3 Ringe

Wir wenden uns nun algebraischen Strukturen mit zwei Verknüpfungen zu. Als Modelle stehen uns dabei etwa die Strukturen $\mathfrak{Z}$ und $\mathfrak{Q}$ mit den Verknüpfungen Addition und Multiplikation vor Augen. Es handelt sich bei beiden um Ringe mit zusätzlichen speziellen Eigenschaften. Aus der umfangreichen Theorie der Ringe greifen wir nur einige Ergebnisse heraus, die ständig gebraucht werden. Wir beginnen mit einer allgemeinen Vorbetrachtung.

§ 19 Algebraische Strukturen

Bevor wir uns speziellen Strukturen mit zwei Verknüpfungen zuwenden, stellen wir einige allgemeine Definitionen und Sätze auf, die nach den entsprechenden Erörterungen in Kapitel 2 hinreichend plausibel geworden sind.

Definition: *Es seien S_1 und S_2 algebraische Strukturen mit jeweils n Verknüpfungen; wir bezeichnen mit*

$$\circ_1, \circ_2, \ldots, \circ_n \text{ die Verknüpfungssymbole von } S_1$$

und mit

$$\otimes_1, \otimes_2, \ldots, \otimes_n \text{ die Verknüpfungssymbole von } S_2.$$

Eine Abbildung $f\colon S_1 \to S_2$ heißt relationstreu oder Homomorphismus von S_1 in S_2, wenn (eventuell nach einer Umnumerierung) für jedes i, $1 \leqq i \leqq n$, und alle $x, y \in S_1$ gilt:

$$f(x \circ_i y) = f(x) \otimes_i f(y);$$

sie heißt Homomorphismus von S_1 auf S_2, wenn sie zusätzlich surjektiv ist, und in diesem Fall nennen wir S_2 ein homomorphes Bild von S_1 und schreiben $S_1 \curlyeqsucc S_2$.
Ein Isomorphismus von S_1 in S_2 ist eine injektive relationstreue Abbildung $f\colon S_1 \to S_2$; sie heißt Isomorphismus von S_1 auf S_2, wenn sie sogar bijektiv und relationstreu ist; in diesem Fall heißen S_1 und S_2 isomorph, und wir schreiben $S_1 \simeq S_2$.
Ein Automorphismus von S_1 ist ein Isomorphismus $f\colon S_1 \to S_1$ von S_1 auf sich. Unter einem Endomorphismus von S_1 schließlich versteht man einen Homomorphismus von S_1 in sich.

Isomorphe Strukturen definieren wieder eine Äquivalenzklasse und werden nicht als wesentlich voneinander verschieden angesehen. Aus $S_1 \curlyeqsucc S_2$ und $S_2 \curlyeqsucc S_3$ folgt $S_1 \curlyeqsucc S_3$.

Definition: *Es sei S eine algebraische Struktur mit den Verknüpfungen $\circ_1, \circ_2, \ldots, \circ_n$ und „$\equiv$" eine Äquivalenzrelation auf S. Diese Äquivalenzrelation heißt Kongruenzrelation, wenn für jedes i, $1 \leqq i \leqq n$, gilt:*

$$a \equiv a', b \equiv b' \Rightarrow a \circ_i b \equiv a' \circ_i b'.$$

Das kann man auch so interpretieren: In einer Kongruenzbeziehung aus S dürfen die in ihr auftretenden Elemente von S durch kongruente ersetzt werden (vgl. etwa die spätere Aufgabe 20.2).
Wie Satz 15.1 beweist man den

Satz 1: *Die Menge A aller Automorphismen einer algebraischen Struktur S mit n Verknüpfungen ist eine Gruppe, die sogenannte Automorphismengruppe von S.*

Es sei nun weiterhin S_1 eine algebraische Struktur mit den Elementen $a, a', b, b', s, \ldots$ und den n Verknüpfungen $\circ_1, \circ_2, \ldots, \circ_n$; gesucht seien alle homomorphen Bilder von S_1. Angenommen, auf S_1 ist eine Kongruenzrelation „$\equiv$" erklärt. Dann zerfällt S_1 in Kongruenzklassen. Die Menge dieser Klassen sei $S_2 = \{K(a), K(b), \ldots\}$. Wir erklären auf S_2 die Verknüpfungen $\otimes_1, \otimes_2, \ldots, \otimes_n$ durch $K(a) \otimes_i K(b) = K(a \circ_i b)$; das sind wirklich Verknüpfungen auf S_2, weil sich nach der Definition der Kongruenzrelation die rechten Seiten nicht ändern, wenn die Repräsentanten a, b von $K(a), K(b)$ durch andere Repräsentanten a', b' ersetzt werden. Für $s \in S_1$ setzen wir nun $f(s) = K(s) \in S_2$ und definieren dadurch eine surjektive Abbildung $f\colon S_1 \to S_2$. Diese Abbildung ist relationstreu:

$$f(a \circ_i b) = K(a \circ_i b) = K(a) \otimes_i K(b) = f(a) \otimes_i f(b).$$

Also gilt $S_1 \curlywedge S_2$.

Umgekehrt sei jetzt ein homomorphes Bild S_3 von S_1 vorgelegt, $S_1 \curlywedge S_3$; der vermittelnde Homomorphismus sei f. Dann ist durch $a \sim a' \Leftrightarrow f(a) = f(a')$ eine Äquivalenzrelation auf S_1 erklärt; S_1 zerfällt in Äquivalenzklassen derart, daß genau die Elemente einer Klasse dasselbe Bild besitzen. Diese Äquivalenzrelation ist sogar eine Kongruenzrelation: Aus $a \sim a'$ und $b \sim b'$ folgt

$$f(a \circ_i b) = f(a) \otimes_i f(b) = f(a') \otimes_i f(b') = f(a' \circ_i b'),$$

also $a \circ_i b \sim a' \circ_i b'$. Wir betrachten die Menge $S_2 = \{K(a), K(b), \ldots\}$ aller dieser Kongruenzklassen und behaupten $S_2 \simeq S_3$; dabei seien die Verknüpfungen auf S_2 wie oben eingeführt. Zunächst definiert $\varphi(K(a)) = f(a)$ eine Abbildung $\varphi\colon S_2 \to S_3$, weil $f(a)$ von der Wahl des Repräsentanten von $K(a)$ nicht abhängt, und diese Abbildung ist ersichtlich bijektiv. Sie ist auch relationstreu, und das bedeutet insgesamt $S_2 \simeq S_3$. Abgesehen von Isomorphien ist also das homomorphe Bild S_3 von S_1 eines der bereits oben gefundenen homomorphen Bilder S_2.
Wir fassen zusammen.

Satz 2: *Es sei S_1 eine algebraische Struktur mit Elementen $a, b, \ldots$ und den n Verknüpfungen $\circ_i$, $1 \leqq i \leqq n$. Ferner sei auf S_1 eine Kongruenzrelation*

erklärt. Dann werden auf der Menge $S_2 = \{K(a), K(b), \ldots\}$ *der Kongruenzklassen von* S_1 *durch* $K(a) \otimes_i K(b) = K(a \circ_i b)$ *ebenfalls* n *Verknüpfungen* $\otimes_i$, $1 \leqq i \leqq n$, *definiert, und es gilt* $S_1 \backsimeq S_2$. *Jedes homomorphe Bild von* S_1 *ist einer derart gewonnenen Struktur* S_2 *isomorph.*

Das Aufsuchen aller homomorphen Bilder einer algebraischen Struktur S mit n Verknüpfungen ist also gleichbedeutend mit der Aufgabe, alle Kongruenzrelationen von S ausfindig zu machen.
Wie Satz 12.3 ergibt sich schließlich noch der

Satz 3: *Es sei* S *eine algebraische Struktur mit Elementen* $a, b, \ldots$ *und den* n *Verknüpfungen* $\circ_i$, $1 \leqq i \leqq n$. *Ferner sei* $S = K(a) \cup K(b) \cup \ldots$ *eine Zerlegung von* S *in paarweise verschiedene Äquivalenzklassen. Genau dann definiert* $K(a) \otimes_i K(b) = K(a \circ_i b)$ *für jedes* i, $1 \leqq i \leqq n$, *eine Verknüpfung auf der Menge* $\{K(a), K(b), \ldots\}$ *der Äquivalenzklassen, wenn die durch die Partition von* S *erklärte Äquivalenzrelation eine Kongruenzrelation ist.*

§ 20 Das Rechnen in Ringen

20.1 Wir beginnen mit der folgenden

Definition: *Eine algebraische Struktur* R *mit einer additiv und einer multiplikativ geschriebenen Verknüpfung heißt ein Ring, wenn folgendes gilt:*
(1) R *ist bezüglich der Addition eine abelsche Gruppe.*
(2) R *ist bezüglich der Multiplikation eine Halbgruppe.*
(3) Für alle Elemente $a, b, c \in R$ *gelten die Distributivgesetze*

$$a(b + c) = (ab) + (ac) =_{Df} ab + ac,$$
$$(b + c)a = (ba) + (ca) =_{Df} ba + ca.$$

(Das Zeichen für die Multiplikation soll also wie üblich stärker binden als das für die Addition.)
Ein Ring R *heißt kommutativ, wenn für alle* $a, b \in R$ *gilt:* $ab = ba$.

Die Forderung (1) bestimmt die Eigenschaften der Addition, die Forderung (2) beschreibt die Multiplikation; in (3) schließlich wird ein Zusammenhang zwischen den Verknüpfungen hergestellt.
Jeder Ring R besitzt als additiv geschriebene abelsche Gruppe genau ein Nullelement 0, das für jedes $a \in R$ die Beziehung $a + 0 = 0 + a = a$ erfüllt. Enthält ein Ring $R \neq \{0\}$ ein Element $1 \in R$ mit $1a = a1 = a$ für jedes $a \in R$, so nennen wir dieses Element *Einselement* von R. Es gibt Ringe ohne Einselement (vgl. Beispiel 2). Zwei Einselemente $1, 1'$ kann ein Ring R wegen $1 = 1 \cdot 1' = 1'$ nicht besitzen.
Wie bei Gruppen erklärt man die Begriffe Unterring und echter Unterring.

Beispiel 1. Die Strukturen $\mathfrak{Z}, \mathfrak{Q}, \mathfrak{R}, \mathfrak{C}$ sind kommutative Ringe mit Einselement.

Beispiel 2. Die Menge $n\mathfrak{Z} = \{\ldots, -2n, -n, 0, n, 2n, \ldots\}$ aller durch ein festes $n \in \mathfrak{N}$, $n \neq 1$, teilbaren ganzen Zahlen ist ein kommutativer echter Unterring von $\mathfrak{Z}$ ohne Einselement.

Beispiel 3. Die Menge aller reellen zweireihigen quadratischen Matrizen ist ein nichtkommutativer Ring mit Einselement bezüglich der Matrizenaddition und -multiplikation.

