b_1b_2k) + (a_1a_2 + a_2b_1)\sqrt{k}.$$

qed.

Nullelement und Einselement stimmen mit den entsprechenden Elementen aus Γ überein; der Ring ist nullteilerfrei. Für $k > 0$ sind alle Ringelemente reell, während für $k < 0$ auch nichtreelle komplexe Zahlen auftreten. Insbesondere nennt man den Ring der Elemente $a + b\sqrt{-1} = a + bi$ den *Ring der ganzen Gaußschen Zahlen.*

Die gleichen Überlegungen gelten, wenn man etwa a und b rationalzahlig mit rationalem (nicht quadratischem) $k \neq 0$ wählt. Die so entstehenden Ringe sind sogar Körper, da man ja zu jedem von Null verschiedenen Element $a + b\sqrt{k}$ ein Inverses angeben kann:

$$(a + b\sqrt{k})^{-1} = \frac{a - b\sqrt{k}}{a^2 - b^2k} = \frac{a}{a^2 - b^2k} - \frac{b}{a^2 - b^2k}\sqrt{k}.$$

Da k nach Voraussetzung nicht quadratisch ist, folgt aus $a + b\sqrt{k} \neq 0$ stets $a^2 - b^2k \neq 0$. Für den Körper der Elemente $a + b\sqrt{-1} = a + bi$ ist auch die Bezeichnung *Gaußscher Zahlkörper* gebräuchlich.

b) *Die Gesamtheit aller Zahlen* $\frac{a}{b^n}$ *mit beliebigen ganzen Zahlen* a *und beliebigen ganzzahligen Potenzen einer festen ganzen Zahl* $b \neq 0$ *bildet einen kommutativen Ring.*

Beweis

Entsprechend den Ausführungen unter a) begnügen wir uns mit dem Nachweis von *A I*, *A III* und *M I*:

$$\frac{a_1}{b^{n_1}} \pm \frac{a_2}{b^{n_2}} = \frac{a_1 b^{n_2} \pm a_2 b^{n_1}}{b^{n_1+n_2}}$$

$$\frac{a_1}{b^{n_1}} \cdot \frac{a_2}{b^{n_2}} = \frac{a_1 a_2}{b^{n_1+n_2}}$$

qed.

Endomorphismenring eines Moduls[1] **B (26.5)**

Es sei $\mathfrak{G}$ ein Modul und $\mathfrak{R}$ die Menge aller Endomorphismen σ_1, σ_2, σ_3, ... von $\mathfrak{G}$ (vgl. D(18.5)). Durch Erklärung zweier geeigneter Verknüpfungen der Endomorphismen wird $\mathfrak{R}$ zu einem (im allgemeinen nichtkommutativen) Ring, dem sogenannten Endomorphismenring von $\mathfrak{G}$. Dabei liegt es nahe, für die Multiplikation zweier Endomorphismen wie bei Automorphismen die Nacheinanderausführung zu wählen. Für die Erklärung der Addition haben wir zunächst kein entsprechendes Vorbild; es erweist sich als zweckmäßig, die Summe zweier Endomorphismen mit Hilfe der Summe der durch sie gelieferten Bilder festzulegen.

Die Anwendung eines Endomorphismus $\sigma \in \mathfrak{R}$ auf ein Element $a \in \mathfrak{G}$ bezeichnen wir in Exponentenschreibweise:

$$a \to \sigma(a) = a^{\sigma}.$$

Damit erhalten wir die eben erläuterten Verknüpfungen als

$$\left.\begin{aligned} a^{[\sigma_1+\sigma_2]} &= a^{\sigma_1} + a^{\sigma_2} \\ a^{[\sigma_1 \cdot \sigma_2]} &= (a^{\sigma_1})^{\sigma_2} \end{aligned}\right\} \quad \text{für alle } a \in \mathfrak{G}.$$

Ehe wir nachweisen, daß die Menge der Endomorphismen mit den so erklärten Verknüpfungen in der Tat einen Ring bildet, behandeln wir ein

Konkretes Beispiel eines Endomorphismenringes

Wir betrachten als Modul $\mathfrak{G}$ den Restklassenmodul ganzer Zahlen modulo 4:

$$\mathfrak{G} = \{[0], [1], [2], [3]\}.$$

1) B(26.5) macht den Leser mit einer für die moderne Algebra prinzipiell wichtigen Begriffsbildung bekannt, hat aber weniger den Charakter eines erläuternden Beispieles; beim ersten Studium kann es daher übergangen werden.

Es gibt vier Endomorphismen, die durch die folgende Zuordnung gekennzeichnet sind:

	σ_0	σ_1	σ_2	σ_3
$[1] \to$	[0]	[1]	[2]	[3]
$[2] \to$	[0]	[2]	[0]	[2]
$[3] \to$	[0]	[3]	[2]	[1]
$[0] \to$	[0]	[0]	[0]	[0]

Wir wissen nämlich bereits (vgl. B(15.4)), daß es genau zwei Automorphismen gibt (σ_1 und σ_3). Darüber hinaus kommen als homomorphe Bilder entsprechend den möglichen Kernen $\mathfrak{G}$ bzw. $\{[0], [2]\}$ eines Homomorphismus nur der Nullmodul bzw. ein zyklischer Modul der Ordnung 2 in Frage, die tatsächlich genau einmal in $\mathfrak{G}$ vorhanden sind. Das liefert die Endomorphismen σ_0 und σ_2.

Als Beispiel für die Addition und Multiplikation von Endomorphismen berechnen wir:

$$[1]^{[\sigma_2+\sigma_3]} = [1]^{\sigma_2} + [1]^{\sigma_3} = [2] + [3] = [1]$$
$$[2]^{[\sigma_2+\sigma_3]} = [2]^{\sigma_2} + [2]^{\sigma_3} = [0] + [2] = [2]$$
$$\cdots\cdots\cdots\cdots\cdots\cdots$$

Also ergibt sich $\sigma_2 + \sigma_3 = \sigma_1$.

$$[1]^{[\sigma_2 \cdot \sigma_3]} = ([1]^{\sigma_2})^{\sigma_3} = [2]^{\sigma_3} = [2]$$
$$[2]^{[\sigma_2 \cdot \sigma_3]} = ([2]^{\sigma_2})^{\sigma_3} = [0]^{\sigma_3} = [0]$$
$$\cdots\cdots\cdots\cdots\cdots$$

Also ergibt sich $\sigma_2 \cdot \sigma_3 = \sigma_2$.

Insgesamt erhält man folgende Strukturtafeln:

$+$	σ_0	σ_1	σ_2	σ_3
σ_0	σ_0	σ_1	σ_2	σ_3
σ_1	σ_1	σ_2	σ_3	σ_0
σ_2	σ_2	σ_3	σ_0	σ_1
σ_3	σ_3	σ_0	σ_1	σ_2

$\cdot$	σ_0	σ_1	σ_2	σ_3
σ_0	σ_0	σ_0	σ_0	σ_0
σ_1	σ_0	σ_1	σ_2	σ_3
σ_2	σ_0	σ_2	σ_0	σ_2
σ_3	σ_0	σ_3	σ_2	σ_1

Vergleicht man sie mit den Strukturtafeln des Restklassenringes von Γ modulo 4 (siehe Aufg. 3), so erkennt man, daß bis auf die Bezeichnung der Elemente die gleiche Struktur vorliegt (siehe auch Aufg. 5 von § 29).

Allgemeiner Beweis der Ringeigenschaft

A I: Die Summe $\sigma_1 + \sigma_2$ ist eine eindeutige Abbildung von $\mathfrak{G}$ in $\mathfrak{G}$, da sie nach Definition jedem Element $a \in \mathfrak{G}$ eindeutig das Element $a^{\sigma_1} + a^{\sigma_2} \in \mathfrak{G}$ zuordnet. Diese Abbildung ist relationstreu für alle $a \in \mathfrak{G}$ und $b \in \mathfrak{G}$ wegen

$$(a+b)^{[\sigma_1+\sigma_2]} = (a+b)^{\sigma_1} + (a+b)^{\sigma_2} = a^{\sigma_1} + b^{\sigma_1} + a^{\sigma_2} + b^{\sigma_2}$$
$$= a^{[\sigma_1+\sigma_2]} + b^{[\sigma_1+\sigma_2]},$$

ist also wieder ein Endomorphismus von $\mathfrak{G}$.

A II: $$a^{[\sigma_1+(\sigma_2+\sigma_3)]} = a^{\sigma_1} + a^{(\sigma_2+\sigma_3)} = a^{\sigma_1} + (a^{\sigma_2} + a^{\sigma_3})$$
$$= (a^{\sigma_1} + a^{\sigma_2}) + a^{\sigma_3} = a^{(\sigma_1+\sigma_2)} + a^{\sigma_3}$$
$$= a^{[(\sigma_1+\sigma_2)+\sigma_3]}.$$

A III$_1$: Nullelement von $\mathfrak{R}$ ist derjenige Endomorphismus σ_0, der alle $a \in \mathfrak{G}$ auf das Nullelement $o \in \mathfrak{G}$ abbildet. Aus $a^{\sigma_0} = o$ folgt nämlich

$$a^{[\sigma+\sigma_0]} = a^{\sigma} + a^{\sigma_0} = a^{\sigma} + o = a^{\sigma}.$$

A III$_2$: Zu jedem Endomorphismus $\sigma \in \mathfrak{R}$ ist durch die folgende Zuordnung ein entgegengesetzter Endomorphismus $(-\sigma)$ erklärt:

$$a^{-\sigma} = -(a^{\sigma}) \text{ für alle } a \in \mathfrak{G}.$$

Diese Zuordnung ist eindeutig und vermittelt wegen

$$(a+b)^{-\sigma} = -((a+b)^{\sigma}) = -(a^{\sigma} + b^{\sigma}) = -(a^{\sigma}) + (-(b^{\sigma}))$$
$$= a^{-\sigma} + b^{-\sigma}$$

eine relationstreue Abbildung. Dabei gilt $\sigma + (-\sigma) = \sigma_0$, da

$$a^{[\sigma+(-\sigma)]} = a^{\sigma} + (-(a^{\sigma})) = o = a^{\sigma_0}$$

für alle $a \in \mathfrak{G}$ erfüllt ist.

A IV: $a^{[\sigma_1+\sigma_2]} = a^{\sigma_1} + a^{\sigma_2} = a^{\sigma_2} + a^{\sigma_1} = a^{[\sigma_2+\sigma_1]}$.

M I: Das Produkt $\sigma_1 \cdot \sigma_2$ ist eine eindeutige Abbildung von $\mathfrak{G}$ in $\mathfrak{G}$, da es nach Definition jedem Element $a \in \mathfrak{G}$ eindeutig das Element $(a^{\sigma_1})^{\sigma_2}$ zuordnet. Diese Abbildung ist ebenfalls relationstreu:

$$(a+b)^{[\sigma_1\cdot\sigma_2]} = ((a+b)^{\sigma_1})^{\sigma_2} = (a^{\sigma_1} + b^{\sigma_1})^{\sigma_2} = (a^{\sigma_1})^{\sigma_2} + (b^{\sigma_1})^{\sigma_2}$$
$$= a^{[\sigma_1\cdot\sigma_2]} + b^{[\sigma_1\cdot\sigma_2]}.$$

M II: $a^{[\sigma_1(\sigma_2\cdot\sigma_3)]} = ((a^{\sigma_1})^{\sigma_2})^{\sigma_3} = a^{[(\sigma_1\cdot\sigma_2)\sigma_3]}$.

D: $a^{[\sigma_1(\sigma_2+\sigma_3)]} = (a^{\sigma_1})^{(\sigma_2+\sigma_3)} = (a^{\sigma_1})^{\sigma_2} + (a^{\sigma_1})^{\sigma_3}$

$= a^{\sigma_1\sigma_2} + a^{\sigma_1\sigma_3} = a^{[\sigma_1\sigma_2+\sigma_1\sigma_2]}$.

Entsprechend beweist man die zweite Relation von *D*.

qed.

Entartete Ringe **B (26.6)**

Man kann aus jedem Modul $\mathfrak{G}$ in trivialer Weise einen Ring herstellen, indem man eine Multiplikation so definiert, daß alle Produkte gleich dem Nullelement o des Moduls gesetzt werden. $\mathfrak{G}$ erfüllt dann offensichtlich auch *M I*, ***M II*** und *D*, ist also ein Ring. Er besteht nach Konstruktion nur aus Nullteilern; diese Feststellung ist jedoch nicht etwa zureichend, den eigentlichen Sachverhalt zu kennzeichnen. Nur aus Nullteilern besteht nämlich ein Ring $\mathfrak{R}$ schon dann, wenn es zu jedem Element $a \in \mathfrak{R}$ wenigstens ein Element $b \neq o$ aus $\mathfrak{R}$ gibt mit $ab = o$, während hier jedes Element $b \in \mathfrak{R}$ diese Eigenschaft hat.

Selbstverständlich sind solche entarteten Ringe für sich völlig uninteressant; man muß sie jedoch bei manchen allgemeinen Aussagen über Ringe als Grenzfälle mit in Betracht ziehen.

Aufgaben zu § 26

1. Der in B(26.2) behandelte volle Matrizenring $\mathfrak{M}_n(\Delta)$ ist ein handliches Beispiel eines nichtkommutativen Ringes mit Nullteilern. Man veranschauliche sich an ihm den Inhalt von S(25.8) und S(25.9). Darüber hinaus zeige man folgende Besonderheiten des Matrizenringes:

   a) Jeder linke Nullteiler ist auch ein rechter Nullteiler und umgekehrt.
   b) Jedes Linksinverse ist zugleich Rechtsinverses und umgekehrt.
   c) Ein Element (a_{ik}) des Matrizenringes ist entweder Nullteiler oder besitzt ein Inverses.

   Der Beweis dieser drei Eigenschaften gestaltet sich am übersichtlichsten, indem man zeigt, daß für linke wie rechte Nullteiler das Verschwinden der Determinante $|a_{ik}|$ und für die Existenz von Links- wie Rechtsinversen das Nichtverschwinden dieser Determinante notwendig und hinreichend ist.

2. Unter Verwendung der sich aus der Kommutativität ergebenden Vereinfachungen stelle man die entsprechenden Betrachtungen für die in B(26.3b) genannten Restklassenringe an.

3. Man stelle die Strukturtafeln bezüglich beider Verknüpfungen für die Restklassenringe mod m mit $m = 2, 3, 4, 5, 6$ auf.
4. Man konstruiere einen Körper mit drei Elementen durch Angabe seiner Strukturtafeln und vergleiche diese mit den Strukturtafeln des Restklassenringes mod 3.
5. Entsprechend konstruiere man einen Körper mit vier Elementen.
6. Die Automorphismengruppe Φ eines Moduls $\mathfrak{G}$ ist in der multiplikativen Halbgruppe des Endomorphismenringes $\mathfrak{R}$ von $\mathfrak{G}$ enthalten. Φ besteht aus genau denjenigen Endomorphismen, die in $\mathfrak{R}$ ein (zweiseitiges) Inverses besitzen.
7. Es sei $\mathfrak{G}$ ein einfacher Modul, der also nur die beiden trivialen Untermoduln besitzt. Dann ist der Endomorphismenring $\mathfrak{R}$ von $\mathfrak{G}$ ein kommutativer Körper.

§ 27. Potenzen und Vielfache von Ringelementen

In einem beliebigen Ring $\mathfrak{R}$ läßt sich bezüglich der multiplikativen Verknüpfung für jedes $a \in \mathfrak{R}$ entsprechend D(3.1) die n-te Potenz a^n für alle natürlichen Exponenten $n \geqq 2$ erklären. Dafür gelten die in F(3.2) formulierten Potenzgesetze

$$I: \; a^n a^m = a^{n+m},$$

$$II: \; (a^n)^m = a^{n \cdot m},$$

$$III: \; (ab)^n = a^n b^n \text{ für } ab = ba;$$

denn diese Gesetze beruhen allein auf der Gültigkeit von *M I* und *M II*, wie wir bereits im § 3 bemerkten. Offensichtlich bleiben sie auch bei der ergänzenden Festlegung von $a^1 = a$ erhalten.

Die weiteren Aussagen aus § 3 lassen sich nur bei zusätzlichen Voraussetzungen über den Ring $\mathfrak{R}$ bzw. über einzelne seiner Elemente übertragen. So ist, falls $\mathfrak{R}$ ein (eindeutig bestimmtes) Einselement e enthält, $a^0 = e$ für alle $a \neq o$ aus $\mathfrak{R}$ und $a^{-n} = (a^{-1})^n$ für diejenigen $a \in \mathfrak{R}$ erklärbar, die ein (eindeutig bestimmtes) Inverses $a^{-1} \in \mathfrak{R}$ besitzen. Die genannten Potenzgesetze gelten dann auch für diese Erweiterungen des Potenzbegriffes in $\mathfrak{R}$[1]). Ist $\mathfrak{R}$ sogar ein Körper, so sind die Voraussetzungen des letzten Absatzes für alle $a \neq o$ aus $\mathfrak{R}$ erfüllt.

---

1) Alle bisherigen Aussagen beziehen sich nur auf die multiplikative Halbgruppe von $\mathfrak{R}$ und können also auch schon für die in § 24 behandelten Halbgruppen ausgesprochen werden.

Entsprechend läßt sich bezüglich der additiven Verknüpfung für jedes $a \in \mathfrak{R}$ die Vielfachenbildung na wie in D(3.7) für $n \geqq 2$ erklären. Da $\mathfrak{R}$ hinsichtlich der Addition Modul ist, gelten alle im § 3 auf D(3.7) folgenden Überlegungen:

D(3.9) und F(3.10):
$$1a = a$$
$$0a = o$$
$$(-n)a = -(na) = n(-a);$$

F(3.8) und S(3.11):
$$na + ma = (n + m)a$$
$$m(na) = (m \cdot n)a$$
$$n(a + b) = na + nb.$$

Darüber hinaus läßt sich jedoch für Ringe neben der Vielfachenbildung $n(a + b)$ einer Summe auch die Vielfachenbildung $n(a \cdot b)$ eines Produktes umformen:

$$n(a \cdot b) = (na) \cdot b = a \cdot (nb).$$

Beweis

Für $n = 0$ ist diese Relation trivial. Ist $n > 0$, so gilt

$$n(ab) = \underbrace{ab + ab + \cdots + ab}_{n} = \underbrace{(a + a + \cdots + a)}_{n} b = (na)b$$
$$= a\underbrace{(b + b + \cdots + b)}_{n} = a(nb).$$

Im Falle $n < 0$, also $n = -s$ mit $s > 0$, ergibt sich:

$$n(ab) = (-s)(ab) = s(-ab)$$

und daraus einerseits

$$s((-a)b) = (s(-a))b = ((-s)a)b = (na)b$$

und andererseits

$$s(a(-b)) = a(s(-b)) = a((-s)b) = a(nb).$$

qed.

Damit haben wir die uns bereits bekannte „Operatoranwendung" des Ringes Γ der ganzen Zahlen auf einen beliebigen Modul ausgedehnt zu einer Operatoranwendung dieses Ringes auf einen beliebigen Ring $\mathfrak{R}$. Wir betonen nochmals, daß diese Operatoranwendung von Γ auf $\mathfrak{R}$ nicht mit der multiplikativen Verknüpfung in $\mathfrak{R}$ verwechselt werden darf. Auf eine ständige Unterscheidung der Bezeichnung haben wir jedoch schon im obigen Beweis verzichtet.

Nur im Falle, daß $\mathfrak{R}$ mit Γ übereinstimmt bzw. Γ enthält, fällt die Operatoranwendung mit der Ringmultiplikation zusammen.

Die letzte Relation der soeben zusammengestellten Regeln der Operatoranwendung von Γ auf einen Ring $\mathfrak{R}$ gibt an, wie die mit Hilfe der additiven Verknüpfung erklärte Vielfachenbildung auf ein Produkt wirkt. Die umgekehrte Fragestellung, wie nämlich die mit Hilfe der multiplikativen Verknüpfung erklärte Potenzbildung einer Summe vorzunehmen ist, beantwortet für positive Exponenten n der bekannte *binomische Lehrsatz*, der in beliebigen Ringen für kommutativ multiplizierbare Elemente a und b gilt:

$$(a+b)^n = \binom{n}{0} b^n + \binom{n}{1} a^1 b^{n-1} + \cdots + \binom{n}{n-1} a^{n-1} b^1 + \binom{n}{n} a^n$$
$$= \sum_{\nu=0}^{n} \binom{n}{\nu} a^\nu b^{n-\nu} \text{ [1)]}.$$

Durch die bekannte Umschreibung der Binomialkoeffizienten in

$$(a+b)^n = \sum_{\nu=0}^{n} \frac{n!}{\nu!\,(n-\nu)!}\, a^\nu b^{n-\nu} = \sum_{\nu+\mu=n} \frac{n!}{\nu!\,\mu!}\, a^\nu b^\mu$$

erleichtert man die Verallgemeinerung zum *polynomischen Lehrsatz*, die der viel einfacheren Ausdehnung der anderen Regeln der Potenz- und Vielfachenrechnung auf mehr als zwei Glieder entspricht:

$$(a+b+\cdots+c)^n = \sum_{\nu+\mu+\cdots+\lambda=n} \frac{n!}{\nu!\,\mu!\ldots\lambda!}\, a^\nu b^\mu \ldots c^\lambda.$$

Es gilt ebenfalls in beliebigen Ringen unter Voraussetzung der Vertauschbarkeit aller auftretenden Ringelemente $a, b, \ldots, c$ bei der Multiplikation. Auf den Beweis können wir hier verzichten, da die Operatoranwendung der als Binomial- bzw. Polynomialkoeffizienten auftretenden natürlichen Zahlen auf die (vertauschbar vorausgesetzten) Ringelemente formal ebenso verläuft, als ob alle Ausdrücke gewöhnliche Zahlen wären. Der Beweis läßt sich also ohne weiteres aus der Zahlenrechnung übertragen (vgl. etwa v. MANGOLDT-KNOPP, Einf. in die höhere Mathem. Bd. I, 1. Abschnitt, Nr. 19 und 21).

Wir setzen nunmehr voraus, daß der Ring $\mathfrak{R}$ ein eindeutig bestimmtes Einselement e besitzt, und greifen die bereits in § 25 angedeutete

---

1) In dieser wie in den folgenden Summenformeln sind Faktoren mit dem Exponenten 0 wegzulassen. Diese Übereinkunft ist notwendig, da die Existenz eines Einselementes e mit $a^0 = b^0 = \cdots = e$ in beliebigen Ringen nicht gewährleistet ist.

Frage auf, wie sich dieses multiplikativ bestimmte Einselement bezüglich der additiven Verknüpfung verhält. Dazu betrachten wir die von $e \in \mathfrak{R}$ erzeugte additive zyklische Gruppe $\langle e \rangle$. Sie ist Untermodul des als Modul aufgefaßten Ringes und enthält genau alle ganzzahligen Vielfachen

$$ge \text{ von } e \text{ mit } g = 0, \pm 1, \pm 2, \ldots$$

Nach S(6.3), angewendet auf additive Gruppen, ergeben sich zwei Möglichkeiten:

a) Die Vielfachen von e sind alle voneinander verschieden; $\langle e \rangle$ besteht aus unendlich vielen Elementen.

b) Die Vielfachen von e sind nicht alle voneinander verschieden; $\langle e \rangle$ besteht aus genau n Elementen, wobei n als die kleinste natürliche Zahl mit $ne = o$ bestimmt ist.

Offensichtlich ist $e = 1$ aus dem Ring Γ der ganzen Zahlen ein Beispiel für a) und $e = [1]$ aus dem Restklassenring von Γ modulo n ein Beispiel für b).

Dieses verschiedene Verhalten verwenden wir zur Kennzeichnung der Ringe mit Einselement:

Definition **D (27.1)**

Es sei $\mathfrak{R}$ ein Ring mit Einselement e. Unter der Charakteristik von $\mathfrak{R}$ versteht man, falls

a) *$\langle e \rangle$ von unendlicher Ordnung ist, die Zahl* 0;

b) *$\langle e \rangle$ von endlicher Ordnung n ist, die Zahl n.*

Satz **S (27.2)**

Die Charakteristik eines nullteilerfreien Ringes (also erst recht eines kommutativen Körpers[1]*) ist entweder* 0 *oder eine Primzahl $n = p$.*

Beweis

Es ist zu zeigen, daß kein $n = n_1 \cdot n_2 \neq p$ als Charakteristik in Frage kommt. Dies ergibt sich aber unmittelbar, da dann $n_1 e$ und $n_2 e$ wegen (vgl. Aufg. 1)

$$n_1 e \cdot n_2 e = (n_1 \cdot n_2) e = ne = o$$

1) In der Literatur ist es teilweise üblich, die Charakteristik nur für kommutative Körper zu definieren; andererseits kann die Charakteristik sogar unabhängig vom Einselement und damit auch für Ringe ohne Einselement erklärt werden.

vom Nullelement verschiedene Nullteiler wären im Widerspruch zur Voraussetzung. qed.

Die übliche Zahlenrechnung ist (neben der kommutativen Multiplikation und der Nullteilerfreiheit) dadurch ausgezeichnet, daß sie sich in Ringen mit der Charakteristik 0 abspielt. In Ringen mit von von 0 verschiedener Charakteristik (also etwa in jedem Restklassenring von Γ modulo n) gelten einige besondere, zusätzliche Rechenregeln. Als Beispiele bringen wir:

Folgerung **F (27.3)**

Es sei n die Charakteristik des Ringes $\mathfrak{R}$. Dann ist nicht nur $ne = o$, sondern auch für jedes $a \in \mathfrak{R}$

$$ga = o$$

für alle ganzzahligen Vielfachen $g = g'n$ von n.

Beweis

Nach den Regeln der Vielfachenbildung gilt zunächst

$$ge = (g'n)e = g'(ne) = g'o = o,$$

und damit weiter

$$ga = g(ea) = (ge)a = oa = o.$$

qed.

Folgerung **F (27.4)**

Es sei $\mathfrak{R}$ ein Ring mit Primzahlcharakteristik p. Dann gilt für kommutativ multiplizierbare Elemente a und b aus $\mathfrak{R}$

$$(a+b)^p = a^p + b^p, \quad (a-b)^p = a^p - b^p$$

und allgemeiner für $n = 1, 2, 3, \ldots$

$$(a+b)^{p^n} = a^{p^n} + b^{p^n}, \quad (a-b)^{p^n} = a^{p^n} - b^{p^n}.$$

Beweis

Nach dem binomischen Lehrsatz ergibt sich zunächst

$$(a+b)^p = a^p + \binom{p}{1} a^{p-1}b + \cdots + \binom{p}{p-1} ab^{p-1} + b^p.$$

Da aber jeder Binomialkoeffizient $\binom{p}{i}$ mit $i = 1, \ldots, p-1$ wegen

$$\binom{p}{i} = \frac{p(p-1)\ldots(p-i+1)}{1 \cdot 2 \cdot \ldots \cdot i}$$

ein ganzzahliges Vielfaches von p ist[1]), verschwinden nach F (27.3) alle Summanden außer a^p und b^p.

Setzt man für b nachträglich $(-b)$, erhält man

$$(a - b)^p = a^p + (-1)^p b^p.$$

Für alle ungeraden Primzahlen ist aber $(-1)^p = -1$; für $p = 2$ folgt $(a - b)^2 = a^2 + b^2$ und weiter (vgl. Aufg. 4) $a^2 + b^2 = a^2 - b^2$.

Die Verallgemeinerung ergibt sich aus dem schon Bewiesenen unmittelbar durch vollständige Induktion.

qed.

Folgerung **F (27.5)**

Es sei $\mathfrak{R}$ ein Körper der Charakteristik p. Dann ist für ganzzahlige Vielfache eines beliebigen $a \neq o$ aus $\mathfrak{R}$

$$ha = ka \text{ genau für } h \equiv k \bmod p.$$

Beweis

Aus $ha = ka$ folgt $he = ke$ (Multiplikation mit a^{-1}) und umgekehrt. Nun ist e nach Voraussetzung primitives Element einer (additiven) zyklischen Gruppe der Ordnung p, so daß nach S (6.6) die Kongruenz $h \equiv k \bmod p$ für $he = ke$ und damit für $ha = ka$ notwendig und hinreichend ist.

qed.

Aufgaben zu § 27

1. Man beweise unter Verwendung der Regeln für die Vielfachenbildung, daß für beliebige ganze Zahlen n_1 und n_2 und das Einselement e eines Ringes gilt:
$$n_1 e \cdot n_2 e = (n_1 \cdot n_2) e.$$

2. Ist n eine positive ganze Zahl und existiert für ein Element $a \in \mathfrak{R}$ ein Element $c \in \mathfrak{R}$ mit $c^n = a$, so nennt man c eine n-te Wurzel aus a, wofür man auch schreibt:
$$c = \sqrt[n]{a} = a^{\frac{1}{n}}.$$
Darauf aufbauend verallgemeinere man den Potenzbegriff erneut unter Zulassung rationaler Exponenten und zeige, daß auch für solche Potenzen die Gesetze *I*, *II* und *III* gültig bleiben, wenn nur die entsprechenden Elemente in $\mathfrak{R}$ vorhanden sind.

---

1) Dieser Schluß beruht wesentlich auf der Primzahleigenschaft der Charakteristik p, da sich andernfalls Teiler der Charakteristik im Binomialkoeffizienten wegkürzen können.

Man beschreibe die inhaltliche Bedeutung dieser Regeln unter Berücksichtigung der Tatsache, daß es durchaus mehrere Elemente $c_1, c_2, \ldots$ in $\mathfrak{R}$ geben kann, für die $c_i^n = a$ gilt.

3. Welche Charakteristik hat der in § 26, Aufg. 5 konstruierte Körper aus vier Elementen?
4. In Ringen der Charakteristik 2 stimmt jedes Element mit seinem entgegengesetzten Element überein.
5. Man verallgemeinere F (27.4) für Potenzen von Summen mit mehr als zwei Summanden.
6. Mit Hilfe von Aufg. 5 beweise man erneut den kleinen FERMATschen Satz für die prime Restklassengruppe mod p.
7. Im Restklassenkörper mod p ist die p-te Wurzel jedes Elementes x eindeutig bestimmt und gleich x.

§ 28. Unterringe und Ideale

Im § 26 haben wir eine Reihe von Ringen bzw. Körpern aufgezählt, die in anderen Ringen bzw. Körpern enthalten sind. So umfaßt etwa der Körper der komplexen Zahlen den Körper der reellen Zahlen, dieser wiederum den Körper der rationalen Zahlen, letzterer schließlich den Ring der ganzen Zahlen. Auch die speziellen Ringe aus B (26.4a) sind im Körper der reellen bzw. komplexen Zahlen enthalten, die aus B (26.4b) im Körper der rationalen Zahlen. Nachdem wir schon in der Gruppentheorie die Fruchtbarkeit einer genaueren Untersuchung solcher Verhältnisse kennengelernt haben, kommen wir auch hier zu entsprechenden Begriffsbildungen:

Definition **D (28.1)**

Eine Untermenge $\mathfrak{S}$ eines Ringes bzw. Körpers $\mathfrak{R}$ heißt ein

a) *Unterring von $\mathfrak{R}$, wenn sie mit den in $\mathfrak{R}$ festgelegten Verknüpfungen für sich die Ringaxiome erfüllt;*

b) *Unterkörper von $\mathfrak{R}$, wenn sie mit den in $\mathfrak{R}$ festgelegten Verknüpfungen für sich die Körperaxiome erfüllt.*

Umgekehrt nennt man dann $\mathfrak{R}$ Oberring bzw. Oberkörper von $\mathfrak{S}$.

Jeder Unterkörper ist also erst recht Unterring. Da es sich bezüglich der Addition stets um Gruppen handelt, überträgt sich F (5.4); insbesondere ist das Nullelement des Ringes allen seinen Unter-

ringen als Nullelement gemeinsam. Damit enthält jeder Ring sich selbst und den nur aus dem Nullelement bestehenden Nullring als triviale Unterringe. Desgleichen enthält ein Körper sich selbst als trivialen Unterkörper, jedoch pflegt man den in ihm enthaltenen Nullring eben nur als Unterring, nicht als Unterkörper aufzufassen entsprechend der Fußnote zu D(25.1). Ferner ist wegen F(5.4) einem Körper und seinen Unterkörpern das Einselement und damit die Charakteristik gemeinsam, während bei Ringen eine solche Aussage im allgemeinen nicht möglich ist.

Satz **S (28.2)**

Es sei $\mathfrak{R}$ ein beliebiger Ring.

a) *Eine nichtleere Untermenge $\mathfrak{S} \leqq \mathfrak{R}$ ist dann und nur dann ein Unterring von $\mathfrak{R}$, wenn für beliebige Elemente $a \in \mathfrak{S}$ und $b \in \mathfrak{S}$ gilt*

$$(1) \quad a - b \in \mathfrak{S}$$

$$(2) \quad a \cdot b \in \mathfrak{S}.$$

b) *Ein Unterring $\mathfrak{S} \leqq \mathfrak{R}$ ist genau dann Unterkörper von $\mathfrak{R}$, wenn er wenigstens zwei Elemente enthält und für alle $b \neq o$ zusätzlich gilt*

$$(3) \quad b^{-1} \in \mathfrak{S}.$$

Beweis

Wir benutzen die bekannten Kriterien aus § 5.

a) Die Forderung (1) kennzeichnet $\mathfrak{S}$ als Untermodul. Nach (2) führt die Multiplikation aus $\mathfrak{S}$ nicht heraus, als Multiplikation innerhalb $\mathfrak{R}$ ist sie eindeutig; beides zusammen besagt *M I. M II* und *D* sind aber für alle Elemente aus $\mathfrak{R}$, also erst recht für die aus $\mathfrak{S}$ erfüllt.

b) Die Forderungen (2) und (3) kennzeichnen die Menge der von o verschiedenen Elemente aus $\mathfrak{S}$ als multiplikative Gruppe, also ist $\mathfrak{S}$ Körper. qed.

Man kann natürlich wieder die Forderungen (2) und (3) zu der Forderung

$$a \cdot b^{-1} \in \mathfrak{S}$$

zusammenfassen und entsprechend statt (1) auch

$$a + b \in \mathfrak{S} \quad \text{und} \quad -b \in \mathfrak{S}$$

nehmen.

Als Beispiel für die Anwendung unserer Kriterien zeigen wir zunächst, daß die Menge aller geraden Zahlen ein Unterring des Ringes Γ der ganzen Zahlen ist. Es sind nämlich Differenz und Produkt gerader Zahlen selbst wieder gerade Zahlen (vgl. auch Aufg. 1). Dieser Unterring der geraden Zahlen ist ein Ring, in dem im Gegensatz zu Γ kein Einselement existiert.

Weiterhin betrachten wir ein Beispiel für einen Unterring, der wohl ein eindeutig bestimmtes Einselement hat, das aber nicht mit dem Einselement des gesamten Ringes übereinstimmt. Wir wählen dazu im vollen Matrizenring $\mathfrak{M}_n(\Delta)$ aus B (26.2 a) die Untermenge $\mathfrak{S}$ aller Matrizen

$$\begin{pmatrix} a_{11} & a_{12} & 0 & \dots & 0 \\ a_{21} & a_{22} & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \dots & 0 \end{pmatrix}$$

mit beliebigen reellen Zahlen a_{11}, a_{12}, a_{21}, a_{22}. $\mathfrak{S}$ ist Unterring, denn Differenz und Produkt solcher Matrizen ergeben immer wieder Matrizen der gleichen Gestalt. Als Einselemente liegen vor:

in $\mathfrak{M}_n(\Gamma)$

$$\begin{pmatrix} 1 & & & & 0 \\ & 1 & & & \\ & & 1 & & \\ & & & \ddots & \\ 0 & & & & 1 \end{pmatrix},$$

in $\mathfrak{S}$

$$\begin{pmatrix} 1 & & & & 0 \\ & 1 & & & \\ & & 0 & & \\ & & & \ddots & \\ 0 & & & & 0 \end{pmatrix}.$$

Schließlich betrachten wir die Menge aller Diagonalmatrizen

$$\begin{pmatrix} a & & 0 \\ & \ddots & \\ 0 & & a \end{pmatrix}$$

mit beliebigen reellen a. Auch sie bildet einen Unterring von $\mathfrak{M}_n(\Delta)$, der sogar ein kommutativer Körper ist, denn (1), (2) und (3) sind offensichtlich erfüllt. Dieses Beispiel ist insofern lehrreich, als es zeigt, daß

a) ein Ring, der selber nicht Körper ist, einen Unterkörper enthalten kann;
b) ein nichtkommutativer Ring einen kommutativen Unterring enthalten kann;
c) ein Ring mit Nullteilern einen nullteilerfreien Ring enthalten kann.

Beispiele dafür, daß auch in einem Körper Unterringe vorhanden sein können, die selbst nicht Körper sind, haben wir bereits am Anfang des Paragraphen genannt. Es bestehen also die verschiedensten Möglichkeiten. Dagegen kann natürlich ein kommutativer Ring nur kommutative Unterringe und ein nullteilerfreier Ring nur nullteilerfreie Unterringe enthalten.

Satz **S (28.3)**

Der Durchschnitt $\mathfrak{S} \cap \mathfrak{T} \cap \ldots$ *von beliebig vielen Unterringen (bzw. Unterkörpern)* $\mathfrak{S}, \mathfrak{T}, \ldots$ *eines Ringes* $\mathfrak{R}$ *ist wieder Unterring (bzw. Unterkörper) von* $\mathfrak{R}$.

Beweis

Die Untermoduleigenschaft des Durchschnittes ist nach S(5.10) klar. Ist weiterhin $a \in \mathfrak{S} \cap \mathfrak{T} \cap \ldots$ und $b \in \mathfrak{S} \cap \mathfrak{T} \cap \ldots$, so ist $a \in \mathfrak{S}, a \in \mathfrak{T}, \ldots$ und $b \in \mathfrak{S}, b \in \mathfrak{T}, \ldots$, also $a \cdot b \in \mathfrak{S}, a \cdot b \in \mathfrak{T}, \ldots$ und daher $a \cdot b \in \mathfrak{S} \cap \mathfrak{T} \cap \ldots$. Nach S (28.2 a) ist damit für Unterringe die Behauptung bereits gezeigt.

Falls $\mathfrak{S}, \mathfrak{T}, \ldots$ sogar Körper sind, kann man von deren multiplikativen Gruppen nach S(5.10) wieder direkt auf die multiplikative Gruppe des Durchschnitts schließen. qed.

Bemerkung

Der entsprechende Satz gilt für die Vereinigungsbildung selbst für zwei Komponenten im allgemeinen nicht, da er bereits für Moduln nicht erfüllt ist.

Damit läßt sich der Nullring als Durchschnitt aller Unterringe eines Ringes $\mathfrak{R}$ erklären. In diesem Sinne ist er der kleinste in $\mathfrak{R}$ enthaltene Unterring. Entsprechend führt die Durchschnittsbildung aller Unterkörper eines Körpers $\mathfrak{R}$ zu einem eindeutig bestimmten kleinsten in $\mathfrak{R}$ enthaltenen Unterkörper. Er enthält wenigstens die Elemente o und e aus $\mathfrak{R}$.

Definition **D (28.4)**

Der als Durchschnitt aller Unterkörper eindeutig bestimmte kleinste Unterkörper eines Körpers $\mathfrak{R}$ *heißt der* Primkörper *von* $\mathfrak{R}$.

Allgemein verwendet man die Bezeichnung Primkörper für einen Körper, der keinen echten Unterkörper besitzt.

So ist z. B. der Körper P der rationalen Zahlen Primkörper und insbesondere etwa der Primkörper des Körpers Δ der reellen Zahlen. Eine nähere Kennzeichnung von Primkörpern nehmen wir in S(29.2) vor.

Nach diesen allgemeinen Aussagen über Unterringe wenden wir uns nun speziellen Unterringen zu, die in der Ring- und Körpertheorie in mehrfacher Hinsicht bedeutungsvoll sind:

Definition **D (28.5)**

Eine nichtleere Untermenge eines beliebigen Ringes $\mathfrak{R}$ *heißt*

a) *ein* Linksideal $\mathfrak{l}$ *von* $\mathfrak{R}$, *wenn für beliebige Elemente* $a \in \mathfrak{l}$, $b \in \mathfrak{l}$ *und* $r \in \mathfrak{R}$ *gilt*

$$(1) \quad a - b \in \mathfrak{l}, \qquad (2) \quad r \cdot a \in \mathfrak{l};$$

b) *ein* Rechtsideal $\mathfrak{r}$ *von* $\mathfrak{R}$, *wenn für beliebige Elemente* $a \in \mathfrak{r}$, $b \in \mathfrak{r}$ *und* $r \in \mathfrak{R}$ *gilt*

$$(1) \quad a - b \in \mathfrak{r}, \qquad (2) \quad a \cdot r \in \mathfrak{r};$$

c) *ein* zweiseitiges Ideal $\mathfrak{a}$ *von* $\mathfrak{R}$, *wenn* $\mathfrak{a}$ *sowohl Links- als auch Rechtsideal ist.*

Nach (1) ist jedes Linksideal $\mathfrak{l}$ in additiver Hinsicht Untermodul von $\mathfrak{R}$. In multiplikativer Hinsicht besagt (2), daß ein beliebiges Element des Linksideals mit einem beliebigen Ringelement von links multipliziert, immer wieder ein Element des Linksideals ergibt. Damit ist jedes Linksideal $\mathfrak{l}$ Unterring von $\mathfrak{R}$, denn wenn der linke Faktor sogar ein beliebiges Element aus $\mathfrak{R}$ sein darf, so doch erst recht ein Element aus $\mathfrak{l}$. Dagegen ist nicht notwendig jeder Unterring von $\mathfrak{R}$ Linksideal von $\mathfrak{R}$. Das liegt daran, daß im allgemeinen die Bedingung (2) aus D(28.5a) mehr fordert als die Bedingung (2) von S(28.2).

Das Entsprechende gilt für Rechtsideale von rechts und damit für zweiseitige Ideale von beiden Seiten. Selbstverständlich fallen in kommutativen Ringen alle drei Begriffe zusammen.

Jeder Ring $\mathfrak{R}$ enthält zwei triviale zweiseitige Ideale, nämlich die beiden trivialen Unterringe, die offensichtlich auch den Bedingungen (2) von D (28.5 a) und D (28.5 b) genügen. Dabei nennt man das nur aus dem Nullelement von $\mathfrak{R}$ bestehende Ideal *Nullideal* und den gesamten Ring $\mathfrak{R}$ aus später ersichtlichen Gründen *Einheitsideal.*

Ein nichttriviales Beispiel für ein Linksideal des vollen Matrizenringes $\mathfrak{M}_n(\Delta)$ ist die Menge aller Matrizen, deren Elemente bis auf die der k-ten Spalte alle Null sind:

$$\begin{pmatrix} 0 & \dots & 0 & a_{1k} & 0 & \dots & 0 \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & \dots & 0 & a_{nk} & 0 & \dots & 0 \end{pmatrix}.$$

Entsprechend ist die Menge aller Matrizen, deren Elemente bis auf die der i-ten Zeile alle verschwinden, ein Rechtsideal von $\mathfrak{M}_n(\Delta)$. Für ein Beispiel eines zweiseitigen Ideals eines Schiefringes vergleiche man Aufg. 3. Dagegen sind die bereits nach S (28.2) genannten Unterringe von $\mathfrak{M}_n(\Delta)$ weder Links- noch Rechtsideale von $\mathfrak{M}_n(\Delta)$. Ein einfaches Beispiel eines nichttrivialen Ideals in einem kommutativen Ring ist der Unterring der geraden Zahlen im Ring Γ der ganzen Zahlen.

Da wir den Idealbegriff insbesondere für Aussagen in kommutativen Ringen benötigen, beschränken wir uns bei der folgenden Beschreibung gewisser Ideale auf den kommutativen Fall.

Satz **S (28.6)**

Es sei $\mathfrak{R}$ ein kommutativer Ring und a ein fest gewähltes Element aus $\mathfrak{R}$. Dann ist die Menge aller Elemente $ra + ga$ mit beliebigen $r \in \mathfrak{R}$ und $g \in \Gamma$ ein Ideal von $\mathfrak{R}$, das von a erzeugte Ideal (a). Es ist das kleinste Ideal von $\mathfrak{R}$, welches a enthält.

Beweis

Diese Menge ist Ideal von $\mathfrak{R}$ wegen

(1) $$(ra + ga) - (r'a + g'a) = (r - r')a + (g - g')a$$
mit $r - r' \in \mathfrak{R}$ und $g - g' \in \Gamma$;

(2) $$r'(ra + ga) = r'ra + gr'a = (r'r + gr')a + 0a$$
mit $r'r + gr' \in \mathfrak{R}$ und $0 \in \Gamma$ [1]).

---

1) Nach der in § 27 abgeleiteten Regel für die Vielfachenbildung eines Produktes gilt nämlich $r'(ga) = (gr')a = g(r'a)$.

Weiterhin ist $a \in (a)$ wegen $a = oa + 1a$ mit $o \in \mathfrak{R}$ und $1 \in \Gamma$. Andererseits folgt für jedes Ideal $\mathfrak{a}$ von $\mathfrak{R}$ aus $a \in \mathfrak{a}$ auch $(a) \subseteq \mathfrak{a}$, denn mit a enthält $\mathfrak{a}$ nach D (28.5) alle Ringvielfachen von a (Eigenschaft (2)) und alle ganzzahligen Vielfachen von a (Eigenschaft (1)) und damit deren Summe. Also ist (a) tatsächlich das kleinste Ideal von $\mathfrak{R}$, welches a enthält. qed.

Wir bemerken, daß auch schon die Menge aller Produkte ra mit festem $a \in \mathfrak{R}$ und beliebigem $r \in \mathfrak{R}$ ein Ideal von $\mathfrak{R}$ bildet. Das Beispiel des Ringes $\mathfrak{R}$ der geraden Zahlen mit $a = 4$ zeigt jedoch, daß das Ideal aller Ringvielfachen von a (also im Beispiel die Menge der Elemente $0, \pm 8, \pm 16, \ldots$) das Element a selbst nicht zu enthalten braucht. Dagegen gilt:

Folgerung **F (28.7)**

Ist $\mathfrak{R}$ ein kommutativer Ring mit Einselement e, so besteht das von einem Ringelement a erzeugte Ideal (a) bereits aus allen Ringvielfachen ra.

Beweis

Nach S (28.6) genügt es nachzuweisen, daß in diesem Falle die ganzzahligen Vielfachen ga als Ringvielfache von a geschrieben werden können:

$$ga = g(ea) = (ge)a \quad \text{mit} \quad ge \in \mathfrak{R}. \qquad \text{qed.}$$

Definition **D (28.8)**

Es sei $\mathfrak{R}$ ein kommutativer Ring. Dann nennt man ein Ideal $\mathfrak{a}$ von $\mathfrak{R}$ Hauptideal, wenn es von einem Element a erzeugt werden kann. Falls jedes Ideal von $\mathfrak{R}$ Hauptideal ist, heißt $\mathfrak{R}$ Hauptidealring.

Hauptideale sind z. B. in jedem Ring das Nullideal (o) und in einem Ring $\mathfrak{R}$ mit Einselement e das Einheitsideal $\mathfrak{R} = (e)$. Weiter ist das Ideal der geraden Zahlen im Ringe der ganzen Zahlen Hauptideal mit 2 oder auch -2 als erzeugendem Element.

Entsprechende Überlegungen[1]) für mehrere Elemente führen zum

1) S (28.9) ist offensichtlich ein Spezialfall von S (28.11), den wir deshalb auch nur beweisen.

Satz **S (28.9)**

Es seien $a_1, a_2, \ldots, a_n$ fest gewählte Elemente aus einem kommutativen Ring $\mathfrak{R}$. Dann ist die Menge aller Elemente

$$\sum_{i=1}^{n} r_i a_i + \sum_{i=1}^{n} g_i a_i$$

mit beliebigen $r_1, \ldots, r_n$ aus $\mathfrak{R}$ und $g_1, \ldots, g_n$ aus Γ ein Ideal von $\mathfrak{R}$, das von $a_1, a_2, \ldots, a_n$ erzeugte Ideal $(a_1, a_2, \ldots, a_n)$. Es ist das kleinste Ideal von $\mathfrak{R}$, welches die Elemente $a_1, \ldots, a_n$ gleichzeitig enthält.

Ist $\mathfrak{R}$ ein Ring mit Einselement, so ist die Angabe von $\Sigma g_i a_i$ überflüssig.

Als Beispiel bilden wir in dem Ring aller Zahlen $a + b\sqrt{-5}$ mit $a \in \Gamma$ und $b \in \Gamma$ (vgl. B (26.4)) das von den Elementen

$$a_1 = 2 \quad \text{und} \quad a_2 = 1 + \sqrt{-5}$$

erzeugte Ideal

$$\mathfrak{a} = (a_1, a_2) = \left(2, 1 + \sqrt{-5}\right).$$

Da $\mathfrak{R}$ die Zahl 1 als Einselement besitzt, besteht $\mathfrak{a}$ aus allen Elementen

$$\begin{aligned} r_1 a_1 + r_2 a_2 &= \left(x + y\sqrt{-5}\right) \cdot 2 + \left(u + v\sqrt{-5}\right) \cdot \left(1 + \sqrt{-5}\right) \\ &= (2x + u - 5v) + (2y + u + v)\sqrt{-5}, \end{aligned}$$

wobei x, y, u, v beliebige ganze Zahlen sind.

Definition **D (28.10)**

Es sei $\mathfrak{R}$ ein kommutativer Ring. Dann nennt man ein Ideal $\mathfrak{a}$ von $\mathfrak{R}$ ein Ideal mit endlicher Basis, wenn es von endlich vielen Elementen $a_1, \ldots, a_n$ erzeugt werden kann.

Falls jedes Ideal von $\mathfrak{R}$ ein Ideal mit endlicher Basis ist, so sagt man: In $\mathfrak{R}$ gilt der Basissatz für Ideale.

So ist etwa die Menge aller Elemente $a + b\sqrt{-5}$ des eben betrachteten Ringes $\mathfrak{R}$, für welche $a \equiv b \bmod 2$ gilt, d. h., für welche die ganzen Zahlen a und b entweder beide gerade oder beide ungerade sind, ein Ideal von $\mathfrak{R}$. Es gilt nämlich

(1) $(a_1 + b_1\sqrt{-5}) - (a_2 + b_2\sqrt{-5}) = (a_1 - a_2) + (b_1 - b_2)\sqrt{-5}$, wobei aus $a_1 \equiv b_1\,(2)$, $a_2 \equiv b_2\,(2)$ folgt $a_1 - a_2 \equiv b_1 - b_2\,(2)$;

(2) $(x + y\sqrt{-5}) \cdot (a + b\sqrt{-5}) = (xa - 5yb) + (xb + ya)\sqrt{-5}$, wobei aus $a \equiv b\,(2)$ folgt $xa - 5yb \equiv xb + ya\,(2)$.

Dieses Ideal ist ein Ideal mit endlicher Basis; es stimmt nämlich mit dem oben behandelten Ideal $\mathfrak{a}$ überein. In der Tat gilt einerseits

$$2x + u - 5v \equiv 2y + u + v \bmod 2,$$

während umgekehrt je zwei ganze Zahlen a und b mit $a \equiv b \bmod 2$ in der Form

$$a = 2x + u - 5v, \quad b = 2y + u + v$$

ausgedrückt werden können; man wähle etwa

$$u = a, \qquad v = x = 0, \qquad y = \frac{b - a}{2}.$$

Dagegen ist dieses Ideal $\mathfrak{a}$ kein Hauptideal. Wir zeigen dies indirekt, indem wir die Annahme $\mathfrak{a} = (r + s\sqrt{-5})$ zum Widerspruch führen. Dann folgte nämlich aus $2 \in \mathfrak{a}$, d. h. $2 = (x + y\sqrt{-5})(r + s\sqrt{-5})$:

$$2 = rx - 5sy$$

$$0 = sx + ry.$$

Dies liefert $2r = (r^2 + 5s^2) \cdot x$, also

$$x = \frac{2r}{r^2 + 5s^2}.$$

Wegen $x \in \Gamma$ darf dies kein echter Bruch sein, also ergibt sich $s = 0$ und mithin $\mathfrak{a} = (r)$. Aus $1 + \sqrt{-5} \in \mathfrak{a}$, d. h. $1 + \sqrt{-5} = (u + v\sqrt{-5})r$ erhält man dann aber

$$1 = u \cdot r,$$

also $r = \pm 1$ und damit den Widerspruch $\mathfrak{a} = (r) = \mathfrak{R}$.

Der betrachtete Ring $\mathfrak{R}$ ist daher kein Hauptidealring; wir werden aber in B (43.12a) zeigen, daß jedes Ideal von $\mathfrak{R}$ eine endliche Basis hat und damit in diesem Ring der Basissatz für Ideale gilt.

Satz **S (28.11)**

Es sei $\mathfrak{R}$ ein kommutativer Ring und $\mathfrak{M}$ eine beliebige Untermenge von $\mathfrak{R}$. Dann ist die Menge aller endlicher Summen

$$\sum_{i=1}^{n} r_i a_i + \sum_{i=1}^{n} g_i a_i$$

mit beliebigen $r_1, \ldots, r_n$ aus $\mathfrak{R}$, $g_1, \ldots, g_n$ aus Γ und auch beliebigen $a_1, \ldots, a_n$ aus $\mathfrak{M}$ ein Ideal von $\mathfrak{R}$, das von $\mathfrak{M}$ erzeugte Ideal $(\mathfrak{M})$. Es ist das kleinste Ideal von $\mathfrak{R}$, welches $\mathfrak{M}$ enthält.

Ist $\mathfrak{R}$ ein Ring mit Einselement, so ist die Angabe von $\Sigma g_i a_i$ wieder überflüssig.

Beweis

In der Tat erfüllt die Menge $(\mathfrak{M})$ die beiden Idealeigenschaften:

(1) Zwei beliebige Elemente aus $(\mathfrak{M})$ können zunächst durch Hinzufügen einiger Summanden $o\,a_i + 0\,a_i$ so umgeschrieben werden, daß in beiden Elementen die gleichen $a_1, \ldots, a_n$ aus $\mathfrak{M}$ auftreten. Dann folgt

$$(\Sigma r_i a_i + \Sigma g_i a_i) - (\Sigma r_i' a_i + \Sigma g_i' a_i) = \Sigma (r_i - r_i') a_i + \Sigma (g_i - g_i') a_i$$
$$\text{mit } r_i - r_i' \in \mathfrak{R} \text{ und } g_i - g_i' \in \Gamma.$$

(2) Für jedes Element aus $(\mathfrak{M})$ und $r' \in \mathfrak{R}$ gilt

$$r'(\Sigma r_i a_i + \Sigma g_i a_i) = \Sigma (r' r_i + r' g_i) a_i + \Sigma 0\, a_i$$
$$\text{mit } r' r_i + r' g_i \in \mathfrak{R} \text{ und } 0 \in \Gamma.$$

Wie im Beweis von S(28.6) schließt man, daß $\mathfrak{M} \subseteqq (\mathfrak{M})$ gilt und andererseits jedes Ideal, welches $\mathfrak{M}$ umfaßt, auch $(\mathfrak{M})$ enthält. Der Zusatz ergibt sich unmittelbar wie in F(28.7). qed.

Bemerkung

In Anlehnung an die in der Gruppentheorie eingeführte Komplexrechnung verabreden wir folgende Schreibweisen:

Für die Menge aller Ringvielfachen ra (bzw. ar) von a schreiben wir $\mathfrak{R}a$ (bzw. $a\mathfrak{R}$), für die Menge aller ganzzahligen Vielfachen $ga = ag$ von a entsprechend $\Gamma a = a\Gamma$ und addieren solche Mengen im Sinne der in Moduln erklärten Komplexaddition.

Diese Bezeichnungen ordnen sich einer allgemeinen Komplexrechnung in beliebigen Ringen unter, auf die wir hier jedoch nicht näher

eingehen. Wir machen aber darauf aufmerksam, daß diese Komplexverknüpfungen im allgemeinen nicht distributiv sind. So enthält z. B. $4\Gamma + 6\Gamma$ mehr Elemente als $(4+6)\Gamma$, denn die erste Menge besteht genau aus allen Ausdrücken $4g_1 + 6g_2$ (wobei $g_1 \neq g_2$ möglich ist), während die zweite nur die Elemente $4g_1 + 6g_1 = 10g_1$ enthält.

Mit dieser Bezeichnung läßt sich die Idealerzeugung in $\mathfrak{R}$ beschreiben durch

$$(a) = \mathfrak{R}a + \Gamma a$$

bzw. durch

$$(a_1, a_2, \ldots, a_n) = \sum_1^n \mathfrak{R}a_i + \sum_1^n \Gamma a_i = (a_1) + (a_2) + \cdots + (a_n),$$

wobei bei Existenz eines Einselementes die Ausdrücke mit Γ entfallen.

Aufgaben zu § 28

1. Alle Untermoduln im Ringe Γ der ganzen Zahlen sind
   a) genau alle Unterringe von Γ,
   b) genau alle Ideale von Γ.
2. Γ ist Hauptidealring.
3. Der volle Matrizenring $\mathfrak{M}_n(\Gamma)$ enthält z. B. den vollen Matrizenring $\mathfrak{M}_n(2\Gamma)$ als zweiseitiges Ideal.
4. Ein Körper hat außer den trivialen Idealen weder Links- noch Rechtsideale.
5. Ein kommutativer Ring $\mathfrak{R}$, der nur die beiden trivialen Ideale enthält, ist entweder ein Körper oder ein entarteter Ring (vgl. B(26.6)).
6. Es sei $\mathfrak{R}$ ein Ring und $\mathfrak{S}$ ein Unterring von $\mathfrak{R}$. Dann ist wohl jeder Unterring von $\mathfrak{S}$ erst recht Unterring von $\mathfrak{R}$, aber nicht notwendig ein Ideal von $\mathfrak{S}$ ein Ideal von $\mathfrak{R}$.
7. Der Durchschnitt beliebig vieler Linksideale $\mathfrak{l}_1, \mathfrak{l}_2, \ldots$ eines Ringes $\mathfrak{R}$ ist wieder Linksideal von $\mathfrak{R}$. Die entsprechende Aussage gilt auch für Rechtsideale und damit für zweiseitige Ideale.
8. Die Komplexsumme endlich vieler Linksideale $\mathfrak{l}_1, \mathfrak{l}_2, \ldots, \mathfrak{l}_n$ eines Ringes $\mathfrak{R}$ ist wieder Linksideal von $\mathfrak{R}$. Die entsprechende Aussage gilt auch für Rechtsideale und damit für zweiseitige Ideale.
9. In Verallgemeinerung von $(a_1, a_2, \ldots, a_n) = (a_1) + (a_2) + \ldots + (a_n)$ beweise man:
   In einem kommutativen Ring ist das von der Vereinigungsmenge $\mathfrak{M}_1 \cup \mathfrak{M}_2 \cup \ldots \cup \mathfrak{M}_n$ erzeugte Ideal $(\mathfrak{M}_1, \mathfrak{M}_2, \ldots, \mathfrak{M}_n)$ gleich der Komplexsumme $(\mathfrak{M}_1) + (\mathfrak{M}_2) + \ldots + (\mathfrak{M}_n)$ der von den Teilmengen erzeugten Ideale.

VI. RINGKONSTRUKTIONEN, HOMOMORPHE ABBILDUNGEN

Bei den folgenden allgemeinen Aussagen über Ringe lassen wir uns von der Fragestellung leiten, aus bereits vorliegenden Ringen andere Ringe herzustellen. Wir werden eine Reihe von solchen Verfahren kennenlernen, die überdies mannigfach miteinander kombinierbar sind. Ein großer Teil der in der Mathematik betrachteten Ringe läßt sich auf diese Weise — oft in mehreren Schritten — aus dem Ringe der ganzen Zahlen gewinnen. Diese Feststellung ermöglicht gewisse systematische Betrachtungen und zeigt, daß auch die abstrakten algebraischen Begriffsbildungen ihren Ursprung in konkreten und praktisch bewährten Dingen haben und die Verbindung zu diesen nicht verlieren.

§ 29. Isomorphie und Automorphie

In Analogie zu den Betrachtungen in der Gruppentheorie wird man auch hier sagen, daß zwei Ringe gleiche Struktur besitzen, wenn sie sich zwar durch die Bezeichnung ihrer Elemente unterscheiden, sich aber die Addition und Multiplikation je zweier Elemente in beiden Ringen auf die gleiche Weise vollzieht. So haben wir schon in den Aufgaben von § 26 bemerkt, daß für Körper mit drei bzw. vier Elementen nur jeweils eine Struktur möglich ist.

Allgemein setzt ein solcher Vergleich natürlich eine geeignete eineindeutige Zuordnung zwischen den Elementen beider Ringe voraus, die überhaupt erst das Parallellaufen von Addition und Multiplikation in beiden Ringen zu verfolgen gestattet[1]). Dieses Parallellaufen bedeutet dann, daß aus $a + b = c$ und $a \cdot b = d$ für die zugeordneten Elemente $\bar{a} + \bar{b} = \bar{c}$ bzw. $\bar{a} \cdot \bar{b} = \bar{d}$ folgt, also die Relationstreue bezüglich beider Verknüpfungen.

1) Unter Umständen liegt diese Zuordnung sofort auf der Hand (wie etwa bei den obigen Beispielen), während sonst das Problem gerade darin besteht, eine solche geeignete Zuordnung zu finden bzw. im negativen Falle nachzuweisen daß es keine geben kann.

Wir werden daher wie schon in der Gruppentheorie die strukturelle Gleichheit als Isomorphie mit Hilfe isomorpher Abbildungen festlegen, wobei sich auch hier wieder alle Aussagen, die für einen Ring auf Grund der Addition und Multiplikation ausgesprochen werden können, auf jeden zu ihm isomorphen Ring übertragen.

Definition **D (29.1)**

Es sei $\mathfrak{R}$ ein beliebiger Ring und $\overline{\mathfrak{R}}$ eine Menge, in der zwei eindeutige Verknüpfungen (Addition und Multiplikation) erklärt sind.
Dann heißt $\mathfrak{R}$ isomorph abgebildet auf $\overline{\mathfrak{R}}$, in Zeichen $\mathfrak{R} \overset{\sim}{\longleftrightarrow} \overline{\mathfrak{R}}$, wenn eine eineindeutige Abbildung von $\mathfrak{R}$ auf $\overline{\mathfrak{R}}$ vermöge der Zuordnung

$$a \to \bar{a} \quad \text{mit} \quad a \in \mathfrak{R},\ a \in \overline{\mathfrak{R}}$$

vorliegt, die relationstreu bezüglich beider Verknüpfungen ist:

$$\left.\begin{aligned} \overline{a+b} &= \bar{a} + \bar{b} \\ \overline{a \cdot b} &= \bar{a} \cdot \bar{b} \end{aligned}\right\} \text{ für alle } a \text{ und } b \text{ aus } \mathfrak{R}.$$

Man nennt die Abbildung selbst einen Isomorphismus, $\mathfrak{R}$ das Original und $\overline{\mathfrak{R}}$ das isomorphe Bild.
Insbesondere heißen zwei Ringe isomorph, wenn einer von ihnen auf den anderen isomorph abgebildet werden kann[1]).

Im Sinne unserer Vorbemerkung wäre jetzt zu zeigen, daß für das isomorphe Bild $\overline{\mathfrak{R}}$ die gleichen Gesetzmäßigkeiten gelten wie für das Original $\mathfrak{R}$, also etwa: Das isomorphe Bild eines Ringes ist wieder ein Ring, das eines Körpers wieder ein Körper, mit $\mathfrak{R}$ ist auch $\overline{\mathfrak{R}}$ kommutativ (vgl. auch Aufg. 1). Wir dürfen die einfachen Beweise dafür hier übergehen, zumal sich diese Aussagen im Rahmen allgemeinerer Zusammenhänge erneut ergeben werden (vgl. § 33).
Weiterhin ist die identische Abbildung und zu jedem Isomorphismus die inverse Abbildung wieder ein Isomorphismus; das gleiche gilt für die Nacheinanderausführung zweier isomorpher Abbildungen (man verallgemeinert entsprechend den Beweis zu S(4.6)). Die als Isomorphie eingeführte strukturelle Gleichheit ist also in der Tat eine Äquivalenzrelation.

1) Obwohl wir $\mathfrak{R} \overset{\sim}{\longleftrightarrow} \overline{\mathfrak{R}}$ zunächst als Symbol für einen bestimmten Isomorphismus eingeführt haben, kennzeichnet es doch zugleich $\mathfrak{R}$ und $\overline{\mathfrak{R}}$ als isomorph schlechthin. In der Literatur ist dafür auch wieder $\mathfrak{R} \cong \overline{\mathfrak{R}}$ üblich.

Wir geben zunächst zwei Beispiele. Der aus den Matrizen

$$\overline{A} = \begin{pmatrix} a_{11} & a_{12} & 0 & \dots & 0 \\ a_{21} & a_{22} & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \dots & 0 \end{pmatrix}$$

bestehende Unterring von $\mathfrak{M}_n(\Delta)$ ist isomorph zum Matrizenring $\mathfrak{M}_2(\Delta)$ vermöge der Zuordnung

$$A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \to \overline{A}.$$

Weiterhin ist der Ring der Diagonalmatrizen

$$\bar{a} = \begin{pmatrix} a & & 0 \\ & \ddots & \\ 0 & & a \end{pmatrix} \quad \text{mit} \quad a \in \Delta$$

vermöge der Zuordnung $a \to \bar{a}$ isomorph zum Körper Δ der reellen Zahlen.

Von besonderer Bedeutung ist die folgende Anwendung des Isomorphiebegriffes auf die in D(28.4) erklärten Primkörper. Sie besteht darin, daß die Struktur eines solchen Körpers bereits durch seine Charakteristik, also durch das additive Verhalten seines Einselementes e bestimmt ist:

Satz **S (29.2)**

a) *Jeder Primkörper* Π_0 *der Charakteristik* 0 *ist isomorph zum Körper* P *der rationalen Zahlen.*

b) *Jeder Primkörper* Π_p *der Charakteristik* p *ist isomorph zum Restklassenkörper des Ringes* Γ *der ganzen Zahlen modulo* p.

Beweis

Es sei e das Einselement des betrachteten Primkörpers $\mathfrak{K}$. Mit e enthält $\mathfrak{K}$ alle ganzzahligen Vielfachen ge von e, die einen Unterring $\mathfrak{R}$ bilden, der vermöge

$$g \to ge$$

isomorph ist zum Ring Γ der ganzen Zahlen (im Falle a der Charakteristik 0) bzw. zum Restklassenring von Γ modulo p (im Falle b der Charakteristik p). Die Zuordnung ist nämlich nach Definition eindeutig und eineindeutig, da aus

$$ge = g'e, \text{ also } (g - g')e = o$$

im Falle a) $g = g'$, im Falle b) nach F(27.5) $g \equiv g' (p)$ folgt. Die Relationstreue ergibt sich aus

$$ge + g'e = (g + g')e,$$
$$ge \cdot g'e = (g \cdot g')e.$$

Als isomorphes Bild eines Ringes ist $\mathfrak{R}$ natürlich selbst ein Ring. Für den Fall b) ist damit die Behauptung bereits bewiesen; denn der Restklassenring von Γ modulo p ist nach B(26.3c) ein Körper, also auch der zu ihm isomorphe Unterring $\mathfrak{R}$ des Primkörpers $\mathfrak{K}$, der nach D(28.4) mit ihm zusammenfallen muß.
Im Fall a) ist zunächst klar, daß der kleinste Γ umfassende Körper der Körper P der rationalen Zahlen ist; entsprechend ist der Primkörper $\mathfrak{K}$ der kleinste Körper, der den zu Γ isomorphen Ring $\mathfrak{R}$ umfaßt. Aus den wesentlich allgemeineren Untersuchungen des nächsten Paragraphen wird sich ergeben, daß damit auch P und $\mathfrak{K}$ zueinander isomorph sind. qed.

Auch hier betrachten wir wieder den Fall, daß bei einer isomorphen Abbildung Original und Bild zusammenfallen:

Definition **D (29.3)**

Unter einem Automorphismus eines Ringes $\mathfrak{R}$ versteht man einen Isomorphismus von $\mathfrak{R}$ auf sich selbst.

So ergibt z. B. der Übergang von jeder komplexen Zahl zum konjugiert komplexen Wert einen Automorphismus des Körpers Z der komplexen Zahlen. Diese Zuordnung vermittelt nämlich eine eineindeutige Abbildung von Z auf Z, welche nach den Rechenregeln für komplexe Zahlen relationstreu ist (vgl. auch Aufg. 2 von §15).
Desgleichen liefert die Zuordnung

$$a + b\sqrt{k} \to a - b\sqrt{k}$$

im Ring $\Gamma + \Gamma\sqrt{k}$ (vgl. B(26.4)) einen Automorphismus dieses Ringes (vgl. Aufg. 2).

In Analogie zu den entsprechenden Überlegungen im §15 zeigen wir:

Satz **S (29.4)**

Die Menge Φ aller Automorphismen eines Ringes $\mathfrak{R}$ ist eine Gruppe, die sogenannte Automorphismengruppe von $\mathfrak{R}$. Als Verknüpfung dient dabei die Nacheinanderausführung der durch die Automorphismen bewirkten Abbildungen.

Beweis

Wir fassen Φ als Komplex in der Gruppe $\mathfrak{T}$ aller eineindeutigen Abbildungen von $\mathfrak{R}$ auf sich selbst auf. Damit ist für zwei durch

$$\left.\begin{aligned} a &\to a^{\sigma_1} \\ a &\to a^{\sigma_2} \end{aligned}\right\} \quad \text{für alle } a \in \mathfrak{R}$$

gegebene Automorphismen σ_1 und σ_2 bereits bekannt, daß ihr Produkt

$$a \to a^{[\sigma_1\sigma_2]} = (a^{\sigma_1})^{\sigma_2}$$

wieder eine eineindeutige Abbildung von $\mathfrak{R}$ auf sich ist. Das gleiche gilt für die durch

$$a \to (a^{\sigma})^{\sigma^{-1}} = a \quad \text{für alle } a \in \mathfrak{R}$$

erklärte inverse Abbildung σ^{-1} des Automorphismus σ.

Unter Verwendung des Untergruppenkriteriums aus S(5.5) haben wir also nur noch zu zeigen, daß die eineindeutigen Abbildungen $\sigma_1\sigma_2$ und σ^{-1} auch relationstreu, also wieder Automorphismen sind:

$$\begin{aligned} (a+b)^{[\sigma_1\sigma_2]} &= ((a+b)^{\sigma_1})^{\sigma_2} = (a^{\sigma_1} + b^{\sigma_1})^{\sigma_2} = (a^{\sigma_1})^{\sigma_2} + (b^{\sigma_1})^{\sigma_2} \\ &= a^{[\sigma_1\sigma_2]} + b^{[\sigma_1\sigma_2]} \\ (a \cdot b)^{[\sigma_1\sigma_2]} &= ((a \cdot b)^{\sigma_1})^{\sigma_2} = (a^{\sigma_1} \cdot b^{\sigma_1})^{\sigma_2} = (a^{\sigma_1})^{\sigma_2} \cdot (b^{\sigma_1})^{\sigma_2} \\ &= a^{[\sigma_1\sigma_2]} \cdot b^{[\sigma_1\sigma_2]} \end{aligned}$$

$$\begin{aligned} (a^{\sigma} + b^{\sigma})^{\sigma^{-1}} &= ((a+b)^{\sigma})^{\sigma^{-1}} = a + b = (a^{\sigma})^{\sigma^{-1}} + (b^{\sigma})^{\sigma^{-1}} \\ (a^{\sigma} \cdot b^{\sigma})^{\sigma^{-1}} &= ((a \cdot b)^{\sigma})^{\sigma^{-1}} = a \cdot b = (a^{\sigma})^{\sigma^{-1}} \cdot (b^{\sigma})^{\sigma^{-1}}. \end{aligned}$$

qed.

Wir erwähnen, daß in den beiden obengenannten Beispielen jeweils außer dem angegebenen Automorphismus nur noch der identische Automorphismus vorhanden und damit die Automorphismengruppe isomorph zur zyklischen Gruppe der Ordnung 2 ist. Jeder dieser Automorphismen ist also zu sich selbst invers, wie man auch unmittelbar durch zweimalige Anwendung bestätigt.

Auf die Bedeutung von Automorphismengruppen insbesondere für die Untersuchung gewisser Körper werden wir im dritten Teil zu sprechen kommen. Wie wir schon einmal bemerkten, liegt hier der entscheidende Ansatzpunkt gruppentheoretischer Methoden für algebraische Betrachtungen.

Abschließend präzisieren wir für Ringe ein in der Mathematik auch sonst häufig angewendetes

Ersetzungsverfahren **S (29.5)**

Es seien $\mathfrak{R}$ *und* $\overline{\mathfrak{S}}$ *zwei Ringe, die kein Element gemeinsam haben. Weiterhin enthalte* $\overline{\mathfrak{S}}$ *einen zu* $\mathfrak{R}$ *isomorphen Unterring* $\overline{\mathfrak{R}}$ *mit*

$$\mathfrak{R} \overset{\sim}{\longleftrightarrow} \overline{\mathfrak{R}} \text{ vermöge } a \to \bar{a}.$$

Dann läßt sich ein zu $\overline{\mathfrak{S}}$ *isomorpher Ring* $\mathfrak{S}$ *konstruieren, der* $\mathfrak{R}$ *umfaßt, indem man in* $\overline{\mathfrak{S}}$ *jedes* $\bar{a} \in \overline{\mathfrak{R}}$ *durch sein Original* $a \in \mathfrak{R}$ *ersetzt.*

Ist also vorgegeben

$$\begin{array}{c} \overline{\mathfrak{S}} \\ | \\ \overline{\mathfrak{R}} \overset{\sim}{\longleftrightarrow} \mathfrak{R} \end{array} \text{ mit } \overline{\mathfrak{S}} \cap \mathfrak{R} = \emptyset\ ^{1}),$$

so liefert die angegebene Ersetzung einen Ring $\mathfrak{S}$ mit

$$\begin{array}{ccc} \overline{\mathfrak{S}} & \overset{\sim}{\longleftrightarrow} & \mathfrak{S} \\ | & & | \\ \overline{\mathfrak{R}} & \overset{\sim}{\longleftrightarrow} & \mathfrak{R}. \end{array}$$

Beweis

Bei der Ersetzung der Elemente $\bar{a} \in \overline{\mathfrak{R}}$ durch die ihnen entsprechenden Originale $a \in \mathfrak{R}$ entsteht zunächst die Menge

$$\mathfrak{S} = (\overline{\mathfrak{S}} \setminus \overline{\mathfrak{R}}) \cup \mathfrak{R}.$$

In ihr erklären wir die Addition und Multiplikation zweier Elemente a und b wie folgt:

a) falls $a \in \mathfrak{R}$ und $b \in \mathfrak{R}$, bilden wir ihre Summe und ihr Produkt wie in $\mathfrak{R}$;

b) falls $a \in (\overline{\mathfrak{S}} \setminus \overline{\mathfrak{R}})$ und $b \in (\overline{\mathfrak{S}} \setminus \overline{\mathfrak{R}})$, bilden wir Summe und Produkt wie in $\overline{\mathfrak{S}}$; liegt dabei ein Ergebnis in $\overline{\mathfrak{R}}$, ersetzen wir es durch das entsprechende Element aus $\mathfrak{R}$;

1) Wir bezeichnen wieder (vgl. Teil 1, Anhang I) mit ø die leere Menge und mit $\overline{\mathfrak{S}} \setminus \overline{\mathfrak{R}}$ die Differenzmenge der Mengen $\overline{\mathfrak{S}}$ und $\overline{\mathfrak{R}}$.

c) falls $a \in \mathfrak{R}$ und $b \in (\overline{\mathfrak{S}} \setminus \overline{\mathfrak{R}})$, ersetzen wir a durch sein Bild $a \in \overline{\mathfrak{R}}$ und rechnen mit $\bar{a}$ und b wie in $\overline{\mathfrak{S}}$; ein gegebenenfalls nicht in $\overline{\mathfrak{S}} \setminus \overline{\mathfrak{R}}$, also in $\overline{\mathfrak{R}}$ liegendes Ergebnis wird wieder durch das entsprechende Element aus $\mathfrak{R}$ ersetzt.

Analog verfährt man für $a \in (\overline{\mathfrak{S}} \setminus \overline{\mathfrak{R}})$ und $b \in \mathfrak{R}$.

Auf diese Weise sind in $\mathfrak{S}$ Addition und Multiplikation für alle Elemente eindeutig festgelegt, und zwar so, daß diese Verknüpfungen in $\mathfrak{S}$ ebenso vorgenommen werden wie in $\overline{\mathfrak{S}}$. Damit ist $\mathfrak{S}$ ein zu $\overline{\mathfrak{S}}$ isomorpher Oberring von $\mathfrak{R}$, also ein Ring mit den geforderten Eigenschaften. qed.

Übrigens ist es oft bequem, die Ersetzung der Elemente $\bar{a} \in \overline{\mathfrak{R}}$ durch die Elemente $a \in \mathfrak{R}$ (nachträglich) als eine Identifizierung aufzufassen und in $\mathfrak{S}$ beide Bezeichnungen $\bar{a}$ und a für das gleiche Element zuzulassen: die letztere, um es als Element von $\mathfrak{R}$ zu kennzeichnen, die erstere, um das Rechnen gemäß b) und c) verfolgen zu können.

Die in diesem Beweis durchgeführte Konstruktion ist dem Leser aus dem Aufbau der Zahlenrechnung geläufig. Jeder Erweiterungsbereich $\overline{\mathfrak{S}}$ wird ja etwa mit Hilfe von Zahlenpaaren, deren Elemente dem ursprünglichen Bereich $\mathfrak{R}$ angehören, konstruiert und hat mit $\mathfrak{R}$ zunächst kein Element gemeinsam. Jedoch existiert in $\overline{\mathfrak{S}}$ ein isomorphes Bild $\overline{\mathfrak{R}}$ von $\mathfrak{R}$, und erst die Ersetzung von $\overline{\mathfrak{R}}$ durch $\mathfrak{R}$ in $\overline{\mathfrak{S}}$ ergibt eine den ursprünglichen Bereich $\mathfrak{R}$ enthaltende Erweiterung $\mathfrak{S}$. Auf die naheliegenden Beispiele des Übergangs von den ganzen zu den rationalen Zahlen bzw. von den reellen zu den komplexen Zahlen kommen wir noch ausführlicher zu sprechen. Auch bei der Einführung der reellen Zahlen liegt der entsprechende Sachverhalt vor: Die reellen Zahlen werden etwa als die Gesamtheit aller DEDEKINDschen Schnitte im Bereich der rationalen Zahlen erklärt. Diese Gesamtheit wird durch geeignete Definition von Verknüpfungen zwischen den Schnitten zu einem Körper $\overline{\mathfrak{S}}$, der einen zum Körper der rationalen Zahlen $\mathfrak{R}$ isomorphen Unterkörper $\overline{\mathfrak{R}}$ enthält. Die Ersetzung der Elemente von $\overline{\mathfrak{R}}$ durch die Elemente von $\mathfrak{R}$ gemäß unserem Satz liefert dann den angestrebten Erweiterungskörper $\mathfrak{S}$ von $\mathfrak{R}$. Im übrigen wird das gleiche Verfahren auch bei der Konstruktion der ganzen Zahlen aus den natürlichen Zahlen angewendet. Dieses Vorgehen ist gerechtfertigt, da ein S(29.5) entsprechender Satz für beliebige algebraische Strukturen gilt.

Weiterhin läßt sich jeder Körper der Charakteristik 0 als Oberkörper des Körpers P der rationalen Zahlen auffassen, indem man nach S(29.5) seinen Primkörper Π_0 durch den zu ihm gemäß S(29.2a) isomorphen Körper P ersetzt. Entsprechend kann man jeden Körper der Charakteristik p als Oberkörper des Restklassenkörpers von Γ modulo p betrachten.

Aufgaben zu § 29

1. Bei einem Isomorphismus eines Ringes $\mathfrak{R}$ auf einen Ring $\overline{\mathfrak{R}}$ werden aufeinander abgebildet:

   Nullelement auf Nullelement,

   zueinander entgegengesetzte Elemente auf ebensolche,

   eventuell vorhandene Links- bzw. Rechtseinselemente auf Elemente mit der gleichen Eigenschaft.

   Entsprechendes gilt in Ringen mit Einselement für Links- und Rechtsinverse.

2. Die Zuordnung $a + b\sqrt{k} \to a - b\sqrt{k}$ vermittelt einen Automorphismus von $\Gamma + \Gamma\sqrt{k}$ und ebenso von $\mathrm{P} + \mathrm{P}\sqrt{k}$.

3. Der Ring Γ der ganzen Zahlen, der Körper P der rationalen Zahlen und alle Restklassenringe von Γ mod m besitzen nur den identischen Automorphismus.

4. Man spreche die im Beweis von S(29.5) angegebene Erklärung von Addition und Multiplikation für den Fall aus, daß es sich bei $\mathfrak{S}$ um die Menge aller möglichen Brüche ganzer Zahlen und bei $\mathfrak{R}$ um die Menge der ganzen Zahlen handelt.

5. In Verallgemeinerung des in B(26.5) angeführten Beispieles beweise man: Der Endomorphismenring eines zyklischen Moduls $\mathfrak{G}$ der Ordnung n ist isomorph zum Restklassenring von Γ modulo n.

§ 30. Quotientenkörper und Quotientenringe

Der Übergang vom Ring der ganzen Zahlen zum Körper der rationalen Zahlen entspringt der Absicht, einen Zahlenbereich zu erhalten, in dem jede Gleichung $mx = n$ mit ganzzahligen Koeffizienten m und n ($m \neq 0$) lösbar ist. Die dazu benötigten Brüche $\frac{n}{m}$ bilden bereits den genannten Körper der rationalen Zahlen. Man hat also nicht nur die Lösbarkeit der ursprünglich gegebenen linearen Gleichungen mit ganzzahligen Koeffizienten erreicht, sondern auch von

selbst die Lösbarkeit jeder linearen Gleichung mit diesen Brüchen als Koeffizienten, natürlich mit Ausnahme der Division durch Null.

Wir untersuchen allgemein, unter welchen Bedingungen und in welcher Weise zu einem Ring ein solcher aus Quotienten bestehender Oberkörper konstruierbar ist. Diese Konstruktion wird dann selbstverständlich den Aufbau der gewöhnlichen Bruchrechnung als Spezialfall umfassen, wenn wir insbesondere vom Ring der ganzen Zahlen ausgehen (vgl. aber die Bemerkungen hinter S(30.2)).

Da ein Körper keine Nullteiler enthält, ist es offenbar notwendig, von einem nullteilerfreien Ring auszugehen. Darüber hinaus beschränken wir uns auf kommutative Ringe, denn es gibt nichtkommutative, nullteilerfreie Ringe, die nicht Unterring irgendeines Schiefkörpers sind[1]). Dagegen gilt allgemein:

Satz **S (30.1)**

Es sei $\mathfrak{R}$ ein Integritätsbereich. Dann gibt es einen $\mathfrak{R}$ enthaltenden Quotientenkörper $\mathfrak{K}$, dessen sämtliche Elemente sich als Quotienten von Elementen aus $\mathfrak{R}$ schreiben lassen. Dieser Körper $\mathfrak{K}$ ist ebenfalls kommutativ.

Beweis

1. Wir zeigen die Behauptung zunächst unter der einschränkenden Voraussetzung, daß es überhaupt einen (nicht notwendig kommutativen) Körper $\mathfrak{K}^*$ gibt, der den Ring $\mathfrak{R}$ umfaßt. Dann existiert zu jedem Element $b \neq o$ aus $\mathfrak{R}$ in $\mathfrak{K}^*$ ein eindeutig bestimmtes Inverses b^{-1}. Jedes solche zu einem Element von $\mathfrak{R}$ gehörige Inverse ist mit jedem Element $a \in \mathfrak{R}$ vertauschbar; denn wegen der Kommutativität von $\mathfrak{R}$ gilt

$$ab = ba$$

und daher

$$a = bab^{-1}$$

$$b^{-1}a = ab^{-1}.$$

Dies ermöglicht für alle Elemente $ab^{-1} \in \mathfrak{K}^*$ mit $a \in \mathfrak{R}$ und $b \in \mathfrak{R}$ die Quotientenschreibweise

$$ab^{-1} = b^{-1}a = \frac{a}{b}.$$

1) Wir müssen dafür auf einen Beweis verzichten und verweisen auf: A. MALCEV, On the immersion of an algebraic ring into a field; Math. Annalen 113 (1937), S. 686—691.

Für diese Quotienten bestätigt man leicht auf Grund ihrer Definition als Elemente von $\mathfrak{R}^*$ die folgenden Rechenregeln (vgl. Aufg. 1):

(I) Es ist $\frac{a}{b} = \frac{a'}{b'}$ genau dann, wenn $ab' = a'b$;

(II) $\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$;

(III) $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$.

Die Quotienten bilden einen kommutativen Unterkörper $\mathfrak{K}$ von $\mathfrak{R}^*$:

a) Die Differenz zweier Quotienten ist nämlich wieder ein Quotient gemäß

$$\frac{a}{b} - \frac{c}{d} = ab^{-1} - cd^{-1} = ab^{-1} + (-c)d^{-1}$$
$$= \frac{a}{b} + \frac{(-c)}{d} = \frac{ad + (-c)b}{bd}.$$

(Für das Weitere stellen wir noch fest, daß für den damit vorliegenden Modul $\mathfrak{K}$ die nach (I) untereinander gleichen Elemente

$$\frac{o}{b} \text{ für alle } b \neq o \text{ aus } \mathfrak{R}$$

das Nullelement darstellen.)

b) Der Quotient zweier Quotienten $\frac{a}{b}$ und $\frac{c}{d}$ mit vom Nullelement verschiedenem Nenner $\frac{c}{d}$ ist ebenfalls ein Quotient gemäß

$$\left(\frac{a}{b}\right) \cdot \left(\frac{c}{d}\right)^{-1} = (ab^{-1}) \cdot (cd^{-1})^{-1} = (ab^{-1}) \cdot (dc^{-1}) = \left(\frac{a}{b}\right) \cdot \left(\frac{d}{c}\right) = \frac{ad}{bc},$$

da ja $c \neq o$ gilt nach der vorangegangenen Bemerkung.

Damit ist das Kriterium von S(28.2) unter Zusammenfassung von (2) und (3) erfüllt und die Körpereigenschaft von $\mathfrak{K}$ nachgewiesen. Die Kommutativität von $\mathfrak{K}$ ergibt sich unmittelbar nach (III) aus der Kommutativität von $\mathfrak{R}$.
Unter den Quotienten treten die Elemente $a \in \mathfrak{R}$ vermöge

$$a = a(bb^{-1}) = (ab)b^{-1} = \frac{ab}{b}$$

selbst mit auf, also gilt $\mathfrak{R} \subseteq \mathfrak{K}$.

2. Die im ersten Teil des Beweises gewonnenen Einsichten in die Struktur des Quotientenkörpers von $\mathfrak{R}$ gestatten uns nun, allein

mit Hilfe des vorgegebenen (nullteilerfreien, kommutativen) Ringes $\mathfrak{R}$ einen Quotientenkörper zu konstruieren und damit seine Existenz unabhängig von der einschränkenden Voraussetzung unter 1. nachzuweisen.

Hierbei können wir natürlich nicht ohne weiteres wie im ersten Teil des Beweises mit den Quotienten von Ringelementen arbeiten, da diese ja in ihrer Gesamtheit erst in einem umfassenden Körper existieren, den wir gerade erst konstruieren wollen. Wir schaffen uns vielmehr einen neuen Rechenbereich $\overline{\mathfrak{R}}$, dessen Elemente alle möglichen geordneten Paare

$$(a, b) \text{ mit } b \neq o$$

von Elementen aus $\mathfrak{R}$ sind. Für diese Elementenpaare erklären wir solche Rechenregeln, daß sie sich am Ende unserer Überlegung als die gesuchten Quotienten ergeben werden. Wie wir dies vorzunehmen haben, entnehmen wir den obigen Regeln (I), (II), (III). Falls uns nämlich überhaupt die Konstruktion eines Quotientenkörpers gelingt, müssen ja für seine Elemente die Aussagen unter 1. gültig sein.

(I) Es ist $(a, b) = (a', b')$ genau dann, wenn $ab' = a'b$;

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

(III) $(a, b) \cdot (c, d) = (ac, bd)$.

Diese Setzungen sind in der Tat möglich, denn wir bemerken:

Die in (I) unter den Elementen von $\overline{\mathfrak{R}}$ erklärte Gleichheit ist

a) reflexiv wegen $ab = ab$;

b) symmetrisch, weil aus $ab' = a'b$ folgt $a'b = ab'$;

c) transitiv, weil aus $ab' = a'b$ und $a'b'' = a''b'$ zunächst $ab''b' = a'b''b = a''b'b$ und damit $b'(ab'' - a''b) = o$ folgt; aus $b' \neq o$ und der Nullteilerfreiheit von $\mathfrak{R}$ ergibt sich die Behauptung.

Die in (II) für die Elemente von $\overline{\mathfrak{R}}$ erklärte Addition ergibt wieder ein eindeutig bestimmtes Element von $\overline{\mathfrak{R}}$. Mit b und d ist nämlich nach Voraussetzung über $\mathfrak{R}$ auch bd verschieden von $o \in \mathfrak{R}$. Ferner ist die Summe unabhängig von der nach (I) möglichen verschiedenen Schreibweise der Summanden:

$$\text{Aus } (a, b) = (a', b') \text{ und } (c, d) = (c', d')$$
$$\text{folgt } (ad + bc, bd) = (a'd' + b'c', b'd'),$$

weil aus $ab' = a'b$ und $cd' = c'd$

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

Die in (III) für die Elemente von $\overline{\mathfrak{R}}$ erklärte Multiplikation ergibt wieder ein eindeutig bestimmtes Element von $\overline{\mathfrak{R}}$, wie man analog dem eben Gesagten nachweist.

Wir zeigen als Nächstes, daß $\overline{\mathfrak{R}}$ ein kommutativer Körper ist. Von den Körperaxiomen sind bereits *A I* und *M I* nachgewiesen; *A IV* und *M IV* ergeben sich unmittelbar aus (II) bzw. (III), deren rechte Seiten bei gleichzeitiger Vertauschung von a und c sowie b und d erhalten bleiben; *A II*, *M II* und *D* folgen ohne weiteres durch Ausrechnung (vgl. Aufg. 2). Ferner stellt (o, b) mit beliebigem $b \neq o$ das Nullelement von $\overline{\mathfrak{R}}$ dar ($A\ III_1$) und $(-a, b)$ das zu (a, b) entgegengesetzte Element ($A\ III_2$). Desgleichen ist (b, b) mit beliebigem $b \neq o$ das Einselement von $\overline{\mathfrak{R}}$ ($M\ III_1$) und (b, a) das zu $(a, b) \neq (o, b)$ inverse Element ($M\ III_2$).

Dieser Körper $\overline{\mathfrak{R}}$ enthält einen zu $\mathfrak{R}$ isomorphen Unterring $\overline{\mathfrak{R}}$ vermöge der Zuordnung

$$a \to \overline{a} = (ab, b) \text{ mit beliebigem } b \neq o.$$

Diese Zuordnung ist eindeutig wegen $(ab, b) = (ab', b')$ nach (I) und eineindeutig, denn aus $(ab, b) = (a'b, b)$ folgt $a = a'$ ebenfalls nach (I) und der Nullteilerfreiheit von $\mathfrak{R}$. Die Relationstreue ergibt sich aus

$$\overline{a_1} + \overline{a_2} = (a_1b, b) + (a_2b, b) = ((a_1 + a_2)b^2, b^2) = \overline{a_1 + a_2},$$

$$\overline{a_1} \cdot \overline{a_2} = (a_1b, b) \cdot (a_2b, b) = ((a_1 \cdot a_2)b^2, b^2) = \overline{a_1 \cdot a_2}.$$

Vermöge S(29.5) können wir einen zu $\overline{\mathfrak{R}}$ isomorphen Körper $\mathfrak{K}$ angeben, der den Ring $\mathfrak{R}$ enthält, indem wir die Elemente $(ab, b) \in \overline{\mathfrak{R}}$ durch die Elemente $a \in \mathfrak{R}$ ersetzen, d. h. $\overline{\mathfrak{R}}$ mit $\mathfrak{R}$ gemäß $(ab, b) = a$ identifizieren. Dieser Körper $\mathfrak{K}$ besteht dann in der Tat nur aus Quotienten von Elementen aus $\mathfrak{R}$, denn jedes seiner Elemente läßt sich gemäß

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

als Quotient von Elementen aus $\mathfrak{R}$ schreiben.

qed.

Satz **S (30.2)**

Der Quotientenkörper $\mathfrak{K}$ von $\mathfrak{R}$ ist durch $\mathfrak{R}$ bis auf Isomorphie eindeutig bestimmt. Er ist der kleinste den Ring $\mathfrak{R}$ enthaltende Körper, und jeder $\mathfrak{R}$ umfassende (nicht notwendig kommutative) Körper $\mathfrak{K}^*$ enthält genau einen zu $\mathfrak{K}$ isomorphen Unterkörper.

Beweis

Alle Elemente eines Quotientenkörpers von $\mathfrak{R}$ lassen sich als Quotienten von Elementen aus $\mathfrak{R}$ schreiben. Da das Rechnen mit diesen Quotienten vermöge der Regeln (I), (II), (III) vollständig durch in $\mathfrak{R}$ vorzunehmende Rechenoperationen gekennzeichnet wird, hat jeder Quotientenkörper die gleiche Struktur (vgl. auch Aufg. 3). Ferner enthält jeder $\mathfrak{R}$ umfassende Körper $\mathfrak{K}^*$ auch alle mit Elementen aus $\mathfrak{R}$ in $\mathfrak{K}^*$ zu bildenden Quotienten, also einen Quotientenkörper von $\mathfrak{R}$. Andererseits kann $\mathfrak{K}^*$ nicht zwei voneinander verschiedene Quotientenkörper von $\mathfrak{R}$ enthalten, da sonst wenigstens eine Gleichung $bx = a$ mit a und $b \neq o$ aus $\mathfrak{R}$ zwei verschiedene Lösungen haben müßte (nämlich je eine aus jedem Quotientenkörper) im Widerspruch zur Eindeutigkeit der Division in $\mathfrak{K}^*$. qed.

Für die elementare Bruchrechnung entnehmen wir aus unseren Überlegungen, daß die Struktur des Körpers der rationalen Zahlen durch die für ganze Zahlen gültigen Rechengesetze eindeutig festgelegt ist, wobei man die Aussagen über die Anordnung sowohl der ganzen Zahlen als auch der rationalen Zahlen zunächst vollkommen beiseite lassen kann. Die im Schulunterricht von vornherein übliche Unterscheidung von echten und unechten Brüchen hat also weniger inhaltliche als methodische Gründe.

Auch die allgemein in der Zahlenrechnung übliche Übertragung der für Brüche ganzer Zahlen gültigen Rechenregeln auf alle auftretenden Quotienten hat ihre letzte Begründung in der eindeutigen Bestimmtheit des Quotientenkörpers zu jedem Unterring des Körpers der komplexen Zahlen.

Wir besprechen abschließend eine Verallgemeinerung unserer Gedankengänge. Betrachten wir noch einmal die im zweiten Teil des Beweises von S (30.1) verwendeten Elementenpaare (a, b). Als erste Komponente a treten alle Elemente aus $\mathfrak{R}$ auf, während für die zweite Komponente nur die Elemente $b \neq o$ zugelassen sind[1]). Wir können jetzt der zweiten Komponente weitere Be-

1) Von dieser Einschränkung haben wir beim Beweis mehrfach Gebrauch gemacht, und sie läßt sich in der Tat nicht vermeiden, weil ein zugelassenes Elementenpaar (o, o) jedem anderen Paar (a, b) nach (I) gleich wäre.

schränkungen auferlegen, indem wir die Elemente b aus einer geeigneten, nicht leeren Untermenge $\mathfrak{F} < \mathfrak{R}$ entnehmen. Von dieser Untermenge ist außer $o \notin \mathfrak{F}$ zu fordern, daß sie mit je zwei Elementen b und d auch das Produkt bd enthält (also eine Halbgruppe ist), damit die durch (II) und (III) erklärten Verknüpfungen Elementenpaare der gleichen Art als Ergebnis liefern. Wie man sich leicht überzeugt, kann man dann für diese Elementenpaare ebenso wie im vorn geführten Beweis die Gültigkeit aller Axiome mit Ausnahme von $M\,III_2$ zeigen. Ein zu (a, b) inverses Element (b, a) läßt sich dagegen nur für die Elementenpaare angeben, bei denen auch $a \in \mathfrak{F}$ gilt.

Auf diese Weise erhalten wir einen aus Quotienten von Elementen aus $\mathfrak{R}$ bestehenden *Quotientenring*, der wieder nach S(29.5) Oberring von $\mathfrak{R}$ ist und andererseits ein Unterring des Quotientenkörpers von $\mathfrak{R}$. Dieser Quotientenring von $\mathfrak{R}$ ist (bis auf Isomorphie) nur von der zugrunde gelegten multiplikativen Halbgruppe $\mathfrak{F} < \mathfrak{R}$ abhängig, deren Elemente als zweite Komponente der Elementenpaare, also als Nenner der entsprechenden Quotienten zugelassen werden. Der Quotientenkörper selbst ist insbesondere derjenige Quotientenring, der durch die multiplikative Halbgruppe aller von o verschiedenen Ringelemente bestimmt ist. Beispiele für Quotientenringe geben wir in Aufgabe 6.

Diese Überlegungen lassen sich schließlich auf kommutative Ringe mit Nullteilern übertragen, für die wir zwar keinen Quotientenkörper, aber eben doch gewisse Quotientenringe bilden können. Wir brauchen dann nämlich nur die Halbgruppe $\mathfrak{F}$ aus der Menge der Nichtnullteiler von $\mathfrak{R}$ zu wählen, da wir von der vorn für den ganzen Ring geforderten Eigenschaft der Nullteilerfreiheit doch nur für die zweiten Komponenten Gebrauch gemacht haben. Der größtmögliche Quotientenring von $\mathfrak{R}$ entsteht dabei, wenn man für $\mathfrak{F}$ die Menge aller Nichtnullteiler von $\mathfrak{R}$ nimmt (vgl. Aufg. 2 von § 25).

Aufgaben zu § 30

1. Man beweise die im ersten Teil des Beweises von S(30.1) aufgeführten Rechenregeln.
2. Man zeige die Gültigkeit der Axiome *A II*, *M II* und *D* in dem im Text eingeführten Bereich $\mathfrak{K}$.
3. Quotientenkörper isomorpher Integritätsbereiche sind ebenfalls isomorph. Man beweise dies durch Angabe einer Zuordnung ihrer Elemente.

4. Man bestimme den Quotientenkörper des Ringes der ganzen GAUSSschen Zahlen.
5. In der Schulmathematik pflegt man die Regeln für das Kürzen und Erweitern, für die Addition von Brüchen mit gleichen Nennern und für die Multiplikation beliebiger Brüche nach einleitenden anschaulichen Beispielen als stets verbindlich zu erklären. Man zeige, daß diese Regeln unseren Festlegungen (I), (II), (III) gleichwertig sind.
6. Die in B(26.4b) genannten Ringe sind Quotientenringe des Ringes Γ der ganzen Zahlen. Man gebe die zugehörige Halbgruppe $\mathfrak{F}$ an und bilde, von anderen Halbgruppen aus Γ ausgehend, entsprechende Beispiele von Quotientenringen.

§ 31. Ringe aus geordneten Elementensystemen

Die im vorangehenden Paragraphen durchgeführte Konstruktion von Quotientenringen beruht auf folgenden Grundgedanken:

1) Aus der Menge $\mathfrak{R}$ der Elemente eines vorgegebenen Ringes bildet man mit Hilfe einer geeigneten Halbgruppe $\mathfrak{F} \subset \mathfrak{R}$ als neue Menge die Menge aller geordneten Elementenpaare (a, b) mit $a \in \mathfrak{R}$, $b \in \mathfrak{F}$, also die sogenannte Produktmenge $\mathfrak{R} \times \mathfrak{F}$.

2) In $\mathfrak{R} \times \mathfrak{F}$ wird eine (meist sofort mit „$=$“ bezeichnete) Äquivalenzrelation erklärt, die eine Klasseneinteilung in $\mathfrak{R} \times \mathfrak{F}$ hervorruft. Dies geschieht natürlich in einer für den beabsichtigten Zweck geeigneten Weise, denn diese Äquivalenzklassen sollen ja die Elemente der angestrebten algebraischen Struktur werden[1]).

3) Zwischen diesen Äquivalenzklassen von $\mathfrak{R} \times \mathfrak{F}$ bzw. ihren Repräsentanten werden mit Hilfe der Rechenoperationen in $\mathfrak{R}$ eine additive und eine multiplikative Verknüpfung erklärt, und zwar so, daß damit die Menge der Äquivalenzklassen zu einer dem Ziel des ganzen Vorgehens entsprechenden algebraischen Struktur wird.

4) Schließlich ergibt sich, daß die konstruierte algebraische Struktur einen zum Ring $\mathfrak{R}$ isomorphen Unterring enthält und damit als Erweiterung von $\mathfrak{R}$ aufgefaßt werden kann, welche überdies die gewünschten Eigenschaften besitzt.

Völlig analoge Gedankengänge findet man bei der Konstruktion der verschiedensten algebraischen Strukturen wieder, wovon dem Leser bereits einige Beispiele aus dem Aufbau der Zahlenrechnung

1) Das übliche repräsentantenweise Rechnen darf über diesen grundsätzlichen Sachverhalt nicht hinwegtäuschen.

bekannt sind. So kann man einmal von der algebraischen Struktur N (lies Ny) der natürlichen Zahlen (die nicht einmal ein Ring ist) ausgehen in der Absicht, einen Rechenbereich zu schaffen, in dem auch jede Subtraktion durchführbar ist. Dazu erklärt man in der Produktmenge $N \times N$ die Äquivalenzrelation und die beiden Verknüpfungen wie folgt:

(I) Es ist $(a, b) = (a', b')$ genau dann, wenn $a + b' = a' + b$;

(II) $(a, b) + (c, d) = (a + c, b + d)$;

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

Man erhält auf diese Weise den *Ring der ganzen Zahlen.* Der entsprechende Übergang vom Ring der ganzen Zahlen zum *Körper der rationalen Zahlen* ist in unseren allgemeinen Überlegungen des § 30 enthalten. Schließlich kann man zum Körper Δ der reellen Zahlen einen Oberkörper Z konstruieren, in dem jede algebraische Gleichung zweiten Grades lösbar ist. Zu diesem Zweck legt man in der Produktmenge $\Delta \times \Delta$ fest:

(I) Es ist $(a, b) = (a', b')$ genau dann, wenn $a = a'$ und $b = b'$;

(II) $(a, b) + (c, d) = (a + c, b + d)$;

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

In dem so entstehenden *Körper der komplexen Zahlen* ist dann sogar jede algebraische Gleichung lösbar (sog. Fundamentalsatz der klassischen Algebra). Zu der üblichen Schreibweise der komplexen Zahlen gelangt man wie folgt:

Die Zahlenpaare $(a, 0)$ bilden vermöge der Zuordnung $a \to (a, 0)$ für alle $a \in \Delta$ einen zum Körper Δ der reellen Zahlen isomorphen Unterkörper, den wir gemäß S(29.5) mit Δ identifizieren können. Dann lassen sich alle Zahlenpaare (a, b) gemäß

$$(a, b) = (a, 0) \cdot (1, 0) + (b, 0) \cdot (0, 1) = a \cdot (1, 0) + b \cdot (0, 1) = a + b\,i$$

schreiben, wenn man die Abkürzung i für das spezielle Zahlenpaar $(0, 1)$ mit $(0, 1)^2 = (-1, 0) = -1$ einführt.

Die Verschiedenheit der in diesen drei Beispielen erfolgten Festlegungen läßt bereits erwarten, daß die sich auf diese Weise ergebenden Konstruktionsmöglichkeiten algebraischer Strukturen außerordentlich vielfältig sein werden. Wir wollen jedoch betonen, daß solche Konstruktionen nicht schon um ihrer selbst willen, sondern nur im Hinblick auf die Lösung bestimmter Aufgaben Interesse verdienen. So kann man sich etwa auf einem solchen Wege

leicht überzeugen, daß nicht alle aus der Zahlenrechnung geläufigen Gesetze aus den Ringaxiomen folgen. Beispielsweise erhält man aus der Menge der Elementenpaare von $\mathfrak{R} \times \mathfrak{R}$ vermöge der nachstehenden Setzungen einen *Ring mit Nullteilern*, auch wenn der Ring $\mathfrak{R}$ nullteilerfrei ist (vgl. Aufg. 1):

(I) Es ist $(a, b) = (a', b')$ genau dann, wenn $a = a'$ und $b = b'$;

(II) $(a, b) + (c, d) = (a + c, b + d)$;

(III) $(a, b) \cdot (c, d) = (ac, bd)$.

Entsprechend konstruiert man etwa aus einem Ring mit eindeutig bestimmten Einselement e auf folgende Weise einen *Ring mit mehreren Linkseinselementen* (vgl. Aufg. 2):

(I) Es ist $(a, b) = (a', b')$ genau dann, wenn $a = a'$ und $b = b'$;

(II) $(a, b) + (c, d) = (a + c, b + d)$;

(III) $(a, b) \cdot (c, d) = (ac, ad)$.

Von besonderer Bedeutung ist das folgende Beispiel eines *nichtkommutativen Körpers*. Seine Elemente gewinnen wir zunächst als Paare komplexer Zahlen, die wir dann als Quadrupel reeller Zahlen schreiben. Das erklärt seinen Namen *Quaternionenkörper*.

Wir bezeichnen die Elemente des Körpers Z der komplexen Zahlen mit griechischen Buchstaben und erklären in der Produktmenge $Z \times Z$:

(I) Es ist $(\alpha, \beta) = (\alpha', \beta')$ genau dann, wenn $\alpha = \alpha'$ und $\beta = \beta'$;

(II) $(\alpha, \beta) + (\gamma, \delta) = (\alpha + \gamma, \beta + \delta)$;

(III) $(\alpha, \beta) \cdot (\gamma, \delta) = (\alpha\gamma - \beta\bar{\delta}, \alpha\delta + \beta\bar{\gamma})$.

Unter $\bar{\gamma}$ bzw. $\bar{\delta}$ verstehen wir dabei die zu γ bzw. δ konjugiert komplexe Zahl.

Damit erhalten wir tatsächlich einen Schiefkörper, der den Körper der komplexen Zahlen umfaßt:

1) Die in (I) festgelegte Gleichheit der Zahlenpaare bedeutet komponentenweise Gleichheit der Zahlen und ist damit eine Äquivalenzrelation.

2) Desgleichen überträgt sich die Moduleigenschaft von den Zahlen auf die Zahlenpaare vermöge der komponentenweisen Festsetzung der Addition (II).

3) *M I:* ist nach Definition erfüllt[1]).

M II: $[(\alpha, \beta)\ (\gamma, \delta)]\ (\varkappa, \lambda) = (\alpha\gamma - \beta\bar{\delta}, \alpha\delta + \beta\bar{\gamma})\ (\varkappa, \lambda)$
$= ((\alpha\gamma - \beta\bar{\delta})\varkappa - (\alpha\delta + \beta\bar{\gamma})\bar{\lambda}, (\alpha\gamma - \beta\bar{\delta})\lambda + (\alpha\delta + \beta\bar{\gamma})\bar{\varkappa})$,
$(\alpha, \beta)\ [(\gamma, \delta)\ (\varkappa, \lambda)] = (\alpha, \beta)\ (\gamma\varkappa - \delta\bar{\lambda}, \gamma\lambda + \delta\bar{\varkappa})$
$= (\alpha(\gamma\varkappa - \delta\bar{\lambda}) - \beta(\bar{\gamma}\bar{\lambda} + \bar{\delta}\varkappa), \alpha(\gamma\lambda + \delta\bar{\varkappa}) + \beta(\bar{\gamma}\varkappa - \bar{\delta}\lambda))$.
Der Vergleich der Komponenten zeigt die Gültigkeit des Assoziativgesetzes.

M III$_1$: Linkseinselement ist das Zahlenpaar (1, 0).

M III$_2$: Zu jedem vom Nullelement (0, 0) verschiedenen Element (γ, δ) existiert ein Linksinverses (α, β), da die aus

$$(\alpha, \beta)\ (\gamma, \delta) = (1, 0)$$

für α und β folgenden Gleichungen

$$\alpha\gamma - \bar{\delta}\beta = 1$$
$$\alpha\delta + \beta\bar{\gamma} = 0$$

nur dann nicht lösbar sind, wenn die Koeffizientendeterminante verschwindet:

$$\begin{vmatrix} \gamma & -\bar{\delta} \\ \delta & \bar{\gamma} \end{vmatrix} = \gamma\bar{\gamma} + \delta\bar{\delta} = 0.$$

Das wäre aber gleichbedeutend mit $\gamma = \delta = 0$.

M IV: Das Kommutativgesetz ist dagegen nicht erfüllt, wie man entweder unmittelbar (III) entnimmt oder leicht durch ein Beispiel zeigt:

$$(i, 0)\ (0, 1) = (0, i) \neq (0, -i) = (0, 1)\ (i, 0).$$

4) Wegen der Nichtkommutativität der Multiplikation müssen beide Relationen des distributiven Gesetzes nachgewiesen werden, wobei wir jedoch die analoge Durchrechnung der zweiten Relation dem Leser überlassen:

$$(\alpha, \beta)\ [(\gamma, \delta) + (\varkappa, \lambda)] = (\alpha, \beta)\ (\gamma + \varkappa, \delta + \lambda)$$
$$= (\alpha(\gamma + \varkappa) - \beta(\bar{\delta} + \bar{\lambda}), \alpha(\delta + \lambda) + \beta(\bar{\gamma} + \bar{\varkappa}),$$
$$(\alpha, \beta)\ (\gamma, \delta) + (\alpha, \beta)\ (\varkappa, \lambda) = (\alpha\gamma - \beta\bar{\delta}, \alpha\delta + \beta\bar{\gamma}) + (\alpha\varkappa - \beta\bar{\lambda}, \alpha\lambda + \beta\bar{\varkappa})$$
$$= (\alpha\gamma - \beta\bar{\delta} + \alpha\varkappa - \beta\bar{\lambda}, \alpha\delta + \beta\bar{\gamma} + \alpha\lambda + \beta\bar{\varkappa}).$$

---

1) Man beachte, daß bei der durch (I) erklärten Klasseneinteilung von $Z \times Z$ jede Klasse aus genau einem Element besteht. Die Frage nach der Abhängigkeit der Festlegungen (II) und (III) von der Wahl der Repräsentanten ist hier also gegenstandslos.

5) Die Zahlenpaare $(\alpha, 0)$ bilden einen zum Körper der komplexen Zahlen isomorphen Unterkörper des Quaternionenkörpers. Die Anwendung des Ersetzungsverfahrens S (29.5) vollendet unseren Beweis.

Da auch für das Zahlenpaar $j = (0, 1)$ die Beziehung

$$(0, 1)^2 = (-1, 0) = -1$$

gilt, könnte man in Analogie zu unseren obigen Bemerkungen über die Schreibweise der komplexen Zahlen auf folgende Umschreibung kommen:

$$(\alpha, \beta) = (\alpha, 0)\,(1, 0) + (\beta, 0)\,(0, 1) = \alpha\,(1, 0) + \beta\,(0, 1) = \alpha + \beta j.$$

Diese Bezeichnung ist jedoch deswegen unbefriedigend und sogar irreführend, weil man mit den Ausdrücken $\alpha + \beta j \in Z + Zj$ nicht unter Übertragung der für komplexe Zahlen $a + bi \in \Delta + \Delta i$ geläufigen Regeln, natürlich nun mit $j^2 = -1$, rechnen kann. Zwar gilt noch

$$\begin{aligned}(\alpha, \beta) + (\gamma, \delta) &= (\alpha + \beta j) + (\gamma + \delta j) = (\alpha + \gamma) + (\beta + \delta) j \\ &= (\alpha + \gamma, \beta + \delta),\end{aligned}$$

dagegen könnte man

$$(\alpha + \beta j)\,(\gamma + \delta j) = \alpha\gamma + \beta j\,\delta j + \beta j\,\gamma + \alpha\,\delta j$$

nur bei Vertauschbarkeit von j mit δ und γ, also von j mit jeder komplexen Zahl, in der angestrebten Weise weiter vereinfachen; es gilt jedoch nach obigem bereits $ij = -ji$.

Wir können jedoch auf eine andere Art zu einer Schreibweise unserer Zahlenpaare (α, β) als Summe gewisser Körperelemente gelangen, die mit den Rechenregeln eines Schiefkörpers in Einklang steht. Dazu erinnern wir uns daran, daß die komplexen Zahlen ihrerseits Paare reeller Zahlen sind. Daher können wir das Element (α, β) anstatt durch zwei in fester Reihenfolge angegebene komplexe Zahlen ebensogut durch vier in fester Reihenfolge angegebene reelle Zahlen kennzeichnen:

$$(\alpha, \beta) = ((a, b), (c, d)) = (a, b, c, d).$$

Die Rechenregeln (I), (II), (III) für die Paare komplexer Zahlen ergeben die entsprechenden Regeln für die Quadrupel reeller Zahlen:

(I) Es ist $(a, b, c, d) = (a', b', c', d')$ genau dann,
wenn $a = a', b = b', c = c', d = d'$;

(II) $(a, b, c, d) + (a', b', c', d') = (a + a', b + b', c + c', d + d')$;

III) $(a, b, c, d) \cdot (a', b', c', d') =$
$(aa' - bb' - cc' - dd', ab' + ba' + cd' - dc',$
$ac' - bd' + ca' + db', ad' + bc' - cb' + da')$.

Damit haben wir zunächst ein Beispiel für die Konstruktion einer algebraischen Struktur mit Hilfe geordneter n-tupel ($n = 4$) aus Elementen einer bestimmten Struktur (vgl. auch Aufg. 3). Weiterhin schreiben wir die Quadrupel wie folgt um:

$$\begin{aligned}(a, b, c, d) &= (a, 0, 0, 0) + (0, b, 0, 0) + (0, 0, c, 0) + (0, 0, 0, d)\\ &= a(1, 0, 0, 0) + b(0, 1, 0, 0) + c(0, 0, 1, 0) + d(0, 0, 0, 1).\end{aligned}$$

Wir können nämlich die Menge der Quadrupel $(x, 0, 0, 0)$ gemäß $x = (x, 0, 0, 0)$ mit dem Körper der reellen Zahlen identifizieren, womit sich die Richtigkeit unserer Zerlegung nach (II) und (III) ergibt. Ferner erhalten wir für die Elemente

$$1 = (1, 0, 0, 0),\ i = (0, 1, 0, 0),\ j = (0, 0, 1, 0),\ k = (0, 0, 0, 1)$$

nach (III) die Multiplikationstafel

$\cdot$	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

Unter Berücksichtigung dieser Multiplikationsvorschriften entspricht das nach den formalen Regeln vorgenommene Rechnen mit den „Quaternionen"

$$(a, b, c, d) = a + bi + cj + dk$$

in der Tat unseren Festlegungen (I), (II) und (III). Die leichte Nachrechnung bleibt dem Leser überlassen.

Die so einfache Struktur der Quaternionen überrascht angesichts ihrer schwerfälligen Einführung als Zahlenpaare bzw. Zahlenquadrupel. Von den für alle Elemente des Quaternionenkörpers in (II) und (III) erklärten Rechenverknüpfungen legen bezüglich der Multiplikation bereits die $4 \cdot 4$ Produkte der Elemente $1, i, j, k$ alles fest. Entsprechendes gilt für den Körper der komplexen Zahlen mit

$\cdot$	1	i
1	1	i
i	i	-1 .

Diese einfachen Ergebnisse erhielten wir allerdings erst aus der Konstruktion mit Hilfe von Zahlenpaaren bzw. Zahlenquadrupeln. In vielen Fällen ist es aber möglich, solche umständlichen Kon-

struktionen mit Hilfe von n-tupeln durch geeignete allgemeine Begriffsbildungen ein für alle mal vorwegzunehmen. Im nächsten Kapitel werden wir diese Problemstellung wieder aufgreifen, sogar unter Ausdehnung auf geordnete Elementensysteme mit abzählbar unendlich vielen Komponenten. Ein konkretes Beispiel für die zuletzt genannte Verallgemeinerung lernen wir schon im folgenden Paragraphen kennen.

Aufgaben zu § 31

1. Man konstruiere entsprechend den Angaben im Text einen Ring mit Nullteilern.
2. Ebenso konstruiere man einen Ring mit mehreren Linkseinselementen.
3. Welcher Zusammenhang besteht zwischen Matrizenringen und Ringen geordneter Elementensysteme?
4. Man berechne das Inverse eines von Null verschiedenen Elementes $a + bi + cj + dk$ des Quaternionenkörpers.
5. Der Quaternionenkörper ist isomorph zu einem Unterkörper des vollen Matrizenringes $\mathfrak{M}_2(Z)$ über dem Körper Z der komplexen Zahlen vermöge der Zuordnung

$$a + bi + cj + dk \to \begin{pmatrix} a + bi & c + di \\ -c + di & a - bi \end{pmatrix}.$$

Welche wesentlich einfachere Behandlung der Quaternionen ergibt sich aus dieser Tatsache?

§ 32. Polynomringe

Bereits in der Schulmathematik werden rationale und insbesondere ganze rationale Funktionen in einer Variablen, etwa mit reellen Zahlen als Koeffizienten, betrachtet. Diese bilden strenggenommen mit der für Funktionen üblichen Addition und Multiplikation einen neuen Rechenbereich, in dem die gleichen formalen Regeln gelten wie beim Rechnen mit Zahlen, wovon man freilich in der Schulmathematik meist stillschweigend Gebrauch zu machen pflegt. Wir verallgemeinern und präzisieren dies, indem wir von einem belie-

bigen Ring $\mathfrak{R}$ ausgehend einen Ring konstruieren, der gerade aus allen ganzen rationalen Funktionen mit Koeffizienten aus $\mathfrak{R}$ besteht.

Unter einer ganzen rationalen Funktion oder einem Polynom mit Koeffizienten aus $\mathfrak{R}$ versteht man in diesem Zusammenhang einfach einen Ausdruck

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

mit Elementen a_i aus $\mathfrak{R}$ und einem nicht zu $\mathfrak{R}$ gehörigen Element x. Von diesem Element x wird nichts weiter verlangt, als daß es einerseits mit den Elementen aus $\mathfrak{R}$ zusammen den für Ringe gültigen Rechenregeln genügt (also etwa in einem gemeinsamen Oberring mit diesen Elementen liegt) und dabei mit den Elementen aus $\mathfrak{R}$ vertauschbar ist, andererseits aber keine algebraische Gleichung

$$b_0 + b_1 x + \cdots + b_n x^n = o$$

mit nicht sämtlich verschwindenden Koeffizienten $b_i \in \mathfrak{R}$ erfüllt. Man nennt ein solches Element x eine *Unbestimmte über* $\mathfrak{R}$ (vgl. auch Aufg. 1).

Diese in der Algebra übliche Auffassung der ganzen rationalen Funktionen unterscheidet sich wesentlich von dem allgemeinen Funktionsbegriff, welcher der Analysis und auch der Schulmathematik zugrunde liegt. Dort steht im Vordergrund die (eindeutige) Zuordnung der Elemente eines Argumentbereiches, den die unabhängige Variable x durchläuft, zu den Elementen eines Wertebereiches, den die abhängige Variable $y = f(x)$ durchläuft. Das macht den Funktionsbegriff und damit alle ihn betreffenden Aussagen prinzipiell abhängig vom Argumentbereich. Dagegen stützt sich die algebraische Auffassung von vornherein auf formale Rechenausdrücke, in denen x nicht mehr stellvertretend für Elemente eines bestimmten Argumentbereiches steht, sondern als ein von jeder Konkretisierung unabhängiges Rechensymbol auftritt. Dies hat den Vorteil, daß man die „Unbestimmte x" nachträglich wieder als „Variable x" innerhalb der verschiedensten Argumentbereiche deuten kann. Die Möglichkeit einer solchen allgemeinen Behandlung von ganzen rationalen Funktionen beruht auf dem folgenden Existenzbeweis, wobei wir den Leser auf analoge Entwicklungen in § 30 hinweisen.

Satz **S (32.1)**

Es sei $\mathfrak{R}$ ein beliebiger Ring mit Einselement e[1]). Dann gibt es einen $\mathfrak{R}$ umfassenden Polynomring in einer Unbestimmten, dessen Elemente genau alle Polynome in dieser Unbestimmten mit Koeffizienten aus $\mathfrak{R}$ sind.

Beweis

1. Wir setzen zunächst voraus, daß es einen Ring $\mathfrak{R}^*$ gibt, der sowohl $\mathfrak{R}$ als auch eine Unbestimmte x enthält, die mit allen Elementen aus $\mathfrak{R}$ vertauschbar ist; ferner sei $e \in \mathfrak{R}$ auch Einselement für $\mathfrak{R}^*$. Damit liegen in $\mathfrak{R}^*$ auch alle Polynome

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n = \sum_{\nu=0}^{n} a_\nu x^\nu$$

mit nicht notwendig vom Nullelement o verschiedenen Koeffizienten $a_\nu \in \mathfrak{R}$, wobei für n jede natürliche Zahl zugelassen ist. Diese Zahl n kann für jeweils endlich viele Polynome als gleich angenommen werden, indem man gegebenenfalls einige Glieder mit dem Koeffizienten o hinzugefügt denkt.

Aus den in $\mathfrak{R}^*$ gültigen Gesetzen und den über das Element x gemachten Voraussetzungen folgen für diese Polynome die Rechenregeln:

(I) Es ist $\sum_{\nu=0}^{n} a_\nu x^\nu = \sum_{\nu=0}^{n} b_\nu x^\nu$ genau dann, wenn $a_\nu = b_\nu$ für alle ν;

(II) $\left(\sum_{\nu=0}^{n} a_\nu x^\nu\right) + \left(\sum_{\nu=0}^{n} b_\nu x^\nu\right) = \sum_{\nu=0}^{n} (a_\nu + b_\nu) x^\nu$;

(III) $\left(\sum_{\nu=0}^{n} a_\nu x^\nu\right) \cdot \left(\sum_{\mu=0}^{m} b_\mu x^\mu\right) = \sum_{\lambda=0}^{n+m} \left(\sum_{\nu+\mu=\lambda} a_\nu b_\mu\right) x^\lambda$.

In der Tat kennzeichnen diese Regeln genau das Rechnen mit Polynomen, wie man es etwa mit $\mathfrak{R} = \Delta$ schon von der Schulmathematik her gewohnt ist. Insbesondere entspricht die durch (I) beschriebene koeffizientenweise Gleichheit der Forderung, daß die

1) Wir bemerken, daß der Satz in der angegebenen Formulierung auch für einen Ring $\mathfrak{R}$ ohne Einselement e gilt. Die Forderung $e \in \mathfrak{R}$ hat jedoch den Vorteil, daß die Unbestimmte dann selbst im Polynomring enthalten ist. Dies vermeidet rein formale Schwierigkeiten insbesondere im zweiten Teil des Beweises (wie etwa Setzungen der Form $a_0 x^0 = a_0$, die bei Existenz eines Einselementes von selbst erfüllt sind) und macht die Überlegungen durchsichtiger.

Unbestimmte x keiner algebraischen Gleichung mit Koeffizienten aus $\mathfrak{R}$ genügt; denn $\Sigma a_\nu x^\nu = \Sigma b_\nu x^\nu$ ist ja gleichbedeutend mit $\Sigma (a_\nu - b_\nu) x^\nu = o$.

Wie man unmittelbar sieht, bildet die Gesamtheit der betrachteten Polynome einen Unterring $\mathfrak{S}$ von $\mathfrak{R}^*$. $\mathfrak{S}$ enthält in Gestalt der „Polynome" $a_0 + ox + ox^2 + \cdots$ alle Elemente von $\mathfrak{R}$ sowie insbesondere $x = o + ex + ox^2 + \cdots$.

2. Um nunmehr die Existenz eines Polynomringes unabhängig von der einschränkenden Voraussetzung unter 1. nachzuweisen, benutzen wir die dort gewonnenen strukturellen Einsichten. Jedes Polynom $f(x) \in \mathfrak{R}^*$ ist durch die Angabe seiner abzählbar unendlich vielen Koeffizienten aus $\mathfrak{R}$ bestimmt, von denen freilich nur endlich viele verschieden vom Nullelement sind. Auch die Addition und Multiplikation von Polynomen wird auf das Rechnen mit diesen Koeffizienten zurückgeführt. Es ist also möglich, die Polynome und ihre Verknüpfungen nur mit Hilfe von Elementen aus $\mathfrak{R}$ zu beschreiben und somit den Polynomring unabhängig von $\mathfrak{R}^*$ zu konstruieren.

Wir schaffen uns daher als neuen Rechenbereich die Gesamtheit $\overline{\mathfrak{S}}$ aller geordneten Elementensysteme

$$(a_0, a_1, a_2, \ldots)$$

mit abzählbar unendlich vielen Komponenten aus $\mathfrak{R}$, von denen nur endlich viele verschieden vom Nullelement sind. Dabei haben wir natürlich im Blick, daß a_ν die Rolle des Koeffizienten von x^ν übernehmen soll, vermeiden aber zunächst eine Schreibweise wie $\Sigma a_\nu x^\nu$, da diese nicht nur der erst zu erklärenden Addition und Multiplikation vorgreifen würde, sondern strenggenommen auch der Existenz einer Unbestimmten x mit den vorn beschriebenen Eigenschaften. Vielmehr sind die Verknüpfungen gerade so festzulegen, daß nachträglich $(a_0, a_1, a_2, \ldots)$ als $\Sigma a_\nu x^\nu$ gedeutet werden kann. Eine Anleitung geben uns dazu die Überlegungen unter 1., gemäß deren zu definieren ist:

(I) Es ist $(a_0, a_1, \ldots) = (a_0', a_1', \ldots)$ genau dann, wenn $a_i = a_i'$ für alle i;

(II) $(a_0, a_1, \ldots) + (b_0, b_1, \ldots) = (a_0 + b_0, a_1 + b_1, \ldots, a_i + b_i, \ldots)$;

(III) $(a_0, a_1, \ldots) \cdot (b_0, b_1, \ldots) = \left(a_0 b_0, a_0 b_1 + a_1 b_0, \ldots, \sum_{k+l=i} a_k b_l, \ldots\right)$.

Offensichtlich ist die in (I) erklärte Gleichheit reflexiv, symmetrisch und transitiv. Damit sind (II) und (III) eindeutige, nicht aus dem Bereich herausführende Verknüpfungen. Also haben wir von den Ringaxiomen bereits *A I* und *M I* nachgewiesen. Durch die komponentenweise Festsetzung in (II) überträgt sich jeweils die Gültigkeit von *A II*, *A III* und *A IV* von $\mathfrak{R}$ auf den Bereich $\overline{\mathfrak{S}}$ der betrachteten Elementensysteme. Die Assoziativität und Distributivität der durch (III) festgelegten Multiplikation ergeben sich durch Ausrechnung:

M II:

$$\begin{aligned}((.., a_i, ..)\,(.., b_i, ..))\,(.., c_i, ..) &= \Big(.., \sum_{k+l=i} a_k b_l, ..\Big)(.., c_i, ..)\\ &= \Big(.., \sum_{m+n=i} \Big(\sum_{k+l=m} a_k b_l\Big) c_n, ..\Big)\\ &= \Big(.., \sum_{k+l+n=i} a_k b_l c_n, ..\Big),\\ (.., a_i, ..)\,((.., b_i, ..)\,(.., c_i, ..)) &= (.., a_i, ..)\Big(.., \sum_{l+n=i} b_l c_n, ..\Big)\\ &= \Big(.., \sum_{k+m=i} a_k \Big(\sum_{l+n=m} b_l c_n\Big), ..\Big)\\ &= \Big(.., \sum_{k+l+n=i} a_k b_l c_n, ..\Big);\end{aligned}$$

D:

$$\begin{aligned}(.., a_i, ..)\,((.., b_i, ..) + (.., c_i, ..)) &= (.., a_i, ..)\,(.., b_i + c_i, ..)\\ &= \Big(.., \sum_{k+l=i} a_k (b_l + c_l), ..\Big)\\ &= \Big(.., \sum_{k+l=i} a_k b_l + \sum_{k+l=i} a_k c_l, ..\Big)\\ &= \Big(.., \sum_{k+l=i} a_k b_l, ..\Big) + \Big(.., \sum_{k+l=i} a_k c_l, ..\Big)\\ &= (.., a_i, ..)\,(.., b_i, ..) + (.., a_i, ..)\,(.., c_i, ..).\end{aligned}$$

Entsprechend verläuft der Beweis der zweiten Relation des distributiven Gesetzes.

Die Gesamtheit $\overline{\mathfrak{S}}$ der geordneten Elementensysteme $(a_0, a_1, \ldots)$ wird also vermöge der Festsetzungen (I), (II), (III) zu einem Ring. Wie man sich leicht überzeugt, bilden die speziellen Elementensysteme $(a, o, o, \ldots)$ vermöge der Zuordnung

$$a \to (a, o, o, \ldots)$$

einen zu $\mathfrak{R}$ isomorphen Unterring $\overline{\mathfrak{R}} \subseteq \overline{\mathfrak{S}}$. Durch Ersetzung von $(a, o, o, \ldots)$ durch a gemäß S(29.5) erhält man einen zu $\overline{\mathfrak{S}}$ isomorphen Oberring $\mathfrak{S}$ von $\mathfrak{R}$.

Dieser Ring $\mathfrak{S}$ kann als Polynomring über $\mathfrak{R}$ aufgefaßt werden. Er enthält nämlich ein Element x, das in dem vorn erklärten Sinne Unbestimmte über $\mathfrak{R}$ ist und gestattet, alle Elemente aus $\mathfrak{S}$ als Polynome in x zu schreiben. Ein solches Element ist

$$x = (o, e, o, \ldots).$$

Dazu beweist man zunächst durch vollständige Induktion (Aufg. 3), daß $x^i (i > 0)$ gleich demjenigen Elementensystem ist, in dem alle Komponenten bis auf die i-te Komponente[1]) verschwinden, während letztere gleich e ist:

$$x^i = (o, \ldots, o, \underset{\underset{i}{\smile}}{e}, o, \ldots).$$

Damit gilt für alle Elemente aus $\mathfrak{S}$:

$$\begin{aligned}(a_0, a_1, a_2, \ldots) &= (a_0, o, o, \ldots) + (o, a_1, o, \ldots) + (o, o, a_2, \ldots) + \ldots \\ &= a_0 + a_1(o, e, o, \ldots) + a_2(o, o, e, \ldots) + \ldots \\ &= a_0 + a_1 x + a_2 x^2 + \ldots .\end{aligned}$$

Dabei ist $x = (o, e, o, \ldots)$ tatsächlich eine Unbestimmte, da aus

$$\begin{aligned}&b_0 + b_1 x + \cdots + b_m x^m = o, \text{ also aus} \\ &(b_0, b_1, \ldots, b_m, \ldots) = (o, o, \ldots, o, \ldots)\end{aligned}$$

das Verschwinden aller Koeffizienten folgt. Abschließend bemerken wir, daß wegen

$$(a, o, o, \ldots)\,(o, e, o, \ldots) = (o, e, o, \ldots)\,(a, o, o, \ldots)$$

die Unbestimmte x mit allen Elementen aus $\mathfrak{R}$ vertauschbar ist. qed.

Satz **S (32.2)**

Über einem Ring $\mathfrak{R}$ mit Einselement ist der Polynomring in einer Unbestimmten durch $\mathfrak{R}$ bis auf Isomorphie eindeutig bestimmt. Er ist der kleinste den Ring $\mathfrak{R}$ und diese Unbestimmte enthaltende Ring. Dagegen können mehrere (zwar isomorphe, aber verschiedene) Polynomringe über $\mathfrak{R}$ in einem gemeinsamen Oberring enthalten sein.

---

1) Man beachte, daß die Abzählung der Komponenten mit 0 beginnt.

Beweis

Die Eindeutigkeitsaussage folgt aus unseren Betrachtungen im ersten Teil des obigen Beweises, nach denen das Rechnen in Polynomringen vermöge der Regeln (I), (II), (III) bereits durch Rechenoperationen mit den Koeffizienten aus $\mathfrak{R}$ festgelegt ist (vgl. auch Aufg. 4). Ferner enthält jeder Ring $\mathfrak{R}^*$ mit $\mathfrak{R}$ und einer Unbestimmten auch alle Polynome in dieser Unbestimmten. Dagegen kann ein solcher Oberring durchaus mehrere voneinander verschiedene Unbestimmte und damit die zugehörigen Polynomringe enthalten. qed.

Unsere bisherigen Überlegungen zeigen, daß man einen beliebigen Ring $\mathfrak{R}$ mit Einselement durch Hinzunahme einer Unbestimmten zu einem Oberring erweitern kann. Dieser Oberring ist seiner Struktur nach eindeutig bestimmt als der Ring aller Polynome in dieser Unbestimmten mit Koeffizienten aus $\mathfrak{R}$. Man nennt diesen Vorgang die *Adjunktion einer Unbestimmten* x zum Ring $\mathfrak{R}$ und bezeichnet den entstehenden Polynomring mit $\mathfrak{R}[x]$.

Das Rechnen in $\mathfrak{R}[x]$ verläuft gemäß den in Ringen üblichen Regeln unter Berücksichtigung der Vertauschbarkeit von x mit allen Elementen von $\mathfrak{R}$. Insbesondere ist also $\mathfrak{R}[x]$ genau dann kommutativ, wenn $\mathfrak{R}$ es ist. Wir bemerken schließlich, daß man unter dem *Grad des Polynoms* $f(x) = \sum a_\nu x^\nu \neq o$ den Exponenten der höchsten Potenz von x versteht, deren Koeffizient nicht verschwindet. Dieser Koeffizient wird auch höchster Koeffizient oder Anfangskoeffizient genannt.

Dem Nullelement o des Polynomringes $\mathfrak{R}[x]$ pflegt man im allgemeinen keinen Grad zuzuordnen. Es ist aber zur Vermeidung von Fallunterscheidungen üblich, bei abschätzenden Gradaussagen wie etwa „Der Grad von $f(x)$ ist kleiner als n" oder „$f(x)$ ist höchstens vom Grad n" zuzulassen, daß $f(x)$ auch gleich o sein kann.

Weiterhin können wir unsere Überlegungen nunmehr auf den Fall anwenden, daß unser Ausgangsring selbst schon ein Polynomring $\mathfrak{R}[x_1]$ in einer Unbestimmten x_1 über $\mathfrak{R}$ ist. Dann lehren unsere Sätze die Existenz eines Polynomringes $\mathfrak{R}[x_1][x_2]$ in einer Unbestimmten x_2 über $\mathfrak{R}[x_1]$. Seine Elemente sind Polynome

$$F(x_2) = \sum_{\nu_2} A_{\nu_2} x_2^{\nu_2}$$

mit Koeffizienten $A_{\nu_2} = \sum_{\nu_1} a_{\nu_1 \nu_2} x_1^{\nu_1}$, die Polynome aus $\mathfrak{R}[x_1]$ sind.

Das ergibt eingesetzt:

$$F(x_2) = f(x_1, x_2) = \sum_{\nu_2} \left(\sum_{\nu_1} a_{\nu_1 \nu_2} x_1^{\nu_2} \right) x_2^{\nu_1} = \sum_{\nu_1, \nu_2} a_{\nu_1 \nu_2} x_1^{\nu_1} x_2^{\nu_2}.$$

Diese letzte Schreibweise wird dadurch gerechtfertigt, daß in der Tat x_1 und x_2 bezüglich $\mathfrak{R}$ die gleiche Rolle spielen: Bisher wissen wir nur, daß x_1 Unbestimmte über $\mathfrak{R}$ und x_2 Unbestimmte über $\mathfrak{R}[x_1]$ ist; wir werden zeigen, daß auch umgekehrt x_2 Unbestimmte über $\mathfrak{R}$ und x_1 Unbestimmte über $\mathfrak{R}[x_2]$ ist. Aus einer Relation

$$\sum_{\nu_2} A_{\nu_2} x_2^{\nu_2} = o$$

folgt nämlich nach Voraussetzung über x_2 das Verschwinden aller Koeffizienten $A_{\nu_2} \in \mathfrak{R}[x_1]$, also erst recht das Verschwinden von solchen Koeffizienten, die schon in $\mathfrak{R}$ liegen. Also ist x_2 Unbestimmte über $\mathfrak{R}$, d. h., in $\mathfrak{R}[x_1][x_2]$ ist der Polynomring $\mathfrak{R}[x_2]$ enthalten. Über diesem Polynomring $\mathfrak{R}[x_2]$ ist x_1 Unbestimmte, denn aus jeder Relation

$$\sum_{\nu_1} B_{\nu_1} x_1^{\nu_1} = o \quad \text{mit} \quad B_{\nu_1} = \sum_{\nu_2} b_{\nu_1 \nu_2} x_2^{\nu_2} \in \mathfrak{R}[x_2]$$

folgt in $\mathfrak{R}[x_1][x_2]$ unter Verwendung der Vertauschbarkeit von x_1 und x_2 wegen

$$\sum_{\nu_1} \left(\sum_{\nu_2} b_{\nu_1 \nu_2} x_2^{\nu_2} \right) x_1^{\nu_1} = \sum_{\nu_2} \left(\sum_{\nu_1} b_{\nu_1 \nu_2} x_1^{\nu_1} \right) x_2^{\nu_2} = o$$

nach Voraussetzung über x_2 (Unbestimmte über $\mathfrak{R}[x_1]$) zunächst $\sum_{\nu_1} b_{\nu_1 \nu_2} x_1^{\nu_1} = o$ für alle ν_2 und damit nach Voraussetzung über x_1 (Unbestimmte über $\mathfrak{R}$) $b_{\nu_1 \nu_2} = o$ für alle ν_1 und ν_2, also $B_{\nu_1} = o$ für alle ν_1.

Damit können wir zusammenfassend feststellen, daß für die fortgesetzte Bildung von Polynomringen

$$\mathfrak{R}[x_1][x_2] = \mathfrak{R}[x_2][x_1]$$

gilt und wir die Eigenschaften der Elemente x_1 und x_2 bezüglich $\mathfrak{R}$ festlegen können durch:

1) Sowohl x_1 als auch x_2 ist Unbestimmte über $\mathfrak{R}$.
2) x_1 und x_2 sind *voneinander unabhängige Unbestimmte über* $\mathfrak{R}$ in dem Sinne, als eine Gleichung

$$f(x_1, x_2) = \sum_{\nu_1, \nu_2} a_{\nu_1 \nu_2} x_1^{\nu_1} x_2^{\nu_2} = o$$

das Verschwinden alle r Koeffizienten $a_{\nu_1 \nu_2} \in \mathfrak{R}$ nach sich zieht

Demzufolge nennt man den Ring $\mathfrak{R}[x_1][x_2]$ einfach den durch *Adjunktion der voneinander unabhängigen Unbestimmten x_1 und x_2 über $\mathfrak{R}$ entstehenden Polynomring* $\mathfrak{R}[x_1, x_2]$. Er ist seiner Struktur nach vollständig bestimmt als der Ring aller Polynome mit Koeffizienten aus $\mathfrak{R}$ in zwei Unbestimmten, die untereinander und mit den Elementen von $\mathfrak{R}$ kommutativ multiplizierbar sind und der obengenannten Bedingung 2) genügen.

In Ausdehnung dieser Überlegungen ergibt sich

Satz **S (32.3)**

Es sei $\mathfrak{R}$ ein beliebiger Ring mit Einselement. Dann gibt es einen $\mathfrak{R}$ umfassenden Polynomring

$$\mathfrak{R}[x_1, x_2, \ldots, x_n]$$

in n (voneinander unabhängigen[1])) Unbestimmten $x_1, x_2, \ldots, x_n$ über $\mathfrak{R}$, dessen Elemente genau alle Polynome

$$f(x_1, x_2, \ldots, x_n) = \sum_{\nu_1, \ldots, \nu_n} a_{\nu_1 \nu_2 \ldots \nu_n} x_1^{\nu_1} x_2^{\nu_2} \ldots x_n^{\nu_n}$$

in diesen Unbestimmten mit Koeffizienten $a_{\nu_1 \nu_2 \ldots \nu_n}$ aus $\mathfrak{R}$ sind. Dieser Polynomring ist durch $\mathfrak{R}$ und die Anzahl n der Unbestimmten bis auf Isomorphie eindeutig bestimmt, und er ist der kleinste Ring, der $\mathfrak{R}$ und diese n Unbestimmten enthält.

Die Kommutativität von $\mathfrak{R}$ ist ebenfalls wieder notwendig und hinreichend für die Kommutativität von $\mathfrak{R}[x_1, x_2, \ldots, x_n]$.

Um den Gradbegriff auch auf Polynome in mehreren Unbestimmten zu übertragen, erklären wir zunächst den *Grad eines Gliedes*

$$a_{\nu_1 \nu_2 \ldots \nu_n} x_1^{\nu_1} x_2^{\nu_2} \ldots x_n^{\nu_n} \neq 0$$

von $f(x_1, x_2, \ldots, x_n)$ als die Exponentensumme $\nu_1 + \nu_2 + \cdots + \nu_n$. Unter dem *Grad des Polynoms* $f(x_1, x_2, \ldots, x_n) \neq 0$ versteht man dann das Maximum der Grade seiner Glieder. Dabei ist es möglich, daß alle Glieder eines Polynoms in n Unbestimmten den gleichen Grad m haben, der dann also mit dem Grad des Polynoms übereinstimmt. In diesem Falle spricht man von einem *homogenen Polynom* oder einer *Form*, genauer von einer *n-ären Form m-ten*

1) Es ist üblich, unter n Unbestimmten stillschweigend n voneinander unabhängige Unbestimmte zu verstehen.

Grades. Wir erwähnen in diesem Zusammenhange, daß sich jedes Polynom in n Unbestimmten als Summe von n-ären Formen schreiben läßt und daß das Produkt zweier Formen in n Unbestimmten wieder eine solche ist (vgl. Aufg. 6).

Weitere wichtige Aussagen über Polynomringe erhalten wir mit dem folgenden

Satz **S (32.4)**

Über einem nullteilerfreien Ring sind alle Polynomringe ebenfalls nullteilerfrei.

Beweis

Wir zeigen den Satz zunächst für $\mathfrak{R}[x]$. Es seien $f(x) \neq o$ und $g(x) \neq o$ zwei Polynome mit den höchsten Koeffizienten a_r bzw. b_s. Dann ist der höchste Koeffizient des Produktes $f(x) \cdot g(x)$ offensichtlich $a_r b_s$, da $a_r b_s$ wegen der Nullteilerfreiheit von $\mathfrak{R}$ nicht verschwindet. Also ist $f(x) \cdot g(x) \neq o$.

Dieses Ergebnis überträgt sich sofort durch vollständige Induktion auf $\mathfrak{R}[x_1, x_2, \ldots, x_n]$. qed.

Folgerung **F (32.5)**

In beliebigen Polynomringen gilt:

a) *Der Grad der Summe von Polynomen ist kleiner oder gleich dem Maximum der Grade der Summanden*[1]).

b) *Der Grad des Produktes von Polynomen ist kleiner oder gleich der Summe der Grade der Faktoren.*

Für nullteilerfreie Koeffizientenbereiche liegt bei b) *sogar stets Gleichheit vor.*

Beweis

Die Behauptung a) ist klar. Bei b) dürfen wir uns auf zwei Faktoren $f(x_1, x_2, \ldots, x_n)$ vom Grade r und $g(x_1, x_2, \ldots, x_n)$ vom Grade s beschränken. Es sei $\bar{f}(x_1, x_2, \ldots, x_n)$ bzw. $\bar{g}(x_1, x_2, \ldots, x_n)$ jeweils die Summe der Glieder vom Grade r bzw. s, also jeweils der höchste

1) Gleichheit tritt jedenfalls dann ein, wenn das Maximum nur von einem Summanden angenommen wird.

homogene Bestandteil von f bzw. g; im Falle $n = 1$ ist also einfach $\bar{f} = a_r x^r$ und $\bar{g} = b_s x^s$. Falls nun $\mathfrak{R}[x_1, x_2, \ldots, x_n]$ nullteilerfrei ist, kann das Produkt $\bar{f} \cdot \bar{g}$ nicht verschwinden und liefert offensichtlich die Glieder höchsten Grades von $f \cdot g$, nämlich Glieder vom Grad $r + s$. Beim Auftreten von Nullteilern ist jedoch $\bar{f} \cdot \bar{g} = o$ möglich, womit der Grad von $f \cdot g$ kleiner als $r + s$ wird. qed.

Die Möglichkeiten, von der algebraischen Auffassung der ganzen rationalen Funktion (auch in mehreren Unbestimmten) zum Funktionsbegriff der Analysis (entsprechend ebenfalls in mehreren Variablen) überzugehen, umfaßt das folgende

Einsetzungsprinzip **S (32.6)**

Man kann für die Unbestimmten $x_1, x_2, \ldots, x_n$ in jedes Polynom $f(x_1, x_2, \ldots, x_n) \in \mathfrak{R}[x_1, x_2, \ldots, x_n]$ Elemente $\xi_1\ \xi_2, \ldots, \xi_n$ aus einem Oberring $\mathfrak{R}^*$ von $\mathfrak{R}$ einsetzen, falls $e\,\xi_i = \xi_i$ gilt (e Einselement von $\mathfrak{R}$) und die ξ_i untereinander und mit den Elementen aus $\mathfrak{R}$ vertauschbar sind.

Bei dieser Einsetzung gehen alle Gleichheits- und Verknüpfungsrelationen zwischen Polynomen aus $\mathfrak{R}[x_1, x_2, \ldots, x_n]$ in ebensolche Relationen zwischen Elementen von $\mathfrak{R}^*$ über. Allerdings können unter Umständen dabei weitere Gleichheiten entstehen.

Ist insbesondere $\mathfrak{R}^*$ ein Integritätsbereich mit Einselement, so sind $\xi_1, \xi_2, \ldots, \xi_n$ beliebig aus $\mathfrak{R}^*$ wählbar.

Beweis

Aus dem Polynom $f(x_1, x_2, \ldots, x_n) \in \mathfrak{R}[x_1, x_2, \ldots, x_n]$ wird durch Einsetzung von $\xi_1, \xi_2, \ldots, \xi_n$ aus $\mathfrak{R}^*$ ein eindeutig bestimmtes Element $f(\xi_1, \xi_2, \ldots, \xi_n) \in \mathfrak{R}^*$. $f(\xi_1, \xi_2, \ldots, \xi_n)$ ist also im Sinne der Analysis der Wert der Funktion $f(x_1, x_2, \ldots, x_n)$ für das Argumentsystem $\xi_1, \xi_2, \ldots, \xi_n$. Dabei gilt:

Aus $f(x_1, \ldots, x_n) = g(x_1, \ldots, x_n)$
folgt $f(\xi_1, \ldots, \xi_n) = g(\xi_1, \ldots, \xi_n)$.

Aus $f(x_1, \ldots, x_n) + g(x_1, \ldots, x_n) = h(x_1, \ldots, x_n)$
folgt $f(\xi_1, \ldots, \xi_n) + g(\xi_1, \ldots, \xi_n) = h(\xi_1, \ldots, \xi_n)$.

Aus $f(x_1, \ldots, x_n) \cdot g(x_1, \ldots, x_n) = h(x_1, \ldots, x_n)$
folgt $f(\xi_1, \ldots, \xi_n) \cdot g(\xi_1, \ldots, \xi_n) = h(\xi_1, \ldots, \xi_n)$.

Es wird nämlich nach Voraussetzung mit den Elementen $\xi_1, \xi_2, \ldots, \xi_n$ in $\mathfrak{R}^*$ ebenso gerechnet wie mit den Unbestimmten $x_1, x_2, \ldots, x_n$ in $\mathfrak{R}[x_1, x_2, \ldots, x_n]$. Die Möglichkeit der Entstehung neuer Gleichheiten lehrt etwa das folgende Beispiel:

Es sei $\mathfrak{R} = \mathfrak{R}^* = \Gamma$. Dann ist

$$f(x) = 3x^2 + 2 + 4x + 6 = g(x)$$

aber für $\xi = 2$

$$f(2) = 3 \cdot 2^2 + 2 = 4 \cdot 2 + 6 = g(2).$$

Für den Spezialfall, daß $\mathfrak{R}^*$ ein Integritätsbereich mit Einselement e^* ist, bleibt wegen der Kommutativität nur $e\xi = \xi$ für alle $\xi \in \mathfrak{R}^*$ zu zeigen. Letzteres folgt aber aus $e^* = e$ wegen $e^*e = e = ee$ und der Nullteilerfreiheit von $\mathfrak{R}^*$. qed.

Im Falle kommutativer, nullteilerfreier Koeffizientenbereiche lassen sich die entsprechenden Betrachtungen auf gebrochen rationale Funktionen übertragen. Man kann dann nämlich wegen S(32.4) zum Quotientenkörper von $\mathfrak{R}[x]$ bzw. $\mathfrak{R}[x_1, x_2, \ldots, x_n]$ übergehen, dessen Elemente Quotienten

$$\varphi(x) = \frac{\sum a_\nu x^\nu}{\sum b_\mu x^\mu} \quad \text{bzw.} \quad \varphi(x_1, \ldots, x_n) = \frac{\sum a_{\nu_1 \nu_2 \ldots \nu_n} x_1^{\nu_1} x_2^{\nu_2} \ldots x_n^{\nu_n}}{\sum b_{\mu_1 \mu_1 \ldots \mu_n} x_1^{\mu_1} x_2^{\mu_2} \ldots x_n^{\mu_n}}$$

mit nicht verschwindendem Nenner sind. Für sie gilt dann das gleiche Einsetzungsprinzip mit der Einschränkung, daß die auftretenden Nenner bei der Einsetzung der ξ_i nicht o werden dürfen. Übrigens kann man diesen Übergang in zwei Schritten vornehmen, indem man zunächst den Quotientenkörper $\mathfrak{K}$ von $\mathfrak{R}$ und dann den Quotientenkörper von $\mathfrak{K}[x]$ bzw. $\mathfrak{K}[x_1, x_2, \ldots, x_n]$ bildet. Man bezeichnet den so erhaltenen Quotientenkörper mit $\mathfrak{K}(x)$ bzw. $\mathfrak{K}(x_1, x_2, \ldots, x_n)$ und spricht von der *Körperadjunktion von einer bzw. mehreren Unbestimmten* zu $\mathfrak{K}$, die also von der vorn eingeführten Ringadjunktion $\mathfrak{K}[x]$ bzw. $\mathfrak{K}[x_1, x_2, \ldots, x_n]$ wohl zu unterscheiden ist. Dieser geschickte Bezeichnungsunterschied durch eckige bzw. runde Klammern hat sich allgemein eingebürgert und gestattet, in beiden Fällen abkürzend einfach von Adjunktion zu sprechen.

Im Zusammenhang mit den Untersuchungen im nächsten Paragraphen wird sich die Adjunktion von Unbestimmten als entscheidendes Hilfsmittel für wesentlich allgemeinere Ringerweiterungen herausstellen.

Aufgaben zu § 32

1. Man zeige durch Beispiele, daß „Unbestimmte" ein Relativbegriff bezüglich des zugrunde gelegten Ringes ist.
2. Im Unterschied zur Addition (II) wird die Multiplikation (III) in Polynomringen nicht komponentenweise erklärt. Wie wirkt sich dies auf die entsprechenden Nachweise der Ringaxiome aus?
3. Man beweise $(o, e, o, \ldots)^i = (o, \ldots, o, \overset{i}{\smile} e, o, \ldots)$ entsprechend den Ausführungen im Beweis von S (32.1).
4. Es seien $\mathfrak{R}$ und $\overline{\mathfrak{R}}$ zwei zueinander isomorphe Ringe mit Einselement. Dann sind auch die Polynomringe in einer Unbestimmten über $\mathfrak{R}$ bzw. $\overline{\mathfrak{R}}$ zueinander isomorph. Man beweise dies unter Angabe einer Zuordnung der Elemente.
5. Auf den ersten Blick erstaunlich ist folgender Sachverhalt: Jeder Polynomring $\mathfrak{R}[x]$ enthält unendlich viele echt ineinander enthaltene, zu $\mathfrak{R}[x]$ isomorphe Unterringe.
6. Das Produkt homogener Polynome in n Unbestimmten ist wieder homogen.
7. Faßt man die Unbestimmte x als erzeugendes Element des Polynomringes $\mathfrak{R}[x]$ auf, so sind folgende Wechsel des erzeugenden Elementes möglich:
   a) Ist $\mathfrak{R}$ ein beliebiger Ring, so gilt für jedes a aus $\mathfrak{R}$
   $$\mathfrak{R}[x] = \mathfrak{R}[a + x].$$
   b) Ist $\mathfrak{K}$ ein beliebiger Körper, so gilt für jedes a und $b \neq o$ aus $\mathfrak{K}$
   $$\mathfrak{K}[x] = \mathfrak{K}[a + bx].$$
   Im Fall b) gilt bei kommutativem Körper $\mathfrak{K}$ für den Quotientenkörper $\mathfrak{K}(x)$ von $\mathfrak{K}[x]$ sogar
   $$\mathfrak{K}(x) = \mathfrak{K}\left(\frac{a + bx}{c + dx}\right),$$
   falls die Elemente a, b, c, d aus $\mathfrak{K}$ der Bedingung $ad - bc \neq o$ genügen.
8. Es sei Π_p der Restklassenkörper von Γ modulo p. Dann gilt im Polynomring $\Pi_p[x]$ stets die Beziehung
   $$f(x^p) = (f(x))^p$$

§ 33. Homomorphie

Parallel zu den entsprechenden Überlegungen in der Gruppentheorie, deren Wiederholung wir an dieser Stelle empfehlen, verallgemeinern wir auch für Ringe den Begriff der isomorphen Abbildung. Dies wird uns neben der Möglichkeit, aus einem Ring $\mathfrak{R}$ durch Abbildungen neue Ringe zu erhalten, strukturelle Einsichten über den Ring $\mathfrak{R}$ selbst vermitteln.

Definition **D (33.1)**

Es sei $\mathfrak{R}$ ein beliebiger Ring und $\overline{\mathfrak{R}}$ eine Menge, in der zwei eindeutige Verknüpfungen (Addition und Multiplikation) erklärt sind.

Dann heißt $\mathfrak{R}$ homomorph abgebildet auf $\overline{\mathfrak{R}}$, in Zeichen $\mathfrak{R} \overset{\sim}{\to} \overline{\mathfrak{R}}$, wenn eine eindeutige Abbildung von $\mathfrak{R}$ auf $\overline{\mathfrak{R}}$ vermöge der Zuordnung

$$a \to \bar{a} \text{ mit } a \in \mathfrak{R},\ \bar{a} \in \overline{\mathfrak{R}}$$

vorliegt, die relationstreu bezüglich beider Verknüpfungen ist:

$$\left.\begin{aligned} \overline{a+b} &= \bar{a} + \bar{b} \\ \overline{a \cdot b} &= \bar{a} \cdot \bar{b} \end{aligned}\right\} \text{ für alle } a \text{ und } b \text{ aus } \mathfrak{R}.$$

Man nennt die Abbildung selbst einen Homomorphismus, $\mathfrak{R}$ das Original und $\overline{\mathfrak{R}}$ das homomorphe Bild.

Auch für homomorphe Ringabbildungen ergeben sich die in D (18.5) für homomorphe Gruppenabbildungen zusammengestellten acht Möglichkeiten und Begriffsbildungen, die genau wie dort benannt werden. Alle diese Abbildungen ergeben bei Nacheinanderausführung Abbildungen der gleichen Art, während eine inverse Abbildung natürlich nur bei Isomorphismen bzw. Automorphismen vom isomorphen Bild auf das Original möglich ist, die dann wieder eine Abbildung der gleichen Art darstellt.

Die im § 29 behauptete Übertragung der Gesetzmäßigkeiten vom Original auf das isomorphe Bild findet nun im wesentlichen bereits bei homomorphen Abbildungen statt.

Folgerung **F (33.2)**

Das homomorphe Bild $\overline{\mathfrak{R}}$ eines Ringes $\mathfrak{R}$ ist selbst ein Ring. Dabei überträgt sich etwaige Kommutativität und Körpereigenschaft[1]).

Den Beweis dieser wie der nächsten Aussage überlassen wir dem Leser (vgl. Aufg. 1).

---

1) Letzteres abgesehen von der trivialen Nullabbildung, bei der alle Elemente $a \in \mathfrak{R}$ auf das Nullelement $o \in \overline{\mathfrak{R}}$ abgebildet werden.

Folgerung **F (33.3)**

Es sei $\overline{\mathfrak{R}}$ das homomorphe Bild eines Ringes $\mathfrak{R}$. Dann gilt:

a) *Das Nullelement von $\mathfrak{R}$ wird auf das Nullelement von $\overline{\mathfrak{R}}$ und das zu $a \in \mathfrak{R}$ entgegengesetzte Element auf das zu $\bar{a} \in \overline{\mathfrak{R}}$ entgegengesetzte Element abgebildet.*

b) *Jedes (eventuell existierende) Linkseinselement von $\mathfrak{R}$ wird auf ein Linkseinselement von $\overline{\mathfrak{R}}$ abgebildet. Entsprechendes gilt (soweit vorhanden) für jedes Rechtseinselement und damit für das Einselement von $\mathfrak{R}$.*

c) *Falls $\mathfrak{R}$ und damit $\overline{\mathfrak{R}}$ ein Einselement besitzen, wird jedes (eventuell existierende) Linksinverse von $a \in \mathfrak{R}$ auf ein Linksinverses von $\bar{a} \in \overline{\mathfrak{R}}$ abgebildet. Entsprechendes gilt wieder (soweit vorhanden) für Rechtsinverse und damit für Inverse.*

Beispiel **B (33.4)**

Der bereits in B (26.3) eingeführte Restklassenring $\overline{\mathfrak{R}}$ von Γ mod m ist homomorphes Bild von $\mathfrak{R} = \Gamma$ vermöge der Zuordnung

$$a \to \bar{a} = [a].$$

Die Eindeutigkeit dieser Zuordnung und die Relationstreue bezüglich der Addition wurde bereits in B (18.4c) nachgewiesen. Es gilt aber auch

$$\bar{a} \cdot \bar{b} = [a] \cdot [b] = [a \cdot b] = \overline{a \cdot b}$$

nach der Definition der Restklassenmultiplikation. Damit ergibt sich die Ringeigenschaft der Menge der Restklassen mod m erneut unmittelbar aus F (33.2).

Unser nächstes Ziel ist der S (18.11) entsprechende Homomorphiesatz für Ringe. Auch die zu ihm führenden Überlegungen verlaufen parallel den Erörterungen in § 18, nur daß die Rolle der Normalteiler in der Gruppentheorie hier von den zweiseitigen Idealen des entsprechenden Ringes übernommen wird.

Zunächst gilt S (18.7) offensichtlich für eindeutige Abbildungen beliebiger Mengen, also auch für Ringe:

Satz **S (33.5)**

Jede homomorphe Abbildung eines Ringes $\mathfrak{R}$ auf einen Ring $\overline{\mathfrak{R}}$ vermittelt eine Klasseneinteilung von $\mathfrak{R}$ in Klassen $\mathfrak{A}, \mathfrak{B}, \ldots$ bildgleicher Elemente.

Satz **S (33.6)**

Die Klasse $\mathfrak{m}$ *derjenigen Elemente* $m, m', \ldots$ *von* $\mathfrak{R}$, *die bei dem Homomorphismus* $\mathfrak{R} \overset{\sim}{\longrightarrow} \overline{\mathfrak{R}}$ *auf das Nullelement* $\bar{o} \in \overline{\mathfrak{R}}$ *abgebildet werden, ist ein eindeutig bestimmtes zweiseitiges Ideal von* $\mathfrak{R}$ *und heißt der Kern dieses Homomorphismus. Die übrigen Klassen bildgleicher Elemente von* $\mathfrak{R}$ *sind genau die Restklassen der additiven Gruppe* $\mathfrak{R}^+$ *von* $\mathfrak{R}$ *nach dem Ideal* $\mathfrak{m}$, *aufgefaßt als Untermodul von* $\mathfrak{R}^+$.

Beweis

Es bleibt wegen S (18.8), angewendet auf $\mathfrak{R}^+$, nur zu zeigen, daß $\mathfrak{m}$ nicht nur Untermodul[1]) von $\mathfrak{R}^+$, sondern sogar zweiseitiges Ideal von $\mathfrak{R}$ ist. Das folgt aus

$$\left.\begin{aligned} \overline{r \cdot m} &= \bar{r} \cdot \overline{m} = \bar{r} \cdot \bar{o} = \bar{o} \\ \overline{m \cdot r} &= \overline{m} \cdot \bar{r} = \bar{o} \cdot \bar{r} = \bar{o} \end{aligned}\right\} \text{ für alle } m \in \mathfrak{m}, r \in \mathfrak{R}.$$

qed.

Satz **S (33.7)**

a) *Faßt man die Restklassen* $a + \mathfrak{m} = [a]$ *von* $\mathfrak{R}^+$ *nach irgendeinen zweiseitigen Ideal* $\mathfrak{m}$ *von* $\mathfrak{R}$ *als Elemente einer neuen Menge auf, die nach den beiden Vorschriften*

$$(*) \qquad \begin{aligned} [a] + [b] &= [a + b] \\ [a] \cdot [b] &= [a \cdot b] \end{aligned}$$

zu verknüpfen sind, so bildet diese Menge einen Ring, den sogenannten Restklassenring $\mathfrak{R}/\mathfrak{m}$ *von* $\mathfrak{R}$ *nach* $\mathfrak{m}$.

b) *Der Ring* $\mathfrak{R}$ *wird auf den Restklassenring* $\mathfrak{R}/\mathfrak{m}$ *homomorph abgebildet vermöge der Zuordnung* $a \to [a]$. *Der Kern dieses Homomorphismus ist* $\mathfrak{m}$, *die Abbildung wird wieder der natürliche Homomorphismus von* $\mathfrak{R}$ *bezüglich* $\mathfrak{m}$ *genannt.*

Beweis

Wegen F (33.2) genügt es nachzuweisen, daß durch (*) in der Menge der Restklassen eine eindeutige Addition und eine eindeutige Multiplikation erklärt werden und daß $\mathfrak{R}$ homomorph auf diese Menge abgebildet wird.

---

1) Man beachte, daß in abelschen Gruppen jede Untergruppe auch Normalteiler ist.

Es ist also zunächst die Unabhängigkeit der in (*) festgelegten Verknüpfungen von der speziellen Wahl der Repräsentanten zu zeigen. Das folgt für die Addition bereits aus der Moduleigenschaft von $\mathfrak{m}$[1]: Ist nämlich $[a] = [a']$, also $a - a' \in \mathfrak{m}$, und $[b] = [b']$, also $b - b' \in \mathfrak{m}$, so gilt

$$(a - a') + (b - b') = (a + b) - (a' + b') \in \mathfrak{m}, \text{ also } [a + b] = [a' + b'].$$

Bei der Überlegung für die Multiplikation gehen auch die übrigen Eigenschaften des zweiseitigen Ideals $\mathfrak{m}$ ein: Aus $a - a' \in \mathfrak{m}$ und $b - b' \in \mathfrak{m}$ ergibt sich

$$ab - a'b = (a - a')b \in \mathfrak{m} \quad \text{und} \quad a'b - a'b' = a'(b - b') \in \mathfrak{m}$$

und damit auch

$$(ab - a'b) + (a'b - a'b') = ab - a'b' \in \mathfrak{m}, \text{ also } [a \cdot b] = [a' \cdot b'].$$

Die Zuordnung $a \to [a]$ vermittelt offensichtlich eine eindeutige Abbildung von $\mathfrak{R}$ auf die Menge der Restklassen. Die Relationstreue spiegelt sich in den Verknüpfungen (*) unmittelbar wider.

qed.

Satz **S (33.8)**

Es sei $\mathfrak{R} \xrightarrow{\sim} \overline{\mathfrak{R}}$ *ein Homomorphismus vermöge der Zuordnung* $a \to \bar{a}$ *mit dem Kern* $\mathfrak{m}$. *Dann ist* $\overline{\mathfrak{R}}$ *isomorph zum Restklassenring* $\mathfrak{R}/\mathfrak{m}$ *vermöge der Zuordnung* $\bar{a} \to [a] = \varphi(\bar{a})$.

Umgekehrt ist jedes isomorphe Bild $\overline{\mathfrak{R}}$ *des Restklassenringes* $\mathfrak{R}/\mathfrak{m}$ *ein homomorphes Bild von* $\mathfrak{R}$.

Beweis

Über das bereits in S(18.10) Bewiesene hinaus brauchen wir nur noch die Relationstreue der Zuordnung φ gegenüber der Multiplikation zu zeigen:

$$\varphi(\bar{a}) \cdot \varphi(\bar{b}) = [a] \cdot [b] = [a \cdot b] = \varphi(\overline{a \cdot b}) = \varphi(\bar{a} \cdot \bar{b}).$$

Man beachte aber, daß diese Formel ihrem Inhalt nach nicht die schon im Beweis von S(18.10) auftretende Formel ist, da letztere ja jetzt als Aussage über den Modul $\mathfrak{R}^+$ additiv zu lesen ist.

---

1) Alle Aussagen von S(33.7), die sich nicht auf die Multiplikation beziehen, kann man auch als Aussagen über den Restklassenmodul von $\mathfrak{R}^+$ nach dem Untermodul $\mathfrak{m}$ unmittelbar aus S(18.9) entnehmen, wenn man nur berücksichtigt, daß die Vorschrift $[a] + [b] = [a + b]$ genau der Komplexaddition im Modul $\mathfrak{R}^+$ entspricht.

Die Umkehrung beruht einfach darauf, daß die Nacheinanderausführung zweier homomorpher Abbildungen wieder einen Homomorphismus ergibt.

qed.

Damit erhalten wir wieder als eine zweckmäßige Zusammenfassung des Wesentlichen den

Homomorphiesatz für Ringe **S (33.9)**

Jeder Ring $\overline{\mathfrak{R}}$, *auf den der Ring* $\mathfrak{R}$ *homomorph abgebildet ist, ist isomorph einem Restklassenring* $\mathfrak{R}/\mathfrak{m}$, *wobei das zweiseitige Ideal* $\mathfrak{m}$ *von* $\mathfrak{R}$ *der Kern des Homomorphismus ist. Andererseits ist jeder Restklassenring* $\mathfrak{R}/\mathfrak{m}$ *von* $\mathfrak{R}$ *nach einem zweiseitigen Ideal* $\mathfrak{m}$ *von* $\mathfrak{R}$ *homomorphes Bild von* $\mathfrak{R}$.