Beispiel 4. Die Menge $R = \{x: x = a + b\sqrt{2}, a, b \in \mathfrak{Z}\} \subset \mathfrak{R}$ ist ein kommutativer Unterring von $\mathfrak{R}$ mit Einselement. Aus $x, y \in R$, etwa $x = a + b\sqrt{2}$ und $y = c + d\sqrt{2}$, folgt ja sowohl $x + y = (a + c) + (b + d)\sqrt{2} \in R$ als auch $xy = (ac + 2bd) + (ad + bc)\sqrt{2} \in R$; außerdem gilt $0 \in R$ und $-x \in R$. Alle weiteren Forderungen sind schon in $\mathfrak{R}$ und damit erst recht in $R \subset \mathfrak{R}$ erfüllt.

Sind a, b Elemente eines Ringes R, so schreiben wir statt $-(ab)$ wieder nur $-ab$. Wir beweisen nun die bekannten Vorzeichenregeln.

Satz 1: *In Ringen gelten die Rechenregeln* $a \cdot 0 = 0 \cdot a = 0$, $a(-b) = (-a)b = -ab$, $(-a)(-b) = ab$, $a(b - c) = ab - ac$ *und* $(b - c)a = ba - ca$.

Beweis: Nach (3) ist $a^2 = a(a + 0) = a^2 + a \cdot 0$, also $a \cdot 0 = 0$, weil die Gleichung $a^2 + x = a^2$ nach Aussage c) von Satz 6.1 genau eine Lösung x hat; aus $a^2 = (a + 0)a$ folgt entsprechend $0 \cdot a = 0$. Ferner gilt sowohl $ab + (-ab) = 0$, als auch $ab + a(-b) = a(b + (-b)) = a \cdot 0 = 0$, und wie eben folgt $a(-b) = -ab$; aus $ab + (-a)b = 0$ bekommt man nach demselben Muster $(-a)b = -ab$. Damit wird $(-a)(-b) = a(-(-b)) = ab$. Schließlich ist $a(b - c) = a(b + (-c)) = ab + a(-c) = ab - ac$, und analog ergibt sich die letzte Behauptung.

Folgerung: Besitzt ein Ring R ein Einselement 1, so ist $1 \neq 0$.

Man kann leicht endliche Ringe konstruieren. Die wichtigsten sind die im folgenden betrachteten Restklassenringe modulo n.

Beispiel 5. Es sei n eine feste natürliche Zahl, $\mathfrak{Z}$ der *Ring* der ganzen Zahlen und

$$\mathfrak{Z}_n = \{K(0), K(1), \ldots, K(n - 1)\}$$

die Menge der Restklassen modulo n. Wir zeigen, daß die zugrundeliegende Äquivalenzrelation

$$a \equiv a' \Leftrightarrow n \mid (a - a')$$

eine Kongruenzrelation auf dem *Ring* $\mathfrak{Z}$ ist: Es gelte $a \equiv a'$, $b \equiv b'$. Diese Äquivalenzrelationen bedeuten die Existenz ganzer Zahlen λ, μ mit $a' = a + \lambda n$, $b' = b + \mu n$; für gewisse ganze Zahlen $\varrho = \lambda + \mu$, $\sigma = \mu a + \lambda b + \lambda\mu n$ wird also $a' + b' = a + b + \varrho n$ sowie $a'b' = ab + \sigma n$, und das heißt $a + b \equiv a' + b'$ sowie $ab \equiv a'b'$. Nach Satz 19.3 werden also durch

$$K(a) + K(b) = K(a + b), \quad K(a)K(b) = K(ab)$$

eine Addition und eine Multiplikation auf der Menge $\mathfrak{Z}_n$ der Kongruenzklassen erklärt. In Erinnerung an § 9.1 können wir sagen, daß der additiven Restklassengruppe modulo n in natürlicher Weise noch eine Multiplikation auf-

geprägt wurde. Wir zeigen jetzt, daß damit $\mathfrak{Z}_n = \{K(0), K(1), \ldots, K(n-1)\}$ ein kommutativer Ring wird. Die Forderung (1) ist nach § 9.1 erfüllt. Das Assoziativgesetz der Multiplikation

$$\begin{aligned}(K(a)K(b))K(c) &= K(ab)K(c) = K((ab)c)\\ &= K(a(bc)) = K(a)K(bc) = K(a)(K(b)K(c))\end{aligned}$$

folgt aus dem entsprechenden Assoziativgesetz von $\mathfrak{Z}$; also gilt (2). Eine analoge Rechnung liefert die Kommutativität der Multiplikation von $\mathfrak{Z}_n$, so daß wir für (3) nur noch eines der beiden Distributivgesetze nachzuprüfen brauchen:

$$\begin{aligned}K(a)(K(b)+K(c)) &= K(a)K(b+c) = K(a(b+c)) = K(ab+ac)\\ &= K(ab)+K(ac) = K(a)K(b)+K(a)K(c).\end{aligned}$$

Damit wissen wir: $\mathfrak{Z}_n$ ist für $n>1$ ein kommutativer Ring mit dem Einselement $K(1)$. Er heißt der *Restklassenring modulo n*. Solange keine Verwechslungen mit der zyklischen Gruppe der Ordnung n zu befürchten sind, behalten wir für ihn die Bezeichnung $\mathfrak{Z}_n$ bei. Man addiert und multipliziert in $\mathfrak{Z}_n$ wie in $\mathfrak{Z}$, setzt aber Vielfache von n gleich Null. Für $n = 1$ besteht $\mathfrak{Z}_n$ aus der Null $K(0)$ allein (*Nullring*).
Für die Kongruenzrelation $a \equiv a' \Leftrightarrow n \mid (a - a')$ pflegt man eine der beiden Schreibweisen

$$a \equiv a' \bmod n \quad \text{oder} \quad a \equiv a' \,(n)$$

zu wählen.

Anwendung: Wir zeigen auf zwei nur durch die Schreibweise unterschiedene Arten, daß $2^{32}+1$ durch 641 teilbar ist. Beide Male gehen wir von der Identität $2^4 + 5^4 = 5 \cdot 2^7 + 1 = 641$ aus.
a) Es ist $5 \cdot 2^7 \equiv -1$ (641). Denkt man sich diese Kongruenz viermal hingeschrieben und die linken und rechten Seiten multipliziert, so bekommt man $(5 \cdot 2^7)^4 \equiv (-1)^4 \bmod 641$ oder $5^4 \cdot 2^{28} \equiv 1$ (641). Hierin darf man wegen $5^4 \equiv -2^4$ (641) den Faktor 5^4 durch -2^4 ersetzen. Das liefert $-2^{32} \equiv 1$ (641) oder $641 \mid (2^{32}+1)$.
b) Im Restklassenring $\mathfrak{Z}_{641}$ gilt $K(5 \cdot 2^7) = K(-1)$. Potenziert man beide Seiten mit 4, so bekommt man $K(5^4 \cdot 2^{28}) = K(1)$. Für die linke Seite kann man auch $K(5^4) \cdot K(2^{28})$ oder $K(-2^4) \cdot K(2^{28}) = K(-2^{32})$ schreiben. Das ergibt $K(-2^{32}) = K(1)$ oder $641 \mid (2^{32}+1)$.

Oft wird man den Restklassenring $\mathfrak{Z}_n$ einfach in der Gestalt $\{0, 1, \ldots, n-1\}$ schreiben und dabei beachten, daß die hingeschriebenen Elemente keine ganzen Zahlen sind.

Aufgabe 1: Man gebe die Verknüpfungstafeln des Restklassenringes $\mathfrak{Z}_6$ an.

Aufgabe 2: Man löse die Kongruenz $5x \equiv 7$ (13).

Aufgabe 3. Durch Rechnen im Restklassenring $\mathfrak{Z}_8$ zeige man: Keine natürliche Zahl n der Form $8k+7$ ist Summe von drei Quadratzahlen.

20.2 Im Restklassenring $\mathfrak{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ gilt $2 \cdot 3 = 0$, in $\mathfrak{Z}_{16}$ etwa $2 \cdot 8 = 0$; ist n keine Primzahl, so gibt es in $\mathfrak{Z}_n$ Elemente $a \neq 0$, $b \neq 0$, deren Produkt ab Null ist.

Definition: *Ein Element $a \neq 0$ eines Ringes R heißt linker Nullteiler, wenn ein $b \neq 0$ in R existiert, so daß $ab = 0$ ist. Ein Element $b \neq 0$, $b \in R$, heißt rechter Nullteiler, wenn ein $a \neq 0$, $a \in R$, existiert, so daß $ab = 0$ ist. Ein Ring R heißt nullteilerfrei, wenn er keine Nullteiler enthält.*

Ein Ring R ist also genau dann nullteilerfrei, wenn für alle $a, b \in R$ aus $ab = 0$ folgt: $a = 0$ oder $b = 0$. Nullteilerfreie Ringe sind zum Beispiel $\mathfrak{Z}, \mathfrak{Q}, \mathfrak{R}, \mathfrak{C}$. Dasselbe gilt für die Restklassenringe $\mathfrak{Z}_p = \{K(0), K(1), \ldots, K(p-1)\}$ mit Primzahlindex p. Aus $K(a)K(b) = K(ab) = K(0)$ folgt ja $p|ab$ in $\mathfrak{Z}$, also etwa $p|a$ oder $K(a) = K(0)$.

Gilt in einem Ring $ab = ac$, so folgt auch für $a \neq 0$ nicht notwendig $b = c$; in $\mathfrak{Z}_{12}$ gilt etwa $2 \cdot 3 = 2 \cdot 9$, aber es ist $3 \neq 9$. Ist aber R nullteilerfrei, $a \in R$ und $a \neq 0$, so folgt aus $ab = ac$ zunächst $a(b - c) = 0$, also tatsächlich $b - c = 0$ oder $b = c$; entsprechend wird $ba = ca \Rightarrow b = c$. Wir formulieren dieses Ergebnis.

Satz 2: *Ist R ein nullteilerfreier Ring mit Elementen $a, b, c, \ldots$, so gelten für $a \neq 0$ die Kürzungsregeln*

$$ab = ac \Rightarrow b = c, \quad ba = ca \Rightarrow b = c.$$

Wir betrachten nun einen *nullteilerfreien Ring $R \neq \{0\}$ mit Einselement* und sehen uns die Elemente $1, 1 + 1, 1 + 1 + 1, \ldots$ an. Es können zwei Fälle eintreten. Entweder keines von ihnen ist Null, und das ist gleichbedeutend damit, daß sie paarweise voneinander verschieden ausfallen; wir sagen dann, R habe die *Charakteristik* Null und schreiben $\chi(R) = 0$. Oder es gibt ein $n \in \mathfrak{N}$ mit $1 + 1 + \ldots + 1 = 0$ (n Summanden 1); dann gibt es auch ein kleinstes n dieser Art. Dieses minimale n ist zunächst ungleich Eins und muß außerdem eine Primzahl p sein, weil aus $n = kl$ mit natürlichen Zahlen $k < n$, $l < n$ und $\sum_1^n 1 = \sum_1^k 1 \cdot \sum_1^l 1 = 0$ wegen der Nullteilerfreiheit von R folgt: $\sum_1^k 1 = 0$ oder $\sum_1^l 1 = 0$. Wir sagen in diesem Fall, R habe die *Charakteristik p* und schreiben $\chi(R) = p$.

Ist R ein Ring mit $\chi(R) = p$, ist also $1 \in R$ und R nullteilerfrei, so verschwindet eine Summe $r + r + \ldots + r$ von m Summanden $r \in R$, falls p in m aufgeht. Um das einzusehen, schreibe man

$$r + r + \ldots + r = 1 \cdot r + 1 \cdot r + \ldots + 1 \cdot r = (1 + 1 + \ldots + 1) \cdot r.$$

Es ist $\chi(\mathfrak{Z}) = \chi(\mathfrak{Q}) = \chi(\mathfrak{R}) = \chi(\mathfrak{C}) = 0$; für Primzahlen p gilt $\chi(\mathfrak{Z}_p) = p$.

Definition: *Ein vom Nullring verschiedener kommutativer nullteilerfreier Ring heißt Integritätsbereich.*

Beispiele für Integritätsbereiche waren etwa $\mathfrak{Z}, \mathfrak{Q}, \mathfrak{R}, \mathfrak{C}, \mathfrak{Z}_p$ (p Primzahl). Auch

die Ringe in den obigen Beispielen 2 und 4 sind als Unterringe von $\mathfrak{Z}$ und $\mathfrak{R}$ Integritätsbereiche.

Wir betrachten nun einen beliebigen Ring R mit Einselement. In ihm wird die Frage nach multiplikativen Inversen von Ringelementen sinnvoll. Wir treffen die folgenden Verabredungen.

Definition: *Es sei R ein Ring mit Einselement. Dann heißt $b \in R$ Rechtsinverses von $a \in R$, wenn $ab = 1$ gilt. Das Element $b \in R$ heißt Linksinverses von $a \in R$, wenn $ba = 1$ ist. Das Element $b \in R$ heißt Inverses von $a \in R$, wenn $ab = ba = 1$ ist. Ein $a \in R$ heißt Einheit, wenn a in R ein Inverses besitzt.*

Ist schließlich R ein beliebiger Ring und $m \in \mathfrak{Z}$, so sind noch die nachstehenden Vereinbarungen praktisch: Es sei für $a \in R$

$$ma = \begin{cases} a + a + \ldots + a \ (m \text{ Summanden}) & \text{für } m > 0 \\ 0 & \text{für } m = 0 \\ -a - a - \ldots - a \ ((-m) \text{ Summanden}) & \text{für } m < 0. \end{cases}$$

Das ist eine äußere Komposition von R mit $\mathfrak{Z}$; Verwechslungen mit der Ringmultiplikation sind nicht zu befürchten. Es gelten Rechenregeln wie $(m_1 + m_2)a = m_1a + m_2a$, $m_1(m_2a) = (m_1m_2)a$ und $m(ab) = (ma)b = a(mb)$ ($m_i, m \in \mathfrak{Z}$, $a, b \in R$). Besitzt R ein Einselement, so kann man ma auch als ein Produkt des Ringelementes

$$m = \begin{cases} 1 + 1 + \ldots + 1 \ (m \text{ Summanden}) & \text{für } m > 0 \\ 0 & \text{für } m = 0 \\ -1 - 1 - \ldots - 1 \ ((-m) \text{ Summanden}) & \text{für } m < 0 \end{cases}$$

mit $a \in R$ ansehen; m kann dann auch Nullteiler sein, wie etwa die Gleichung $3 + 3 = (1 + 1)3 = 2 \cdot 3 = 0$ in $\mathfrak{Z}_6$ zeigt.

Aufgabe 4: Der Ring R enthalte wenigstens einen von Null verschiedenen Nichtnullteiler. Dann ist das Ringaxiom $a + b = b + a$ eine Folge der übrigen. Beweis?

Aufgabe 5: Man beweise die folgenden Aussagen.

a) In Ringen gilt $a(b_1 + b_2 + \ldots + b_n) = ab_1 + ab_2 + \ldots + ab_n$ und $(b_1 + b_2 + \ldots + b_n)a = b_1a + b_2a + \ldots + b_na$.

b) In einem nullteilerfreien Ring ist ein Produkt $a_1a_2 \ldots a_n$ nur Null, wenn einer der Faktoren Null ist.

c) In einem Ring R mit Einselement besitzt ein linker (rechter) Nullteiler kein Links-(Rechts-)Inverses.

d) Ist $1 \in R$ und besitzt $a \in R$ ein Linksinverses b und ein Rechtsinverses c, so ist $b = c$, und a besitzt kein von b verschiedenes Rechts- oder Linksinverses.

e) Ist $1 \in R$ und besitzt $a \in R$ ein Inverses, so ist es eindeutig bestimmt (Bezeichnung: a^{-1}).

f) Ist $1 \in R$ und besitzt jedes $a \in R$, $a \neq 0$, ein Inverses $a^{-1} \in R$, so ist R nullteilerfrei.

g) Es sei R ein Ring mit Einselement und $E \subset R$ die Menge aller Einheiten von R. Dann ist E eine Gruppe bezüglich der Multiplikation.

Aufgabe 6: Es sei R ein Ring mit Einselement und $a \in R$. Zeige:
a) Ist b ein Rechtsinverses von a, so ist es auch jedes der Elemente $b + (ba - 1)a^k$ $(k = 0, 1, 2, \ldots)$.
b) Besitzt a genau ein Rechtsinverses b, so ist b das Inverse von a.
c) Das Element a besitzt entweder kein Rechtsinverses, genau ein Rechtsinverses oder unendlich viele Rechtsinverse (vgl. auch Aufgabe 25.1).

Aufgabe 7: Es sei R ein kommutativer Ring. Man beweise den *binomischen Lehrsatz*

$$(a + b)^n = \sum_{\nu=0}^{n} \binom{n}{\nu} a^{n-\nu} b^{\nu} \quad (a, b, \in R, n \in \mathfrak{N}).$$

Aufgabe 8: Es sei I ein Integritätsbereich mit Einselement und Primzahlcharakteristik p. Dann gelten die folgenden Rechenregeln:
a) $(a + b)^p = a^p + b^p, (a - b)^p = a^p - b^p \quad (a, b \in I)$.
b) $(a + b)^{p^k} = a^{p^k} + b^{p^k}, (a - b)^{p^k} = a^{p^k} - b^{p^k}$ $(a, b \in I; k = 0, 1, 2, \ldots)$.
c) $(a_1 + a_2 + \ldots + a_n)^p = a_1^p + a_2^p + \ldots + a_n^p$ $(a_\nu \in I)$.
Beweis?

20.3 Wir treffen nun eine vielfach nützliche

Verabredung: Ist R ein Ring, so bezeichne R_0 die Menge der von Null verschiedenen Ringelemente.
Im folgenden beschäftigen wir uns mit gewissen Ringen, die besonders oft auftreten.

Definition: *Ein Ring R heißt Schiefkörper, wenn R_0 eine Gruppe bezüglich der Multiplikation ist. Ein kommutativer Schiefkörper heißt Körper. R_0 heißt dann die multiplikative Gruppe des Schiefkörpers (Körpers).*

Vielfach werden Schiefkörper auch einfach Körper genannt; ist die Multiplikation kommutativ, spricht man dann von einem kommutativen Körper.
In den uns bekannten Beispielen $\mathfrak{Q}, \mathfrak{R}, \mathfrak{C}$ liegen immer schon Körper vor. Es sind ja $\mathfrak{Q}, \mathfrak{R}, \mathfrak{C}$ kommutative Ringe, und nach § 6.2 sind $\mathfrak{Q}_0, \mathfrak{R}_0, \mathfrak{C}_0$ Gruppen bezüglich der Multiplikation.
Es sei S ein Schiefkörper. Dann enthält die multiplikative Gruppe S_0 ein Einselement $1 \neq 0$, und diese Eins ist Einselement von S. Außerdem besitzt jedes $a \in S$, $a \neq 0$, ein Inverses $a^{-1} \in S$. Deswegen sind Gleichungen der Art $ax = b$ oder $ya = b$ $(a, b \in S, a \neq 0)$ in S eindeutig lösbar. Ein Schiefkörper kann auch keine Nullteiler enthalten; denn aus $ab = 0$ und $a \neq 0$ folgt $a^{-1}(ab) = b = 0$.
Der Nachweis dafür, daß ein Ring schon ein Schiefkörper ist, wird in den meisten Fällen nicht über die obige Definition sondern mit Hilfe des folgenden Satzes geführt.

Satz 3: *Ein Ring $R \neq \{0\}$ ist genau dann ein Schiefkörper, wenn er ein Einselement und zu jedem $a \in R$, $a \neq 0$, ein Inverses a^{-1} enthält.*

Beweis: Nach dem bereits Erörterten bleibt zu zeigen, daß ein Ring $R \neq \{0\}$ ein Schiefkörper ist, wenn er ein Einselement und zu jedem $a \in R$,

$a \neq 0$, ein Inverses enthält. In diesem Fall gilt aber $1 \in R_0$; aus $a \in R_0$ folgt $a^{-1} \in R_0$; die Multiplikation in R_0 ist assoziativ; schließlich liegt auch das Produkt ab von Elementen $a, b \in R_0$ wieder in R_0, weil $ab = 0$ den Widerspruch $a^{-1}(ab) = b = 0$ zur Folge hätte. Es ist also R_0 eine Gruppe bezüglich der Multiplikation, was zu zeigen war.
Auch der folgende Satz ist sehr einfach.

Satz 4: *Jeder endliche nullteilerfreie Ring $R \neq \{0\}$ ist ein Schiefkörper. Speziell ist jeder endliche Integritätsbereich ein Körper.*

Beweis: Nach Satz 2 ist R_0 bezüglich der Ringmultiplikation eine reguläre Halbgruppe. Sie ist ferner endlich, nach Aufgabe 13.1 also eine Gruppe.

Die Restklassenringe $\mathfrak{Z}_p$ (p Primzahl) sind demnach endliche Körper. Die übrigen Restklassenringe $\mathfrak{Z}_n$ enthalten Nullteiler, sind also keine Körper. Später (§ 60) wird sich noch zeigen, daß jeder endliche Schiefkörper bereits ein Körper ist. Die endlichen Körper wiederum werden wir alle angeben können (§ 59).
Sind a und $b \neq 0$ Körperelemente, so gilt $ab^{-1} = b^{-1}a$. An Stelle von ab^{-1} schreibt man dann auch vielfach $\frac{a}{b}$ oder $a:b$. Wir zeigen nun, daß in Körpern die bekannten Bruchrechenregeln gelten.

Satz 5: *In Körpern gelten die Bruchrechenregeln* $\frac{a}{b} = \frac{ac}{bc}$ $(b \neq 0,\ c \neq 0)$, $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$ $(b \neq 0,\ d \neq 0)$, $\frac{a}{b} : \frac{c}{d} = \frac{ad}{bc}$ $(bcd \neq 0)$, $\frac{a}{b} \pm \frac{c}{d} = \frac{ad \pm bc}{bd}$ $(b \neq 0,\ d \neq 0)$.