Als eine Aussage, die schon für den Modul $\mathfrak{R}^+$ gilt, entnehmen wir F(18.12) unmittelbar:

Folgerung **F (33.10)**

a) *Ein Homomorphismus* $\mathfrak{R} \xrightarrow{\sim} \overline{\mathfrak{R}}$ *ist dann und nur dann ein Isomorphismus, wenn sein Kern* $\mathfrak{m}$ *gleich dem Nullideal von* $\mathfrak{R}$ *ist.*

b) *Das homomorphe Bild* $\overline{\mathfrak{R}}$ *eines Ringes* $\mathfrak{R}$ *ist dann und nur dann der nur aus dem Nullelement bestehende Nullring, wenn der Kern* $\mathfrak{m}$ *des Homomorphismus* $\mathfrak{R} \xrightarrow{\sim} \overline{\mathfrak{R}}$ *gleich dem Einheitsideal* $\mathfrak{R}$ *ist.*

Als besonders wichtig stellen wir wieder heraus, daß man nach dem Homomorphiesatz mit den zweiseitigen Idealen eines Ringes $\mathfrak{R}$ alle homomorphen Bilder von $\mathfrak{R}$ kennt, da diese bis auf Isomorphie mit den entsprechenden Restklassenringen von $\mathfrak{R}$ übereinstimmen. Das Rechnen in diesen Restklassenringen erfolgt meistens repräsentantenweise, indem man wieder von der Gleichheit der Restklassen zur Äquivalenz der in ihnen enthaltenen Elemente übergeht. Entsprechend unseren Ausführungen am Ende von § 7 und von § 18 schreibt man diese Äquivalenz als *Kongruenz modulo* $\mathfrak{m}$

$$a \equiv b \bmod \mathfrak{m} \quad \text{oder} \quad a \equiv b\,(\mathfrak{m}).$$

Die damit gewonnene Kongruenzrechnung in einem beliebigen Ring $\mathfrak{R}$ nach einem zweiseitigen Ideal $\mathfrak{m}$ enthält natürlich die Kongruenzrechnung in $\mathfrak{R}^+$ nach dem Untermodul $\mathfrak{m}$, gestattet aber nicht nur

additiv, sondern auch multiplikativ mit solchen Kongruenzen zu rechnen:

$$\text{Aus } a \equiv a' (\mathfrak{m}) \text{ und } b \equiv b' (\mathfrak{m}) \text{ folgt } \begin{cases} a + b \equiv a' + b' (\mathfrak{m}), \\ a - b \equiv a' - b' (\mathfrak{m}), \\ a \cdot b \equiv a' \cdot b' (\mathfrak{m}). \end{cases}$$

Beachtet man ferner, daß der Ring Γ der ganzen Zahlen für jeden Ring, also auch für $\mathfrak{R}/\mathfrak{m}$ Operatorenbereich ist, erhält man noch:

$$\text{Aus } a \equiv a' (\mathfrak{m}) \text{ und } g \in \Gamma \text{ folgt } ga \equiv ga' (\mathfrak{m}).$$

Ist $\mathfrak{m}$ insbesondere Hauptideal in einem kommutativen Ring $\mathfrak{R}$, welches von einem Element m erzeugt wird, so schreibt man wieder entsprechend

$$\begin{array}{lll} \text{statt} & a \equiv b \bmod (m) & \text{bzw. } a \equiv b ((m)) \\ \text{einfach} & a \equiv b \bmod m & \text{bzw. } a \equiv b (m). \end{array}$$

Damit haben wir endgültig den schon oft angedeuteten allgemeinen Standpunkt erreicht, von dem aus die Kongruenzrechnung mit ganzen Zahlen als ein Spezialfall der Kongruenzrechnung in beliebigen Ringen erscheint. Von den damit gegebenen Einsichten macht man bei der Behandlung der entsprechenden Fragen der elementaren Zahlentheorie oft Gebrauch (vgl. Aufg. 4).

Weiterhin sind von besonderer Wichtigkeit die Restklassenringe von Polynomringen. Sie ermöglichen es nämlich, zu einem Ring $\mathfrak{R}$ nicht nur Unbestimmte, sondern auch Elemente mit ganz bestimmten algebraischen Eigenschaften zu adjungieren.

Vorläufig geben wir dafür nur ein Beispiel, indem wir zeigen, daß der Körper der komplexen Zahlen seiner Struktur nach ein Restklassenring des Polynomrings $\Delta[x]$ über dem Körper Δ der reellen Zahlen ist und man darauf aufbauend auch zu einer Einführung der komplexen Zahlen unabhängig von dem im § 31 beschriebenen Verfahren gelangen kann.

Dazu gehen wir zunächst vom Körper Δ der reellen Zahlen aus und betrachten den Polynomring in einer Unbestimmten $\Delta[x]$. In diesem Ring bilden wir das von dem Element $f(x) = x^2 + 1$ erzeugte Hauptideal $(x^2 + 1)$, welches nach F (28.7) genau aus allen Ringvielfachen von $x^2 + 1$ besteht. Der Restklassenring $\Delta[x]/(x^2 + 1)$ ist bis auf Isomorphie genau der Körper Z der komplexen Zahlen. Um dies zu zeigen, kennzeichnen wir zunächst das Rechnen in $\Delta[x]/(x^2 + 1)$, indem wir zu Kongruenzen modulo $x^2 + 1$ in $\Delta[x]$ übergehen. Als

vollständiges Repräsentantensystem kann man dabei gerade die Menge aller linearen Polynome $a + bx$ nehmen. Es ist nämlich

1. jedes Polynom $f(x)$ einem solchen Polynom kongruent, da alle Glieder von $f(x)$ mit einem Grad $\geqq 2$ wegen $x^2 \equiv -1 \bmod (x^2+1)$ sukzessive reduziert werden können

   (Beispiel: $f(x) = 5 + 2x^2 + 3x^3 + x^4 \equiv 4 - 3x \bmod (x^2+1)$);

2. $a + bx \equiv c + dx \bmod (x^2+1)$ genau für $a = c$ und $b = d$, da das Ideal (x^2+1) nach F(32.5) als Elemente außer der 0 nur Polynome höheren als ersten Grades enthält und damit aus $(a-c) + (b-d)x \in (x^2+1)$ folgt $a - c = b - d = 0$.

Insbesondere repräsentieren dabei die konstanten Polynome eine zu Δ isomorphe Teilmenge.

Die behauptete Isomorphie zwischen $\Delta[x]/(x^2+1)$ und $\mathbf{Z}$ erhält man nun gerade dadurch, daß man jedem Repräsentanten $a + bx$ die komplexe Zahl $a + bi$ zuordnet:

$$a + bx \text{ modulo } (x^2+1) \to a + bi.$$

Diese Zuordnung ist nach den eben durchgeführten Überlegungen eineindeutig und auch relationstreu, da man ja mit komplexen Zahlen einfach wie mit „Polynomen" in i unter gleichzeitiger Berücksichtigung der Nebenbedingung $i^2 + 1 = 0$ rechnet. Mit anderen Worten: Die Kongruenzrechnung in $\Delta[x]$ modulo (x^2+1) präzisiert gerade das für komplexe Zahlen übliche Rechenverfahren.

Umgekehrt kann man dies verwenden, um ohne das Hilfsmittel der Zahlenpaarbildung einen (möglichst kleinen) Oberkörper von Δ zu konstruieren, der ein Element enthält, dessen Quadrat gleich -1 ist, also eben den Körper $\mathbf{Z}$ der komplexen Zahlen[1]). Man schließt nämlich der Reihe nach:

a) Die Restklassen von $\Delta[x]/(x^2+1)$ werden gerade durch die linearen Polynome $a + bx$ repräsentiert (wie oben).

b) $\Delta[x]/(x^2+1)$ ist Körper, da für alle $a + bx \not\equiv 0$ vermöge der Kongruenz

$$\left(\frac{a}{a^2+b^2} + \frac{-b}{a^2+b^2}x\right) \cdot (a + bx) \equiv 1 \bmod (x^2+1)$$

ein Inverses existiert.

---

1) Der Vollständigkeit halber bemerken wir, daß es in der Tat bis auf Isomorphie nur einen Oberkörper von Δ gibt, der die genannten Eigenschaften besitzt — eine Aussage, die wir übrigens später (vgl. Teil III, § 53) aus allgemeineren Betrachtungen erhalten werden.

c) $\Delta[x]/(x^2+1)$ enthält eine zu Δ isomorphe Untermenge (wie oben) und wird offenbar von ihr und der Restklasse $[x]$ [1]) erzeugt, wobei gilt:

$$[x]^2 = [-1].$$

Faßt man gemäß dem Ersetzungsverfahren S(29.5) $\Delta[x]/(x^2+1)$ als Oberkörper von Δ auf, so ist das Ziel unserer Konstruktion bereits erreicht; natürlich wird man noch zur Vereinfachung der Schreibweise die Restklasse $[x]$ wieder durch das Symbol i ersetzen.

Freilich ist damit für eine elementare Einführung der komplexen Zahlen an sich nichts gewonnen, denn man benutzt ja Ergebnisse, die sogar auf der Bildung von unendlichen Elementensystemen beruhen, dafür aber auch viel weiter reichen und nicht etwa nur als Hilfsmittel zur Einführung der komplexen Zahlen gedacht sind. Mit anderen Worten, erst der wesentlich größere Aufwand an allgemeiner Theorie gestattet die einfache Behandlung des vorliegenden konkreten Spezialfalles, während das zwar umständlichere Verfahren der Zahlenpaarbildung praktisch nur das Rechnen mit reellen Zahlen voraussetzt.

An dieser Stelle sind einige Bemerkungen über die Einführung der komplexen Zahlen im Schulunterricht angebracht. Eine solche kann nicht darauf verzichten, die komplexen Zahlen als prinzipiell neuen Zahlenbereich zu betrachten, in dem Rechenverknüpfungen zu erklären und die aus ihnen folgenden Rechengesetze abzuleiten sind; insbesondere ist nachzuweisen, daß damit eine Erweiterung des Bereiches der reellen Zahlen in der angestrebten Weise erreicht ist. Da jede komplexe Zahl durch zwei reelle Zahlen zu kennzeichnen ist, wäre zur Durchführung dieser Betrachtungen die Zahlenpaarschreibweise am angemessensten. Immerhin kann man $a + bi$ als Symbol für (a, b) aus Gründen der Faßlichkeit vorziehen, obwohl damit zunächst $+$ und $\cdot$ in doppelter Bedeutung auftreten, nämlich einmal als Schreibsymbole in $a + b \cdot i$, zum andern als Verknüpfungszeichen für die Addition und Multiplikation dieser komplexen Zahlen. Dieser Unterschied wäre strenggenommen beizubehalten, bis man die Übereinstimmung beider Bedeutungen zeigen kann, ein Nachteil, den gerade die Zahlenpaarschreibweise vermeidet. Eine Abkürzung dieser Überlegungen in der Art, daß man zu den reellen Zahlen einfach noch ein Symbol i hinzunimmt und unter der Annahme der weiteren Gültigkeit der formalen Regeln der Buchstabenrechnung mit $i^2 = -1$ „losrechnet", ist zu verwerfen. Sie kann sich auch nicht etwa darauf stützen, daß dieses Verfahren ja genau der eben besprochenen Restklassenbildung entspräche. Sie gewährt zwar demjenigen, der sie kennt, die Beruhigung, daß dieses „Losrechnen" nicht zu falschen Ergebnissen führt.

---

1) Man verwechsle die (hier fettgedruckten) eckigen Klammern der Restklassenbildung nicht mit den Zeichen für die Ringadjunktion.

Eine Einführung der komplexen Zahlen ist aber ein solcher Weg keinesfalls, da er gerade die entscheidenden Überlegungen — ausgesprochen oder stillschweigend — als bereits bewiesen voraussetzt.

Aufgaben zu § 33

1. Man beweise F(33.2) und F(33.3).
2. Die Restklassenringe mod m kennzeichnen bis auf Isomorphie alle homomorphen Bilder des Ringes Γ der ganzen Zahlen.
3. Welche homomorphen Bilder hat ein Körper?
4. Ein Gebiet der elementaren Zahlentheorie ist die Behandlung linearer Kongruenzen $ax \equiv b\,(m)$ in ganzen Zahlen. Die diesbezüglichen zahlentheoretischen Aussagen lassen sich als solche über den Restklassenring $\Gamma/(m)$ auffassen. In diesem Sinne beweise man zunächst:
   a) Für die Lösbarkeit der Kongruenz $ax \equiv 1\,(m)$ ist die Bedingung $(a, m) = 1$ notwendig und hinreichend. Die Lösung ist dann in dem Sinne eindeutig bestimmt, daß genau die Zahlen einer Restklasse mod m Lösungen sind.
   b) $x \equiv a^{\varphi(m)-1}$ ist Lösung der Kongruenz $ax \equiv 1\,(m)$ mit $(a, m) = 1$. Man kennzeichne den niedrigsten Exponenten $\nu > 0$, für den $x \equiv a^{\nu}$ diese Kongruenz erfüllt.
   c) Für die Lösbarkeit der Kongruenz $ax \equiv b\,(m)$ ist die Bedingung $(a, m) = 1$ jedenfalls hinreichend, da ihre Auflösung dann unmittelbar auf die von $ax \equiv 1\,(m)$ zurückgeführt werden kann. Für die Eindeutigkeit der Lösung ist dabei die Bedingung $(a, m) = 1$ sogar notwendig und hinreichend.

   Insbesondere ist mit diesen Aussagen der Fall $(a, m) = 1$ vollständig erledigt; das ist insofern entscheidend, als sich der allgemeine Fall $(a, m) = d$ darauf zurückführen läßt, wie wir im § 41 sehen werden.
5. Man löse die folgenden Kongruenzen:
   a) $2x \equiv 3\,(15)$; b) $5x \equiv 7\,(36)$; c) $9x \equiv 44\,(58)$.
6. Man beweise die folgenden Teilbarkeitsregeln (für dekadisch geschriebene Zahlen) durch Übergang zu den entsprechenden Kongruenzen:
   a) 2, 4 bzw. 8 gehen in einer Zahl a auf, wenn sie in der von der letzten Ziffer, den beiden letzten Ziffern bzw. den drei letzten Ziffern von a gebildeten Zahl aufgehen.
   b) 3 bzw. 9 gehen in einer Zahl a auf, wenn sie in der Summe aller Ziffern (der sog. Quersumme) von a aufgehen.
   c) 11 geht in einer Zahl a auf, wenn 11 in der durch abwechselnde Addition und Subtraktion der Ziffern von a entstehenden Zahl (der sog. alternierenden Quersumme) aufgeht.
7. Man kennzeichne das Einsetzungsprinzip S(32.6) als homomorphe Abbildung. Welche Möglichkeit ergibt sich daraus, etwa die Struktur des Restklassenringes $\Gamma[x]/(x - g)$ mit beliebigem $g \in \Gamma$ zu beschreiben?
8. Man gebe Nullteiler des Restklassenringes $P[x]/(x^4 - 4)$ an.

§ 34. Unterringe und Ideale bei homomorphen Abbildungen

Um zu eingehenderen Strukturaussagen über homomorphe Abbildungen zu gelangen, untersuchen wir wiederum die Abbildung von Untermengen, indem wir analog wie im § 19 vorgehen und uns auf die dortigen Ergebnisse stützen (vgl. dazu Aufg. 4). Im Hinblick auf spätere Anwendungen beschränken wir uns auf kommutative Ringe, unbeschadet der Tatsache, daß sich fast alle Aussagen dieses Paragraphen auf den nichtkommutativen Fall übertragen lassen.

Satz **S (34.1)**

Bei einem Homomorphismus $\mathfrak{R} \xrightarrow{\sim} \overline{\mathfrak{R}}$ *wird jeder Unterring* $\mathfrak{S} \subseteq \mathfrak{R}$ *auf einen Unterring* $\overline{\mathfrak{S}} \subseteq \overline{\mathfrak{R}}$ *abgebildet.*

Umgekehrt ist das vollständige Original $\mathfrak{T}$ *eines Unterringes* $\overline{\mathfrak{S}} \subseteq \overline{\mathfrak{R}}$, *also die Menge aller derjenigen Elemente von* $\mathfrak{R}$, *die auf die Elemente von* $\overline{\mathfrak{S}}$ *abgebildet werden, ein Unterring von* $\mathfrak{R}$. *Man erhält* $\mathfrak{T}$ *aus jedem Unterring* $\mathfrak{S} \subseteq \mathfrak{R}$ *mit dem Bild* $\overline{\mathfrak{S}} \subseteq \overline{\mathfrak{R}}$ *vermöge*

$$\mathfrak{T} = \mathfrak{S} + \mathfrak{m}.$$

Das vollständige Original $\mathfrak{T}$ *von* $\overline{\mathfrak{S}}$ *enthält alle Unterringe* $\mathfrak{S} \subseteq \mathfrak{R}$, *die bei* $\mathfrak{R} \xrightarrow{\sim} \overline{\mathfrak{R}}$ *auf* $\overline{\mathfrak{S}} \subseteq \overline{\mathfrak{R}}$ *abgebildet werden, und* $\mathfrak{T}$ *ist von allen diesen Unterringen der einzige, der den Kern* $\mathfrak{m}$ *des Homomorphismus umfaßt.*

Beweis

Der erste Teil der Behauptung folgt unmittelbar aus F (33.2).

Von der Umkehrung brauchen wir wegen S (19.2) nur noch nachzuweisen, daß $\mathfrak{T}$ nicht nur Untermodul von $\mathfrak{R}^+$, sondern sogar Unterring von $\mathfrak{R}$ ist. Das Produkt zweier Elemente $t = s + m$ und $t' = s' + m'$ von $\mathfrak{T}$ ist aber selbst Element von $\mathfrak{T}$ wegen

$$tt' = ss' + (ms' + sm' + mm') \in \mathfrak{S} + \mathfrak{m}.$$

qed.

Aus dieser eindeutigen Zuordnung zwischen den Unterringen von $\overline{\mathfrak{R}}$ und ihren vollständigen Originalen in $\mathfrak{R}$ ergibt sich insbesondere

Folgerung **F (34.2)**

Sämtliche Unterringe eines Ringes $\mathfrak{R}$, *auf den ein Ring* $\mathfrak{R}$ *mit dem Kern* $\mathfrak{m}$ *homomorph abgebildet ist, erhält man bereits als Bilder derjenigen Unterringe von* $\mathfrak{R}$, *die den Kern* $\mathfrak{m}$ *umfassen.*

Als Beispiel betrachten wir die homomorphe Abbildung von Γ auf $\Gamma/(15)$. Sämtliche Unterringe von $\Gamma/(15)$ erhalten wir als Bilder derjenigen Unterringe von Γ, die den Kern $\mathfrak{m} = (15)$ dieses Homomorphismus umfassen, also als Bilder der Unterringe[1]) (1), (3), (5) und (15). Andererseits werden alle Unterringe (1), (2), (3), ... von Γ auf einen der damit möglichen vier Unterringe von $\Gamma/(15)$ abgebildet.

Wir geben in der folgenden Tabelle neben den vollständigen Originalen (willkürlich) je ein weiteres Original an:

$$\Gamma \xrightarrow{\sim} \Gamma/(15)$$

$$(1), \ldots, (11), \ldots \xrightarrow{\sim} \Gamma/(15) = \{[0], [1], \ldots, [14]\}$$

$$(3), \ldots, (21), \ldots \xrightarrow{\sim} \{[0], [3], [6], [9], [12]\}$$

$$(5), \ldots, (20), \ldots \xrightarrow{\sim} \{[0], [5], [10]\}$$

$$(15), \ldots, (45), \ldots \xrightarrow{\sim} \{[0]\}.$$

Dieses Beispiel erläutert zugleich, daß bei einem natürlichen Homomorphismus eines Ringes $\mathfrak{R}$ wieder vollständiges Original und Bild jeweils durch Zusammenfassung der einzelnen Elemente zu Restklassen bzw. durch Auflösung dieser Restklassen zu einzelnen Elementen auseinander hervorgehen.

In Ergänzung zu S (34.1) erhält man aus S (19.4) als Aussage über die Klasse der auf das Nullelement abgebildeten Elemente:

Satz **S (34.3)**

Der durch den Homomorphismus $\mathfrak{R} \xrightarrow{\sim} \overline{\mathfrak{R}}$ *mit dem Kern* $\mathfrak{m}$ *bewirkte Homomorphismus der Unterringe* $\mathfrak{S} \xrightarrow{\sim} \overline{\mathfrak{S}}$ *hat den Kern* $\mathfrak{S} \cap \mathfrak{m}$. *Es ist also*

$$\overline{\mathfrak{S}} \xleftrightarrow{\sim} \mathfrak{S}/(\mathfrak{S} \cap \mathfrak{m}).$$

---

1) Zur Vereinfachung der Bezeichnung benutzen wir, daß jeder Unterring von Γ gleich einem der Ideale (1), (2), (3), ... ist. Übrigens veranschaulicht unser Beispiel wegen dieser Eigenschaft von Γ nicht nur S (34.2), sondern auch S (34.4).

Insbesondere ist damit der Durchschnitt irgendeines Unterringes von $\mathfrak{R}$ mit einem Ideal von $\mathfrak{R}$ stets ein Ideal dieses Unterringes. Ebenso überträgt sich der 1. Isomorphiesatz für Gruppen auch auf Ringe (vgl. Aufg. 1), jedoch ist seine Formulierung meist nur für Ideale üblich. Das gleiche gilt für den 2. Isomorphiesatz (vgl. Aufg. 3), in dem ohnehin keine Unterringe auftreten, die nicht auch Ideale des Ringes sind.

Für das Folgende ist wichtig, daß die eineindeutige Zuordnung zwischen den Unterringen von $\overline{\mathfrak{R}}$ und ihren vollständigen Originalen in $\mathfrak{R}$ auch für Ideale gilt:

Satz **S (34.4)**

a) *Bei einem Homomorphismus* $\mathfrak{R} \xrightarrow{\sim} \overline{\mathfrak{R}}$ *wird jedes Ideal* $\mathfrak{a}$ *von* $\mathfrak{R}$ *auf ein Ideal* $\bar{\mathfrak{a}}$ *von* $\overline{\mathfrak{R}}$ *abgebildet.*

b) *Umgekehrt ist das vollständige Original* $\mathfrak{t}$ *eines Ideals* $\bar{\mathfrak{a}}$ *von* $\overline{\mathfrak{R}}$ *ein Ideal von* $\mathfrak{R}$.

Beweis

Wegen S(34.1) brauchen wir nur zu beweisen, daß die Multiplikation mit Ringelementen aus $\bar{\mathfrak{a}}$ bzw. $\mathfrak{t}$ nicht herausführt.

a) $\bar{\mathfrak{a}}$ enthält mit jedem Element $\bar{a}$ auch alle Ringvielfachen $\bar{r} \cdot \bar{a}$, da $\bar{r} \cdot \bar{a} = \overline{ra}$ das Bild eines Elementes aus dem Ideal $\mathfrak{a}$ ist.

b) $\mathfrak{t}$ enthält mit jedem Element t auch alle Ringvielfachen rt. Es wird nämlich t auf ein Element $\bar{t}$ aus dem Ideal $\bar{\mathfrak{a}}$ von $\overline{\mathfrak{R}}$ abgebildet, und damit ist rt Original des Elementes $\overline{rt} = \bar{r} \cdot \bar{t}$ aus $\bar{\mathfrak{a}}$.

qed.

Aus diesem Satz ergibt sich, daß ein Restklassenring $\mathfrak{R}/\mathfrak{m}$ dann und nur dann keine (nichttrivialen) Ideale enthält, wenn in $\mathfrak{R}$ kein Ideal $\mathfrak{a}$ mit $\mathfrak{m} < \mathfrak{a} < \mathfrak{R}$ existiert[1]). Sehen wir von entarteten Ringen ab, so ist letzteres nach den Aufgaben 4 und 5 von § 28 also ein Kriterium für die Körpereigenschaft des Restklassenringes:

---

1) Diese Aussage entspricht ihrem Inhalt nach S(20.3) für Gruppen; wir werden auch sogleich den entsprechenden Begriff des maximalen Ideals bilden, dagegen beschäftigen wir uns hier nur mit solchen „einfachen Ringen", die kommutativ und nicht entartet, also Körper sind.

Definition **D (34.5)**

Ein von $\mathfrak{R}$ *verschiedenes Ideal* $\mathfrak{m}$ *von* $\mathfrak{R}$ *heißt maximales oder auch teilerloses*[1]) *Ideal von* $\mathfrak{R}$, *wenn für jedes Ideal* $\mathfrak{a}$ *von* $\mathfrak{R}$ *mit* $\mathfrak{m} \subseteqq \mathfrak{a} \subseteqq \mathfrak{R}$ *entweder* $\mathfrak{a} = \mathfrak{m}$ *oder* $\mathfrak{a} = \mathfrak{R}$ *gilt.*

Satz **S (34.6)**

Es sei $\mathfrak{R}$ *ein Ring mit Einselement. Dann ist* $\mathfrak{R}/\mathfrak{m}$ *genau dann ein Körper, wenn das Ideal* $\mathfrak{m}$ *von* $\mathfrak{R}$ *maximal ist.*

Die Voraussetzung über $\mathfrak{R}$ garantiert dabei, daß der Restklassenring $\mathfrak{R}/\mathfrak{m}$ ebenfalls ein Einselement enthält und damit nicht entartet ist. Sie kann natürlich entfallen, wenn letzteres von $\mathfrak{R}/\mathfrak{m}$ aus anderen Gründen bekannt ist.

Diesen Sachverhalt kennen wir bereits für den Ring Γ der ganzen Zahlen, denn dort sind die von einer Primzahl erzeugten Hauptideale genau die maximalen Ideale. Andererseits lehren die Restklassenringe von Γ, daß das homomorphe Bild eines Ringes Nullteiler besitzen kann, sogar wenn das Original nullteilerfrei ist. Bei maximalen Idealen als Kern ist das (für Ringe mit Einselement) nach S (34.6) ausgeschlossen. Es gibt aber auch Ideale mit dieser Eigenschaft, die nicht maximal sind. Betrachten wir nämlich etwa in $\mathfrak{R} = \Gamma[x_1, x_2, \ldots, x_n]$ das von x_n erzeugte Hauptideal (x_n), so ist der Restklassenring $\mathfrak{R}/(x_n)$ isomorph zu $\Gamma[x_1, x_2, \ldots, x_{n-1}]$ und damit nullteilerfrei; wegen $(x_n) \subset (x_n, x_{n-1}) \subset \mathfrak{R}$ ist (x_n) aber kein maximales Ideal von $\mathfrak{R}$. Wir erklären daher:

Definition **D (34.7)**

Ein Ideal $\mathfrak{p}$ *von* $\mathfrak{R}$ *heißt Primideal von* $\mathfrak{R}$, *wenn der Restklassenring* $\mathfrak{R}/\mathfrak{p}$ *nullteilerfrei ist.*

Ein Ideal $\mathfrak{p}$ ist also genau dann Primideal von $\mathfrak{R}$, wenn allgemein für die Kongruenzrechnung in $\mathfrak{R}$ modulo $\mathfrak{p}$ gilt:

$$\text{Aus } ab \equiv o\,(\mathfrak{p}) \text{ und } a \not\equiv o\,(\mathfrak{p}) \text{ folgt } b \equiv o\,(\mathfrak{p}).$$

---

1) Diese Bezeichnung erklärt sich aus der Verwendung des Idealbegriffes in der Teilbarkeitslehre. Bei ihrer Behandlung in Kapitel VII werden wir sehen, daß die Ideale durchaus nicht nur als Kerne von homomorphen Abbildungen bedeutungsvoll sind. Es ist dabei mitunter üblich, auch den Ring $\mathfrak{R}$ als teilerloses Ideal von $\mathfrak{R}$ zu bezeichnen.

Damit kann man die Primidealeigenschaft auch unabhängig vom Restklassenring kennzeichnen:

$$\text{Aus } a\,b \in \mathfrak{p} \text{ und } a \notin \mathfrak{p} \text{ folgt } b \in \mathfrak{p}$$

für alle a und b aus $\mathfrak{R}$.

Das Einheitsideal ist trivialerweise stets prim, das Nullideal dagegen genau dann, wenn der Ring selbst nullteilerfrei ist. Weiterhin wissen wir bereits, daß in einem Ring mit Einselement jedes maximale Ideal erst recht Primideal ist, während das Umgekehrte nur in gewissen Ringen der Fall ist, wie etwa im Ring der ganzen Zahlen.

Die hier eingeführten idealtheoretischen Begriffsbildungen sind für die Algebra und Zahlentheorie, aber auch für viele Anwendungsgebiete, wie z. B. die algebraische Geometrie, von großer Bedeutung. Wir werden an späterer Stelle einiges davon kennenlernen.

Aufgaben zu § 34

1. Man beweise den 1. Isomorphiesatz für Ringe:
   Ist $\mathfrak{R}$ ein Ring, $\mathfrak{S}$ ein Unterring und $\mathfrak{m}$ ein Ideal von $\mathfrak{R}$, so gilt:
   $$(\mathfrak{S} + \mathfrak{m})/\mathfrak{m} \overset{\sim}{\longleftrightarrow} \mathfrak{S}/(\mathfrak{S} \cap \mathfrak{m}).$$
2. Es sei $\mathfrak{R}$ homomorph abgebildet auf $\overline{\mathfrak{R}}$ mit dem Ideal $\mathfrak{m}$ von $\mathfrak{R}$ als Kern und $\overline{\mathfrak{R}}$ homomorph abgebildet auf $\overline{\overline{\mathfrak{R}}}$ mit dem Ideal $\bar{\mathfrak{a}}$ von $\overline{\mathfrak{R}}$ als Kern. Dann wird $\mathfrak{R}$ homomorph abgebildet auf $\overline{\overline{\mathfrak{R}}}$, wobei der Kern dieses Homomorphismus das vollständige Original $\mathfrak{t}$ von $\bar{\mathfrak{a}}$ ist.
3. Man beweise den 2. Isomorphiesatz für Ringe:
   Ist $\mathfrak{R}$ ein Ring, $\mathfrak{a}$ ein Ideal von $\mathfrak{R}$ und $\mathfrak{b} \subseteq \mathfrak{a}$ ein Ideal von $\mathfrak{R}$, so gilt:
   $$(\mathfrak{R}/\mathfrak{b})/(\mathfrak{a}/\mathfrak{b}) \overset{\sim}{\longleftrightarrow} \mathfrak{R}/\mathfrak{a}.$$
4. Man stelle eine Übersicht der einander entsprechenden Aussagen aus § 19 und § 34 auf.
5. Für jede ganze Zahl m gilt:
   $$\Gamma[x]/(m) \overset{\sim}{\longleftrightarrow} (\Gamma/(m))[x].$$
   Man beschreibe den damit ausgedrückten Sachverhalt und beweise ihn, wobei man sich am besten unter Verwendung von Aufgabe 4 aus § 32 darauf stützt, daß $\Gamma[x]/(m)$ selbst als Polynomring in einer Unbestimmten über einem zu $\Gamma/(m)$ isomorphen Unterring aufgefaßt werden kann.
   Wie ist diese Aussage zu verallgemeinern, wenn man Γ durch einen beliebigen Ring $\mathfrak{R}$ mit Einselement ersetzt?
6. Man zeige, daß (x) Primideal, nicht aber maximales Ideal von $\mathfrak{R} = \Gamma[x]$ ist.
7. Es sei Δ der Körper der reellen Zahlen. Dann ist das von $x^2 + 1$ erzeugte Ideal in $\Delta[x]$ Primideal.
8. Man zeige mit Hilfe von Aufg. 3, daß die nichttrivialen Ideale von $\Gamma/(15)$ maximal sind. Ringe mit Nullteilern können also nullteilerfreie homomorphe Bilder besitzen.

VII. ALGEBRAISCHE STRUKTUREN MIT OPERATORENBEREICHEN

Wir wenden uns in diesem Kapitel speziell dem schon mehrfach aufgetretenen Begriff der Operatoranwendung zu. Dabei beginnen wir allgemein mit beliebigen Gruppen, für deren Elemente eine solche Anwendung gewisser Operatoren erklärt ist, um dann zu abelschen Gruppen überzugehen, deren Operatorenbereiche Ringe oder sogar Körper sind. Abschließend lernen wir den für moderne Untersuchungen zentralen Begriff der „Algebra" kennen und erledigen damit insbesondere das schon am Ende von § 31 angeschnittene Problem der allgemeinen Herstellung von Ringen aus geordneten Elementensystemen.

Die in diesem Kapitel behandelten Begriffsbildungen sind für viele Gebiete der Mathematik von grundlegender Bedeutung. Auch eine Reihe weitergehender algebraischer Untersuchungen (etwa die allgemeine Strukturtheorie und die Darstellungstheorie) baut auf ihnen auf, doch können wir darauf hier nicht weiter eingehen. So ist auch alles Folgende von diesem Kapitel nahezu unabhängig; lediglich ab Kapitel X werden einige Aussagen über endliche $\mathfrak{R}$-Moduln benötigt, die sich der Leser jedoch mit Hilfe des kleingedruckten Teiles am Ende von § 37 aneignen kann, ohne das gesamte Kapitel studieren zu müssen.

§ 35. Gruppen mit Operatorenbereichen

In unseren bisherigen Betrachtungen galt unsere Aufmerksamkeit im wesentlichen solchen algebraischen Operationen, die je zwei in bestimmter Reihenfolge gegebenen Elementen einer Menge $\mathfrak{M}$ eindeutig ein weiteres Element dieser Menge zuordnen. Derartige *innere Verknüpfungen* entsprechen also eindeutigen Abbildungen der Produktmenge $\mathfrak{M} \times \mathfrak{M}$ in die Menge $\mathfrak{M}$. Daneben traten aber auch schon als *äußere Verknüpfungen* zu bezeichnende Operationen

auf, nämlich Operatoranwendungen, die je einem Element eines Operatorenbereiches Ω und einem Element einer Menge $\mathfrak{M}$ ein weiteres Element von $\mathfrak{M}$ zuordnen. Hierbei handelt es sich also um eindeutige Abbildungen der Produktmenge $\Omega \times \mathfrak{M}$ (oder $\mathfrak{M} \times \Omega$) in die Menge $\mathfrak{M}$.

So ist z. B. der Ring der ganzen Zahlen Operatorenbereich für jeden Modul, ja sogar für jeden Ring (vgl. § 3 und § 27); ebenso ist der Körper der reellen Zahlen Operatorenbereich sowohl für den Modul der Vektoren der analytischen Geometrie als auch für den Modul der Matrizen vom Typ (n, m) mit reellen Matrizenelementen (vgl. Aufgaben 10 und 11 von § 3). Die für solche äußeren Verknüpfungen einer algebraischen Struktur $\mathfrak{M}$ mit dem Operatorenbereich Ω geltenden Gesetzmäßigkeiten hängen natürlich jeweils von den inneren Verknüpfungen ab, die in $\mathfrak{M}$ bzw. in Ω erklärt sind. In diesem Paragraphen betrachten wir speziell den Fall, daß in $\mathfrak{M}$ eine den Gruppenaxiomen genügende (innere) Verknüpfung gegeben ist und lassen eventuell in Ω existierende (innere) Verknüpfungen unberücksichtigt.

Definition **D (35.1)**

Es sei $\mathfrak{G}$ eine Gruppe und Ω eine nichtleere Menge. Dann heißt $\mathfrak{G}$ eine Gruppe mit dem Operatorenbereich Ω, wenn eine Operatoranwendung der Elemente $\alpha, \beta, \ldots$ aus Ω auf die Elemente $a, b, \ldots$ aus $\mathfrak{G}$ erklärt ist, die folgenden Axiomen genügt:

O I: Die Operatoranwendung von α auf a liefert ein eindeutig bestimmtes Element αa aus $\mathfrak{G}$.

O II: Die Operatoranwendung ist distributiv:

$$\alpha(a + b) = \alpha a + \alpha b, \text{ falls } \mathfrak{G} \text{ eine additive Gruppe ist;}$$

$$\alpha(a \cdot b) = \alpha a \cdot \alpha b, \text{ falls } \mathfrak{G} \text{ eine multiplikative Gruppe ist.}$$

Nach unserer Schreibweise müßten wir Ω genauer als Linksoperatorenbereich bezeichnen, denn man könnte ja statt αa ebensogut $a\alpha$ und damit $\mathfrak{G}$ als Gruppe mit Ω als Rechtsoperatorenbereich schreiben. Eine solche Unterscheidung ist jedoch im allgemeinen (vgl. aber die Fußnote auf Seite 95) erst erforderlich, wenn man auch Relationen berücksichtigt, die sich aus (eventuell erklärten) inneren Verknüpfungen von Ω ergeben (vgl. Aufg. 1).

Die Anwendung jedes Operators $\alpha \in \Omega$ liefert dabei einen Endomorphismus der Gruppe $\mathfrak{G}$. Sie ordnet nämlich nach *O I* jedem $a \in \mathfrak{G}$ eindeutig das Element $\alpha a \in \mathfrak{G}$ zu, und wegen *O II* ist diese Zuordnung relationstreu. Umgekehrt ist natürlich die Menge aller Endomorphismen von $\mathfrak{G}$ beziehungsweise jede ihrer Untermengen Operatorenbereich für $\mathfrak{G}$. Insbesondere ergibt sich aus bekannten Eigenschaften homomorpher Abbildungen (vgl. F(18.3)):

Folgerung **F (35.2)**

In einer Gruppe $\mathfrak{G}$ mit dem Operatorenbereich Ω gilt für jedes $\alpha \in \Omega$ und $a \in \mathfrak{G}$:

$\alpha o = o$ *und* $\alpha(-a) = -(\alpha a)$, *falls $\mathfrak{G}$ additiv ist;*

$\alpha e = e$ *und* $\alpha(a^{-1}) = (\alpha a)^{-1}$, *falls $\mathfrak{G}$ multiplikativ ist.*

Mit D(35.1) sind wir zu einer Erweiterung des Gruppenbegriffes gelangt, die gruppentheoretische Aussagen auf einen weiteren Kreis algebraischer Strukturen zu übertragen gestattet. Dazu ist es natürlich erforderlich, die entsprechenden Begriffe der gewöhnlichen Gruppentheorie mit der Operatoranwendung in Zusammenhang zu bringen.

Definition **D (35.3)**

Es sei $\mathfrak{G}$ eine Gruppe mit dem Operatorenbereich Ω. Dann heißt eine Untergruppe $\mathfrak{H} \leqq \mathfrak{G}$ eine (bezüglich Ω) zulässige Untergruppe von $\mathfrak{G}$, wenn $\mathfrak{H}$ selbst den Operatorenbereich Ω gestattet:

$$\text{Aus } h \in \mathfrak{H} \text{ folgt } \alpha h \in \mathfrak{H} \text{ für alle } \alpha \in \Omega.$$

Eine zulässige Untergruppe ist also selbst eine Gruppe mit dem Operatorenbereich Ω. Zum Beispiel sind alle Untermoduln eines beliebigen Moduls bezüglich des Operatorenbereiches Γ zulässige Untergruppen. Weiterhin bilden die in B(2.3b) genannten Vektoren einer Ebene bzw. einer Geraden einen bezüglich des Operatorenbereiches Δ zulässigen Untermodul des Moduls aller Vektoren des dreidimensionalen Raumes. Ferner sind die Linksideale eines Ringes $\mathfrak{R}$ zulässige Untermoduln von $\mathfrak{R}^-$, wenn man $\mathfrak{R}$ als Linksoperatorenbereich für $\mathfrak{R}^-$ mit der gewöhnlichen Ringmultiplikation als Operatoranwendung auffaßt; das gleiche gilt für die

Rechtsideale mit $\mathfrak{R}$ als Rechtsoperatorenbereich[1]). Nimmt man schließlich als Operatorenbereich für eine Gruppe $\mathfrak{G}$ die Menge aller inneren Automorphismen von $\mathfrak{G}$, so sind die zulässigen Untergruppen gerade die Normalteiler von $\mathfrak{G}$. Entsprechend liefert die Menge aller Automorphismen von $\mathfrak{G}$ als Operatorenbereich für $\mathfrak{G}$ als zulässige Untergruppen die sogenannten charakteristischen Untergruppen von $\mathfrak{G}$.

Definition **D (35.4)**

Es seien $\mathfrak{G}$ und $\overline{\mathfrak{G}}$ zwei Gruppen mit demselben Operatorenbereich Ω. Dann heißt $\mathfrak{G}$ (bezüglich Ω) operatorhomomorph abgebildet auf $\overline{\mathfrak{G}}$, wenn ein Homomorphismus von $\mathfrak{G}$ auf $\overline{\mathfrak{G}}$ vorliegt, der auch noch relationstreu bezüglich der Operatoranwendung ist:

$$\text{Aus } a \to \overline{a} \text{ folgt } \alpha a \to \overline{\alpha}\,\overline{a} = \alpha\,\overline{a}$$

für alle $a \in \mathfrak{G}$ und $\alpha \in \Omega$. Die Abbildung selbst nennt man dann einen Operatorhomomorphismus.

Entsprechend erklärt man *Operatorisomorphismen, Operatorendomorphismen* usw. Üblicherweise verwendet man die Zeichen $\xrightarrow{\sim}$ und $\xleftarrow{\sim}$ weiter, da sich ihre richtige Deutung im allgemeinen aus dem Zusammenhang ergibt.

Es ist nun von entscheidender Wichtigkeit und das eigentliche Ziel der Untersuchungen dieses Paragraphen, daß alle Aussagen über die Homomorphie gewöhnlicher Gruppen für die Operatorhomomorphie von Gruppen mit Operatorenbereichen weitergelten, wenn man nur solche Normalteiler in Betracht zieht, die selbst zulässige Untergruppen sind. Solche Normalteiler nennt man abkürzend zulässige Normalteiler. Dabei führen wir die folgenden Beweise ohne Beschränkung der Allgemeinheit für multiplikative Gruppen durch.

Satz **S (35.5)**

Der Kern $\mathfrak{N}$ eines Operatorhomomorphismus $\mathfrak{G} \xrightarrow{\sim} \overline{\mathfrak{G}}$ ist zulässiger Normalteiler bezüglich des vorliegenden Operatorenbereiches Ω.

---

1) Die Unterscheidung der Operatoranwendung von links und von rechts ist an dieser Stelle erforderlich, da die Ringmultiplikation als innere Verknüpfung von $\mathfrak{R}$ hier als äußere Verknüpfung eines Untermoduls von $\mathfrak{R}^+$ mit $\mathfrak{R}$ aufgefaßt wird. Damit können aber αa und $a\alpha$, die ja als Produkte in $\mathfrak{R}$ erklärt sind, voneinander verschieden sein.

Beweis

Da es sich hierbei nur um eine Ergänzung von S(18.8) handelt, bleibt lediglich zu zeigen, daß der Normalteiler $\mathfrak{N}$ eine zulässige Untergruppe ist. Für jedes $n \in \mathfrak{N}$ gilt aber nach F(35.2)

$$\alpha n \to \overline{\alpha n} = \alpha \bar{n} = \alpha \bar{e} = \bar{e},$$

also ist $\alpha n \in \mathfrak{N}$ für alle $\alpha \in \Omega$. qed.

Satz **S (35.6)**

a) *Die Faktorgruppe $\mathfrak{G}/\mathfrak{N}$ einer Gruppe $\mathfrak{G}$ mit dem Operatorenbereich Ω nach einem zulässigen Normalteiler von $\mathfrak{G}$ ist vermöge der Definition*

(*) $$\alpha [a] = [\alpha a] \quad \textit{für } \alpha \in \Omega$$

selbst Gruppe mit dem Operatorenbereich Ω.

b) *Die Abbildung $\mathfrak{G} \xrightarrow{\sim} \mathfrak{G}/\mathfrak{N}$ ist dann sogar ein Operatorhomomorphismus bezüglich Ω.*

Beweis

a) Über S(18.9) hinaus ist nur zu beweisen, daß Ω Operatorenbereich für $\mathfrak{G}/\mathfrak{N}$ ist.

O I: Die Erklärung $\alpha [a] = [\alpha a]$ ist in der Tat eindeutig, d. h. von dem Repräsentanten a der Nebenklasse $[a] = a\mathfrak{N}$ unabhängig. Aus $[a] = [a']$, also $a'a^{-1} \in \mathfrak{N}$ folgt nämlich $\alpha(a'a^{-1}) \in \mathfrak{N}$ nach Voraussetzung über $\mathfrak{N}$ und damit nach *O II* (für $\mathfrak{G}$) und F(35.2)

$$\alpha (a'a^{-1}) = (\alpha a')\,(\alpha a^{-1}) = (\alpha a')\,(\alpha a)^{-1} \in \mathfrak{N},$$

also $[\alpha a] = [\alpha a']$.

O II: Die Distributivität der Operatoranwendung überträgt sich von $\mathfrak{G}$ auf $\mathfrak{G}/\mathfrak{N}$:

$$\alpha ([a] \cdot [b]) = \alpha [a \cdot b] = [\alpha (a \cdot b)] = [\alpha a \cdot \alpha b] = [\alpha a] \cdot [\alpha b]$$
$$= (\alpha [a]) \cdot (\alpha [b]).$$

b) Es genügt wieder, die Relationstreue bezüglich der Operatoranwendung nachzuweisen. Diese ist aber nach (*) erfüllt:

$$\text{Aus } \; a \to [a] \; \text{ folgt } \; \alpha a \to [\alpha a] = \alpha [a]. \qquad \text{qed.}$$

Satz **S (35.7)**

Es sei $\mathfrak{G} \xrightarrow{\sim} \overline{\mathfrak{G}}$ *ein Operatorhomomorphismus vermöge der Zuordnung* $a \to \bar{a}$ *mit dem Kern* $\mathfrak{N}$. *Dann ist* $\overline{\mathfrak{G}}$ *operatorisomorph zur Faktorgruppe* $\mathfrak{G}/\mathfrak{N}$ *vermöge* $\bar{a} \to [a] = \varphi(\bar{a})$. *Umgekehrt ist jedes operatorisomorphe Bild* $\overline{\mathfrak{G}}$ *der Faktorgruppe* $\mathfrak{G}/\mathfrak{N}$ *ein operatorhomomorphes Bild von* $\mathfrak{G}$. *Allen Aussagen dieses Satzes liegt dabei ein fester Operatorenbereich zugrunde.*

Beweis

Wegen S (18.10) genügt der Nachweis der Relationstreue der Zuordnung φ bezüglich der Operatoranwendung:

$$\alpha\varphi(a) = \alpha[a] = [\alpha a] = \varphi(\overline{\alpha a}) = \varphi(\alpha \bar{a}).$$

Die Umkehrung ergibt sich daraus, daß auch die Nacheinanderausführung zweier operatorhomomorpher Abbildungen wieder einen Operatorhomomorphismus liefert. qed.

Das Wesentliche dieser drei Aussagen faßt man wieder zusammen im

Homomorphiesatz für Gruppen mit Operatorenbereichen **S (35.8)**

Jede Gruppe $\overline{\mathfrak{G}}$ *mit dem Operatorenbereich* Ω, *auf die die Gruppe* $\mathfrak{G}$ *mit demselben Operatorenbereich operatorhomomorph abgebildet ist, ist operatorisomorph einer Faktorgruppe* $\mathfrak{G}/\mathfrak{N}$, *wobei der (zulässige) Normalteiler* $\mathfrak{N} \leqq \mathfrak{G}$ *der Kern des Homomorphismus ist. Andererseits ist jede Faktorgruppe* $\mathfrak{G}/\mathfrak{N}$ *von* $\mathfrak{G}$ *nach einem zulässigen Normalteiler* $\mathfrak{N}$ *operatorhomomorphes Bild von* $\mathfrak{G}$.

Durch die entsprechenden Nachweise der sich auf die Operatorhomomorphie beziehenden Ergänzungen übertragen sich auch die Aussagen aus § 19, insbesondere: Das operatorhomomorphe Bild einer zulässigen Untergruppe ist selbst zulässige Untergruppe; umgekehrt ist das vollständige Original einer zulässigen Untergruppe ebenfalls zulässige Untergruppe. Das Entsprechende gilt für Normalteiler. Daraus folgt, daß für zulässige Normalteiler einer Gruppe mit einem Operatorenbereich die beiden Isomorphiesätze auch hinsichtlich der Operatorisomorphie richtig bleiben.

Darauf aufbauend kann man schließlich auch noch die im Kapitel IV abgeleiteten Sätze über Normal- und Kompositionsreihen auf Gruppen mit Operatorenbereichen ausdehnen.

Aufgaben zu § 35

1. Man kennzeichne die in § 15 eingeführte Schreibweise für die Automorphismen einer Gruppe $\mathfrak{G}$ als Operatoranwendung dieser Automorphismen auf die Elemente von $\mathfrak{G}$. Unter Berücksichtigung der durch die Gruppeneigenschaft von Φ gegebenen inneren Verknüpfung des Operatorenbereiches ist die Schreibweise als Rechtsoperatoren vorzuziehen. Warum?

2. Charakteristische Untergruppen sind:
   a) $\mathfrak{E}$ und $\mathfrak{G}$ in jeder Gruppe $\mathfrak{G}$,
   b) $\mathfrak{A}_n$ in $\mathfrak{S}_n$,
   c) $\langle(13)(24)\rangle$ (als Zentrum!) in $\langle(13), (14)(23)\rangle$.

3. Es sei $\mathfrak{G}$ eine Gruppe mit dem Operatorenbereich Ω. Dann kann auch jede zu Ω gleichmächtige Menge Ω^* als Operatorenbereich für $\mathfrak{G}$ genommen werden. Ebenso kann man jede zu $\mathfrak{G}$ isomorphe Gruppe $\overline{\mathfrak{G}}$ als Gruppe mit dem Operatorenbereich Ω auffassen.

4. Ebenso wie man in D (35.4) bezüglich der inneren Verknüpfung von $\overline{\mathfrak{G}}$ nur *M I* zu fordern brauchte (vgl. F (18.2)), könnte man sich bezüglich der Operatoranwendung auf $\overline{\mathfrak{G}}$ mit *O I* begnügen, weil *O II* beim Vorliegen eines Operatorhomomorphismus ohnehin folgt. In diesem Sinne wäre eine Aussage wie „das operatorhomomorphe Bild einer Gruppe mit dem Operatorenbereich Ω ist selbst eine Gruppe mit diesem Operatorenbereich" zu interpretieren.

5. Über Aufgabe 4 hinaus kann man sogar noch auf die Forderung von *O I* für $\overline{\mathfrak{G}}$ verzichten, wenn man dafür die Zulässigkeit des als Kern bei dem Homomorphismus $\mathfrak{G} \xrightarrow{\sim} \overline{\mathfrak{G}}$ auftretenden Normalteilers voraussetzt und die Operatoranwendung durch
$$\alpha\,\overline{a} = \overline{\alpha\, a} \text{ für } \alpha \in \Omega \text{ und } \overline{a} \in \overline{\mathfrak{G}}$$
von $\mathfrak{G}$ auf $\overline{\mathfrak{G}}$ überträgt. Dann ist $\overline{\mathfrak{G}}$ ebenfalls Gruppe mit dem Operatorenbereich Ω und operatorhomomorphes Bild von $\mathfrak{G}$. (Ein Spezialfall dieser Aufgabe wurde in S (35.6) gelöst.)

6. Es sei $\mathfrak{R}$ ein Ring und $\mathfrak{a}$ ein zweiseitiges Ideal von $\mathfrak{R}$. Welcher Unterschied besteht zwischen der homomorphen Abbildung des Ringes $\mathfrak{R}$ auf $\mathfrak{R}/\mathfrak{a}$ und der operatorhomomorphen Abbildung des Moduls $\mathfrak{R}^+$ mit dem Linksoperatorenbereich $\mathfrak{R}$ auf $\mathfrak{R}^+/\mathfrak{a}$?

§ 36. $\mathfrak{R}$-Moduln und Vektorräume über Ringen

In Fortsetzung unserer Untersuchungen im vorigen Paragraphen berücksichtigen wir nun auch den Fall, daß im Operatorenbereich innere Verknüpfungen gegeben sind. Dabei setzen wir voraus, daß die Gruppe $\mathfrak{G}$ abelsch ist und damit als Modul geschrieben werden

kann und daß der Operatorenbereich ein Ring $\mathfrak{R}$ ist. Wie wir über D(35.1) hinausgehend die inneren Verknüpfungen von $\mathfrak{R}$ axiomatisch zu berücksichtigen haben, können wir ebenfalls aus den am Anfang von § 35 nochmals erwähnten Beispielen entnehmen.

Definition **D (36.1)**

Es sei $\mathfrak{G}$ ein Modul mit den Elementen $a, b, \ldots$ und $\mathfrak{R}$ ein Ring mit den Elementen $\alpha, \beta, \ldots$.

Dann heißt $\mathfrak{G}$ ein $\mathfrak{R}$-Linksmodul, wenn eine linksseitige Operatoranwendung der Elemente von $\mathfrak{R}$ auf die Elemente von $\mathfrak{G}$ erklärt ist, die folgende Eigenschaften besitzt:

O I: αa *ist ein eindeutig bestimmtes Element von* $\mathfrak{G}$

O II: $\alpha(a+b) = \alpha a + \alpha b$

O III: $(\alpha+\beta)a = \alpha a + \beta a$

O III′: $(\alpha \cdot \beta)a = \alpha(\beta a)$

Insbesondere heißt ein $\mathfrak{R}$-Linksmodul $\mathfrak{G}$ unitär, wenn $\mathfrak{R}$ ein Einselement ε besitzt und dieses Einsoperator für alle Elemente aus $\mathfrak{G}$ ist:

O IV: $\varepsilon a = a$.

Entsprechend erklärt man den Begriff des $\mathfrak{R}$-Rechtsmoduls[1]).

Es versteht sich von selbst, wie die Relationen dieser Definition für den Fall mehrerer Summanden bzw. Faktoren auszudehnen sind. Ferner folgen aus *O II* und *O III* weitere Relationen, die teilweise schon in F(35.2) aufgetreten sind und die insbesondere lehren, daß wir die Nullelemente $o_{\mathfrak{G}} \in \mathfrak{G}$ und $o_{\mathfrak{R}} \in \mathfrak{R}$ in der Bezeichnung nicht zu unterscheiden brauchen (vgl. Aufg. 3):

Folgerung **F (36.2)**

Es gilt für beliebige $\alpha \in \mathfrak{R}$ und $a \in \mathfrak{G}$:

$$o_{\mathfrak{R}} a = \alpha o_{\mathfrak{G}} = o_{\mathfrak{G}}$$
$$(-\alpha)a = \alpha(-a) = -(\alpha a).$$

1) Wir werden aber im folgenden unter $\mathfrak{R}$-Moduln stets $\mathfrak{R}$-Linksmoduln verstehen und nur diese behandeln, da sich ja offensichtlich alle Aussagen über $\mathfrak{R}$-Linksmoduln unter Vertauschung von „links" und „rechts" auf $\mathfrak{R}$-Rechtsmoduln übertragen lassen.

Weiterhin ist jeder zulässige Untermodul eines $\mathfrak{R}$-Moduls wieder ein $\mathfrak{R}$-Modul, und man verwendet abkürzend die Bezeichnung $\mathfrak{R}$-Untermodul. Alle $\mathfrak{R}$-Untermoduln eines unitären $\mathfrak{R}$-Moduls sind selbst unitär (vgl. Aufg. 4).

Bei dem folgenden grundlegenden Beispiel handelt es sich um eine Verallgemeinerung bekannter Betrachtungen aus der analytischen Geometrie. Dazu gehen wir von der Menge aller geordneten n-tupel $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ mit Elementen aus einem (nicht notwendig kommutativen) Ring $\mathfrak{R}$ aus und erklären zunächst Gleichheit und Addition solcher n-tupel:

(I) Es ist $(\alpha_1, \ldots, \alpha_n) = (\alpha_1', \ldots, \alpha_n')$ genau dann, wenn $\alpha_1 = \alpha_1', \ldots, \alpha_n = \alpha_n'$.

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

Durch diese Festlegungen wird die Menge der n-tupel zu einem Modul $\mathfrak{G}$, da sich die Moduleigenschaft von $\mathfrak{R}$ durch komponentenweises Rechnen überträgt. Insbesondere ist $(o, o, \ldots, o)$ das Nullelement und $(-\alpha_1, -\alpha_2, \ldots, -\alpha_n)$ das zu $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ entgegengesetzte Element. Dieser Modul $\mathfrak{G}$ wird vermöge der Festsetzung

$$\alpha(\alpha_1, \ldots, \alpha_n) = (\alpha\alpha_1, \ldots, \alpha\alpha_n) \text{ für alle } \alpha \in \mathfrak{R}$$

zu einem $\mathfrak{R}$-Linksmodul und sogar zu einem unitären $\mathfrak{R}$-Linksmodul, falls $\mathfrak{R}$ ein Einselement besitzt (vgl. Aufg. 2).

Nimmt man für $\mathfrak{R}$ speziell den Körper der reellen (oder auch der komplexen) Zahlen, so geht unser Beispiel in die übliche Erklärung von Vektoren mit n Komponenten, ihrer Gleichheit, ihrer Summe und ihres Produktes mit einem Skalar über. Auch im folgenden mag man sich diesen Spezialfall vor Augen halten, zumal ihm viele Begriffsbildungen und Benennungen entlehnt werden. So stellen wir z. B. fest, daß sich jeder solche Vektor eindeutig als *Linearkombination*

$$(\alpha_1, \alpha_2, \ldots, \alpha_n) = \alpha_1 u_1 + \alpha_2 u_2 + \ldots + \alpha_n u_n$$

der n Vektoren

$$u_1 = (1, 0, \ldots, 0)$$
$$u_2 = (0, 1, \ldots, 0)$$
$$\ldots\ldots\ldots\ldots$$
$$u_n = (0, 0, \ldots, 1)$$

mit Koeffizienten $\alpha_1, \alpha_2, \ldots, \alpha_n$ aus $\mathfrak{R}$ schreiben läßt, während zwischen diesen Basisvektoren keine lineare Relation besteht. In Verallgemeinerung dieses Sachverhaltes erklären wir:

Definition **D (36.3)**

Es sei $\mathfrak{G}$ ein $\mathfrak{R}$-Modul. Dann heißt eine (endliche oder unendliche) Untermenge $\mathfrak{M}$ von $\mathfrak{G}$ linear abhängig, wenn es irgendwie endlich viele (voneinander verschiedene) Elemente $a_1, a_2, \ldots, a_r$ aus $\mathfrak{M}$ gibt, für die mit geeigneten $\lambda_1, \lambda_2, \ldots, \lambda_r$ aus $\mathfrak{R}$

$$\lambda_1 a_1 + \lambda_2 a_2 + \ldots + \lambda_r a_r = o$$

gilt, ohne daß alle $\lambda_i = o$ sind. Folgt dagegen aus jeder solchen Linearkombination stets $\lambda_1 = \lambda_2 = \ldots = \lambda_r = o$, so heißt die Menge $\mathfrak{M} \subseteq \mathfrak{G}$ linear unabhängig.

Offensichtlich ist jede Obermenge einer linear abhängigen Menge erst recht linear abhängig, während jede Untermenge (und damit auch jedes Element) einer linear unabhängigen Menge wieder linear unabhängig ist.

Definition **D (36.4)**

Existiert in einem $\mathfrak{R}$-Modul $\mathfrak{G}$ eine Untermenge $\mathfrak{M}$ derart, daß jedes Element $a \in \mathfrak{G}$ als Linearkombination

$$a = \alpha_1 u_1 + \alpha_2 u_2 + \ldots + \alpha_r u_r$$

aus endlich vielen $u_i \in \mathfrak{M}$ mit $\alpha_i \in \mathfrak{R}$ geschrieben werden kann, so nennen wir $\mathfrak{M}$ ein Erzeugendensystem von $\mathfrak{G}$ über $\mathfrak{R}$.

Insbesondere heißt $\mathfrak{G}$ ein endlicher $\mathfrak{R}$-Modul, wenn es wenigstens ein endliches Erzeugendensystem gibt[1]*, bzw. ein Vektorraum über $\mathfrak{R}$, wenn $\mathfrak{G}$ wenigstens ein linear unabhängiges Erzeugendensystem besitzt. Ein linear unabhängiges Erzeugendensystem eines Vektorraumes $\mathfrak{G}$ über $\mathfrak{R}$ heißt auch Basis von $\mathfrak{G}$ über $\mathfrak{R}$.*

---

1) Ein endlicher $\mathfrak{R}$-Modul $\mathfrak{G}$ braucht nicht etwa „endlich" im Sinne der Mengenlehre zu sein; vielmehr wird er im allgemeinen unendlich viele Elemente enthalten, die sich jedoch bereits aus den endlich vielen Elementen $u_1, u_2, \ldots, u_n$ eines festgewählten Erzeugendensystems $\mathfrak{M}$ mit Koeffizienten aus $\mathfrak{R}$ linear kombinieren lassen. Mit Hilfe der Komplexschreibweise kann man dies durch

$$\mathfrak{G} = \mathfrak{R}u_1 + \mathfrak{R}u_2 + \ldots + \mathfrak{R}u_n$$

ausdrücken, wenn man unter $\mathfrak{R}u$ den Komplex aller Elemente αu von $\mathfrak{G}$ versteht, der aus festem $u \in \mathfrak{G}$ durch Anwendung aller Operatoren $\alpha \in \mathfrak{R}$ hervorgeht.

Zur Erläuterung des Begriffes „Erzeugendensystem" sei folgendes bemerkt: Ist $\mathfrak{M}$ eine beliebige Teilmenge eines $\mathfrak{R}$-Moduls $\mathfrak{G}$, so kann man einerseits die Gesamtheit aller Linearkombinationen $\Sigma\alpha_i u_i$ mit $\alpha_i \in \mathfrak{R}$, $u_i \in \mathfrak{M}$ betrachten; sie bildet offensichtlich einen $\mathfrak{R}$-Untermodul von $\mathfrak{G}$, den wir für den Augenblick durch $\mathfrak{R}\mathfrak{M}$ symbolisieren. Andererseits kann man zu $\mathfrak{R}\mathfrak{M}$ noch die Gesamtheit aller ganzzahligen Linearkombinationen $\Sigma g_i u_i$ mit $g_i \in \Gamma$, $u_i \in \mathfrak{M}$ hinzunehmen und erhält ebenfalls einen $\mathfrak{R}$-Untermodul von $\mathfrak{G}$, den wir mit $\mathfrak{R}\mathfrak{M} + \Gamma\mathfrak{M}$ bezeichnen. Offenbar gilt:

$$\mathfrak{R}\mathfrak{M} \subseteq \mathfrak{R}\mathfrak{M} + \Gamma\mathfrak{M} \subseteq \mathfrak{G}.$$

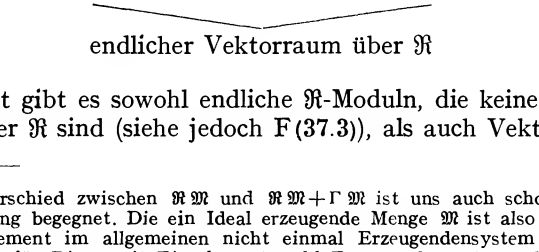
Dabei ist $\mathfrak{R}\mathfrak{M} + \Gamma\mathfrak{M}$ der kleinste $\mathfrak{R}$-Modul, der $\mathfrak{M}$ enthält, also im bisherigen Sprachgebrauch der „von $\mathfrak{M}$ erzeugte" $\mathfrak{R}$-Modul (vgl. etwa D(5.12) und S(5.13) für Gruppen, S(28.6) bis S(28.11) für Ideale). Dagegen heißt $\mathfrak{M}$ gemäß D(36.4) Erzeugendensystem von $\mathfrak{G}$, wenn $\mathfrak{R}\mathfrak{M} = \mathfrak{G}$ gilt. Die obige Beziehung lehrt dann, daß ein Erzeugendensystem im Sinne von D(36.4) im Einklang mit der bisherigen Sprechweise $\mathfrak{G}$ als den kleinsten $\mathfrak{R}$-Modul liefert, der $\mathfrak{M}$ enthält. Das Umgekehrte braucht hingegen nicht zu gelten, denn es ist durchaus

$$\mathfrak{R}\mathfrak{M} \subset \mathfrak{R}\mathfrak{M} + \Gamma\mathfrak{M} = \mathfrak{G}$$

möglich (man wähle etwa für $\mathfrak{R}$ den Ring der geraden Zahlen, für $\mathfrak{G}$ den Modul aller ganzzahligen Vielfachen von 4 und $\mathfrak{M} = \mathfrak{G}$)[1]).

Für den ohnehin im Vordergrund stehenden Fall (vgl. auch S(36.5)), daß $\mathfrak{G}$ ein unitärer $\mathfrak{R}$-Modul ist, gilt natürlich $\mathfrak{R}\mathfrak{M} = \mathfrak{R}\mathfrak{M} + \Gamma\mathfrak{M}$, so daß dann auch umgekehrt jede Teilmenge $\mathfrak{M}$ von $\mathfrak{G}$, für die $\mathfrak{G}$ der kleinste $\mathfrak{M}$ umfassende $\mathfrak{R}$-Modul ist, Erzeugendensystem im Sinne von D(36.4) ist.

Die gegenseitige Beziehung der damit definierten Strukturbegriffe lehrt die folgende Übersicht:



In der Tat gibt es sowohl endliche $\mathfrak{R}$-Moduln, die keine Vektorräume über $\mathfrak{R}$ sind (siehe jedoch F(37.3)), als auch Vektorräume

---

1) Der Unterschied zwischen $\mathfrak{R}\mathfrak{M}$ und $\mathfrak{R}\mathfrak{M} + \Gamma\mathfrak{M}$ ist uns auch schon bei der Idealerzeugung begegnet. Die ein Ideal erzeugende Menge $\mathfrak{M}$ ist also für Ringe ohne Einselement im allgemeinen nicht einmal Erzeugendensystem im Sinne von D(36.4), für Ringe mit Einselement wohl Erzeugendensystem, aber im allgemeinen keine Basis im Sinne von D(36.4) des als $\mathfrak{R}$-Modul aufgefaßten Ideals (vgl. Aufg. 5). Daß man trotzdem im Zusammenhang mit Idealen das Wort „Basis" wie in D(28.10), also entgegen der allgemeinen Begriffsbildung für $\mathfrak{R}$-Moduln gebraucht, hat sich durch die historische Entwicklung eingebürgert.

über $\mathfrak{R}$, die keine endlichen $\mathfrak{R}$-Moduln sind. Wir geben Beispiele dafür in den Aufgaben 5 und 6. Dagegen ist der $\mathfrak{R}$-Linksmodul $\mathfrak{G}$ der n-tupel $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ mit Elementen α_i aus einem Ring mit einem Rechtseinselement ε[1]) sowohl endlicher $\mathfrak{R}$-Modul als auch Vektorraum über $\mathfrak{R}$, also endlicher Vektorraum über $\mathfrak{R}$. Ein endliches Erzeugendensystem bilden nämlich etwa (vgl. die entsprechenden Überlegungen vor D(36.3))

$$\begin{aligned} u_1 &= (\varepsilon, o, \ldots, o) \\ u_2 &= (o, \varepsilon, \ldots, o) \\ &\cdots\cdots\cdots\cdots \\ u_n &= (o, o, \ldots, \varepsilon). \end{aligned}$$

Dieses System ist auch linear unabhängig, da

$$\begin{aligned} \sum_{i=1}^{n} \lambda_i u_i &= (\lambda_1, o, \ldots, o) + \ldots + (o, o, \ldots, \lambda_n) \\ &= (\lambda_1, \lambda_2, \ldots, \lambda_n) = o \end{aligned}$$

dann und nur dann gilt, wenn alle λ_i verschwinden. Offensichtlich ist dagegen jedes aus $u_1, u_2, \ldots, u_n$ durch Hinzunahme weiterer Elemente aus $\mathfrak{G}$ entstehende Erzeugendensystem linear abhängig. So sind also alle in der analytischen Geometrie betrachteten n-dimensionalen Vektorräume endliche Vektorräume über dem Körper $\mathfrak{R}$ der reellen (bzw. komplexen) Zahlen im Sinne unserer Definition D(36.4).

Ferner bilden die komplexen Zahlen einen Vektorraum über dem Körper der reellen Zahlen mit den Basiselementen 1 und i, entsprechend die Quaternionen mit den Basiselementen $1, i, j, k$. Auch die in B(26.4a) betrachteten Strukturen sind Vektorräume mit den Basiselementen 1 und $\sqrt{k}$ über dem Ring der ganzen Zahlen bzw. über dem Körper der rationalen Zahlen. Solche Körper und Ringe, die man als Vektorräume über anderen Körpern und Ringen auffassen kann, sind ja entsprechend unserer Einleitung ein wesentliches Ziel dieses Kapitels. Wir werden ihre Gesetzmäßigkeiten in § 38 genauer untersuchen.

---

1) Wie wir hier nur mitteilen wollen, gilt auch umgekehrt: Existiert über einem Ring $\mathfrak{R}$ ein (linksseitiger) Vektorraum, so besitzt $\mathfrak{R}$ wenigstens ein Rechtseinselement (G. PICKERT, Math. Ann. 120 (1948) S. 158).

Die Vorteile, die die Existenz[1]) eines Erzeugendensystemes $\mathfrak{M}$ für eine bequeme Schreibweise der Elemente eines $\mathfrak{R}$-Moduls als Linearkombinationen mit sich bringt, liegen auf der Hand. Insbesondere ist ein solcher $\mathfrak{R}$-Modul stets unitär, wenn nur der Ring $\mathfrak{R}$ ein Einselement besitzt:

Satz **S (36.5)**

Ist $\mathfrak{R}$ ein Ring mit Einselement ε, so besitzt ein $\mathfrak{R}$-Modul $\mathfrak{G}$ dann und nur dann ein Erzeugendensystem, wenn ε Einsoperator ist. Damit sind also endliche $\mathfrak{R}$-Moduln sowie Vektorräume über einem Ring $\mathfrak{R}$ mit Einselement stets unitär.

Beweis

Läßt sich jedes Element $a \in \mathfrak{G}$ als Linearkombination $a = \Sigma \alpha_i u_i$ von Elementen $u_1, \ldots, u_r$ eines Erzeugendensystems $\mathfrak{M}$ von $\mathfrak{G}$ mit Koeffizienten $\alpha_1, \ldots, \alpha_r$ aus $\mathfrak{R}$ schreiben, so folgt

$$\varepsilon a = \varepsilon \Sigma \alpha_i u_i = \Sigma \varepsilon (\alpha_i u_i) = \Sigma (\varepsilon \alpha_i) u_i = \Sigma \alpha_i u_i = a.$$

Ist umgekehrt ε Einsoperator für $\mathfrak{G}$, so besitzt $\mathfrak{G}$ wenigstens ein Erzeugendensystem über $\mathfrak{R}$, nämlich $\mathfrak{G}$ selbst. qed.

Die Bedeutung der linearen Unabhängigkeit eines Erzeugendensystems lehrt der folgende (von der Existenz eines Einselementes unabhängige)

Satz **S (36.6)**

Ein Erzeugendensystem $\mathfrak{M}$ eines $\mathfrak{R}$-Moduls $\mathfrak{G}$ ist dann und nur dann linear unabhängig, wenn in der Linearkombination

$$a = \alpha_1 u_1 + \alpha_2 u_2 + \ldots + \alpha_r u_r \quad \text{mit } u_i \in \mathfrak{M},\ \alpha_i \in \mathfrak{R}$$

eines jeden Elementes $a \in \mathfrak{G}$ die Koeffizienten $\alpha_1, \alpha_2, \ldots, \alpha_r$ eindeutig bestimmt sind.

Beweis

1. Gestattet ein Element $a \in \mathfrak{G}$ zwei verschiedene Linearkombinationen, so können wir zunächst erreichen, daß in beiden dieselben Elemente $u_i \in \mathfrak{M}$ auftreten, indem wir eventuell fehlende mit dem Koeffizienten o hinzufügen. Aus

$$a = \alpha_1 u_1 + \alpha_2 u_2 + \ldots + \alpha_r u_r$$
$$a = \alpha_1' u_1 + \alpha_2' u_2 + \ldots + \alpha_r' u_r$$

1) Daß es auch $\mathfrak{R}$-Moduln gibt, die kein Erzeugendensystem besitzen, zeigt das Beispiel im Kleindruck nach **D (36.4)**.

folgt dann nach *O III* und F(36.2)

$$o = (\alpha_1 - \alpha_1')\,u_1 + (\alpha_2 - \alpha_2')\,u_2 + \ldots + (\alpha_r - \alpha_r')\,u_r,$$

wobei nach Voraussetzung nicht alle Koeffizienten $(\alpha_i - \alpha_i')$ verschwinden. Also ist $\mathfrak{M}$ linear abhängig.

2. Ist umgekehrt $\mathfrak{M}$ linear abhängig, existiert also eine Linearkombination

$$o = \lambda_1 u_1 + \lambda_2 u_2 + \ldots + \lambda_r u_r,$$

in der es wenigstens einen Koeffizienten $\lambda_i \neq o$ gibt, so haben wir bereits zwei verschiedene Darstellungen des Elementes $o \in \mathfrak{G}$. Es ist nämlich nach F(36.2) auch

$$o = o\,u_1 + o\,u_2 + \ldots + o\,u_r. \qquad \text{qed.}$$

Nach S(36.6) ist also in einem Vektorraum $\mathfrak{G}$ über $\mathfrak{R}$ jedes Element durch das System seiner Koeffizienten bezüglich einer festen Basis umkehrbar eindeutig gekennzeichnet. Darüber hinaus ist aber auch das Rechnen mit Elementen aus $\mathfrak{G}$ vollständig zurückzuführen auf das Rechnen mit ihren Koeffizientensystemen:

Satz **S(36.7)**

Über einem Ring $\mathfrak{R}$ sind alle Vektorräume, die eine Basis von n Elementen haben, zueinander operatorisomorph.

Beweis

Es seien $\mathfrak{G}$ und $\overline{\mathfrak{G}}$ zwei Vektorräume über $\mathfrak{R}$ mit den Basen $\{u_1, \ldots, u_n\}$ bzw. $\{\bar{u}_1, \ldots, \bar{u}_n\}$. Dann vermittelt die Zuordnung

$$a = \sum_i \alpha_i u_i \to \bar{a} = \sum_i \alpha_i \bar{u}_i$$

einen Operatorisomorphismus von $\mathfrak{G}$ auf $\overline{\mathfrak{G}}$. Sie ist nämlich wegen der linearen Unabhängigkeit beider Basen nach S(36.6) eineindeutig, wobei offensichtlich alle Elemente von $\overline{\mathfrak{G}}$ als Bilder auftreten. Die Relationstreue bezüglich der Addition und Operatoranwendung ergibt sich unter Verwendung von *O III* und *O III'* für $\mathfrak{G}$ mit

$$a + b = \Sigma \alpha_i u_i + \Sigma \beta_i u_i = \Sigma (\alpha_i + \beta_i) u_i$$
$$\alpha a = \alpha \Sigma \alpha_i u_i = \Sigma \alpha (\alpha_i u_i) = \Sigma (\alpha \alpha_i) u_i$$

unter Verwendung von *O III* und *O III'* für $\overline{\mathfrak{G}}$ aus

$$\overline{a + b} = \Sigma (\alpha_i + \beta_i) \bar{u}_i = \Sigma \alpha_i \bar{u}_i + \Sigma \beta_i \bar{u}_i = \bar{a} + \bar{b}$$
$$\overline{\alpha a} = \Sigma (\alpha \alpha_i) \bar{u}_i = \Sigma \alpha (\alpha_i \bar{u}_i) = \Sigma \alpha \alpha_i \bar{u}_i = \alpha \bar{a}. \qquad \text{qed.}$$

Zum Verständnis dieses Satzes beachte man, daß die Basis eines Vektorraumes (von Ausnahmefällen abgesehen) nicht eindeutig bestimmt ist (vgl. z. B. Aufg. 8). Viele Betrachtungen der analytischen Geometrie beruhen ja gerade auf dem Übergang von einer Basis zu einer anderen, wobei allerdings alle Basen aus jeweils gleich vielen Elementen bestehen. Es ist aber auch möglich, daß ein Vektorraum über einem Ring $\mathfrak{R}$ Basen mit verschieden vielen Elementen hat[1]). Die Voraussetzung in S(36.7) ist also so zu verstehen, daß in jedem der Vektorräume wenigstens eine Basis von n Elementen existiert, unabhängig davon, welche Basen sonst noch vorhanden sind (vgl. allerdings S(37.5)).

S(36.7) gilt allgemein ohne die Einschränkung auf endliche Basen, wenn man ihn statt für Basen gleicher Elementanzahl für gleichmächtige Basen formuliert. Die Überlegungen des Beweises treffen nämlich auch für zwei unendliche Basen gleicher Mächtigkeit zu, da deren Elemente ebenfalls nach Voraussetzung eineindeutig aufeinander bezogen werden können und jedes Element nach D(36.4) Linearkombination von nur endlich vielen Basiselementen ist. Die Summationen werden dann lediglich über die in den Linearkombinationen von a oder b tatsächlich auftretenden Basiselemente erstreckt.

Folgerung **F(36.8)**

Jeder Vektorraum $\mathfrak{G}$ über einem Ring $\mathfrak{R}$ mit Rechtseinselement ε, der eine Basis von n Elementen besitzt, ist operatorisomorph zum Vektorraum $\overline{\mathfrak{G}}$ aller geordneten n-tupel $(\alpha_1, \ldots, \alpha_n)$ mit Elementen α_i aus $\mathfrak{R}$.

Wie schon gezeigt, besitzt $\overline{\mathfrak{G}}$ als Basis nämlich die n Elemente $\bar{u}_1 = (\varepsilon, o, \ldots, o), \ldots, \bar{u}_n = (o, o, \ldots, \varepsilon)$. Die im Beweis von S(36.7) angegebene Zuordnung wird bezüglich dieser Basis zu

$$a = \sum_i \alpha_i u_i \to \bar{a} = \sum_i \alpha_i \bar{u}_i = (\alpha_1, \ldots, \alpha_n).$$

Wir haben damit in den aus solchen n-tupeln gebildeten Vektorräumen passende Modelle für jeden endlichen Vektorraum im Einklang mit der Tatsache, daß entsprechend der Beweisführung von S(36.7) die n Basiselemente eines Vektorraumes ohnehin keine andere Bedeutung haben, als die Stellung des jeweiligen Koeffizienten aus $\mathfrak{R}$ festzulegen.

1) So gibt etwa C. J. EVERETT einen Vektorraum an, der Basen von jeder endlichen Elementenanzahl hat (Bull. Amer. Math. Soc. 48 (1942) S. 312—316).

Wir begnügen uns damit, F (36.8) wenigstens auf Vektorräume mit abzählbar unendlichen Basen auszudehnen. Man braucht nämlich von den n-tupeln nur zu geordneten Elementensystemen $(\alpha_1, \alpha_2, \ldots)$ mit abzählbar unendlich vielen Komponenten überzugehen, wobei jeweils nur endlich viele α_i verschieden von o sind. Gleichheit, Addition sowie Operatoranwendung ist wie bei n-tupeln zu erklären. Dann erhalten wir einen Vektorraum mit den abzählbar unendlich vielen Basiselementen

$$(\varepsilon, o, o, \ldots), (o, \varepsilon, o, \ldots), \ldots,$$

der ein Modell aller Vektorräume mit abzählbar unendlichen Basen ist.

Von diesem Modell haben wir übrigens bereits bei der Konstruktion des Polynomringes $\mathfrak{R}[x]$ Gebrauch macht, wobei gerade die Potenzen von $x = (o, \varepsilon, o, \ldots)$ die eben genannten Basiselemente abgeben. Allerdings wird dort die Operatoranwendung der Elemente aus $\mathfrak{R}$ nicht als solche definiert, sondern folgt nach der Identifizierung von $a \in \mathfrak{R}$ mit $(a, o, o, \ldots)$ aus der Festlegung der Produktbildung.

Abschließend wollen wir noch auf den Zusammenhang eingehen, der zwischen Matrizenringen und endlichen Vektorräumen besteht. Es kann nämlich jeder Operatorendomorphismus eines solchen Vektorraumes bei Zugrundelegung einer festen endlichen Basis eineindeutig durch eine Matrix charakterisiert werden, und die Rechenregeln für Matrizen sind gerade so beschaffen, daß die Summe der Matrizen der Summe der zugehörigen Endomorphismen und das Produkt zweier Matrizen der Nacheinanderausführung dieser Endomorphismen entspricht.

Satz **S (36.9)**

Es sei $\mathfrak{R}$ ein Ring mit Einselement und $\mathfrak{G}$ ein Vektorraum über $\mathfrak{R}$ mit einer Basis von n Elementen. Dann ist der Ring $\mathfrak{S}$ aller Operatorendomorphismen von $\mathfrak{G}$ isomorph zum vollen Matrizenring $\mathfrak{M}_n(\mathfrak{R})$.

Beweis

1. Wir stellen zunächst fest, daß die Menge $\mathfrak{S}$ aller Operatorendomorphismen von $\mathfrak{G}$ tatsächlich ein Ring ist. Dazu können wir uns auf B (26.5) stützen, da nämlich jeder Operatorendomorphismus von $\mathfrak{G}$ erst recht ein Endomorphismus von $\mathfrak{G}$ im gewöhnlichen Sinne ist und wir damit lediglich $\mathfrak{S}$ als Unterring des Endomorphismenringes von $\mathfrak{G}$ nachzuweisen haben. Differenz und Produkt zweier Operatorendomorphismen σ_1 und σ_2 sind aber nicht nur wieder

Endomorphismen (vgl. B(26.5)), sondern sogar Operatorendomorphismen wegen

$$(\alpha a)^{\sigma_1-\sigma_2} = (\alpha a)^{\sigma_1} - (\alpha a)^{\sigma_2} = \alpha a^{\sigma_1} - \alpha a^{\sigma_2} = \alpha (a^{\sigma_1} - a^{\sigma_2}) = \alpha a^{\sigma_1-\sigma_2}$$

$$(\alpha a)^{\sigma_1 \cdot \sigma_2} = ((\alpha a)^{\sigma_1})^{\sigma_2} = (\alpha a^{\sigma_1})^{\sigma_2} = \alpha (a^{\sigma_1})^{\sigma_2} = \alpha a^{\sigma_1 \cdot \sigma_2}.$$

2. Als nächstes zeigen wir, daß der Ring $\mathfrak{S}$ eineindeutig *in* den Ring $\mathfrak{M}_n(\mathfrak{R})$ abgebildet werden kann. Dazu benutzen wir, daß nach Voraussetzung jedes Element von $\mathfrak{G}$ eindeutig als Linearkombination

$$a = \alpha_1 u_1 + \ldots + \alpha_n u_n \qquad (\alpha_i \in \mathfrak{R})$$

von n fest gewählten Basiselementen $u_1, \ldots, u_n$ schreibbar ist. Jeder Operatorendomorphismus $\sigma \in \mathfrak{S}$ bestimmt nun einerseits zu jedem Basiselement u_i eindeutig ein Bild $u_i^\sigma = \overline{u_i}$ und ist andererseits damit bereits vollständig festgelegt. Nach D(35.4) gilt nämlich für jedes $a \in \mathfrak{G}$

$$a^\sigma = \bar{a} = \overline{\sum \alpha_i u_i} = \sum \overline{\alpha_i u_i} = \sum \alpha_i \overline{u_i}.$$

Die Bilder der Basiselemente sind aber selbst Elemente aus $\mathfrak{G}$ und daher Linearkombinationen

$$(\dagger) \qquad u_i^\sigma = \overline{u_i} = \sum_{k=1}^{n} \alpha_{ik} u_k \qquad (i = 1, \ldots, n).$$

Auf diese Weise ist dem Operatorendomorphismus $\sigma \in \mathfrak{S}$ die Matrix $(\alpha_{ik}) \in \mathfrak{M}_n(\mathfrak{R})$ nach S(36.6) eineindeutig zugeordnet.

3. Diese Abbildung ist sogar eine Abbildung von $\mathfrak{S}$ *auf* $\mathfrak{M}_n(\mathfrak{R})$, d. h., zu jeder beliebigen Matrix $(\alpha_{ik}) \in \mathfrak{M}_n(\mathfrak{R})$ gibt es einen Operatorendomorphismus $\sigma \in \mathfrak{S}$, der vermöge (†) diese Matrix zum Bild hat.

Um dieses σ zu finden, erklären wir mit Hilfe der Matrix (α_{ik}) zunächst eine eindeutige Abbildung der Basiselemente u_i von $\mathfrak{G}$ auf Elemente $\overline{u_i} \in \mathfrak{G}$:

$$(*) \qquad u_i \to \overline{u_i} = \sum_{k=1}^{n} \alpha_{ik} u_k \qquad (i = 1, \ldots, n).$$

Diese läßt sich zu einer eindeutigen Abbildung aller Elemente von $\mathfrak{G}$ ausdehnen vermöge der Festsetzung:

$$(**) \qquad a = \sum_i x_i u_i \to \bar{a} = \sum_i \alpha_i \overline{u_i} = \sum_{i,k} \alpha_i \alpha_{ik} u_k.$$

In der Tat ist (**) eine Erweiterung der Abbildung (*), da das Einselement ε gemäß S(36.5) Einsoperator ist und damit (**) für den Fall $a = u_i = o u_1 + \ldots + \varepsilon u_i + \ldots + o u_n$ in (*) übergeht[1]). Die so erhaltene eindeutige Abbildung von $\mathfrak{G}$ in sich ist auch relationstreu bezüglich der Addition und der Operatoranwendung, wie aus (**) hervorgeht. Sie ist also tatsächlich der gesuchte Operatorendomorphismus $\sigma \in \mathfrak{S}$, der vermöge (†) auf die Matrix (α_{ik}) abgebildet wird.