Beweis: Die erste Regel besagt dasselbe wie $ab^{-1} = ac(bc)^{-1}$; für $a = 0$ ist das sicher richtig; für $a \neq 0$ ist es eine richtige Beziehung in der multiplikativen Gruppe des Körpers. Die zweite Regel besagt $ab^{-1}cd^{-1} = ac(bd)^{-1}$; wegen der Kommutativität der Multiplikation ist das ebenfalls richtig. Ebenso gilt richtig $ab^{-1}(cd^{-1})^{-1} = ad(bc)^{-1}$. Die letzte Regel $ab^{-1} \pm cd^{-1} = (ad \pm bc)(bd)^{-1}$ schließlich bestätigt man, indem man rechter Hand nach dem Distributivgesetz ausmultipliziert.
In einem Körper addiert, subtrahiert, multipliziert und dividiert man also wie gewohnt. Diese vier Rechenoperationen bezeichnet man auch als *die rationalen Operationen.*
Sind K und L Körper mit $K \subset L$ und sind die Verknüpfungen von K und L in K dieselben, so heißt K ein Unterkörper von L und L ein Oberkörper von K.
Viele mathematische Theorien lassen sich in Körpern entwickeln. Dies gilt beispielsweise für die Auflösung linearer Gleichungssysteme. Ebenso sind die Determinantensätze in Körpern gültig; als Beispiel sei die CRAMERsche Regel erwähnt. Da Körper nullteilerfreie Ringe mit Einselement sind, besitzen sie eine Charakteristik. Speziell gelten für Körper auch die Rechenregeln der Aufgaben 7 und 8.

Wir sehen uns noch einen Körper an, der an das obige Beispiel 4 erinnert.
Beispiel 6. Wie in Beispiel 4 sieht man, daß

$$K = \{x: x = a + b\sqrt{2},\ a, b \in \mathfrak{Q}\} \subset \mathfrak{R}$$

ein kommutativer Unterring von $\mathfrak{R}$ ist. Wir zeigen nach Satz 3, daß K ein Körper ist. Zunächst gilt $1 \in K$. Ein Element $a + b\sqrt{2}$ aus K schließlich, für das a und b nicht beide Null sind, besitzt das Inverse

$$(a + b\sqrt{2})^{-1} = \frac{a - b\sqrt{2}}{(a + b\sqrt{2})(a - b\sqrt{2})} = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2} \in K;$$

es ist ja der Nenner $a^2 - 2b^2 \neq 0$. Analog kann man weitere Zwischenkörper K mit $\mathfrak{Q} \subset K \subset \mathfrak{R}$ angeben.

20.4 Für das Rechnen in Körpern geben wir noch eine einfache zahlentheoretische Anwendung.

Satz 6: *Die natürliche Zahl $p \neq 1$ ist dann und nur dann Primzahl, wenn*

$$(p - 1)! \equiv -1 \bmod p$$

ist (sogenannte Wilsonsche *Kongruenz).*

Beweis: Ist p nicht Primzahl, also $p = kl$ mit natürlichen Zahlen $k < p$ und $l < p$, so teilt $k \neq 1$ den Ausdruck $(p - 1)!$, also nicht $(p - 1)! + 1$; erst recht kann p dann kein Teiler von $(p - 1)! + 1$ sein. Es bleibt also das Bestehen der Kongruenz für Primzahlen p zu zeigen. Für $p = 2$ ist sie erfüllt; es sei also $p \geqq 3$.
Es sei zunächst L ein beliebiger Körper. Wir bestimmen alle $\xi \in L$ mit $\xi^2 = 1$. Wir haben nach allen ξ mit $\xi^2 - 1 = (\xi - 1)(\xi + 1) = 0$ zu suchen. Da L nullteilerfrei ist, folgt $\xi = 1$ oder $\xi = -1$. Für den Fall $L = \mathfrak{Z}_p$, $p \geqq 3$, bedeutet das: Genau die beiden voneinander verschiedenen Elemente $K(1)$ und $K(p - 1)$ aus $\mathfrak{Z}_p = \{K(0), K(1), K(2), \ldots, K(p - 1)\}$ sind ihre eigenen Inversen; jedes andere von $K(0)$ verschiedene Element aus $\mathfrak{Z}_p$ fällt nicht mit seinem Inversen zusammen.
Nun bilden wir in $\mathfrak{Z}_p$ das Produkt

$$s = K(1)\,K(2)\,K(3) \ldots K(p - 1)$$

und fassen rechter Hand jeden Faktor mit seinem Inversen zusammen; das Ergebnis ist $s = K(1)\,K(p - 1)$. Das heißt aber $K((p - 1)!) = K(p - 1) = K(-1)$ oder $(p - 1)! \equiv -1 \bmod p$.

Aufgabe 9: Man zeige das Folgende.
a) $K_1 = \{x: x = a + b\sqrt{3},\ a, b \in \mathfrak{Q}\}$ und $K_2 = \{x: x = a + b\sqrt{5},\ a, b \in \mathfrak{Q}\}$ sind nichtisomorphe Unterkörper von $\mathfrak{R}$.
b) $M = \{x: x = a + b\sqrt[3]{2},\ a, b \in \mathfrak{Q}\} \subset \mathfrak{R}$ ist kein Unterkörper von $\mathfrak{R}$.

Aufgabe 10: Man beweise die folgenden Aussagen.
a) Jeder Schiefkörper der Charakteristik Null enthält einen Unterkörper iso-

morph $\mathfrak{Q}$, und $\mathfrak{Q}$ enthält keinen echten Unterkörper. (Deshalb heißt $\mathfrak{Q}$ auch der kleinste oder der *Primkörper der Charakteristik Null.*)
b) Jeder Schiefkörper der Primzahlcharakteristik p enthält einen Unterkörper isomorph $\mathfrak{Z}_p$, und $\mathfrak{Z}_p$ enthält keinen echten Unterkörper. (Deshalb heißt $\mathfrak{Z}_p$ auch der kleinste oder der *Primkörper der Charakteristik p.*)

Aufgabe 11: Es gibt genau einen Körper K mit $|K| = 4$. In ihm sind die Gleichungen $x^2 = x \pm 1$ lösbar. Beweis?

Aufgabe 12: Der Unterkörper $K = \{x: x = a + b\sqrt{2},\ a, b \in \mathfrak{Q}\}$ von $\mathfrak{R}$ besitzt seinerseits nur die Unterkörper $\mathfrak{Q}$ und K. Beweis?

Aufgabe 13: Man löse das Kongruenzsystem

$$\begin{aligned} x + y + z &\equiv 2 \ (7) \\ 2x - 3y + z &\equiv -1 \ (7) \\ -x + 2y + 3z &\equiv 2 \ (7). \end{aligned}$$

Man löse dasselbe System modulo 8. Ist es auch modulo 17 lösbar?

Aufgabe 14: Es sei S ein Schiefkörper und $Z \subset S$ die Menge aller derjenigen Elemente $z \in S$, die mit jedem $s \in S$ vertauschbar sind: $sz = zs$ für jedes $s \in S$. Dieses sogenannte *Zentrum* Z des Schiefkörpers S ist ein Körper. Beweis?

§ 21 Homomorphe Bilder von Ringen

21.1 Es sei R_1 ein Ring mit Elementen $a, b, c, \ldots$ und R_2 eine algebraische Struktur mit zwei Verknüpfungen, die ebenfalls additiv bzw. multiplikativ geschrieben seien. In § 19 ist nun definiert, wann R_2 ein homomorphes Bild von R_1 genannt wird. Wir formulieren es noch einmal: Die algebraische Struktur R_2 heißt homomorphes Bild des Ringes R_1, wenn eine surjektive relationstreue Abbildung $f: R_1 \to R_2$ existiert. Die Relationstreue von f besteht dabei aus den beiden Forderungen

$$\begin{aligned} f(a + b) &= f(a) + f(b), \\ f(ab) &= f(a)f(b). \end{aligned}$$

Wir schreiben in diesem Fall $R_1 \simeq R_2$ und nennen f einen Ringhomomorphismus von R_1 auf R_2.
In Analogie zu Satz 12.1 bekommen wir zunächst den

Satz 1: *Das homomorphe Bild $R_2 = f(R_1)$ eines Ringes R_1 ist ein Ring. Dabei geht das Nullelement von R_1 in das Nullelement von R_2 über. Besitzt R_1 ein Einselement 1 und ist $f(R_1)$ nicht der Nullring, so ist $f(1)$ Einselement von R_2. Ist R_1 kommutativ, so ist es auch R_2.*

Beweis: Bezüglich der Addition ist R_2 nach Satz 12.1 eine abelsche Gruppe, und $f(0)$ ist das Nullelement von R_2. Für die ersten beiden Behaup-

tungen bleibt also zu zeigen, daß sich das Assoziativgesetz der Multiplikation und die Distributivgesetze von R_1 auf R_2 übertragen. Das sieht man, da sich jedes Element von R_2 in der Gestalt $f(r)$ mit einem $r \in R_1$ schreiben läßt, wie im Beispiel 5 von § 20; hier schreibt man nur f statt K. Aus $1 \in R_1$ folgt $f(1)f(r) = f(1r) = f(r)$ und $f(r)f(1) = f(r1) = f(r)$, und das ist die dritte Behauptung. Aus der Kommutativität von R_1 folgt schließlich noch $f(a)f(b) = f(ab) = f(ba) = f(b)f(a)$, also die Kommutativität von R_2.
Als Beispiel betrachte man die Ringe $\mathfrak{Z}$ und $\mathfrak{Z}_n$ (§ 20, Beispiel 5). Die durch $f(m) = K(m)$ erklärte Abbildung $f: \mathfrak{Z} \to \mathfrak{Z}_n$ definiert einen Ringhomomorphismus. Dieses Beispiel zeigt auch, daß das homomorphe Bild eines nullteilerfreien Ringes Nullteiler besitzen kann; man wähle etwa $n = 6$.

21.2 Nützlich ist für das Folgende die

Definition: *Ist R ein Ring, $r \in R$ und $T \subset R$, so sei*

$$r + T = \{x: x = r + t, t \in T\},$$
$$rT = \{x: x = rt, t \in T\};$$

entsprechend seien $T + r$ und Tr erklärt.

Der nun eingeführte Begriff des Ideals ist in der Algebra von außerordentlicher Bedeutung.

Definition: *Eine Teilmenge $\mathfrak{a}$ des Ringes R heißt ein Ideal, wenn gilt:*
(1) Es ist $\mathfrak{a}$ eine Gruppe bezüglich der Addition.
(2) Für jedes $r \in R$ ist $r\mathfrak{a} \subset \mathfrak{a}$ und $\mathfrak{a}r \subset \mathfrak{a}$.

Da in der Forderung (2) speziell $r \in \mathfrak{a}$ gewählt werden kann, ist ein Ideal $\mathfrak{a}$ gewiß ein Unterring von R; darüber hinaus liegen die Produkte ar und ra sogar schon dann immer in $\mathfrak{a}$, wenn nur einer der Faktoren a aus $\mathfrak{a}$ stammt. Wir bezeichnen Ideale meist mit kleinen deutschen Buchstaben.

Beispiel 1. Jeder Ring R besitzt die Ideale $\{0\}$ und R.

Beispiel 2. Die sämtlichen Ideale des Ringes $\mathfrak{Z}$ sind unter den sämtlichen additiven Untergruppen $\{0\}$ und $n\mathfrak{Z}$ $(n = 1, 2, 3, \ldots)$ von $\mathfrak{Z}$ zu finden (vgl. § 12.2). Alle diese Untergruppen sind aber, wie unmittelbar zu sehen ist, bereits Ideale von $\mathfrak{Z}$. Alle Ideale von $\mathfrak{Z}$ sind also $\{0\}$ und $n\mathfrak{Z}$ $(n = 1, 2, 3, \ldots)$.

Beispiel 3. Ein Schiefkörper S besitzt nur die Ideale $\{0\}$ und S. Ist nämlich $\mathfrak{a} \subset S$ ein von $\{0\}$ verschiedenes Ideal, so gibt es ein $a \in \mathfrak{a}$, $a \neq 0$, und in S existiert das Inverse a^{-1} von a. Nach (2) wird also $a^{-1}a = 1 \in \mathfrak{a}$ und nun auch $s = s1 \in \mathfrak{a}$ für jedes $s \in S$.

Unser Ziel ist die Bestimmung aller homomorphen Bilder eines vorgelegten Ringes R. Der folgende Satz schafft die Möglichkeit einer Anwendung von Satz 19.2 (vgl. auch Satz 12.4).

Satz 2: *Es sei R ein Ring und „$\equiv$" eine Äquivalenzrelation auf R. Diese Äquivalenzrelation ist genau dann eine Kongruenzrelation, wenn die Äquivalenzklassen die Nebenklassen $r + \mathfrak{a}$ eines Ideals $\mathfrak{a} \subset R$ sind. Dabei ist $\mathfrak{a}$ die Menge aller $a \in R$ mit $a \equiv 0$.*

Beweis:
a) Ist „$\equiv$“ eine Kongruenzrelation auf R, so wird durch sie nach Satz 12.4 eine Partition auf R definiert, die aus den Nebenklassen $r + \mathfrak{a}$ eines Normalteilers, also einer Untergruppe $\mathfrak{a}$ der additiven Gruppe von R besteht. Dabei besteht $\mathfrak{a}$ aus allen $a \in R$ mit $a \equiv 0$. Wir haben zu zeigen: Aus $a \in \mathfrak{a}$ und $r \in R$ folgt $ra \in \mathfrak{a}$ und $ar \in \mathfrak{a}$. Dazu multipliziere man die Kongruenzen $a \equiv 0$ und $r \equiv r$. Es wird dann $ra \equiv 0$ und $ar \equiv 0$, also $ra \in \mathfrak{a}$ und $ar \in \mathfrak{a}$.
b) Die Nebenklassen $r + \mathfrak{a}$ einer additiven Untergruppe $\mathfrak{a}$ von R definieren eine Partition, also eine Äquivalenzrelation „$\equiv$“ auf R; erst recht gilt dies, falls $\mathfrak{a}$ sogar ein Ideal ist. Nach Satz 8.2 lautet die Äquivalenzrelation:

$$a \equiv a' \quad \Leftrightarrow \quad a' - a \in \mathfrak{a}.$$

Es sei nun $a \equiv a'$ und $b \equiv b'$. Zu zeigen ist $a + b \equiv a' + b'$ und $ab \equiv a'b'$. Mit Elementen $\alpha_i \in \mathfrak{a}$ lauten die Voraussetzungen $a' = a + \alpha_1$ und $b' = b + \alpha_2$. Addition liefert $a' + b' = a + b + \alpha_3$, also $a + b \equiv a' + b'$. Multiplikation ergibt $a'b' = ab + a\alpha_2 + \alpha_1 b + \alpha_1\alpha_2 = ab + \alpha_4$, also $ab \equiv a'b'$; dabei wurden (2) und (1) benutzt.

Eine Kongruenzrelation „$\equiv$“ auf einem Ring R ist also durch die Angabe des Ideals $\mathfrak{a} \subset R$ aller Ringelemente r mit $r \equiv 0$ eindeutig bestimmt. Man schreibt deshalb $a \equiv a' \bmod \mathfrak{a}$, und das bedeutet $a' - a \in \mathfrak{a}$. Nur im Falle $R = \mathfrak{Z}$ haben sich an Stelle von $a \equiv a' \bmod n\mathfrak{Z}$ die bereits in § 20.1 eingeführten kürzeren Schreibweisen eingebürgert.
Es sei R ein Ring und $\mathfrak{a}$ ein Ideal aus R. Wir denken an die additive Struktur von R und bezeichnen die Menge $\{\mathfrak{a}, r + \mathfrak{a}, s + \mathfrak{a}, \ldots\}$ der voneinander verschiedenen unter den Nebenklassen von $\mathfrak{a}$ wie in § 12 mit $R/\mathfrak{a}$. Nach Satz 2 entspricht $R/\mathfrak{a}$ einer Aufteilung von R in Kongruenzklassen, und nach Satz 19.2 werden durch

$$\begin{aligned}(r + \mathfrak{a}) \;+\; (s + \mathfrak{a}) &= (r + s) \;+\; \mathfrak{a},\\ (r + \mathfrak{a}) \;\cdot\; (s + \mathfrak{a}) &= rs \;+\; \mathfrak{a}\end{aligned}$$

eine Addition und eine Multiplikation auf $R/\mathfrak{a}$ erklärt; die Addition ist bereits aus § 12 bekannt. Da $R/\mathfrak{a}$ aus den verschiedenen Kongruenzklassen modulo $\mathfrak{a}$ besteht, ist die algebraische Struktur $R/\mathfrak{a}$ auf Grund von Satz 19.2 sogar ein homomorphes Bild des Ringes R; der zugehörige Homomorphismus ist definiert durch $f(r) = r + \mathfrak{a}$. Nach Satz 1 ist also $R/\mathfrak{a}$ ein Ring. Dies rechtfertigt die

Definition: *Ist $\mathfrak{a}$ ein Ideal des Ringes R, so heißt $R/\mathfrak{a}$ der Restklassenring von R nach $\mathfrak{a}$.*

Man rechnet in $R/\mathfrak{a}$ wie in R und behandelt dabei Elemente aus $\mathfrak{a}$ wie Null. Auch bei der folgenden Definition denken wir in erster Linie an die additive Struktur von R.

Definition: *Unter dem Kern $\mathfrak{k}$ eines Ringhomomorphismus f von R auf R^* versteht man die Menge aller $r \in R$ mit $f(r) = 0$.*

In Analogie zu Satz 12.2 steht nun der folgende *Homomorphiesatz für Ringe*; er besagt in der Hauptsache, daß mit den Restklassenringen $R/\mathfrak{a}$ alle homomorphen Bilder von R gefunden sind.

Satz 3: *Es sei R ein Ring. Dann gelten die folgenden Aussagen.*
a) *Ist $\mathfrak{a}$ ein Ideal von R, so ist der Restklassenring $R/\mathfrak{a}$ ein homomorphes Bild von R. Der vermittelnde Homomorphismus f lautet $f(r) = r + \mathfrak{a}$.*
b) *Ist f ein Ringhomomorphismus von R auf R^* mit dem Kern $\mathfrak{k}$, so ist $\mathfrak{k}$ ein Ideal von R.*
c) *Ist f ein Ringhomomorphismus von R auf R^* mit dem Kern $\mathfrak{k}$, so gilt $R^* \simeq R/\mathfrak{k}$. Der Isomorphismus $\varphi\colon R/\mathfrak{k} \to R^*$ lautet $\varphi(r + \mathfrak{k}) = f(r)$.*
d) *Ein Ringhomomorphismus f von R auf R^* ist genau dann ein Isomorphismus, wenn der Kern von f nur aus der Null allein besteht.*

Beweis:
a) Das wurde bereits gezeigt.
b) Nach Satz 12.2 ist $\mathfrak{k}$ eine additive Untergruppe von R. Aus $k \in \mathfrak{k}$ und $r \in R$ folgt ferner $f(rk) = f(r)f(k) = 0$, also $rk \in \mathfrak{k}$, und $f(kr) = f(k)f(r) = 0$, also $kr \in \mathfrak{k}$.
c) Nach Satz 2 und Satz 19.2 ist R^* einem Restklassenring von R isomorph. Wir bezeichnen ihn mit $R/\mathfrak{a}$. Der vermittelnde Isomorphismus $\varphi\colon R/\mathfrak{a} \to R^*$ war $\varphi(r + \mathfrak{a}) = f(r)$. Dabei besteht $\mathfrak{a}$ aus allen denjenigen Elementen $k \in R$, für die $f(k) = f(0)$ die Null von R^* ist: $\mathfrak{a} = \mathfrak{k}$.
d) Die Abbildung f ist genau dann bijektiv, wenn ihr Kern $\{0\}$ ist.

Beispiel 1. Ein beliebiger Ring R hat $R/\{0\}$ als isomorphes und den Nullring R/R als homomorphes Bild.

Beispiel 2. Der Ring $\mathfrak{Z}$ hat $\mathfrak{Z}/\{0\}$ als isomorphes Bild. Die sämtlichen weiteren homomorphen Bilder $\mathfrak{Z}/n\mathfrak{Z}$ sind die Restklassenringe $\mathfrak{Z}_n$.

Beispiel 3. Die einzigen homomorphen Bilder eines Schiefkörpers S sind $S/\{0\}$, also S selbst, und der Nullring S/S.

21.3 Wir beschließen unsere Überlegungen mit dem Analogon zu Satz 14.2 für Ringhomomorphismen; an Stelle der Normalteiler stehen jetzt die Ideale.