4. Die in 2. hergestellte Zuordnung ist relationstreu bezüglich der Addition und Multiplikation. Mit

$$\sigma \to (\alpha_{ik}): \qquad u_i^{\sigma} = \sum_k \alpha_{ik} u_k$$

$$\tau \to (\beta_{ik}): \qquad u_i^{\tau} = \sum_k \beta_{ik} u_k$$

gilt nämlich

$$\sigma + \tau \to (\alpha_{ik} + \beta_{ik}) \text{ und } \sigma \cdot \tau \to \left(\sum_k \alpha_{ik} \beta_{kl}\right)$$

wegen:

$$u_i^{\sigma+\tau} = u_i^{\sigma} + u_i^{\tau} = \sum_k \alpha_{ik} u_k + \sum_k \beta_{ik} u_k = \sum_k (\alpha_{ik} + \beta_{ik}) u_k$$

$$u_i^{\sigma \cdot \tau} = (u_i^{\sigma})^{\tau} = \left(\sum_k \alpha_{ik} u_k\right)^{\tau} = \sum_k \alpha_{ik} u_k^{\tau} = \sum_k \alpha_{ik} \left(\sum_l \beta_{kl} u_l\right)$$

$$= \sum_l \left(\sum_k \alpha_{ik} \beta_{kl}\right) u_l .$$

qed.

Der gewählte Beweisgang läßt deutlich hervortreten, daß die Erklärung von Summe und Produkt quadratischer Matrizen ihrer Auffassung als lineare Abbildungen entspricht. Insbesondere ist damit die Gültigkeit der Ringaxiome für $\mathfrak{M}_n(\mathfrak{R})$ erneut und unabhängig von den Rechnungen in B(26.2) nachgewiesen. Natürlich hätte man auch umgekehrt den Matrizenring auf die Menge $\mathfrak{S}$ aller Operatorendomorphismen isomorph abbilden und damit die Ringeigenschaft von $\mathfrak{S}$ zeigen können. Bei einem solchen Vorgehen entfällt der Teil 1 des Beweises.

---

1) Die Tatsache, daß die Abbildung (**) die Abbildung (*) umfaßt, ist keineswegs selbstverständlich und hängt entscheidend von der Voraussetzung $\varepsilon \in \mathfrak{R}$ ab. Man kann auch allgemein beweisen, daß S(36.9) ohne diese Voraussetzung nicht gilt.

Satz **S (36.10)**

Es sei $\mathfrak{R}$ ein Ring mit Einselement und $\mathfrak{G}$ ein Vektorraum über $\mathfrak{R}$ mit einer Basis von n Elementen. Dann ist die Gruppe Φ aller Operatorautomorphismen von $\mathfrak{G}$ isomorph zur Gruppe aller invertierbaren Matrizen aus $\mathfrak{M}_n(\mathfrak{R})$, der sogenannten vollen linearen Gruppe GL $(n, \mathfrak{R})$.

Beweis

Bei dem im vorangegangenen Satz abgeleiteten Isomorphismus $\mathfrak{S} \longleftrightarrow \mathfrak{M}_n(\mathfrak{R})$ werden nach F (33.2c) insbesondere jeweils solche Elemente aufeinander abgebildet, die ein (zweiseitiges) Inverses besitzen. Es ist also nur zu zeigen, daß diese Elemente $\sigma \in \mathfrak{S}$ genau die Operatorautomorphismen sind. In Aufgabe 6 von § 26 haben wir diesen Sachverhalt bereits kennengelernt, falls man den Operatorenbereich von $\mathfrak{G}$ unberücksichtigt läßt. Der dort geführte Beweis ist aber unabhängig davon, ob es sich bei σ um einen Endomorphismus oder einen Operatorendomorphismus handelt, da er nur aus der Existenz von σ^{-1} auf die von σ vermittelte Zuordnung schließt.

qed.

Damit sind die Matrizen[1]) allgemein in die Zusammenhänge eingeordnet, die dem Leser für den Spezialfall, daß der Ring etwa der Körper der reellen Zahlen ist, aus der analytischen Geometrie geläufig sind. Statt von Operatorendomorphismen spricht man dort allerdings meist von linearen Abbildungen und insbesondere von linearen Transformationen, wenn es sich um Operatorautomorphismen, also um eineindeutige Abbildungen des Raumes auf sich handelt. Letztere sind in diesem Falle bekanntlich dadurch gekennzeichnet, daß die Determinante der zugehörigen Matrix nicht verschwindet.

Wir bemerken noch, daß man an dieses grundlegende Beispiel angelehnt auch oft bei beliebigen $\mathfrak{R}$-Moduln die Bezeichnungen „lineare Abbildung" bzw. „lineare Transformation" verwendet.

---

1) Nichtquadratische Matrizen sind Operatorhomomorphismen eines Vektorraumes in einen anderen zuzuordnen. Auch dann korrespondieren Summen und (mögliche) Produkte von Matrizen zu entsprechenden Verknüpfungen der Operatorhomomorphismen.

Aufgaben zu § 36

1. Man gebe die Relationen aus D(36.1) für einen $\mathfrak{R}$-Rechtsmodul an und begründe, warum man für kommutative Ringe $\mathfrak{R}$ zwischen $\mathfrak{R}$-Links- und $\mathfrak{R}$-Rechtsmoduln nicht zu unterscheiden braucht.

2. Man zeige, daß der Modul $\mathfrak{G}$ der n-tupel $(\alpha_1, \ldots, \alpha_n)$ mit $\alpha_i \in \mathfrak{R}$ vermöge $\alpha(\alpha_1, \ldots, \alpha_n) = (\alpha\alpha_1, \ldots, \alpha\alpha_n)$ für alle $\alpha \in \mathfrak{R}$ zum $\mathfrak{R}$-Linksmodul wird. Er ist unitär, falls $\mathfrak{R}$ ein Einselement ε besitzt.

3. Man beweise F(36.2).

4. Man beweise die im Text auf Seite 100 angegebenen Behauptungen über die zulässigen Untermoduln eines $\mathfrak{R}$-Moduls $\mathfrak{G}$.

5. Beispiel für einen endlichen $\mathfrak{R}$-Modul, der kein Vektorraum über $\mathfrak{R}$ ist, ist jedes Ideal $\mathfrak{a} = (a_1, a_2, \ldots, a_n)$ eines kommutativen Ringes $\mathfrak{R}$ mit Einselement, das kein Hauptideal ist, also etwa $(2, 1 + \sqrt{-5})$ von $\Gamma + \Gamma\sqrt{-5}$ (vgl. Ende § 28) oder $(2, x)$ von $\Gamma[x]$ (Beweis?).

6. Faßt man den Polynomring $\mathfrak{R}[x]$ als Modul $\mathfrak{G}$ mit dem Operatorenbereich $\mathfrak{R}$ auf, so erhält man einen Vektorraum über $\mathfrak{R}$, der kein endliches Erzeugendensystem besitzt.

7. Alle Matrizen vom Typ (m, n) mit Elementen aus einem (nicht notwendig kommutativen) Ring $\mathfrak{R}$ mit Einselement ε bilden einen endlichen Vektorraum $\mathfrak{G}$ über $\mathfrak{R}$. Die Operatoranwendung wird dabei erklärt durch
$$\alpha(a_{ik}) = (\alpha\, a_{ik}).$$

8. Für den Modul $\mathfrak{G}$ der n-tupel $(\alpha_1, \ldots, \alpha_n)$ mit Elementen α_i aus einem Ring $\mathfrak{R}$ mit Einselement ε bilden neben der im Text angegebenen Basis auch die folgenden n-tupel eine Basis:
$$\begin{aligned} v_1 &= (\varepsilon, o, o, \ldots, o) \\ v_2 &= (\varepsilon, \varepsilon, o, \ldots, o) \\ &\cdots\cdots\cdots\cdots \\ v_n &= (\varepsilon, \varepsilon, \varepsilon, \ldots, \varepsilon). \end{aligned}$$

9. Ein Operatorendomorphismus eines Vektorraumes $\mathfrak{G}$ über einem Ring $\mathfrak{R}$ mit Einselement ε ist genau dann ein Operatorautomorphismus, wenn er eine Basis von $\mathfrak{G}$ wieder in eine Basis von $\mathfrak{G}$ überführt.

§ 37. $\mathfrak{R}$-Moduln und Vektorräume über Körpern

Die im vorangegangenen Paragraphen angestellten Betrachtungen lassen sich wesentlich weiterführen, wenn man vom Operatorenbereich sogar die Körpereigenschaft fordert. Diese einschränkende Voraussetzung gleicht unsere Untersuchungen bedeutend mehr an

die dem Leser aus der Vektorrechnung bekannten Strukturverhältnisse an, was eben gerade daran liegt, daß dort mit einem Körper (nämlich dem der reellen oder komplexen Zahlen) als Operatorenbereich gearbeitet wird. Grundlegend für die sich gegenüber $\mathfrak{R}$-Moduln ergebenden weitergehenden Aussagen ist der folgende

Satz **S (37.1)**

In einem unitären $\mathfrak{R}$-Modul $\mathfrak{G}$ mit einem (nicht notwendig kommutativen) Körper $\mathfrak{R}$ als Operatorenbereich folgt aus der linearen Abhängigkeit von r Elementen $a_1, a_2, \ldots, a_r$, daß sich wenigstens ein a_i aus den übrigen linear kombinieren läßt.

Beweis

Nach Voraussetzung gibt es eine Relation

$$\sum_{k=1}^{r} \lambda_k a_k = o,$$

in der nicht alle $\lambda_k \in \mathfrak{R}$ verschwinden. Dann gilt sogar für alle a_i mit $\lambda_i \neq o$:

$$a_i = \sum_{k \neq i} (-\lambda_i^{-1} \lambda_k) a_k.$$

qed.

Dieser Satz hängt in der Tat wesentlich von der Körpereigenschaft des Operatorenbereiches ab und gilt in einem $\mathfrak{R}$-Modul $\mathfrak{G}$ im allgemeinen nicht. Nehmen wir z. B. als $\mathfrak{R}$ den Ring der ganzen Zahlen und als $\mathfrak{G}$ die additive Gruppe dieses Ringes, so sind etwa die Elemente 3 und 7 wegen

$$7 \cdot 3 + (-3) \cdot 7 = 0$$

linear abhängig. Es ist aber weder 3 ein ganzzahliges Vielfaches von 7 noch 7 ein solches von 3.

Folgerung **F (37.2)**

Es sei $\mathfrak{G}$ ein unitärer $\mathfrak{R}$-Modul über einem Körper $\mathfrak{R}$. Dann kann man aus jedem linear abhängigen Erzeugendensystem $\mathfrak{M}$ ein geeignetes Element a streichen, derart daß die Restmenge $\mathfrak{M} \setminus a$ Erzeugendensystem bleibt.

Beweis

Nach D(36.3) gibt es endlich viele linear abhängige Elemente $a_1, a_2, \ldots, a_r$ aus $\mathfrak{M}$. Daraus läßt sich gemäß S(37.1) wenigstens ein a_i aus den übrigen linear kombinieren und kann in dem Erzeugendensystem $\mathfrak{M}$ durch die Linearkombination ersetzt werden.

qed.

Da jeder endliche $\mathfrak{K}$-Modul gemäß S(36.5) unitär ist, ergibt sich daraus durch wiederholte Anwendung[1]) die wichtige

Folgerung **F(37.3)**

Jeder endliche $\mathfrak{K}$-Modul über einem Körper $\mathfrak{K}$ ist ein endlicher Vektorraum über $\mathfrak{K}$.

Liegt also ein Körper $\mathfrak{K}$ als Operatorenbereich vor, so braucht man nicht zwischen endlichen $\mathfrak{K}$-Moduln und endlichen Vektorräumen über $\mathfrak{K}$ zu unterscheiden. Darüber hinaus wird sich im folgenden für eine solche algebraische Struktur ergeben, daß alle linear unabhängigen Erzeugendensysteme aus der gleichen Anzahl von Elementen bestehen. Im Gegensatz zu den Verhältnissen bei Vektorräumen über beliebigen Ringen ist es damit hier unmöglich, daß zwei Vektorräume zueinander operatorisomorph sind, die Basen verschiedener Elementanzahl besitzen.

Vorbereitend beweisen wir dazu den

Satz **S(37.4)**

Es sei $\mathfrak{G}$ ein endlicher Vektorraum über einem Körper $\mathfrak{K}$. Dann kann jedes System linear unabhängiger Elemente $v_1, v_2, \ldots, v_m$ aus $\mathfrak{G}$ durch Elemente einer beliebigen endlichen Basis $\{u_1, u_2, \ldots, u_n\}$ von $\mathfrak{G}$ zu einer Basis von $\mathfrak{G}$ ergänzt werden.

Beweis

Auf Grund der Basiseigenschaft von $\{u_1, u_2, \ldots, u_n\}$ bilden erst recht die Elemente

$$v_1, v_2, \ldots, v_m, u_1, u_2, \ldots, u_n$$

1) Unter Verwendung transfiniter Induktion kann man aus F(37.2) sogar schließen, daß jeder unitäre $\mathfrak{K}$-Modul Vektorraum über $\mathfrak{K}$ ist.

ein Erzeugendensystem von $\mathfrak{G}$. Da dieses offensichtlich linear abhängig ist, gibt es nach S(37.1) wenigstens ein Element, welches sich aus den übrigen linear kombinieren läßt. Insbesondere sei x das erste Element, das schon Linearkombination der vorangehenden Elemente ist. Dieses Element x muß nach Voraussetzung über $v_1, v_2, \ldots, v_m$ ein u_i sein, welches also weggelassen werden kann. Mit dem verbleibenden Erzeugendensystem verfährt man ebenso. Das Verfahren führt nach endlich vielen Schritten zu einer Basis, in der $v_1, v_2, \ldots, v_m$ enthalten sind. qed.

Hauptsatz über endliche Vektorräume **S (37.5)**

Alle Basen eines endlichen Vektorraumes $\mathfrak{G}$ über einem Körper $\mathfrak{K}$ haben gleichviele Elemente. Diese somit eindeutig bestimmte Anzahl von Basiselementen heißt die Dimension[1]) *oder der Rang von $\mathfrak{G}$ über $\mathfrak{K}$ und ist die maximale Anzahl über $\mathfrak{K}$ linear unabhängiger Elemente von $\mathfrak{G}$.*

Beweis

Es sei $\{u_1, u_2, \ldots, u_n\}$ eine Basis mit kleinstmöglichen n und $\{v_1, v_2, \ldots\}$ eine beliebige andere Basis, die nach dem Bisherigen sogar unendlich sein könnte. Entsprechend S(37.4) ergänzen wir das nur aus einem Element bestehende (linear unabhängige System) $\{v_1\}$ mit Elementen aus $\{u_1, u_2, \ldots, u_n\}$ zu einer Basis. Wegen der linearen Abhängigkeit des Systems $\{v_1, u_1, u_2, \ldots, u_n\}$ besteht diese Basis aus höchstens n und damit nach Wahl von n aus genau n Elementen. Danach ergänzen wir das (linear unabhängige) System $\{v_1, v_2\}$ durch Elemente aus der eben gewonnenen Basis $\{v_1, u_{i_1}, u_{i_2}, \ldots, u_{i_{n-1}}\}$ und erhalten so eine neue Basis $\{v_1, v_2, u_{j_1}, u_{j_2}, \ldots, u_{j_{n-2}}\}$, die wieder genau n Elemente enthält. So fortfahrend gelangen wir also nach n Schritten zu einer Basis $\{v_1, v_2, \ldots, v_n\}$, die mit $\{v_1, v_2, \ldots\}$ übereinstimmen muß.

Daraus folgt im Zusammenhang mit S(37.4), daß jedes linear unabhängige System $\{v_1, v_2, \ldots, v_m\}$ aus $m \leqq n$ Elementen besteht. qed.

---

1) Wir machen darauf aufmerksam, daß in der Literatur mitunter die Dimension für endliche Vektorräume über beliebigen Ringen eingeführt wird. Diese Dimension ist jedoch dann entsprechend unseren Bemerkungen nach S(36.7) nicht notwendig eindeutig bestimmt.

Mit den beiden letzten Sätzen gleichwertig ist der berühmte

Austauschsatz von STEINITZ **S (37.6)**

Es sei $\mathfrak{G}$ ein endlicher Vektorraum über einem Körper $\mathfrak{K}$. Sind dann $v_1, v_2, \ldots, v_m$ irgendwelche linear unabhängige Elemente aus $\mathfrak{G}$, so gibt es in jeder Basis $\{u_1, u_2, \ldots, u_n\}$ ein Teilsystem $\{u_{i_1}, u_{i_2}, \ldots, u_{i_m}\}$ von genau m Elementen, welches man gegen $\{v_1, v_2, \ldots, v_m\}$ austauschen kann, so daß das durch diesen Austausch aus $\{u_1, u_2, \ldots, u_n\}$ entstehende System wieder eine Basis ist. Insbesondere ist also $m \leqq n$.

Dieser Satz unterscheidet sich nämlich von S(37.4) nur durch die Anzahlaussagen, die sich unmittelbar durch Hinzuziehung von S(37.5) ergeben. Umgekehrt impliziert ein unabhängiger Beweis[1]) von S(37.6) die Gültigkeit von S(37.4) und gestattet, S(37.5) zu folgern: Für zwei endliche Basen $\{v_1, v_2, \ldots, v_m\}$ und $\{u_1, u_2, \ldots, u_n\}$ ergibt sich nämlich $m \leqq n$ und $n \leqq m$; eine unendliche Basis kann aber nicht existieren, da sie ja mehr als n linear unabhängige Elemente enthalten müßte.

Wendet man den Austauschsatz insbesondere auf ein System von n linear unabhängigen Elementen an, so ergibt sich:

Folgerung **F (37.7)**

In einem n-dimensionalen Vektorraum $\mathfrak{G}$ über einem Körper $\mathfrak{K}$ bildet jedes System von n linear unabhängigen Elementen eine Basis von $\mathfrak{G}$.

Zusammenfassend können wir also feststellen: In einem n-dimensionalen Vektorraum $\mathfrak{G}$ über einem Körper $\mathfrak{K}$ lassen sich irgendwelche linear unabhängige Elemente $v_1, v_2, \ldots, v_m (m < n)$ durch Hinzunahme geeigneter Elemente (die sogar aus einem vorgegebenen System $\{u_1, u_2, \ldots, u_n\}$ linear unabhängiger Elemente gewählt werden können) zu n linear unabhängigen Elementen ergänzen. Je n linear unabhängige Elemente bilden eine Basis, gestatten also alle Elemente von $\mathfrak{G}$ linear zu kombinieren; dagegen sind mehr als n Elemente stets linear abhängig.

Es ist nun für Anwendungen wichtig, daß schon ein geringer Teil dieser Aussagen genügt, um einen $\mathfrak{K}$-Modul als endlichen Vektorraum zu kennzeichnen:

---

1) Vgl. etwa VAN DER WAERDEN, Mod. Alg. I, § 36, oder G. PICKERT,, Einf. in die Alg., § 10; die dort verwendete Formulierung des Austauschsatzes für endliche Unterräume eines beliebigen $\mathfrak{K}$-Moduls über einem Schiefkörper $\mathfrak{K}$ kennzeichnet den gleichen Sachverhalt.

Satz **S (37.8)**

Lassen sich in einem unitären $\mathfrak{R}$-Modul $\mathfrak{G}$ irgendwie n linear unabhängige Elemente $u_1, u_2, \ldots, u_n$ angeben, derart daß für alle weiteren $v \in \mathfrak{G}$ die Elemente $u_1, u_2, \ldots, u_n, v$ linear abhängig sind, so ist $\mathfrak{G}$ ein n-dimensionaler Vektorraum über $\mathfrak{R}$ und $\{u_1, u_2, \ldots, u_n\}$ eine Basis von $\mathfrak{G}$.

Beweis

Es ist nur zu zeigen, daß $\{u_1, u_2, \ldots, u_n\}$ Erzeugendensystem von $\mathfrak{G}$ ist. Wegen der vorausgesetzten linearen Unabhängigkeit ist dann nämlich $\{u_1, u_2, \ldots, u_n\}$ als Basis und damit $\mathfrak{G}$ als Vektorraum nachgewiesen; die Anzahl n der u_i ist dabei die nach S (37.5) eindeutig bestimmte Dimension von $\mathfrak{G}$.

Nun besteht aber nach Voraussetzung für jedes weitere $v \in \mathfrak{G}$ eine Beziehung

$$\lambda v + \sum_{i=1}^{n} \lambda_i u_i = o \,,$$

in der nicht alle auftretenden Koeffizienten verschwinden. Insbesondere gilt dabei $\lambda \neq o$ wegen der linearen Unabhängigkeit von $u_1, u_2, \ldots, u_n$. Multiplikation dieser Gleichung mit λ^{-1} lehrt die lineare Kombinierbarkeit von v aus $u_1, u_2, \ldots, u_n$.

qed.

Folgerung **F (37.9)**

Jeder zulässige Untermodul $\mathfrak{H}$ eines n-dimensionalen Vektorraumes $\mathfrak{G}$ über $\mathfrak{R}$ (also jeder in $\mathfrak{G}$ enthaltene $\mathfrak{R}$-Modul) ist selbst Vektorraum über $\mathfrak{R}$; insbesondere hat ein solcher Unterraum $\mathfrak{H}$ im Falle $\mathfrak{H} < \mathfrak{G}$ eine Dimension $m < n$.

Beweis

Es sei $\{v_1, v_2, \ldots, v_m\}$ ein System linear unabhängiger Elemente aus $\mathfrak{H} < \mathfrak{G}$; nach F (37.7) ist dann stets $m < n$. Insbesondere ist ein solches System mit größtmöglichen m gemäß S (37.8) eine Basis für $\mathfrak{H}$.

qed.

Während für jedes tiefere Eindringen in algebraische Betrachtungen eine Kenntnis der Begriffsbildungen „Operatorgruppe — $\mathfrak{R}$-Modul — Vektorraum — hyperkomplexes System" und ihrer Zusammenhänge unerläßlich ist, kommt man bei verschiedenen Anwendungen bereits mit den Gesetzmäßigkeiten in endlichen Vektorräumen über (kommutativen) Körpern aus, etwa

in dem Umfang, wie wir sie eben nochmals zusammengestellt haben. Geht man nur auf solche Anwendungen aus, so gibt es natürlich weniger weit ausholende Wege zu diesen Hilfsmitteln. Dabei kann man etwa wie folgt verfahren:

Man erklärt (oft nur für konkrete Spezialfälle) die „Operatoranwendung" der Elemente eines Körpers $\mathfrak{R}$ auf die Elemente eines Moduls $\mathfrak{G}$ und konstatiert die Gültigkeit der Gesetzmäßigkeiten *O I*, *O II*, *O III*, *O III'*, *O IV*, arbeitet also in einem unitären $\mathfrak{R}$-Modul. Desgleichen definiert man die lineare Abhängigkeit von Elementen aus $\mathfrak{G}$ über $\mathfrak{R}$ (vgl. D(36.1) und D(36.3)).

Als nächstes interessiert man sich für Systeme, die aus möglichst vielen linear unabhängigen Elementen von $\mathfrak{G}$ bestehen. Gibt es ein endliches System $\{u_1, u_2, \ldots, u_n\}$ dieser Art, so sind also nach Definition je $n+1$ und mehr Elemente aus $\mathfrak{G}$ linear abhängig. Man nennt dann $\{u_1, u_2, \ldots, u_n\}$ ein *Maximalsystem*[1]) und $\mathfrak{G}$ einen n-dimensionalen Vektorraum über $\mathfrak{R}$[2]).

Man beweist nun der Reihe nach:

1. *Jedes Maximalsystem ist Erzeugendensystem*, d. h., jedes $v \in \mathfrak{G}$ läßt sich in der Form
$$v = \lambda_1 u_1 + \lambda_2 u_2 + \cdots + \lambda_n u_n$$
aus $u_1, u_2, \ldots, u_n$ mit Koeffizienten $\lambda_1, \lambda_2, \ldots, \lambda_n$ aus $\mathfrak{R}$ linear kombinieren. Das folgt unmittelbar aus der linearen Abhängigkeit der $n+1$ Elemente $v, u_1, u_2, \ldots, u_n$ unter Verwendung der Körpereigenschaft von $\mathfrak{R}$ (vgl. den entsprechenden Schluß im Beweis zu S(37.8)).

2. *Die Koeffizienten $\lambda_1, \lambda_2, \ldots, \lambda_n$ sind in dieser Darstellung durch v eindeutig bestimmt*, denn dies folgt aus
$$v = \sum \lambda_i u_i = \sum \lambda_i' u_i, \text{ also } \sum (\lambda_i - \lambda_i') u_i = o$$
wegen der linearen Unabhängigkeit von $u_1, u_2, \ldots, u_n$.

3. *Es ist nicht möglich, alle Elemente von $\mathfrak{G}$ bereits aus weniger als n Elementen $v_1, v_2, \ldots, v_m$ linear zu kombinieren.* Sonst müßten sich nämlich insbesondere die Elemente $u_1, u_2, \ldots, u_n$ eines Maximalsystems in der Form
$$u_i = \sum_{k=1}^{m} \lambda_{ik} v_k \qquad (i = 1, 2, \ldots, n)$$
darstellen lassen. Nun besitzt aber das homogene lineare Gleichungssystem
$$\sum_{i=1}^{n} \xi_i \lambda_{ik} = o \qquad (k = 1, 2, \ldots, m)$$

---

1) Dieser Ansatzpunkt kennzeichnet den wesentlichen Unterschied zu der in diesem Kapitel dargestellten allgemeinen Betrachtungsweise: Diese geht von „Erzeugendensystemen" aus und fragt erst in zweiter Linie danach, ob diese linear unabhängig gewählt werden können, während man hier vom Begriff des Maximalsystems zu dem des Erzeugendensystems gelangt.

2) Man beachte, daß entsprechend dem veränderten Ausgangspunkt diese Definition der Dimension einen anderen Inhalt hat (z. B. ist sie von vornherein eindeutig!) als die in S(32.5) festgelegte, wie überhaupt zunächst auch eine andere Definition des Vektorraumes vorliegt.

eine nichttriviale Lösung $\xi_1, \xi_2, \ldots, \xi_n$ in $\mathfrak{R}$, da mehr Unbekannte als Gleichungen vorliegen, wie man aus der linearen Algebra entnimmt. Daraus folgt jedoch

$$\sum_{i=1}^{n} \xi_i u_i = \sum_{i=1}^{n} \xi_i \sum_{k=1}^{m} \lambda_{ik} v_k = \sum_{k=1}^{m} \left(\sum_{i=1}^{n} \xi_i \lambda_{ik} \right) v_k = o$$

im Widerspruch zur linearen Unabhängigkeit von $u_1, u_2, \ldots, u_n$.

Damit ist insbesondere gezeigt, daß in dem so erklärten n-dimensionalen Vektorraum jedes Maximalsystem (nach 1.) ein linear unabhängiges Erzeugendensystem ist[1]) und daß umgekehrt jedes linear unabhängige Erzeugendensystem (nach 3. und wegen der linearen Unabhängigkeit) aus n Elementen bestehen muß[2]) und damit Maximalsystem ist.

Unsere Überlegungen lehren darüber hinaus, daß man den Begriff des Maximalsystems nachträglich schwächer fassen kann. In der Aussage unter 1. wird nämlich nur verwendet, daß jedes System von $n + 1$ Elementen, in dem $u_1, u_2, \ldots, u_n$ enthalten sind, nicht aber jedes beliebige System von $n + 1$ Elementen linear abhängig ist. Ein solches im abgeschwächten Sinne maximale System ist also schon Erzeugendensystem und damit im eigentlichen Sinne Maximalsystem[3]).

Aufgaben zu § 37

1. Es sei $\mathfrak{G}$ der Vektorraum der Quadrupel $(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ über dem Körper P der rationalen Zahlen.

   a) Die folgenden vier Elemente von $\mathfrak{G}$ bilden eine Basis für $\mathfrak{G}$:

   $$u_1 = (2, 3, 1, 4),$$
   $$u_2 = (1, 1, 5, 3),$$
   $$u_3 = (1, 2, 0, 1),$$
   $$u_4 = (0, 1, 5, 4).$$

   b) Entsprechend dem Austauschsatz von Steinitz ergänze man die linear unabhängigen Elemente

   $$v_1 = (1, 2, -4, 1)$$
   $$v_2 = (1, 0, -10, -7)$$

   mit Hilfe der u_i zu einer Basis von $\mathfrak{G}$.

2. In der linearen Algebra definiert man den Rang einer Matrix A vom Typ (m, n) mit Elementen aus einem kommutativen Körper $\mathfrak{R}$ als den Rang r des von ihren Spaltenvektoren erzeugten Vektorraumes, der mit dem Rang des von ihren Zeilenvektoren erzeugten Vektorraumes übereinstimmt. Bekanntlich hat A genau dann den Rang r, wenn wenigstens eine ihrer r-reihigen Unterdeterminanten D_r verschieden von o ist, während alle $(r + 1)$-reihigen Unterdeterminanten verschwinden.

---

1) Damit ist $\mathfrak{G}$ auch endlicher Vektorraum im Sinne von D(36.4) und diese Aussage gerade der Inhalt von F(37.7). Hieraus ergibt sich übrigens auch F(37.9).

2) Dies entspricht dem Hauptsatz über endliche Vektorräume, woraus sich insbesondere die Gleichheit beider Dimensionsbegriffe ergibt.

3) Damit erkennt man, daß bereits in S(37.8) die Übereinstimmung beider Vektorraumbegriffe nachgewiesen wird, natürlich vom Standpunkt der allgemeinen Theorie.

Nach KRONECKER ist damit gleichwertig, daß alle aus $D_r \neq o$ durch Ränderung entstehenden $(r+1)$-reihigen Determinanten gleich o sind. Man zeige, daß sich diese Beschränkung aus dem Austauschsatz von STEINITZ ergibt.

3. Im Sinne von Aufg. 4 in § 35 ist das operatorhomomorphe Bild eines endlichen Vektorraumes über einem Körper $\mathfrak{K}$ wieder ein endlicher Vektorraum über $\mathfrak{K}$.

4. Man zeige am Beispiel der operatorhomomorphen Abbildung des Vektorraumes Γ^+ über dem Ring Γ auf den Γ-Modul $\Gamma^+/(m)$ $(m \neq 0)$, daß die Aussage von 3. von der Körpereigenschaft des Operatorenbereiches abhängig ist.

§ 38. Algebren

Wir gehen nunmehr allgemein dazu über, die Strukturen solcher Ringe und Körper zu untersuchen, die als Vektorräume über einem geeigneten anderen Ring oder Körper aufzufassen sind. Dem entspricht natürlich umgekehrt die Fragestellung, ob ein Vektorraum sogar Ring oder Körper ist bzw. durch geeignete Definition einer Multiplikation als innerer Verknüpfung dazu gemacht werden kann.

Definition **D (38.1)**

Unter einer Algebra (oder einem hyperkomplexen System) über einem kommutativen Ring $\mathfrak{R}$ mit Einselement versteht man einen Schiefring $\mathfrak{A}$, dessen additive Gruppe ein Vektorraum über $\mathfrak{R}$ ist, wobei in Ergänzung der Gesetze aus D (36.1) *noch*

$O\,II'$: $\quad \alpha(a \cdot b) = (\alpha a) \cdot b = a \cdot (\alpha b)$

für alle α aus $\mathfrak{R}$ und a, b aus $\mathfrak{A}$ gefordert wird[1]*. Falls dabei $\mathfrak{A}$ sogar Schiefkörper ist, nennt man $\mathfrak{A}$ auch Divisionsalgebra.*

Im Einklang mit D (36.4) spricht man von einer endlichen Algebra über $\mathfrak{R}$, wenn $\mathfrak{A}$ endlicher Vektorraum über $\mathfrak{R}$ ist. Wir werden uns hier im allgemeinen auf die Betrachtung solcher Algebren beschränken.

---

1) Auch diese Forderung wird durch die Gesetze der Operatoranwendung des Ringes Γ auf einen beliebigen Ring nahegelegt. Allgemein können wir den in § 27 behandelten diesbezüglichen Sachverhalt so kennzeichnen, daß jeder Ring auch Γ-Modul ist, der überdies $O\,II'$ erfüllt. Doch ist damit nicht etwa jeder Ring eine Algebra über Γ, da er nämlich kein Vektorraum über Γ zu sein braucht, wie etwa $\Gamma'(m)$ (vgl. Aufg. 4 von § 37).

Für einen Körper $\mathfrak{K}$ als Operatorenbereich ist dann nach S(37.5) die Anzahl der Elemente einer Basis eindeutig bestimmt; diese Anzahl bezeichnet man hier vorzugsweise als *Rang* von $\mathfrak{A}$ über $\mathfrak{K}$ (und nicht als Dimension).

In diesem Sinne bilden die komplexen Zahlen und die Quaternionen endliche Algebren über dem Körper der reellen Zahlen, desgleichen die in B(26.4 a) betrachteten Ringe über Γ bzw. P; weiterhin ist der volle Matrizenring $\mathfrak{M}_n(\mathfrak{R})$ über einem kommutativen Ring $\mathfrak{R}$ eine endliche Algebra über $\mathfrak{R}$. Alle diese Strukturen sind uns nämlich aus den vorhergehenden Paragraphen bereits als endliche Vektorräume bekannt, und die Gültigkeit von *O II'* kann man jeweils leicht nachprüfen.

Die Bedeutung der Forderung *O II'* zeigt die folgende Überlegung. Jedes Element a einer endlichen Algebra $\mathfrak{A}$ über $\mathfrak{R}$ läßt sich als Linearkombination

$$a = \alpha_1 u_1 + \ldots + \alpha_n u_n$$

der Elemente u_i einer Basis von $\mathfrak{A}$ mit eindeutig bestimmten $\alpha_i \in \mathfrak{R}$ schreiben. Das Produkt zweier Elemente $a = \sum \alpha_i u_i$ und $b = \sum \beta_i u_i$ aus $\mathfrak{A}$ ist dann vermöge *O II'* bereits durch n^2 Produkte je zweier Basiselemente bestimmt:

$$(*) \quad a \cdot b = \Big(\sum_i \alpha_i u_i\Big)\Big(\sum_j \beta_j u_j\Big) = \sum_{i,j} \alpha_i u_i \beta_j u_j = \sum_{i,j} \alpha_i \beta_j u_i u_j.$$

Man beherrscht also die Multiplikation in $\mathfrak{A}$ bereits, wenn man die Multiplikationstabelle

	u_j
	$\vdots$
u_i	$\ldots\ u_i u_j$

der Basiselemente kennt. Freilich ist dabei im allgemeinen $u_i u_j$ nicht wieder eine Basiselement, sondern wie jedes Element von $\mathfrak{A}$ eine Linearkombination[1])

$$u_i u_j = \sum_{k=1}^{n} \gamma_{ij}^{k} u_k.$$

1) Zur besseren Übersicht pflegt man den dritten Index k hochzustellen; er darf dann natürlich nicht mit einem Exponenten verwechselt werden.

Die dabei auftretenden eindeutig bestimmten n^3 Koeffizienten $\gamma_{ij}^k \in \mathfrak{R}$ werden die *Strukturkonstanten* von $\mathfrak{A}$ (bezüglich der Basis $\{u_1, \ldots, u_n\}$) genannt; sie kennzeichnen die Multiplikation in $\mathfrak{A}$ vollständig.

Diese Betrachtungen lassen sich auch auf nichtendliche Algebren übertragen, da nach D (36.4) auch bezüglich einer unendlichen Basis jedes Element eine Linearkombination nur endlich vieler Basiselemente ist. Selbstverständlich gibt es dann unendlich viele Strukturkonstanten. Für eine abzählbar unendliche Basis $\{u_1, u_2, \ldots\}$ läßt sich dabei auch die Summenschreibweise ohne jede Umdeutung der Indizes formal übernehmen, desgleichen die Bezeichnung der Strukturkonstanten mit γ_{ij}^k, wobei jeder Index die Menge der natürlichen Zahlen durchläuft. Entsprechend D (36.4) gibt es für jeweils festes i und j nur endlich viele γ_{ij}^k, die vom Nullelement verschieden sind.

Damit haben wir jetzt für beliebige Algebren den Standpunkt gewonnen, den wir für den Spezialfall der Quaternionen und der komplexen Zahlen bereits am Ende von § 31 erreichten. Wir werden nun allgemein zeigen, wie man umgekehrt, von Vektorräumen ausgehend, Ringe als Algebren herstellen kann.

Satz **S (38.2)**

Um aus einem endlichen Vektorraum $\mathfrak{A}$ über einem kommutativen Ring $\mathfrak{R}$ mit Einselement eine Algebra über $\mathfrak{R}$ zu machen, genügt es, eine eindeutige und assoziative Multiplikation der Basiselemente von $\mathfrak{A}$ zu erklären.
Die Festlegung des Produktes zweier beliebiger Elemente $a = \sum \alpha_i u_i$ und $b = \sum \beta_j u_j$ aus $\mathfrak{A}$ hat dann zwangsläufig zu erfolgen gemäß:

$$a \cdot b = \left(\sum_i \alpha_i u_i\right)\left(\sum_j \beta_j u_j\right) = \sum_{i,j} \alpha_i \beta_j u_i u_j .$$

Beweis

Die Herleitung der Formel (*) zeigt bereits, daß nur die getroffene Festlegung der Multiplikation von a und b mit einer vorgegebenen Multiplikationsvorschrift der Basiselemente verträglich ist. Auch wird so je zwei Elementen a und b aus $\mathfrak{A}$ wegen der eindeutigen Bestimmtheit ihrer Koeffizienten α_i bzw. β_j eindeutig ein Element $a \cdot b \in \mathfrak{A}$ als Produkt zugeordnet. Wir zeigen unter Benutzung der für Vektorräume gültigen Rechenregeln, daß dann auch *O II'*, *D* und *M II* erfüllt sind.

O II': $\alpha(ab) = \alpha\sum\alpha_i\beta_j u_i u_j \qquad = \sum\alpha(\alpha_i\beta_j)u_i u_j$

$(\alpha a)b = (\sum(\alpha\alpha_i)u_i)\,(\sum\beta_j u_j) = \sum(\alpha\alpha_i)\beta_j u_i u_j$

$a(\alpha b) = (\sum\alpha_i u_i)\,(\sum(\alpha\beta_j)u_j) = \sum\alpha_i(\alpha\beta_i)u_i u_j$ [1]).

D: $a(b+c) = \sum_i \alpha_i u_i\Big(\sum_j(\beta_j+\gamma_j)u_j\Big) = \sum_{i,j}\alpha_i(\beta_j+\gamma_j)u_i u_j$

$ab + ac = \sum_{i,j}\alpha_i\beta_j u_i u_j + \sum_{i,j}\alpha_i\gamma_j u_i u_j = \sum_{i,j}(\alpha_i\beta_j+\alpha_i\gamma_j)u_i u_j$

Entsprechend zeigt man die andere Relation des Distributivgesetzes.

M II: Die Assoziativität der Basiselemente überträgt sich auf Grund von *D* und *O II'* auf alle Elemente (vgl. Aufg. 4):

$$(ab)c = \Big(\sum_{i,j}\alpha_i\beta_j u_i u_j\Big)\Big(\sum_k\gamma_k u_k\Big) = \sum_{i,j,k}(\alpha_i\beta_j)\gamma_k(u_i u_j)u_k$$

$$a(bc) = \Big(\sum_i\alpha_i u_i\Big)\Big(\sum_{j,k}\beta_j\gamma_k u_j u_k\Big) = \sum_{i,j,k}\alpha_i(\beta_j\gamma_k)u_i(u_j u_k).$$

qed.

Auch dieser Satz gilt wieder für beliebige Algebren. Während nämlich in den Summen des obigen Beweises u_i jeweils alle Elemente der Basis $\{u_1, \ldots, u_n\}$ durchläuft, sondert man im Falle unendlicher Basen nur die (endlich vielen) Basiselemente aus, die in wenigstens einer der Linearkombinationen für a, b und c tatsächlich auftreten. Mit dieser Summationsvorschrift enthalten alle Summen nur endlich viele Summanden, und der Beweis verläuft genau wie oben.

Man kann also jeden Vektorraum (über einem kommutativen Ring mit Einselement) zu einem Ring machen, wenn es nur gelingt, für die Basiselemente eine eindeutige und assoziative Multiplikation festzusetzen. Hieraus folgt, daß es in der Tat für den Nachweis der

---

1) Man beachte, daß an dieser Stelle und damit in den nachfolgenden Beweis von *M II* die vorausgesetzte Kommutativität von $\mathfrak{R}$ eingeht. Über nichtkommutativen Ringen lassen sich Algebren im Sinne von D(38.1) nach G. PICKERT, Math. Ann. 120 (1948) S.158ff. nur durch ganz spezielle Wahl der Multiplikationsvorschriften konstruieren.

Allerdings kann man den Begriff der Algebra dahingehend verallgemeinern, daß man an Stelle von *O II'* nur noch $\alpha(a\cdot b) = (\alpha a)\cdot b$ fordert. Für solche Algebren gilt die Aussage von S(38.2) auch für nichtkommutative Ringe $\mathfrak{R}$ jedenfalls dann, wenn die Strukturkonstanten mit allen Elementen von $\mathfrak{R}$ vertauschbar sind; man muß dazu natürlich den Beweis von *M II* mit Hilfe der Strukturkonstanten ansetzen.

Unter diesen verallgemeinerten Algebrenbegriff fallen übrigens dann auch die vollen Matrizenringe $\mathfrak{M}_n(\mathfrak{R})$ und die Polynomringe $\mathfrak{R}[x]$ über beliebigen Schiefringen $\mathfrak{R}$.

Ringeigenschaft der komplexen Zahlen bzw. Quaternionen ausreicht, diese als Vektorräume über dem Körper der reellen Zahlen einzuführen und die Assoziativität der Multiplikation der Basiselemente zu prüfen. Dies ergänzt unsere Betrachtungen am Ende von § 33 über die Einführung der komplexen Zahlen, als hier genau die Theorie vorliegt, auf deren Grundlage man tatsächlich in dem von der Basis $\{1, i\}$ über dem Körper der reellen Zahlen erzeugten Vektorraum (nach Prüfung der Assoziativität der durch $1 \cdot 1 = 1$, $1 \cdot i = i \cdot 1 = i$, $i \cdot i = -1$ festgelegten Multiplikation) „losrechnen" könnte. Schneidet man aber die Überlegungen dieser allgemeinen Theorie, die natürlich vor einer elementaren Einführung der komplexen Zahlen niemals vorliegt, auf eben diesen Spezialfall zu, führt man genau die gleichen Schritte durch wie bei der Zahlenpaarbildung.

Auch der Nachweis der Ringeigenschaft von $\mathfrak{M}_n(\mathfrak{R})$ läßt sich (für einen kommutativen Ring $\mathfrak{R}$ mit Einselement) mit diesen Hilfsmitteln leicht erbringen. Man erklärt einfach für die in Aufg. 7 von § 36 eingeführten Basiselemente e_{ik} die Multiplikation

$$e_{ik} \cdot e_{lm} = \begin{cases} e_{im} & \text{für } k = l \\ o & \text{für } k \neq l, \end{cases}$$

die offensichtlich assoziativ ist.

Ein weiteres wichtiges Beispiel für solche Konstruktionen von Ringen erhält man, wenn man von einer beliebigen Gruppe $\mathfrak{G}$ der Ordnung n und einem Vektorraum über einem Ring $\mathfrak{R}$ mit einer Basis aus n Elementen $u_1, \ldots, u_n$ ausgeht und letztere in beliebiger Reihenfolge mit den Gruppenelementen identifiziert. Damit hat man nämlich für die Basiselemente eine eindeutige und assoziative Multiplikation erklärt, so daß eine Algebra entsteht, nämlich der sogenannte *Gruppenring* von $\mathfrak{G}$ über $\mathfrak{R}$ (vgl. Aufg. 6). Die Bedeutung dieser Begriffsbildung liegt u. a. darin, daß sie eine gewisse Verbindung zwischen der Gruppen- und Ringtheorie herstellt und somit gestattet, Aussagen der einen Theorie für die andere nutzbar zu machen.

Analog kann man auch Gruppenringe von Gruppen mit unendlich vielen Elementen bilden. In beiden Fällen reicht es dabei sogar aus, von einer Halbgruppe $\mathfrak{H}$ auszugehen. Nehmen wir für $\mathfrak{H}$ etwa alle Potenzen x^i einer Unbestimmten x mit ganzzahligen Exponenten $i \geqq 0$, so erhalten wir auf diese

Weise den Polynomring $\mathfrak{R}[x]$ als Algebra über dem kommutativen Ring $\mathfrak{R}$ mit Einselement. Eine analoge Konstruktion von Polynomringen über nichtkommutativen Ringen mit Einselement ist dagegen nur bei Verzicht auf OII' möglich (vgl. dazu die Fußnote auf S. 122 und Aufg. 3).

Die Einführung der Multiplikation in einem Vektorraum kann auch so geschehen, daß man ein System von Strukturkonstanten vorgibt. Diese liefern ihrer Definition nach eine eindeutige Multiplikation der Basiselemente, jedoch muß man für die Assoziativität beachten:

Satz **S (38.3)**

Die durch die Strukturkonstanten γ_{ij}^{k} festgelegte Multiplikation ist dann und nur dann assoziativ, wenn die folgenden Relationen erfüllt sind:

$$\sum_h \gamma_{ij}^{h}\,\gamma_{hk}^{l} = \sum_h \gamma_{jk}^{h}\,\gamma_{ih}^{l} \quad \textit{für alle } i, j, k, l.$$

Beweis

Aus den Gleichungen

$$(u_i u_j)\,u_k = \sum_h \gamma_{ij}^{h} u_h u_k = \sum_{h,l} \gamma_{ij}^{h}\gamma_{hk}^{l} u_l$$

$$u_i (u_j u_k) = u_i \sum_h \gamma_{jk}^{h} u_h = \sum_{h,l} \gamma_{jk}^{h}\gamma_{ih}^{l} u_l$$

folgt unsere Behauptung, je nachdem ob man die linken oder rechten Seiten als gleich voraussetzt.

qed.

Auch für diese Aussage ist eine Beschränkung auf endliche Basen nicht erforderlich. Für abzählbar unendliche Basen gilt nach unserer Bemerkung vor S (38.2) ohnehin alles formal weiter. Im überabzählbaren Falle sind bezüglich der Indizierung der Strukturkonstanten geeignete Vereinbarungen zu treffen.

Abschließend bemerken wir noch, daß wohl entsprechend unseren Betrachtungen die über einem kommutativen Ring $\mathfrak{R}$ mit Einselement durch Vorgabe der Strukturkonstanten konstruierte Algebra (bis auf Operatorisomorphie) eindeutig bestimmt ist, aber die gleiche Algebra über $\mathfrak{R}$ durchaus mit Hilfe verschiedener Systeme von Strukturkonstanten beschrieben werden kann. Letzteres folgt schon daraus, daß man in einem Vektorraum von einer Basis zu einer anderen Basis übergehen kann.

Aufgaben zu § 38

1. Es sei $\mathfrak{A}$ eine Algebra über dem kommutativen Ring $\mathfrak{R}$ mit dem Einselement ε. Dann kann $\mathfrak{R}$ genau dann als Unterring von $\mathfrak{A}$ aufgefaßt werden, wenn $\mathfrak{A}$ ein Linkseinselement e_L enthält.

2. Es ist mitunter üblich, für eine Algebra $\mathfrak{A}$ über einem kommutativen Ring $\mathfrak{R}$ noch $\alpha a = a\alpha$ für alle $\alpha \in \mathfrak{R}$ und $a \in \mathfrak{A}$ zu fordern. Man überlege sich, welche Bedeutung diese Forderung hat.

3. Ein Polynomring $\mathfrak{R}[x]$ über einem nichtkommutativen Ring $\mathfrak{R}$ ist wohl Vektorraum über $\mathfrak{R}$, erfüllt aber nicht *O II'*.

4. Man überlege sich, wie *D* und *O II'* beim Nachweis von *M II* im Beweis von S(38.2) im einzelnen eingehen.

5. Die Quaternionen bilden über dem Körper der komplexen Zahlen wohl einen Vektorraum, aber keine Algebra.

6. Es sei $\mathfrak{A}$ der Gruppenring der symmetrischen Gruppe $\mathfrak{S}_3$ über dem Körper P der rationalen Zahlen. Ein beliebiges seiner Elemente bezeichnen wir mit

$$a = \sum_{i=1}^{6} \alpha_i s_i \qquad (\alpha_i \in \mathrm{P}),$$

wobei $s_1 = (1)$, $s_2 = (123)$, $s_3 = (132)$, $s_4 = (12)$, $s_5 = (13)$, $s_6 = (23)$ gesetzt ist. Man berechne in $\mathfrak{A}$:

a) $(2s_1 - s_2 - s_3) \cdot (s_1 + s_2 + s_3 - s_4 - s_5 - s_6)$,
b) $(-s_2 + s_3 + s_4 - s_6)^2$,
c) $(\frac{2}{3} s_1 + \frac{1}{3} s_3 - \frac{1}{3} s_4 + \frac{1}{3} s_5)^2$.

VIII. TEILBARKEITSLEHRE

Bereits am Anfang der Ring- und Körpertheorie (§ 25) haben wir darauf hingewiesen, daß die Vielfalt der mit dem Ringbegriff erfaßten Strukturen wesentlich auf dem Verzicht bestimmter Forderungen bezüglich der Umkehrung der Multiplikation beruht. Eine genauere Einsicht in diese, für den betreffenden Ring charakteristischen Verhältnisse wird man erhalten, wenn man allgemein von der Fragestellung „Welche Elemente sind durch welche Elemente dividierbar?" ausgeht. Mit der sich daraus entwickelnden Teilbarkeitslehre wollen wir uns im folgenden beschäftigen. Dabei beschränken wir uns zur Vermeidung von Komplikationen (Unterscheidung der Division von links und von rechts, Mehrdeutigkeit der Division) auf den ohnehin wichtigsten Fall, daß die betreffenden Ringe kommutativ und nullteilerfrei sind. Das Entsprechende gilt hinsichtlich der Voraussetzung eines Einselementes.

Nach Bereitstellung der grundlegenden Begriffsbildungen untersuchen wir, welche besonderen Eigenschaften des Ringes der ganzen Zahlen dem sog. Fundamentalsatz der Zahlentheorie über die eindeutige Zerlegbarkeit ganzer Zahlen in ein Produkt von Primzahlen zugrunde liegen. Diese Eigenschaften lassen sich so allgemein formulieren, daß sie zur Kennzeichnung von Ringen dienen können, in denen dann ein analoger Satz nachweisbar ist. Dies ist von großer Bedeutung, denn die weitreichenden Folgerungen des Fundamentalsatzes der Zahlentheorie für das Rechnen mit ganzen Zahlen und ihren Brüchen übertragen sich auf das Rechnen in solchen Ringen und ihren Quotientenkörpern. Diese Analogien gehen so weit, daß man alle diesbezüglichen Ausführungen (§§ 39–41) einfach als Aussagen über den Ring $\mathfrak{R} = \Gamma$ und seinen Quotientenkörper $\mathfrak{K} = P$ als ein Kapitel der elementaren Zahlentheorie lesen kann. Dabei sind die spezielleren Betrachtungen aus § 41 für alles Folgende entbehrlich.

Diese einfache, der gewöhnlichen Zahlenrechnung entsprechende Struktur weisen jedoch nicht alle Integritätsbereiche mit Einselement auf, wie wir durch Beispiele zeigen werden. Damit ent-

steht die Frage, ob sich auch in die Teilbarkeitsverhältnisse solcher Ringe irgendwelche allgemeine Einsichten gewinnen lassen. Dies ist in der Tat in einer Reihe von Fällen mit Hilfe idealtheoretischer Überlegungen möglich, worauf wir in den beiden letzten Paragraphen dieses Kapitels eingehen. Diese idealtheoretische Verallgemeinerung der Teilbarkeitslehre spielt eine wesentliche Rolle in der algebraischen Zahlentheorie und stellt einen der historischen Entwicklung entsprechenden Zugang zur allgemeinen Idealtheorie dar. Freilich können wir in dem uns hier gesteckten Rahmen zu diesen mathematischen Disziplinen allenfalls hinleiten und Gesichtspunkte vermitteln, die gewisse Gesetzmäßigkeiten der Elementarmathematik deutlicher werden lassen. Wir bemerken noch, daß diese Überlegungen im wesentlichen bereits an die Paragraphen 39 und 40 anschließen und ebenfalls in die folgenden Kapitel nicht mehr eingehen.

§ 39. Teilbarkeit

In einem Körper existiert zu zwei beliebigen Elementen a und $b \neq o$ stets ein Element x, so daß die Beziehung $a = bx$ besteht, während dies in einem Ring im allgemeinen nur für geeignete Elementenpaare a, b der Fall ist. Mit den sich daraus ergebenden Sachverhalten werden wir uns nun beschäftigen, wobei der zugrunde gelegte Ring $\mathfrak{R}$ im folgenden stets als Integritätsbereich mit Einselement e angenommen wird.

Definition **D (39.1)**

Ein Element $b \in \mathfrak{R}$ heißt Teiler eines Elementes $a \in \mathfrak{R}$, wenn es ein Element $x \in \mathfrak{R}$ gibt, so daß $a = bx$ gilt. Man bezeichnet dies durch $b \mid a$, das Gegenteil durch $b \nmid a$.

Äquivalente Formulierungen sind: b geht auf in a bzw. a ist Vielfaches von b oder a ist teilbar durch b.

Das in der Gleichung $a = bx$ auftretende Element x ist offenbar ebenfalls Teiler von a und (wegen der Gültigkeit von *M III** in $\mathfrak{R}$) für $b \neq o$ eindeutig bestimmt. Man bezeichnet x auch als den zu b *komplementären Teiler* von a. Aus D (39.1) ergeben sich unmittelbar einige grundlegende Teilbarkeitsrelationen für alle Elemente aus $\mathfrak{R}$ (vgl. Aufg. 1):

Folgerung **F (39.2)**

a) $a \mid a$.

b) $e \mid a$.

c) $a \mid o$, *aber* $o \mid a$ *nur für* $a = o$.

d) *Aus* $b \mid a$ *folgt* $b \mid ac$.

e) *Aus* $b \mid a$ *folgt* $bc \mid ac$ *und, falls* $c \neq o$, *auch umgekehrt.*

f) *Aus* $a_1 \mid a_2$ *und* $a_2 \mid a_3$ *folgt* $a_1 \mid a_3$.

g) *Aus* $b_1 \mid a_1$ *und* $b_2 \mid a_2$ *folgt* $b_1 b_2 \mid a_1 a_2$.

h) *Aus* $b \mid a_1$ *und* $b \mid a_2$ *folgt* $b \mid c_1 a_1 + c_2 a_2$, *insbesondere also* $b \mid a_1 \pm a_2$.

Die letzten drei Relationen lassen sich dabei mühelos durch vollständige Induktion ausdehnen.

Definition **D (39.3)**

Ein Element $\varepsilon \in \mathfrak{R}$ *heißt Einheit von* $\mathfrak{R}$, *wenn es Teiler des Einselementes* $e \in \mathfrak{R}$ *ist:* $\varepsilon \mid e$.

Man sieht unmittelbar, daß genau diejenigen Elemente aus $\mathfrak{R}$ Einheiten von $\mathfrak{R}$ sind, die in $\mathfrak{R}$ ein Inverses besitzen, ein Kriterium, das auch oft zur Definition der Einheiten von $\mathfrak{R}$ benutzt wird. Eine dritte Möglichkeit der Kennzeichnung ergibt sich aus der Tatsache, daß genau die Einheiten von $\mathfrak{R}$ Teiler jedes Elementes $a \in \mathfrak{R}$ sind; denn aus $\varepsilon \mid a$ für alle $a \in \mathfrak{R}$ folgt erst recht $\varepsilon \mid e$, während $\varepsilon \mid e$ wegen $e \mid a$ wiederum $\varepsilon \mid a$ ergibt. Insbesondere ist das Einselement e selbst eine Einheit. Da weiterhin sowohl das Produkt $\varepsilon_1 \varepsilon_2$ als auch der Quotient $\varepsilon_1 \varepsilon_2^{-1}$ zweier Einheiten wieder Einheiten sind, ergibt sich:

Folgerung **F (39.4)**

Die Einheiten von $\mathfrak{R}$ *bilden eine multiplikative Gruppe.*

Beispiele

a) Der Ring Γ der ganzen Zahlen hat als Einheiten offensichtlich genau die Elemente $+1$ und -1.

b) Die Einheiten des Polynomringes $\mathfrak{R}[x]$ über einem Integritätsbereich $\mathfrak{R}$ mit Einselement sind die Einheiten von $\mathfrak{R}$ (vgl. Aufg. 2).

c) Ein beliebiger kommutativer Körper hat alle vom Nullelement verschiedenen Elemente als Einheiten.

Definition **D (39.5)**

Zwei Elemente $a \in \mathfrak{R}$ und $b \in \mathfrak{R}$ heißen assoziiert (in Zeichen: $a \cong b$), wenn sie sich nur um eine Einheit als Faktor unterscheiden:

$$a = \varepsilon b \quad \text{und damit} \quad b = \varepsilon^{-1} a.$$

Assoziierte Elemente sind also gegenseitig Teiler voneinander, und umgekehrt sind gegenseitig durcheinander teilbare Elemente assoziiert, denn aus $b \mid a$ und $a \mid b$, also $a = bx$ und $b = ay$ folgt $a = axy$, d. h. $xy = e$. Insbesondere sind also alle Einheiten von $\mathfrak{R}$ zueinander assoziiert.

Die Beziehung $a \cong b$ ist offensichtlich reflexiv, symmetrisch und transitiv, also eine Äquivalenzrelation. Ihr entspricht eine Einteilung aller Elemente von $\mathfrak{R}$ in *Klassen assoziierter Elemente*, die für alle Teilbarkeitsaussagen in $\mathfrak{R}$ von grundlegender Bedeutung ist:

Satz **S (39.6)**

Alle auf Teilbarkeitsrelationen beruhenden Aussagen bleiben richtig, wenn man darin auftretende Elemente durch zu ihnen assoziierte Elemente ersetzt.

Beweis

Es genügt zu zeigen, daß sich aus $b \mid a$ stets $\varepsilon_1 b \mid \varepsilon_2 a$ für beliebige Einheiten ε_1 und ε_2 aus $\mathfrak{R}$ ergibt. Aus $a = bx$ folgt aber $\varepsilon_2 a = \varepsilon_1 b (\varepsilon_1^{-1} \varepsilon_2 x)$. qed.

Alle Teilbarkeitsaussagen sind also ihrem Wesen nach immer Aussagen über Klassen zueinander assoziierter Elemente. Man trägt dem Rechnung, indem man entweder den Zusatz „bis auf Einheiten" oder „bis auf assoziierte Elemente" (stillschweigend oder ausdrücklich) hinzufügt oder statt des Gleichheitszeichens $=$ das Zeichen $\cong$ verwendet. Oft ist es sogar vorteilhaft, alle Aussagen auf ein geeignet gewähltes System von Repräsentanten zu beschränken.

Ein solches normiertes System ist für den Ring Γ der ganzen Zahlen, wo jeweils die Elemente $+a$ und $-a$ zueinander assoziiert sind, die Menge der natürlichen Zahlen einschließlich der Null. Für den Polynomring $\mathfrak{K}[x]$ über einem Körper $\mathfrak{K}$ erhält man ein solches System in der Menge aller Polynome mit dem höchsten Koeffizienten e.

Über die Teiler irgendeines Elementes $a \in \mathfrak{R}$ läßt sich allgemein folgendes feststellen:

Falls $a = \varepsilon$ eine Einheit von $\mathfrak{R}$ ist, so sind die und nur die Einheiten von $\mathfrak{R}$ (also gerade die zu ε assoziierten Elemente) Teiler von ε. Letzteres ergibt sich daraus, daß aus $b \mid \varepsilon$ wegen $\varepsilon \mid e$ auch $b \mid e$ folgt.

Ist a keine Einheit von $\mathfrak{R}$, so gibt es neben den zu a assoziierten Elementen noch weitere Teiler von a. Solche Teiler, für die also $b \mid a$, aber $a \nmid b$ gilt, nennt man *echte Teiler* von a, was man auch durch $b \parallel a$ bezeichnet. So gilt in diesem Falle stets $\varepsilon \parallel a$ für jede Einheit ε von $\mathfrak{R}$. Es bleibt nun die Frage, ob es außer den zu a assoziierten Elementen und den Einheiten von $\mathfrak{R}$, die man gemeinsam die *trivialen Teiler* von a nennt, noch weitere Teiler von a gibt oder nicht.

Definition **D (39.7)**

Ein Element $p \neq o$ aus $\mathfrak{R}$, welches keine Einheit ist, heißt Primelement von $\mathfrak{R}$, wenn es nur triviale Teiler hat.

Es ist natürlich für einen beliebigen Ring fraglich, ob es überhaupt solche Elemente gibt, die nur assoziierte Elemente oder Einheiten als Teiler besitzen. Der Ring Γ der ganzen Zahlen hat die Primelemente $\pm 2, \pm 3, \pm 5, \ldots$, deren positiv normierten Repräsentanten die *Primzahlen* $+2, +3, +5, \ldots$ sind. Im Polynomring $\mathfrak{R}[x]$ heißen die Primelemente auch *irreduzible* Polynome.

Die Primelemente eines Ringes $\mathfrak{R}$ spielen eine wichtige Rolle bei der Zerlegung der Elemente von $\mathfrak{R}$ in Faktoren. Nennt man nämlich ein Element $c \neq o$ aus $\mathfrak{R}$ *unzerlegbar* in $\mathfrak{R}$, wenn aus $c = ab$ mit $a \in \mathfrak{R}$ und $b \in \mathfrak{R}$ stets $a \cong c$, $b \cong e$ oder $a \cong e$, $b \cong c$ folgt, so sind neben den Einheiten gerade die Primelemente die unzerlegbaren Elemente von $\mathfrak{R}$ (vgl. Aufg. 6)[1]).

Auf die Frage, in welchen Ringen die zerlegbaren Elemente als (u. U. eindeutiges) Produkt von Primelementen geschrieben werden können, kommen wir im nächsten Paragraphen zu sprechen. Zuvor geben wir aber noch einige für die Teilbarkeitslehre wichtige Begriffe an.

---

1) In der Literatur ist es mitunter üblich, die Bezeichnungen „Primelement" und „unzerlegbares Element" synonym zu gebrauchen, indem man entweder in die erste Begriffsbildung die Einheiten mit einbezieht (was aber die Formulierung des Eindeutigkeitssatzes S(40.3) erschwert) oder den zweiten Begriff auf Nichteinheiten verengt. Aus der letzten Auffassung leitet sich auch sprachlich die Bezeichnung „irreduzibles Polynom" her.

Definition **D (39.8)**

a) *Ein Element* $t \in \mathfrak{R}$ *heißt gemeinsamer Teiler der Elemente* $a_1, a_2, \ldots, a_n$ *aus* $\mathfrak{R}$, *wenn* t *Teiler aller dieser Elemente ist:*

$$t|a_1,\ t|a_2,\ \ldots,\ t|a_n.$$

b) *Insbesondere heißt ein Element* $d \in \mathfrak{R}$ *größter gemeinsamer Teiler von* $a_1, a_2, \ldots, a_n$, *wenn außer*

(*) $$d|a_1,\ d|a_2,\ \ldots,\ d|a_n$$

noch gilt, daß jeder gemeinsame Teiler t *dieser Elemente auch Teiler von* d *ist:*

(**) *Aus* $t|a_1, t|a_2, \ldots, t|a_n$ *folgt* $t|d$.

Folgerung **F (39.9)**

Existiert für die Elemente $a_1, a_2, \ldots, a_n$ *aus* $\mathfrak{R}$ *ein größter gemeinsamer Teiler* d, *so ist dieser bis auf Einheiten aus* $\mathfrak{R}$ *eindeutig bestimmt. Dies berechtigt zur Bezeichnung*

$$d \cong (a_1, a_2, \ldots, a_n).$$

Beweis

Jeder andere größte gemeinsame Teiler d' kann nämlich als gemeinsamer Teiler die Rolle von t in (**) übernehmen, d. h., es gilt $d'|d$. Geht man dagegen von dem größten gemeinsamen Teiler d' aus, erhält man umgekehrt $d|d'$. Die Elemente d und d' sind also zueinander assoziiert. qed.

Definition **D (39.10)**

a) *Ein Element* $v \in \mathfrak{R}$ *heißt gemeinsames Vielfaches der Elemente* $a_1, a_2, \ldots, a_n$ *aus* $\mathfrak{R}$, *wenn* v *ein Vielfaches aller dieser Elemente ist:*

$$a_1|v,\ a_2|v,\ \ldots,\ a_n|v.$$

b) *Insbesondere heißt ein Element* $f \in \mathfrak{R}$ *kleinstes gemeinsames Vielfaches von* $a_1, a_2, \ldots, a_n$, *wenn außer*

(†) $$a_1|f,\ a_2|f,\ \ldots,\ a_n|f$$

noch gilt, daß jedes gemeinsame Vielfache v *dieser Elemente auch Vielfaches von* f *ist:*

(††) *Aus* $a_1|v, a_2|v, \ldots, a_n|v$ *folgt* $f|v$.

Folgerung **F (39.11)**

Existiert für die Elemente $a_1, a_2, \ldots, a_n$ aus $\mathfrak{R}$ ein kleinstes gemeinsames Vielfaches f, so ist dieses bis auf Einheiten aus $\mathfrak{R}$ eindeutig bestimmt. Dies berechtigt zur Bezeichnung

$$f \cong [a_1, a_2, \ldots, a_n].$$

Beweis

Ist nämlich f' ein weiteres kleinstes gemeinsames Vielfaches, so erfüllt es als gemeinsames Vielfaches nach (††) $f \mid f'$. Die Vertauschung der Rollen von f und f' ergibt umgekehrt $f' \mid f$, was $f \cong f'$ bedeutet. qed.

Über die Existenz von größten gemeinsamen Teilern und kleinsten gemeinsamen Vielfachen läßt sich dagegen ohne weitere Voraussetzungen über den Integritätsbereich $\mathfrak{R}$ nichts aussagen. Wir werden jedoch im folgenden hinreichende Bedingungen kennenlernen, die für eine Reihe von Ringen (insbesondere für den Ring der ganzen Zahlen) diese Existenz gewährleisten. Im allgemeinen kann dabei den Bezeichnungen „größter" und „kleinster" kein anschaulicher Sinn beigelegt werden; vielmehr sind diese Bezeichnungen vom Spezialfall des Ringes Γ der ganzen Zahlen übernommen worden. Dort gilt nämlich $|d| \geqq |t|$ für $d \cong (a_1, a_2, \ldots, a_n)$ und jeden gemeinsamen Teiler t von $a_1, a_2, \ldots, a_n$[1]), wie unmittelbar aus $t \mid d$, also $d = tx$ folgt. Entsprechend ist $|f| \leqq |v|$. Wir bemerken noch, daß es meist üblich ist, im Ring Γ den größten gemeinsamen Teiler und das kleinste gemeinsame Vielfache positiv zu normieren und dann $d = (a_1, a_2, \ldots, a_n)$ bzw. $f = [a_1, a_2, \ldots, a_n]$ zu schreiben. Schließlich vereinbart man die folgenden Sprechweisen:

Definition **D (39.12)**

a) *Die Elemente $a_1, a_2, \ldots, a_n$ aus $\mathfrak{R}$ heißen teilerfremd, wenn sie einen größten gemeinsamen Teiler d mit $d \cong e$ besitzen (e Einselement von $\mathfrak{R}$).*

b) *Die Elemente $a_1, a_2, \ldots, a_n$ aus $\mathfrak{R}$ heißen paarweise teilerfremd, wenn die Elemente a_i, a_j jedes herausgegriffenen Paares teilerfremd sind.*

---

1) Der Fall $a_1 = a_2 = \ldots = a_n = 0$ ist für diese Überlegung auszuschließen.

Aufgaben zu § 39

1. Man beweise F(39.2).
2. Man beweise die im Text aufgestellte Behauptung über die Einheiten von $\mathfrak{R}[x]$.
3. Die Einheiten eines Ringes $\mathfrak{R} = \Gamma + \Gamma\sqrt{k}$ aus B(26.4a) können mit Hilfe des folgenden Kriteriums bestimmt werden: Ein Element $\varepsilon = u + v\sqrt{k}$ ist dann und nur dann Einheit von $\mathfrak{R}$, wenn die sogenannte Norm
$$N(\varepsilon) = (u + v\sqrt{k})(u - v\sqrt{k}) = u^2 - kv^2$$
den Wert ± 1 annimmt.
Nach dem Beweis dieses Kriteriums berechne man sämtliche Einheiten der Ringe $\Gamma + \Gamma i$, $\Gamma + \Gamma\sqrt{-5}$, $\Gamma + \Gamma\sqrt{-6}$ und zeige, daß der Ring $\Gamma + \Gamma\sqrt{26}$ unendlich viele Einheiten hat.
4. Zwei Elemente a und b erzeugen genau dann das gleiche Hauptideal, wenn $a \cong b$ gilt.
5. Man veranschauliche sich das gegenseitige Verhältnis von echten und unechten, trivialen und nichttrivialen Teilern eines Elementes, etwa am Beispiel der Zahl $12 \in \Gamma$.
6. Ein Element $a \neq o$ aus $\mathfrak{R}$ ist genau dann unzerlegbar in $\mathfrak{R}$, wenn a eine Einheit oder ein Primelement von $\mathfrak{R}$ ist.
7. Für den größten gemeinsamen Teiler und das kleinste gemeinsame Vielfache gilt:
$$(a_1, a_2, \ldots, a_n) \cong ((a_1, a_2, \ldots, a_{n-1}), a_n),$$
$$[a_1, a_2, \ldots, a_n] \cong [[a_1, a_2, \ldots, a_{n-1}], a_n].$$
8. In $\mathfrak{R}[x]$ ist der Grad des größten gemeinsamen Teilers mehrerer Polynome größer oder gleich dem Grad eines beliebigen gemeinsamen Teilers dieser Polynome. Entsprechend ist der Grad des kleinsten gemeinsamen Vielfachen kleiner oder gleich dem Grad eines beliebigen gemeinsamen Vielfachen.

§ 40. Zerlegung in Primelemente

Im Ring $\mathfrak{R} = \Gamma$ der ganzen Zahlen gelten die folgenden, für die Arithmetik grundlegenden Aussagen:

Existenz von Primteilern **S (40.1)**

Jedes Element aus $\mathfrak{R}$, das weder Nullelement noch Einheit ist, besitzt wenigstens einen Primteiler, das heißt einen Teiler, der Primelement von $\mathfrak{R}$ ist.

Existenz der Primzerlegung **S (40.2)**

Jedes Element aus $\mathfrak{R}$, das weder Nullelement noch Einheit ist, besitzt eine Darstellung als Produkt endlich vieler, nicht notwendig verschiedener Primelemente von $\mathfrak{R}$.

Eindeutigkeit der Primzerlegung **S (40.3)**

Die in S(40.2) *genannte Zerlegung in Primfaktoren ist eindeutig bis auf die Reihenfolge dieser Faktoren und ihre Ersetzung durch assoziierte Elemente.*

Die Existenz und Eindeutigkeit der Zerlegung ganzer Zahlen in Primfaktoren, der natürlich die Existenz von Primteilern zugrunde liegt, ist der Inhalt des sog. *Fundamentalsatzes der elementaren Zahlentheorie.* In der Schulmathematik wird er im allgemeinen nur für natürliche Zahlen[1]) verwendet, wobei sich allerdings ein Beweis im Schulunterricht verbietet. Dadurch entsteht leider allzuoft der Eindruck der Selbstverständlichkeit dieses Satzes, obwohl seine Gültigkeit eine Besonderheit des Ringes der ganzen Zahlen ist, die durchaus nicht in jedem Ringe vorzuliegen braucht.

In den Beweis müssen dementsprechend spezielle Eigenschaften des Ringes Γ der ganzen Zahlen eingehen. Solche Eigenschaften beruhen letzten Endes auf der Anordnung, die für die natürlichen Zahlen ihrer Entstehung nach gegeben ist und durch sie in den Ring Γ hineingetragen wird. Vom Standpunkt der Zahlentheorie ist daher ein solcher Beweis des Fundamentalsatzes anzustreben, der unmittelbar an diese Anordnungsaussagen anknüpft und möglichst unter Vermeidung allgemeiner theoretischer Überlegungen rasch zum Ziele führt. So verfährt ein erst in unserer Zeit von E. ZERMELO angegebener Beweis, der die angegebene Beschränkung der Hilfsmittel durch geschickte und kunstvolle Schlüsse erreicht. Wir verzichten jedoch hier auf seine Darstellung[2]), da ein solcher ganz auf die Verhältnisse im Ring Γ zugeschnittener Beweis naturgemäß wenig verallgemeinerungsfähig ist.

---

1) Damit beschränkt man sich zugleich auf positiv normierte Primfaktoren, so daß z. B. für 6 nur die Zerlegungen $6 = 2 \cdot 3 = 3 \cdot 2$, nicht aber die Zerlegungen

$$6 = (-2)(-3) = (-3)(-2)$$

betrachtet werden, was eine Verschärfung von S(40.3) mit sich bringt.

2) Den Beweis von ZERMELO findet man etwa in H. HASSE, Zahlentheorie, 1949, Akademie-Verlag Berlin, S. 3; H. HASSE, Vorlesungen über Zahlentheorie, 1950, J. Springer Berlin, S. 6.

Dagegen wird hier der Fundamentalsatz aus solchen Aussagen abgeleitet werden, die nicht nur für den Ring der ganzen Zahlen, sondern auch für eine Reihe anderer Ringe gültig sind. Dies geschieht in drei Abschnitten, in denen jeweils eine besondere Eigenschaft des Ringes Γ aus der Anordnung hergeleitet wird, während dann die Untersuchungen ohne größeren Aufwand gleich für alle Ringe mit dieser Eigenschaft weitergeführt werden können[1]). Dabei setzen wir Kommutativität, Nullteilerfreiheit und Existenz eines Einselementes wie in § 39 stets voraus. Auf einige Beispiele wird in einem letzten Abschnitt näher eingegangen.

Primzerlegung in Ringen mit Teilerkettensatz

Hilfssatz **S (40.4)**

Es sei a eine von Null verschiedene ganze Zahl. Dann ist der Absolutbetrag jedes echten Teilers von a kleiner als $|a|$, d. h.:

$$\text{Aus } a \neq 0 \text{ und } b \parallel a \text{ folgt } |b| < |a|.$$

Beweis

Aus $a = bx$ ergibt sich nach der bekannten Regel für den Betrag eines Produktes $|a| = |bx| = |b| \cdot |x|$. Da nach unseren Voraussetzungen x weder Null noch Einheit ist, also $|x| > 1$ ist, folgt nach dem Monotoniegesetz der Multiplikation

$$|a| = |b| \cdot |x| > |b| \cdot 1 = |b|.$$

qed.

Teilerkettensatz **S (40.5)**

Im Ring der ganzen Zahlen bricht jede Kette $a_1, a_2, a_3, \ldots$ echter Teiler

$$a_2 \parallel a_1, \quad a_3 \parallel a_2, \quad \ldots, \quad a_{i+1} \parallel a_i, \ldots$$

nach endlich vielen Gliedern ab.

Beweis

Da wegen $a_2 \parallel a_1$ höchstens das erste Glied einer Teilerkette gleich Null sein kann, folgt aus dem Hilfssatz

$$|a_2| > |a_3| > \ldots > |a_i| > \ldots .$$

1) Eine Übersicht über die folgenden Beweisgänge findet sich am Ende dieses Bandes.

Die Anordnung der ganzen Zahlen lehrt aber, daß es nur endlich viele positive Zahlen gibt, die kleiner als $|a_2|$ sind.

qed.

Definition **D (40.6)**

Ein Ring, in dem jede Kette echter Teiler nach endlich vielen Gliedern abbricht, heißt ein Ring mit Teilerkettensatz.

Satz **S (40.7)**

In jedem Ring $\mathfrak{R}$ *mit Teilerkettensatz gelten die Aussagen* S(40.1) *und* S(40.2).

Beweis

1. Es sei $a \neq o$ ein von einer Einheit verschiedenes Element aus $\mathfrak{R}$. Falls a selbst Primelement ist, bleibt nichts mehr zu beweisen. Andernfalls hat $a = a_1$ einen echten, von einer Einheit verschiedenen Teiler a_2. Die gleiche Überlegung zeigt, daß a_2 entweder Primelement ist oder einen ebensolchen Teiler a_3 besitzt. Dieses Verfahren liefert nach endlich vielen Schritten einen Primteiler a_n von a, da andernfalls die Teilerkette

$$a_2 \parallel a_1, \quad a_3 \parallel a_2, \ldots$$

entgegen der Voraussetzung nicht abbrechen würde.

2. Es sei a wie oben gewählt. Nach dem eben bewiesenen Satz S(40.1) existiert wenigstens ein Primteiler von a. Entweder ist nun dieser Primteiler (bis auf Einheiten) a selbst oder ein echter Teiler p_1 von a. Im ersten Falle ist die „Primzerlegung" von a von der trivialen Form $a = a$. Im zweiten Falle hat man zunächst

$$a = p_1 a_1,$$

wobei a_1 ein von einer Einheit verschiedener echter Teiler von a ist. Entsprechend erhält man: Entweder ist a_1 Primelement und die Zerlegung von a beendet, oder a_1 besitzt einen echten Primteiler p_2, also

$$a = p_1 p_2 a_2,$$

wobei a_2 ein von einer Einheit verschiedener echter Teiler von a_1 ist.

So weiterschließend kommt man zu einer Primzerlegung

$$a = p_1 p_2 \cdots p_n,$$

da man sonst eine nicht abbrechende Teilerkette

$$a_1 \parallel a,\ a_2 \parallel a_1,\ a_3 \parallel a_2, \ldots$$

erhalten würde. qed.

Dagegen reicht die in diesem Abschnitt gemachte Voraussetzung nicht aus, um auch die Eindeutigkeitsaussage S (40.3) zu beweisen. Wir werden Ringe mit Teilerkettensatz kennenlernen, in denen wohl jedes Element nach dem eben Bewiesenen als Produkt von Primelementen geschrieben werden kann, ohne daß jedoch diese Darstellung stets eindeutig ist (vgl. B (40.20)).

Primzerlegung in euklidischen Ringen

Auf Grund der in Γ vorliegenden Anordnung gilt für ganze Zahlen der sog. *euklidische Algorithmus*[1]). Er beruht darauf, daß für beliebige ganze Zahlen a und $b \neq 0$ zwei weitere ganze Zahlen q und r gefunden werden können, die die Relation

$$a = bq + r \quad \text{mit} \quad 0 \leqq |r| < |b|$$

erfüllen. In Verallgemeinerung dieses Sachverhaltes erklären wir:

Definition **D (40.8)**

Ein Integritätsbereich $\mathfrak{R}$ heißt ein euklidischer Ring, wenn jedem Element $a \neq o$ aus $\mathfrak{R}$ eine nichtnegative ganze Zahl $g(a)$ zugeordnet werden kann, so daß die folgenden Bedingungen erfüllt sind:

(1) $g(ab) \geqq g(a)$.

(2) *Zu je zwei Elementen a und $b \neq o$ aus $\mathfrak{R}$ existieren zwei Elemente q und r aus $\mathfrak{R}$, die der Relation*

$$a = bq + r \quad \textit{mit} \quad r = o \quad \textit{oder} \quad g(r) < g(b)$$

genügen (Division mit Rest).

---

1) EUKLID von Alexandria, um 300 v. Chr., „Elemente" Buch VII.

Nach unserer obigen Bemerkung ist der Ring der ganzen Zahlen ein euklidischer Ring, wobei einfach $g(a) = |a|$ zu setzen ist. Ein weiteres Beispiel für einen euklidischen Ring ist der Polynomring $\mathfrak{K}[x]$ über einem Körper $\mathfrak{K}$; als $g(f(x))$ ist dabei der Grad von $f(x)$ zu nehmen[1]). Auch der Ring $\Gamma + \Gamma i$ der ganzen GAUSSschen Zahlen ist mit $g(a + bi) = N(a + bi) = a^2 + b^2$ ein euklidischer Ring (vgl. Aufg. 3).

Hilfssatz **S (40.9)**

In einem euklidischen Ring gilt:

$$\text{Aus } a \neq o \text{ und } b \parallel a \text{ folgt } g(b) < g(a).$$

Beweis

In der nach (2) möglichen Darstellung $b = aq + r$ ist $r \neq o$, da sonst $a \mid b$ entgegen der Voraussetzung $b \parallel a$ wäre. Also ist $g(r) < g(a)$. Aus $a = bx$ und

$$r = b - aq = b(e - xq)$$

folgt andererseits nach (1)

$$g(r) \geqq g(b),$$

woraus sich bereits die Behauptung ergibt. qed.

Teilerkettensatz **S (40.10)**

Jeder euklidische Ring ist ein Ring mit Teilerkettensatz.

Beweis

Für die Elemente $a_1, a_2, a_3, \ldots$ einer Teilerkette

$$a_2 \parallel a_1, \quad a_3 \parallel a_2, \ldots$$

folgt wegen $a_i \neq o$ für $i \geqq 2$ nach dem eben bewiesenen Hilfssatz

$$g(a_2) > g(a_3) > \ldots.$$

Diese Folge nichtnegativer Zahlen mit abnehmendem Betrag muß aber nach endlich vielen Gliedern abbrechen. qed.

---

1) Der in B (40.19) geführte Beweis für diese Behauptung kann bereits an dieser Stelle gelesen werden.

Damit ist bereits der Anschluß zu S(40.7) hergestellt, wonach aus dem Teilerkettensatz die Gültigkeit von S(40.1) und S(40.2), also die Existenz der Primzerlegung folgt. Darüber hinaus ist es unter unseren jetzigen Voraussetzungen auch möglich, die Eindeutigkeit dieser Zerlegung nachzuweisen, was das Ziel der nun folgenden Betrachtungen ist.

Hauptsatz über den größten gemeinsamen Teiler **S (40.11)**

In einem euklidischen Ring $\mathfrak{R}$ *gilt der Hauptsatz über den größten gemeinsamen Teiler, d. h.:*

1. *Zu je n Elementen* $a_1, a_2, \ldots, a_n$ *aus* $\mathfrak{R}$ *gibt es stets einen größten gemeinsamen Teiler* $d \cong (a_1, a_2, \ldots, a_n) \in \mathfrak{R}$.
2. *Der größte gemeinsame Teiler* $d \cong (a_1, a_2, \ldots, a_n)$ *läßt sich aus* $a_1, a_2, \ldots, a_n$ *mit geeigneten Koeffizienten* $c_1, c_2, \ldots, c_n$ *aus* $\mathfrak{R}$ *linear kombinieren:*

$$d = c_1 a_1 + c_2 a_2 + \ldots + c_n a_n.$$

Beweis

Den Fall $a_1 = a_2 = \ldots = a_n = o$ dürfen wir mit $d = o$ im folgenden beiseite lassen. Ferner beschränken wir uns zunächst auf zwei Elemente $a_1 = a$ und $a_2 = b$, wobei $b \neq o$ angenommen werden darf. Wir verwenden zum Beweis den in fortgesetzter Division mit Rest bestehenden euklidischen Algorithmus:

$$\begin{aligned}
a &= bq_0 + r_1 && \text{mit } g(r_1) < g(b),\\
b &= r_1 q_1 + r_2 && \text{mit } g(r_2) < g(r_1),\\
r_1 &= r_2 q_2 + r_3 && \text{mit } g(r_3) < g(r_2),\\
&\vdots && \vdots\\
r_{n-2} &= r_{n-1} q_{n-1} + r_n && \text{mit } g(r_n) < g(r_{n-1}),\\
r_{n-1} &= r_n q_n + o.
\end{aligned}$$

Das Verfahren muß wegen $g(r_1) > g(r_2) > \ldots$ nach endlich vielen Schritten abbrechen, wobei r_n der letzte von o verschiedene Rest sei.