Satz 4: *Es sei $f\colon R \to R^*$ ein Ringhomomorphismus von R auf R^* mit dem Kern $\mathfrak{k}$, ferner M die Menge aller Ideale $\mathfrak{a}$ von R mit $\mathfrak{k} \subset \mathfrak{a} \subset R$ und weiterhin M^* die Menge aller Ideale $\mathfrak{a}^*$ von R^*. Dann definiert $\varphi(\mathfrak{a}) = f(\mathfrak{a})$ eine bijektive Abbildung $\varphi\colon M \to M^*$, und es ist $\varphi^{-1}(\mathfrak{a}^*) = f^{-1}(\mathfrak{a}^*)$.*

Beweis: Betrachtet man zunächst f als einen Homomorphismus der additiven Gruppen von R und R^*, so bleibt über Satz 14.1 hinaus nur zu zeigen, daß mit $\mathfrak{a} \subset R$ auch $f(\mathfrak{a})$ und mit $\mathfrak{a}^* \subset R^*$ auch $f^{-1}(\mathfrak{a}^*)$ ein Ideal ist. Es sei also zunächst $\mathfrak{a}$ ein Ideal von R. Da sich jedes $r^* \in R^*$ in der Gestalt $f(r)$ mit einem $r \in R$ schreiben läßt, wird $r^*f(\mathfrak{a}) = f(r)f(\mathfrak{a}) = f(r\mathfrak{a}) \subset f(\mathfrak{a})$ und $f(\mathfrak{a})r^* = f(\mathfrak{a})f(r) = f(\mathfrak{a}r) \subset f(\mathfrak{a})$; also ist die additive Untergruppe $f(\mathfrak{a})$ von R^* sogar ein Ideal. Ist umgekehrt $\mathfrak{a}^*$ ein Ideal von R^* und $r \in R$, so werden $rf^{-1}(\mathfrak{a}^*)$ und $f^{-1}(\mathfrak{a}^*)r$ durch f in $\mathfrak{a}^*$ abgebildet; also gilt $rf^{-1}(\mathfrak{a}^*) \subset f^{-1}(\mathfrak{a}^*)$ und $f^{-1}(\mathfrak{a}^*)r \subset f^{-1}(\mathfrak{a}^*)$, und auch die additive Untergruppe $f^{-1}(\mathfrak{a}^*)$ von R ist sogar ein Ideal.

Aufgabe 1: Man bestimme alle homomorphen Bilder des Restklassenringes $\mathfrak{Z}_n$.

Aufgabe 2: Es seien $\mathfrak{k}$ und $\mathfrak{a}$ Ideale des Ringes R mit $\mathfrak{k} \subset \mathfrak{a} \subset R$. Dann gilt

$$R/\mathfrak{a} \simeq (R/\mathfrak{k})/(\mathfrak{a}/\mathfrak{k}).$$

Beweis?

§ 22 Einbettung von Integritätsbereichen in Körper

22.1 Die folgenden Überlegungen stehen in deutlicher Analogie zu denen in § 13. Es sei ein Ring R gegeben. Wir fragen: Wann gibt es einen Schiefkörper $S \supset R$? Damit das möglich ist, muß sicher R nullteilerfrei sein, weil S keine Nullteiler enthält. Wieder kennt man Beispiele nichtkommutativer nullteilerfreier Ringe, die eine Einbettung in Schiefkörper nicht gestatten; aber es gilt der wichtige

Satz 1: *Jeder Integritätsbereich I läßt sich in einen eindeutig bestimmten kleinsten Oberkörper Q, den Quotientenkörper von I, einbetten. Das heißt: Zu einem vorgegebenen Integritätsbereich I gibt es einen Körper Q mit folgenden Eigenschaften.*
(1) $Q \supset I$.
(2) Ist K ein Körper, der I umfaßt, $K \supset I$, so gilt $K \supset Q \supset I$.
(3) Ist Q' ein Körper, der an Stelle von Q die Bedingungen (1) und (2) erfüllt, so gilt $Q' = Q$.

Beweis: Angenommen, die Existenz eines Körpers Q mit den Eigenschaften (1) und (2) sei bereits bewiesen. Dann gilt gewiß die Eindeutigkeitsaussage (3). Denn für $K = Q'$ bekommt man $Q' \supset Q$, und analog wird umgekehrt $Q \supset Q'$, insgesamt also $Q' = Q$. Zu zeigen bleibt also die Existenz eines Körpers Q mit den Eigenschaften (1) und (2).
Wieder nehmen wir für den Augenblick an, es gäbe einen Körper $K \supset I$; dann enthält er speziell die Teilmenge

$$U_K = \{y: y = \frac{a}{b},\ a, b \in I,\ b \neq 0\} \supset I.$$

Mit den Bruchrechenregeln von Satz 20.5 prüft man nach, daß U_K ein Unterkörper von K ist. Ist ferner U ein Unterkörper von K, der I umfaßt, so liegen in U auch die Lösungen der Gleichungen $yb = a, a, b \in I, b \neq 0$, und das heißt $U \supset U_K$. In K ist also U_K der kleinste Unterkörper, der I umfaßt. Wären wir von einem anderen Körper $K^* \supset I$ ausgegangen und hätten entsprechend U_{K^*} gebildet, so brauchten wir wegen $U_K \simeq U_{K^*}$ diese beiden Körper nicht als verschieden anzusehen. Also ist U_K der zu konstruierende Körper Q. Unsere Konstruktion muß sich an den in U_K gültigen Rechenregeln

$$\frac{a}{b} = \frac{c}{d} \quad \Leftrightarrow \quad ad = bc, \tag{4}$$

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \tag{5}$$

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} \tag{6}$$

orientieren ($bd \neq 0$).
Nun bilden wir das cartesische Produkt $M = I \times I_0 \neq \mathfrak{L}$ aller Paare (a, b) mit $a, b \in I$, $b \neq 0$, stellen uns unter (a, b) den Bruch $\frac{a}{b}$ vor und definieren

$$(a, b) \sim (c, d) \Leftrightarrow ad = bc. \tag{4'}$$

Das ist eine Äquivalenzrelation auf M; der Nachweis erfolgt wie in Aufgabe 5.2 und benutzt die Kommutativität und in Gestalt von Satz 20.2 die Nullteilerfreiheit von I. Die Addition und die Multiplikation auf M werden durch

$$(a, b) + (c, d) = (ad + bc, bd), \tag{5'}$$

$$(a, b) \cdot (c, d) = (ac, bd) \tag{6'}$$

erklärt; wegen $b \neq 0$, $d \neq 0$ und der Nullteilerfreiheit von I ist, wie es sein muß, $bd \neq 0$. Die Äquivalenzrelation auf M wird nun eine Kongruenzrelation: Aus $(a, b) \sim (a', b')$ und $(c, d) \sim (c', d')$, also $ab' = ba'$ und $cd' = dc'$, folgt, wie man leicht bestätigt, $(ad + bc)b'd' = bd(a'd' + b'c')$ und $acb'd' = bda'c'$, also $(a, b) + (c, d) \sim (a', b') + (c', d')$ und $(a, b) \cdot (c, d) \sim (a', b') \cdot (c', d')$.

Es sei A die Menge der Kongruenzklassen von M und $[a, b]$ die Klasse von (a, b). Nach Satz 19.3 werden durch $[a, b] + [c, d] = [ad + bc, bd]$ und $[a, b] \cdot [c, d] = [ac, bd]$ eine Addition und eine Multiplikation auf A erklärt. Wir wollen zeigen, daß A ein Körper ist. Zur Vereinfachung der dazu nötigen Rechnungen bemerken wir, daß für $c \neq 0$ gilt: $[a, b] = [ac, bc]$; es ist ja $(a, b) \sim (ac, bc)$. Man darf also in den Klassensymbolen erweitern oder kürzen. Ferner gibt es wenigstens ein $h \in I$, $h \neq 0$; dieses Element h sei im folgenden fest gewählt. Bei der Addition dreier Klassen kann man wegen der Möglichkeit des Erweiterns annehmen, die zweiten Komponenten seien alle dieselben, und bekommt so das Assoziativgesetz

$$([a, d] + [b, d]) + [c, d] = [a + b, d] + [c, d] = [(a + b) + c, d]$$
$$= [a + (b + c), d] = [a, d] + [b + c, d] = [a, d] + ([b, d] + [c, d]).$$

Die Addition ist auch kommutativ, $[0, h]$ ist Nullelement und $[-a, b]$ additives Inverses von $[a, b]$. Die Multiplikation ist ersichtlich assoziativ und kommutativ. Es gilt das Distributivgesetz

$$[a, d]([b, d] + [c, d]) = [a, d] \cdot [b + c, d] = [ab + ac, d^2]$$
$$= [ab, d^2] + [ac, d^2] = [a, d] \cdot [b, d] + [a, d] \cdot [c, d].$$

Einselement ist $[h,h] \in A$. Es gilt $[a, b] = [0, h]$ genau dann, wenn $a = 0$ ist; eine von Null verschiedene Klasse $[a, b]$ wird also durch $a \neq 0$ gekennzeichnet, und sie besitzt dann das Inverse $[b, a] \in A$.

In dem Körper A betrachten wir die Teilmenge T aller Klassen der Gestalt $[ah, h]$, $a \in I$. Die Summe $[ah, h] + [bh, h] = [(a + b)h, h]$ und das Produkt $[ah, h] \cdot [bh, h] = [abh, h]$ zweier Klassen aus T liegen wieder in T. Die durch $\varphi(a) = [ah, h]$ definierte Abbildung $\varphi: I \to T$ erweist sich als bijektiv, und die Gleichungen $\varphi(a + b) = [(a + b)h, h] = [ah, h] + [bh, h] = \varphi(a) + \varphi(b)$ und $\varphi(ab) = [abh, h] = [ah, h] \cdot [bh, h] = \varphi(a)\varphi(b)$ zeigen ihre Relationstreue. Also gilt $T \simeq I$.
Wir ersetzen die Teilstruktur T von A durch I und bekommen auf diese Weise einen zu A isomorphen Körper $Q \supset I$. Der Körper A besteht aus allen Klassen $[a, b] = [ah, h] \cdot [h, bh] = [ah, h] \cdot [bh, h]^{-1}$, also Q aus allen Elementen y der Form $ab^{-1} = \frac{a}{b}$, $b \neq 0$. Es ist also Q der zu konstruierende Körper, und Satz 1 ist bewiesen.

22.2 In § 13 wurde aus der additiven Struktur $\mathfrak{N}$ die additive Gruppe von $\mathfrak{Z}$ konstruiert. Auf der Teilmenge $\mathfrak{N} \subset \mathfrak{Z}$ ist nun nach Satz 2.1 auch eine Multiplikation erklärt. Nach den Regeln von Satz 20.1 besteht höchstens eine Möglichkeit, diese Multiplikation derart auf ganz $\mathfrak{Z}$ auszudehnen, daß $\mathfrak{Z}$ ein Ring wird. Umgekehrt: Definiert man die Multiplikation gemäß Satz 20.1 auf ganz $\mathfrak{Z}$, so kann man das Erfülltsein des Assoziativ-, Kommutativ- und Distributivgesetzes dieser zweiten Verknüpfung von $\mathfrak{Z}$ mit Hilfe von Satz 2.1 durch wenige Fallunterscheidungen nachprüfen. Damit ist der kommutative Ring $\mathfrak{Z}$ aus $\mathfrak{N}$ konstruiert. Er enthält keine Nullteiler; denn gäbe es von Null verschiedene a, b mit $ab = 0$ in $\mathfrak{Z}$, so auch in $\mathfrak{N}$, was nicht der Fall ist. Nach Satz 1 besitzt $\mathfrak{Z}$ also einen Quotientenkörper; wir nennen ihn $\mathfrak{Q}$ und haben damit auch den Körper $\mathfrak{Q}$ der rationalen Zahlen aus $\mathfrak{N}$ gewonnen.