Dieses Element r_n ist größter gemeinsamer Teiler von a und b. Liest man nämlich die obigen Gleichungen von unten nach oben, so er-

hält man der Reihe nach (vgl. F(39.2h)):

$$r_n \mid r_{n-1},\ r_n \mid r_{n-2},\ \ldots,\ r_n \mid r_1,\ r_n \mid b,\ r_n \mid a.$$

Also ist r_n gemeinsamer Teiler von a und b. Für jeden anderen gemeinsamen Teiler t von a und b folgt aber, wenn man nunmehr die Gleichungen von oben nach unten liest:

$$t \mid r_1,\ t \mid r_2,\ \ldots,\ t \mid r_n.$$

Damit ist bereits $r_n \cong (a, b)$ gezeigt.

Zum Beweis der zweiten Behauptung betrachten wir nochmals die Gleichungen von oben nach unten. Wegen der ersten Gleichung ist nämlich r_1 Linearkombination von a und b, diese eingesetzt in die zweite Gleichung liefert r_2 ebenfalls als Linearkombination von a und b, usw., bis die vorletzte Gleichung die behauptete Linearkombination für den größten gemeinsamen Teiler r_n ergibt.

Die Existenz des größten gemeinsamen Teilers für mehr als zwei Elemente folgt unmittelbar aus der Beziehung (vgl. Aufg. 7 von § 39)

$$(a_1, a_2, \ldots, a_\nu) = ((a_1, a_2, \ldots, a_{\nu-1}), a_\nu).$$

Entsprechend erhält man die behauptete Linearkombination von $d \cong (a_1, a_2, \ldots, a_n)$ durch sukzessive Berechnung der Linearkombinationen von (a_1, a_2), von $((a_1, a_2), a_3), \ldots,$ schließlich von $((a_1, a_2, \ldots, a_{n-1}), a_n)$.

Man beachte, daß alle Schritte dieses Beweises konstruktiv sind (vgl. Aufg. 7).

qed.

Dieser eben bewiesene Hauptsatz über den größten gemeinsamen Teiler nimmt nun für den Beweis der Eindeutigkeit der Primzerlegung dieselbe zentrale Stellung ein wie der Teilerkettensatz für den Beweis der Existenz der Primzerlegung. Wie sich herausstellen wird, folgt nämlich S(40.3) allein unter der Voraussetzung, daß in dem betrachteten Ring $\mathfrak{R}$ stets $d \cong (a_1, a_2, \ldots, a_n)$ existiert und aus $a_1, a_2, \ldots, a_n$ linear kombiniert werden kann. Vorbereitend zeigen wir dazu:

Hilfssatz **S (40.12)**

Es sei $\mathfrak{R}$ ein Ring, in dem der Hauptsatz über den größten gemeinsamen Teiler gilt. Dann folgt in $\mathfrak{R}$:

a) *Ein Teiler eines Produktes, der zu dem einen Faktor teilerfremd ist, geht in dem anderen Faktor auf, d. h.:*

$$\text{Aus } t \mid ab \text{ und } (t, a) \cong e \text{ folgt } t \mid b.$$

b) *Ein Primelement p geht in einem Element a entweder auf oder ist teilerfremd zu ihm, d. h.:*

$$\text{Entweder } p \mid a \text{ oder } (p, a) \cong e.$$

Beweis

a) Der größte gemeinsame Teiler e von t und a läßt sich zufolge des Hauptsatzes mit Koeffizienten y und z aus $\mathfrak{R}$ linear kombinieren:

$$e = yt + za.$$

Multiplikation dieser Gleichung mit b und Verwendung von $t \mid ab$, also $ab = tx$, ergibt die Behauptung:

$$b = ytb + zab = ytb + ztx = t(yb + zx).$$

b) Ist $d \cong (p, a)$ nicht assoziiert zu e, so erhält man aus $d \mid p$ zunächst $d \cong p$, da p Primelement ist. Aus $d \mid a$ folgt damit aber bereits $p \mid a$. qed.

Die beiden Aussagen des Hilfssatzes liefern unmittelbar die für den Beweis der Eindeutigkeit der Primzerlegung entscheidende, ja mit ihr gleichwertige

Folgerung **F (40.13)**

Es sei $\mathfrak{R}$ ein Ring, in dem der Hauptsatz über den größten gemeinsamen Teiler gilt. Dann folgt in $\mathfrak{R}$

$$\text{aus } p \mid ab \text{ entweder } p \mid a \text{ oder } p \mid b \text{ oder beides.}$$

Beweis

Für $p \mid a$ ist nichts mehr zu beweisen. Andernfalls folgt aus S(40.12b) $(p, a) \cong e$ und damit aus S(40.12a) $p \mid b$. qed.

Diese Aussage läßt sich durch mehrfache Anwendung auf ein Produkt von mehr als zwei Faktoren verallgemeinern:

Aus $p \mid a_1 a_2 \ldots a_m$ *folgt* $p \mid a_i$ *für wenigstens ein* i.

Wir verwenden sie in dieser Form zum Beweis der Eindeutigkeit der Primzerlegung.

Satz **S (40.14)**

Ein Ring $\mathfrak{R}$, *in dem der Hauptsatz über den größten gemeinsamen Teiler gilt, erfüllt* S(40.3)*:*

$$\text{Aus } a \cong p_1 p_2 \cdots p_n \cong q_1 q_2 \cdots q_m$$

folgt $n = m$ *und* $p_i \cong q_i$ *bei geeigneter Numerierung.*

Beweis

Ohne Beschränkung der Allgemeinheit sei $n \leq m$. Im Falle $n = 1$ ergibt sich die Behauptung sofort aus der Unzerlegbarkeit des Primelementes p_1. Wir führen vollständige Induktion von $n - 1$ auf n durch.

Gemäß der oben formulierten Aussage folgt aus $p_n \mid q_1 q_2 \ldots q_m$ jedenfalls $p_n \mid q_i$ für wenigstens ein i. Bei geeigneter Numerierung können wir also $p_n \mid q_m$ annehmen. Da p_n und q_m Primelemente sind, gilt sogar $p_n \cong q_m$, und wir gelangen durch Division zu

$$p_1 p_2 \cdots p_{n-1} \cong q_1 q_2 \cdots q_{m-1}.$$

Die Induktionsvoraussetzung vollendet mit $n - 1 = m - 1$, also $n = m$ und $p_i \cong q_i$ für $i = 1, 2, \ldots, n - 1$ den Beweis. qed.

Damit sind insbesondere für euklidische Ringe, also auch für den Ring der ganzen Zahlen, den Polynomring $\mathfrak{R}[x]$ über einem Körper $\mathfrak{R}$ und den Ring $\Gamma + \Gamma i$ der ganzen GAUSSschen Zahlen die am Anfang dieses Paragraphen aufgestellten Sätze vollständig bewiesen.

Primzerlegung in Hauptidealringen

Wir hätten uns schließlich von vornherein darauf stützen können, daß der Ring der ganzen Zahlen ein Hauptidealring ist (vgl. Aufg.2 von § 28). Man kann nämlich daraus unmittelbar sowohl den Teilerkettensatz als auch den Hauptsatz über den größten gemeinsamen Teiler ableiten, aus denen dann in der jeweils besprochenen

Weise die Sätze S(40.1), S(40.2) und S(40.3) folgen. Damit führen wir übrigens einen zweiten Beweis für die Gültigkeit dieser Sätze in euklidischen Ringen, denn es gilt:

Satz **S (40.15)**

Jeder euklidische Ring ist Hauptidealring[1]).

Beweis

Wir zeigen, daß jedes Ideal eines euklidischen Ringes $\mathfrak{R}$ Hauptideal ist. Für das Nullideal ist das klar. Jedes andere Ideal $\mathfrak{a}$ enthält wenigstens ein Element $a \neq o$. Unter allen diesen Elementen gibt es dann solche, für die $g(a)$ einen möglichst kleinen Wert annimmt. Ein solches Element a erzeugt das Ideal $\mathfrak{a}$. Ist nämlich b ein beliebiges Element aus $\mathfrak{a}$, so gilt

$$b = aq + r \text{ mit } r = o \text{ oder } g(r) < g(a);$$

letzteres ist jedoch wegen $b - aq = r \in \mathfrak{a}$ nicht möglich, da $g(a)$ für alle Idealelemente minimal gewählt war. Also ist $r = o$, d. h., es lassen sich alle Elemente $b \in \mathfrak{a}$ als Ringvielfache aq darstellen, womit $\mathfrak{a}$ als Hauptideal nachgewiesen ist. qed.

Wie der Leser bemerkt haben wird, beruht dieser Beweis auf einer Verallgemeinerung der entsprechenden Schlüsse für den Ring Γ der ganzen Zahlen mit $g(a) = |a|$. Wir lernten diesen Beweisgang bereits in Aufg. 14 von § 5 kennen, was daran liegt, daß im speziellen Falle des Ringes Γ die Untermoduln von Γ^+ mit den Idealen von Γ zusammenfallen (vgl. nochmals die Aufgaben 1 und 2 von § 28).

Wir kommen nun zu den beiden angekündigten Aussagen über Hauptidealringe, wobei wir wieder daran erinnern, daß die betrachteten Ringe als Integritätsbereiche mit Einselement angenommen werden.

Teilerkettensatz **S (40.16)**

Jeder Hauptidealring ist ein Ring mit Teilerkettensatz.

Beweis

In dem Hauptidealring $\mathfrak{R}$ liege eine beliebige Teilerkette vor:

$$a_2 \| a_1, \; a_3 \| a_2, \ldots.$$

1) Wir bemerken, daß für diese Feststellung die Bedingung (1) von D(40.8) nicht notwendig ist.

Dann betrachten wir die Menge $\mathfrak{a}$ aller Elemente $a \in \mathfrak{R}$, die durch ein Element a_i der Teilerkette teilbar sind.

Wir zeigen zunächst, daß die so definierte Menge $\mathfrak{a}$ ein Ideal von $\mathfrak{R}$ ist:

(1) Es seien a und a' zwei Elemente aus $\mathfrak{a}$. Dann existieren also zwei Elemente a_i und a_j der Teilerkette mit

$$a_i \mid a \quad \text{und} \quad a_j \mid a'.$$

Ohne Beschränkung der Allgemeinheit dürfen wir $j \geqq i$ annehmen, so daß aus $a_j \mid a_i$ folgt

$$a_j \mid a \quad \text{und} \quad a_j \mid a'.$$

Daraus ergibt sich aber bereits

$$a_j \mid a - a', \quad \text{also} \quad a - a' \in \mathfrak{a}.$$

(2) Ist $a \in \mathfrak{a}$, also wieder $a_i \mid a$, so folgt für ein beliebiges Element $r \in \mathfrak{R}$

$$a_i \mid ra, \quad \text{also} \quad ra \in \mathfrak{a}.$$

Dieses Ideal $\mathfrak{a}$ ist nach Voraussetzung ein Hauptideal, welches etwa von dem Element $\alpha \in \mathfrak{a}$ erzeugt werde, wobei wegen der Existenz des Einselementes in $\mathfrak{R}$ sogar gilt (vgl. F (28.7)):

$$\mathfrak{a} = \mathfrak{R}\alpha.$$

Mit den nun bereitgestellten Hilfsmitteln kann man die Annahme, daß die Teilerkette nicht nach endlich vielen Gliedern abbricht, zum Widerspruch führen. Wegen $\alpha \in \mathfrak{a}$ folgt aus der Definition von $\mathfrak{a}$ die Existenz eines Elementes a_k der Teilerkette mit

$$a_k \mid \alpha.$$

Das in einer nicht abbrechenden Teilerkette vorhandene Element a_{k+1} erfüllt dann wegen $a_{k+1} \mid a_k$ ebenfalls

$$a_{k+1} \mid \alpha.$$

Andererseits bestehen aber die Relationen

$$\alpha \mid a_k \quad \text{und} \quad \alpha \mid a_{k+1},$$

da jedes Element der Teilerkette nach Definition in $\mathfrak{a}$ enthalten ist und damit wegen $\mathfrak{a} = \mathfrak{R}\alpha$ Ringvielfaches von α ist.

Damit gilt jedoch $a_k \cong \alpha$ und $a_{k+1} \cong \alpha$ und somit wegen der Transitivität dieser Beziehung $a_k \cong a_{k+1}$ im Widerspruch zu $a_{k+1} \parallel a_k$.

qed.

Hauptsatz über den größten gemeinsamen Teiler **S (40.17)**

In jedem Hauptidealring gilt der Hauptsatz über den größten gemeinsamen Teiler.

Beweis

Es seien $a_1, a_2, \ldots, a_n$ Elemente eines Hauptidealringes $\mathfrak{R}$. Wir betrachten das von diesen Elementen erzeugte Ideal[1])

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

das nach Voraussetzung schon von einem geeigneten Element $\alpha \in \mathfrak{a}$ erzeugt werden kann. Wegen der Existenz eines Einselementes in $\mathfrak{R}$ gilt weiterhin

$$\mathfrak{a} = \mathfrak{R}a_1 + \mathfrak{R}a_2 + \ldots + \mathfrak{R}a_n = \mathfrak{R}\alpha,$$

woraus sich insbesondere die Darstellungen

$$a_1 = r_1\alpha, \quad a_2 = r_2\alpha, \quad \ldots, \quad a_n = r_n\alpha,$$
$$\alpha = c_1a_1 + c_2a_2 + \ldots + c_na_n$$

mit geeigneten Elementen r_i und c_i aus $\mathfrak{R}$ ergeben. Die ersten n Gleichungen lehren, daß α gemeinsamer Teiler von $a_1, a_2, \ldots, a_n$ ist, während aus der letzten Gleichung folgt, daß jeder gemeinsame Teiler t von $a_1, a_2, \ldots, a_n$ auch Teiler von α ist und das somit als größter gemeinsamer Teiler $(a_1, a_2, \ldots, a_n)$ nachgewiesene Element α aus $a_1, a_2, \ldots, a_n$ linear kombiniert werden kann.

qed.

Beispiele

Trotz der strukturellen Klarheit der Sätze S (40.1), S (40.2) und S (40.3) und der weitreichenden Folgerungen, die man aus ihrer Gültigkeit in einem Ringe ziehen kann und auf die wir im nächsten Paragraphen etwas näher eingehen werden, ist die tatsächliche Zerlegung eines Elementes in konkreten Fällen mitunter außerordent-

---

1) Man beachte, daß durch $(a_1, \ldots, a_n)$ sowohl das von den Elementen $a_1, \ldots, a_n$ erzeugte Ideal als auch der größte gemeinsame Teiler dieser Elemente bezeichnet wird. Da es aber natürlich aus dem Zusammenhang jeweils hervorgeht, ob das Ideal $(a_1, \ldots, a_n)$ oder das Element $(a_1, \ldots, a_n)$ gemeint ist, erscheint diese doppelte Verwendung der gleichen Bezeichnung sogar recht glücklich; denn wie der Beweis lehrt, ist (in Hauptidealringen) das von den Elementen $a_1, \ldots, a_n$ erzeugte Ideal gerade das von ihrem größten gemeinsamen Teiler erzeugte Hauptideal (vgl. auch S (42.7) ff.):

$$\mathfrak{a} = (a_1, \ldots, a_n) = (\alpha) = ((a_1, \ldots, a_n)).$$

lich mühevoll. Die Schwierigkeiten beginnen meist schon mit der Feststellung, welche Einheiten in dem betreffenden Ring vorhanden sind und ob ein bestimmtes Element überhaupt zerlegbar oder selbst Primelement ist. Im folgenden behandeln wir dazu einige Beispiele und schließen mit der Betrachtung einiger Ringe, in denen wohl eine Primzerlegung existiert, diese aber nicht für alle Elemente eindeutig ist.

Ring der ganzen Zahlen **B (40.18)**

Bei Untersuchungen im Ring der ganzen Zahlen beschränkt man sich im allgemeinen, wie erwähnt, auf die Betrachtung positiver Zahlen, da ja die Einheiten ± 1 und die durch sie hervorgerufene übersichtliche Klasseneinteilung in assoziierte Elemente von vornherein bekannt sind. Dagegen gibt es bis heute noch kein praktisch verwertbares Kriterium, von einer beliebigen Zahl festzustellen, ob sie Primzahl ist. Man ist vielmehr gezwungen, unmittelbar auf die Definition zurückzugehen und sämtliche eventuell in Frage kommenden Teiler durchzuprobieren[1]). Ja es ist sogar sehr problematisch, wenigstens gewisse Sorten von Zahlen, etwa durch eine Formel, anzugeben, die Primzahlen sind.

Bekannt ist in dieser Beziehung eine Vermutung von FERMAT, daß alle Zahlen $2^{2^n}+1$ für $n = 0, 1, 2, \ldots$ Primzahlen seien. In der Tat liefert diese Formel für $n = 0, 1, 2, 3, 4$ die Primzahlen 3, 5, 17, 257, 65537; dagegen ist schon die Zahl

$$2^{2^5}+1 = 4294967297 = 641 \cdot 6700417$$

keine Primzahl, wie EULER als erster bewiesen hat. Es ist bis heute ungeklärt, ob es überhaupt noch einen Exponenten n gibt, für den $2^{2^n}+1$ Primzahl ist. Lediglich für

$$n = 6, 7, 8, 9, 11, 12, 18, 23, 36, 38, 73$$

ist diese Frage bisher negativ entschieden.

Entsprechendes gilt für die von MERSENNE[2]) aufgestellte Formel $2^q - 1$, in der q selbst die Reihe der Primzahlen durchlaufen soll. Auch hier erhält man für $q = 2, 3, 5, 7$ die Primzahlen 3, 7, 31, 127, während

$$2^{11} - 1 = 2047 = 23 \cdot 89$$

zerfällt. Allerdings liefern hier die Zahlen

$$q = 13, 17, 19, 31, 61, 89, 107, 127$$

---

1) Von der Mühseligkeit dieses Verfahrens überzeuge sich der Leser etwa bei dem Versuch, die im folgenden auftretenden Zahlen 641 und 6700417 als Primzahlen nachzuweisen.

2) MARIN MERSENNE, 1588—1648.

weitere MERSENNEsche Primzahlen, während sonst alle Primzahlen $q \leqq 257$ (mit Ausnahme der noch fraglichen Zahl $q = 193$) keine Primzahlen ergeben. Ob es jedoch unendlich viele MERSENNEsche Primzahlen gibt, ist ebenfalls noch nicht geklärt.

Erst in neuester Zeit ist es gelungen, teilweise auf recht komplizierte Art, Folgen von Zahlen anzugeben, die sämtlich unzerlegbar sind. Ein weiteres Eingehen darauf verbietet sich aber an dieser Stelle.

Um so beachtlicher ist es, daß sich schon in den Elementen von EUKLID[1]) der nach ihm benannte Satz findet: „Es gibt mehr Primzahlen als jede vorgelegte Anzahl von Primzahlen." Die Folge der Primzahlen ist also unendlich, obgleich die Primzahlen in den heute bis zur Größenordnung 10^7 vorliegenden Tabellen ständig seltener werden und man überdies die Existenz von beliebig großen Lücken nachweisen kann.

Auf die Probleme, die sich aus einem genaueren Studium der Verteilung der Primzahlen in der Folge der natürlichen Zahlen ergeben, wollen wir den Leser hier wenigstens hinweisen. Im Mittelpunkt dieser Untersuchungen steht die sog. Primzahlfunktion $\pi(x)$, die für jede natürliche Zahl x die Anzahl der Primzahlen im Intervall $2 \leqq p \leqq x$ angibt, also:

$$\pi(2) = 1,\ \pi(3) = 2, \ldots, \pi(100) = 25, \ldots, \pi(1000) = 168, \ldots .$$

Obwohl keine einfache Formel für $\pi(x)$ bekannt ist, lassen sich doch Abschätzungen ermitteln, die für wachsende x immer genauer werden. So vermutete schon GAUSS den Primzahlsatz, daß sich $\frac{x}{\ln x}$ der gesuchten Funktion $\pi(x)$ für $x \to \infty$ asymptotisch annähert, d. h.

$$\lim_{x \to \infty} \frac{\pi(x)}{\frac{x}{\ln x}} = 1 .$$

Die ersten gesicherten Resultate zum Beweis dieses Satzes erzielte jedoch erst in der Mitte des vorigen Jahrhunderts der bekannte russische Mathematiker TSCHEBYSCHEW[2]), die einen wesentlichen Schritt an die Lösung des Problems heranführten. Der endgültige Beweis gelang 1896 gleichzeitig dem Franzosen J. HADAMARD und dem Belgier Ch. DE LA VALLÉE-POUSSIN mit tiefliegenden funktionentheoretischen Hilfsmitteln. Ein „elementarer", d. h. von solchen Hilfsmitteln freier Beweis konnte erst 1948 von A. SELBERG und P. ERDÖS erbracht werden.

Eine weitere Abschätzung für $\pi(x)$, die sogar genauere Werte als die eben besprochene liefert, geht auf RIEMANN[3]) zurück und beruht wesentlich auf

---

1) Elemente, Buch IX, Satz 20. Für den Beweis dieser wie der unmittelbar folgenden zahlentheoretischen Aussagen verweisen wir auf entsprechende Lehrbücher.

2) P. L. TSCHEBYSCHEW, 1821—1894.

3) BERNHARD RIEMANN, 1826—1866.

einem 1895 von H. v. MANGOLDT bewiesenen Satz. Sie wird durch den sog. Integrallogarithmus gegeben:

$$\operatorname{li} x = 1{,}04 + \int_2^x \frac{dy}{\ln y}.$$

Polynomring $\mathfrak{R}[x]$ **B (40.19)**

Wir zeigen zunächst, daß der Polynomring $\mathfrak{R}[x]$ über einem Körper $\mathfrak{R}$ ein euklidischer Ring ist, indem wir jedem Polynom $f(x) \neq o$ aus $\mathfrak{R}[x]$ als nichtnegative ganze Zahl $g(f(x))$ seinen Grad zuordnen.

Jedenfalls ist damit die Bedingung (1) aus D (40.8) erfüllt (vgl. F (32.5)). Bedingung (2) verlangt den Nachweis, daß für je zwei Polynome $f(x)$ und $h(x) \neq o$ aus $\mathfrak{R}[x]$ eine Darstellung

$$f(x) = h(x)q(x) + r(x) \text{ mit } r(x) = o \text{ oder } g(r(x)) < g(h(x))$$

existiert.

Für den Fall $f(x) = o$ oder $g(f(x)) < g(h(x))$ ist mit

$$f(x) = h(x) \cdot o + f(x)$$

alles erfüllt. Es sei also $n = g(f(x)) \geqq g(h(x)) = m$ und

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots, \quad h(x) = b_m x^m + b_{m-1}x^{m-1} + \ldots$$

Dann bilden wir mit

$$f(x) - \frac{a_n}{b_m} x^{n-m} h(x) = \left(a_n - \frac{a_n}{b_m} b_m\right) x^n + \left(a_{n-1} - \frac{a_n}{b_m} b_{m-1}\right) x^{n-1} + \ldots$$

ein Polynom $f_1(x)$ vom Grad $l \leqq n - 1$:

$$f_1(x) = c_l x^l + c_{l-1}x^{l-1} + \ldots$$

Entsprechend erhalten wir durch

$$f_1(x) - \frac{c_l}{b_m} x^{l-m} h(x) = \left(c_l - \frac{c_l}{b_m} b_m\right) x^l + \left(c_{l-1} - \frac{c_l}{b_m} b_{l-1}\right) x^{l-1} + \ldots$$

ein Polynom $f_2(x)$ vom Grade $k \leqq l - 1$.

Dieses Verfahren setzen wir fort, bis sich ein Polynom $f_i(x) = o$ oder $f_i(x) = r(x)$ mit einem Grad $g(r(x)) < m$ ergibt. Wir erhalten so

$$f(x) - \left(\frac{a_n}{b_m} x^{n-m} + \frac{c_l}{b_m} x^{l-m} + \ldots\right) h(x) = r(x),$$

also in der Tat wie behauptet[1])

$$f(x) = h(x)\,q(x) + r(x).$$

Nach unseren Ausführungen über euklidische Ringe läßt sich daher jedes Polynom $f(x) \in \mathfrak{R}[x]$ als Produkt von irreduziblen Polynomen schreiben. Dabei sind die einzelnen Faktoren bis auf die Reihenfolge und bis auf Einheiten, d. h. bis auf die Multiplikation mit einem Element $a \neq o$ aus $\mathfrak{R}$, eindeutig bestimmt. So gilt z. B. in $P[x]$:

$$\begin{aligned} \tfrac{1}{6}x^4 + \tfrac{2}{3}x + \tfrac{1}{2} &= (\tfrac{1}{2}x^2 - x + \tfrac{3}{2})\,(x+1)\,(\tfrac{1}{3}x + \tfrac{1}{3}) \\ &= (\tfrac{1}{6}x^2 - \tfrac{1}{3}x + \tfrac{1}{2})\,(x+1)^2; \end{aligned}$$

wie man sich leicht überzeugt, sind die in beiden Zerlegungen auftretenden Faktoren irreduzibel und paarweise assoziiert.

Allgemein ist es auch in $\mathfrak{R}[x]$ sehr schwierig, die Unzerlegbarkeit eines Polynoms $f(x)$ festzustellen bzw. es zu zerlegen. Etwas günstiger sind die Verhältnise, wenn die Koeffizienten von $f(x)$ bereits in einem Ring $\mathfrak{R}$ liegen, von dem $\mathfrak{R}$ Quotientenkörper ist. Allerdings erfordert dies die Untersuchung der Teilbarkeitsverhältnisse in Polynomringen $\mathfrak{R}[x]$, deren Koeffizientenbereich $\mathfrak{R}$ kein Körper ist. Solche Polynomringe sind aber im Gegensatz zu $\mathfrak{R}[x]$ keine Hauptidealringe (vgl. Aufg. 8 bzw. für den Spezialfall $\mathfrak{R} = \Gamma$ Aufg. 5 von § 36), und es ist damit fraglich, ob in ihnen der Satz von der eindeutigen Zerlegbarkeit in Primelemente gilt. Wir werden aber in einem späteren Kapitel (§ 48) ausführlich darlegen, daß sich die Gültigkeit dieses Satzes von $\mathfrak{R}$ auf $\mathfrak{R}[x]$ überträgt. Gestützt auf die Zerlegung der Elemente von $\mathfrak{R}$ kann man dann gewisse Kriterien für die Zerlegung von Polynomen aus $\mathfrak{R}[x]$ und sogar aus $\mathfrak{R}[x]$ angeben. Unter Umständen ist es auch möglich, die Zerlegung eines Polynoms in irreduzible Faktoren in endlich vielen Schritten zu konstruieren.

Ringe der Form $\Gamma + \Gamma\sqrt{k}$ **B (40.20)**

Wie wir im folgenden zeigen werden, gelten in allen diesen Ringen, die wir schon in B(26.4a) kennenlernten, die Sätze S(40.1) und S(40.2). Ob jedoch die damit existierende Primzerlegung im Sinne von S(40.3) eindeutig ist oder nicht, hängt von der Wahl der ganzen

1) Wie man sich leicht überlegt, sind dabei $r(x)$ und $q(x)$ durch $f(x)$ und $h(x)$ eindeutig bestimmt. Diese Eindeutigkeit der Division mit Rest ist eine Besonderheit des Ringes $\mathfrak{R}[x]$, die z. B. für den Ring Γ nicht gilt (vgl. etwa die Lösung zu Aufg. 7).

Zahl k ab. So erhält man z. B. für $k = -1$ den Ring der ganzen GAUSSschen Zahlen $\Gamma + \Gamma i$, der euklidisch ist und damit S(40.3) erfüllt. Dagegen wird sich z. B. in den Ringen mit $k = -5, -6, +26$ die Primzerlegung geeigneter Elemente als nicht eindeutig herausstellen. Wie wir hier nur mitteilen wollen, gibt es sowohl für $k > 0$ als auch für $k < 0$ weitere Ringe, in denen die Primzerlegung eindeutig (z. B. $k = -7, 2, 3$) oder nicht eindeutig ist (z. B. $k = -14, 10, 82$). Die allgemeine Frage, welche der beiden Fälle für einen bestimmten Wert für k vorliegt, ist ein schwieriges zahlentheoretisches Problem, auf das wir hier selbstverständlich nicht eingehen können.

Im folgenden sei zunächst $\mathfrak{R} = \Gamma + \Gamma\sqrt{k}$ ein beliebiger der von uns betrachteten Ringe. Die Bestimmung seiner Einheiten läuft nach Aufg. 3 von § 39 auf die ganzzahlige Lösung der sog. PELLschen Gleichung[1])

$$N(\varepsilon) = u^2 - kv^2 = \pm 1$$

hinaus. Auch die Entscheidung, ob ein vorgelegtes Element von $\mathfrak{R}$ Primelement ist, bzw. die Herstellung der (nicht notwendig eindeutigen) Primzerlegung der übrigen Elemente kann prinzipiell auf Untersuchungen im Ring Γ zurückgeführt werden. Man darf jedoch nicht übersehen, daß die dabei auftretenden (ganzzahlig zu lösenden) Gleichungen oft sehr schwer zu behandeln sind.

Wie schon das Vorgehen in Aufg. 3 von § 39 vermuten läßt, spielt bei diesen Überlegungen die Norm eines Elementes $\alpha = a + b\sqrt{k} \in \mathfrak{R}$

$$N(\alpha) = (a + b\sqrt{k})(a - b\sqrt{k}) = a^2 - kb^2$$

eine wichtige Rolle. Wir beweisen den dafür grundlegenden Satz:

Die Norm eines Produktes ist gleich dem Produkt der Normen der Faktoren:

$$N(\alpha_1 \cdot \alpha_2 \cdot \ldots \cdot \alpha_n) = N(\alpha_1) \cdot N(\alpha_2) \cdot \ldots \cdot N(\alpha_n).$$

Es sei also $\alpha_i = a_i + b_i\sqrt{k}$ und

$$(a_1 + b_1\sqrt{k}) \cdot \ldots \cdot (a_n + b_n\sqrt{k}) = a + b\sqrt{k}.$$

Bei Anwendung des durch die Zuordnung $a + b\sqrt{k} \to a - b\sqrt{k}$ gegebenen Automorphismus von $\mathfrak{R}$ (vgl. § 29) geht diese Gleichung über in

$$(a_1 - b_1\sqrt{k}) \cdot \ldots \cdot (a_n - b_n\sqrt{k}) = a - b\sqrt{k}.$$

---

1) JOHN PELL, 1610—1685.

Damit erhalten wir, wie behauptet,

$$(a_1 + b_1\sqrt{k})(a_1 - b_1\sqrt{k}) \dots (a_n + b_n\sqrt{k})(a_n - b_n\sqrt{k}) = (a + b\sqrt{k})(a - b\sqrt{k}).$$

Dieser allgemeine Satz, aus dem sich über $N(\varepsilon)N(\varepsilon^{-1}) = 1$ unmittelbar $N(\varepsilon) = \pm 1$ ergibt, lag bereits der Lösung von Aufg. 3 aus § 39 zugrunde. Weiterhin liefert er die den Hilfssätzen S(40.4) bzw. S(40.9) entsprechende Aussage:

Aus $\alpha \neq o$ *und* $\beta \| \alpha$ *folgt* $|N(\beta)| < |N(\alpha)|$.

Das ergibt sich nämlich sofort aus $\alpha = \beta\xi$ und $N(\xi) \neq \pm 1$ wegen $N(\alpha) = N(\beta) \cdot N(\xi)$ und $N(\alpha) = a^2 - kb^2 \neq 0$ nach Wahl von k.

Daraus folgt wieder unmittelbar die *Gültigkeit des Teilerkettensatzes, also die Existenz der Primzerlegung in* $\mathfrak{R} = \Gamma + \Gamma\sqrt{k}$.

Ferner ist für die Möglichkeit einer Zerlegung

$$\alpha = \alpha_1 \alpha_2 \dots \alpha_n$$

eines beliebigen Elementes $\alpha \in \mathfrak{R}$ nach dem grundlegenden Satz offenbar notwendig, daß die Norm $N(\alpha)$ im Ringe Γ zerlegt werden kann, nämlich gemäß

$$N(\alpha) = N(\alpha_1)N(\alpha_2) \dots N(\alpha_n).$$

Es kommen also nur solche $a_i + b_i\sqrt{k}$ *als Teiler in Frage, deren Norm* $a_i^2 - kb_i^2$ *ein Teiler von* $N(\alpha)$ *ist.* Daher läuft alles hinaus auf die ganzzahlige Lösung von Gleichungen der Form

$$x^2 - ky^2 = t \quad \text{mit} \quad t \mid N(\alpha).$$

Insbesondere ist α *sicher dann Primelement von* $\mathfrak{R}$, *wenn seine Norm* $N(\alpha)$ *ein Primelement von* Γ *ist.* Dieser Satz ist jedoch nicht umkehrbar.

Allgemein wollen wir noch betonen, daß unabhängig von der Gültigkeit von S(40.3) Primelemente von Γ im Ringe $\Gamma + \Gamma\sqrt{k}$ nichttriviale Zerlegungen haben können (vgl. das nächste Beispiel). Dies unterstreicht die Abhängigkeit des Begriffes „Primelement" von dem jeweils betrachteten Ring.

a) Im Ring $\Gamma + \Gamma i$ hat das in Γ unzerlegbare Element 5 die Zerlegung

$$5 = (2 + i)(2 - i) = (1 + 2i)(1 - 2i),$$

wobei die auftretenden Faktoren die Norm 5 haben und daher Primelemente von $\Gamma + \Gamma i$ sind. Im Einklang mit S(40.3) gilt $2 - i \cong 1 + 2i$ wegen $i(2 - i) = 2i + 1$ und entsprechend $2 + i \cong 1 - 2i$ wegen $(-i)(2 + i) = -2i + 1$.

b) Im Ringe $\Gamma + \Gamma\sqrt{-5}$ hat dagegen etwa das Element 6 zwei wesentlich verschiedene Zerlegungen:

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}).$$

In der Tat sind die angegebenen Teiler unzerlegbar. Es ist nämlich

$$N(2) = 4,\ N(3) = 9,\ N(1 \pm \sqrt{-5}) = 6,$$

so daß eventuell vorhandene nichttriviale Teiler von 2 bzw. von 3 bzw. von $1 \pm \sqrt{-5}$ die Normen 2 oder 3 haben müßten[1]). Solche Elemente $x + y\sqrt{-5}$ gibt es aber nicht, da keine der beiden Gleichungen

$$x^2 + 5y^2 = 2 \quad \text{und} \quad x^2 + 5y^2 = 3$$

eine Lösung in ganzen Zahlen x und y hat.

Ferner sind die in beiden Zerlegungen auftretenden Primelemente nicht paarweise zueinander assoziiert, da in $\Gamma + \Gamma\sqrt{-5}$ nur die beiden Einheiten ± 1 vorliegen (vgl. Aufg. 3 von § 39).

Schließlich zeigen wir, daß die beiden Zerlegungen im wesentlichen, d.h. bis auf assoziierte Faktoren, die einzigen für das Element 6 möglichen sind. Jeder Teiler t von 6 muß ja eine Norm $N(t)$ haben, die in $N(6) = 36$ aufgeht. Es kommen also in Frage

$$N(t) = 1, 2, 3, 4, 6, 9, 12, 18, 36.$$

Dabei liefert $N(t) = 1$ nur Einheiten und demzufolge $N(t) = 36$ nur zu 6 assoziierte Elemente. Elemente t mit $N(t) = 2$ bzw. $N(t) = 3$ treten, wie oben gezeigt, in $\Gamma + \Gamma\sqrt{-5}$ nicht auf, so daß also 6 auch keine Teiler mit der Norm 18 bzw. 12 haben kann.

---

1) Man beachte, daß für $k < 0$ stets $N(\alpha) \geqq 0$ ist.

Die verbleibenden Möglichkeiten treten als Normen

$$N(\pm 2) = 4,\ N(\pm 3) = 9 \quad \text{und}$$

$$N\left(\pm\left(1+\sqrt{-5}\right)\right) = N\left(\pm\left(1-\sqrt{-5}\right)\right) = 6$$

der bereits betrachteten Teiler von 6 auf. Es bleibt nachzuweisen, daß es keine weiteren Teiler von 6 mit diesen Normen gibt. Die Gleichungen

$$x^2 + 5y^2 = 4 \quad \text{und} \quad x^2 + 5y^2 = 6$$

sind aber in der Tat nur mit

$$x = \pm 2,\ y = 0 \quad \text{bzw.} \quad x = \pm 1,\ y = \pm 1$$

lösbar. Damit ist die Frage bereits erledigt, da es wieder zu einem Teiler von 6 mit der Norm 9 einen Komplementärteiler von 6 mit der Norm 4 geben müßte.

c) Nicht immer ergeben sich die erforderlichen Nachweise so einfach wie bisher, wie schon das nun folgende Beispiel des Ringes $\Gamma + \Gamma\sqrt{26}$ zeigt. Dabei beschränken wir uns allerdings darauf, zu zeigen, daß 26 wenigstens die beiden wesentlichen Zerlegungen

$$26 = 2 \cdot 13 = \sqrt{26} \cdot \sqrt{26}$$

besitzt. Dazu betrachten wir wieder die Normen

$$N(2) = 4,\ N(13) = 169,\ N\left(\sqrt{26}\right) = 26.$$

Würden von 2, 13 und $\sqrt{26}$ nichttriviale Teiler t existieren, müßten diese also die Norm ± 2 oder ± 13 haben. Die Gleichungen

$$N(t) = x^2 - 26y^2 = \pm 2 \quad \text{bzw.} \quad N(t) = x^2 - 26y^2 = \pm 13$$

sind aber mit ganzen Zahlen x und y unlösbar, was man durch Betrachtung geschickt gewählter Kongruenzen erkennt:

Aus der Lösbarkeit der Gleichung

$$x^2 - 26y^2 = \pm 2$$

folgt erst recht die Lösbarkeit der Kongruenz

$$x^2 - 26y^2 \equiv \pm 2 \bmod 13,$$

mithin

$$x^2 \equiv \pm 2 \bmod 13.$$

Diese Kongruenz ist aber unlösbar, wie man leicht durchprobiert.

Entsprechend folgert man aus der zweiten Gleichung die Kongruenz

$$x^2 - 26y^2 \equiv \pm 13 \bmod 8,$$

mithin

$$x^2 - 2y^2 \equiv \pm 5 \bmod 8.$$

Zum Nachweis der Unlösbarkeit dieser Kongruenz beachte man, daß x^2 bzw. y^2 mod 8 nur die Werte 0, 1 und 4 annehmen kann. Weiterhin muß x^2 ungerade sein, so daß nur $x^2 \equiv 1$ (8) in Frage kommt. Die Kongruenz

$$1 - 2y^2 \equiv \pm 5 \bmod 8$$

erweist sich aber durch Einsetzen der drei Möglichkeiten für y^2 als unlösbar.

Schließlich ist weder 2 noch 13 assoziiert zu $\sqrt{26}$, da sich nämlich die Normen assoziierter Elemente α und β wegen $\alpha = \varepsilon\beta$, also $N(\alpha) = N(\varepsilon)N(\beta) = \pm N(\beta)$ nur um einen Faktor ± 1 unterscheiden können.

Aufgaben zu § 40

1. Der in B(40.19) geführte Nachweis, daß $\mathfrak{R}[x]$ ein euklidischer Ring ist, verwendet wesentlich die Körpereigenschaft von $\mathfrak{R}$. Unter welcher Einschränkung läßt sich jedoch die Division mit Rest auch in einem Polynomring $\mathfrak{R}[x]$ über einem Ring $\mathfrak{R}$ durchführen?

2. Es sei $\mathfrak{K}$ der Quotientenkörper von $\mathfrak{R}$, $f(x)$ ein beliebiges Polynom aus $\mathfrak{R}[x]$ und $h(x)$ ein solches, dessen höchster Koeffizient eine Einheit von $\mathfrak{R}$ ist. Gilt dann $h(x) \mid f(x)$ in $\mathfrak{K}[x]$, d. h., existiert ein Polynom $q(x) \in \mathfrak{K}[x]$ mit

$$f(x) = h(x) \cdot q(x),$$

so liegt der Quotient $q(x)$ bereits in $\mathfrak{R}[x]$. Man zeige dies unter Verwendung von Aufg. 1.

3. Der Ring der ganzen Gaussschen Zahlen ist ein euklidischer Ring.

Anleitung: Man ordne jedem Element $\alpha = a + bi$ als $g(\alpha)$ seine Norm $N(\alpha) = a^2 + b^2$ zu und beachte, daß $\sqrt{N(\alpha)}$ mit dem gewöhnlichen Betrag der komplexen Zahlen übereinstimmt, der für alle komplexen Zahlen erklärt ist und für den $|\alpha \cdot \beta| = |\alpha| \cdot |\beta|$ gilt. Sind nun α und $\beta \neq 0$ Elemente von $\Gamma + \Gamma i$, so erhält man

$$\alpha = \beta\gamma + \varrho \quad \text{mit} \quad \varrho = 0 \quad \text{oder} \quad N(\varrho) < N(\beta)$$

wie folgt: Man bestimmt zunächst das Element $\gamma' = \alpha\beta^{-1} \in \mathrm{P} + \mathrm{P}i$ und daraus γ, indem man Real- und Imaginärteil von γ' durch die nächstliegenden ganzen Zahlen ersetzt.

Zum Beweis von $N(\varrho) < N(\beta)$ im Falle $\varrho \neq 0$ bediene man sich der Umschreibung:

$$\alpha = \beta\gamma' = \beta\gamma + \beta(\gamma' - \gamma),$$
$$\varrho = \alpha - \beta\gamma = \beta(\gamma' - \gamma).$$

4. Die in diesem Paragraphen stets vorausgesetzte Existenz des Einselementes e ist in einem euklidischen Ring $\mathfrak{R}$ ohnehin erfüllt. (Man verwende, daß sich jedes Ideal $\mathfrak{a}$ von $\mathfrak{R}$ in der Form $\mathfrak{a} = \mathfrak{R}a$ angeben läßt.)

5. In einem euklidischen Ring sind genau die Elemente ε Einheiten, für die $g(\varepsilon) = g(e)$ erfüllt ist.

6. Für assoziierte Elemente a und b aus einem euklidischen Ring gilt $g(a) = g(b)$. Man zeige durch ein Beispiel in $\mathrm{P}[x]$, daß das Umgekehrte nicht in jedem euklidischen Ring richtig ist.

7. Man stelle die folgenden größten gemeinsamen Teiler mit Hilfe des euklidischen Algorithmus als Linearkombinationen in Γ, in $\mathrm{P}[x]$ bzw. in $\Gamma + \Gamma i$ dar:
   a) (144, 89),
   b) $(2x^6 + 3x^5 - 4x^4 - 5x^3 - 2x - 2,\ x^5 - 2x^3 - 1)$,
   c) $(31 - 2i,\ 6 + 8i)$.

8. Es sei $\mathfrak{R}$ ein Integritätsbereich mit Einselement, aber kein Körper. Dann ist $\mathfrak{R}[x]$ kein Hauptidealring. Zum Beweis betrachte man etwa das Ideal (a, x), wobei $a \in \mathfrak{R}$ weder o noch Einheit ist (ein solches Element würde in einem Körper nicht existieren!).

9. Man gebe sämtliche wesentlich verschiedenen Zerlegungen des Elementes 6 im Ringe $\mathfrak{R} = \Gamma + \Gamma\sqrt{-6}$ an.

10. Desgleichen bestimme man sämtliche wesentlich verschiedenen Zerlegungen von 21 im Ringe $\mathfrak{R} = \Gamma + \Gamma\sqrt{-5}$.

§ 41. ZPE-Ringe

Wir wenden uns nunmehr den strukturellen Aussagen zu, die sich aus der Existenz und Eindeutigkeit der Primzerlegung, also aus der Gültigkeit von S(40.1), S(40.2) und S(40.3) für einen Ring $\mathfrak{R}$ ergeben.

Definition **D (41.1)**

Ein Integritätsbereich $\mathfrak{R}$ mit Einselement e heißt ZPE-Ring, wenn für jedes seiner (vom Nullelement und von den Einheiten verschiedenen) Elemente eine (bis auf Reihenfolge und Einheitsfaktoren) eindeutige **Z***erlegung in* ***Prim-E****lemente existiert.*

Beispiele für ZPE-Ringe sind nach den Ergebnissen der vorangegangenen Paragraphen der Ring der ganzen Zahlen, jeder euklidische Ring und allgemeiner jeder Hauptidealring. Es gibt jedoch auch ZPE-Ringe, die nicht Hauptidealringe sind, worauf wir bereits am Ende von B(40.19) hingewiesen haben.

Für die Teilbarkeitslehre in ZPE-Ringen ergeben sich aus der Gültigkeit des Fundamentalsatzes über die Existenz und Eindeutigkeit der Primzerlegung naturgemäß eine Reihe wesentlicher Folgerungen sowie neue strukturelle Gesichtspunkte für die grundlegenden Begriffsbildungen.

Teilbarkeitslehre in ZPE-Ringen

Nach Voraussetzung ist jedes von einer Einheit verschiedene Element $a \neq o$ eines ZPE-Ringes $\mathfrak{R}$ eindeutig (bis auf Reihenfolge und Einheitsfaktoren) als Produkt von Primelementen schreibbar:

$$a \cong p_1 p_2 \cdots p_n .$$

Indem man eventuell auftretende gleiche Primfaktoren zu Potenzen zusammenfaßt, erhält man daraus mit geeigneter Numerierung eine Darstellung von a als Potenzpunkt verschiedener Primelemente:

$$a \cong p_1^{\nu_1} p_2^{\nu_2} \cdots p_r^{\nu_r} .$$

Erklärung **D (41.2)**

Es erweist sich als nützlich, ein solches Potenzprodukt aus endlich vielen Faktoren als *formal-unendliches* Potenzprodukt

$$a \cong \prod_p p^{\alpha_p}$$

zu schreiben. Dieses Potenzprodukt erstreckt sich über ein vollständiges Repräsentantensystem der Klassen aller Primelemente p von $\mathfrak{R}$, denen jeweils ein Exponent α_p zugeordnet ist. Dabei stimmt dieser Exponent α_p für die wirklich in a aufgehenden Repräsentanten $p = p_\varrho$ $(\varrho = 1, \ldots, r)$ mit ν_ϱ überein und ist sonst 0. Fast alle Faktoren des obigen Produktes sind also $p^0 = e$, und das Produkt der nur endlich vielen Faktoren $p_\varrho^{\nu_\varrho} \neq e$ wird als der Wert des „formal-unendlichen" Produktes angesehen.

Beispiele für diese Schreibweise wählen wir aus dem Ring Γ der ganzen Zahlen. Als Repräsentantensystem der Klassen $\{+p, -p\}$ aller Primelemente nehmen wir die Menge aller Primzahlen $\{2, 3, 5, 7, \ldots\}$. Dann ist etwa:

$$140 \cong 2^2 \cdot 5^1 \cdot 7^1 \cong \prod_p p^{\alpha_p} \text{ mit } \alpha_2 = 2, \alpha_3 = 0, \alpha_5 = 1, \alpha_7 = 1, \alpha_{11} = \alpha_{13} = \ldots = 0.$$

$$-825 \cong 3^1 \cdot 5^2 \cdot 11^1 \cong \prod_p p^{\alpha_p} \text{ mit } \alpha_2 = 0, \alpha_3 = 1, \alpha_5 = 2, \alpha_7 = 0, \alpha_{11} = 1, \alpha_{13} = \alpha_{17} = \ldots = 0.$$

Eventuelle anfängliche Schwierigkeiten mit dieser abstrakten Schreibweise werden bei weitem durch ihre Vorteile aufgewogen, die sich im folgenden herausstellen. Die Tragweite der neuen Auffassung beruht auf dem

Satz **S (41.3)**

Jedes von einer Einheit verschiedene Element $a \neq o$ bzw. jedes zu a assoziierte Element aus $\mathfrak{R}$ bestimmt eindeutig ein ganzzahliges Exponentensystem α_p mit

$$\alpha_p \geqq 0 \text{ für alle } p,$$
$$\text{fast alle } \alpha_p = 0,$$
$$\text{wenigstens ein } \alpha_p > 0;$$

umgekehrt bestimmt jedes Exponentensystem dieser Art eindeutig eine Klasse assoziierter (vom Nullelement und den Einheiten verschiedener) Elemente von $\mathfrak{R}$.

Ergänzung

Das gleiche gilt für die Klasse der Einheiten von $\mathfrak{R}$ mit dem Exponentensystem $\alpha_p = 0$ für alle p:

$$e \cong \prod_p p^0.$$

Der erste Teil der Behauptung stellt nur eine neue Formulierung des Fundamentalsatzes dar, während die Umkehrung sofort klar ist. Die Ergänzung entspricht unmittelbar der nach der obigen Einführung formal-unendlicher Produkte sinnvollen Setzung $\prod_p p^0 = e$.

Folgerung **F (41.4)**

Die Multiplikation von Elementen aus $\mathfrak{R}$ entspricht der komponentenweisen Addition ihrer Exponentensysteme:

$$a \cdot b \cong \left(\prod_p p^{\alpha_p}\right)\left(\prod_p p^{\beta_p}\right) \cong \prod_p p^{\alpha_p + \beta_p}.$$

Diese Aussage entspricht der üblichen Potenzrechnung, da ja nur endlich viele Faktoren wirklich auftreten. So ist etwa

$$140 \cdot (-825) \cong 2^2 \cdot 3^1 \cdot 5^3 \cdot 7^1 \cdot 11^1 \cong \Pi p^{\alpha_p + \beta_p}$$

mit $\alpha_2 + \beta_2 = 2 + 0 = 2$ $\quad \alpha_7 + \beta_7 = 1 + 0 = 1$

$\alpha_3 + \beta_3 = 0 + 1 = 1$ $\quad \alpha_{11} + \beta_{11} = 0 + 1 = 1$

$\alpha_5 + \beta_5 = 1 + 2 = 3$ $\quad \alpha_p + \beta_p = 0 + 0 = 0$ für alle $p > 11$.

F (41.4) ist ein deutliches Beispiel, wie vorteilhaft die Einführung der formal-unendlichen Produktbildung ist. Während sich zwar in jedem konkreten Falle endliche Potenzprodukte von Primelementen ohne weiteres multiplizieren lassen, müßte man bei allgemeinen Untersuchungen zur Vereinfachung des Produktes $(p_1^{\nu_1} p_2^{\nu_2} \dots p_r^{\nu_r})(q_1^{\mu_1} q_2^{\mu_2} \dots q_s^{\mu_s})$ Fallunterscheidungen der Art $p_i = q_j$ oder $p_i \neq q_j$ heranziehen. Eine Umgehung dieser Fallunterscheidung durch Hinzufügen der nur in einem Faktor auftretenden Primelemente mit den Exponenten 0 zum anderen Faktor ist aber bereits ein Ansatz der Auffassung als formal-unendliches Produkt.

Ferner erhält man ohne weiteres folgendes

Teilbarkeitskriterium **S (41.5)**

Für zwei Elemente $a \cong \prod_p p^{\alpha_p}$, $b \cong \prod_p p^{\beta_p}$ gilt

$$b \mid a \text{ genau dann, wenn } \beta_p \leqq \alpha_p \text{ für alle } p.$$

Dabei ist der Komplementärteiler x aus $a = bx$ gegeben durch

$$x \cong \prod_p p^{\alpha_p - \beta_p}.$$

Insbesondere ist $\alpha_p > 0$ hinreichend und notwendig für $p \mid a$.

Aus F (41.4) oder auch aus S (41.5) entnimmt man, daß sich das bisher ausgeschlossene Nullelement von $\mathfrak{R}$ durch eine auf den ersten Blick eigenartig anmutende Setzung in die Teilbarkeitsbetrachtungen einordnen läßt. Bedenkt man nämlich, daß die

multiplikativen Eigenschaften des Nullelementes o vollständig durch

$a \cdot o = o$ für alle $a \in \mathfrak{R}$ oder auch durch

$a \mid o$ für alle $a \in \mathfrak{R}$ und $o \mid a$ nur für $a = o$

gekennzeichnet sind, so rechtfertigt sich die formale

Festlegung **D (41.6)**

Dem Nullelement $o \in \mathfrak{R}$ wird das Exponentensystem $\alpha_p = \infty$ für alle p zugeordnet:

$$o = \prod_p p^{\infty}.$$

Nach dieser neuen Formulierung der allgemeinen Grundlagen der Teilbarkeitslehre wenden wir uns der Behandlung des größten gemeinsamen Teilers und des kleinsten gemeinsamen Vielfachen zu, die sich ebenfalls unter Zugrundelegung des Fundamentalsatzes recht übersichtlich durchführen läßt.

Satz **S (41.7)**

Für beliebige Elemente $a = \prod_p p^{\alpha_p}$, $b = \prod_p p^{\beta_p}, \ldots$ aus $\mathfrak{R}$ existiert stets ein größter gemeinsamer Teiler und ein kleinstes gemeinsames Vielfaches, und es gilt:

a) $d \cong (a, b, \ldots) \cong \prod_p p^{\delta_p}$ mit $\delta_p = Min\ (\alpha_p, \beta_p, \ldots)$,

b) $f \cong [a, b, \ldots] \cong \prod_p p^{\varphi_p}$ mit $\varphi_p = Max\ (\alpha_p, \beta_p, \ldots)$.

Beweis

a) Wegen $\delta_p \leqq \alpha_p$, $\delta_p \leqq \beta_p, \ldots$ für alle p ist $\prod_p p^{\delta_p}$ nach S(41.5) gemeinsamer Teiler von $a, b, \ldots$. Für jeden anderen gemeinsamen Teiler $t = \prod_p p^{\tau_p}$ gilt aber ebenfalls nach S(41.5) $\tau_p \leqq \alpha_p$, $\tau_p \leqq \beta_p, \ldots$, also auch $\tau_p \leqq \delta_p$ für alle p, d. h. jedoch $t \mid \prod_p p^{\delta_p}$. Also ist $\prod_p p^{\delta_p}$ nach D(39.8) und F(39.9) assoziiert zu $d \cong (a, b, \ldots)$.

b) Hier schließt man analog.

qed.

Diese für ZPE-Ringe mögliche Kennzeichnung des größten gemeinsamen Teilers und des kleinsten gemeinsamen Vielfachen erweist sich als wesentlich vorteilhafter als die in § 39 gegebenen Definitionen, zumal die dort geforderten Eigenschaften, wie der eben geführte Beweis zeigt, auf Grund des Teilbarkeitskriteriums S(41.5) wieder unmittelbar zum Ausdruck kommen. Sie gewährleistet nämlich nicht nur die Existenz und die Eindeutigkeit (bis auf Einheiten) des größten gemeinsamen Teilers und des kleinsten gemeinsamen Vielfachen, sondern gestattet sogar ihre tatsächliche Angabe, wenn man nur die Primzerlegung der beteiligten Elemente kennt. Auch die Unabhängigkeit gegenüber Zusammenfassungen wie $((a, b), c), \ldots)$ oder $[a, [b, c], \ldots]$ usw. (vgl. Aufg. 6 von § 39) ist jetzt eine unmittelbare Folge der entsprechenden Eigenschaften der Minimums- und Maximumsbildung. Darüber hinaus ergeben sich sehr leicht weitere diesbezügliche Aussagen:

Folgerung **F (41.8)**

Größter gemeinsamer Teiler und kleinstes gemeinsames Vielfaches sind homogene Bildungen:

$$(ta, tb, \ldots) \cong t(a, b, \ldots),$$
$$[ta, tb, \ldots] \cong t[a, b, \ldots].$$

Beweis

$$\text{Min } (\tau_p + \alpha_p, \tau_p + \beta_p, \ldots) = \tau_p + \text{Min } (\alpha_p, \beta_p, \ldots),$$
$$\text{Max } (\tau_p + \alpha_p, \tau_p + \beta_p, \ldots) = \tau_p + \text{Max } (\alpha_p, \beta_p, \ldots).$$

qed.

Folgerung **F (41.9)**

Ist $d \cong (a, b, \ldots)$, also $a = da_0$, $b = db_0, \ldots$, so sind die Komplementärteiler a_0, $b_0, \ldots$ zueinander teilerfremd:

$$(a_0, b_0, \ldots) \cong e.$$

Beweis

$$d \cong (a, b, \ldots) \cong (da_0, db_0, \ldots) \cong d(a_0, b_0, \ldots)$$

qed.

Folgerung **F (41.10)**

Für eine Einheit ε und das Nullelement o aus $\mathfrak{R}$ gilt:

$$(\varepsilon, a, b, \ldots) \cong e, \quad (o, a, b, \ldots) \cong (a, b, \ldots);$$
$$[o, a, b, \ldots] = o, \quad [\varepsilon, a, b, \ldots] \cong [a, b, \ldots].$$

Beweis

$$\text{Min}\ (0, \alpha_p, \beta_p, \ldots) = 0, \quad \text{Min}\,(\infty, \alpha_p, \beta_p, \ldots) = \text{Min}\ (\alpha_p, \beta_p, \ldots);$$
$$\text{Max}\,(\infty, \alpha_p, \beta_p, \ldots) = \infty, \quad \text{Max}\,(0, \alpha_p, \beta_p, \ldots) = \text{Max}\ (\alpha_p, \beta_p, \ldots).$$

qed.

Folgerung **F (41.11)**

Es sei z das Produkt der Ringelemente $a, b, \ldots, r$, und $a', b', \ldots, r'$ seien die aus z durch Streichen des Faktors a bzw. $b \ldots$ bzw. r entstehenden Elemente. Dann erhält man folgenden Zusammenhang zwischen dem größten gemeinsamen Teiler und dem kleinsten gemeinsamen Vielfachen:

$$(a, b, \ldots, r)\,[a', b', \ldots, r'] \cong [a, b, \ldots, r]\,(a', b', \ldots, r') \cong z.$$

Daraus ergibt sich insbesondere für zwei Ringelemente a und b:

$$(a, b)\,[a, b] \cong ab.$$

Beweis

$$\text{Min}\,(\alpha_p, \beta_p, \ldots, \varrho_p)$$
$$+ \text{Max}\,(0 + \beta_p + \ldots + \varrho_p, \alpha_p + 0 + \ldots + \varrho_p, \ldots, \alpha_p + \beta_p + \ldots + 0)$$
$$= \alpha_p + \beta_p + \ldots + \varrho_p,$$

denn ist etwa γ_p das gesuchte Minimum, so wird diejenige Summe $\alpha_p + \beta_p + \ldots + \varrho_p$, in der γ_p fehlt, das gesuchte Maximum. Der Beweis der zweiten Beziehung ergibt sich unter Vertauschung von Minimum und Maximum. qed.

Die bisherigen Ausführungen zeigen wohl deutlich, wie vorteilhaft ein Aufbau der Teilbarkeitslehre auf dem Fundamentalsatz ist. Auch die nachstehenden Überlegungen über die damit möglichen Einsichten in die Struktur des Quotientenkörpers werden dies unterstreichen. Man wird daher bei der Behandlung der Teilbarkeitslehre eines Ringes bestrebt sein, möglichst rasch zum Beweis des Fundamentalsatzes zu gelangen, um dann in den hier dargelegten

Weg einzubiegen. Selbstverständlich müssen dabei die schon zur Formulierung des Fundamentalsatzes notwendigen Begriffe wie Teiler, Einheit und Primelement stets vorweggenommen werden, sowie in jedem konkreten Falle die jeweils zu seinem Beweis benötigten Teilbarkeitsaussagen. Dies kann unter Umständen verhältnismäßig viel sein, wie unsere Untersuchungen für euklidische Ringe und Hauptidealringe im vorigen Paragraphen zeigen; manchmal ist es aber auch möglich, nahezu mit den schon zur Formulierung benötigten Begriffen auszukommen, wie etwa der Beweis von ZERMELO gerade für den wichtigen Fall des Ringes der ganzen Zahlen lehrt.

In dieser Hinsicht wirkt sich im Schulunterricht der notwendige Verzicht auf den Beweis des Fundamentalsatzes methodisch günstig aus, da dadurch jedes Vorgreifen vermieden wird und die gesamte Teilbarkeitslehre (natürlicher bzw. ganzer und rationaler Zahlen) konsequent auf dem Fundamentalsatz aufgebaut werden kann. Der Leser wird auch bestätigen, daß die Ausführungen dieses Paragraphen — gelesen als Aussagen über Zahlen und selbstverständlich der hier angestrebten abstrakt-eleganten Formulierung und Allgemeinheit entkleidet — genau den im Schulunterricht vorzunehmenden Überlegungen entsprechen, so z. B. die Einführung des größten gemeinsamen Teilers und des kleinsten gemeinsamen Vielfachen sowie die unten zu besprechende Hauptnennerdarstellung.

Freilich müssen wir auch nochmals auf den Nachteil dieser Sachlage hinweisen. In der ständigen Gewöhnung, bei allen Überlegungen sich auf den „selbstverständlich gültigen" Fundamentalsatz zu stützen, liegt die Gefahr, bei einer Nachholung seines Beweises sich auf Aussagen zu beziehen, die man schon gar nicht mehr als Folgerungen dieses Satzes erkennt. In dieser Art sind einem etwa die Aussagen von S (40.12) und F (40.13) als Folgerungen aus dem Fundamentalsatz selbstverständlich, während sie jedoch, wenn sie zu seinem Beweis verwendet werden sollen, zuvor unabhängig von ihm nachzuweisen sind.

Ausdehnung auf den Quotientenkörper

Reduzierte Quotientendarstellung S (41.12)

Jedes Element $a \neq o$ des Quotientenkörpers $\mathfrak{K}$ eines ZPE-Ringes $\mathfrak{R}$ ist bis auf Einheiten eindeutig als „gekürzter" Quotient von Elementen m und n aus $\mathfrak{R}$ darstellbar:

$$a = \frac{m}{n} \quad mit \quad (m, n) \cong e.$$

Jede andere Darstellung von a entsteht daraus durch „Erweitern" d. h. durch Multiplikation von m und n mit einem beliebigen, von o verschiedenen Ringelement.

Beweis

Nach Definition des Quotientenkörpers $\mathfrak{K}$ von $\mathfrak{R}$ gibt es wenigstens eine Darstellung

$$a = \frac{r}{s} \quad \text{mit} \quad r \in \mathfrak{R},\ s \in \mathfrak{R}.$$

Es sei $d \cong (r, s)$, also $r = dr_0$, $s = ds_0$ und nach F (41.9) $(r_0, s_0) \cong e$. Daraus folgt bereits, daß jede Quotientendarstellung von a durch Kürzen in eine reduzierte Quotientendarstellung übergeführt werden kann, aus der sie dann durch Erweitern entsteht.

Es bleibt zu zeigen, daß für ein Element $a \in \mathfrak{K}$ bis auf Einheiten nur eine reduzierte Quotientendarstellung möglich ist. Aus

$$a = \frac{m}{n} = \frac{m'}{n'} \quad \text{mit} \quad (m, n) \cong (m', n') \cong e$$

folgt aber über $mn' = nm'$

$$\text{einerseits } n' \mid nm' \text{ und damit } n' \mid n,$$

$$\text{andererseits } n \mid mn' \text{ und damit } n \mid n'.$$

Daher ist $n \cong n'$ und mithin $m \cong m'$. qed.

Hauptnennerdarstellung **S (41.13)**

Endlich viele Elemente $a_1, a_2, \ldots, a_k$ des Quotientenkörpers $\mathfrak{K}$ von $\mathfrak{R}$, von denen wenigstens ein $a_i \neq o$ ist, sind bis auf Einheiten eindeutig als Quotienten von Ringelementen in der Form

$$a_1 = \frac{z_1}{n},\ a_2 = \frac{z_2}{n}, \ldots,\ a_k = \frac{z_k}{n} \quad \textit{mit} \quad (z_1, z_2, \ldots, z_k, n) \cong e$$

darstellbar. Dabei ist der „Hauptnenner" das kleinste gemeinsame Vielfache $n \cong [n_1, n_2, \ldots, n_k]$ der Nenner in den reduzierten Bruchdarstellungen von $a_1, a_2, \ldots, a_k$.

Jede andere Darstellung von $a_1, a_2, \ldots, a_k$ mit einem gemeinsamen Nenner entsteht aus dieser Hauptnennerdarstellung durch Erweitern.

Beweis

Aus den reduzierten Bruchdarstellungen

$$a_1 = \frac{m_1}{n_1},\ a_2 = \frac{m_2}{n_2}, \ldots,\ a_k = \frac{m_k}{n_k}$$

erhält man unter Verwendung des kleinsten gemeinsamen Vielfachen $n \cong [n_1, n_2, \ldots, n_k]$ eine Darstellung der verlangten Art:

$$a_1 = \frac{a_1 n}{n} = \frac{z_1}{n}, \ldots, a_k = \frac{a_k n}{n} = \frac{z_k}{n}.$$

Wäre nämlich $d \cong (z_1, z_2, \ldots, z_k, n)$ keine Einheit, so könnte man alle Quotienten dieser Darstellung mit d kürzen und würde so eine neue Darstellung mit dem gemeinsamen Nenner n_0 aus $n = dn_0$ erhalten, wobei also $n_0 \mid n$, aber $n \nmid n_0$ gilt. Dies ist aber bereits ein Widerspruch, denn aus S(41.12) folgt andererseits, daß jeder gemeinsame Nenner von $a_1, a_2, \ldots, a_k$ (also insbesondere n_0) gemeinsames Vielfaches der Nenner $n_1, n_2, \ldots, n_k$ ist und damit ein Vielfaches des kleinsten gemeinsamen Vielfachen n.

Diese Darstellung ist nun durch die Bedingung $(z_1, \ldots, z_k, n) = e$ bis auf Einheiten eindeutig festgelegt. Gilt nämlich

$$a_1 = \frac{r_1}{s}, \ldots, a_k = \frac{r_k}{s} \quad \text{mit} \quad (r_1, \ldots, r_k, s) \cong e,$$

so ist jedenfalls s (nach den gleichen Schlüssen wie eben) Vielfaches von n. Aus $s = nt$ folgt aber durch Vergleich beider Darstellungen auch $r_i = z_i t$ wegen $r_i n = z_i s = z_i nt$, und man erhält aus

$$e \cong (r_1, \ldots, r_k, s) \cong (z_1 t, \ldots, z_k t, nt) \cong t(z_1, \ldots, z_k, n)$$

$t \cong e$, also $s \cong n$ und $r_i \cong z_i$.

Jede andere Darstellung

$$a_1 = \frac{z_1'}{n'}, \; a_2 = \frac{z_2'}{n'}, \ldots, a_k = \frac{z_k'}{n'}$$

mit einem von einer Einheit verschiedenen größten gemeinsamen Teiler $(z_1', z_2', \ldots, z_k', n')$ läßt sich mit diesem zur Hauptnennerdarstellung kürzen, entsteht also aus der letzteren durch Erweitern. qed.

Für den Spezialfall $\mathfrak{R} = \Gamma$ und $\mathfrak{R} = \mathrm{P}$ kann man zwar durch positive Normierung der Nenner von Äquivalenzen zu Gleichheiten übergehen und ferner durch Verwendung der in Γ und P gegebenen Anordnung (vgl. die Bemerkungen nach F (39.11)) die Schlüsse anschaulicher machen, jedoch bleiben die vorzunehmenden Überlegungen von diesen darstellungsmäßigen (und auch methodisch sehr wertvollen) Vereinfachungen inhaltlich unberührt. Es ist klar, daß die Sätze S (41.12) und S (41.13) der Behandlung der Bruchrechnung im Schulunterricht unausgesprochen zugrunde liegen, ohne daß sie selbst ihres abstrakten Inhaltes wegen (zumindest was die Eindeutigkeitsaussagen an betrifft) auf der entsprechenden Altersstufe angegeben werden können.

Abschließend gehen wir kurz auf die Möglichkeit ein, die gesamte Teilbarkeitslehre auf die Elemente des Quotientenkörpers $\mathfrak{K}$ von $\mathfrak{R}$ auszudehnen. Ausgangspunkt dafür ist (vgl. S(41.3)) die folgende

Verallgemeinerung des Fundamentalsatzes **S (41.14)**

Jedes Element $a \neq o$ des Quotientenkörpers $\mathfrak{K}$ von $\mathfrak{R}$ ist eindeutig als formal-unendliches Potenzprodukt

$$a = \frac{m}{n} \cong \frac{\prod\limits_p p^{\mu_p}}{\prod\limits_p p^{\nu_p}} \cong \prod_p p^{\alpha_p}$$

schreibbar, d.h., jedem Element $a \neq o$ aus $\mathfrak{K}$ bzw. den zu ihm assoziierten Elementen[1]*) wird eineindeutig ein ganzzahliges Exponentensystem α_p zugeordnet mit*

$$\alpha_p \gtrless 0 \text{ für alle } p,$$

$$\text{fast alle } \alpha_p = 0.$$

Ist dabei $(m, n) \cong e$, so gilt $\alpha_p = \mu_p$ für $\mu_p \neq 0$, $\alpha_p = -\nu_p$ für $\nu_p \neq 0$ und $\alpha_p = 0$ sonst.

Insbesondere ordnet sich das Nullelement o wieder ein mit dem Exponentensystem $\alpha_p = \infty$ für alle p.

Wie man sich leicht überzeugt, gilt nach dieser Ausdehnung ganz allgemein

$$a \cdot b \cong \left(\prod_p p^{\alpha_p}\right)\left(\prod_p p^{\beta_p}\right) \cong \prod_p p^{\alpha_p + \beta_p}.$$

$$\frac{a}{b} \cong \frac{\prod\limits_p p^{\alpha_p}}{\prod\limits_p p^{\beta_p}} \cong \prod_p p^{\alpha_p - \beta_p}.$$

---

1) In dieser Darstellung der Elemente von $\mathfrak{K}$ vernachlässigen wir (nämlich beim Übergang von m und n zu den entsprechenden formal-unendlichen Potenzprodukten) Faktoren, die Einheiten aus $\mathfrak{R}$ sind. Auch Elemente von $\mathfrak{K}$, die sich nur um einen solchen Faktor unterscheiden, nennen wir zueinander assoziiert und verwenden das Zeichen $\cong$. Dies ist offensichtlich eine Äquivalenzrelation für die Elemente von $\mathfrak{K}$, die für die Elemente von $\mathfrak{R}$ mit der in D(39.5) erklärten Äquivalenzrelation übereinstimmt.
Diese Ausdehnung der Beziehung $\cong$ auf alle Elemente von $\mathfrak{K}$ macht sie sogar strukturell durchsichtiger, da die Klassen assoziierter Elemente damit zu den Nebenklassen werden, aus denen die Zerlegung der multiplikativen Gruppe von $\mathfrak{K}$ nach der multiplikativen Gruppe der Einheiten von $\mathfrak{R}$ besteht.

Nennt man in Analogie zum Sprachgebrauch im Falle Γ und P ein Element $a \in \mathfrak{R}$ ein *ganzes Element von* $\mathfrak{R}$, so erhält man das

Ganzheitskriterium **S (41.15)**

Ein Element a aus $\mathfrak{R}$ ist dann und nur dann ganz, wenn gilt:

$$a \cong \prod_p p^{\alpha_p} \quad \text{mit} \quad \alpha_p \geqq 0 \text{ für alle } p.$$

In einem Körper $\mathfrak{K}$ ist der in D(39.1) erklärte Teilbarkeitsbegriff unfruchtbar, da ja (abgesehen von der Sonderrolle des Nullelementes) in diesem Sinne in $\mathfrak{K}$ jedes Element durch jedes Element teilbar ist. Dagegen kann man für die Elemente von $\mathfrak{K}$ eine sinnvolle Teilbarkeitsrelation einführen, wenn man zuvor die Elemente irgendeines Ringes $\mathfrak{R} \subset \mathfrak{K}$, dessen Quotientenkörper mit $\mathfrak{K}$ zusammenfällt, als ganze Elemente von $\mathfrak{K}$ auszeichnet:

Definition **D (41.16)**

Ein Element $b \in \mathfrak{K}$ heißt Teiler eines Elementes $a \in \mathfrak{K}$, wenn es ein ganzes Element x (also ein Element $x \in \mathfrak{R}$) gibt, so daß $a = bx$ gilt, also:

$$b \mid a \text{ genau für } a = bx \text{ mit ganzem } x^1).$$

So ist z.B. in P bezüglich Γ

$$\frac{5}{22} \mid \frac{35}{2} \quad \text{wegen} \quad \frac{35}{2} = \frac{5}{22} \cdot 77, \text{ aber}$$

$$\frac{30}{7} \nmid \frac{75}{14}, \quad \text{da} \quad \frac{75}{14} = \frac{30}{7} \cdot x \text{ nicht ganzzahlig lösbar ist.}$$

Ist nun, wie wir jetzt wieder voraussetzen, $\mathfrak{R}$ ein ZPE-Ring mit dem Quotientenkörper $\mathfrak{K}$, so erhalten wir in Verallgemeinerung von S(41.5) für die eben definierte Teilbarkeit das

Teilbarkeitskriterium **S (41.17)**

Für zwei Elemente $a \cong \prod_p p^{\alpha_p}$, $b \cong \prod_p p^{\beta_p}$ gilt

$$b \mid a \text{ genau dann, wenn } \beta_p \leqq \alpha_p \text{ für alle } p.$$

Dabei ist der Komplementärteiler $x \in \mathfrak{R}$ aus $a = bx$ gegeben durch

$$x \cong \prod_p p^{\alpha_p - \beta_p}.$$

---

1) Offenbar ist diese Definition eine sinnvolle Verallgemeinerung von D(39.1), da sie für den Fall, daß a und b sogar in $\mathfrak{R}$ liegen, mit ihr übereinstimmt.

So ist in dem erstgenannten Beispiel

$$\begin{array}{rcl} \beta_2 = -1 & \leqq & -1 = \alpha_2 \\ \beta_5 = +1 & \leqq & +1 = \alpha_5 \\ \beta_7 = \ \ 0 & \leqq & +1 = \alpha_7 \\ \beta_{11} = -1 & \leqq & \ \ 0 = \alpha_{11} \end{array} \quad \text{und damit } x \cong \prod_p p^{\alpha_p - \beta_p} \text{ mit } \begin{array}{l} \alpha_2 - \beta_2 = 0 \\ \alpha_5 - \beta_5 = 0 \\ \alpha_7 - \beta_7 = 1 \\ \alpha_{11} - \beta_{11} = 1 \end{array}$$

Dagegen ist im zweiten Falle $1 = \beta_2 \geqq \alpha_1 = -1$, woraus bereits $b \nmid a$ folgt.

Auch die Aussagen dieser erweiterten Teilbarkeitsbeziehung in $\mathfrak{R}$ sind wieder invariant gegenüber Multiplikation der in ihnen auftretenden Elemente mit Einheiten des zugrunde gelegten Ringes $\mathfrak{R}$. Auf einen Ausbau der Teilbarkeitslehre in Quotientenkörpern von ZPE-Ringen wollen wir jedoch verzichten, obgleich sich durch diese abstraktere Betrachtungsweise manches vereinfachen und zusammenfassen läßt. Übrigens verlaufen die meisten Überlegungen formal wie bei Ringen, da ja im wesentlichen alles auf die Anordnung der Exponenten α_p zurückgespielt wird, die sich durch Zulassung negativer Werte nicht ändert.

Vielmehr wollen wir uns noch einigen spezielleren Fragestellungen zuwenden, die sich an die bisher behandelte Teilbarkeitslehre anschließen lassen. Allerdings sind zu ihrer Beantwortung im allgemeinen über die Gültigkeit des Fundamentalsatzes hinausgehende Voraussetzungen erforderlich, nämlich daß der betrachtete Ring Hauptidealring oder sogar euklidischer Ring ist. Solche Probleme sind etwa die Auflösung diophantischer Gleichungen und linearer Kongruenzen sowie die Zerlegung von Elementen des Quotientenkörpers in eine Summe von Partialbrüchen bzw. ihre Entwicklung in einen Kettenbruch.

Diophantische Gleichungen und lineare Kongruenzen

Die Beziehung $a \mid b$ kann man etwa als Kriterium dafür betrachten, daß in $\mathfrak{R}$ die lineare Gleichung $ax = b$ mit einem Element $x \in \mathfrak{R}$ lösbar ist.

In Verallgemeinerung dessen untersuchen wir lineare Gleichungen in mehreren Unbekannten

$$a_1 x_1 + a_2 x_2 + \ldots + a_n x_n = b$$

mit den Koeffizienten $a_1, a_2, \ldots, a_n, b$ aus $\mathfrak{R}$, die in $\mathfrak{R}$ gelöst werden sollen. Dem dabei besonders wichtigen Fall $\mathfrak{R} = \Gamma$ entlehnen wir für solche Gleichungen auch die Bezeichnung *diophantische Gleichungen*[1]).

Satz **S (41.18)**

In einem Hauptidealring $\mathfrak{R}$ ist die diophantische Gleichung

$$a_1 x_1 + a_2 x_2 + \ldots + a_n x_n = b$$

dann und nur dann lösbar, wenn der größte gemeinsame Teiler $d \cong (a_1, a_2, \ldots, a_n)$ in b aufgeht.

Ist $\mathfrak{R}$ ein euklidischer Ring, so ist wenigstens eine Lösung $x_1, x_2, \ldots, x_n$ im Falle der Lösbarkeit konstruktiv angebbar.

Beweis

Die Bedingung ist in jedem ZPE-Ring notwendig, denn in einem solchen Ring existiert der größte gemeinsame Teiler d, und aus $d \mid a_i$, also $d \mid a_i x_i$ für $i = 1, \ldots, n$ folgt $d \mid b$.

Ist umgekehrt $\mathfrak{R}$ ein Hauptidealring und in ihm die genannte diophantische Gleichung vorgelegt, so existiert wegen der Gültigkeit des Hauptsatzes über den größten gemeinsamen Teiler für $d \cong (a_1, a_2, \ldots, a_n)$ eine Linearkombination

$$a_1 c_1 + a_2 c_2 + \ldots + a_n c_n = d,$$

wobei $c_1, c_2, \ldots, c_n$ Elemente aus $\mathfrak{R}$ sind. Nun gilt nach Voraussetzung $b = d b_0$ mit $b_0 \in \mathfrak{R}$, also ist

$$x_1 = c_1 b_0, \quad x_2 = c_2 b_0, \ldots, \quad x_n = c_n b_0$$

eine Lösung der verlangten Art.

Handelt es sich insbesondere um einen euklidischen Ring $\mathfrak{R}$, so kann man eine Linearkombination des größten gemeinsamen Teilers durch sukzessive Verwendung des euklidischen Algorithmus konstruktiv herstellen. qed.

---

1) DIOPHANTOS von Alexandria, um 250 n. Chr., untersuchte jedoch keine „Diophantischen Gleichungen" im Sinne des heutigen Sprachgebrauches, sondern rationalzahlige Lösungen quadratischer Gleichungen.

Folgerung **F (41.19)**

Jede Lösung $x_1, x_2, \ldots, x_n$ *der diophantischen Gleichung*

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = b$$

ist auch Lösung der durch $d \cong (a_1, a_2, \ldots, a_n)$ *„gekürzten" diophantischen Gleichung*

$$a'_1x_1 + a'_2x_2 + \ldots + a'_nx_n = b'$$

und umgekehrt, wobei also gilt:

$$a_1 = da'_1,\ a_2 = da'_2,\ \ldots,\ a_n = da'_n,\ b = db' \text{ und } (a'_1, a'_2, \ldots, a'_n) \cong e.$$

Als Beispiel lösen wir in $\mathfrak{R} = \Gamma$ die diophantische Gleichung

$$45x_1 + 30x_2 + 18x_3 = 6.$$

Wie man unmittelbar sieht (in komplizierteren Fällen wird man sich zur Berechnung von d der Primzerlegung oder des euklidischen Algorithmus bedienen), ist $d = (45, 30, 18) = 3$, also die diophantische Gleichung lösbar. Zweckmäßigerweise löst man die „gekürzte" Gleichung

$$15x_1 + 10x_2 + 6x_2 = 2.$$

Nun bietet sich als eine Linearkombination für $1 = (15, 10, 6)$ sofort an

$$15 \cdot (-1) + 10 \cdot 1 + 6 \cdot 1 = 1,$$

woraus man eine Lösung der diophantischen Gleichung erhält:

$$x_1 = -2,\ x_2 = 2,\ x_3 = 2.$$

Auch bei den folgenden Überlegungen muß der Leser vor allem an den ohnehin wichtigsten Fall $\mathfrak{R} = \Gamma$ denken. Unsere für Hauptidealringe bzw. euklidische Ringe durchgeführten Betrachtungen zeigen jedoch, ohne die Beweisführung irgendwie zu erschweren, welche dieser Eigenschaften jeweils auch den für Γ spezialisierten Aussagen wesentlich zugrunde liegen.

Um nun die Frage nach der Gesamtheit aller Lösungen anzugreifen, beschränken wir uns zunächst auf Gleichungen mit zwei Unbekannten, die in einem engen Zusammenhang mit linearen Kongruenzen[1]) stehen. Man erkennt nämlich unmittelbar:

---

1) Wir erinnern daran, daß allgemein die Restklassenbildung mod m als solche modulo dem Hauptideal $\mathfrak{m} = (m)$ aufzufassen ist.

Satz **S (41.20)**

Jede Lösung x der linearen Kongruenz

$$ax \equiv b \bmod m$$

entspricht einer Lösung x, y der korrespondierenden diophantischen Gleichung

$$ax + my = b$$

und umgekehrt.

Dieser Satz gestattet nun, einerseits die Existenzaussagen aus S(41.18) sowie F(41.19) auf lineare Kongruenzen zu übertragen und andererseits die für solche Kongruenzen leichter übersehbare allgemeine Lösung für diophantische Gleichungen auszunützen.

Satz **S (41.21)**

In einem Hauptidealring $\mathfrak{R}$ ist die lineare Kongruenz

$$ax \equiv b \bmod m$$

genau dann lösbar, wenn der größte gemeinsame Teiler $d \cong (a, m)$ in b aufgeht.

Ist $\mathfrak{R}$ sogar euklidischer Ring, so ist im Falle der Lösbarkeit wenigstens eine Lösung x konstruktiv herstellbar.

Folgerung **F (41.22)**

Jede Lösung x der linearen Kongruenz

$$ax \equiv b \bmod m$$

ist auch Lösung der durch $d \cong (a, m)$ „gekürzten" linearen Kongruenz

$$a'x \equiv b' \bmod m'$$

und umgekehrt[1]*, wobei also gilt:*

$$a = da',\ m = dm',\ b = db' \quad \text{und} \quad (a', m') \cong e.$$

Man beachte, daß sich das „Kürzen" einer linearen Kongruenz strenggenommen auf die zugehörige diophantische Gleichung bezieht und damit der Modul ebenfalls verändert wird. Übrigens entspricht dieses Kürzen auch der folgenden allgemeinen Aussage über die „Division" von Kongruenzen, die sich leicht aus der Definition der Kongruenz ergibt:

$$rt \equiv st(m) \text{ ist gleichwertig mit } r \equiv s\left(\frac{m}{(m, t)}\right),$$

1) Gerade diese „gekürzten" linearen Kongruenzen waren für $\mathfrak{R} = \Gamma$ in Aufgabe 4 von § 33 vollständig behandelt worden; insbesondere lehrt F(41.22), wie die dort angekündigte Zurückführung des allgemeinen Falles auf den Fall $(a, m) = 1$ vorzunehmen ist.

So ist etwa in $\mathfrak{R} = \Gamma$ die lineare Kongruenz

$$15x \equiv 6 \bmod 21$$

lösbar, da $(15, 21) = 3$ in 6 aufgeht. Wir gehen wieder zur „gekürzten" Kongruenz

$$5x \equiv 2 \bmod 7$$

über. Für die korrespondierende diophantische Gleichung

$$5x + 7y = 2$$

erhält man aber aus der Linearkombination

$$5 \cdot 3 + 7\,(-2) = 1$$

$x = 6$, $y = -4$ als Lösung, also löst $x = 6$ die vorgegebene Kongruenz.

Der Vollständigkeit halber wollen wir bemerken, daß man auch umgekehrt konkrete Lösungen einer diophantischen Gleichung

$$a_1 x + a_2 y = b$$

in zwei Unbekannten mit Hilfe einer der beiden „korrespondierenden" linearen Kongruenzen $a_1 x \equiv b\,(a_2)$ bzw. $a_2 y \equiv b\,(a_1)$

erhalten kann, falls man diese auf andere Weise zu lösen vermag. Gerade im Falle $\mathfrak{R} = \Gamma$ ist dies immer und oft mit viel weniger Aufwand möglich (vgl. Fußnote zu F(41.22)).

Man beachte, daß zwar einer linearen Kongruenz eindeutig die korrespondierende diophantische Gleichung zugeordnet ist, dagegen einer diophantischen Gleichung in zwei Unbekannten zwei korrespondierende lineare Kongruenzen entsprechen. Gerade das kann man unter Umständen ausnutzen, um die Lösung einer linearen Kongruenz über die zugehörige diophantische Gleichung auf die Lösung der zweiten korrespondierenden linearen Kongruenz zurückzuführen, was mitunter vorteilhaft ist. Als Beispiel hierzu behandeln wir Aufg. 5c von § 33 auf diese Weise: Zu $9x \equiv 44\,(58)$ korrespondiert

$$9x + 58y = 44$$

und damit

$$58y \equiv 44\,(9), \quad \text{also} \quad 4y \equiv 8\,(9).$$

Man erkennt sofort $y = 2$ als Lösung dieser Kongruenz und berechnet daraus $x = -8$ als Lösung der ursprünglichen Kongruenz.

Wie wir bereits bemerkten, ist nun die Gesamtheit der Lösungen einer linearen Kongruenz leicht zu übersehen:

Satz **S (41.23)**

Die Gesamtheit aller Lösungen der linearen Kongruenz

$$a'x \equiv b' \bmod m' \quad mit \quad (a', m') \cong e$$

ist genau die Menge aller mod m' zu x kongruenten Elemente von $\mathfrak{R}$. Man erhält also aus einer bereits bekannten Lösung x_0 die allgemeine Lösung als

$$x = x_0 + rm',$$

wobei r alle Elemente von $\mathfrak{R}$ durchläuft.

Nach F(41.22) *ist dies die allgemeine Lösung jeder linearen Kongruenz*

$$ax \equiv b \bmod m \quad mit \quad (a, m) \cong d \quad und \quad d \mid b,$$

die durch „Kürzen" in die obige Kongruenz übergeführt werden kann.

Beweis

Die angegebenen Elemente $x = x_0 + rm'$ sind mit x_0 Lösungen von $a'x \equiv b' \bmod m'$, da $rm' \equiv o \bmod m'$ ist. Andererseits folgt aus

$$a'x \equiv b' \bmod m', \quad a'y \equiv b' \bmod m'$$

zunächst $a'(x - y) \equiv o \bmod m'$, d. h. $m' \mid a'(x - y)$. Da nach Voraussetzung $(a', m') \cong e$ ist, ergibt sich daraus $m' \mid x - y$, also

$$x \equiv y \bmod m'. \qquad \text{qed.}$$

Der zweite Teil dieses Beweises entspricht den (für $\mathfrak{R} = \Gamma$ schon durchgeführten) Schlüssen, daß im Restklassenring $\mathfrak{R}/(m')$ diejenigen Restklassen, deren Elemente mit m' den größten gemeinsamen Teiler e haben (vgl. Aufg. 7), keine Nullteiler sind, also nach S(25.8) in $\mathfrak{R}/(m')$ die Lösung der Gleichung

$$[a'][x] = [b']$$

eindeutig ist.

Entsprechend kann man eine beliebige Kongruenz

$$ax \equiv b \bmod m \quad \text{mit} \quad (a, m) \cong d \quad \text{und} \quad d \mid b$$

als eine Gleichung im Restklassenring mod m betrachten:

$$[a][x] = [b].$$

Die allgemeine Lösung dieser Kongruenz

$$x = x_0 + rm' \quad \text{mit} \quad m = dm', \; r \in \mathfrak{R}$$

ist uns aber zunächst nur als Restklasse $[x_0] \bmod m'$, d. h. nicht als Element des Restklassenringes $\mathfrak{R}/(m)$ gegeben (der bereits erledigte Fall mit $(m) = (m')$, also $m \cong m'$ und $d \cong e$ ausgenommen). In der Tat zerfällt aber dann die Restklasse $[x_0] \bmod m'$ in Restklassen $[x_0 + r_0 m'] \bmod m$, wobei r_0 ein vollständiges Repräsentantensystem mod d durchläuft.

Zum Beweis überlegt man sich, daß wir den alle Ringelemente durchlaufenden Parameter r aus

$$x = x_0 + rm'$$

in der Form $r = sd + r_0$ ansetzen können, wenn nunmehr s als Parameter alle Ringelemente und r_0 unabhängig davon die Elemente eines vollständigen Repräsentantensystems von $\mathfrak{R}$ mod d durchläuft. Wir erhalten also

$$x = x_0 + (sd + r_0)m' = (x_0 + r_0 m') + sm.$$

So haben wir im obigen Beispiel in $\mathfrak{R} = \Gamma$ für die Kongruenz

$$5x \equiv 2 \bmod 7, \quad \text{d. h.} \quad [5]\,[x] = [2] \bmod 7$$

die Lösung $x_0 = 6$ bereits gefunden, also ist wegen $(5, 7) \cong 1$ die allgemeine Lösung

$$x = 6 + 7r \quad \text{oder aber} \quad [x] = [6] \bmod 7.$$

Die ursprüngliche Kongruenz

$$15x \equiv 6 \bmod 21, \quad \text{d. h.} \quad [15]\,[x] = [6] \bmod 21$$

hat also ebenfalls die allgemeine Lösung

$$x = 6 + 7r,$$

die jedoch wegen $r = 3s + r_0$ mit $r_0 = 0, 1, 2$ in drei Restklassen zerfällt:

$$\left.\begin{array}{l} [x] = [6 + 0 \cdot 7] = [6] \\ [x] = [6 + 1 \cdot 7] = [13] \\ [x] = [6 + 2 \cdot 7] = [20] \end{array}\right\} \bmod 21.$$

Satz **S (41.24)**

Die Gesamtheit aller Lösungen der diophantischen Gleichung

$$ax + my = b \quad \textit{mit} \quad (a, m) \cong d, \quad a = da', \; m = dm', \; b = db'$$

erhält man aus einer bekannten Lösung x_0, y_0 in der Form

$$x = x_0 + rm', \quad y = \frac{b - ax_0}{m} - ra' = y_0 - ra',$$

wobei r alle Elemente von $\mathfrak{R}$ durchläuft.

Beweis

Nach S(41.20) und S(41.23) liefert $x = x_0 + rm'$ genau alle x, die in Lösungen x, y von $ax + my = b$ auftreten. Das jeweils zugehörige y erhält man unmittelbar durch Einsetzen:

$$y = \frac{b - ax}{m} = \frac{b - ax_0 - arm'}{m} = y_0 - \frac{arm'}{m} = y_0 - ra'.$$

qed.

So erhält man z. B. für die diophantische Gleichung

$$45x + 30y = -30,$$

unter Verwendung der speziellen Lösung $x_0 = -2$, $y_0 = 2$ die allgemeine Lösung

$$x = -2 + 2r, \quad y = 2 - 3r$$

Mit S(41.24) ist man im Prinzip in der Lage, auch jede Lösung einer diophantischen Gleichung mit mehr als zwei Unbekannten sukzessive zu berechnen, wie wir am Beispiel der diophantischen Gleichung

$$a_1 x + a_2 y + a_3 z = b$$

zeigen wollen. Dabei ist es zweckmäßig, von vornherein die natürlich als lösbar vorausgesetzte Gleichung durch den größten gemeinsamen Teiler der Koeffizienten gekürzt zu denken, also $(a_1, a_2, a_3) \cong e$ anzunehmen. Schreiben wir die vorgelegte Gleichung in der Form

$$a_1 x + a_2 y = b - a_3 z,$$

so erhalten wir eine diophantische Gleichung in den zwei Unbekannten x und y, die genau dann lösbar ist, wenn (a_1, a_2) in dem rechts stehenden Ausdruck aufgeht. Dies liefert für die dritte Unbekannte z die Bedingung

$$a_3 z \equiv b \bmod (a_1, a_2).$$

Es existieren also genau für solche Werte z, die Lösungen

$$z = z_0 + s \cdot (a_1, a_2)$$

dieser Kongruenz sind, Lösungen x, y, z der ursprünglichen diophantischen Gleichung. Man braucht daher nur für jeden konkreten Wert z dieser Art die zugehörigen x und y aus einer diophantischen Gleichung in zwei Unbekannten zu berechnen.

Dieses Verfahren liefert jedoch im Gegensatz zu S(41.24) keine geschlossene Darstellung für die Gesamtheit aller Lösungen[1]). Man ist also gezwungen, die gesuchten Lösungen einzeln zu berechnen, was offensichtlich nnr sinnvoll ist, wenn für das vorliegende Problem von den unendlich vielen möglichen Lösungen nur eine end-

1) Das liegt daran, daß wir mit Hilfe von S(41.24) nicht die Abhängigkeit der Lösungen x, y der diophantischen Gleichung

$$a_1 x + a_2 y = b - a_3(z_0 + s \cdot (a_1, a_2))$$

von dem rechts stehenden Parameter s erhalten. Wie wir hier nur mitteilen wollen, ist es jedoch möglich, auf andere Weise geschlossene Parameterdarstellungen für die allgemeine Lösung einer diophantischen Gleichung in n Unbestimmten zu gewinnen (Lit.: TH. SKOLEM, Diophantische Gleichungen, Ergebn. d. Math. u. ihrer Grenzgeb., Bd. 5, Heft 4, 1938).

liche Anzahl interessiert. Bei praktischen Aufgaben ist das glücklicherweise fast immer der Fall, da dabei die gesuchten Werte x, y und z innerhalb von gewissen (oft sogar recht engen) Grenzen gewählt werden müssen.

Beispiel:

Praktischen Sortierungsproblemen entsprechen bekannte Scherzaufgaben wie die folgende: Von drei Zigarettensorten mit einem Stückpreis von 10, 12 bzw. 15 Pfennigen sind für genau eine Mark Zigaretten zu kaufen. Damit ergeben sich für die Lösungen x, y, z der entsprechenden diophantischen Gleichung

$$10x + 12y + 15z = 100$$

die Einschränkungen

$$0 \leqq x \leqq 10,\ 0 \leqq y \leqq 8,\ 0 \leqq z \leqq 6.$$

Aus der Lösbarkeitsbedingung für

$$10x + 12y = 100 - 15z$$

erhält man

$$15z \equiv 100 \bmod 2,$$
$$z = 0 + 2s.$$

Die Behandlung der sich aus $z = 0, 2, 4, 6$ ergebenden diophantischen Gleichungen in x und y liefert insgesamt die folgenden in Frage kommenden Lösungen:

$$\begin{aligned} z = 0: &\quad x = 4,\ y = 5 \\ &\quad x = 10,\ y = 0 \\ z = 2: &\quad x = 1,\ y = 5 \\ &\quad x = 7,\ y = 0 \\ z = 4: &\quad x = 4,\ y = 0 \\ z = 6: &\quad x = 1,\ y = 0. \end{aligned}$$

Partialbruchzerlegung

Wie wir schon bei der Behandlung des Quotientenkörpers in § 30 erwähnten, bringt man im Schulunterricht die in der Anordnung der Zahlen gelegenen anschaulichen Vorteile viel früher ins Spiel, als für den strukturellen Aufbau der rationalen Zahlen prinzipiell erforderlich wäre.

S(41.12) und S(41.13) lehren, daß sogar die Darstellung als weitmöglichst gekürzter Bruch und die Hauptnennerdarstellung mehrerer Brüche von der Anordnung unabhängig sind, da diese Sätze in beliebigen ZPE-Ringen gelten. Auch die für die elementare Bruchrechnung so wichtige Unterscheidung zwischen „echten" und „unechten" Brüchen ist in dem Sinne von der Anordnung der ganzen Zahlen unabhängig, als sie sich auf beliebige euklidische Ringe übertragen läßt:

Definition **D (41.25)**

Es sei $\mathfrak{R}$ ein euklidischer Ring und $g(r)$ die seinen Elementen gemäß D(40.8) *zugeordnete nichtnegative ganze Zahl. Dann heißt ein Element $a \neq o$ des Quotientenkörpers $\mathfrak{K}$ von $\mathfrak{R}$ ein „echter Bruch", wenn in der reduzierten Quotientendarstellung*[1])

$$a = \frac{m}{n} \qquad g(m) < g(n) \quad \textit{gilt.}$$

Folgerung **F (41.26)**

Jedes Element $a \in \mathfrak{K}$ läßt sich als Summe eines ganzen Elementes q (d. h. $q \in \mathfrak{R}$) und eines echten Bruches darstellen.

Beweis

Falls nicht $a = \frac{m}{n}$ selbst schon ein ganzes Element oder ein echter Bruch ist, erhält man durch Division mit Rest

$$m = qn + r \quad \text{mit} \quad g(r) < g(n),$$

also

$$a = \frac{m}{n} = q + \frac{r}{n},$$

wobei mit m und n offensichtlich auch r und n teilerfremd sind. qed.

---

1) Der Rückgang auf die reduzierte Quotientendarstellung ist im allgemeinen erforderlich, da eine Erweiterung der Definition auf eine beliebige Quotientendarstellung

$$a = \frac{m \cdot d}{n \cdot d}$$

die gleichzeitige Gültigkeit von $g(m) < g(n)$ und $g(m \cdot d) < g(n \cdot d)$ zur Voraussetzung hätte. Diese Bedingung ist wohl in $\mathfrak{R} = \Gamma$ und $\mathfrak{R} = K[u]$ (vgl. S(41.27)), nicht aber in jedem euklidischen Ring erfüllt.

Wegen F (41.26) konzentriert sich das Interesse auf die Behandlung echter Brüche.

Partialbruchzerlegung **S (41.27)**

Es sei ein echter Bruch $a = \frac{m}{n} \in \mathfrak{R}$ *und für den Nenner n eine Zerlegung* $n = n_1 \cdot n_2$ *in teilerfremde Faktoren vorgegeben. Dann läßt sich a als Summe zweier Brüche mit den Nennern* n_1 *und* n_2 *schreiben:*

$$a = \frac{m}{n} = \frac{x}{n_1} + \frac{y}{n_2}.$$

Insbesondere kann wenigstens einer dieser Brüche als echter Bruch gewählt werden.

Zusatz

In den wichtigsten Fällen, wie etwa für $\mathfrak{R} = \Gamma$ *und* $\mathfrak{R} = \mathrm{K}[u]$ *(Polynomring in einer Unbestimmten u über einem beliebigen Körper* K*), kann man sogar erreichen, daß beide Brüche echt sind.*

Beweis

Die diophantische Gleichung

$$m = n_2 x + n_1 y$$

ist wegen $(n_1, n_2) \cong e$ in $\mathfrak{R}$ stets lösbar. Aus einer speziellen Lösung x_0, y_0 erhält man die allgemeine Lösung vermöge

$$\begin{aligned} x &= x_0 + r \cdot n_1 \\ y &= y_0 - r \cdot n_2 \end{aligned} \qquad \text{für alle } r \in \mathfrak{R}.$$

Schreibt man eine dieser Gleichungen, etwa die erste, in der Form

$$x_0 = n_1(-r) + x,$$

so erkennt man, daß sich $g(x) < g(n_1)$ auf Grund der Division mit Rest durch geeignete Wahl von $(-r)$ erreichen läßt. Dann ist aber

$$\frac{m}{n_1 \cdot n_2} = \frac{x}{n_1} + \frac{y}{n_2}$$

eine Darstellung der verlangten Art.

Die zusätzliche Behauptung für $\mathfrak{R} = \Gamma$ und $\mathfrak{R} = \mathrm{K}[u]$ erkennt man wie folgt: In

$$m = n_2 x + n_1 y$$

ist $g(m) < g(n_1 n_2)$ nach Voraussetzung und etwa $g(x) < g(n_1)$ nach Konstruktion.

Im Falle $\mathfrak{R} = \Gamma$ kann man ohne Beschränkung der Allgemeinheit die Zahlen $m, n_1\ n_2$ und x positiv wählen. Dann folgt wegen $g(r) = |r|$ für alle $r \in \Gamma$ aus $g(x) < g(n_1)$ unmittelbar $g(x n_2) < g(n_1 n_2)$, also mit $g(m) < g(n_1 n_2)$ auch $g(m - n_2 x) = g(n_1 y) < g(n_1 n_2)$, woraus sich wiederum $g(y) < g(n_2)$ ergibt, was hier zu zeigen war.

Im Falle $\mathfrak{R} = \mathrm{K}[u]$ mit dem Grad des Polynoms $r \in \mathfrak{R}$ als $g(r)$ folgt in jedem Falle aus $g(x) < g(n_1)$ auch $g(x n_2) < g(n_1 n_2)$. Mit $g(m) < g(n_1 n_2)$ ergibt dies $g(n_1 y) < g(n_1 n_2)$ und letzteres wieder $g(y) < g(n_2)$.

qed.

Folgerung **F (41.28)**

Man kann also jedes Element $a = \frac{m}{n}$ *des Quotientenkörpers* $\mathfrak{K}$ *von* $\mathfrak{R}$ *als Summe eines ganzen Elementes und einer Anzahl echter Brüche darstellen, deren Nenner gerade die Primelementpotenzen* $p_i^{\nu_i}$ *des Nenners* n *in der reduzierten Quotientendarstellung von* a *sind.*

Beispiele

a) In $\mathfrak{R} = \Gamma$ muß sich $\frac{15}{91}$ in der Form

$$\frac{15}{91} = \frac{x}{7} + \frac{y}{13}$$

mit $|x| < |7|$ und $|y| < |13|$ schreiben lassen. Dazu haben wir die diophantische Gleichung

$$15 = 13x + 7y$$

zu lösen. Aus der Kongruenz

$$15 \equiv 13x \bmod 7, \text{ also}$$

$$1 \equiv -1x \bmod 7$$

erhält man die spezielle Lösung $x_0 = -1$ und damit $y_0 = 4$, also die allgemeine Lösung

$$x = -1 + 7r$$

$$y = 4 - 13r.$$

Unter allen Lösungen sind diejenigen mit $r = 0$ und $r = 1$ wegen $|x| < |7|$ und $|y| < |13|$ geeignet:

$$\frac{15}{91} = \frac{-1}{7} + \frac{4}{13} = \frac{6}{7} + \frac{-9}{13}.$$

An diesem Beispiel erkennen wir zugleich, daß die Partialbruchzerlegung im allgemeinen nicht eindeutig ist.

b) Es sei $\mathfrak{R} = \mathrm{P}[u]$; wir suchen eine Partialbruchzerlegung für

$$\frac{6u^4 - 3u^3 + 20u^2 - 1}{u^5 - u^4 + 3u^3 - 3u^2}.$$

Der Nenner gestattet folgende Zerlegung:

$$u^5 - u^4 + 3u^3 - 3u^2 = (u-1) \cdot u^2 \cdot (u^2 + 3)$$

in paarweise teilerfremde Faktoren; demzufolge setzen wir an:

$$\frac{6u^4 - 3u^3 + 20u^2 - 1}{(u-1) \cdot u^2 \cdot (u^2+3)} = \frac{x}{u-1} + \frac{y}{u^2} + \frac{z}{u^2+3}.$$

Wir haben also die diophantische Gleichung

$$6u^4 - 3u^3 + 20u^2 - 1 = x(u^4 + 3u^2) + y(u^3 - u^2 + 3u - 3) + z(u^3 - u^2)$$

in $\mathrm{P}[u]$ zu lösen. Da wir uns jedoch nur für Lösungen x, y, z interessieren, deren Grade kleiner als die Grade der zugehörigen Nenner sind, können wir durch den Ansatz

$$x = x_0, \quad y = y_0 + y_1 u, \quad z = z_0 + z_1 u$$

und nachfolgenden Koeffizientenvergleich das Problem auf die Lösung eines linearen Gleichungssystems in P zurückführen:

Koeffizienten von
$$\begin{cases} u^4: & x_0 + & & y_1 + & z_1 = & 6 \\ u^3: & & y_0 - & y_1 + z_0 - & z_1 = & -3 \\ u^2: & 3x_0 - & y_0 + 3y_1 - & z_0 & = & 20 \\ u^1: & & 3y_0 - 3y_1 & & = & 0 \\ u^0: & & -3y_0 & & = & -1. \end{cases}$$

Durch sukzessives Einsetzen erhält man die Lösung:

$$x_0 = \frac{11}{2}, \quad y_0 = \frac{1}{3}, \quad y_1 = \frac{1}{3}, \quad z_0 = -\frac{17}{6}, \quad z_1 = \frac{1}{6}.$$

Damit haben wir als Partialbruchzerlegung:

$$\frac{6u^4 - 3u^3 + 20u^2 - 1}{u^5 - u^4 + 3u^3 - 3u^2} = \frac{\frac{11}{2}}{u-1} + \frac{\frac{1}{3} + \frac{1}{3}u}{u^2} + \frac{\frac{-17}{6} + \frac{1}{6}u}{u^2+3}$$

Bekanntlich spielt die Partialbruchzerlegung eine wichtige Rolle bei der Integration gebrochen rationaler Funktionen. Da man dort von vornherein den Körper der reellen oder sogar der komplexen Zahlen zugrundelegt, kommen für die in F(41.28) auftretenden irreduziblen Faktoren p_i des Nenners n nur quadratische und lineare Polynome bzw. nur lineare Polynome in Frage. (Dies ergibt sich aus dem sog. Fundamentalsatz der klassischen Algebra, auf den wir in Teil 3, § 51 zu sprechen kommen.)

Allerdings ist mit den Summanden

$$\frac{z(u)}{(p(u))^\nu} \quad \text{mit} \quad g(z) < g(p^\nu)$$

für die Integration noch nicht sehr viel gewonnen. Man kann sie aber weiter zerlegen in der Form

$$(*) \qquad \frac{z(u)}{(p(u))^\nu} = \frac{z_1(u)}{(p(u))^\nu} + \frac{z_2(u)}{(p(u))^{\nu-1}} + \ldots + \frac{z_\nu(u)}{p(u)},$$

wobei der Grad der Zähler $z_i(u)$ kleiner als der Grad von $p(u)$ gewählt werden kann. Nach der obigen Bemerkung treten also als Zähler höchstens lineare Polynome bzw. nur Konstante auf, so daß die Summanden in (*) leicht integrierbar sind. Dabei ergibt sich (*) durch sukzessive Anwendung der Division mit Rest:

$$z = pq_1 + z_1, \quad \text{also} \quad \frac{z}{p^\nu} = \frac{z_1}{p^\nu} + \frac{q_1}{p^{\nu-1}},$$

$$q_1 = pq_2 + z_2, \quad \text{also} \quad \frac{q_1}{p^{\nu-1}} = \frac{z_2}{p^{\nu-1}} + \frac{q_2}{p^{\nu-2}}, \ldots.$$

Übrigens folgt in gleicher Weise für die Summanden $\frac{z}{p^\nu}$ einer Partialbruchzerlegung einer rationalen Zahl die Darstellung

$$\frac{z}{p^\nu} = \frac{z_1}{p^\nu} + \frac{z_2}{p^{\nu-1}} + \ldots + \frac{z_\nu}{p},$$

die sich auch sofort aus der Systemdarstellung der ganzen Zahl $z < p^\nu$ mit der Grundzahl p ergibt:

$$z = z_1 + z_2 p + \ldots + z_\nu p^{\nu-1}.$$

Wir wollen abschließend nur noch bemerken, daß die Zerlegung von gebrochen rationalen Funktionen mit Koeffizienten aus einem beliebigen Körper K in Partialbrüche gemäß F(41.28) stets eindeutig bestimmt ist[1]).

---

1) Für einen allgemeinen Eindeutigkeitsbeweis, der zugleich die Eindeutigkeit für verschiedene Zerlegungstypen zeigt (u. a. auch für die im Kleindruck angegebene weitere Aufspaltung der Zerlegung aus F(41.28)), verweisen wir auf LUGOWSKI-WEINERT, Wiss. Zeitschr. d. Päd. Hochsch. Potsdam, Jahrg. 4, Heft 1.

Kettenbruchentwicklung

Es ist für viele Untersuchungen von grundlegender Bedeutung, daß sich jede reelle Zahl als regelmäßiger Kettenbruch

$$z = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \cfrac{1}{\ddots}}}}$$

entwickeln läßt, d. h. als Kettenbruch, in dem alle auftretenden Zähler gleich 1 und alle q_i ganze, $q_1, q_2, q_3, \ldots$ sogar positive ganze Zahlen sind. Eine solche Darstellung ist eindeutig und bricht genau für rationale Zahlen nach endlich vielen Schritten ab[1]).

Ohne daß wir auf diesbezügliche Untersuchungen hier näher eingehen können (wir verweisen hierfür auf das in dieser Reihe erschienene Buch „Kettenbrüche" von KHINTCHINE) wollen wir nur den Zusammenhang zwischen den endlichen regelmäßigen Kettenbruchentwicklungen rationaler Zahlen und dem euklidischen Algorithmus hervorheben[2]). Dieser läßt sich nämlich gleich allgemein für die Elemente des Quotientenkörpers eines beliebigen euklidischen Ringes aussprechen:

---

1) Eine dabei für endliche regelmäßige Kettenbrüche stets mögliche Abänderung

$$z = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \ddots + \cfrac{1}{q_n}}} = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \ddots + \cfrac{1}{(q_n - 1) + \cfrac{1}{1}}}}$$

sieht man bezüglich der Eindeutigkeitsaussage als nicht wesentlich an.

2) Wir machen aber darauf aufmerksam, daß die eigentliche Bedeutung von Kettenbruchentwicklungen darin liegt, sehr gute Annäherungen reeller Zahlen durch rationale Zahlen zu ermöglichen.

Satz **S (41.29)**

Jedes Element $\frac{a}{b}$ *des Quotientenkörpers* $\mathfrak{K}$ *von* $\mathfrak{R}$ *läßt sich mit Hilfe des euklidischen Algorithmus in* $\mathfrak{R}$ *in einen endlichen Kettenbruch entwickeln.*

Beweis

Die Relationen des euklidischen Algorithmus lassen sich umschreiben zu:

$$a = bq_0 + r_1 \qquad \frac{a}{b} = q_0 + \frac{r_1}{b} = q_0 = \frac{e}{\frac{b}{r_1}}$$

$$b = r_1 q_1 + r_2 \qquad \frac{b}{r_1} = q_1 + \frac{r_2}{r_1} = q_1 + \frac{e}{\frac{r_1}{r_2}}$$

$$r_1 = r_2 q_2 + r_3 \qquad \frac{r_1}{r_2} = q_2 + \frac{r_3}{r_2} = q_2 + \frac{e}{\frac{r_2}{r_3}}$$

$$\vdots \qquad\qquad \vdots$$

$$r_{n-1} = r_n q_n + o \qquad \frac{r_{n-1}}{r_n} = q_n .$$

Sukzessives Einsetzen der rechts stehenden Ausdrücke liefert die Behauptung.

qed.

Als Beispiel für $\mathfrak{R} = \Gamma$ betrachten wir $\frac{-11}{9}$:

$$\begin{aligned} -11 &= 9 \cdot (-2) + 7, \\ 9 &= 7 \cdot 1 \quad + 2 \\ 7 &= 2 \cdot 3 \quad + 1 \\ 2 &= 1 \cdot 2 \end{aligned} \qquad \text{also } -\frac{11}{9} = -2 + \cfrac{1}{1 + \cfrac{1}{3 + \frac{1}{2}}}$$

In $\mathfrak{R} = \Gamma$ erhält man bei diesem Verfahren die regelmäßige Kettenbruchentwicklung, wenn man (wie eben geschehen) die beim euklidischen Algorithmus auftretenden Reste stets positiv wählt.

Andernfalls ergibt sich etwa

$$\begin{aligned} -11 &= \quad 9 \cdot (-1) - 2, \\ 9 &= (-2) \cdot (-4) + 1 \\ -\ 2 &= \quad 1 \cdot (-2) \end{aligned} \qquad \text{also } -\frac{11}{9} = -1 + \cfrac{1}{-4 + \cfrac{1}{-2}}$$

Daraus ersieht man, daß die vorn erwähnte Eindeutigkeitsaussage für $\mathfrak{R} = \Gamma$ wesentlich von der in der Forderung „regelmäßig" enthaltenen positiven Normierung abhängt. In beliebigen euklidischen Ringen kann man also im allgemeinen nur noch fordern, daß alle auftretenden Zähler gleich e sind, woraus sich jedoch keine Eindeutigkeitsaussage ableiten läßt.

Aufgaben zu § 41

1. Man untersuche die gegenseitigen Teilbarkeitsverhältnisse der Zahlen $a = 3740, b = 6171, c = 123420, d = 187$ durch Angabe der zugehörigen Exponentensysteme.

2. Man gebe ein in ZPE-Ringen gültiges Kriterium für Teilerfremdheit und paarweise Teilerfremdheit an.

3. Die Elemente $a, b, \ldots, r$ seien verschieden von o. Dann gilt genau dann $[a, b, \ldots, r] \cong ab \ldots r$, wenn diese Elemente paarweise teilerfremd sind.

4. Man beweise die beiden folgenden Beziehungen:

   Aus $a \mid m, b \mid m, \ldots$ folgt $[a, b, \ldots] \mid m$.

   Aus $a \mid a', b \mid b', \ldots$ folgt $[a, b, \ldots] \mid [a', b', \ldots]$.

5. Welche der Aussagen, die im § 40 zum Beweis der Existenz und Eindeutigkeit der Primzerlegung herangezogen wurden, gelten umgekehrt in jedem ZPE-Ring?

6. Ein Element a des ZPE-Ringes $\mathfrak{R}$, das selbst keine n-te Potenz ($n > 1$) eines Elementes aus $\mathfrak{R}$ ist, hat auch im Quotientenkörper von $\mathfrak{R}$ keine n-te Wurzel. (Insbesondere: eine ganze Zahl a, die nicht n-te Potenz einer anderen ganzen Zahl ist, hat auch keine rationale n-te Wurzel; oder: ein Polynom $f(x) \in \mathfrak{R}[x]$, das nicht n-te Potenz eines anderen Polynoms aus $\mathfrak{R}[x]$ ist, hat auch keine rationale Funktion $g(x) \in \mathfrak{R}(x)$ als n-te Wurzel.)

7. In Verallgemeinerung der Überlegungen aus B(2.8) beweise man: Für jeden Restklassenring $\mathfrak{R}/(m)$ eines ZPE-Ringes $\mathfrak{R}$ gilt, daß alle Elemente $a, a', \ldots$ einer Restklasse mod m mit m den gleichen größten gemeinsamen Teiler haben.

8. Man behandle die folgenden diophantischen Gleichungen nach den verschiedenen möglichen Lösungswegen:

$$16x - 28y = 36$$
$$34x + 30y = 36$$
$$41x + 36y = 7.$$

9. Man gebe sämtliche möglichen Zerlegungen von $\frac{1}{315}$ in eine Summe von drei echten Partialbrüchen an.

10. Man zerlege

$$\frac{2u^3 + \frac{25}{2}u^2 + 4u - 2}{(u^2 + 3u - 1)(u + 2)(u - 2)} \in \mathrm{P}(u)$$

in Partialbrüche.

11. Die folgenden rationalen Zahlen sind als regelmäßige Kettenbrüche anzugeben:

$$\frac{78}{53}, \quad \frac{67}{92}, \quad \frac{1217}{510}.$$

§ 42. Idealtheoretische Auffassung der Teilbarkeitslehre in Hauptidealringen

Die Gültigkeit des Satzes über die Existenz und Eindeutigkeit der Zerlegung in Primelemente macht die Teilbarkeitsverhältnisse in ZPE-Ringen besonders übersichtlich. Die Absicht, auch für weitere Klassen von Ringen ähnliche strukturelle Gesetzmäßigkeiten zu gewinnen, führte in den letzten Jahrzehnten des vorigen Jahrhunderts zur Entwicklung des für die gesamte Algebra so fruchtbaren Idealbegriffes. Mit seiner Hilfe ist es in der Tat möglich, immer weitergehende Verallgemeinerungen des obengenannten Zerlegungssatzes anzugeben, je nach Wahl der Voraussetzungen über die betrachteten Ringe.

Wir werden uns hier allerdings auf den ersten Schritt dieser Verallgemeinerungen beschränken.

Um überhaupt erst einmal eine Verbindung zwischen der Teilbarkeitslehre und dem Idealbegriff herzustellen, formen wir in diesem Paragraphen zunächst die im § 39 entwickelten Aussagen für Elemente in Aussagen für die von ihnen erzeugten Hauptideale um. Dies liegt auch deswegen nahe, da einerseits die Teilbarkeitsaus-

sagen immer Klassen assoziierter Elemente betreffen und andererseits jede Klasse assoziierter Elemente genau ein Hauptideal bestimmt (vgl. Aufg. 4 von § 39). Dabei ist es ab D (42.6) erforderlich, daß sich die so geführten Überlegungen auf alle Ideale des Ringes erstrecken, also ein Hauptidealring vorliegt. Der Leser kann aber im Hinblick auf die in § 43 ohnehin vorzunehmenden Verallgemeinerungen von vornherein unter $\mathfrak{R}$ einen Hauptidealring verstehen, natürlich gemäß unseren Einschränkungen ohne Nullteiler und mit Einselement.

Definition **D (42.1)**

Ein Ideal (b) *von* $\mathfrak{R}$ *heißt Teiler eines Ideals* (a) *von* $\mathfrak{R}$, *wenn* b *ein Teiler von* a *ist. Entsprechend nennt man* (a) *ein Vielfaches von* (b).

Diese Definition ist von der Wahl der erzeugenden Elemente von (a) und (b) unabhängig, da mit $b \mid a$ auch $b' \mid a'$ gilt für alle $a' \cong a$ und $b' \cong b$. Übrigens kann man diese Unabhängigkeit auch aus dem nachstehenden Kriterium entnehmen, in dem nicht mehr auf erzeugende Elemente zurückgegriffen wird und welches sich daher für eine spätere Verallgemeinerung eignet:

Satz **S (42.2)**

Ein Ideal (b) *von* $\mathfrak{R}$ *ist Teiler eines Ideals* (a) *von* $\mathfrak{R}$ *genau dann, wenn* $(b) \supseteq (a)$ *gilt.*

Beweis

Aus $b \mid a$ folgt $a = b\,x$ mit $x \in \mathfrak{R}$ und damit $a \in (b)$, also $(a) \subseteq (b)$ und umgekehrt. qed.

So ist z. B. im Ring Γ der ganzen Zahlen wegen $6 \mid 18$ das Ideal (6) ein Teiler des Ideals (18); man beachte dabei, daß eine Deutung von $(6) \supseteq (18)$ im Sinne von „größer und kleiner" der entsprechenden Beziehung für die erzeugenden Elemente entgegenläuft.

Mit diesem Teilbarkeitsbegriff für Ideale entsprechen den Elementaussagen a), b), c) und f) von F (39.2) der Reihe nach die Idealaussagen:

$$(a) \supseteq (a), \quad \mathfrak{R} = (e) \supseteq (a), \quad (a) \supseteq (o),$$

$$\text{aus } (a_1) \supseteq (a_2) \text{ und } (a_2) \supseteq (a_3) \text{ folgt } (a_1) \supseteq (a_3).$$

Um auch die weiteren Relationen von F(39.2) übertragen zu können, benötigen wir zunächst eine Multiplikation zwischen den Idealen von $\mathfrak{R}$:

Definition **D (42.3)**

Unter dem Produkt zweier Ideale (a) *und* (b) *von* $\mathfrak{R}$ *versteht man das von* $a \cdot b$ *erzeugte Ideal von* $\mathfrak{R}$*:*

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

Auch diese Definition ist von der Wahl der erzeugenden Elemente unabhängig; es folgt nämlich aus $a' \cong a$ und $b' \cong b$ stets $a'b' \cong ab$. Dieser Nachweis kann wiederum ersetzt werden durch die Berufung auf das folgende, von den erzeugenden Elementen freie Kriterium:

Satz **S (42.4)**

Das Produkt $(a) \cdot (b) = (a \cdot b)$ *besteht aus genau allen endlichen Summen* $\sum a_i b_i$ *mit beliebigen* $a_i \in (a)$ *und* $b_i \in (b)$.

Beweis

Offensichtlich enthält die Menge dieser Summen alle Ringvielfachen $r \cdot ab = ra \cdot b$ von ab, also (ab).

Umgekehrt gilt wegen $a_i = ar_i$ und $b_i = br_i'$ für jede dieser Summen

$$\sum a_i b_i = \sum ar_i \cdot br_i' = ab \sum r_i r_i' \in (ab).$$

qed.

Die Anwendung dieser Idealmultiplikation auf D(42.1) ergibt ersichtlich ein weiteres Kriterium der Teilbarkeit von Hauptidealen, für die wir ab jetzt auch das Zeichen $(b) \mid (a)$ verwenden[1]):

Satz **S (42.5)**

Ein Ideal (b) *von* $\mathfrak{R}$ *ist Teiler eines Ideals* (a) *von* $\mathfrak{R}$ *genau dann, wenn in* $\mathfrak{R}$ *ein Ideal* (x) *existiert mit* $(a) = (b) \cdot (x)$.

---

1) Dies hat seinen Grund darin, daß bei der Verallgemeinerung dieser Begriffe auf beliebige Ideale — zu der wir in diesem Paragraphen ja nur einführende Vorüberlegungen anstellen — die Aussagen von S(42.2) und S(42.5) nicht mehr gleichwertig zu sein brauchen (vgl. dazu die Fußnote auf Seite 194).

Wir kommen nunmehr zurück auf die Übertragung der Aussagen von F(39.2) und erhalten:

d) Aus $(b) \supseteq (a)$ folgt $(b) \supseteq (a) \cdot (c)$.

e) Aus $(b) \supseteq (a)$ folgt $(b) \cdot (c) \supseteq (a) \cdot (c)$
und, falls $(c) \neq (o)$, auch umgekehrt.

g) Aus $(b_1) \supseteq (a_1)$ und $(b_2) \supseteq (a_2)$ folgt $(b_1) \cdot (b_2) \supseteq (a_1) \cdot (a_2)$.

h) Aus $(b) \supseteq (a_1)$ und $(b) \supseteq (a_2)$ folgt $(b) \supseteq (c_1) \cdot (a_1) + (c_2) \cdot (a_2)$.

Dabei ergibt sich h) unter zweimaliger Verwendung von d), da (b) als Modul mit $(c_1) \cdot (a_1)$ und $(c_2) \cdot (a_2)$ natürlich auch die Summe $(c_1) \cdot (a_1) + (c_2) \cdot (a_2) = (c_1 a_1) + (c_2 a_2)$ enthält, die nach den Bemerkungen am Ende von § 28 mit dem Ideal $(c_1 a_1, c_2 a_2)$ übereinstimmt. Die einfache Umdeutung der entsprechenden Elementaussagen würde hier nur die schwächere Relation $(b) \supseteq (c_1 a_1 + c_2 a_2)$ liefern (vgl. Aufg. 2).

Die Vorteile der idealtheoretischen Auffassung der Teilbarkeit werden besonders deutlich, wenn man analog zu D(39.8) den Begriff des größten gemeinsamen Teilers für Ideale bildet.

Definition **D (42.6)**

Ein Ideal $\mathfrak{d}$ *von* $\mathfrak{R}$ *heißt größter gemeinsamer Teiler der Ideale* $(a_1), (a_2), \ldots, (a_n)$ *von* $\mathfrak{R}$, *wenn gilt:*

(*) $\mathfrak{d}$ *ist gemeinsamer Teiler dieser Ideale.*

(**) *Ist irgendein Ideal* $\mathfrak{t}$ *gemeinsamer Teiler dieser Ideale, so ist* $\mathfrak{t}$ *auch Teiler von* $\mathfrak{d}$.

Satz **S (42.7)**

In einem Hauptidealring ist der größte gemeinsame Teiler $\mathfrak{d}$ *der Ideale* $(a_1), (a_2), \ldots, (a_n)$ *eindeutig bestimmt als das von dem größten gemeinsamen Teiler* d *der Elemente* $a_1, a_2, \ldots, a_n$ *erzeugte Hauptideal*

$$\mathfrak{d} = (d).$$

Dieses Ideal stimmt mit dem von den Elementen $a_1, a_2, \ldots, a_n$ *erzeugten Ideal überein:*

$$\mathfrak{d} = (a_1, a_2, \ldots, a_n) = (a_1) + (a_2) + \ldots + (a_n).$$

Beweis

Berücksichtigt man, daß alle auftretenden Ideale Hauptideale sein müssen, und denkt beim Lesen von D(42.6) an die mit dem Wort Teiler in D(42.1) festgelegte Beziehung zwischen den erzeugenden Elementen, so ergibt sich: Das von dem größten gemeinsamen Teiler d der Elemente $a_1, \ldots, a_n$ erzeugte Ideal $\mathfrak{d} = (d)$ erfüllt (*) und (**); gelten umgekehrt (*) und (**) für irgendein Ideal $\mathfrak{d} = (d')$, so ist d' größter gemeinsamer Teiler von $a_1, \ldots, a_n$, also $(d') = (d)$.

Stützt man sich dagegen auf das Kriterium S(42.2), so erhält D(42.6) die Gestalt:

(*) $\mathfrak{d} \supseteq (a_1), \ldots, \mathfrak{d} \supseteq (a_n)$;

(**) aus $\mathfrak{t} \supseteq (a_1), \ldots, \mathfrak{t} \supseteq (a_n)$ folgt $\mathfrak{t} \supseteq \mathfrak{d}$.

Damit ist der größte gemeinsame Teiler $\mathfrak{d}$ als das (mengenmäßig) kleinste Ideal bestimmt, das die Ideale $(a_1), \ldots, (a_n)$ enthält[1]). Letzteres ist aber gemäß unseren Überlegungen am Ende von § 28 genau das Ideal $(a_1, \ldots, a_n) = (a_1) + \ldots + (a_n)$. qed.

Somit ordnet sich in Hauptidealringen die elementmäßige Bezeichnung des größten gemeinsamen Teilers $d \cong (a_1, a_2, \ldots, a_n)$ der idealtheoretischen Begriffsbildung unter, wenn man bei Ersetzung von $\cong$ durch $=$ zu den erzeugten Idealen übergeht:

$$(d) = ((a_1, a_2, \ldots, a_n)) = (a_1, a_2, \ldots, a_n).$$

Insbesondere liegt dem Hauptsatz über den größten gemeinsamen Teiler, den wir zunächst für euklidische Ringe (vgl. S(40.11)), dann aber allgemein für Hauptidealringe (vgl. S(40.17)) bewiesen haben, diese Formel zugrunde (vgl. auch Fußnote auf Seite 145).

Völlig analoge Überlegungen lassen sich für das kleinste gemeinsame Vielfache anstellen:

Definition **D(42.8)**

Ein Ideal $\mathfrak{f}$ *von* $\mathfrak{R}$ *heißt kleinstes gemeinsames Vielfaches der Ideale* $(a_1), (a_2), \ldots, (a_n)$ *von* $\mathfrak{R}$, *wenn gilt:*

1) Man beachte, daß sich auch hier die Begriffe „größer und kleiner" beim Übergang vom Element- zum Idealstandpunkt umkehren.

(†) $\mathfrak{f}$ *ist gemeinsames Vielfaches dieser Ideale.*

(††) *Ist irgendein Ideal* $\mathfrak{v}$ *gemeinsames Vielfaches dieser Ideale, so ist* $\mathfrak{v}$ *auch Vielfaches von* $\mathfrak{f}$.

Satz **S (42.9)**

In einem Hauptidealring ist das kleinste gemeinsame Vielfache $\mathfrak{f}$ *der Ideale* $(a_1), (a_2), \ldots, (a_n)$ *eindeutig bestimmt als das von dem kleinsten gemeinsamen Vielfachen* f *der Elemente* $a_1, a_2, \ldots, a_n$ *erzeugte Hauptideal*

$$\mathfrak{f} = (f).$$

Dieses Ideal stimmt mit dem Durchschnitt der Ideale $(a_1), (a_2), \ldots, (a_n)$ *überein:*

$$\mathfrak{f} = (a_1) \wedge (a_2) \wedge \ldots \wedge (a_n).$$

Beweis

Die erste Aussage ergibt sich wieder unter Zugrundelegung der Teilbarkeitsbeziehungen zwischen den erzeugenden Elementen der betrachteten Ideale wie im Beweis von S (42.7).

Für den zweiten Teil schreiben wir D (42.8) unter Verwendung des Kriteriums S (42.2):

(†) $\mathfrak{f} \subseteq (a_1), \ldots, \mathfrak{f} \subseteq (a_n)$;

(††) aus $\mathfrak{v} \subseteq (a_1), \ldots, \mathfrak{v} \subseteq (a_n)$ folgt $\mathfrak{v} \subseteq \mathfrak{f}$.

Also ist das kleinste gemeinsame Vielfache $\mathfrak{f}$ das (mengenmäßig) größte Ideal, welches in allen Idealen $(a_1), \ldots, (a_n)$, also in deren Durchschnitt enthalten ist. Entsprechend Aufg. 7 von § 28 ist dieser Durchschnitt selbst ein Ideal und damit $\mathfrak{f} = (a_1) \wedge \ldots \wedge (a_n)$.

qed.

Wir kommen schließlich zu dem für die elementmäßige Auffassung der Teilbarkeitslehre entscheidenden Begriff des Primelements. Die bisher in diesem Paragraphen verfolgten Gesichtspunkte würden es nahelegen, in Hauptidealringen die von Primelementen erzeugten Ideale als Primideale zu bezeichnen; als solche sind aber bereits allgemein diejenigen Ideale definiert (vgl. D (34.7)), nach denen der Restklassenring nullteilerfrei ist.

Diese beiden Auffassungen stimmen jedoch hier überein, wenn man von den trivialen Primidealen (o) und $\mathfrak{R}$ absieht:

Satz **S (42.10)**

In einem Hauptidealring $\mathfrak{R}$ sind die nichttrivialen Primideale genau die von Primelementen erzeugten Ideale.

Beweis

Es sei (p) ein von einem Primelement p von $\mathfrak{R}$ erzeugtes Ideal. Wir haben die Nullteilerfreiheit des Restklassenringes $\mathfrak{R}/(p)$ zu zeigen, also die Aussage:

$$\text{Aus } ab \equiv o\,(p) \text{ und } a \not\equiv o\,(p) \text{ folgt } b \equiv o\,(p).$$

Das ergibt sich aber unmittelbar aus F (40.13).

Umgekehrt sei $\mathfrak{p} = (c)$ ein nichttriviales Primideal von $\mathfrak{R}$. Wäre dabei c kein Primelement, so müßte es entweder eine Einheit oder ein zerlegbares Element von $\mathfrak{R}$ sein. Der erste Fall ist wegen $\mathfrak{p} \neq \mathfrak{R}$ ausgeschlossen. Im zweiten Fall wäre c ein Produkt nichttrivialer Teiler a und b, was ebenfalls zum Widerspruch führt. Aus $ab = c$ folgt nämlich $c \nmid a$ wegen $a \mid c$ (sonst $a \cong c$) und $c \nmid b$ wegen $b \mid c$ (sonst $b \cong c$), also

$$a \not\equiv o\,(\mathfrak{p}) \text{ und } b \not\equiv o\,(\mathfrak{p}), \text{ aber doch } ab \equiv o\,(\mathfrak{p}).$$

qed.

Die Tatsache, daß in einem Hauptidealring gerade die von Primelementen erzeugten Ideale nullteilerfreie Restklassenringe liefern, war der historische Anlaß, Ideale mit der letzteren Eigenschaft „Primideale" zu nennen. Im Laufe der Entwicklung stellte sich jedoch heraus, daß diese Entsprechung in allgemeineren Ringen gar nicht mehr vorzuliegen braucht.

So sind zwar noch unter den Hauptidealen eines ZPE-Ringes genau diejenigen Primideale, die von einem Primelement erzeugt werden; für sie läßt sich nämlich der oben geführte Beweis wörtlich übertragen, da F (40.13) in jedem ZPE-Ring gültig ist (vgl. Aufg. 5 von § 41). Allerdings gibt es — falls ein solcher Ring eben nicht Hauptidealring ist — außerdem noch Primideale, die nicht Hauptideale sind, z. B. das Ideal $(2, x)$ (vgl. Aufg. 5 von § 36) in dem Ring $\Gamma[x]$, der nach unseren Bemerkungen in B (40.19) ZPE-Ring ist.

Dagegen gilt diese Entsprechung schon nicht mehr in Ringen, die wohl S (40.1) und S (40.2), nicht aber S (40.3) erfüllen. Zum Beispiel ist im Ring $\Gamma + \Gamma\sqrt{-5}$ wegen (vgl. B (40.20b)).

$$6 = 2 \cdot 3 = (1 + \sqrt{-5}) \cdot (1 - \sqrt{-5})$$

das von dem Primelement 2 erzeugte Hauptideal (2) kein Primideal, denn es ist einerseits $1 + \sqrt{-5} \not\equiv 0 \bmod (2)$ und $1 - \sqrt{-5} \not\equiv 0 \bmod (2)$, aber andererseits $(1 + \sqrt{-5})(1 - \sqrt{-5}) \equiv 0 \bmod (2)$. Offensichtlich läßt sich diese Überlegung an jede nichteindeutige Zerlegung eines Elementes in Primelemente anschließen.

Die Primideale eines Hauptidealringes verdienen ihren Namen aber nicht nur im Hinblick auf die sie erzeugenden Primelemente, sondern auch bezüglich der beiden idealtheoretischen Kriterien der Teilbarkeit[1]). Unter Verwendung von D(42.1) ergibt sich nämlich aus S(42.10) unmittelbar:

Satz **S(42.11)**

Ein Ideal $\mathfrak{p}$ *eines Hauptidealringes* $\mathfrak{R}$ *mit* $(o) < \mathfrak{p} < \mathfrak{R}$ *ist Primideal von* $\mathfrak{R}$ *genau dann, wenn es außer sich selbst und dem ganzen Ring keine Teiler besitzt. Das bedeutet*

nach S(42.2)*: aus* $\mathfrak{p} \subseteq \mathfrak{a} \subseteq \mathfrak{R}$ *folgt* $\mathfrak{p} = \mathfrak{a}$ *oder* $\mathfrak{a} = \mathfrak{R}$,
d. h., $\mathfrak{p}$ *ist ein maximales Ideal;*

nach S(42.5)*: aus* $\mathfrak{p} = \mathfrak{a}\mathfrak{b}$ *folgt* $\mathfrak{p} = \mathfrak{a}$ *und* $\mathfrak{b} = \mathfrak{R}$ *oder* $\mathfrak{p} = \mathfrak{b}$ *und* $\mathfrak{a} = \mathfrak{R}$,
d. h., $\mathfrak{p}$ *ist ein unzerlegbares Ideal.*

Insbesondere lehrt die Übertragung der in Hauptidealringen gültigen Sätze S(40.1), S(40.2) und S(40.3) über die Existenz und Eindeutigkeit der Zerlegung eines Elementes in Primelemente, daß die Primideale bezüglich der Idealmultiplikation die gleiche Rolle spielen wie die Primelemente bezüglich der Elementmultiplikation:

Satz **S(42.12)**

In einem Hauptidealring $\mathfrak{R}$ *besitzt jedes Ideal* $\mathfrak{a}$ *mit* $(o) < \mathfrak{a} < \mathfrak{R}$ *eine Darstellung als Produkt endlich vieler, nicht notwendig verschiedener Primideale* $\mathfrak{p}_i < \mathfrak{R}$, *und diese Darstellung ist bis auf die Reihenfolge der Faktoren eindeutig:*

$$\mathfrak{a} = \mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_n.$$

Diese idealtheoretische Aussage über die Zerlegung von Idealen in Primideale, die in Hauptidealringen nur als eine andere Formulierung der ZPE-Ring-Eigenschaft erscheint, ist nun Gegenstand der folgenden Überlegungen. Sie gilt nämlich auch in einer Reihe von Ringen, in denen die entsprechende Aussage für Elemente nicht mehr gültig ist, und vermag diese bei strukturellen Überlegungen weitgehend zu ersetzen.

---

1) Der folgende Satz gilt zwar nicht nur in Hauptidealringen (er ist z. B. auch für die im nächsten Paragraphen behandelten Ringe mit Teilerkettensatz und Faktorsatz erfüllt), doch ist seine Gültigkeit ebenfalls auf gewisse Ringe beschränkt. So hatten wir bereits in § 34 Beispiele von Primidealen angegeben, die nicht maximal sind. Übrigens liefert S(42.11) ein oft handliches Kriterium dafür, daß ein Ring kein Hauptidealring ist (vgl. Aufg. 5).

Aufgaben zu § 42

1. Man veranschauliche sich die F (39.2) entsprechenden Idealaussagen durch konkrete Beispiele etwa im Ring Γ der ganzen Zahlen, indem man sich überlegt, aus welchen Elementen die auftretenden Hauptideale bestehen.

2. Für die Hauptideale $(x_1 + x_2)$, (x_1) und (x_2) gilt zwar immer
$$(x_1 + x_2) \subseteqq (x_1) + (x_2),$$
wobei jedoch im allgemeinen echtes Enthaltensein vorliegt. Man gebe im Ringe Γ Beispiele für beide Fälle.

3. Man bestimme die Summe der folgenden Ideale aus $P[x]$:
$$(x^3 - 2x^2 - x + 2),\ (x^2 - 1),\ (x^2 + x - 2).$$

4. Man berechne den Durchschnitt der Ideale (12), (33) und (44) aus Γ.

5. Man beweise die Behauptung aus Aufgabe 8 von § 40 erneut unter Verwendung der Tatsache, daß in Hauptidealringen alle (nichttrivialen) Primideale maximal sind.

§ 43. Zerlegung in Primideale

Gemäß den bereits im vorigen Paragraphen gemachten Bemerkungen wenden wir uns nunmehr dem ersten Schritt einer idealtheoretischen Verallgemeinerung des in ZPE-Ringen gültigen Zerlegungssatzes zu. Die dazu notwendigen Begriffsbildungen werden uns durch die vorbereitenden Betrachtungen in Hauptidealringen nahegelegt, müssen aber natürlich unabhängig davon neu gefaßt werden.

Alle auftretenden Ringe sind dabei stets Integritätsbereiche mit Einselement.

In Anlehnung an S (42.4) treffen wir zunächst die

Definition **D (43.1)**

Es seien $\mathfrak{a}$ *und* $\mathfrak{b}$ *zwei Ideale von* $\mathfrak{R}$. *Dann versteht man unter dem Produkt* $\mathfrak{a} \cdot \mathfrak{b}$ *das aus allen endlichen Summen* $\sum a_i \cdot b_i$ *mit beliebigen* $a_i \in \mathfrak{a}$ *und* $b_i \in \mathfrak{b}$ *bestehende Ideal von* $\mathfrak{R}$.

In der Tat bildet die Menge dieser Summen ein Ideal von $\mathfrak{R}$, da sowohl Subtraktion als auch Multiplikation mit Ringelementen aus dieser Menge nicht herausführt.

Weiterhin ist D(43.1) wirklich eine Verallgemeinerung der in D(42.3) für Hauptideale bereits festgelegten Multiplikation, wie aus S(42.4) hervorgeht. Darüber hinaus gilt: Sind $\mathfrak{a}$ und $\mathfrak{b}$ Ideale mit endlicher Basis, so ist auch das Produkt $\mathfrak{a} \cdot \mathfrak{b}$ ein Ideal mit endlicher Basis; und zwar folgt (vgl. Aufg. 2) aus $\mathfrak{a} = (a_1, a_2, \ldots, a_n)$ und $\mathfrak{b} = (b_1, b_2, \ldots, b_m)$

$$\mathfrak{a} \cdot \mathfrak{b} = (a_1 b_1, a_1 b_2, \ldots, a_1 b_m, a_2 b_1, \ldots\ldots, a_n b_m).$$

Die Idealmultiplikation ist offensichtlich kommutativ und assoziativ, die Ideale von $\mathfrak{R}$ bilden also eine abelsche Halbgruppe, insbesondere ist das Einheitsideal das Einselement dieser Halbgruppe. Ferner ist die Idealmultiplikation mit der Addition von Idealen (im Sinne der Komplexaddition von Moduln) distributiv verbunden (vgl. Aufg. 1):

$$\mathfrak{a} \cdot (\mathfrak{b} + \mathfrak{c}) = \mathfrak{a} \cdot \mathfrak{b} + \mathfrak{a} \cdot \mathfrak{c}.$$

Wir bemerken noch, daß $\mathfrak{a} \cdot \mathfrak{b} \subseteq \mathfrak{a} \cdot \mathfrak{R} = \mathfrak{a}$ und $\mathfrak{a} \cdot \mathfrak{b} \subseteq \mathfrak{R} \cdot \mathfrak{b} = \mathfrak{b}$ und daher auch $\mathfrak{a} \cdot \mathfrak{b} \subseteq \mathfrak{a} \cap \mathfrak{b}$ gilt. Schließlich läßt sich mit Hilfe der Idealmultiplikation ein Primideal $\mathfrak{p}$ von $\mathfrak{R}$ wie folgt kennzeichnen:

Satz **S (43.2)**

Ein Ideal $\mathfrak{p}$ von $\mathfrak{R}$ ist genau dann Primideal, wenn für alle Ideale $\mathfrak{a}$ und $\mathfrak{b}$ von $\mathfrak{R}$ gilt:

$$\textit{Aus } \mathfrak{p} \supseteq \mathfrak{a}\mathfrak{b} \textit{ und } \mathfrak{p} \not\supseteq \mathfrak{a} \textit{ folgt } \mathfrak{p} \supseteq \mathfrak{b}.$$

Beweis

Die angegebene Bedingung ist notwendig; denn wäre $\mathfrak{a} \not\subseteq \mathfrak{p}$ und $\mathfrak{b} \not\subseteq \mathfrak{p}$, aber $\mathfrak{a} \cdot \mathfrak{b} \subseteq \mathfrak{p}$, so existierten von o verschiedene Elemente $a \in \mathfrak{a}$ und $b \in \mathfrak{b}$ mit $a \notin \mathfrak{p}$ und $b \notin \mathfrak{p}$, während doch im Widerspruch zur Primidealeigenschaft von $\mathfrak{p}$ gelten würde: $ab \in \mathfrak{a} \cdot \mathfrak{b} \subseteq \mathfrak{p}$.

Die Bedingung ist aber auch hinreichend, da sie, angewendet auf Hauptideale $\mathfrak{a} = (a)$ und $\mathfrak{b} = (b)$, unmittelbar $\mathfrak{p}$ als Primideal kennzeichnet:

$$\text{Aus } a \cdot b \in \mathfrak{p} \quad \text{und} \quad a \notin \mathfrak{p}$$

folgt zunächst

$$(a \cdot b) = (a)\,(b) \subseteq \mathfrak{p} \quad \text{und} \quad (a) \not\subseteq \mathfrak{p}$$

und damit gemäß unserer Bedingung

$$(b) \subseteq \mathfrak{p}, \text{ d. h. } b \in \mathfrak{p}.$$

qed.

Man kann natürlich diese Aussage wieder durch mehrfache Anwendung auf ein Produkt von mehr als zwei Idealen verallgemeinern und erhält:

Aus $\mathfrak{p} \supseteq \mathfrak{a}_1 \mathfrak{a}_2 \ldots \mathfrak{a}_n$ *folgt* $\mathfrak{p} \supseteq \mathfrak{a}_i$ *für wenigstens ein* i.

Für die Erklärung der Teilbarkeit von Idealen stehen uns als Vorbild die beiden Kriterien S(42.2) und S(42.5) zur Verfügung. Die ihnen entsprechenden Verallgemeinerungen werden sich jedoch als im allgemeinen nicht gleichwertig erweisen, und wir legen daher fest[1]):

Definition **D (43.3)**

a) *Ein Ideal* $\mathfrak{b}$ *aus* $\mathfrak{R}$ *heißt Teiler eines Ideals* $\mathfrak{a}$ *aus* $\mathfrak{R}$, *wenn* $\mathfrak{b} \supseteq \mathfrak{a}$ *gilt. Entsprechend nennt man* $\mathfrak{a}$ *ein Vielfaches von* $\mathfrak{b}$.

b) *Ein Ideal* $\mathfrak{b}$ *aus* $\mathfrak{R}$ *heißt Faktor eines Ideals* $\mathfrak{a}$ *aus* $\mathfrak{R}$, *wenn in* $\mathfrak{R}$ *ein Ideal* $\mathfrak{x}$ *existiert mit* $\mathfrak{a} = \mathfrak{b} \cdot \mathfrak{x}$. *Nur in diesem Falle schreibt man* $\mathfrak{b} | \mathfrak{a}$.

Nach unseren obigen Bemerkungen folgt aus $\mathfrak{a} = \mathfrak{b} \cdot \mathfrak{x}$ stets $\mathfrak{b} \supseteq \mathfrak{a}$; ein Faktor ist also erst recht Teiler. Das Umgekehrte ist aber nicht immer richtig.

So gilt z. B. in $\mathfrak{R} = \Gamma[x]$ wohl $(2, x) \supset (x)$, dagegen existiert kein Ideal $\mathfrak{x}$ aus $\mathfrak{R}$, das die Gleichung $(x) = (2, x) \cdot \mathfrak{x}$ erfüllt. Letzteres ergibt sich etwa so: Wegen $(x) \subseteq \mathfrak{x}$ müßte man $\mathfrak{x}$ in der Form $\mathfrak{x} = (g, x)$ mit geeignetem $g \in \Gamma$ ansetzen. Dann enthielte aber $(x) = (2, x)\, \mathfrak{x} = (2, x)\, (g, x)$ das Element $2g$, woraus $g = 0$ folgt. Es gilt jedoch $(x) \neq (2, x)\, (x)$ wegen $x \notin (2x, x^2)$. Allerdings werden wir uns hier bald insbesondere solchen Ringen zuwenden, wo auch jeder Teiler ein Faktor ist.

Zunächst ist jedoch festzustellen, daß sowohl a) als auch b) sinnvolle Übertragungen des Teilbarkeitsbegriffes für Elemente auf Ideale darstellen. So gelten z. B. alle grundlegenden Teilbarkeits-

---

1) D (43.3) entspricht der meist üblichen Festlegung dieser Begriffe, die sich historisch aus der Betrachtung von Ringen herausgebildet hat, in denen (wie z. B. in Hauptidealringen) beide Auffassungen gleichwertig sind. Ohne Zweifel wäre es glücklicher gewesen, nicht nur das Zeichen „$\mathfrak{b}|\mathfrak{a}$", sondern auch die Bezeichnung „Teiler" für die schärfere Begriffsbildung b) zu verwenden, zumal für a) ohnehin „umfassendes Ideal" zur Verfügung steht.

Übrigens erklärt sich aus D (43.3a) die Bezeichnung „teilerlos" für maximale Ideale. Ebenso entspringt aus ihr die Sprechweise „a teilt b" für „$a \ni b$" als Abkürzung von „a teilt (b), d. h. $a \supseteq (b)$".

relationen aus F(39.2), jedoch mit Ausnahme der Umkehrung von F(39.2e), sowohl für $\mathfrak{b} \supseteq \mathfrak{a}$ als auch für $\mathfrak{b} \mid \mathfrak{a}$ (vgl. Aufg. 3).

Auch stimmen beide Beziehungen für den Fall, daß die auftretenden Ideale $\mathfrak{a} = (a)$ und $\mathfrak{b} = (b)$ Hauptideale von $\mathfrak{R}$ sind, mit der Teilbarkeitsaussage $b \mid a$ für die erzeugenden Elemente überein.

Wir übertragen schließlich auch den Begriff des größten gemeinsamen Teilers gemäß D(42.6), verstehen also unter $\mathfrak{d}$ ein Ideal mit den Eigenschaften

(*) $\mathfrak{d} \supseteq \mathfrak{a}_1, \ldots, \mathfrak{d} \supseteq \mathfrak{a}_n$,

(**) aus $\mathfrak{t} \supseteq \mathfrak{a}_1, \ldots, \mathfrak{t} \supseteq \mathfrak{a}_n$ folgt $\mathfrak{t} \supseteq \mathfrak{d}$.

Das legt den *größten gemeinsamen Teiler* $\mathfrak{d}$ der Ideale $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_n$ als das (mengenmäßig) kleinste Ideal fest, welches $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_n$ umfaßt. Also ist $\mathfrak{d}$ das von der Menge $\mathfrak{a}_1 \cup \mathfrak{a}_2 \cup \ldots \cup \mathfrak{a}_n$ erzeugte Ideal[1]), d. h. (vgl. Aufg. 9 von § 28)

$$\mathfrak{d} = (\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_n) = \mathfrak{a}_1 + \mathfrak{a}_2 + \ldots + \mathfrak{a}_n.$$

Damit ist es möglich, unter $(\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_n)$ die Aufforderung zu verstehen, den größten gemeinsamen Teiler dieser Ideale zu bilden, ohne mit der früher festgelegten Bedeutung dieser Bezeichnung als Idealerzeugung in Widerspruch zu geraten.

Entsprechend ist in Analogie zu D(42.8) das *kleinste gemeinsame Vielfache* der Ideale $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_n$ ein Ideal $\mathfrak{f}$ mit den Eigenschaften

(†) $\mathfrak{f} \subseteq \mathfrak{a}_1, \ldots, \mathfrak{f} \subseteq \mathfrak{a}_n$,

(††) aus $\mathfrak{v} \subseteq \mathfrak{a}_1, \ldots, \mathfrak{v} \subseteq \mathfrak{a}_n$ folgt $\mathfrak{v} \subseteq \mathfrak{f}$.

---

1) Die Analogie zum zweiten Teil der Behauptung von S(42.7) ist offensichtlich. Dagegen gilt der erste Teil dieses Satzes in beliebigen Ringen auch dann nicht mehr, wenn die auftretenden Ideale $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ Hauptideale sind. So ist z. B. in $\Gamma[x]$ mit $\mathfrak{a}_1 = (x)$ und $\mathfrak{a}_2 = (2)$, also $d \cong (x, 2) \cong 1$:

$$(\mathfrak{a}_1, \mathfrak{a}_2) = (x, 2) \neq (d) = (1).$$

Wir bemerken noch, daß die Begriffsbildung des größten gemeinsamen Teilers für Ideale wesentlich auf D(43.3a) beruht. Zwar kann man auch von D(43.3b) ausgehend analogisieren und etwa einen „größten gemeinsamen Faktor $\mathfrak{g}$" von $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$ mit den E.genschaften

$$\mathfrak{g} \mid \mathfrak{a}_1, \ldots, \mathfrak{g} \mid \mathfrak{a}_n$$
$$\text{aus } \mathfrak{h} \mid \mathfrak{a}_1, \ldots, \mathfrak{h} \mid \mathfrak{a}_n \text{ folgt } \mathfrak{h} \mid \mathfrak{g}$$

erklären, doch braucht im allgemeinen ein solches Ideal $\mathfrak{g}$ gar nicht zu existieren, geschweige denn mit $\mathfrak{a}_1 + \ldots + \mathfrak{a}_n$ übereinzustimmen.

Damit ist das kleinste gemeinsame Vielfache $\mathfrak{f}$ das (mengenmäßig) größte Ideal, welches in den Idealen $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_n$ enthalten ist, was genau erfüllt wird von

$$\mathfrak{f} = \mathfrak{a}_1 \cap \mathfrak{a}_2 \cap \ldots \cap \mathfrak{a}_n.$$

Eine entsprechende Bezeichnungsübertragung $\mathfrak{f} = [\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_n]$ schafft eine oft sehr praktische Symbolik für den Durchschnitt von Idealen.

Für die angestrebte Zerlegung von Idealen in Produkte von Primidealen sind nun einschränkende Voraussetzungen über die betrachteten Ringe erforderlich, und zwar verlangen wir die Gültigkeit der beiden folgenden Sätze:

Teilerkettensatz **S (43.4)**

Jede Kette echter Teiler $\mathfrak{a}_1 < \mathfrak{a}_2 < \mathfrak{a}_3 < \ldots$ *von Idealen aus* $\mathfrak{R}$ *bricht nach endlich vielen Gliedern ab.*

Faktorsatz **S (43.5)**

Jeder Teiler $\mathfrak{b}$ *eines Ideales* $\mathfrak{a}$ *von* $\mathfrak{R}$ *ist auch Faktor von* $\mathfrak{a}$, *d.h.:*

$$\textit{Aus } \mathfrak{b} \supseteqq \mathfrak{a} \textit{ folgt } \mathfrak{b} \mid \mathfrak{a}.$$

In der Tat wird sich mit Hilfe dieser beiden Sätze der Zerlegungssatz für Ideale ähnlich wie im § 40 der Zerlegungssatz für Elemente ableiten lassen[1]). Dazu stellen wir noch einige Aussagen bereit, die übrigens bereits allein aus dem Faktorsatz folgen:

---

1) Vergleicht man die damit an den Ring $\mathfrak{R}$ gestellten Forderungen mit denjenigen, die im § 40 den Beweis des Zerlegungssatzes für Elemente ermöglichten, so ist die Analogie zwischen dem Teilerkettensatz für Elemente und dem Teilerkettensatz für Ideale offensichtlich (vgl. auch Aufg. 5).

Jedoch kann auch der Faktorsatz als Übertragung des Hauptsatzes über den größten gemeinsamen Teiler für Elemente angesehen werden. Allerdings muß man dazu den Begriff des größten gemeinsamen Teilers für Elemente zum Begriff des „größten gemeinsamen Faktors" für Ideale (vgl. Fußnote auf Seite 195) in Korrespondenz setzen, also dessen Existenz und Übereinstimmung mit der Summe der betreffenden Ideale verlangen. Diese Forderung ist aber mit dem Faktorsatz gleichwertig:

Seine Gültigkeit besagt ja gerade die Äquivalenz von „Faktor" und „Teiler", und für den größten gemeinsamen Teiler von Idealen ist die genannte Forderung stets erfüllt. Umgekehrt folgt aus ihr der Faktorsatz, denn aus $\mathfrak{b} \supset \mathfrak{a}$ ergibt sich unter Verwendung der Existenz des größten gemeinsamen Faktors $\mathfrak{g}$ von $\mathfrak{a}$ und $\mathfrak{b}$ und seiner Darstellung $\mathfrak{g} = \mathfrak{a} + \mathfrak{b}$ die Beziehung $\mathfrak{b}\mathfrak{x} = \mathfrak{a}$; als Faktor von $\mathfrak{a}$ erfüllt $\mathfrak{g}$ nämlich $\mathfrak{g}\mathfrak{x} = \mathfrak{a}$, und aus $\mathfrak{g} = \mathfrak{a} + \mathfrak{b}$ und $\mathfrak{b} \supseteqq \mathfrak{a}$ folgt $\mathfrak{g} = \mathfrak{b}$.

Satz **S (43.6)**

Gilt im Ring $\mathfrak{R}$ *der Faktorsatz, so ist jedes von* (o) *verschiedene Ideal von* $\mathfrak{R}$ *Faktor eines von* (o) *verschiedenen Hauptideals von* $\mathfrak{R}$.
Diese Aussage wird auch als spezieller Faktorsatz bezeichnet.

Beweis

Es sei $\mathfrak{b}$ ein Ideal von $\mathfrak{R}$ und $b \neq o$ ein Element von $\mathfrak{b}$. Dann gilt auch $\mathfrak{b} \subseteq (b)$, woraus bereits nach dem Faktorsatz $\mathfrak{b} \mid b$ folgt. qed.

Wichtig für unsere Überlegungen ist die Tatsache, daß sich daraus die Eindeutigkeit des Komplementärfaktors $\mathfrak{x}$ zu einem Faktor $\mathfrak{b} \neq (o)$ von $\mathfrak{a}$ ergibt[1]:

Folgerung **F (43.7)**

Gilt im Ring $\mathfrak{R}$ *der spezielle Faktorsatz, so folgt aus* $\mathfrak{b}\mathfrak{x} = \mathfrak{b}\mathfrak{y}$ *und* $\mathfrak{b} \neq (o)$ *stets* $\mathfrak{x} = \mathfrak{y}$.

Beweis

Nach dem speziellen Faktorsatz existiert ein Ideal $\mathfrak{z}$ mit $\mathfrak{b}\mathfrak{z} = (b) \neq (o)$. Multipliziert man $\mathfrak{b}\mathfrak{x} = \mathfrak{b}\mathfrak{y}$ mit diesem Ideal $\mathfrak{z}$, so ergibt sich

$$(b)\mathfrak{x} = (b)\mathfrak{y}.$$

Alle Elemente von $(b)\mathfrak{x}$ haben die Gestalt

$$\Sigma (br_i)x_i = b\Sigma r_i x_i = bx$$

mit $r_i \in \mathfrak{R}$, $x_i \in \mathfrak{x}$, also $x = \Sigma r_i x_i \in \mathfrak{x}$. Entsprechend haben alle Elemente von $(b)\mathfrak{y}$ die Form by mit $y \in \mathfrak{y}$. Also existiert zu beliebigem $x \in \mathfrak{x}$ ein $y \in \mathfrak{y}$ mit $bx = by$, und wegen $b \neq o$ ist $x = y$, d. h. $\mathfrak{x} \subseteq \mathfrak{y}$. Analog folgt $\mathfrak{y} \subseteq \mathfrak{x}$. qed.

Aus F (43.7) ergibt sich nun, daß auch in Ringen mit Faktorsatz die Primideale durch die Eigenschaften ausgezeichnet sind, die wir für die Primideale eines Hauptidealringes bereits in S (42.11) festgestellt haben:

---

1) Die Rolle, die F (43.7) im folgenden und insbesondere im Beweis von S (43.9 bc) spielt, wird verständlich, wenn man bedenkt, daß in der Teilbarkeitslehre für Elemente die Eindeutigkeit des Komplementärteilers x in $a = bx$ $(b \neq o)$ auf Grund unserer allgemeinen Voraussetzung der Nullteilerfreiheit stets gewährleistet ist.

Satz **S (43.8)**

Gilt in einem Ring $\mathfrak{R}$ *der Faktorsatz, so sind für ein Ideal* $\mathfrak{p}$ *mit* $(o) < \mathfrak{p} < \mathfrak{R}$ *folgende Aussagen gleichwertig:*

a) $\mathfrak{p}$ *ist Primideal von* $\mathfrak{R}$;

b) $\mathfrak{p}$ *ist maximales Ideal von* $\mathfrak{R}$;

c) $\mathfrak{p}$ *ist unzerlegbares Ideal von* $\mathfrak{R}$.

Beweis

Aus a) folgt c): Ist nämlich ein Primideal $\mathfrak{p} = \mathfrak{a}\mathfrak{b}$ Produkt zweier Ideale, so gilt wie stets $\mathfrak{p} \subseteq \mathfrak{a}$ und $\mathfrak{p} \subseteq \mathfrak{b}$; andererseits folgt aus S(43.2) $\mathfrak{p} \supseteq \mathfrak{a}$ oder $\mathfrak{p} \supseteq \mathfrak{b}$. Im ersten Falle gilt $\mathfrak{p} = \mathfrak{a}$, also $\mathfrak{p} = \mathfrak{a}\mathfrak{R} = \mathfrak{a}\mathfrak{b}$ und damit gemäß F(43.7) $\mathfrak{b} = \mathfrak{R}$, im zweiten Falle entsprechend $\mathfrak{p} = \mathfrak{b}$ und damit $\mathfrak{a} = \mathfrak{R}$.

Aus c) folgt b), da sich aus $\mathfrak{p} \subseteq \mathfrak{b} \subseteq \mathfrak{R}$ nach S(43.5) $\mathfrak{p} = \mathfrak{b}\mathfrak{x}$ ergibt, also aus der Unzerlegbarkeit von $\mathfrak{p}$ entweder $\mathfrak{b} = \mathfrak{p}$ oder $\mathfrak{b} = \mathfrak{R}$.

Aus b) folgt a), da gemäß unseren Überlegungen am Ende von § 34 die Maximalität stets die Primidealeigenschaft nach sich zieht. qed.

Nunmehr kommen wir zu dem grundlegenden Satz über die[1])

Zerlegung von Idealen in Primideale **S (43.9)**

In einem Ring $\mathfrak{R}$ *sind Teilerkettensatz und Faktorsatz hinreichend für folgende Aussagen:*

a) *Jedes Ideal* $\mathfrak{a}$ *aus* $\mathfrak{R}$ *(mit* $(o) < \mathfrak{a} < \mathfrak{R}$*) besitzt wenigstens einen Primteiler, d. h., es existiert ein Primideal* $\mathfrak{p}$ *mit* $\mathfrak{a} \subseteq \mathfrak{p} < \mathfrak{R}$.

b) *Jedes Ideal* $\mathfrak{a}$ *aus* $\mathfrak{R}$ *(mit* $(o) < \mathfrak{a} < \mathfrak{R}$*) besitzt eine Darstellung als Produkt endlich vieler, nicht notwendig verschiedener Primteiler:*

$$\mathfrak{a} = \mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_n.$$

c) *Diese Zerlegung ist eindeutig bis auf die Reihenfolge der Faktoren.*

Ein Ring, in dem eine solche **Zerlegung in Prim-Ideale** *für jedes seiner Ideale existiert, heißt ZPI-Ring.*

---

1) Eine Übersicht über die Beweisgänge findet sich ebenfalls am Ende des Bandes.

Beweis

a) Für ein Primideal $\mathfrak{a}$ ist die Behauptung trivial. Ist jedoch $\mathfrak{a}$ kein Primideal, so ist $\mathfrak{a}$ auch kein maximales Ideal; dann existiert also ein Ideal $\mathfrak{a}_1$ mit

$$\mathfrak{a} < \mathfrak{a}_1 < \mathfrak{R}.$$

Dieselbe Schlußweise auf $\mathfrak{a}_1$ angewendet usw. liefert nach endlich vielen Schritten einen Primteiler $\mathfrak{a}_n = \mathfrak{p}$, da andernfalls eine unendliche Kette echter Teiler entstehen würde im Widerspruch zum Teilerkettensatz.

b) Nach dem soeben Bewiesenen existiert zu jedem Ideal $\mathfrak{a}$ wenigstens ein Primideal $\mathfrak{p}_1$ mit $\mathfrak{R} > \mathfrak{p}_1 \geqq \mathfrak{a}$. Für $\mathfrak{a} = \mathfrak{p}_1$ ist nichts mehr zu zeigen; andernfalls existiert zufolge des Faktorsatzes ein Ideal $\mathfrak{a}_1 < \mathfrak{R}$ mit

$$\mathfrak{a} = \mathfrak{p}_1 \mathfrak{a}_1.$$

Entsprechend schließt man: Entweder ist $\mathfrak{a}_1$ Primideal und damit eine Zerlegung von $\mathfrak{a}$ gefunden, oder es existiert ein Primideal $\mathfrak{p}_2$ mit $\mathfrak{R} > \mathfrak{p}_2 > \mathfrak{a}_1$, also wieder nach dem Faktorsatz ein Ideal $\mathfrak{a}_2 < \mathfrak{R}$ mit

$$\mathfrak{a}_1 = \mathfrak{p}_2 \mathfrak{a}_2, \quad \text{also} \quad \mathfrak{a} = \mathfrak{p}_1 \mathfrak{p}_2 \mathfrak{a}_2.$$

Um auf diese Weise zu der behaupteten Zerlegung

$$\mathfrak{a} = \mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_n$$

zu gelangen, müssen wir noch nachweisen, daß das Verfahren nach endlich vielen Schritten abbricht.

Das ergibt sich aber aus dem Teilerkettensatz, denn die Ideale $\mathfrak{a} = \mathfrak{a}_0, \mathfrak{a}_1, \mathfrak{a}_2, \dots$ bilden eine Kette echter Teiler. Nach Konstruktion ist nämlich $\mathfrak{a}_{i-1} \leqq \mathfrak{a}_i$; wäre nun $\mathfrak{a}_{i-1} = \mathfrak{a}_i$, so folgte aus $\mathfrak{a}_{i-1} = \mathfrak{p}_i \mathfrak{a}_i$ und $\mathfrak{a}_{i-1} = \mathfrak{a}_i = \mathfrak{R}\mathfrak{a}_i$ wegen F(43.7) $\mathfrak{R} = \mathfrak{p}_i$ im Widerspruch zu $\mathfrak{R} > \mathfrak{p}_i$.

c) Es ist zu zeigen:

$$\text{Aus } \mathfrak{a} = \mathfrak{p}_1 \mathfrak{p}_2 \dots \mathfrak{p}_n = \mathfrak{q}_1 \mathfrak{q}_2 \dots \mathfrak{q}_m$$

folgt $n = m$ und $\mathfrak{p}_i = \mathfrak{q}_i$ bei geeigneter Numerierung.

Ohne Beschränkung der Allgemeinheit sei $n \leq m$. Im Falle $n = 1$ ergibt sich die Behauptung sofort aus der Unzerlegbarkeit des Primideales $\mathfrak{p}_1$. Wir schließen weiter durch vollständige Induktion von $n - 1$ auf n.

Nach der Verallgemeinerung von S (43.2) folgt aus $\mathfrak{p}_n \geqq \mathfrak{q}_1 \mathfrak{q}_2 \cdots \mathfrak{q}_m$ jedenfalls $\mathfrak{p}_n \geqq \mathfrak{q}_i$ für wenigstens ein i, wobei wir durch geeignete Numerierung $\mathfrak{p}_n \geqq \mathfrak{q}_m$ erreichen können. Nach S (43.8) ergibt sich daraus $\mathfrak{p}_n = \mathfrak{q}_m$, und wir gelangen unter Verwendung von F (43.7) zu

$$\mathfrak{p}_1 \mathfrak{p}_2 \cdots \mathfrak{p}_{n-1} = \mathfrak{q}_1 \mathfrak{q}_2 \cdots \mathfrak{q}_{m-1}.$$

Nach Induktionsvoraussetzung gilt aber $n-1 = m-1$, also $n = m$ und $\mathfrak{p}_i = \mathfrak{q}_i$ für $i = 1, 2, \ldots, n-1$, was die Behauptung zeigt[1]). qed.

Als Beispiele für Ringe, die Teilerkettensatz und Faktorsatz erfüllen und damit ZPI-Ringe sind, kann man natürlich sofort die Hauptidealringe heranziehen. Sie sind jedoch dafür in dem Sinne weniger interessant, als sie auch ZPE-Ringe sind und in ihnen die Teilbarkeitslehre für Elemente und Ideale entsprechend der Ausführungen in § 42 nur zwei verschiedene Auffassungen der gleichen Sachverhalte darstellen.

Die eigentliche Bedeutung der Existenz und Eindeutigkeit der Zerlegung in Primideale erweist sich erst für solche Ringe, die nicht mehr ZPE-Ringe sind. Nicht zuletzt ist es mit ihrer Hilfe möglich, die Gesetzmäßigkeiten nicht-eindeutiger Zerlegungen in Primelemente zu erfassen. Einen Einblick in solche Überlegungen geben wir im letzten Teil dieses Paragraphen, indem wir Ringe der Gestalt $\Gamma + \Gamma\sqrt{k}$ für geeignetes k betrachten.

Allerdings ist prinzipiell zu bemerken, daß bei solchen Untersuchungen konkreter Ringe das entscheidende Problem zunächst darin besteht festzustellen, ob in ihnen die in S (43.9) eingehenden Voraussetzungen auch wirklich erfüllt sind. Dies ist oft mit erheblichen Schwierigkeiten verbunden, und es ist dabei sehr vorteilhaft, andere Kriterien zu besitzen, die mit Teilerkettensatz und Faktor-

---

1) Vergleicht man — am besten an Hand der beigefügten Übersichten — die in den Eindeutigkeitsbeweis eingehenden Aussagen, so fällt folgendes auf: Während die in F (40.13) ausgesprochene Eigenschaft der Primelemente nur unter geeigneten Voraussetzungen über den betrachteten Ring erfüllt ist, gilt die ihr entsprechende Aussage S (43.2) über Primideale allgemein. Dagegen ist die hier benötigte Maximalität und Unzerlegbarkeit der Primideale wieder nur in geeigneten Ringen erfüllt im Gegensatz zu der ihr entsprechenden Unzerlegbarkeit der Primelemente, die stets vorliegt und daher in der Übersicht zu § 40 auch gar nicht in Erscheinung tritt.
Der Grund für diesen Unterschied liegt in der Verschiedenartigkeit der Begriffsbildungen, die sich beim Primelement auf eine Aussage über die möglichen Teiler, beim Primideal auf die Nullteilerfreiheit des Restklassenringes bezieht.

satz gleichwertig sind. Auch bei der Behandlung der angekündigten Beispiele werden wir uns auf sie stützen.