Aufgabe 1: Es sei R ein kommutativer Ring und $S \subset R$ die Menge der von Null verschiedenen Nichtnullteiler von R. Ist $S \neq \mathfrak{L}$, so läßt sich R in den Quotientenring R_S aller $\frac{r}{s}$, $r \in R$, $s \in S$, einbetten; es gilt $1 \in R_S$. Beweis?

Aufgabe 2: Es seien I_1 und I_2 isomorphe Integritätsbereiche mit den Quotientenkörpern $Q_1 \supset I_1$ und $Q_2 \supset I_2$. Man zeige, daß sich der Isomorphismus $f: I_1 \to I_2$ von I_1 auf I_2 zu einem Isomorphismus $\varphi: Q_1 \to Q_2$ von Q_1 auf Q_2 fortsetzen läßt. (Das heißt: Es gibt einen Isomorphismus φ von Q_1 auf Q_2 mit $\varphi(a) = f(a)$ für jedes $a \in I_1$.)

§ 23 Der komplexe Zahlkörper $\mathfrak{C}$

23.1 In $\mathfrak{N}$ ist nach § 2 eine Addition erklärt; aber die Gleichung $a + x = b$ mit $a, b \in \mathfrak{N}$ braucht keine Lösung $x \in \mathfrak{N}$ zu haben. In § 13 haben wir die fehlenden Lösungen hinzukonstruiert und dadurch die additive Gruppe von $\mathfrak{Z}$ gewonnen. Die ebenfalls nach § 2 auf $\mathfrak{N} \subset \mathfrak{Z}$ zusätzlich erklärte Multiplikation ließ sich, wie wir gerade sahen, auf ganz $\mathfrak{Z}$ fortsetzen derart, daß $\mathfrak{Z}$ ein Ring wird. Aber die Gleichung $ax = b$, $a \neq 0$, mit $a, b \in \mathfrak{Z}$ war im allgemeinen

in $\mathfrak{Z}$ nicht lösbar. In § 22 haben wir wiederum diese Lösungen hinzukonstruiert und $\mathfrak{Q}$ erhalten.
Ist nun ein Körper K vorgelegt, so kann man fragen, ob in ihm die Gleichung $x^2 + 1 = 0$ lösbar ist, ob es also ein Element $i \in K$ mit $i^2 + 1 = 0$ gibt. Ist es vorhanden, so erfüllen wegen der Nullteilerfreiheit von K genau die Elemente $\pm i$ die Gleichung $x^2 + 1 = x^2 - i^2 = (x + i)(x - i) = 0$. Ist es nicht vorhanden, so konstruieren wir wiederum einen eindeutig bestimmten minimalen Oberkörper $E \supset K$, in dem die Gleichung $x^2 + 1 = 0$ lösbar wird.

Satz 1: *Jeder Körper K läßt sich in einen eindeutig bestimmten kleinsten Oberkörper $E \supset K$ einbetten, in dem die Gleichung $x^2 + 1 = 0$ lösbar ist. Das heißt: Zu einem vorgegebenen Körper K gibt es einen Körper E mit folgenden Eigenschaften:*
(1) $E \supset K$.
(2) Die Gleichung $x^2 + 1 = 0$ besitzt in E eine Lösung.
(3) Ist $L \supset K$ ein Körper, in dem die Gleichung $x^2 + 1 = 0$ lösbar ist, so gilt $L \supset E \supset K$.
(4) Ist E' ein Körper, der an Stelle von E die Bedingungen (1), (2), (3) erfüllt, so gilt $E' = E$.

Beweis: Die Eindeutigkeitsaussage (4) ergibt sich wie in den Beweisen der Sätze 13.1 und 22.1. Zu zeigen bleibt also die Existenz eines Körpers E mit den Eigenschaften (1), (2), (3). Ist die Gleichung $x^2 + 1 = 0$ schon in K lösbar, so ist $E = K$; wir nehmen daher an, daß -1 in K kein Quadrat ist.
Angenommen, es gibt einen Körper $L \supset K$ mit einer Lösung $i \in L$ der Gleichung $x^2 + 1 = 0$; dann enthält L die Teilmenge

$$U_L = \{z : z = a + bi, a, b \in K\} \supset K,$$

und man prüft leicht nach, daß U_L ein Unterkörper von L ist. Speziell liegen wegen

$$(a + bi) + (c + di) = (a + c) + (b + d)i, \tag{5}$$

$$(a + bi) \cdot (c + di) = (ac - bd) + (ad + bc)i \tag{6}$$

Summe und Produkt zweier Elemente aus U_L wieder in U_L, und das Inverse von $a + bi \neq 0$ wird, wie die Probe bestätigt, das Element

$$\frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2} i \in U_L;$$

dabei ist der Nenner $a^2 + b^2$ nicht Null, weil andernfalls $a^2 = -b^2$ und $b \neq 0$, also doch $-1 = \left(\frac{a}{b}\right)^2 \in K$ in K Quadrat wäre im Widerspruch zur Annahme.
Ferner gilt

$$a + bi = c + di \Leftrightarrow a = c \text{ und } b = d; \tag{7}$$

wäre nämlich $a + bi = c + di$ und $b \neq d$, so würde $i = \frac{a - c}{d - b} \in K$ folgen, was

gerade nicht der Fall war. Ist U ein Unterkörper von L, der K und i umfaßt, so gilt gewiß $U \supset U_L$. In L ist also U_L der kleinste Körper mit $U_L \supset K$, in dem die Gleichung $x^2 + 1 = 0$ lösbar ist.
Hätten wir einen anderen Körper $L^* \supset K$ mit einer Lösung $i^* \in L^*$ der Gleichung $x^2 + 1 = 0$ zugrundegelegt, so würde

$$U_L \simeq U_{L^*} = \{z^* : z^* = a + bi^*, a, b \in K\}$$

gelten vermöge $f(a + bi) = a + bi^*$. Also ist U_L der zu konstruierende Körper E. Wieder ist auf Grund der Beziehungen (5), (6), (7) klar, wie wir in unserer folgenden Konstruktion vorzugehen haben.
Wir bilden das cartesische Produkt $M = K \times K$ aller (a, b) mit $a, b \in K$; intuitiv bedeute (a, b) die Zahl $a + bi$. Unsere Vorüberlegung (7) hinsichtlich der Gleichheit zweier solcher Zahlen zeigt, daß wir eine Äquivalenzrelation auf M nicht einzuführen haben. Wir definieren

$$(5') \qquad (a, b) + (c, d) = (a + c, b + d),$$

$$(6') \qquad (a, b) \cdot (c, d) = (ac - bd, ad + bc)$$

und bestätigen in kurzen Rechnungen die Ringaxiome. Die Multiplikation ist kommutativ, $(1, 0)$ ist Einselement, und jedes $(a, b) \neq (0, 0)$ hat in M ein Inverses. Also ist M ein Körper. Jedes $(a, b) \in M$ läßt sich in der Gestalt $(a, b) = (a, 0) + (0, b)$ oder

$$(8) \qquad (a, b) = (a, 0) + (b, 0) \cdot (0, 1)$$

schreiben; dabei ist $(0, 1)^2 = (-1, 0)$.
Nun kommen die Änderungen der Schreibweise. Die Teilstruktur

$$T = \{(a, 0) : a \in K\} \subset M$$

ist isomorph K; man bilde dazu einfach $(a, 0)$ auf a ab. In M ersetzen wir T durch K und schreiben i für $(0, 1)$; dann entsteht ein Erweiterungskörper $E \supset K$, dessen Elemente nach (8) die Gestalt $a + bi$ mit $a, b \in K$ und $i^2 = -1$ haben. Damit ist der gesuchte Körper E konstruiert und Satz 1 bewiesen.

23.2 Aus $K = \mathfrak{R}$ entsteht auf diese Weise der komplexe Zahlkörper $E = \mathfrak{C}$. Damit haben wir, von der Struktur $\mathfrak{N}$ ausgehend, abgesehen von $\mathfrak{R}$ alle Rechenbereiche $\mathfrak{Z}, \mathfrak{Q}, \mathfrak{R}, \mathfrak{C}$ konstruiert und ihre Widerspruchsfreiheit auf die von $\mathfrak{N}$ zurückgeführt. Die Konstruktion von $\mathfrak{R}$ holen wir in § 32 nach.

23.3 Ist K ein Körper, in dem ein $i \in K$ existiert, das die Gleichung $x^2 + 1 = 0$ löst, so sind, wie wir bereits wissen, i und $-i$ die beiden einzigen Lösungen von $x^2 + 1 = 0$. Sie fallen genau dann zusammen, $i = -i$, wenn $(1 + 1)i = 0$, also $\chi(K) = 2$ ist, und in diesem Fall ist einfach $i = 1$.
Von zahlentheoretischem Interesse ist die Frage, in welchen Primkörpern $\mathfrak{Z}_p$ die Gleichung $x^2 + 1 = 0$ lösbar ist. Durch Probieren stellt man beispielsweise fest, daß $x^2 + 1 = 0$ in $\mathfrak{Z}_2$ lösbar, in $\mathfrak{Z}_3$ dagegen unlösbar ist. Die Antwort gibt der

Satz 2: *Es sei p eine Primzahl. Genau dann ist die Gleichung $x^2 + 1 = 0$ in $\mathfrak{Z}_p$ lösbar, wenn $p = 2$ oder $p \equiv 1\,(4)$ ist. Oder: Genau dann ist die Kongruenz $x^2 \equiv -1(p)$ in ganzen Zahlen x lösbar, wenn $p = 2$ oder p eine Primzahl der Gestalt $4n + 1$ ist.*

Beweis: Der Fall $p = 2$ ist bereits erledigt. Wir haben weiter zu zeigen, daß die Gleichung $x^2 + 1 = 0$ für eine Primzahl p der Form $4n + 1$ in $\mathfrak{Z}_p$ lösbar, für eine Primzahl p der Form $4n + 3$ dagegen in $\mathfrak{Z}_p$ unlösbar ist.
a) Es sei $p = 4n + 1$. Wir sind fertig, wenn wir eine natürliche Zahl m mit $m^2 \equiv -1(p)$ angeben können. Nach Satz 20.6 gilt nun $(p-1)! \triangleq -1 \bmod p$. Hierin wird modulo p

$$\begin{aligned}(p-1)! &= 1 \cdot 2 \cdots (2n)(2n+1)(2n+2) \cdots (4n)\\ &\equiv 1 \cdot 2 \cdots (2n)(2n+1-p)(2n+2-p) \cdots (4n-p)\\ &= 1 \cdot 2 \cdots (2n)(-2n)(-(2n-1)) \cdots (-1)\\ &= (2n)!(2n)!.\end{aligned}$$

Wir können also $m = (2n)!$ wählen.
b) Es sei $p = 4n + 3$. Wir nehmen an, es gäbe ein $a \in \mathfrak{Z}_p$ mit $a^2 = -1$, und potenzieren mit der ungeraden Zahl $\frac{p-1}{2}$. Das liefert $a^{p-1} = -1$. Sicher ist a nicht Null, liegt demnach in der multiplikativen Gruppe von $\mathfrak{Z}_p$, die aus $p - 1$ Elementen besteht. Anwendung von Satz 9.4 ergibt also $a^{p-1} = 1$. Aus beidem zusammen folgt $1 = -1$, was wegen $\chi(\mathfrak{Z}_p) \geqq 3$ nicht möglich ist.