Satz **S (43.10)**

Faktorsatz und spezieller Faktorsatz sind gleichwertige Forderungen.

Beweis

Wie wir bereits in S(43.6) nachwiesen, folgt aus dem Faktorsatz der spezielle Faktorsatz.

Umgekehrt gelte in $\mathfrak{R}$ der spezielle Faktorsatz, d. h., jedes Ideal $\mathfrak{b} \neq (o)$ ist Faktor eines Hauptideals (b): $\mathfrak{b}\mathfrak{x} = (b)$. Aus $\mathfrak{b} \supseteq \mathfrak{a}$ folgt dann durch Multiplikation mit $\mathfrak{x}$

$$(b) = \mathfrak{b}\mathfrak{x} \supseteq \mathfrak{a}\mathfrak{x}.$$

Jedes Element $y \in \mathfrak{a}\mathfrak{x}$ liegt daher in (b), kann also in der Form $y = bc$ mit geeignetem $c \in \mathfrak{R}$ geschrieben werden. Durchläuft y alle Elemente von $\mathfrak{a}\mathfrak{x}$, so bilden die zugehörigen Elemente c ein Ideal $\mathfrak{c}$ von $\mathfrak{R}$. Mit $c_1 \in \mathfrak{c}$ und $c_2 \in \mathfrak{c}$, also $bc_1 \in \mathfrak{a}\mathfrak{x}$ und $bc_2 \in \mathfrak{a}\mathfrak{x}$, liegt nämlich wegen $bc_1 - bc_2 = b(c_1 - c_2) \in \mathfrak{a}\mathfrak{x}$ auch $c_1 - c_2$ in $\mathfrak{c}$; entsprechend folgt aus $c \in \mathfrak{c}$ wegen $b(rc) = r(bc) \in \mathfrak{a}\mathfrak{x}$ auch $rc \in \mathfrak{c}$.

Mit diesem Ideal $\mathfrak{c}$ gilt nun

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

Es ist nämlich $(b)\,\mathfrak{c} \supseteq \mathfrak{a}\mathfrak{x}$ nach Konstruktion von $\mathfrak{c}$ klar. Umgekehrt gilt für alle Elemente von $(b)\,\mathfrak{c}$

$$\Sigma(br_i) \cdot c_i = b\Sigma r_i c_i = bc = y \in \mathfrak{a}\mathfrak{x}.$$

Durch Einsetzen von $(b) = \mathfrak{b}\mathfrak{x}$ erhält man somit

$$\mathfrak{b}\mathfrak{x} \cdot \mathfrak{c} = \mathfrak{a}\mathfrak{x}, \text{ also } \mathfrak{b}\mathfrak{c} = \mathfrak{a},$$

letzteres nach F(43.7). qed.

Satz **S (43.11)**

Teilerkettensatz und Basissatz für Ideale sind gleichwertige Forderungen.

Beweis

Aus dem Teilerkettensatz folgt der Basissatz, d. h., jedes Ideal $\mathfrak{a}$ von $\mathfrak{R}$ kann von endlich vielen Elementen erzeugt werden (vgl.

D(28.10)). Ist nämlich a_1 ein beliebiges Element von $\mathfrak{a}$, so ist entweder $(a_1) = \mathfrak{a}$ oder $(a_1) < \mathfrak{a}$. Im zweiten Falle existiert in $\mathfrak{a}$ ein Element $a_2 \notin (a_1)$, und man erhält

$$(a_1) < (a_1, a_2) \leqq \mathfrak{a}.$$

Entsprechend gilt entweder $(a_1, a_2) = \mathfrak{a}$ oder

$$(a_1) < (a_1, a_2) < (a_1, a_2, a_3) \leqq \mathfrak{a}.$$

Wegen der Gültigkeit des Teilerkettensatzes endet dieses Verfahren nach endlich vielen Schritten mit

$$\mathfrak{a} = (a_1, a_2, \ldots, a_n).$$

Hat umgekehrt jedes Ideal von $\mathfrak{R}$ eine endliche Basis, so stimmen in jeder Kette (echter oder unechter) Teiler

$$\mathfrak{a}_1 \leqq \mathfrak{a}_2 \leqq \mathfrak{a}_3 \leqq \ldots$$

von einem gewissen Index N ab alle weiteren Glieder überein:

$$\mathfrak{a}_N = \mathfrak{a}_{N+1} = \ldots.$$

Dazu betrachtet man die Menge $\mathfrak{a}$ aller Elemente, die in wenigstens einem Ideal $\mathfrak{a}_i$ dieser Kette enthalten sind. $\mathfrak{a}$ ist Ideal von $\mathfrak{R}$, denn aus $x \in \mathfrak{a}$ und $y \in \mathfrak{a}$ folgt $x - y \in \mathfrak{a}$ wegen $x \in \mathfrak{a}_i$ und $y \in \mathfrak{a}_k$, also sowohl $x \in \mathfrak{a}_l$ als auch $y \in \mathfrak{a}_l$ und damit $x - y \in \mathfrak{a}_l$ mit $l = \mathrm{Max}(i, k)$, und ebenso aus $x \in \mathfrak{a}$ und $\mathfrak{r} \in \mathfrak{R}$ auch $rx \in \mathfrak{a}$ wegen $x \in \mathfrak{a}_i$, also $rx \in \mathfrak{a}_i$[1]).

Nach Voraussetzung hat $\mathfrak{a}$ eine endliche Basis

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

und jedes a_ν liegt in einem Ideal $\mathfrak{a}_{i(\nu)}$ der Kette und damit in allen folgenden. Ist also $N = \mathrm{Max}(i(1), \ldots, i(n))$, so gilt:

$$a_1 \in \mathfrak{a}_N, \ldots, a_n \in \mathfrak{a}_N, \quad \text{also} \quad \mathfrak{a} \leqq \mathfrak{a}_N.$$

Wegen $\mathfrak{a}_{N+1} \leqq \mathfrak{a}$, $\mathfrak{a}_{N+2} \leqq \mathfrak{a}, \ldots$ folgt daraus die Behauptung.

qed.

Beispiele und Anwendungen **B (43.12)**

a) *In jedem Ring* $\mathfrak{R} = \Gamma + \Gamma\sqrt{k}$ *gilt der Basissatz, wobei* k *wie in* B(26.4) *eine von einer Quadratzahl verschiedene ganze Zahl ist.*

1) Mit anderen Worten: Die Vereinigungsmenge einer Kette einander enthaltender Ideale ist selbst Ideal.

Zum Beweis betrachten wir ein beliebiges Ideal $\mathfrak{a}$ von $\mathfrak{R}$, und $\alpha = a + b\sqrt{k}$ durchlaufe alle Elemente von $\mathfrak{a}$. Die dabei auftretenden ganzen Zahlen b bilden ein Ideal $\mathfrak{g}_b$ von Γ; es liegen nämlich mit b und b' auch $b - b'$ in $\mathfrak{g}_b$ wegen $\alpha - \alpha' = (a + b\sqrt{k}) - (a' + b'\sqrt{k}) \in \mathfrak{a}$ und mit b ersichtlich seine ganzzahligen Vielfachen. Insbesondere gibt es ein $\mathfrak{g}_b$ erzeugendes Element b_1 (Γ ist Hauptidealring!), und wir wählen aus allen $\alpha \in \mathfrak{a}$ ein solches aus, in dem b_1 auftritt:

$$\alpha_1 = a_1 + b_1\sqrt{k}.$$

(Dabei braucht $a_1 \in \Gamma$ durchaus nicht eindeutig bestimmt zu sein.)

Eine entsprechende Überlegung wenden wir auf alle diejenigen Elemente aus $\mathfrak{a}$ an, welche die Form $\alpha = a + 0\sqrt{k}$ haben. Sie bilden ebenfalls ein Ideal $\mathfrak{g}_a$ von Γ, das von a_2 erzeugt werde. Es ist also auch

$$\alpha_2 = a_2 + 0\sqrt{k}$$

ein Element aus $\mathfrak{a}$.

Die so konstruierten Elemente α_1 und α_2 erzeugen aber bereits das ganze Ideal $\mathfrak{a}$:

$$\mathfrak{a} = (\alpha_1, \alpha_2).$$

Ist nämlich $\alpha = a + b\sqrt{k}$ ein beliebiges Element aus $\mathfrak{a}$, so gilt $b \in \mathfrak{g}_b$, also $b = gb_1$ mit $g \in \Gamma$ und damit:

$$\alpha - g\alpha_1 = (a + b\sqrt{k}) - (ga_1 + gb_1\sqrt{k}) = (a - ga_1) + 0\sqrt{k}.$$

Weiterhin ist $a - ga_1 \in \mathfrak{g}_a$, d. h. $a - ga_1 = ha_2$ mit $h \in \Gamma$. Somit ergibt sich die Behauptung aus

$$\alpha - g\alpha_1 - h\alpha_2 = (a - ga_1) - ha_2 = 0.$$

b) Tatsächlich haben wir damit nicht nur gezeigt, daß jedes Ideal $\mathfrak{a}$ von $\mathfrak{R} = \Gamma + \Gamma\sqrt{k}$ zwei Elemente α_1 und α_2 als Idealbasis, d. h. als Erzeugendensystem des als $\mathfrak{R}$-Modul aufgefaßten Ideals $\mathfrak{a}$ besitzt

$$\mathfrak{a} = \mathfrak{R}\alpha_1 + \mathfrak{R}\alpha_2,$$

sondern daß jedes $\alpha \in \mathfrak{a}$ sogar ganzzahlig aus α_1 und α_2 linear kombiniert werden kann, also α_1 und α_2 sogar ein Erzeugendensystem von $\mathfrak{a}$ als Γ-Modul bilden:

$$\mathfrak{a} = \Gamma\alpha_1 + \Gamma\alpha_2.$$

Dabei haben die Elemente α_1 und α_2 die Gestalt

$$\alpha_1 = a_1 + b_1\sqrt{k}, \quad \alpha_2 = a_2,$$

wobei für die auftretenden ganzen Zahlen a_1, b_1 und a_2 überdies die folgenden Beziehungen gelten:

$$b_1 | a_1,\ b_1 | a_2 \quad \text{und} \quad k \equiv \left(\frac{a_1}{b_1}\right)^2 \bmod \frac{a_2}{b_1}.$$

Einmal folgt nämlich aus $a_2 \sqrt{k} \in \mathfrak{a}$, d. h.

$$a_2 \sqrt{k} = g\left(a_1 + b_1 \sqrt{k}\right) + h a_2 \quad \text{mit} \quad g \in \Gamma,\ h \in \Gamma$$

zunächst $a_2 = g b_1$ und damit weiter $a_1 = -h b_1$ wegen

$$0 = g a_1 + h a_2 = g a_1 + h g b_1.$$

Damit sind die behaupteten Teilbarkeitsbeziehungen bereits bewiesen und $\frac{a_1}{b_1}$ bzw. $\frac{a_2}{b_1}$ in Wirklichkeit ganze Zahlen.

Zum anderen ergibt sich die behauptete Kongruenz aus $\left(a_1 + b_1 \sqrt{k}\right) \sqrt{k} \in \mathfrak{a}$, d. h.

$$a_1 \sqrt{k} + b_1 k = g\left(a_1 + b_1 \sqrt{k}\right) + h a_2 \quad \text{mit} \quad g \in \Gamma,\ h \in \Gamma;$$

denn aus dieser Gleichung erhält man $a_1 = g b_1$ und weiter

$$b_1 k = g a_1 + h a_2 = \frac{a_1^2}{b_1} + h a_2, \quad \text{also} \quad k = \left(\frac{a_1}{b_1}\right)^2 + h \frac{a_2}{b_1}.$$

Die Kenntnis dieser Beziehungen ist für das Arbeiten mit den Idealen von $\mathfrak{R}$ oft sehr vorteilhaft. Überdies ist ihr Bestehen nicht nur notwendig, sondern auch hinreichend dafür, daß der Γ-Modul

$$\Gamma\left(a_1 + b_1 \sqrt{k}\right) + \Gamma a_2$$

sogar ein Ideal von $\mathfrak{R}$ ist (vgl. Aufg. 6). Damit haben wir eine allgemeine Kennzeichnung der Ideale von $\mathfrak{R}$ als Γ-Moduln gefunden. Sie gewinnt noch an Übersichtlichkeit, wenn man ohne Beschränkung der Allgemeinheit nur den offensichtlich besonders einfachen Spezialfall $b_1 = 1$ betrachtet; auf die damit erfaßten Ideale lassen sich nämlich alle anderen durch Ausklammern des gemeinsamen Faktors b_1 aus allen Idealelementen zurückführen:

$$\mathfrak{a} = \left(a_1 + b_1 \sqrt{k},\ a_2\right) = (b_1)\left(\frac{a_1}{b_1} + \sqrt{k},\ \frac{a_2}{b_1}\right) = (b_1)\,\mathfrak{a}'.$$

c) *In Ringen* $\mathfrak{R} = \Gamma + \Gamma\sqrt{k}$ *gilt der spezielle Faktorsatz, wenn die ganze Zahl* k *keine quadratischen Faktoren enthält und* $k \not\equiv 1 \bmod 4$ *ist*[1]).

Nach unserer letzten Bemerkung kann jedes Ideal $\mathfrak{a}$ von $\mathfrak{R}$ in der Gestalt $\mathfrak{a} = (b_1)\mathfrak{a}'$ angegeben werden. Existiert nun zu $\mathfrak{a}'$ ein Faktor $\mathfrak{x}$ mit $\mathfrak{a}'\mathfrak{x} = (c)$, so gilt offenbar auch $\mathfrak{a}\mathfrak{x} = (b_1)\mathfrak{a}'\mathfrak{x} = (b_1)(c) = (b_1 c)$. Wir können uns also beim Beweis des speziellen Faktorsatzes auf den Fall $b_1 = 1$ beschränken, zeigen also die Existenz eines geeigneten Faktors für das Ideal $(a_1 + \sqrt{k}, a_2)$. In der Tat gilt:

$$(a_1 + \sqrt{k}, a_2)(a_1 - \sqrt{k}, a_2) = (a_2).$$

Multipliziert man nämlich das Produkt aus, so erhält man

$$(a_1^2 - k,\ a_1 a_2 + a_2\sqrt{k},\ a_1 a_2 - a_2\sqrt{k},\ a_2^2).$$

Hier kann man wegen $a_1^2 \equiv k\,(a_2)$ aus jedem Element den Faktor a_2 herausziehen und erhält:

$$(a_2)\left(\frac{a_1^2 - k}{a_2},\ a_1 + \sqrt{k},\ a_1 - \sqrt{k},\ a_2\right).$$

Damit bleibt nur nachzuweisen, daß der rechtsstehende Faktor das Ideal $\mathfrak{R} = (1)$ ist. Jedenfalls enthält er das Ideal

$$\left(\frac{a_1^2 - k}{a_2},\ 2a_1,\ a_2\right) = (d),$$

welches auch von dem größten gemeinsamen Teiler d der drei auftretenden ganzen Zahlen erzeugt werden kann. Wir vollenden den Beweis, in dem wir $d \cong 1$ zeigen.

Andernfalls würde nämlich mindestens eine Primzahl p in d aufgehen, was sich aber als unmöglich herausstellen wird: Aus $p \mid d$ folgt zunächst

$$p \mid a_2 \quad \text{und} \quad p \left| \frac{a_1^2 - k}{a_2}, \quad \text{also} \quad p^2 \mid a_1^2 - k. \right.$$

---

1) Diese Einschränkungen werden aus der algebraischen Zahlentheorie verständlich: In einem quadratischen Zahlkörper $\mathfrak{P} + \mathfrak{p}\sqrt{k}$ gibt es nämlich genau einen Oberring von $\Gamma + \Gamma\sqrt{k}$ (den sog. Ring der ganzen algebraischen Zahlen dieses Zahlkörpers), der nicht nur den Basissatz, sondern auch den Faktorsatz erfüllt. Die angegebenen Voraussetzungen sind gerade kennzeichnend dafür, daß dieser Oberring mit $\Gamma + \Gamma\sqrt{k}$ selbst übereinstimmt.

Im Falle $p \neq 2$ gilt darüber hinaus $p \mid a_1$ und damit $p^2 \mid k$, was bereits im Widerspruch dazu steht, daß k als quadratfrei vorausgesetzt wurde. Im Falle $p = 2$ erhalten wir $4 \mid a_1^2 - k$, also $a_1^2 \equiv k \bmod 4$. Durch Einsetzen von 0, 1, 2, 3 für a_1 ergibt sich $k \equiv 0$ oder $k \equiv 1 \bmod 4$, was zufolge unserer beiden Voraussetzungen über k ebenfalls ausgeschlossen ist.

d) Zufolge unseren allgemeinen Überlegungen gilt mit dem Basissatz auch der Teilerkettensatz und mit dem speziellen Faktorsatz auch der Faktorsatz, so daß wir erhalten:

Ist k quadratfrei und $k \not\equiv 1$ (4), so ist $\mathfrak{R} = \Gamma + \Gamma\sqrt{k}$ ZPI-Ring.

Damit sind etwa die in B(40.20) behandelten Ringe $\Gamma + \Gamma\sqrt{-1}$, $\Gamma + \Gamma\sqrt{-5}$ und $\Gamma + \Gamma\sqrt{26}$ ZPI-Ringe. Der erste ist (Aufg. 3 von § 40) euklidischer Ring und damit sogar ZPE-Ring, während in den beiden anderen zufolge der angegebenen Elementzerlegungen die Zerlegung in Primelemente nicht eindeutig ist.

e) Wie solche wesentlich verschiedenen Elementzerlegungen zustande kommen, läßt sich nun mit Hilfe der eindeutigen Idealzerlegung verständlich machen.

Wir stellen zunächst allgemein fest, daß jede Zerlegung eines Ideals $\mathfrak{a}$ eines ZPI-Ringes $\mathfrak{R}$ in ein Produkt beliebiger Ideale

$$\mathfrak{a} = \mathfrak{a}_1 \mathfrak{a}_2 \ldots \mathfrak{a}_r$$

durch geeignete Zusammenfassung der Primfaktoren aus der eindeutigen Zerlegung

$$\mathfrak{a} = \mathfrak{p}_1 \mathfrak{p}_2 \ldots \mathfrak{p}_n$$

von $\mathfrak{a}$ in ein Produkt von Primidealen entsteht und umgekehrt. Damit erhalten wir aber auch (bis auf Einheiten) einen Überblick über sämtliche möglichen Zerlegungen eines Elementes $a \in \mathfrak{R}$ in ein Produkt von beliebigen Elementen aus $\mathfrak{R}$. Der Elementzerlegung

$$a \cong a_1 a_2 \ldots a_r$$

entspricht nämlich eindeutig eine Zerlegung des Hauptideals (a) in ein Produkt von Hauptidealen

$$(a) = (a_1)\,(a_2) \ldots (a_r).$$

Man findet daher alle möglichen Zerlegungen von a durch solche Zusammenfassungen der Primfaktoren $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_n$ von (a), die zu

Hauptidealen führen; insbesondere entstehen also alle möglichen Zerlegungen von a in ein Produkt von Primelementen durch Zusammenfassung von $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_n$ zu solchen Hauptidealen, die von Primelementen aus $\mathfrak{R}$ erzeugt werden.

f) Zur Veranschaulichung betrachten wir diese Verhältnisse am konkreten Beispiel des Ringes $\mathfrak{R} = \Gamma + \Gamma\sqrt{-5}$.

In ihm haben wir (vgl. B (40.20 b)) für die Zahl 6 folgende wesentlich verschiedene Zerlegungen in Primelemente gefunden:

$$6 \cong 2 \cdot 3 \cong (1+\sqrt{-5}) \cdot (1-\sqrt{-5}).$$

Die entsprechende Beziehung

$$(6) = (2) \cdot (3) = (1+\sqrt{-5}) \cdot (1-\sqrt{-5})$$

für Hauptideale muß also aus der Zerlegung

$$(6) = \mathfrak{p}_1 \mathfrak{p}_2 \ldots \mathfrak{p}_n$$

von (6) in Primideale durch jeweils geeignete Zusammenfassung der Primfaktoren entstehen.

Wir bestimmen diese Primideale der Reihe nach. Unter ihnen tritt ein $\mathfrak{p}_1$ auf, das Faktor von (2) und von einem der beiden Ideale $(1+\sqrt{-5})$ und $(1-\sqrt{-5})$ ist, also die betreffenden Ideale umfaßt. Wir bilden daher zunächst die Ideale

$$(2) + (1+\sqrt{-5}) = (2, 1+\sqrt{-5}),$$

$$(2) + (1-\sqrt{-5}) = (2, 1-\sqrt{-5})$$

und stellen fest, daß sie beide übereinstimmen, denn es gilt

$$(2, 1+\sqrt{-5}) \ni 1 \cdot 2 + (-1) \cdot (1+\sqrt{-5}) = 1 - \sqrt{-5},$$

$$(2, 1-\sqrt{-5}) \ni 1 \cdot 2 + (-1) \cdot (1-\sqrt{-5}) = 1 + \sqrt{-5}.$$

Dieses Ideal $(2, 1+\sqrt{-5}) = (2, 1-\sqrt{-5})$ ist maximal und fällt daher mit dem Primfaktor $\mathfrak{p}_1$ von (6) zusammen, den wir nunmehr mit $\mathfrak{p}$ bezeichnen. Der Restklassenring von $\mathfrak{R}$ mod $(2, 1-\sqrt{-5})$ ist nämlich ein Körper, denn es ist

$$a + b\sqrt{-5} \equiv a + b \equiv \begin{cases} 0 \\ 1 \end{cases} \bmod (1-\sqrt{-5}, 2)$$

und damit

$$\mathfrak{R}/(2, 1-\sqrt{-5}) \xleftrightarrow{\sim} \Gamma/(2).$$

Entsprechend bilden wir die Ideale

$$(3) + (1+\sqrt{-5}) = (3, 1+\sqrt{-5}),$$
$$(3) + (1-\sqrt{-5}) = (3, 1-\sqrt{-5}),$$

die sich als zwei voneinander verschiedene maximale Ideale herausstellen, womit wir zwei weitere Primfaktoren $\mathfrak{q}'$ und $\mathfrak{q}''$ von (6) gefunden haben. Analog dem eben durchgeführten Schluß erhält man nämlich

$$\mathfrak{R}/(3, 1+\sqrt{-5}) \xleftrightarrow{\sim} \Gamma/(3),$$
$$\mathfrak{R}/(3, 1-\sqrt{-5}) \xleftrightarrow{\sim} \Gamma/(3).$$

Würden nun diese Ideale gleich sein, also etwa $(3, 1+\sqrt{-5})$ auch das Element $1-\sqrt{-5}$ enthalten, so wäre

$$3-(1+\sqrt{-5})-(1-\sqrt{-5}) = 1 \in (3, 1+\sqrt{-5})$$

im Widerspruch zur darüberstehenden Isomorphie.

In der Tat haben wir damit alle Primteiler von (6) gefunden. Es ist nämlich

$$(6) = \mathfrak{p} \cdot \mathfrak{p} \cdot \mathfrak{q}' \cdot \mathfrak{q}''$$

wegen

$$\mathfrak{p}\mathfrak{p} = (2, 1+\sqrt{-5})(2, 1-\sqrt{-5})$$
$$= (4, 2+2\sqrt{-5}, 2-2\sqrt{-5}, 6) = (2)$$

$$\mathfrak{q}'\mathfrak{q}'' = (3, 1+\sqrt{-5})(3, 1-\sqrt{-5})$$
$$= (9, 3+3\sqrt{-5}, 3-3\sqrt{-5}, 6) = (3)$$

oder aber auch wegen

$$\mathfrak{p}\mathfrak{q}' = (2, 1+\sqrt{-5})(3, 1+\sqrt{-5})$$
$$= (6, 2+2\sqrt{-5}, 3+3\sqrt{-5}, -4+2\sqrt{-5}) = (1+\sqrt{-5})$$

$$\mathfrak{p}\mathfrak{q}'' = (2, 1-\sqrt{-5})(3, 1-\sqrt{-5})$$
$$= (6, 2-2\sqrt{-5}, 3-3\sqrt{-5}, -4-2\sqrt{-5}) = (1-\sqrt{-5}).$$

Andere als diese Zusammenfassungen der vier Primfaktoren von (6) liefern keine Hauptideale, also keine anderen Elementzerlegungen von 6. In jeder der noch möglichen Zusammenfassungen tritt nämlich wenigstens $\mathfrak{p}$ oder $\mathfrak{q}'$ oder $\mathfrak{q}''$ als einzelner Faktor auf. Diese Ideale sind aber keine Hauptideale in $\mathfrak{R}$, was wir etwa für $\mathfrak{p}$ zeigen: Wäre

$$(2, 1+\sqrt{-5}) = (a + b\sqrt{-5}),$$

so müßte $a + b\sqrt{-5}$ in 2 aufgehen, also gemäß unserem grundlegenden Satz für die Norm eines Produktes in B(40.20) auch $N(a+b\sqrt{-5})$ in $N(2)$. Wegen $N(2) = 4$ kommt für $N(a+b\sqrt{-5})$ also nur 1, 2 oder 4 in Frage. Im ersten Falle wäre $a + b\sqrt{-5} \cong 1$ im Widerspruch zu $\mathfrak{R} \neq (2, 1+\sqrt{-5})$, im letzten $a + b\sqrt{-5} \cong 2$ im Widerspruch zu $(2) \neq (2, 1+\sqrt{-5})$; Elemente mit der Norm 2 sind aber in $\mathfrak{R}$ gar nicht vorhanden.

g) Wir kehren wieder zum allgemeinen Fall zurück und überlegen uns, welche Bedeutung der in e) angegebene Zusammenhang zwischen der Idealerzeugung von (a) und den Elementzerlegungen von a für die Teilbarkeitslehre der Elemente eines ZPI-Ringes hat.

Erinnern wir uns daran, daß sich in ZPE-Ringen alle diesbezüglichen Fragestellungen auf Größenbeziehungen zwischen den Exponenten der Primelemente in der eindeutigen Zerlegung der Elemente zurückführen ließen. *Ein ähnlicher Sachverhalt liegt nun auch in ZPI-Ringen $\mathfrak{R}$ vor, wenn man nur von den Elementen zu den von ihnen erzeugten Hauptidealen übergeht und die Exponentensysteme der zugehörigen eindeutigen Zerlegung in Primideale betrachtet.* Auch dort ist ein Element b genau dann Teiler eines Elementes a, wenn in den Idealzerlegungen[1])

$$(a) = \prod_{\mathfrak{p}} \mathfrak{p}^{\alpha_\mathfrak{p}} \quad \text{und} \quad (b) = \prod_{\mathfrak{p}} \mathfrak{p}^{\beta_\mathfrak{p}}$$

für die Exponenten $\beta_\mathfrak{p} \leqq \alpha_\mathfrak{p}$ gilt.

---

1) Wir bedienen uns wieder einer Schreibweise der Idealzerlegungen als formal-unendliche Potenzprodukte über alle Primideale von $\mathfrak{R}$ mit $(o) \subset \mathfrak{p} \subset \mathfrak{R}$, in denen fast alle Faktoren $\mathfrak{p}^0 = \mathfrak{R}$ sind:

$$\mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{\alpha_\mathfrak{p}}.$$

Dadurch wird jedem Ideal $\mathfrak{a}$ von $\mathfrak{R}$ eineindeutig ein Exponentensystem ganzer Zahlen $\alpha_\mathfrak{p} \geqq 0$ mit $\alpha_\mathfrak{p} = 0$ für fast alle $\mathfrak{p}$ zugeordnet. Natürlich gilt für das Einheitsideal $\mathfrak{R} = \mathfrak{p}^0$, während für das Nullideal die formale Festlegung $(o) = \prod \mathfrak{p}^\infty$ sinnvoll ist.

Allerdings brauchen nicht allen Exponentensystemen $\beta_\mathfrak{p}$ mit $\beta_\mathfrak{p} \leqq \alpha_\mathfrak{p}$ Elemente b von $\mathfrak{R}$ als Teiler von a zu entsprechen, denn das zugehörige Ideal

$$\mathfrak{b} = \prod_{\mathfrak{p}} \mathfrak{p}^{\beta_\mathfrak{p}}$$

muß ja nicht Hauptideal sein. Dann liegt also nur ein „idealer Teiler" $\mathfrak{b} \mid (a)$ oder auch (vgl. Fußnote auf S. 194) $\mathfrak{b} \mid a$ vor, dem kein „wirklicher Teiler" $b \in \mathfrak{R}$ von a entspricht. Dies trifft im allgemeinen auch für die Primteiler $\mathfrak{p}$ von (a) zu, die also nur „ideale Primteiler" von a zu sein brauchen, wie dies auch in unserem obigen Beispiel der Fall ist.

Dieses Ergebnis ist der historische Ansatzpunkt der Idealtheorie, woraus sich auch die Bezeichnung „Ideal" erklärt. So stieß KUMMER bei seinen Bemühungen, den sog. großen FERMATschen Satz zu beweisen, auf gewisse Ringe aus komplexen Zahlen, in denen die Zerlegung in Primelemente sich als nicht eindeutig erwies. Dies veranlaßte ihn zur Einführung sog. idealer Zahlen, die zunächst rein abstrakt zu den Ringelementen hinzugenommen wurden und eine eindeutige Zerlegung jedes Elements ermöglichten[1]). KRONECKER und DEDEKIND führten allgemein[2]) statt der abstrakten idealen Zahlen die von letzterem als „Ideale" bezeichneten Gesamtheiten von solchen Ringelementen ein, die jeweils eine bestimmte ideale oder wirkliche Zahl als Teiler haben.

So entstand der heutige Idealbegriff, der die ihm einst zugrunde liegenden idealen Zahlen durch konkret faßbare Untermengen des betrachteten Ringes ersetzt.

Wir wissen bereits, daß die Bedeutung dieser Begriffsbildungen weit über die Teilbarkeitslehre in ZPI-Ringen und somit über die an ihrem Anfang stehenden Betrachtungen der algebraischen Zahlentheorie hinausgeht. Heute kann man die Idealtheorie schon als selbständige mathematische Disziplin ansprechen[3]), deren unter

---

1) E. E. KUMMER: Zur Theorie der komplexen Zahlen, Crelle's Journ. f. d. reine und angew. Math. 35 (1847) S. 319.

2) L. KRONECKER:: Grundzüge einer arithmetischen Theorie der algebraischen Größen, Crelle's Journ. 92 (1882) S. 1. Diese Arbeit stellt eine Veröffentlichung seiner schon ab 1858 mündlich weitergegebenen Ergebnisse dar.
R. DEDEKIND: X. Supplement der 2. Aufl. von L. DIRICHLETS Vorlesungen über Zahlentheorie, Braunschweig 1871.

3) Einen diesbezüglichen zusammenfassenden Bericht gibt W. KRULL: Idealtheorie, Ergebn. d. Mathem. u. ihrer Grenzgeb. 4 (1935) Heft 3.

weit allgemeineren Voraussetzungen gültigen Strukturaussagen in den verschiedensten Gebieten Anwendung finden. Als Beispiel sei etwa die für die Eliminationstheorie und für die algebraische Geometrie grundlegende Idealtheorie in Polynomringen genannt.

Aufgaben zu § 43

1. Man zeige das Distributivgesetz der Idealmultiplikation:
$$\mathfrak{a} \cdot (\mathfrak{b} + \mathfrak{c}) = \mathfrak{a} \cdot \mathfrak{b} + \mathfrak{a} \cdot \mathfrak{c}.$$
2. Es gilt für die Multiplikation von Idealen mit endlicher Basis:
$$(a_1, \ldots, a_n) \cdot (b_1, \ldots, b_m) = (a_1 b_1, \ldots, a_j b_k, \ldots, a_n b_m).$$
3. Man beweise die F(39.2) entsprechenden Aussagen für die Beziehungen „$\mathfrak{b} \supseteq \mathfrak{a}$“ und „$\mathfrak{b} \mid \mathfrak{a}$“ (mit Ausnahme der Umkehrung von F(39.2e)).
4. Man beweise unter Verwendung von Aufgabe 1:
$$(\mathfrak{a}, \mathfrak{b}) \cdot [\mathfrak{a}, \mathfrak{b}] \subseteq \mathfrak{a} \cdot \mathfrak{b}.$$
5. Welche Beziehungen bestehen zwischen dem Teilerkettensatz für Elemente und dem für Ideale?
6. In $\mathfrak{R} = \Gamma + \Gamma\sqrt{k}$ ist der Γ-Modul $\Gamma(a_1 + b_1\sqrt{k}) + \Gamma a_2$ Ideal, falls a_1, b_1 und a_2 den im Text angegebenen Bedingungen genügen.
7. Entsprechend B(43.12f) betrachte man die Zerlegung der Zahl 21 in dem Ring $\Gamma + \Gamma\sqrt{-5}$.

LÖSUNGEN DER AUFGABEN

Zu § 24

1. Zur Kontrolle für den Leser geben wir einige naheliegende Beispiele an:

   a) Sämtliche Gruppen sind erst recht Halbgruppen.

   b) Die in B(2.1 c) genannten multiplikativen Gruppen der von Null verschiedenen rationalen, reellen bzw. komplexen Zahlen werden durch Hinzunahme der Null zu nichtregulären Halbgruppen. Sie sind Beispiele für Halbgruppen, in denen ein einziges Element, nämlich die Null, unlösbare Gleichungen $ax = b$ bzw. $ya = b$ liefert, etwa $0x = b$ mit $b \neq 0$.

   c) Die natürlichen Zahlen bilden bezüglich der Multiplikation eine abelsche reguläre Halbgruppe mit Einselement. (Es gibt also reguläre Halbgruppen, die nicht Gruppen sind; vgl. Aufg. 7 in § 1.)

   d) Die ganzen Zahlen bilden entsprechend einschließlich der Null eine nichtreguläre Halbgruppe, ausschließlich der Null eine reguläre Halbgruppe. Das gleiche gilt für alle ganzzahligen Vielfachen einer festen ganzen Zahl.

   e) Die in B(2.4) genannten Matrizen vom Typ (n, n) bilden bezüglich der Matrizenmultiplikation eine nichtabelsche und nichtreguläre Halbgruppe mit Einselement. Durch Nullsetzen aller Elemente einer festen Zeile entstehen Untermengen, die ebenfalls multiplikative Halbgruppen sind. Entsprechendes gilt für Spalten.

   f) Die Restklassen ganzer Zahlen mod m bilden bezüglich der Multiplikation endliche nichtreguläre abelsche Halbgruppen mit Einselement. Genau die primen Restklassen besitzen ein eindeutig bestimmtes Inverses.

2. a) Der Durchschnitt zweier Untermengen von $\mathfrak{M}$ ist wieder eine eindeutig bestimmte Untermenge von $\mathfrak{M}$ ($M\,I$). Die Durchschnittsbildung ist assoziativ ($M\,II$) und kommutativ ($M\,IV$). Die gesamte Menge $\mathfrak{M}$ spielt wegen $\mathfrak{M} \cap \mathfrak{A} = \mathfrak{A}$ für alle Untermengen $\mathfrak{A} \subseteq \mathfrak{M}$ die Rolle des Einselementes.

   b) Ebenso erfüllt die Vereinigungsbildung die Axiome $M\,I$, $M\,II$ und $M\,IV$. Dem Einselement entspricht wegen $\mathfrak{A} \cup \emptyset = \mathfrak{A}$ für alle $\mathfrak{A} \subseteq \mathfrak{M}$ die leere Menge $\emptyset$.

3. Wir wählen etwa

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \quad \text{und} \quad B = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix}.$$

   Dann besitzt die Gleichung $YA = B$ mit

$$Y = \begin{pmatrix} 0 & y_{12} \\ 1 & y_{22} \end{pmatrix}$$

   bei beliebigen y_{12} und y_{22} unendlich viele Lösungen, während die Gleichung

$$AX = \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} = B$$

   unlösbar ist.

Zu § 25

1. Man führe zweimal vollständige Induktion mit folgenden Ansätzen durch:

$$\left(\sum_{\nu=1}^{n} a_\nu\right) \cdot b = \sum_{\nu=1}^{n} a_\nu \cdot b, \text{ Induktion nach } n;$$

$$\left(\sum_{\nu=1}^{n} a_\nu\right)\left(\sum_{\mu=1}^{m} b_\mu\right) = \sum_{\nu=1}^{n} \sum_{\mu=1}^{m} a_\nu \cdot b_\mu, \text{ Induktion nach } m.$$

2. *M I:* Das Produkt zweier Nichtnullteiler ist ebenfalls Nichtnullteiler. Damit nämlich ein Produkt $a \cdot b$ linker Nullteiler ist, also $(a \cdot b) \cdot c = o$ mit $c \neq o$ gilt, ist wegen $a \cdot (b \cdot c) = o$ notwendig, daß wenigstens a oder b linker Nullteiler ist. Entsprechend schließt man dafür, daß $a \cdot b$ rechter Nullteiler ist.

   M II: Das Assoziativgesetz gilt für alle Ringelemente.

   M III:* Die Eindeutigkeit der Division durch Nichtnullteiler ergibt sich aus S(25.8).

3. Wir benutzen, daß in einem Schiefkörper jedes von o verschiedene Element ein Inverses hat. Aus $a \cdot b = o$ mit $a \neq o$ folgt dann durch Multiplikation mit a^{-1} von links, daß $b = o$ ist, während sich aus $b \neq o$ entsprechend $a = o$ ergibt. Ein Produkt kann also nur verschwinden, wenn ein Faktor verschwindet.

4. Die Behauptung ergibt sich aus der Gleichwertigkeit von *M III* und *M III** im endlichen Falle.

Zu § 26

1. a) $|a_{ik}| = 0$ ist gleichbedeutend mit linearer Abhängigkeit der Spalten von $|a_{ik}|$, also mit

$$\sum_k a_{ik} \lambda_k = 0 \quad \text{für alle } i,$$

wobei wenigstens ein $\lambda_k \neq 0$ ist.

(a_{ik}) ist linker Nullteiler genau dann, wenn eine Matrix (b_{kl}) mit

$$\sum_k a_{ik} b_{kl} = 0 \quad \text{für alle } i \text{ und } l$$

existiert, wobei wenigstens ein $b_{kl} \neq 0$ ist.

Offensichtlich sind beide Bedingungen äquivalent. Damit ist das angegebene Kriterium für linke Nullteiler bereits gezeigt. Der entsprechende Ansatz mit der linearen Abhängigkeit der Zeilen von $|a_{ik}|$ ergibt den Nachweis des Kriteriums auch für rechte Nullteiler.

b) Ist $|a_{ik}| \neq 0$, so läßt sich (vgl. B(2.4c)) ein zweiseitiges Inverses zu (a_{ik}) angeben. Existiert umgekehrt zu (a_{ik}) ein Linksinverses (a^*_{ik}) bzw. Rechtsinverses (a^{**}_{ik}), so ist wegen

$$|a^*_{ik}| \cdot |a_{ik}| = 1 \quad \text{bzw.} \quad |a_{ik}| \cdot |a^{**}_{ik}| = 1$$

die Determinante $|a_{ik}| \neq 0$. Diese Umkehrung läßt sich übrigens auch unter Verwendung von a) aus S(25.9) schließen.

c) Da entweder $|a_{ik}| = 0$ oder $|a_{ik}| \neq 0$ ist, ergibt sich c) unmittelbar aus den Beweisen von a) und b).

Man beachte, daß der erste Schluß bei b) und damit natürlich auch die Aussage c) wesentlich von der Körpereigenschaft von Δ abhängt. So gibt es etwa in $\mathfrak{M}_n(\Gamma)$ Matrizen, z. B.

$$\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix},$$

mit von 0 verschiedener Determinante, die trotzdem in $\mathfrak{M}_n(\Gamma)$ kein Inverses besitzen, obwohl sie keine Nullteiler sind.

2. Die Aussagen a) und b) sind trivial. Dagegen gilt ebenfalls die Besonderheit c), daß es im Restklassenring mod m keine Elemente gibt, die nicht Nullteiler sind und kein Inverses besitzen:
Wir wissen bereits, daß zu primen Restklassen $[a]$ mod m mit $(a, m) = 1$ Inverse existieren. Eine Restklasse $[a]$ mod m mit $(a, m) = d > 1$ ist aber wegen $[a] \cdot \left[\frac{m}{d}\right] = [d \cdot a'] \cdot \left[\frac{m}{d}\right] = [a'm] = [0]$ Nullteiler, da $\frac{m}{d}$ eine ganze Zahl kleiner als m ist. Damit ergibt sich die Behauptung nach S(25.9).

3. $m = 2$:

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

$m = 3$:

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$m = 4$:

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$m = 5$:

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$m = 6$:

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

·	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

4. Der Körper besitzt notwendigerweise ein Nullelement o, ein Einselement e und ein weiteres Element a. Damit sind die Strukturtafeln bereits wie folgt festgelegt:

$+$	o	e	a
o	o	e	a
e	e		
a	a		

$\cdot$	o	e	a
o	o	o	o
e	o	e	a
a	o	a	

Da die Elemente bezüglich der Addition einen Modul sowie die von o verschiedenen Elemente bezüglich der Multiplikation eine Gruppe bilden müssen, ist wegen F(7.10) die weitere Ausfüllung der Tafeln eindeutig festgelegt:

$+$	o	e	a
o	o	e	a
e	o	a	o
a	a	o	e

$\cdot$	o	e	a
o	o	o	o
e	o	e	a
a	o	a	e

Von allen Körperaxiomen bleibt nach Konstruktion nur noch das distributive Gesetz D nachzuweisen. Dieses läßt sich durch explizites Nachrechnen rasch verifizieren, zumal von den 3^3 prinzipiellen Möglichkeiten eine Reihe wegen der Kommutativität der Addition gleichwertig und wegen des Auftretens von o und e fast alle trivial sind. Wir haben damit zugleich gezeigt, daß die Strukturtafeln aller Körper mit drei Elementen bis auf die Bezeichnung übereinstimmen. So ist auch der Restklassenring mod 3 von dieser Struktur.

5. Entsprechend 4. sind die Strukturtafeln wie folgt zu beginnen:

$+$	o	e	a	b
o	o	e	a	b
e	e			
a	a			
b	b			

$\cdot$	o	e	a	b
o	o	o	o	o
e	o	e	a	b
a	o	a		
b	o	b		

Für die multiplikative Körpergruppe kommt nach F(7.10) nur die zyklische Gruppe $\mathfrak{Z}_3$ in Frage, dagegen existieren für die additive Gruppe nach Aufg. 6 von § 7 zwei Möglichkeiten:

$\mathfrak{Z}_4$

$+$	o	e	a	b
o	o	e	a	b
e	e	a	b	o
a	a	b	o	e
b	b	o	e	a

$\mathfrak{V}_4$

$+$	o	e	a	b
o	o	e	a	b
e	e	o	b	a
a	a	b	o	e
b	b	a	e	o

$\cdot$	o	e	a	b
o	o	o	o	o
e	o	e	a	b
a	o	a	b	e
b	o	b	e	a

Man überzeugt sich durch ein Beispiel, daß mit der linken Tafel das Distributivgesetz nicht erfüllt wäre:

$$b = a + e = ae + ab = a(e + b) = a \cdot o = o.$$

Dagegen ist, wie der Leser selbst nachprüfen möge, mit der mittleren Tafel das Distributivgesetz gültig.
Zugleich ist damit wieder nachgewiesen, daß es für die Strukturtafeln eines Körpers mit vier Elementen nur eine Möglichkeit gibt.

6. Der identische Automorphismus ε von $\mathfrak{G}$ ist offensichtlich das Einselement von $\mathfrak{R}$. Es sei σ ein Endomorphismus von $\mathfrak{G}$, zu dem in $\mathfrak{R}$ ein Endomorphismus σ^{-1} mit $\sigma\sigma^{-1} = \sigma^{-1}\sigma = \varepsilon$ existiert. Wir zeigen, daß dann σ eine eineindeutige Abbildung von $\mathfrak{G}$ auf sich, also ein Automorphismus von $\mathfrak{G}$ ist.

   a) Wäre σ nicht eineindeutig, so gäbe es wenigstens zwei voneinander verschiedene Elemente a und b aus $\mathfrak{G}$ mit $a^\sigma = b^\sigma$. Aus $\sigma\sigma^{-1} = \varepsilon$ folgt dann $(a^\sigma)\sigma^{-1} = (b^\sigma)\sigma^{-1}$, also $a = b$ im Widerspruch zur Voraussetzung.

   b) Jedes $a \in \mathfrak{G}$ tritt als Bild eines Elementes $b \in \mathfrak{G}$ auf, nämlich von $b = a\sigma^{-1}$, da aus $\sigma\sigma^{-1} = \varepsilon$ folgt $b^\sigma = (a\sigma^{-1})^\sigma = a$.

   Umgekehrt ist selbstverständlich jeder Automorphismus von $\mathfrak{G}$ ein Endomorphismus, der ein zweiseitiges Inverses besitzt, da nach S(15.5) die Menge aller Automorphismen von $\mathfrak{G}$ eine Gruppe ist.

7. Endomorphismen eines einfachen Moduls $\mathfrak{G}$ können nur entweder Automorphismen oder der Nullendomorphismus σ_0 sein. Als Kern einer homomorphen Abbildung (vgl. S(18.8)) kommt nämlich nach der Voraussetzung über $\mathfrak{G}$ nur der Nullmodul (gibt nach F(18.12a) einen Automorphismus) oder der gesamte Modul (gibt nach F(18.12b) die Nullabbildung) in Frage. Nach S(15.5) bilden also alle von dem Nullelement σ_0 von $\mathfrak{R}$ verschiedenen Elemente von $\mathfrak{R}$ eine multiplikative Gruppe, d. h., $\mathfrak{R}$ ist Körper. Dieser Körper ist kommutativ, da ein einfacher Modul gemäß S(20.6) endlich und zyklisch ist und damit nach B(15.4) eine abelsche Automorphismengruppe hat.

Zu § 27

1. Unter den verschiedenen Möglichkeiten, den Beweis zu führen, greifen wir die beiden folgenden heraus:

   a) Wir setzen $n_1 e \cdot n_2 e = (ne) \cdot b$ mit $n = n_1$, $a = e$ und $b = n_2 e$ und erhalten wegen $(ne) \cdot b = n(a \cdot b)$

$$n_1 e \cdot n_2 e = n_1 (e \cdot n_2 e).$$

   Das Einselement e reproduziert aber das Ringelement $n_2 e$, so daß unter Verwendung der Regel *II* aus F(3.8) folgt

$$n_1(e \cdot n_2 e) = n_1(n_2 e) = (n_1 \cdot n_2)e.$$

   b) Wir verwenden die Formel $a \cdot (nb) = (na) \cdot b$ und setzen $a = n_1 e$, $n = n_2$ und $b = e$:

$$n_1 e \cdot n_2 e = n_2(n_1 e) \cdot e.$$

   Damit ergibt sich wie oben

$$n_2(n_1 e) \cdot e = n_2(n_1 e) = (n_2 \cdot n_1)e$$

und daraus wegen $n_2 \cdot n_1 = n_1 \cdot n_2$ die Behauptung.

2. Man legt fest, unter $a^{\frac{m}{n}}$ ein Element $d \in \mathfrak{R}$ zu verstehen, für welches $d^n = a^m$ gilt. Es existiert jedenfalls dann, wenn ein $c \in \mathfrak{R}$ mit $c^n = a$ vorhanden ist, nämlich $d = c^m$ wegen

$$d^n = (c^m)^n = (c^n)^m = a^m,$$

wofür man natürlich auch

$$d = a^{\frac{m}{n}} = \left(\sqrt[n]{a}\right)^m = \sqrt[n]{a^m}$$

schreiben kann. Es gilt dann in der Tat nach den Potenzgesetzen mit ganzzahligen Exponenten:

I: $a^{\frac{m_1}{n_1}} a^{\frac{m_2}{n_2}} = a^{\frac{m_1}{n_1} + \frac{m_2}{n_2}} = a^{\frac{m_1 n_2 + m_2 n_1}{n_1 n_2}}$,

denn aus $d_1^{n_1} = a^{m_1}$ und $d_2^{n_2} = a^{m_2}$ folgt

$$(d_1 d_2)^{n_1 n_2} = d_1^{n_1 n_2} d_2^{n_1 n_2} = a^{m_1 n_2} a^{m_2 n_1} = a^{m_1 n_2 + m_2 n_1}.$$

II: $\left(a^{\frac{m_1}{n_1}}\right)^{\frac{m_2}{n_2}} = a^{\frac{m_1 m_2}{n_1 n_2}}$,

denn aus $d_1^{n_1} = a^{m_1}$ und $d_2^{n_2} = d_1^{m_2}$ folgt

$$d_2^{n_2 n_1} = (d_1^{m_2})^{n_1} = (d_1^{n_1})^{m_2} = (a^{m_1})^{m_2} = a^{m_1 m_2}.$$

III: $a^{\frac{m}{n}} b^{\frac{m}{n}} = (ab)^{\frac{m}{n}}$ für vertauschbare Elemente a und b, denn aus $d_1^n = a^m$ und $d_2^n = b^m$ folgt

$$(d_1 d_2)^n = d_1^n d_2^n = a^m b^m = (ab)^m.$$

Für die inhaltliche Bedeutung dieser Formeln bringen wir ein Beispiel: So besagt

$$\sqrt[n]{a} \cdot \sqrt[n]{b} = \sqrt[n]{ab},$$

daß das Produkt zweier Ringelemente, die n-te Wurzeln aus a bzw. b sind, ein Ringelement ergibt, welches n-te Wurzel aus ab ist. Dagegen braucht dieses Produkt natürlich nicht mit einer willkürlich vorgegebenen n-ten Wurzel von ab aus $\mathfrak{R}$ übereinzustimmen. So folgt etwa aus $\sqrt{4} \cdot \sqrt{9} = \sqrt{36}$, daß $(+2)(-3) = -6$ eine Quadratwurzel aus 36 ist, die natürlich nicht gleich der Quadratwurzel $+6$ aus 36 ist.

3. Der angegebene Körper hat die Charakteristik 2.

4. Das folgt aus $a + a = 2a = o$.

5. Man erhält durch vollständige Induktion nach m unter Verwendung von F(27.4) unmittelbar

$$(a_1 + a_2 + \ldots + a_m)^p = a_1^p + a_2^p + \ldots + a_m^p,$$

$$(a_1 + a_2 + \ldots + a_m)^{p^n} = a_1^{p^n} + a_2^{p^n} + \ldots + a_m^{p^n}.$$

6. Wir fassen die prime Restklassengruppe mod p als multiplikative Gruppe des Restklassenkörpers mod p auf. Jedes seiner Elemente $[a] \neq [0]$ läßt sich als natürliches Vielfaches

$$[a] = a[1] = [1] + [1] + \ldots + [1]$$

gewinnen. Potenzierung mit p ergibt nach Aufg. 4:

$$[a]^p = [1]^p + \ldots + [1]^p = [1] + \ldots + [1] = [a],$$

also wegen der Existenz von $[a]^{-1}$:

$$[a]^{p-1} = [1]$$

oder in Kongruenzschreibweise

$$a^{p-1} \equiv 1 \bmod p.$$

7. Es sei x ein beliebiges Element des Restklassenkörpers mod p. Für zwei Elemente x_1 und x_2, die p-te Wurzel aus x sind, für die also $x_1^p = x_2^p = x$ gilt, folgt nach F(27.4)

$$x_1^p - x_2^p = (x_1 - x_2)^p = 0.$$

Wegen der Nullteilerfreiheit ist $x_1 = x_2$. Andererseits erfüllt x selbst $x^p = x$ nach Aufg. 6.

Zu § 28

1. Sämtliche Untermoduln $\mathfrak{m}$ von Γ sind uns bereits nach Aufgabe 14 von § 5 bekannt. Nur diese kommen als Unterringe in Frage. Als additive zyklische Gruppen bestehen sie aus allen ganzzahligen Vielfachen gm einer nichtnegativen ganzen Zahl m, gestatten also die Darstellung:

$$\mathfrak{m} = \langle m \rangle = \Gamma m = m\Gamma.$$

Alle diese Untermoduln sind aber auch Unterringe, denn die Bedingung (2) aus S(28.2) ist erfüllt, da das Produkt zweier ganzzahliger Vielfachen von m wieder ein solches ist. Sie sind darüber hinaus Ideale von Γ. Multipliziert man nämlich ein ganzzahliges Vielfaches von m mit einer beliebigen ganzen Zahl, erhält man wieder ein ganzzahliges Vielfaches von m.

2. Alle Ideale $\mathfrak{m}$ von Γ bestehen nach Aufg. 1 aus allen ganzzahligen Vielfachen einer nichtnegativen ganzen Zahl m. Es gilt also

$$\mathfrak{m} = (m) = \Gamma m.$$

Man beachte, daß hier der von m erzeugte Untermodul $\langle m \rangle$ mit dem von m erzeugten Hauptideal (m) zusammenfällt, was in beliebigen Ringen im allgemeinen nicht zutrifft. Weiterhin kann sowohl in $\langle m \rangle$ wie in (m) das erzeugende Element m durch $-m$ ersetzt werden.

3. Wir erinnern, daß nach B(26.2c) $\mathfrak{M}_n(\Gamma)$ wie $\mathfrak{M}_n(2\Gamma)$ Ringe sind und offensichtlich

$$\mathfrak{M}_n(2\Gamma) \subset \mathfrak{M}_n(\Gamma)$$

gilt. Es genügt also zu zeigen, daß das Produkt einer beliebigen Matrix aus $\mathfrak{M}_n(\Gamma)$ mit einer beliebigen Matrix aus $\mathfrak{M}_n(2\Gamma)$ unabhängig von der Reihen-

folge der Faktoren stets wieder eine Matrix aus $\mathfrak{M}_n(2\Gamma)$ ergibt. Wenn aber in

$$c_{il} = \sum_{k=1}^{n} a_{ik} b_{kl}$$

alle auftretenden Faktoren ganzzahlig und darüber hinaus alle a_{ik} (bzw. alle b_{kl}) gerade sind, so ist auch c_{il} gerade.

4. Wir zeigen, daß jedes vom Nullideal verschiedene Linksideal $\mathfrak{l}$ eines Schiefkörpers $\mathfrak{R}$ der ganze Körper ist. Ist nämlich $a \neq o$ ein Element von $\mathfrak{l}$, so ist in $\mathfrak{R}$ jede Gleichung $ya = b$ mit $y \in \mathfrak{R}$ lösbar. Es ist also jedes Körperelement b nach der Bedingung (2) für Ideale

$$b = y \cdot a \in \mathfrak{l}$$

auch in $\mathfrak{l}$ enthalten. Mit Hilfe der Gleichung $ax = b$ beweist man die Aussage für Rechtsideale.

5. Es sei $\mathfrak{R}$ kein entarteter Ring. Dann existieren wenigstens zwei Elemente $a \in \mathfrak{R}$ und $b \in \mathfrak{R}$ mit $ab \neq o$. Wir betrachten zunächst das Ideal $a\mathfrak{R}$. Wegen $a\mathfrak{R} \supset ab \neq o$ ist $a\mathfrak{R}$ nicht das Nullideal, also $a\mathfrak{R} = \mathfrak{R}$ nach Voraussetzung über $\mathfrak{R}$. Es muß also auch das Element a selbst in der Form $a \cdot r = a$ mit $r \in \mathfrak{R}$ darstellbar sein. Dieses Element r reproduziert aber bei der Multiplikation nicht nur a, sondern jedes beliebige Element $c \in \mathfrak{R}$, welches ebenfalls als $a \cdot r' = c$ mit $r' \in \mathfrak{R}$ geschrieben werden kann:

$$c \cdot r = a \cdot r' \cdot r = r' \cdot a \cdot r = r' \cdot a = a \cdot r' = c.$$

Damit ist $r = e$ das eindeutig bestimmte Einselement von $\mathfrak{R}$. Wir zeigen, daß jedes Element $d \neq o$ von $\mathfrak{R}$ ein Inverses in $\mathfrak{R}$ hat. Es ist nämlich das Ideal $d\mathfrak{R}$ wegen $d\mathfrak{R} \supset d \cdot e = d \neq o$ verschieden vom Nullideal, also wieder $d\mathfrak{R} = \mathfrak{R}$ nach Voraussetzung über $\mathfrak{R}$. Damit ist aber die Gleichung $d \cdot r'' = e$ mit $r'' \in \mathfrak{R}$ lösbar, also existiert ein Inverses zu d.

6. Die Bedingungen (2) für Ideale aus D (28.5) sind offensichtlich von dem zugrunde gelegten Ring $\mathfrak{R}$ abhängig im Unterschied zu der Bedingung (2) für Unterringe aus S (28.2). So ist z. B. 2Γ Ideal von Γ, aber nicht von P.

7. Der Durchschnitt beliebig vieler Untermoduln ist nach S (5.10) wieder Untermodul. Ist ferner a ein beliebiges Element aus $\mathfrak{l}_1 \cap \mathfrak{l}_2 \cap \ldots$, so folgt $a \in \mathfrak{l}_1$, $a \in \mathfrak{l}_2, \ldots$ und damit $ra \in \mathfrak{l}_1$, $ra \in \mathfrak{l}_2, \ldots$, mithin auch $ra \in \mathfrak{l}_1 \cap \mathfrak{l}_2 \cap \ldots$. Entsprechend verläuft der Beweis für Rechtsideale.

8. Sind a_i und b_i beliebige Elemente aus $\mathfrak{l}_i$ $(i = 1, \ldots, n)$, so gilt mit beliebigem $r \in \mathfrak{R}$:

$$\sum a_i - \sum b_i = \sum (a_i - b_i), \quad r \cdot \sum a_i = \sum r a_i.$$

Also ist $\mathfrak{l}_1 + \mathfrak{l}_2 + \ldots + \mathfrak{l}_n$ Linksideal von $\mathfrak{R}$. Der Beweis für Rechtsideale verläuft ebenso.

9. Einerseits gilt offensichtlich

$$(\mathfrak{M}_1, \ldots, \mathfrak{M}_n) \supseteq (\mathfrak{M}_1) + \ldots + (\mathfrak{M}_n);$$

andererseits enthält $(\mathfrak{M}_1) + \ldots + (\mathfrak{M}_n)$ aber die Vereinigungsmenge $\mathfrak{M}_1 \cup \ldots \cup \mathfrak{M}_n$ und damit als Ideal auch das von ihr erzeugte Ideal:

$$(\mathfrak{M}_1) + \ldots + (\mathfrak{M}_n) \supseteq (\mathfrak{M}_1, \ldots, \mathfrak{M}_n).$$

Zu § 29

1. Die Beweise verlaufen entsprechend den in der Gruppentheorie geführten.

2. Die Zuordnung ist nach Konstruktion eineindeutig; sie vermittelt eine Abbildung von $\Gamma + \Gamma\sqrt{k}$ (bzw. von $\mathrm{P} + \mathrm{P}\sqrt{k}$) auf sich selbst, da $a + b\sqrt{k}$ und $a - b\sqrt{k}$ mit beliebigen ganzzahligen (bzw. rationalen) a und b die gleiche Menge durchlaufen. Die Relationstreue folgt aus

$$(a_1 - b_1\sqrt{k}) + (a_2 - b_2\sqrt{k}) = (a_1 + a_2) - (b_1 + b_2)\sqrt{k}$$
$$(a_1 - b_1\sqrt{k}) \cdot (a_2 - b_2\sqrt{k}) = (a_1 a_2 + k b_1 b_2) - (a_1 b_2 + b_1 a_2)\sqrt{k}\,.$$

3. Bei einem Automorphismus von Γ wird die 1 auf sich selbst abgebildet, also auch $1 + 1 = 2$, $1 + 1 + 1 = 3, \ldots$, und mit $\bar{a} = a$ für $a \geqq 0$ gilt auch $\overline{-a} = -\bar{a} = -a$.

   Derselbe Gedankengang zeigt die Behauptung für die Restklassenringe von $\Gamma \bmod m$.

   Beim Beweis der Behauptung über P schließen wir zunächst für die in P enthaltenen ganzen Zahlen $a, b, \ldots$ wie oben. Dann folgt die Behauptung für alle Brüche $\frac{a}{b}$ aus

$$\frac{a}{b} \to \overline{\left(\frac{a}{b}\right)} = \overline{a b^{-1}} = \bar{a} \cdot \overline{b^{-1}} = \bar{a} \cdot \bar{b}^{-1} = a b^{-1} = \frac{a}{b}\,.$$

4. a) Falls a und b ganze Zahlen sind, wird ihre Summe und ihr Produkt in der für ganze Zahlen üblichen Weise gebildet.

   b) Falls a und b Brüche sind, deren Nenner nicht 1 ist (genauer: deren Zähler kein ganzzahliges Vielfaches des Nenners ist), werden sie nach den Regeln der Bruchrechnung addiert und multipliziert; ist dabei das Ergebnis ein Bruch mit dem Nenner 1, wird dieser durch die im Zähler stehende ganze Zahl ersetzt.

   c) Falls a eine ganze Zahl und b ein Bruch mit von 1 verschiedenem Nenner ist, wird a durch $\frac{a}{1}$ ersetzt und danach wie bei b) verfahren.

   Der Leser vergegenwärtige sich, daß man in der Tat auf diese Weise mit ganzen und gebrochenen Zahlen zu rechnen pflegt, wenngleich man oft Teilschritte durch die große Übung beim praktischen Rechnen überspringt.

5. Gemäß Aufgabe 9 von § 18 erhält man sämtliche Endomorphismen von $\mathfrak{G}$, indem man in den Zuordnungen

$$g a \to \overline{g a} = \lambda(g a) \quad \text{für alle } g$$

   jeweils λ die Werte $0, 1, \ldots, n-1$ annehmen läßt. Wir bezeichnen die so festgelegten Endomorphismen mit σ_λ und behaupten: Der Endomorphismenring $\mathfrak{R} = \{\sigma_0, \sigma_1, \ldots, \sigma_{n-1}\}$ ist isomorph zum Restklassenring von Γ modulo n vermöge der Zuordnung

$$[\lambda] \to \sigma_\lambda\,.$$

In der Tat ist diese Zuordnung offensichtlich eineindeutig und relationstreu wegen

$$b^{\sigma\lambda+\sigma\varkappa} = b^{\sigma\lambda} + b^{\sigma\varkappa} = \lambda b + \varkappa b = (\lambda+\varkappa)\,b = b^{\sigma\lambda+\varkappa}$$

$$b^{\sigma\lambda\cdot\sigma\varkappa} = \left(b^{\sigma\lambda}\right)^{\sigma\varkappa} = (\lambda b)^{\sigma\varkappa} = \lambda\left(b^{\sigma\varkappa}\right) = \lambda(\varkappa b) = (\lambda\cdot\varkappa)\,b = b^{\sigma\lambda\cdot\varkappa}.$$

Zu § 30

1. (I) Die Gleichung

$$\frac{a}{b} = \frac{a'}{b'}$$

bedeutet nach Definition der Quotienten $ab^{-1} = a'b'^{-1}$, und diese Gleichung ist äquivalent mit $ab' = a'b$, wie die Multiplikation mit bb' unter Verwendung der Vertauschbarkeit der Elemente aus $\mathfrak{R}$ untereinander und mit den in $\mathfrak{R}^*$ existierenden Inversen dieser Elemente zeigt.

(II) Entsprechend lautet diese Gleichung

$$ab^{-1} + cd^{-1} = (ad + bc)\cdot(bd)^{-1},$$

deren Richtigkeit die Ausrechnung der rechten Seite bestätigt.

(III) Die entsprechende Gleichung

$$(ab^{-1})\cdot(cd^{-1}) = (ac)\cdot(bd)^{-1}$$

ist ebenfalls auf Grund der Kommutativität von $\mathfrak{R}$ und den sich daraus ergebenden Folgerungen richtig.

2. Die zu beweisenden Relationen

A II	$[(a,b)+(c,d)]+(e,f)$	$=(a,b)+[(c,d)+(e,f)]$
M II	$[(a,b)\cdot(c,d)]\cdot(e,f)$	$=(a,b)\cdot[(c,d)\cdot(e,f)]$
D	$[(a,b)+(c,d)]\cdot(e,f)$	$=(a,b)\cdot(e,f)+(c,d)\cdot(e,f)$

folgen durch sukzessive Umformung ihrer linken Seiten vermöge der im Text genannten Regeln (II) und (III) unter Verwendung der für $\mathfrak{R}$ gültigen Rechengesetze.

3. Es sei $\mathfrak{R} \overset{\sim}{\longleftrightarrow} \overline{\mathfrak{R}}$ vermöge $a \to \bar{a} = \varphi(a)$, $\mathfrak{K}$ ein Quotientenkörper von $\mathfrak{R}$ und $\overline{\mathfrak{K}}$ ein solcher von $\overline{\mathfrak{R}}$. Dann ist $\mathfrak{K} \overset{\sim}{\longleftrightarrow} \overline{\mathfrak{K}}$. Wir können nämlich $\mathfrak{K}$ auf $\overline{\mathfrak{K}}$ abbilden durch eine Zuordnung ψ, die sich auf die vorgegebene Zuordnung φ stützt:

$$\alpha = \frac{a}{b} \to \psi(\alpha) = \frac{\bar{a}}{\bar{b}} = \frac{\varphi(a)}{\varphi(b)}.$$

Dabei ist tatsächlich jedes Element aus $\overline{\mathfrak{K}}$ Bild eines Elementes aus $\mathfrak{K}$, nämlich

$$\frac{\bar{a}}{\bar{b}} \quad \text{von} \quad \alpha = \frac{a}{b} = \frac{\varphi^{-1}(\bar{a})}{\varphi^{-1}(\bar{b})}.$$

Diese Abbildung von $\mathfrak{R}$ auf $\overline{\mathfrak{R}}$ ist eindeutig und eineindeutig; denn es ergeben sich der Reihe nach die folgenden Gleichungen in beiden Richtungen auseinander:

$$\alpha = \alpha', \quad \frac{a}{b} = \frac{a'}{b'}, \quad ab' = a'b, \quad \overline{ab'} = \overline{a'b},$$

$$\overline{a} \cdot \overline{b'} = \overline{a'} \cdot \overline{b}, \quad \frac{\overline{a}}{\overline{b}} = \frac{\overline{a'}}{\overline{b'}}, \quad \psi(\alpha) = \psi(\alpha').$$

Entsprechend ergibt sich die Relationstreue aus:

$$\psi(\alpha) + \psi(\alpha') = \frac{\overline{a}}{\overline{b}} + \frac{\overline{a'}}{\overline{b'}} = \frac{\overline{ab' + a'b}}{\overline{bb'}}$$

$$= \psi\left(\frac{ab' + a'b}{bb'}\right) = \psi\left(\frac{a}{b} + \frac{a'}{b'}\right) = \psi(\alpha + \alpha')$$

$$\psi(\alpha) \cdot \psi(\alpha') = \frac{\overline{a}}{\overline{b}} \cdot \frac{\overline{a'}}{\overline{b'}} = \frac{\overline{aa'}}{\overline{bb'}} = \psi\left(\frac{aa'}{bb'}\right) = \psi\left(\frac{a}{b} \cdot \frac{a'}{b'}\right) = \psi(\alpha \cdot \alpha').$$

Damit ist die Behauptung vollständig bewiesen. Wir bemerken noch, daß sich für $\overline{\mathfrak{R}} = \mathfrak{R}$ wiederum die bis auf Isomorphie eindeutige Bestimmtheit des Quotientenkörpers von $\mathfrak{R}$ ergibt, die wir im Text S(30.2) einfach aus der durch $\mathfrak{R}$ vollständig festgelegten Struktur des Quotientenkörpers gefolgert hatten. Auch die Behauptung unserer Aufgabe hätte kürzer durch den Schluß von der gleichen Struktur der Ringe $\mathfrak{R}$ und $\overline{\mathfrak{R}}$ auf die gleiche Struktur ihrer Quotientenkörper bewiesen werden können.

4. Der Quotientenkörper von $\Gamma + \Gamma i$ ist der Gausssche Zahlkörper $\mathrm{P} + \mathrm{P}i$.

5. Die Regeln für das Kürzen und Erweitern stimmen genau mit der Gleichheitsdefinition (I) überein; das gleiche gilt für die Multiplikation von Brüchen (III). Aus (II) folgt ferner insbesondere

$$\frac{a}{b} + \frac{c}{b} = \frac{ab + cb}{b^2} = \frac{b(a + c)}{b^2} = \frac{a + c}{b},$$

letzteres nach (I). Umgekehrt kann jede Addition von Brüchen wegen (I) auf die Addition von Brüchen mit gleichem Nenner zurückgeführt werden. Die leichtere Faßlichkeit der Addition von Brüchen mit gleichen Nennern erkauft man dabei allerdings durch die Schwierigkeit der Hauptnennerbestimmung, die noch dazu auf dem (in der Schule nicht zu beweisenden) Fundamentalsatz der Zahlentheorie von der eindeutigen Zerlegung in Primfaktoren beruht.

6. Die zu B(26.4b) gehörigen Halbgruppen bestehen aus allen Potenzen mit ganzzahligen Exponenten einer beliebigen ganzen Zahl $b \neq 0$.

Wählt man ferner $\mathfrak{Y}$ als die Gesamtheit aller Potenzprodukte endlich vieler ganzer Zahlen $b_1, b_2, \ldots, b_r$ $(b_i \neq 0)$, erhält man Quotientenringe mit Elementen der Gestalt

$$\frac{a}{b_1^{n_1} b_2^{n_2} \ldots b_r^{n_r}}.$$

Schließlich können wir $\mathfrak{Z}$ auch als die Menge aller zu einer festen Zahl m teilerfremden Zahlen nehmen. Der zugehörige Quotientenring, der alle rationalen Zahlen

$$\frac{a}{b} \quad \text{mit} \quad (b, m) = 1$$

enthält, in deren Nenner also kein Primfaktor von m aufgeht, heißt *der Ring Γ_m der für m ganzen Zahlen*. Solche Ringe spielen in der Zahlentheorie eine große Rolle.

Zu § 31

1. Die Nachprüfung der Ringeigenschaften bereitet keine Schwierigkeit. Nullteiler sind etwa (a, o) und (o, d).

2. Die Gültigkeit der Ringaxiome zeigt man wieder ohne Mühe. Linkseinselemente sind alle Elementenpaare (e, b) mit beliebigem b.

3. Matrizen vom Typ (n, n) sind nichts anderes als geordnete Elementensysteme mit n^2 Komponenten, die nur in einer für die Multiplikation günstigen Weise geschrieben sind.

4. Das Inverse

$$(a + bi + cj + dk)^{-1} = \frac{a - bi - cj - dk}{a^2 + b^2 + c^2 + d^2}$$

existiert genau dann, wenn $a^2 + b^2 + c^2 + d^2 \neq 0$ ist. Nur das Nullelement des Quaternionenkörpers

$$0 + 0i + 0j + 0k$$

erfüllt diese Bedingung nicht.

5. Die Zuordnung ist nach Definition eineindeutig, die Relationstreue ergibt sich unmittelbar durch Ausrechnung der Matrizensummen bzw. -produkte. Umgekehrt hätte man von der Untermenge der genannten Matrizen leicht die Schiefkörpereigenschaft zeigen können, da Differenz und Produkt solcher Matrizen ebensolche Matrizen sind und die Determinante nur für $a = b = c = d = 0$ verschwindet. Die Menge der Quaternionen mit den in ihr erklärten Rechenregeln erweist sich dann als isomorphes Bild dieses Schiefkörpers von selbst als Schiefkörper.

Zu § 32

1. „Unbestimmte" über dem Körper P der rationalen Zahlen sind etwa die Basis e der natürlichen Logarithmen und die Ludolfsche Zahl π; dagegen sind diese Zahlen keine „Unbestimmten" über dem Körper der reellen Zahlen.

   Allgemein trifft dies für alle transzendenten Zahlen zu. Von daher überträgt sich der Sprachgebrauch, irgendwelche Unbestimmte über einem Ring $\mathfrak{R}$ auch „über $\mathfrak{R}$ transzendente Elemente" zu nennen.

2. Während z. B. *A II* in $\mathfrak{R}[x]$ allein aus *A II* in $\mathfrak{R}$ folgt, benötigt man zum Beweis von *M II* in $\mathfrak{R}[x]$ nicht nur *M II* in $\mathfrak{R}$, sondern auch *A II* und *D* in $\mathfrak{R}$.

3. Die Behauptung ist für $i = 1$ trivial. Sie gelte bereits für $i = k$; wir zeigen die Gültigkeit für $i = k + 1$:

$$(o, e, o, \ldots)^{k+1} = (o, e, o, \ldots)^k \, (o, e, o, \ldots)$$

$$= (\underbrace{o, \ldots, o}_{k}, \underbrace{e, o, \ldots}) \, (o, e, o, \ldots)$$

$$= \Big(\ldots, \sum_{\nu+\mu=\lambda} a_\nu b_\mu, \ldots\Big) = (\underbrace{o, \ldots, o}_{k+1}, \underbrace{e, o, \ldots})$$

wegen $a_\nu = \begin{cases} e \text{ für } \nu = k \\ o \text{ sonst} \end{cases}$ und $b_\mu = \begin{cases} e \text{ für } \mu = 1 \\ o \text{ sonst.} \end{cases}$

4. Es sei $\mathfrak{R} \xleftrightarrow{\sim} \overline{\mathfrak{R}}$ vermöge $a \to \bar{a} = \varphi(a)$, $\mathfrak{R}[x]$ ein Polynomring in einer Unbestimmten über $\mathfrak{R}$ und $\overline{\mathfrak{R}}[y]$ ein solcher über $\overline{\mathfrak{R}}$. Dann ist $\mathfrak{R}[x] \xleftrightarrow{\sim} \overline{\mathfrak{R}}[y]$ vermöge einer Zuordnung ψ, die sich auf die vorgegebene Zuordnung φ stützt:

$$f(x) = \Sigma a_\nu x^\nu \to \psi(f(x)) = \Sigma \bar{a}_\nu y^\nu = \Sigma \varphi(a_\nu) y^\nu.$$

Jedes Element $h(y) = \Sigma \bar{c}_\nu y^\nu$ von $\overline{\mathfrak{R}}[y]$ ist dann in der Tat Bild eines Elementes aus $\mathfrak{R}[x]$, nämlich von $f(x) = \Sigma \varphi^{-1}(\bar{c}_\nu) x^\nu$. Zufolge der komponentenweisen Festsetzung der Gleichheit in Polynomringen überträgt sich die Eineindeutigkeit der Zuordnung φ unmittelbar auf die Zuordnung ψ. Um die Relationstreue zu zeigen, setzen wir $f(x) = \Sigma a_\nu x^\nu$ und $g(x) = \Sigma b_\nu x^\nu$:

$$\psi(f(x)) + \psi(g(x)) = \Sigma \bar{a}_\nu y^\nu + \Sigma \bar{b}_\nu y^\nu = \Sigma (\bar{a}_\nu + \bar{b}_\nu) y^\nu$$

$$= \Sigma \overline{(a_\nu + b_\nu)} y^\nu = \psi(\Sigma (a_\nu + b_\nu) x^\nu)$$

$$= \psi(f(x) + g(x));$$

$$\psi(f(x)) \cdot \psi(g(x)) = (\Sigma \bar{a}_\nu y^\nu) \cdot (\Sigma \bar{b}_\nu y^\nu) = \sum_\nu \Big(\sum_{\mu+\lambda=\nu} \bar{a}_\mu \bar{b}_\lambda \Big) y^\nu$$

$$= \sum_\nu \Big(\sum_{\mu+\lambda=\nu} \overline{a_\mu b_\lambda} \Big) y^\nu = \psi\Big(\sum_\nu \Big(\sum_{\mu+\lambda=\nu} a_\mu b_\lambda \Big) x^\nu \Big)$$

$$= \psi(f(x) \cdot g(x)).$$

Die Bemerkungen zur Lösung von Aufg. 3 aus § 30 lassen sich sinngemäß hierher übertragen.

5. $\mathfrak{R}[x] \supset \mathfrak{R}[x^2] \supset \mathfrak{R}[x^4] \supset \ldots$ mit $\mathfrak{R}[x] \xleftrightarrow{\sim} \mathfrak{R}[x^2] \xleftrightarrow{\sim} \mathfrak{R}[x^4] \xleftrightarrow{\sim} \ldots$. Die Isomorphie versteht sich nach S (32.2) von selbst, wenn wir $x^2, x^4, \ldots$ als neue Unbestimmte über $\mathfrak{R}$ ansehen.

6. Es sei $f(x_1, \ldots, x_n)$ ein homogenes Polynom mit den Gliedern $A_i(x_1, \ldots, x_n)$ vom Grad r, $g(x_1, \ldots, x_n)$ ein solches mit den Gliedern $B_i(x_1, \ldots, x_n)$ vom Grad s. Dann ist $f \cdot g = \Sigma A_i B_k$ eine Summe von Produkten $A_i B_k$, die entweder verschwinden oder den Grad $r + s$ haben.

7. Der Polynomring $\mathfrak{R}[y] = \mathfrak{R}[a + x]$ ist sicher in $\mathfrak{R}[x]$ enthalten. Umgekehrt enthält $\mathfrak{R}[y]$ das Polynom $-a + y = x$, also gilt $\mathfrak{R}[x] = \mathfrak{R}[y]$. Die beiden anderen Behauptungen folgen analog mit $y = a + bx$, also

$$x = -\frac{a}{b} + \frac{1}{b} y \quad \text{bzw. mit} \quad y = \frac{a + bx}{c + dx}, \quad \text{also} \quad x = \frac{-a + cy}{b - dy}.$$

8. Schreiben wir das Polynom

$$f(x^p) = b_n(x^p)^n + b_{n-1}(x^p)^{n-1} + \ldots + b_1x^p + b_0$$

mit Koeffizienten aus Π_p in der Form

$$f(x^p) = b_n(x^n)^p + b_{n-1}(x^{n-1})^p + \ldots + b_1x^p + b_0,$$

so folgt unter Verwendung von $b_\nu = b_\nu{}^p$ (kleiner FERMATscher Satz) und der Rechenregel F(27.4):

$$\begin{aligned} f(x^p) &= (b_nx^n)^p + (b_{n-1}x^{n-1})^p + \ldots + (b_1x)^p + b_0{}^p \\ &= (b_nx^n + b_{n-1}x^{n-1} + \ldots + b_1x + b_0)^p = (f(x))^p. \end{aligned}$$

Zu § 33

1. *Beweis zu* F(33.2):

Für die Addition ist gemäß F(18.2) nichts mehr zu beweisen. Aber auch *M I* und *M II* (und gegebenenfalls *M III* bzw. *M IV*) übertragen sich in Analogie zu schon im Beweis von F(4.4) geführten Schlüssen aus dem Original in das Bild. Letzteres gilt auch für D, was wir für die erste Relation zeigen: Es seien $\bar{a}, \bar{b}, \bar{c}$ beliebige Elemente von $\mathfrak{R}$ und a, b, c irgendwelche zugehörigen Originale aus $\mathfrak{R}$. Damit gilt $a(b + c) = ab + ac$, also auch $\overline{a(b + c)} = \overline{ab + ac}$ und wegen der Relationstreue der Abbildung $\bar{a}(\bar{b} + \bar{c}) = \bar{a} \cdot \bar{b} + \bar{a} \cdot \bar{c}$.

Beweis zu F(33.3):

a) entspricht F(18.3), angewandt auf die additive Gruppe des Ringes.

b) bzw. c) folgen für Linkseinselemente bzw. Linksinverse ebenfalls wie im Beweis von F(18.3).

2. Die Behauptung folgt aus dem Homomorphiesatz und Aufg. 1 von § 28.

3. Ein Körper wird nur homomorph abgebildet entweder auf den Nullring oder auf einen zu ihm selbst isomorphen Körper (vgl. Aufg. 4 von § 28).

4. a) Betrachtet man die Kongruenz $ax \equiv 1\,(m)$ als Gleichung $[a][x] = [1]$ im Restklassenring $\Gamma/(m)$, so ist das Problem auf die Frage zurückgeführt, welche Restklassen ein Inverses besitzen. Dies sind aber nach Aufgabe 2 von § 26 genau die primen Restklassen. Die Eindeutigkeitsaussage entspricht der Eindeutigkeit des zweiseitigen Inversen.

b) Es genügt, die prime Restklassengruppe mod m zu betrachten. Nach dem kleinen FERMATschen Satz gilt

$$ax \equiv aa^{\varphi(m)-1} \equiv a^{\varphi(m)} \equiv 1\,(m);$$

der niedrigste Exponent ν mit $ax \equiv aa^\nu \equiv 1\,(m)$ ist offensichtlich die um 1 verminderte Ordnung der von a bestimmten Restklasse.

c) Eine Lösung x der Kongruenz $ax \equiv b\,(m)$ mit $(a, m) = 1$ erhält man aus einer Lösung y der Kongruenz $ay \equiv 1\,(m)$ in der Form $x \equiv yb$. Zur Untersuchung der Eindeutigkeit der Lösung einer beliebigen, als lösbar vorausgesetzten Kongruenz $ax \equiv b\,(m)$ betrachten wir die ihr entsprechende Gleichung $[a][x] = [b]$ in $\Gamma/(m)$. Nach S(25.8) ist $[x]$ genau dann eindeutig bestimmt, wenn $[a]$ kein Nullteiler ist. Dies ist aber wieder nach Aufgabe 2 von § 26 genau für $(a, m) = 1$ der Fall.

5. Unabhängig davon, daß man unter Umständen durch sinnvolles Probieren und Einsetzen oft rascher zu einer Lösung gelangen kann, wollen wir hier die Lösungen mit Hilfe des in Aufgabe 4 angegebenen Verfahrens berechnen.

a) Die Kongruenz $2y \equiv 1\ (15)$ wird durch

$$y \equiv 2^{\varphi(15)-1} \equiv 2^7 \equiv 8\ (15),$$

aber auch schon von

$$y \equiv 2^{4-1} \equiv 2^3 \equiv 8\ (15)$$

gelöst. Damit löst

$$x \equiv 3y \equiv 3 \cdot 8 \equiv 9\ (15)$$

die vorgegebene Kongruenz $2x \equiv 3\ (15)$.

b) Entsprechendes gilt für $5y \equiv 1\ (36)$ und $5x \equiv 7\ (36)$ mit

$$y \equiv 5^{\varphi(36)-1} \equiv 5^{11} \equiv 29\ (36)$$

bzw. $$y \equiv 5^{6-1} \equiv 5^5 \equiv 29\ (36)$$

und $$x \equiv 7y \equiv 7 \cdot 29 \equiv 23\ (36).$$

c) Die Lösung der Kongruenz $9y \equiv 1\ (58)$ ergibt sich wegen $\varphi(58) = 28$ als

$$y \equiv 9^{27} \equiv ((9^3)^3)^3 \equiv (33^3)^3 \equiv 35^3 \equiv 13\ (58).$$

Damit ist

$$x \equiv 44y \equiv 44 \cdot 13 \equiv 50\ (58)$$

die Lösung von $9x \equiv 44\ (58)$. (Dieses Beispiel zeigt deutlich, daß mitunter die Verwendung der Formel $y \equiv a^{\varphi(\ )-1}$ vorteilhafter ist, als etwa durch sukzessives Potenzieren von $a = 9$ zu finden, daß schon $9^{14} \equiv 1\ (58)$ und damit $y \equiv 9^{13}\ (58)$ ist.)

6. Es sei $a = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \ldots + a_n \cdot 10^n = \sum_{i=0}^{n} a_i \cdot 10^i$.

a) $2 \mid a$ genau dann, wenn $a \equiv 0\ (2)$. Dies ist wegen $10^i \equiv 0\ (2)$ für $i > 0$ gleichwertig mit $a_0 \equiv 0\ (2)$.

$4 \mid a$ genau dann, wenn $a \equiv 0\ (4)$. Wegen $10^i \equiv 0\ (4)$ für $i > 1$ ist dies gleichwertig mit $a_0 + a_1 \cdot 10 \equiv 0\ (4)$.

Entsprechend ergibt sich $a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 \equiv 0\ (8)$ im Fall $8 \mid a$ wegen $10^i \equiv 0\ (8)$ für $i > 2$.

b) Es ist $10^i \equiv 1\ (3)$ bzw. (9) für $i > 0$. Also ergibt sich für $3 \mid a$ bzw. $9 \mid a$ das Kriterium

$$a \equiv a_0 + a_1 + \ldots + a_n \equiv 0\ (3) \text{ bzw. } (9).$$

c) Mit $11 \mid a$ ist

$$a \equiv a_0 - a_1 + \ldots + (-1)^n \cdot a_n \equiv 0\ (11)$$

gleichwertig, da $10^i \equiv (-1)^i\ (11)$ ist.

7. $\mathfrak{R}[x_1, x_2, \ldots, x_n]$ wird durch die Ersetzung von $x_1, x_2, \ldots, x_n$ durch $\xi_1, \xi_2, \ldots, \xi_n$ aus $\mathfrak{R}^*$ homomorph auf den von $\mathfrak{R}$ und $\xi_1, \xi_2, \ldots, \xi_n$ erzeugten Unterring von $\mathfrak{R}^*$ abgebildet. Die Zuordnung ist durch

$f(x_1, x_2, \ldots, x_n) \to f(\xi_1, \xi_2, \ldots, \xi_n)$ gegeben. Der Beweis von S(32.6) entspricht dem Nachweis der Eindeutigkeit und der Relationstreue dieser Abbildung.

Übrigens ist der Kern dieses Homomorphismus das von den Elementen $x_i - \xi_i$ erzeugte Ideal $(x_1 - \xi_1, x_2 - \xi_2, \ldots, x_n - \xi_n)$ von $\mathfrak{R}^*[x_1, x_2, \ldots, x_n]$.

Daraus ergibt sich auch die geforderte Deutung von $\Gamma[x]/(x - g)$: Sowohl bei der Ersetzung von x durch g in $\Gamma[x]$ als auch bei der Bildung von $\Gamma[x]/(x - g)$ handelt es sich um homomorphe Abbildungen von $\Gamma[x]$ mit dem Kern $(x - g)$, also nach dem Homomorphiesatz um denselben strukturellen Vorgang. Da sich im ersteren Falle nach dem obigen als Bild (der von Γ und g erzeugte Unterring von Γ, also) Γ ergibt, erhalten wir insbesondere

$$\Gamma[x]/(x - g) \overset{\sim}{\leftarrow} \Gamma.$$

8. Nullteiler sind die Restklassen, die ein Element der Gestalt $(x^2 - 2) \cdot f(x)$ bzw. $(x^2 + 2) \cdot g(x)$ mit beliebigen $f(x)$ und $g(x)$ aus $P[x]$ enthalten. Es gilt nämlich

$$\big((x^2 - 2) \cdot f(x)\big) \cdot \big((x^2 + 2) \cdot g(x)\big) \equiv 0 \text{ modulo } (x^4 - 4) = (x^2 - 2)(x^2 + 2).$$

Dabei kann man $f(x)$ und $g(x)$ auf die verschiedensten Weisen so wählen, daß sowohl $(x^2 - 2)f(x) \not\equiv 0$ als auch $(x^2 + 2)g(x) \not\equiv 0$ modulo $(x^4 - 4)$ ist.

Zu § 34

1. Es sei $\mathfrak{R} \overset{\sim}{\to} \overline{\mathfrak{R}}$ ein Homomorphismus mit dem Kern $\mathfrak{m}$ und dabei $\overline{\mathfrak{S}}$ das Bild von $\mathfrak{S}$. Wendet man dann S(34.3) einmal auf das Original $\mathfrak{S}$ von $\overline{\mathfrak{S}}$ und einmal auf das vollständige Original $\mathfrak{S} + \mathfrak{m}$ von $\overline{\mathfrak{S}}$ an, erhält man wegen

$$\overline{\mathfrak{S}} \overset{\sim}{\leftarrow} \mathfrak{S}/(\mathfrak{S} \cap \mathfrak{m}),$$

$$\overline{\mathfrak{S}} \overset{\sim}{\leftarrow} (\mathfrak{S} + \mathfrak{m})/((\mathfrak{S} + \mathfrak{m}) \cap \mathfrak{m}) = (\mathfrak{S} + \mathfrak{m})/\mathfrak{m}$$

die Behauptung.

2. Für diese reine Mengenaussage genügt es, die auftretenden Ringe durch ihre additiven Gruppen zu ersetzen, für die in S(19.7) alles bewiesen ist.

3. Bei dem Homomorphismus $\mathfrak{R} \overset{\sim}{\to} \hat{\mathfrak{R}} = \mathfrak{R}/\mathfrak{b}$ ist das Bild $\hat{\mathfrak{a}}$ von $\mathfrak{a}$ zunächst isomorph zu $\mathfrak{a}/(\mathfrak{a} \cap \mathfrak{b}) = \mathfrak{a}/\mathfrak{b}$, und es ist $\hat{\mathfrak{a}}$ sogar gleich $\mathfrak{a}/\mathfrak{b}$, da $\hat{\mathfrak{a}}$ ja gerade aus denjenigen Restklassen mod $\mathfrak{b}$ besteht, die von Elementen aus $\mathfrak{a}$ erzeugt werden. Nach S(34.4a) ist $\hat{\mathfrak{a}}$ Ideal von $\hat{\mathfrak{R}}$. Man kann also abbilden

$$\mathfrak{R} \overset{\sim}{\to} \hat{\mathfrak{R}} \overset{\sim}{\to} \hat{\mathfrak{R}}/\hat{\mathfrak{a}} = (\mathfrak{R}/\mathfrak{b})/(\mathfrak{a}/\mathfrak{b}).$$

Nach Aufg.2 ist nun der Kern des Homomorphismus $\mathfrak{R} \overset{\sim}{\to} \hat{\mathfrak{R}}/\hat{\mathfrak{a}}$ das vollständige Original $\mathfrak{a} + \mathfrak{b}$ von $\hat{\mathfrak{a}}$; wegen $\mathfrak{b} \subseteq \mathfrak{a}$ folgt $\mathfrak{a} + \mathfrak{b} = \mathfrak{a}$, also $\hat{\mathfrak{R}}/\hat{\mathfrak{a}} \overset{\sim}{\to} \mathfrak{R}/\mathfrak{a}$.

4. Es entsprechen sich:

S(19.1), S(19.2)	S(34.1)	S(19.5)	Aufgabe 1
		S(19.6)	S(34.4)
F(19.3)	F(34.2)	S(19.7)	Aufgabe 2
S(19.4)	S(34.3)	S(19.8)	Aufgabe 3

5. Die Behauptung besagt: Der Restklassenring von $\Gamma[x]$ nach dem von m in diesem Ring erzeugten Hauptideal $(m) = m \cdot \Gamma[x]$ ist isomorph zu dem Polynomring in der Unbestimmten x über dem Restklassenring $\Gamma/(m)$ nach dem von m in Γ erzeugten Hauptideal $(m) = m \cdot \Gamma$.

Gemäß der Anleitung genügt es zu zeigen, daß der im folgenden mit $\mathfrak{A}$ bezeichnete Ring $\Gamma[x]/(m)$ die dort angegebene Struktur besitzt:

Bei dem natürlichen Homomorphismus

$$\Gamma[x] \longrightarrow \mathfrak{A}$$

wird der Unterring Γ von $\Gamma[x]$ gemäß S(34.1) auf den Unterring $\mathfrak{B}$ von $\mathfrak{A}$ abgebildet, der gerade aus den von ganzen Zahlen repräsentierbaren Restklassen $[g]$ von $\Gamma[x]$ modulo $(m) = m \cdot \Gamma[x]$ besteht. Dieser Ring $\mathfrak{B}$ ist isomorph zu $\Gamma/(m)$; denn beide Ringe sind das Ergebnis homomorpher Abbildungen von Γ, deren Kerne $m \cdot \Gamma[x] \cap \Gamma$ (vgl. S(34.3)) und $m \cdot \Gamma$ offenbar übereinstimmen.

Die Restklasse $y = [x] \in \mathfrak{A}$ ist Unbestimmte über $\mathfrak{B}$; aus einer Kongruenz

$$\Sigma g_\nu x^\nu \equiv 0 \bmod m \cdot \Gamma[x]$$

folgt nämlich, daß jeder Koeffizient g_ν ein ganzzahliges Vielfaches von m ist, so daß also erst recht gilt

$$g_\nu \equiv 0 \bmod m \cdot \Gamma[x] .$$

Der Polynomring $\mathfrak{B}[y] \subseteq \mathfrak{A}$ stimmt aber bereits mit $\mathfrak{A}$ überein; denn jedes Element $[\Sigma g_\nu x^\nu] \in \mathfrak{A}$ ist vermöge

$$[\Sigma g_\nu x^\nu] = \Sigma [g_\nu] \cdot [x]^\nu = \Sigma [g_\nu] \cdot y^\nu$$

auch Element von $\mathfrak{B}[y]$.

Bei der Verallgemeinerung hat man $(m) = m \cdot \Gamma$ durch ein zweiseitiges Ideal $\mathfrak{m}$ von $\mathfrak{R}$ und damit $(m) = m \cdot \Gamma[x]$ durch das von der Menge $\mathfrak{m}$ in $\mathfrak{R}[x]$ erzeugte Ideal $(\mathfrak{m})$ von $\mathfrak{R}[x]$ zu ersetzen. Es gilt dann

$$\mathfrak{R}[x]/(\mathfrak{m}) \longleftrightarrow (\mathfrak{R}/\mathfrak{m})[x],$$

wie man völlig analog beweist.

6. Die Primidealeigenschaft von (x) ist klar, da der Restklassenring $\mathfrak{R}/(x) \longleftrightarrow \Gamma$ nullteilerfrei ist. Wegen $(x) \subset (x, g) \subset \Gamma[x]$ mit beliebigem, von 0 und ± 1 verschiedenen $g \in \Gamma$ ist (x) nicht maximal.

7. Das Ideal $(x^2 + 1)$ ist sogar maximal, da der Restklassenring $\Delta[x]/(x^2 + 1)$ isomorph zum Körper der komplexen Zahlen ist.

8. Wir bilden den Restklassenring von $\Gamma/(15)$ nach dem Ideal $\{[0], [5], [10]\} = (5)/(15)$. Aus dem 2. Isomorphiesatz folgt, daß dieser Restklassenring isomorph zu dem Körper $\Gamma/(5)$ ist:

$$(\Gamma/(15))/((5)/(15)) \longleftrightarrow \Gamma/(5) .$$

Entsprechend schließt man:

$$(\Gamma/(15))/((3)/(15)) \longleftrightarrow \Gamma/(3) .$$

Zu § 35

1. $\sigma \in \Phi$ und $a \in \mathfrak{G}$ bestimmen eindeutig das Element $\sigma(a) = a^\sigma$ von $\mathfrak{G}$. Dabei gilt die Distributivität $(ab)^\sigma = a^\sigma b^\sigma$. Schreiben wir statt a^σ nun $a\sigma$ und damit $(ab)\sigma = (a\sigma)(b\sigma)$, so haben wir genau die Forderungen *O I* und *O II* von D(35.1) in der Schreibweise für Rechtsoperatoren vor uns. Die Exponentenschreibweise ist also im Grunde nichts anderes als ein Ausdruck für die Anwendung der Elemente $\sigma \in \Phi$ als Rechtsoperatoren.

   Die innere Verknüpfung von Φ ergibt eine weitere Grundformel der Operatoranwendung:

$$\text{Aus } a^{[\sigma_1\sigma_2]} = (a^{\sigma_1})^{\sigma_2} \text{ wird nämlich } a(\sigma_1\sigma_2) = (a\sigma_1)\sigma_2,$$

   wofür wir auch sagen können, daß die Operatoranwendung und die Multiplikation in Φ assoziativ verbunden sind. Würde man dagegen statt $\sigma(a) = a^\sigma$ einfach σa, also σ als Linksoperator schreiben, würden zwar *O I* und *O II* wieder gelten, das zuletzt genannte Gesetz aber die weniger übersichtliche Form $(\sigma_1\sigma_2)a = \sigma_2(\sigma_1 a)$ annehmen (vgl. auch die Fußnote zu S(15.5)).

2. a) Jeder Automorphismus bildet $\mathfrak{E}$ auf $\mathfrak{E}$ und $\mathfrak{G}$ auf $\mathfrak{G}$ ab.

   b) $\mathfrak{A}_n$ ist die einzige Untergruppe der Ordnung $\frac{n!}{2}$ in $\mathfrak{S}_n$.

   c) Wir beweisen weitergehend, daß bei jedem Automorphismus einer Gruppe $\mathfrak{G}$ Elemente des Zentrums $\mathfrak{Z}$ wieder auf Elemente des Zentrums abgebildet werden. Aus $ax = xa$ mit $a \in \mathfrak{Z}$ und beliebigem $x \in \mathfrak{G}$ folgt für die Bilder bei einem Automorphismus $\bar{a} \cdot \bar{x} = \bar{x} \cdot \bar{a}$. Da $\bar{x}$ mit x alle Elemente von $\mathfrak{G}$ durchläuft, ist also $\bar{a}$ ebenfalls aus $\mathfrak{Z}$.

3. Wegen $\Omega \longleftrightarrow \Omega^*$ mit $\alpha \to \alpha^*$ sind bei der Operatoranwendung die α durch die α^* ersetzbar, ohne daß die Strukturverhältnisse Änderungen erfahren. Das gleiche Argument gilt wegen der Eineindeutigkeit und Relationstreue isomorpher Abbildungen für die zweite Behauptung.

4. Entsprechend der Formulierung der Aufgabe ist nur zu zeigen, daß sich *O II* von $\mathfrak{G}$ auf $\overline{\mathfrak{G}}$ überträgt. Wegen der Relationstreue der Operatoranwendung (vgl. D(35.4)) und der Gültigkeit von *O I* in $\overline{\mathfrak{G}}$ gilt aber

$$\alpha(a \cdot b) \to \overline{\alpha(a \cdot b)} = \alpha\overline{(a \cdot b)} = \alpha(\bar{a} \cdot \bar{b})$$
$$\alpha a \cdot \alpha b \to \overline{\alpha a \cdot \alpha b} = \overline{\alpha a} \cdot \overline{\alpha b} = \alpha\bar{a} \cdot \alpha\bar{b}.$$

   Aus $\alpha(a \cdot b) = \alpha a \cdot \alpha b$ folgt daher $\alpha(\bar{a} \cdot \bar{b}) = \alpha\bar{a} \cdot \alpha\bar{b}$.

5. Zum Beweis wiederholt man entweder den Beweis von S(35.6) mit der Ersetzung von $[a]$ durch $\bar{a}$ oder schließt begrifflich: $\overline{\mathfrak{G}}$ ist isomorph zu $\mathfrak{G}/\mathfrak{N}$, hat also nach Aufg. 3 den gleichen Operatorenbereich Ω wie $\mathfrak{G}/\mathfrak{N}$ nach S(35.6).

6. Obwohl $\mathfrak{R}/\mathfrak{a}$ und $\mathfrak{R}^+/\mathfrak{a}$ als Mengen dieselben Elemente besitzen, sind sie doch wesentlich voneinander verschiedene algebraische Strukturen. Zwar haben sie die gleiche additive Verknüpfung, die der Abbildung

$$a + b \to [a + b] = [a] + [b]$$

entspricht, aber in $\mathfrak{R}/\mathfrak{a}$ existiert als zweite innere Verknüpfung eine der Abbildung

(*) $$a \cdot b \to [a \cdot b] = [a] \cdot [b]$$

entsprechende Multiplikation, während für $\mathfrak{R}^+/\mathfrak{a}$ eine äußere Verknüpfung gemäß der Abbildung

(**) $$ab \to [ab] = a[b]$$

erklärt ist. Man beachte den Unterschied von (*) und (**):

a) In (*) sind a und b miteinander multiplizierte Ringelemente — in (**) wirkt $a \in \mathfrak{R}$ als Operator auf $b \in \mathfrak{R}^+$.

b) In (*) wird $a \in \mathfrak{R}$ auf das Element $[a] \in \mathfrak{R}/\mathfrak{a}$ tatsächlich abgebildet — in (**) bleibt a als Operator bei der Abbildung ungeändert.

c) Die (*) entsprechende Multiplikation macht den Restklassenmodul zu einem Ring — die (**) entsprechende Operatoranwendung der Elemente von $\mathfrak{R}$ macht den Restklassenmodul zu einem Modul mit dem Operatorenbereich $\mathfrak{R}$.

Wir bemerken noch, daß (**) auch für die Restklassen nach einem Linksideal $\mathfrak{l}$ möglich ist, während in (*) die Zweiseitigkeit des Ideales $\mathfrak{a}$ wesentlich eingeht.

Zu § 36

1. *O I:* $a\alpha$ ist ein eindeutig bestimmtes Element von $\mathfrak{G}$

O II: $(a + b)\alpha = a\alpha + b\alpha$

O III: $a(\alpha + \beta) = a\alpha + a\beta$

O III′: $a(\alpha \cdot \beta) = (a\alpha)\beta$

Faßt man die Aussagen dieser Relationen in Worte wie etwa „ein Operator wird auf eine Summe angewendet, indem man ihn auf jeden einzelnen Summanden anwendet" (*O II*), so erkennt man deutlich, daß die Schreibweise als Links- oder Rechtsmodul bezüglich *O I*, *O II* und *O III* keinerlei inhaltliche Bedeutung hat. Dagegen wird vermöge *O III′* im ersten Falle von einem Produkt $\alpha\beta$ zuerst β, dann α auf a angewendet, im zweiten Falle dagegen zuerst α und dann β. Auch dieser Unterschied ist belanglos, wenn $\mathfrak{R}$ ein kommutativer Ring, also stets $\alpha\beta = \beta\alpha$ ist.

2. *O I:* Nach Definition ist $\alpha a = \alpha(\alpha_1, \ldots, \alpha_n) = (\alpha\alpha_1, \ldots, \alpha\alpha_n)$ ein eindeutig bestimmtes Element von $\mathfrak{G}$.

O II:
$$\begin{aligned}\alpha(a + b) &= \alpha(\alpha_1 + \beta_1, \ldots, \alpha_n + \beta_n) = (\alpha(\alpha_1 + \beta_1), \ldots, \alpha(\alpha_n + \beta_n)) \\ &= (\alpha\alpha_1 + \alpha\beta_1, \ldots, \alpha\alpha_n + \alpha\beta_n) \\ &= (\alpha\alpha_1, \ldots, \alpha\alpha_n) + (\alpha\beta_1, \ldots, \alpha\beta_n) \\ &= \alpha(\alpha_1, \ldots, \alpha_n) + \alpha(\beta_1, \ldots, \beta_n) \\ &= \alpha a + \alpha b.\end{aligned}$$

$$O\,III: \quad (\alpha+\beta)a = (\alpha+\beta)(\alpha_1, \ldots, \alpha_n) = ((\alpha+\beta)\alpha_1, \ldots, (\alpha+\beta)\alpha_n)$$
$$= (\alpha\alpha_1 + \beta\alpha_1, \ldots, \alpha\alpha_n + \beta\alpha_n)$$
$$= (\alpha\alpha_1, \ldots, \alpha\alpha_n) + (\beta\alpha_1, \ldots, \beta\alpha_n)$$
$$= \alpha(\alpha_1, \ldots, \alpha_n) + \beta(\alpha_1, \ldots, \alpha_n)$$
$$= \alpha a + \beta a.$$

$$O\,III': \quad (\alpha\cdot\beta)a = (\alpha\cdot\beta)(\alpha_1, \ldots, \alpha_n) = ((\alpha\cdot\beta)\alpha_1, \ldots, (\alpha\cdot\beta)\alpha_n)$$
$$= (\alpha(\beta\alpha_1), \ldots, \alpha(\beta\alpha_n)) = \alpha(\beta\alpha_1, \ldots, \beta\alpha_n)$$
$$= \alpha(\beta(\alpha_1, \ldots, \alpha_n)) = \alpha(\beta a).$$

$$O\,IV: \quad \varepsilon a = \varepsilon(\alpha_1, \ldots, \alpha_n) = (\varepsilon\alpha_1, \ldots, \varepsilon\alpha_n) = (\alpha_1, \ldots, \alpha_n) = a$$

3. Es gilt:
$$o_{\mathfrak{R}} a = o_{\mathfrak{G}} \text{ wegen } \alpha a = (\alpha + o_{\mathfrak{R}})a = \alpha a + o_{\mathfrak{R}} a$$
$$(-\alpha)a = -(\alpha a) \text{ wegen } (\alpha + (-\alpha))a = \alpha a + (-\alpha)a = o_{\mathfrak{G}}.$$
Der Rest der Behauptung ist schon in F(35.2) enthalten.

4. Die Operatoranwendung auf die Elemente eines zulässigen Untermoduls von $\mathfrak{G}$ führt nach Definition nicht aus ihm heraus; ihre Eindeutigkeit sowie die Gültigkeit der übrigen Axiome aus D(36.1) ist aber sogar für alle Elemente von $\mathfrak{G}$ gewährleistet.

5. Je zwei Elemente a und b aus $\mathfrak{R}$ sind über $\mathfrak{R}$ stets linear abhängig wegen
$$b\cdot a + (-a)\cdot b = o.$$
Das Ideal $(2, x)$ von $\Gamma[x]$ besteht offensichtlich aus allen Polynomen, die ein gerades Absolutglied haben. Wäre nun $(2, x)$ ein Hauptideal $(f(x))$, so müßte $f(x)$ wegen $2 \in (f(x))$ nach F(32.5) eine Konstante und damit eine gerade Zahl sein. Dann hätten aber alle Polynome dieses Ideals nur gerade Koeffizienten im Widerspruch zu unserer obigen Feststellung, daß dies nur für die Absolutglieder zutrifft.

6. $\mathfrak{G}$ ist ein $\mathfrak{R}$-Modul, da die Forderungen aus D(36.1) nur einen Teil der in $\mathfrak{R}[x]$ ohnehin erfüllten Ringgesetze darstellen. Ein Erzeugendensystem ist etwa die Menge aller Potenzen $x^0, x^1, x^2, \ldots$ der Unbestimmten x, das auf Grund der Rechenregeln in $\mathfrak{R}[x]$ linear unabhängig ist.

   Ein endliches Erzeugendensystem kann es aber nicht geben. Für die Grade der endlich vielen Polynome eines solchen Systemes ließe sich nämlich eine obere Schranke angeben, und kein Polynom höheren Grades könnte aus ihnen linear kombiniert werden. In $\mathfrak{G}$ existieren aber Polynome beliebig hohen Grades.

7. Der Beweis verläuft völlig analog zu dem im Text bereits behandelten Spezialfall der Matrizen vom Typ $(1, n)$. Als Basis verwendet man dabei die $m \cdot n$ Matrizen

$$e_{ik} = \begin{pmatrix} & \overset{k}{\vdots} & \\ \cdots & \varepsilon & \cdots \\ & \vdots & \end{pmatrix} (i \qquad \text{(für alle } i \text{ und } k\text{)},$$

deren Elemente bis auf das im Schnittpunkt der i-ten Zeile und der k-ten Spalte gleich o sind, während dort ε steht.

8. Die n-tupel $v_1, v_2, \ldots, v_n$ bilden ein Erzeugendensystem, da die im Text angegebenen Basiselemente $u_1, u_2, \ldots, u_n$ aus ihnen linear kombiniert werden können:

$$u_1 = v_1 \quad \text{und} \quad u_i = v_i - v_{i-1} \text{ für } i = 2, \ldots, n.$$

Aus $\sum_{i=1}^{n} \lambda_i v_i = o$ folgt sukzessive $\lambda_n = o$, $\lambda_{n-1} = o, \ldots, \lambda_1 = o$ und damit die lineare Unabhängigkeit von $v_1, \ldots, v_n$.

9. Es sei σ ein Operatorendomorphismus von $\mathfrak{G}$, der eine Basis $u_1, \ldots, u_n$ von $\mathfrak{G}$ in die Basis $\overline{u_1}, \ldots, \overline{u_n}$ von $\mathfrak{G}$ überführt. Es lassen sich also alle Elemente von $\mathfrak{G}$ eindeutig aus $\overline{u_1}, \ldots, \overline{u_n}$ linear kombinieren, also insbesondere

$$u_i = \sum_{k=1}^{n} \beta_{ik} \overline{u_k} \qquad (i = 1, \ldots, n).$$

Nun ist aber nach S(36.9) dem Operatorendomorphismus σ die Matrix $(\alpha_{ik}) \in \mathfrak{M}_n(\mathfrak{R})$ zugeordnet vermöge

$$\overline{u_i} = \sum_{k=1}^{n} \alpha_{ik} u_k \qquad (i = 1, \ldots, n).$$

Damit gelten die Relationen

$$\overline{u_i} = \sum_{k,l} \alpha_{ik} \beta_{kl} \overline{u_l}, \qquad u_i = \sum_{k,l} \beta_{ik} \alpha_{kl} u_l \qquad (i = 1, \ldots, n).$$

Da sowohl die $\overline{u_i}$ als auch die u_i linear unabhängig sind, gilt

$$\sum_{k} \alpha_{ik} \beta_{kl} = \sum_{k} \beta_{ik} \alpha_{kl} = \begin{cases} \varepsilon \text{ für } i = l, \\ o \text{ für } i \neq l. \end{cases}$$

Die Matrix (β_{ik}) ist also (zweiseitiges) Inverses der Matrix (α_{ik}), woraus nach S(36.10) die Behauptung folgt.

Die Umkehrung ist unmittelbar klar, da selbst Operatorisomorphismen Erzeugendensysteme in Erzeugendensysteme und linear unabhängige Elemente in linear unabhängige Elemente überführen.

Zu § 37

1. a) Die u_i sind linear unabhängig. $\Sigma \lambda_i u_i = o$ führt nämlich auf ein homogenes lineares Gleichungssystem von vier Gleichungen für die vier Unbekannten λ_i, dessen Koeffizientendeterminante nicht verschwindet. Offensichtlich hat $\mathfrak{G}$ die Dimension 4, also bilden die u_i nach F(37.7) eine Basis.

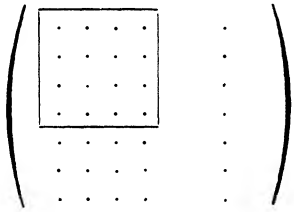
b) Wie man leicht sieht, ist $v_1 = u_1 - u_2$ und $v_2 = u_3 - 2u_4$. Wegen der linearen Unabhängigkeit des herzustellenden Systems $\{v_1, v_2, u_{i_1}, u_{i_2}\}$ dürfen also darin weder u_1 und u_2 noch u_3 und u_4 gleichzeitig auftreten.

Damit bleiben die folgenden vier Möglichkeiten:

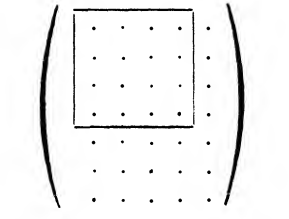
$$\{v_1, v_2, u_1, u_3\},$$
$$\{v_1, v_2, u_1, u_4\},$$
$$\{v_1, v_2, u_2, u_3\},$$
$$\{v_1, v_2, u_2, u_4\}.$$

Man überzeugt sich sofort, daß jedes dieser vier Systeme linear unabhängig und damit eine Basis für $\mathfrak{G}$ ist.

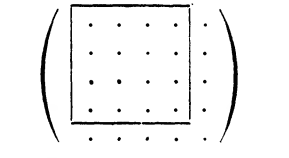
2. Die Bedingung von KRONECKER ist offensichtlich notwendig, aber auch hinreichend: Ohne Einschränkung der Allgemeinheit liege $D_r \neq o$ in der linken oberen Ecke von A:



Dann sind die r Spaltenvektoren von D_r und damit erst recht die (durch Punkte angedeuteten) ersten r Spaltenvektoren von A linear unabhängig. Würden nun $r+1$ linear unabhängige Spaltenvektoren von A existieren, so müßte es auch ein solches System von $r+1$ linear unabhängigen Spaltenvektoren geben, in dem die ersten r enthalten sind (Austauschsatz!). Daher genügt es, sich auf Matrizen der Form



zu beschränken. Eine analoge Betrachtung für die Zeilenvektoren dieser Matrizen führt darauf, daß dann bereits wenigstens eine Matrix der Form



den Rang $r+1$ haben müßte im Widerspruch zur Voraussetzung.

3. a) Das operatorhomomorphe Bild $\overline{\mathfrak{G}}$ einer Gruppe $\mathfrak{G}$ mit einem Operatorenbereich ist entsprechend der zitierten Aufgabe eine Gruppe mit demselben Operatorenbereich, d. h., *O II* ist unter Voraussetzung von *O I* für $\overline{\mathfrak{G}}$ von selbst erfüllt.

b) Insbesondere ist das operatorhomomorphe Bild $\overline{\mathfrak{G}}$ eines $\mathfrak{R}$-Moduls $\mathfrak{G}$ über einem Ring $\mathfrak{R}$ selbst $\mathfrak{R}$-Modul. Es übertragen sich nämlich auch *O III* und *O III'* von $\mathfrak{G}$ auf $\overline{\mathfrak{G}}$:

O III: $(\alpha+\beta)a \to \overline{(\alpha+\beta)a} = (\alpha+\beta)\bar{a}$

$\alpha a + \beta a \to \overline{\alpha a + \beta a} = \overline{\alpha a} + \overline{\beta a} = \alpha\bar{a} + \beta\bar{a}$,

aus $(\alpha+\beta)a = \alpha a + \beta a$ folgt also $(\alpha+\beta)\bar{a} = \alpha\bar{a} + \beta\bar{a}$.

O III': $(\alpha\cdot\beta)a \to \overline{(\alpha\cdot\beta)a} = (\alpha\cdot\beta)\bar{a}$

$\alpha(\beta a) \to \overline{\alpha(\beta a)} = \alpha(\overline{\beta a}) = \alpha(\beta\bar{a})$,

aus $(\alpha\cdot\beta)a = \alpha(\beta a)$ folgt also $(\alpha\cdot\beta)\bar{a} = \alpha(\beta\bar{a})$.

c) Da offensichtlich ein Erzeugendensystem eines $\mathfrak{R}$-Moduls $\mathfrak{G}$ auf ein solches von $\overline{\mathfrak{G}}$ abgebildet wird, gilt weiterhin, daß das operatorhomomorphe Bild eines endlichen $\mathfrak{R}$-Moduls wieder ein endlicher $\mathfrak{R}$-Modul ist.

Damit ist unsere Behauptung bereits bewiesen, da nach F(37.3) für $\mathfrak{R} = \mathfrak{K}$ die Begriffe „endlicher $\mathfrak{K}$-Modul" und „endlicher Vektorraum über $\mathfrak{K}$" zusammenfallen.

4. Γ^+ ist über Γ eindimensionaler Vektorraum mit dem Basiselement $+1$ bzw. -1. Das operatorhomomorphe Bild $\Gamma^+/(m)$ ist nach 3 b) Γ-Modul und hat nach 3 c) zumindest [1] bzw. $[-1] = [m-1]$ als erzeugende Elemente (ja nach F(6.12 b) sogar alle primen Restklassen mod m, die also im allgemeinen keine Bilder der Basiselemente $+1$ bzw. -1 von Γ^+ zu sein brauchen). $\Gamma^+/(m)$ ist aber kein Vektorraum über Γ, da jedes Element $[a]$ für sich genommen wegen $m[a] = [ma] = [0]$ linear abhängig ist.

Zu § 38

1. Es sei $\mathfrak{A}$ eine Algebra mit Linkseinselement e_L. Dann ist $\mathfrak{R} \overset{\sim}{\longleftrightarrow} \mathfrak{R}e_L$ vermöge der Zuordnung $\alpha \to \alpha e_l$ für alle $\alpha \in \mathfrak{R}$, so daß man $\mathfrak{R}$ nach dem Ersetzungsverfahren gemäß S(29.5) mit $\mathfrak{R}e_L$ identifizieren kann. Die Zuordnung ist nämlich nach Konstruktion eindeutig und sogar eineindeutig; denn ist u ein Basiselement von $\mathfrak{A}$, so ergibt sich aus $\alpha e_L = \beta e_L$ auch $\alpha e_l u = \beta e_l u$, also $\alpha u = \beta u$ und damit $\alpha = \beta$ wegen der linearen Unabhängigkeit von u. Die Relationstreue folgt aus *O III*, *O II'* und *O III'*.

Ist umgekehrt $\mathfrak{R} \subseteq \mathfrak{A}$, so ist das Einselement ε des Unterringes $\mathfrak{R}$ Linkseinselement für den gesamten Ring $\mathfrak{A}$. Nach S(36.5) wirkt nämlich ε auf alle Elemente aus $\mathfrak{A}$ von links als Einsoperator.

2. Jede Algebra $\mathfrak{A}$ über $\mathfrak{R}$ im Sinne von D(38.1) gestattet die zusätzliche Festsetzung $\alpha a = a\alpha$, da wir nach Aufg. 1 von § 36 wegen der Kommutativität von $\mathfrak{R}$ zwischen der Operatoranwendung von links und von rechts nicht zu unterscheiden brauchen. Diese Forderung stellt also nur ausdrücklich fest, daß man beide Schreibweisen zuläßt.

3. Wir zeigen, daß aus der Gültigkeit von OII' die Kommutativität von $\mathfrak{R}$ folgt, falls man $\mathfrak{R}[x]$ als Vektorraum über $\mathfrak{R}$ auffaßt. Es gilt nämlich

$$(\alpha\beta)x^2 = \alpha(\beta x)(\alpha x) = (\beta x)(\alpha x) = \beta(x(\alpha x)) = \beta(\alpha x^2) = (\beta\alpha)x^2,$$

woraus nach den in Polynomringen gültigen Rechenregeln $\alpha\beta = \beta\alpha$ für alle α und β aus $\mathfrak{R}$ folgt.

4. Nach Anwendung des distributiven Gesetzes

$$\Big(\sum_{i,j} \alpha_i \beta_j u_i u_j\Big)\Big(\sum_k \gamma_k u_k\Big) = \sum_{i,j,k} (\alpha_i \beta_j u_i u_j)(\gamma_k u_k)$$

braucht nur jeder Summand bei festen i, j, k für sich umgeformt zu werden:

$$\begin{aligned}
&((\alpha_i\beta_j)(u_i u_j))(\gamma_k u_k)\\
&= (\alpha_i\beta_j)((u_i u_j)(\gamma_k u_k)) \quad \text{gemäß} \quad (\alpha a)b = \alpha(ab)\\
&= (\alpha_i\beta_j)(\gamma_k((u_i u_j)u_k)) \quad \text{gemäß} \quad a(\alpha b) = \alpha(ab)\\
&= ((\alpha_i\beta_j)\gamma_k)((u_i u_j)u_k) \quad \text{gemäß} \quad \alpha(\beta a) = (\alpha\beta)a.
\end{aligned}$$

Ähnlich schließt man für $a(bc)$.

5. Bereits in § 31 haben wir die Quaternionen als Zahlenpaare komplexer Zahlen gekennzeichnet, wonach aus den Betrachtungen in § 36 schon der erste Teil der Behauptung folgt.

Dagegen ist OII' nicht erfüllt, wie etwa das aus $\alpha(ab) = a(\alpha b)$ durch Einsetzung von $\alpha = i$, $a = j$, $b = k$ folgende Gegenbeispiel lehrt.

Wir bemerken noch, daß man selbstverständlich über dem Körper der komplexen Zahlen mit der Basis $\{1, j\}$ und der für diese Elemente erklärten (assoziativen) Multiplikation $1 \cdot 1 = 1$, $1 \cdot j = j \cdot 1 = j$, $j \cdot j = -1$ eine Algebra erhält. Diese ist dann wohl als Vektorraum, aber nicht als Algebra isomorph zum Quaternionenkörper, da die Relationstreue bezüglich der Multiplikation nicht gilt, wie aus der entsprechenden Überlegung in § 31 hervorgeht.

6. Man erhält der Reihe nach die Elemente

$$0,\ 0,\ \tfrac{2}{3}s_1 + \tfrac{1}{3}s_3 - \tfrac{1}{3}s_4 + \tfrac{1}{3}s_5.$$

Im Fall a) liegen also zwei Nullteiler vor, im Fall b) ein sogenanntes *nilpotentes* Element, von dem eine Potenz (hier die zweite) gleich 0 ist, im Fall c) ein sogenanntes *idempotentes* Element, dessen Quadrat mit ihm selbst übereinstimmt.

Zu § 39

1. a) $a \mid a$ wegen $a = ae$.
   b) $e \mid a$ wegen $a = ea$.
   c) $a \mid o$ wegen $o = ao$, während aus $o \mid a$ folgt $a = ox = o$.
   d) Aus $a = bx$ folgt $ac = b(xc)$.

e) Aus $a = bx$ folgt $ac = (bc)x$ und umgekehrt für $c \neq 0$.

f) Aus $a_2 = a_1 x_1$ und $a_3 = a_2 x_2$ folgt $a_3 = a_1(x_1 x_2)$.

g) Aus $a_1 = b_1 x_1$ und $a_2 = b_2 x_2$ folgt $a_1 a_2 = (b_1 b_2)(x_1 x_2)$.

h) Aus $a_1 = b x_1$ und $a_2 = b x_2$ folgt $c_1 a_1 + c_2 a_2 = b(c_1 x_1 + c_2 x_2)$.

2. Es sei $\varepsilon = f(x)$ eine Einheit von $\mathfrak{R}[x]$. Dann existiert also in $\mathfrak{R}[x]$ ein zu ε inverses Element $\varepsilon^{-1} = g(x)$ mit

$$\varepsilon \varepsilon^{-1} = f(x) g(x) = e .$$

Nach F(32.5b) ist aber der Grad des Produktes $f(x) g(x)$ gleich der Summe der Grade von $f(x)$ und $g(x)$, d. h., $f(x)$ und $g(x)$ haben den Grad 0, sind also beides Elemente von $\mathfrak{R}$ und dort ersichtlich Einheiten.

Andererseits ist klar, daß jede Einheit von $\mathfrak{R}$ auch Einheit von $\mathfrak{R}[x]$ ist.

3. Wir gehen wieder davon aus, daß $\varepsilon = u + v\sqrt{k}$ eine Einheit des Ringes $\mathfrak{R} = \Gamma + \Gamma\sqrt{k}$ ist und also ein inverses Element $\varepsilon^{-1} = x + y\sqrt{k}$ in $\mathfrak{R}$ existiert:

$$(u + v\sqrt{k})(x + y\sqrt{k}) = 1.$$

Unter Berücksichtigung des in § 29 erwähnten Automorphismus von $\Gamma + \Gamma\sqrt{k}$, der durch die Zuordnung $a + b\sqrt{k} \to a - b\sqrt{k}$ gegeben ist, folgt die Gleichung

$$(u - v\sqrt{k})(x - y\sqrt{k}) = 1.$$

Durch Multiplikation ergibt sich damit

$$N(\varepsilon) \cdot N(\varepsilon^{-1}) = 1,$$

woraus bereits $N(\varepsilon) = \pm 1$ folgt.

Umgekehrt erhält man aus

$$N(\varepsilon) = (u + v\sqrt{k})(u - v\sqrt{k}) = \pm 1$$

unmittelbar $\varepsilon \mid 1$.

Einheiten von $\Gamma + \Gamma i$*:*

Die Gleichung $N(\varepsilon) = u^2 + v^2 = \pm 1$ ist ersichtlich nur durch die Paare $u = \pm 1$, $v = 0$ und $u = 0$, $v = \pm 1$ lösbar.

Einheiten von $\Gamma + \Gamma\sqrt{-5}$ *und* $\Gamma + \Gamma\sqrt{-6}$*:*

Beide Ringe haben nur die Einheiten ± 1. Die entsprechenden Gleichungen

$$u^2 + 5v^2 = \pm 1 \text{ bzw. } u^2 + 6v^2 = \pm 1$$

sind nämlich offenbar nur durch $u = \pm 1$, $v = 0$ lösbar.

Einheiten von $\Gamma + \Gamma\sqrt{26}$*:*

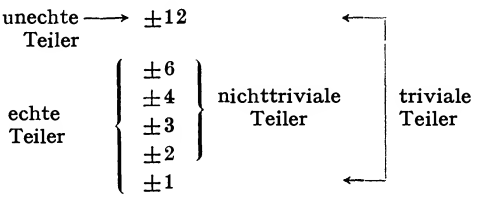
Hier handelt es sich um die Lösung der Gleichung

$$u^2 - 26v^2 = \pm 1,$$

die offensichtlich auch durch $u = \pm 1$, $v = 0$ gelöst wird. Eine weitere Lösung ist etwa $u = \pm 5$, $v = \pm 1$, so daß $5 - \sqrt{26}$, $-5 + \sqrt{26}$, $5 + \sqrt{26}$, $-5 - \sqrt{26}$ Einheiten sind. Alle Potenzen dieser Elemente sind aber nach F(39.4) wieder Einheiten; das liefert bereits unendlich viele Einheiten von $\Gamma + \Gamma\sqrt{26}$.

4. Aus $a \cong b$, also $a = \varepsilon b$ und $b = \varepsilon^{-1}a$, folgt $a \in (b)$ und $b \in (a)$, d. h. aber $(a) \subseteq (b)$ und $(b) \subseteq (a)$.

   Umgekehrt ergibt sich aus $(a) = (b)$, daß $a = r_1 b$ und $b = r_2 a$ und damit $a \cong b$ ist.

5. 

6. Es sei c eine Einheit von $\mathfrak{R}$. Dann folgt aus $c \cong e$ und $c = ab$ mit $a \cong e$ und $b \cong e$ die Unzerlegbarkeit von c.

   Es sei weiterhin $c = p$ Primelement von $\mathfrak{R}$. Dann kommen für die in $p = ab$ auftretenden Teiler a und b gemäß D(39.7) nur Einheiten oder zu p assoziierte Elemente in Frage. Dabei ist der Fall $a \cong b \cong e$ unmöglich, da dann auch p eine Einheit wäre im Widerspruch zu D(39.7). Desgleichen entfällt $a \cong b \cong p$, also $a = \varepsilon_1 p$, $b = \varepsilon_2 p$; daraus folgte nämlich $p = ab = \varepsilon_1 \varepsilon_2 p^2 = \varepsilon p^2$, d. h. $e = \varepsilon p$ und damit wieder $p \cong e$. Die beiden verbleibenden Möglichkeiten $a \cong p$, $b \cong e$ oder $a \cong e$, $b \cong p$ besagen gerade die Unzerlegbarkeit von p.

   Umgekehrt folgt aus der Unzerlegbarkeit von c, daß jeder Teiler von c entweder eine Einheit oder assoziiert zu c ist; diese Eigenschaft besitzen aber gerade die Einheiten und die Primelemente von $\mathfrak{R}$.

7. Es sei $d' \cong (a_1, a_2, \ldots, a_{n-1})$ und $d \cong (d', a_n)$. Dann gilt

$$d \mid a_n \text{ und } d \mid d', \text{ also } d \mid a_n \text{ und } d \mid a_1, \ldots, d \mid a_{n-1},$$

   letzteres wegen $d' \mid a_1, \ldots, d' \mid a_{n-1}$. Andererseits folgt für einen gemeinsamen Teiler t von $a_1, \ldots, a_n$

$$t \mid d' \text{ und } t \mid a_n, \text{ also } t \mid d.$$

   Damit ist also $d \cong (a_1, a_2, \ldots, a_n)$.

   Entsprechend schließt man für das kleinste gemeinsame Vielfache.

8. Der größte gemeinsame Teiler mehrerer Polynome ist Vielfaches jedes gemeinsamen Teilers dieser Polynome, woraus bereits nach F(32.5) die Behauptung folgt.

   Entsprechend ergibt sich die zweite Aussage daraus, daß das kleinste gemeinsame Vielfache Teiler jedes gemeinsamen Vielfachen ist.

Zu § 40

1. Offensichtlich ist das im Text angegebene Divisionsverfahren auch in $\mathfrak{R}[x]$ jedenfalls dann durchführbar, wenn der höchste Koeffizient b_m von $h(x)$ eine Einheit aus $\mathfrak{R}$ ist, sonst jedoch nur bei geeigneter Wahl von $f(x)$.

2. Der Quotient $q(x)$ von $f(x)$ und $h(x)$ läßt sich in $\mathfrak{K}[x]$ nach dem Verfahren der Division mit Rest berechnen. Da jedoch alle Koeffizienten von $f(x)$ und $h(x)$ in $\mathfrak{K}$ liegen und überdies der höchste Koeffizient von $h(x)$ eine Einheit von $\mathfrak{K}$ ist, führt dieses Verfahren, wie unter 1. festgestellt, aus $\mathfrak{K}[x]$ nicht heraus; also gilt $q(x) \in \mathfrak{K}[x]$.

3. Nach unserer Lösungsanleitung dürfen wir uns auf die Abschätzung von $N(\varrho)$ beschränken:

$$N(\varrho) = |\varrho|^2 = |\beta|^2 \cdot |\gamma' - \gamma|^2.$$

Für Real- und Imaginärteil von $\gamma' - \gamma = x + yi$ gilt nun nach Konstruktion: $|x| \leqq \frac{1}{2}$, $|y| \leqq \frac{1}{2}$. Daraus folgt

$$|\gamma' - \gamma|^2 = x^2 + y^2 \leqq \tfrac{1}{4} + \tfrac{1}{4} < 1.$$

Mithin ergibt sich $N(\varrho) < N(\beta)$.

4. In den Beweis von S(40.15) geht offensichtlich die Existenz eines Einselementes in $\mathfrak{K}$ nicht ein, wir können also $\mathfrak{a} = \mathfrak{K}a$ für alle Ideale von $\mathfrak{K}$ verwenden. Insbesondere muß es dann für das Ideal $\mathfrak{K}$ ein solches erzeugendes Element x mit

$$\mathfrak{K} = \mathfrak{K}x$$

geben. Wegen $x \in \mathfrak{K}$ existiert zufolge dieser Gleichung ein Element $y \in \mathfrak{K}$ mit

$$x = yx.$$

Dieses Element y ist Einselement in $\mathfrak{K}$, denn es reproduziert jedes beliebige Element $u = vx$ von $\mathfrak{K}$ vermöge:

$$uy = vxy = vx = u.$$

5. Ist ε Einheit von $\mathfrak{K}$, so folgt aus $\varepsilon \cdot \varepsilon^{-1} = e$

$$g(\varepsilon \cdot \varepsilon^{-1}) = g(e) \geqq g(\varepsilon).$$

Andererseits ist

$$g(e \cdot \varepsilon) = g(\varepsilon) \geqq g(e).$$

Daher ist $g(\varepsilon) = g(e)$ für jede Einheit ε von $\mathfrak{K}$.

Gilt umgekehrt für ein Element $a \in \mathfrak{K}$ die Gleichung $g(a) = g(e)$, so muß in

$$e = aq + r$$

der Rest $r = o$, also a Einheit von $\mathfrak{K}$ sein. Andernfalls folgt nämlich aus $g(r) < g(a)$ der Widerspruch

$$g(e) = g(a) > g(r) = g(r \cdot e) \geqq g(e).$$

6. Aus $a \cong b$, also $a = \varepsilon \cdot b$ und $b = \varepsilon^{-1} \cdot a$ folgt $g(a) = g(b)$ wegen

$$g(a) = g(\varepsilon \cdot b) \geqq g(b),$$
$$g(b) = g(\varepsilon^{-1} \cdot a) \geqq g(a).$$

Die Umkehrung ist zwar etwa für Γ richtig, jedoch z. B. nicht für $\mathrm{P}[x]$; so ist etwa

$$g(x^2 - 3) = g(x^2 + x + 1),$$

ohne daß die beiden Polynome assoziiert sind.

7. a)
$$\begin{aligned} 144 &= 89\cdot 1 + 55 \\ 89 &= 55\cdot 1 + 34 \\ 55 &= 34\cdot 1 + 21 \\ 34 &= 21\cdot 1 + 13 \\ 21 &= 13\cdot 1 + 8 \\ 13 &= 8\cdot 1 + 5 \\ 8 &= 5\cdot 1 + 3 \\ 5 &= 3\cdot 1 + 2 \\ 3 &= 2\cdot 1 + 1 \\ 2 &= 1\cdot 2 + 0 \end{aligned} \qquad \begin{aligned} 55 &= 144 - 89 \\ 34 &= -144 + 2\cdot 89 \\ 21 &= 2\cdot 144 - 3\cdot 89 \\ 13 &= (-3)\cdot 144 + 5\cdot 89 \\ 8 &= 5\cdot 144 - 8\cdot 89 \\ 5 &= (-8)\cdot 144 + 13\cdot 89 \\ 3 &= 13\cdot 144 - 21\cdot 89 \\ 2 &= (-21)\cdot 144 + 34\cdot 89 \\ 1 &= 34\cdot 144 - 55\cdot 89 \end{aligned}$$

Also ist $(144, 89) \cong 1 = 34\cdot 144 - 55\cdot 89$.

Verzichtet man darauf, beim euklidischen Algorithmus in Γ die Reste positiv zu wählen, kommt man mitunter schneller zum Ziel:

$$\begin{aligned} 144 &= 89\cdot 2 - 34 \\ 89 &= 34\cdot 3 - 13 \\ 34 &= 13\cdot 3 - 5 \\ 13 &= 5\cdot 3 - 2 \\ 5 &= 2\cdot 2 + 1 \\ 2 &= 1\cdot 2 + 0 \end{aligned} \qquad \begin{aligned} 34 &= -144 + 2\cdot 89 \\ 13 &= (-3)\cdot 144 + 5\cdot 89 \\ 5 &= (-8)\cdot 144 + 13\cdot 89 \\ 2 &= (-21)\cdot 144 + 34\cdot 89 \\ 1 &= 34\cdot 144 - 55\cdot 89 \end{aligned}$$

b)
$$\begin{aligned} 2x^6+3x^5-4x^4-5x^3-2x-2 &= (x^5-2x^3-1)(2x+3)+(x^3+1) \\ x^5-2x^3-1 &= (x^3+1)(x^2-2)+(-x^2+1) \\ x^3+1 &= (-x^2+1)(-x)+(x+1) \\ -x^2+1 &= (x+1)(-x+1)+0. \end{aligned}$$

Der größte gemeinsame Teiler $(x+1)$ von

$$\begin{aligned} f(x) &= 2x^6+3x^5-4x^4-5x^3-2x-2, \\ h(x) &= x^5-2x^3-1 \end{aligned}$$

läßt sich wie folgt linear kombinieren:

$$\begin{aligned} x^3+1 &= f(x) - (2x+3)\cdot h(x) \\ -x^2+1 &= -(x^2-2)\cdot f(x) + (2x^3+3x^2-4x-5)\cdot h(x) \\ x+1 &= (-x^3+2x+1)\cdot f(x) + (2x^5+3x^3-4x^2-7x-3)\cdot h(x). \end{aligned}$$

c) Um aus $\alpha = 31 - 2i$ und $\beta = 6 + 8i$ gemäß der allgemeinen Theorie die Elemente γ und ϱ zu bestimmen, berechnen wir zunächst

$$\gamma' = \frac{\alpha}{\beta} = \frac{31-2i}{6+8i} = \frac{(31-2i)(6-8i)}{(6+8i)(6-8i)} = \frac{17}{10} - \frac{13}{5}i.$$

Daraus folgt $\gamma = 2 - 3i$ und damit

$$31 - 2i = (6+8i)(2-3i) - 5.$$

So rechnen wir weiter und erhalten:

$$\frac{6+8i}{-5} = -\frac{6}{5} - \frac{8}{5}i$$

$$6 + 8i = (-5)(-1 - 2i) + (1 - 2i).$$

Der nächste Schritt liefert:

$$\frac{-5}{1-2i} = \frac{(-5)(1+2i)}{(1-2i)(1+2i)} = -1 - 2i,$$

d. h., die Division geht auf:

$$-5 = (1 - 2i)(-1 - 2i) + 0.$$

Also ist $(31 - 2i,\ 6 + 8i) \cong 1 - 2i$.

Für die Linearkombination ergibt sich der Reihe nach:

$$-5 = \alpha - (2 - 3i)\beta$$

$$1 - 2i = \beta + (1 + 2i)(-5) = (1 + 2i)\alpha + (-7 - i)\beta.$$

8. Wir zeigen, daß das Ideal (a, x) unter den angegebenen Voraussetzungen kein Hauptideal ist, indem wir die aus $(a, x) = (f(x))$ mit $f(x) \in \mathfrak{R}[x]$ folgenden Beziehungen

$$a \in (f(x)): \quad a = r(x) \cdot f(x)$$
$$x \in (f(x)): \quad x = s(x) \cdot f(x)$$
$$f(x) \in (a, x): \quad f(x) = u(x) \cdot a + v(x) \cdot x$$

mit $r(x)$, $s(x)$, $u(x)$, $v(x)$ aus $\mathfrak{R}[x]$ zum Widerspruch führen.

Aus der ersten Gleichung ergibt sich nämlich (vgl. F(32.5)), daß sowohl $r(x)$ als auch $f(x)$ Polynome 0-ten Grades, also Elemente r_0 bzw. f_0 von $\mathfrak{R}$ sein müssen. Damit folgt entsprechend aus der zweiten Gleichung, d. h. aus $x = s(x) \cdot f_0$ durch Koeffizientenvergleich $s(x) = s_0 \cdot x$ mit $s_0 \in \mathfrak{R}$ und $s_0 \cdot f_0 = e$. Insbesondere ist also f_0 eine Einheit von $\mathfrak{R}$. Schließlich ergibt sich aus der dritten Gleichung $f_0 = u(x) \cdot a + v(x) \cdot x$ auf die gleiche Weise $f_0 = u_0 \cdot a$ mit $u_0 \in \mathfrak{R}$. Damit wäre aber a als Teiler der Einheit f_0 selbst eine Einheit von $\mathfrak{R}$ im Widerspruch zur Wahl von a.

9. Man findet unmittelbar in $\mathfrak{R} = \Gamma + \Gamma\sqrt{-6}$ die Zerlegungen

$$6 = 2 \cdot 3 = (\sqrt{-6}) \cdot (-\sqrt{-6}).$$

Da nach Aufg. 3 von § 39 der Ring $\mathfrak{R}$ nur die Einheiten $+1$ und -1 hat, sind die beiden Zerlegungen jedenfalls wesentlich verschieden. Wir müssen aber noch zeigen, daß die auftretenden Faktoren 2, 3 und $\sqrt{-6}$ in $\mathfrak{R}$ unzerlegbar sind und daß darüber hinaus keine weiteren (von den genannten wesentlich verschiedenen) Zerlegungen von 6 existieren. Beides wird erledigt durch den Nachweis, daß 6 nur 2, 3 und $\sqrt{-6}$ (bzw. die zu ihnen assoziierten Elemente) als nichttriviale Teiler t besitzt. Dazu betrachtet man die Norm

$$N(t) = N(x + y\sqrt{-6}) = x^2 + 6y^2,$$

die gemäß unseren Überlegungen im Text ein (positiver) nichttrivialer Teiler von $N(6) = 36$, also gleich 2, 3, 4, 6, 9, 12 oder 18 sein muß. Nun sind offensichtlich die Gleichungen

$$x^2 + 6y^2 = z \quad \text{mit} \quad z = 2, 3, 12, 18$$

nicht mit ganzen Zahlen x, y lösbar, während die Gleichungen

$$x^2 + 6y^2 = 4 \quad \text{bzw.} \quad x^2 + 6y^2 = 6 \quad \text{bzw.} \quad x^2 + 6y^2 = 9$$

genau die Lösungen

$$x = \pm 2, y = 0 \quad \text{bzw.} \quad x = 0, y = \pm 1 \quad \text{bzw.} \quad x = \pm 3, y = 0$$

besitzen.

10. Im Unterschied zur Aufg. 9 ist es schwieriger, in $\mathfrak{R} = \Gamma + \Gamma\sqrt{-5}$ von $21 = 3 \cdot 7$ wesentlich verschiedene Zerlegungen unmittelbar anzugeben. Wir gehen daher den konstruktiven Weg, von vornherein alle nichttrivialen Teiler von 21 zu bestimmen (natürlich unter Beachtung der beiden Einheiten $+1$ und -1 von $\mathfrak{R}$). Solche Teiler $t = x + y\sqrt{-5}$ müssen wieder eine Norm $N(t) = x^2 + 5y^2$ haben, die ein (positiver) nichttrivialer Teiler von $N(21) = 3^2 \cdot 7^2$ ist. Man überzeugt sich nun durch Einsetzen rasch, daß die Gleichungen

$$x^2 + 5y^2 = z \quad \text{mit} \quad z = 3, 7, 63, 147$$

keine ganzzahligen Lösungen x, y besitzen, während die Gleichungen

$$x^2 + 5y^2 = 9 \quad \text{bzw.} \quad x^2 + 5y^2 = 21 \quad \text{bzw.} \quad x^2 + 5y^2 = 49$$

auf folgende Elemente aus $\mathfrak{R} = \Gamma + \Gamma\sqrt{-5}$ führen:

$$(\pm 1)(3 + 0 \cdot \sqrt{-5}) \text{ bzw. } (\pm 1)(4 + 1 \cdot \sqrt{-5}) \text{ bzw. } (\pm 1)(7 + 0 \cdot \sqrt{-5})$$
$$(\pm 1)(2 + 1 \cdot \sqrt{-5}) \qquad (\pm 1)(4 - 1 \cdot \sqrt{-5}) \qquad (\pm 1)(2 + 3 \cdot \sqrt{-5})$$
$$(\pm 1)(2 - 1 \cdot \sqrt{-5}) \qquad (\pm 1)(1 + 2 \cdot \sqrt{-5}) \qquad (\pm 1)(2 - 3 \cdot \sqrt{-5})$$
$$(\pm 1)(1 - 2 \cdot \sqrt{-5})$$

Es ist nun zu beachten, daß die bisher benutzte Normbedingung natürlich nur notwendig ist, d. h., sie wählt alle diejenigen Elemente von $\mathfrak{R}$ aus, die überhaupt als Teiler in Frage kommen können. Man hat sich also jetzt durch geeignete Produktbildung davon zu überzeugen, welche der oben angegebenen Elemente in der Tat Teiler sind. Auch dabei ist die Beachtung der Normbedingung nützlich: Es kommen hier nur Produktbildungen je eines Elementes der ersten Kolonne mit einem der dritten Kolonne und solche innerhalb der mittleren Kolonne in Frage. Die Ausführung dieser Multiplikationen führt auf die folgenden wesentlich verschiedenen Zerlegungen

$$21 = 3 \cdot 7 = (4 + \sqrt{-5})(4 - \sqrt{-5}) = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5}),$$

während $\pm(2 + \sqrt{-5})$, $\pm(2 - \sqrt{-5})$, $\pm(2 + 3\sqrt{-5})$ und $\pm(2 - 3\sqrt{-5})$ trotz Erfüllung der Normbedingung keine Teiler von 21 sind.

Zu § 41

1. $\alpha_2 = 2,\ \alpha_3 = 0,\ \alpha_5 = 1,\ \alpha_7 = 0,\ \alpha_{11} = 1,\ \alpha_{13} = 0,\ \alpha_{17} = 1, \ldots$
$\beta_2 = 0,\ \beta_3 = 1,\ \beta_5 = 0,\ \beta_7 = 0,\ \beta_{11} = 2,\ \beta_{13} = 0,\ \beta_{17} = 1, \ldots$
$\gamma_2 = 2,\ \gamma_3 = 1,\ \gamma_5 = 1,\ \gamma_7 = 0,\ \gamma_{11} = 2,\ \gamma_{13} = 0,\ \gamma_{17} = 1, \ldots$
$\delta_2 = 0,\ \delta_3 = 0,\ \delta_5 = 0,\ \delta_7 = 0,\ \delta_{11} = 1,\ \delta_{13} = 0,\ \delta_{17} = 1, \ldots$.

Es gilt $c = [a, b]$, $d = (a, b)$ und damit auch $ab = cd$.

2. $(a_1, a_2, \ldots, a_n) \cong e$ gilt genau dann, wenn jedes Primelement p in wenigstens einem a_i mit dem Exponenten 0 auftritt.

$(a_i, a_j) \cong e$ für alle i und j $(i \neq j)$ gilt genau dann, wenn jedes Primelement p in höchstens einem a_i mit einem von 0 verschiedenen Exponenten auftritt.

3. Die Äquivalenz entspricht der Beziehung der Exponenten

$$\mathrm{Max}\,(\alpha_p, \beta_p, \ldots, \varrho_p) = \alpha_p + \beta_p + \ldots + \varrho_p \text{ für alle } p.$$

Letztere ist genau dann erfüllt, wenn für jedes p höchstens ein Exponent aus der Reihe $\alpha_p, \beta_p, \ldots, \varrho_p$ verschieden von 0 ist. Dies ergibt nach Aufg. 2 die Behauptung.

4. Aus $\alpha_p \leqq \mu_p$, $\beta_p \leqq \mu_p, \ldots$ folgt $\mathrm{Max}\,(\alpha_p, \beta_p, \ldots) \leqq \mu_p$ und allgemeiner aus $\alpha_p \leqq \alpha_p'$, $\beta_p \leqq \beta_p' \ldots$, auch $\mathrm{Max}\,(\alpha_p, \beta_p, \ldots) \leqq \mathrm{Max}\,(\alpha_p', \beta_p', \ldots)$ für alle p.

5. In jedem ZPE-Ring $\mathfrak{R}$ gelten

a) der Teilerkettensatz, da nach S(41.5) jedes Element $a \in \mathfrak{R}$ überhaupt nur endlich viele Teiler hat;

b) die erste Aussage von S(40.11) über die Existenz des größten gemeinsamen Teilers (vgl. S(41.7));

c) die Aussagen von S(40.12), wie sich unmittelbar aus der Existenz und Eindeutigkeit der Primzerlegung ergibt;

d) die Aussage von F(40.13), wie man ebenso oder aus S(40.12) folgert.

Dagegen gilt die zweite Aussage von S(40.11) über die lineare Kombinierbarkeit des größten gemeinsamen Teilers nicht in jedem ZPE-Ring. Um dafür ein Beispiel zu geben, müssen wir vorgreifend verwenden, daß $\Gamma[x]$ ein ZPE-Ring ist. In $\Gamma[x]$ haben aber die Polynome $x + 2$ und $x + 4$ offensichtlich den größten gemeinsamen Teiler 1, der sich jedoch nicht aus ihnen linear kombinieren läßt, da beide Absolutglieder durch 2 teilbar sind.

6. Für beliebige Elemente a und b des Quotientenkörpers von $\mathfrak{R}$ ist nach S(41.14) $a \cong b^n$ gleichbedeutend mit $\alpha_p = n \cdot \beta_p$ für alle p. Wegen $n > 1$ folgt also aus $\alpha \geqq 0$ stets $\beta_p \geqq 0$, so daß (vgl. S(41.15)) für Elemente a aus $\mathfrak{R}$, wenn überhaupt, nur n-te Wurzeln b aus $\mathfrak{R}$ in Frage kommen.

Bemerkung: Insbesondere folgt aus dem Bewiesenen, daß die n-te Wurzel einer Primzahl p stets irrational ist. Im Schulunterricht pflegt man diesen Sachverhalt meist für $\sqrt{2}$ zu beweisen.

Wie man sich sofort überzeugt, beruht der übliche Schluß „Wäre $\sqrt{2} = \frac{m}{n}$ und dieser Bruch so weit wie möglich gekürzt, so ..." genau auf der obigen Überlegung für die Primzahl $p = 2$. Er wäre wohl auch für den Schüler wesentlich verständlicher, wenn man ihn durch Zerlegung von m und n in Primfaktoren in der Form

$$\sqrt{2} = \frac{p_1 p_2 \cdots p_r}{q_1 q_2 \cdots q_s}, \text{ also } 2^1 \cdot (q_1 q_2 \cdots q_s)^2 = (p_1 p_2 \cdots p_r)^2$$

ansetzen würde und durch Vergleich der links und rechts auftretenden Potenz von 2 zum Widerspruch gelangte. Dies würde aber eine ausdrückliche Feststellung der sonst weniger offensichtlich verwendeten Eindeutigkeit der Primzerlegung erfordern. (In den oben zitierten üblichen Beweis geht sie selbstverständlich auch ein, nämlich in die Annahme „$\frac{m}{n}$ so weit wie möglich gekürzt", wozu dann $2 \mid m$ und $2 \mid n$ im Widerspruch steht!)

7. Aus $(a, m) \cong d$ und $a' = a + rm$ folgt $(a', m) \cong d$ wie in B(2.8d).

8. Entweder kann man die der Aufgabe entsprechende diophantische Gleichung

$$4x - 7y = 9$$

durch Herstellung einer Linearkombination

$$2 \cdot 4 + 1(-7) = 1$$

mit Hilfe des euklidischen Algorithmus direkt lösen:

$$\begin{aligned} x_0 &= 2 \cdot 9 = 18 & x &= x_0 + (-7)g \\ y_0 &= 1 \cdot 9 = 9 & y &= y_0 - 4g. \end{aligned} \qquad (*)$$

Andernfalls geht man etwa zu der Kongruenz

$$4x \equiv 9 \equiv 2 \ (7)$$

über, deren Lösung

$$x_0 = 4, \ x = 4 + 7g \qquad (**)$$

man entweder durch Probieren oder durch Behandlung der Kongruenz

$$4x \equiv 1 \ (7)$$

entsprechend Aufg. 4 von § 33 gewinnt.

Wie man sich leicht überzeugt, liefern (*) und (**) dieselben Werte für x und damit auch für y.

Entsprechend behandelt man die übrigen Aufgaben und erhält (vgl. auch Aufg. 5 von § 33) die Lösungen

$$\begin{aligned} x &= 9 + 15g & x &= 23 + 36g \\ y &= -9 - 17g, & y &= -26 - 41g. \end{aligned}$$

9. Der Ansatz

$$\frac{1}{315} = \frac{1}{3^2 \cdot 5 \cdot 7} = \frac{x}{3^2} + \frac{y}{5} + \frac{z}{7}$$

führt auf die diophantische Gleichung

$$1 = 35x + 63y + 45z.$$

Der Aufgabenstellung nach sind für die Lösungen die Beschränkungen $|x| < 9$, $|y| < 5$, $|z| < 7$ gegeben. Aus

$$35x + 63y = 1 - 45z$$

erhält man die Lösbarkeitsbedingung

$$45z \equiv 1 \ (7)$$

mit den brauchbaren Lösungen $z = 5$ und $z = -2$.

Die entsprechenden diophantischen Gleichungen für x und y liefern

$$\frac{1}{315} = \frac{-1}{9} + \frac{-3}{5} + \frac{5}{7} = \frac{-1}{9} + \frac{2}{5} + \frac{-2}{7} = \frac{8}{9} + \frac{-3}{5} + \frac{-2}{7}.$$

10. $$\frac{2u^3 + \frac{25}{2}u^2 + 4u - 2}{u^4 + 3u^3 - 5u^2 - 12u + 4} = \frac{-2u + \frac{1}{2}}{u^2 + 3u - 1} + \frac{2}{u+2} + \frac{2}{u-2}.$$

11. $$\frac{78}{53} = 1 + \cfrac{1}{2 + \cfrac{1}{8 + \frac{1}{3}}} \qquad \frac{67}{92} = \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{2 + \frac{1}{8}}}}}$$

$$\frac{1217}{510} = 2 + \cfrac{1}{2 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{3 + \cfrac{1}{5 + \frac{1}{2}}}}}}}$$

Zu § 42

1. Wir geben hier nur ein Beispiel für die Aussage h) an. Es sei

$$(b) = 6\Gamma,\ (a_1) = 60\Gamma,\ (a_2) = 42\Gamma,\ (c_1) = 4\Gamma,\ (c_2) = 5\Gamma.$$

Dann gilt

$$6\Gamma \geqq 60\Gamma \text{ und } 6\Gamma \geqq 42\Gamma,$$

also auch

$$6\Gamma \geqq 4\Gamma \cdot 60\Gamma + 5\Gamma \cdot 42\Gamma = 240\Gamma + 210\Gamma = 30\Gamma.$$

2. Es gilt immer $(x_1 + x_2) \subseteqq (x_1) + (x_2)$, denn das rechts stehende Ideal enthält nach Definition der Komplexsumme das Element $x_1 + x_2$.
Als Beispiel geben wir (s. o.):
$$(450) = (240 + 210) \subset (240) + (210) = (30).$$
Dagegen ist:
$$(30) = (240 - 210) = (240) + (-210) = (30).$$

3. Nach S(42.7) ist die Summe der genannten Ideale
$$(x^3 - 2x^2 - x + 2) + (x^2 - 1) + (x^2 + x - 2)$$
$$= (x^3 - 2x^2 - x + 2,\ x^2 - 1,\ x^2 + x - 2)$$
nichts anderes als der größte gemeinsame Teiler dieser Ideale, also das von dem größten gemeinsamen Teiler der auftretenden Elemente erzeugte Hauptideal. Man berechnet ihn etwa mit Hilfe des euklidischen Algorithmus als das Polynom $x - 1$ und erhält damit:
$$(x^3 - 2x^2 - x + 2) + (x^2 - 1) + (x^2 + x - 2) = (x - 1).$$

4. Der Durchschnitt $(12) \cap (33) \cap (44)$ stimmt nach S(42.9) mit dem kleinsten gemeinsamen Vielfachen der auftretenden Ideale überein, ist also das vom kleinsten gemeinsamen Vielfachen 132 der drei Elemente 12, 33 und 44 erzeugte Hauptideal (132).

5. Das Ideal (x) von $\mathfrak{R}[x]$ ist Primideal, da der zu $\mathfrak{R}$ isomorphe Restklassenring $\mathfrak{R}[x]/(x)$ nullteilerfrei ist. Es ist aber nicht maximal, denn es gilt mit dem betrachteten Ideal (a, x):
$$(x) \subset (a, x) \subset \mathfrak{R}[x].$$
In der Tat liegt in beiden Fällen echtes Enthaltensein vor wegen
$$a \notin (x),\ a \in (a, x) \quad \text{bzw.} \quad e \notin (a, x),\ e \in \mathfrak{R}[x]$$
(aus $e \in (a, x)$, also $e = ra + ox$ folgte nämlich $a \cong e$).
Wir weisen noch darauf hin, daß diese Überlegung für die speziellen Ringe $\Gamma[x]$ und $\Gamma[x_1, \ldots, x_n] = \Gamma[x_1, \ldots, x_{n-1}][x_n]$ bereits in Aufgabe 6 von § 34 bzw. am Ende von § 34 durchgeführt wurden.

Zu § 43

1. Zunächst folgt $\mathfrak{a}(\mathfrak{b} + \mathfrak{c}) \supseteqq \mathfrak{a}\mathfrak{b} + \mathfrak{a}\mathfrak{c}$ aus $\mathfrak{a}(\mathfrak{b} + \mathfrak{c}) \supseteqq \mathfrak{a}\mathfrak{b}$ (wegen $o \in \mathfrak{c}$) und $\mathfrak{a}(\mathfrak{b} + \mathfrak{c}) \supseteqq \mathfrak{a}\mathfrak{c}$ (wegen $o \in \mathfrak{b}$). Andererseits ist jedes Element
$$\sum a_i(b_i + c_i) = \sum a_i b_i + \sum a_i c_i$$
von $\mathfrak{a}(\mathfrak{b} + \mathfrak{c})$ offensichtlich in $\mathfrak{a}\mathfrak{b} + \mathfrak{a}\mathfrak{c}$ enthalten.

2. Jedes Element des Produktes $\mathfrak{a} \cdot \mathfrak{b}$ ist eine endliche Summe
$$\sum_i A_i B_i \quad \text{mit} \quad \begin{cases} A_i = \sum_j r_{ij} a_j \in \mathfrak{a},\ r_{ij} \in \mathfrak{R}, \\ B_i = \sum_k s_{ik} b_k \in \mathfrak{b},\ s_{ik} \in \mathfrak{R}; \end{cases}$$
d. h., es ist
$$\sum_i A_i B_i = \sum_{i,j,k} (r_{ij} s_{ik}) a_j b_k.$$

Daraus folgt $$\mathfrak{a} \cdot \mathfrak{b} \subseteq (a_1 b_1, \ldots, a_j b_k, \ldots, a_n b_m),$$

während die umgekehrte Enthaltenseinsrelation unmittelbar klar ist.

Man kann auch unter Vermeidung jeder Rechnung die Behauptung aus dem distributiven Gesetz der Idealmultiplikation folgern, indem man $\mathfrak{a}$ und $\mathfrak{b}$ in Summen von Hauptidealen zerlegt:

$$[(a_1) + \ldots + (a_n)] \cdot [(b_1) + \ldots + (b_m)] = (a_1 b_1) + \ldots + (a_j b_k) + \ldots + (a_n b_m)$$

3. Wir betrachten zunächst die Beziehung „$\mathfrak{b} \supseteq \mathfrak{a}$", ohne jedoch auf unmittelbar ersichtliche Aussagen näher einzugehen:
   a) $\mathfrak{a} \supseteq \mathfrak{a}$.
   b) $\mathfrak{R} \supseteq \mathfrak{a}$.
   c) $\mathfrak{a} \supseteq (o)$, aber $(o) \supseteq \mathfrak{a}$ nur für $\mathfrak{a} = (o)$.
   d) Aus $\mathfrak{b} \supseteq \mathfrak{a}$ folgt $\mathfrak{b} \supseteq \mathfrak{a}\mathfrak{c}$ (wegen $\mathfrak{a} \supseteq \mathfrak{a}\mathfrak{c}$).
   e) Aus $\mathfrak{b} \supseteq \mathfrak{a}$ folgt $\mathfrak{b}\mathfrak{c} \supseteq \mathfrak{a}\mathfrak{c}$ (vgl. die stärkere Aussage g).
   f) Aus $\mathfrak{a}_1 \supseteq \mathfrak{a}_2$ und $\mathfrak{a}_2 \supseteq \mathfrak{a}_3$ folgt $\mathfrak{a}_1 \supseteq \mathfrak{a}_3$.
   g) Aus $\mathfrak{b}_1 \supseteq \mathfrak{a}_1$ und $\mathfrak{b}_2 \supseteq \mathfrak{a}_2$ folgt $\mathfrak{b}_1\mathfrak{b}_2 \supseteq \mathfrak{a}_1\mathfrak{a}_2$.
   (Alle Summen $\Sigma a_{i_1} a_{i_2} \in \mathfrak{a}_1\mathfrak{a}_2$ sind erst recht Summen $\Sigma b_{i_1} b_{i_2} \in \mathfrak{b}_1\mathfrak{b}_2$.)
   h) Aus $\mathfrak{b} \supseteq \mathfrak{a}_1$ und $\mathfrak{b} \supseteq \mathfrak{a}_2$ folgt $\mathfrak{b} \supseteq \mathfrak{c}_1\mathfrak{a}_1 + \mathfrak{c}_2\mathfrak{a}_2$.
   (Nach d) gilt $\mathfrak{b} \supseteq \mathfrak{c}_1\mathfrak{a}_1$ und $\mathfrak{b} \supseteq \mathfrak{c}_2\mathfrak{a}_2$, woraus wegen der Moduleigenschaft von $\mathfrak{b}$ die Behauptung folgt.)

   Entsprechend verfährt man mit der Beziehung „$\mathfrak{b} \mid \mathfrak{a}$", wobei sich alle Aussagen ohne weiteres aus D(43.3b) ergeben.

   Für a) und b) beachte man $\mathfrak{a} = \mathfrak{R}\mathfrak{a}$, bei h) geht das distributive Gesetz der Idealmultiplikation ein.

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

   Wir bemerken jedoch, daß in dieser Relation das Gleichheitszeichen wohl für Hauptideale eines ZPE-Ringes (nämlich wegen der Gültigkeit der entsprechenden Formel für Elemente, vgl. F(41.11)), nicht aber allgemein richtig ist. So gilt z. B. in $\mathfrak{R} = \Gamma[x]$ mit $\mathfrak{a} = (6, 3x)$ und $\mathfrak{b} = (x)$, also $\mathfrak{a} + \mathfrak{b} = (6, x)$ und $\mathfrak{a} \cap \mathfrak{b} = (3x)$:

$$(18x, 3x^2) = (\mathfrak{a} + \mathfrak{b})\,(\mathfrak{a} \cap \mathfrak{b}) \subset \mathfrak{a}\mathfrak{b} = (6x, 3x^2).$$

5. Gilt in einem Ring der Teilerkettensatz für Ideale, so gilt erst recht der Teilerkettensatz für Elemente. Eine nicht abbrechende Kette von Elementen

$$a_2 \| a_1,\ a_3 \| a_2, \ldots$$

würde nämlich gemäß Aufg. 4 von § 39 eine nicht abbrechende Teilerkette von Hauptidealen

$$(a_1) \subset (a_2) \subset (a_3) \subset \ldots$$

liefern. Umgekehrt kann man natürlich aus dem Teilerkettensatz für Elemente nur schließen, daß jede Kette echt ineinander enthaltener Hauptideale abbricht.

In Hauptidealringen kennzeichnen also beide Formulierungen denselben Sachverhalt.

6. Es genügt zu zeigen, daß die Multiplikation mit einem beliebigen Ringelement $x + y\sqrt{k} \in \mathfrak{R}$ aus dem Modul $\Gamma(a_1 + b_1\sqrt{k}) + \Gamma a_2$ nicht herausführt, wobei wir uns offensichtlich wieder auf den Fall $b_1 = 1$ beschränken können:

$$(g(a_1 + \sqrt{k}) + ha_2)(x + y\sqrt{k}) = g a_1 x + h a_2 x + g y k + (g x + g a_1 y + h a_2 y)\sqrt{k}\,.$$

Setzen wir $k = a_1^2 + n a_2$ gemäß $k \equiv a_1^2 \bmod a_2$, so wird dieser Ausdruck in der Tat zu

$$g'(a_1 + \sqrt{k}) + h' a_2 \in \Gamma(a_1 + \sqrt{k}) + \Gamma a_2,$$

wobei sich die ganzen Zahlen g' und h' durch Koeffizientenvergleich wie folgt bestimmen:

$$g' = g x + g a_1 y + h a_2 y$$
$$h' = h x + g y n - h a_1 y.$$

7. Nach Aufg. 10 von § 40 kennen wir bereits folgende Zerlegungen des Ideals (21) in Produkte von Hauptidealen:

$$(21) = (3)\cdot(7) = (4 + \sqrt{-5})\cdot(4 - \sqrt{-5}) = (1 + 2\sqrt{-5})\cdot(1 - 2\sqrt{-5})\,.$$

Wir suchen die eindeutige Zerlegung in Primideale

$$(21) = \mathfrak{p}_1\mathfrak{p}_2 \ldots \mathfrak{p}_n,$$

aus der sich die obigen jeweils durch geeignete Zusammenfassung der Primfaktoren ergeben. Jedes $\mathfrak{p}_i$ muß also Oberideal (= Teiler = Faktor) wenigstens je eines Ideals der drei obigen Zerlegungen sein. Um sie zu finden, bilden wir zunächst die Ideale $(3, 4 + \sqrt{-5})$ und $(3, 4 - \sqrt{-5})$. Sie sind beide maximal (Restklassenring isomorph zu $\Gamma_{/}(3)$) und voneinander verschieden (aus $(3, 4 + \sqrt{-5}) \ni 4 - \sqrt{-5}$ folgte der Widerspruch $(3, 4 + \sqrt{-5}) \ni 1$), also bereits zwei der gesuchten Primideale.

Insbesondere gilt für ihr Produkt:

$$\mathfrak{p}_1\mathfrak{p}_2 = (3, 4 + \sqrt{-5})(3, 4 - \sqrt{-5}) = (9, 12 - 3\sqrt{-5}, 12 + 3\sqrt{-5}, 21) = (3)\,.$$

Entsprechende Überlegungen führen zu zwei weiteren Primfaktoren $(7, 4 + \sqrt{-5})$ und $(7, 4 - \sqrt{-5})$ mit der Eigenschaft:

$$\mathfrak{p}_3\mathfrak{p}_4 = (7, 4 + \sqrt{-5})(7, 4 - \sqrt{-5}) = (49, 28 - 7\sqrt{-5}, 28 + 7\sqrt{-5}, 21) = (7)\,.$$

Wegen

$$(21) = (3)\cdot(7) = \mathfrak{p}_1\mathfrak{p}_2\cdot\mathfrak{p}_3\mathfrak{p}_4$$

haben wir damit bereits die gesuchte Zerlegung gefunden.

Die anderen möglichen Zusammenfassungen zu je zwei Faktoren (man beachte den Unterschied zu dem im Text durchgeführten Beispiel, in dem zwei der vier Primideale übereinstimmten) ergeben:

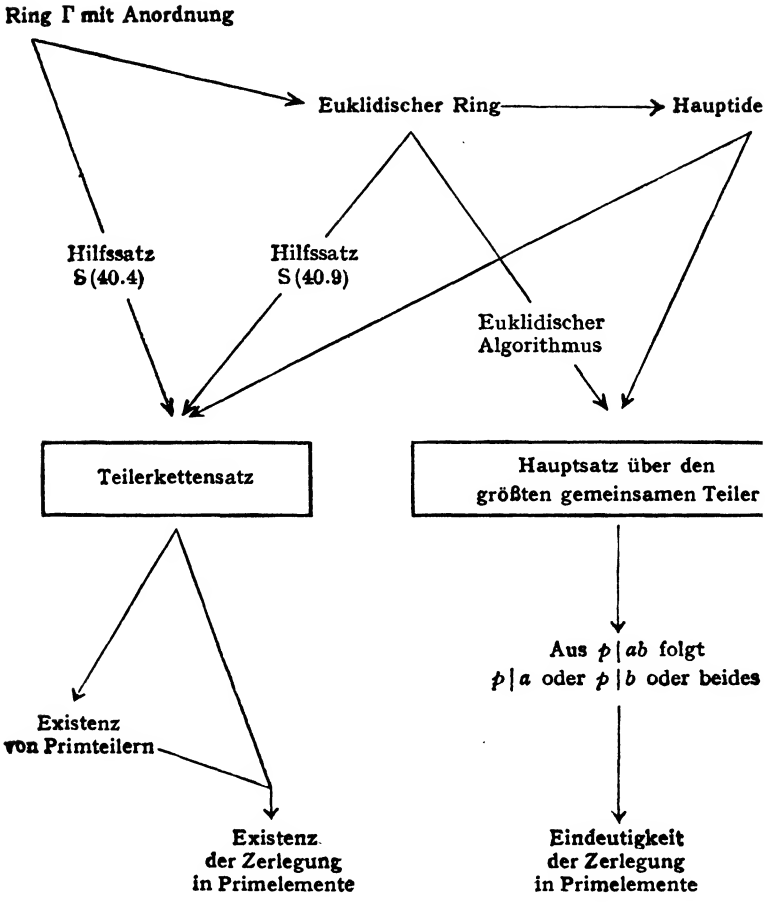
$$(21) = \mathfrak{p}_1\mathfrak{p}_3\cdot\mathfrak{p}_2\mathfrak{p}_4 = (4 + \sqrt{-5})(4 - \sqrt{-5})\,,$$
$$(21) = \mathfrak{p}_1\mathfrak{p}_4\cdot\mathfrak{p}_2\mathfrak{p}_3 = (1 - 2\sqrt{-5})(1 + 2\sqrt{-5})\,.$$

Weitere Zusammenfassungen, wie etwa $\mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3 \cdot \mathfrak{p}_4$ usw., liefern keine Elementzerlegung, da die gefundenen $\mathfrak{p}_i$ keine Hauptideale sind. Es ist übrigens interessant, daß in unserem Beispiel zur Bestimmung der $\mathfrak{p}_i$ bereits die Kenntnis von je zwei der drei Zerlegungen ausreicht. Die vier Primideale bestimmen sich dann jeweils in folgender Form:

$$\mathfrak{p}_1 = (3, 4+\sqrt{-5}) = (3, 1-2\sqrt{-5}) = (4+\sqrt{-5}, 1-2\sqrt{-5})$$
$$\mathfrak{p}_2 = (3, 4-\sqrt{-5}) = (3, 1+2\sqrt{-5}) = (4-\sqrt{-5}, 1+2\sqrt{-5})$$
$$\mathfrak{p}_3 = (7, 4+\sqrt{-5}) = (7, 1+2\sqrt{-5}) = (4+\sqrt{-5}, 1+2\sqrt{-5})$$
$$\mathfrak{p}_4 = (7, 4-\sqrt{-5}) = (7, 1-2\sqrt{-5}) = (4-\sqrt{-5}, 1-2\sqrt{-5}).$$

SACHVERZEICHNIS

Übersicht über die Beweisgänge in § 40



Übersicht über die Beweisgänge in § 43