Aufgabe 1: Es sei M die Menge aller Matrizen der Gestalt

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \qquad (a, b \in \mathfrak{R});$$

auf M seien die Matrizenaddition und die Matrizenmultiplikation eingeführt. Man zeige $M \simeq \mathfrak{C}$.

Aufgabe 2: Es sei K ein Körper, in dem kein Element α mit $\alpha^2 = 2$ existiert. Man konstruiere einen minimalen Oberkörper $E \supset K$, der ein solches Element enthält.

§ 24 Endomorphismenringe abelscher Gruppen

Es sei $G = \{a, b, c, \ldots\}$ eine additiv geschriebene abelsche Gruppe und $R = \{\alpha, \beta, \gamma, \ldots\}$ die Menge aller Endomorphismen von G, also die Menge aller relationstreuen Abbildungen von G in sich (vgl. § 19). Da die identische Abbildung ε in R liegt, ist R nicht leer. Mit $\alpha, \beta \in R$ ist wegen $\alpha\beta(a + b) = \alpha(\beta(a) + \beta(b)) = \alpha\beta(a) + \alpha\beta(b)$ auch $\alpha\beta \in R$, und diese Multiplikation ist assoziativ nach Satz 3.1; sie besitzt das Einselement ε.
Wir führen nun auf R noch eine Addition ein. Dies geschieht, wie es für Funktio-

nen üblich ist, durch die Festsetzung $(\alpha + \beta)(a) = \alpha(a) + \beta(a)$. Wir müssen nur nachprüfen, daß mit $\alpha, \beta \in R$ auch $\alpha + \beta$ ein Endomorphismus ist:

$$\begin{aligned}(\alpha + \beta)(a + b) &= \alpha(a + b) + \beta(a + b) = \alpha(a) + \alpha(b) + \beta(a) + \beta(b) \\ &= \alpha(a) + \beta(a) + \alpha(b) + \beta(b) = (\alpha + \beta)(a) + (\alpha + \beta)(b).\end{aligned}$$

Hierbei haben wir die Kommutativität von G benutzt. Aus der Assoziativität und der Kommutativität der Addition in G folgen dieselben Eigenschaften für die Addition in R. Nullelement in R ist der Endomorphismus o, der jedes $g \in G$ auf die Null abbildet: Die für jedes $\alpha \in R$ und jedes $a \in G$ gültige Beziehung $(\alpha + o)(a) = \alpha(a) + 0 = \alpha(a)$ bedeutet ja $\alpha + o = \alpha$ für jedes $\alpha \in R$. Ist schließlich $\alpha \in R$, so definieren wir $-\alpha \in R$ durch $(-\alpha)(a) = -\alpha(a)$; dabei ist $-\alpha$ wegen $(-\alpha)(a + b) = -(\alpha(a) + \alpha(b)) = -\alpha(b) - \alpha(a) = -\alpha(a) - \alpha(b) = (-\alpha)(a) + (-\alpha)(b)$ wieder ein Endomorphismus und $\alpha + (-\alpha) = o$.
Um zu zeigen, daß R ein Ring ist, weisen wir noch die Distributivgesetze nach. Es ist $\alpha(\beta + \gamma)(a) = \alpha(\beta(a) + \gamma(a)) = \alpha\beta(a) + \alpha\gamma(a) = (\alpha\beta + \alpha\gamma)(a)$ für jedes $a \in G$, also $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$, und entsprechend erhält man $(\beta + \gamma)\alpha = \beta\alpha + \gamma\alpha$. Damit haben wir den

Satz 1: *Die Menge R aller Endomorphismen einer (additiv geschriebenen) abelschen Gruppe G ist (bezüglich der oben eingeführten Verknüpfungen) ein Ring, der sogenannte Endomorphismenring von G.*

Allgemeiner nennt man jeden Ring von Endomorphismen einen *Endomorphismenring*. Die Endomorphismenringe haben für die Theorie der Ringe eine ähnliche Bedeutung wie die Transformationsgruppen für die Gruppentheorie. Es ist nicht schwer, in Analogie zu Satz 7.2 zu zeigen, daß jeder Ring einem Endomorphismenring isomorph ist. Man benutzt dabei das Ergebnis der

Aufgabe 1: Jeder Ring R läßt sich in einen Ring E mit Einselement einbetten. Beweis?

§ 25 Polynomringe

25.1 Unter einem Polynom versteht man in der Algebra formal zwar dasselbe, inhaltlich aber etwas anderes als in der Analysis. Das ändert indes nichts daran, daß die später von uns gewonnenen Sätze doch wieder eine bekannte Gestalt annehmen. Wir beginnen mit der

Definition: *Es seien R und $R^* \supset R$ kommutative Ringe mit demselben Einselement $1 \in R$. Es sei $\alpha \in R^*$. Dann heißt ein Ausdruck der Gestalt*

$$f(\alpha) = \sum_{\nu=0}^{n} a_\nu \alpha^\nu = a_n\alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_0 \in R^* \quad (a_\nu \in R,\ \alpha^0 =_{Df} 1)$$

ein Polynom in α mit Koeffizienten aus R. Die Menge aller Polynome in α mit Koeffizienten aus R wird mit $R[\alpha]$ bezeichnet.

Hierzu machen wir zwei Bemerkungen. Erstens ist es in Anlehnung an die Gepflogenheiten in der Analysis auch in der Algebra üblich, etwa $f(\alpha)$ für ein

Polynom in α zu schreiben, ohne daß man damit f als ein Symbol für eine Abbildung ansieht. Zweitens ist die zu Beginn der Definition ausgesprochene Voraussetzung, etwas umständlicher formuliert, die folgende: Es seien R und $R^* \supset R$ kommutative Ringe mit Einselementen $e \in R^*$ und $1 \in R$, *und es gelte* $e = 1$. Diese letzte Forderung ist, wie man durch Beispiele zeigen kann, nicht von selbst erfüllt (vgl. hierzu die Lösung von Aufgabe 24.1). Sollten aber R^* und R sogar Integritätsbereiche sein, so ist $e = 1$ beweisbar: Es ist ja $1(e - 1) = 1e - 1 \cdot 1 = 1 - 1 = 0$, wegen der Nullteilerfreiheit von R^* also $e = 1$. Speziell bedeutet das: Ist L ein Oberkörper von K, so ist das Einselement von K auch die Eins von L. Da nun $1 \in R$ auch Eins von R^* sein soll, kann man, und das ist der Sinn dieser Forderung, in einem Polynom $f(\alpha)$ Koeffizienten 1 wie gewohnt weglassen.
Es ist klar, daß unter den genannten Voraussetzungen $R[\alpha]$ ein kommutativer Unterring von R^* mit dem Einselement 1 ist. Es gilt ja

$$(1) \qquad \sum_0^n a_\nu \alpha^\nu + \sum_0^m b_\mu \alpha^\mu = \sum_0^M s_\lambda \alpha^\lambda \text{ mit } s_\lambda = a_\lambda + b_\lambda \text{ und } M = \operatorname{Max}(n, m),$$

$$(2) \qquad \sum_0^n a_\nu \alpha^\nu \cdot \sum_0^m b_\mu \alpha^\mu = \sum_0^{n+m} p_\lambda \alpha^\lambda \text{ mit } p_\lambda = a_0 b_\lambda + a_1 b_{\lambda-1} + \ldots + a_\lambda b_0;$$

dabei haben wir $a_\nu = b_\mu = 0$ gesetzt für $\nu > n$ und $\mu > m$. Das additive Inverse $-f(\alpha)$ eines Polynoms $f(\alpha) \in R[\alpha]$ bekommt man, indem man alle Koeffizienten von $f(\alpha)$ mit einem Minuszeichen versieht, und auch die Null ist ein Polynom.

Beispiel 1. Man wähle $R = \mathfrak{Z}$, $R^* = \mathfrak{R}$ und $\alpha = \sqrt{2}$. Der Ring $\mathfrak{Z}[\sqrt{2}]$ ist dann, da die geraden Potenzen von $\sqrt{2}$ Elemente aus $\mathfrak{Z}$ und die ungeraden Potenzen Elemente der Gestalt $m\sqrt{2}$, $m \in \mathfrak{Z}$, liefern, der Ring aus § 20.1, Beispiel 4. Zwei Polynome in $\alpha = \sqrt{2}$ mit Koeffizienten aus $\mathfrak{Z}$ können also dieselben sein, auch wenn sie nicht koeffizientenweise übereinstimmen.

Beispiel 2. Wählen wir $R = \mathfrak{Q}$, $R^* = \mathfrak{R}$ und $\alpha = \sqrt{2}$, so bekommen wir den Ring $\mathfrak{Q}[\sqrt{2}]$, der, wie wir in § 20.3, Beispiel 6, sahen, sogar ein Körper ist.

Beispiel 3. Es ist $\mathfrak{R}[i] = \mathfrak{C}$.

Beispiel 4. Der Ring $\mathfrak{Q}[\sqrt[3]{2}]$ besteht genau aus allen reellen Zahlen der Gestalt $a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2$ mit $a, b, c \in \mathfrak{Q}$.

25.2 Wir gehen wieder von einem kommutativen Ring R mit $1 \in R$ aus und stellen die Frage: Gibt es einen kommutativen Oberring R^* mit demselben Einselement, der ein Element $x \in R^*$ enthält, das die Bedingung

$$(3) \qquad f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0 = 0 \Leftrightarrow a_\nu = 0 \quad (a_\nu \in R;\ \nu = 0, 1, 2, \ldots, n)$$

erfüllt? Das Rechnen in dem Polynomring $R[x]$ wäre dann durch das Rechnen in R und die Forderungen (3), (4), (5) vollständig beschrieben.

Definition: *Es sei R ein kommutativer Ring, $1 \in R$, und R^* ein Oberring von R. Ein Element $x \in R^*$ heißt Unbestimmte über R, wenn es die drei Bedingungen* (3), (4), (5) *erfüllt*:

(4) $1 \cdot x = x \cdot 1 = x$,
(5) $rx = xr$ *für jedes* $r \in R$.

Wir zeigen nun, daß es zu jedem R eine solche Unbestimmte x über R, also auch den Polynomring $R[x]$, gibt.

Satz 1: *Es sei R ein kommutativer Ring und $1 \in R$. Dann existiert ein kommutativer Oberring $R[x] \supset R$ aller Polynome $f(x)$ in einer Unbestimmten x über R mit Koeffizienten aus R. Er besitzt ebenfalls das Einselement* 1.

Beweis: Die letzte Behauptung ist, falls die übrigen bewiesen sind, trivial. Wir führen nun wieder eines unserer Konstruktionsverfahren durch. Mengentheoretisch gesichert ist die Existenz der Menge R^∞ aller unendlichen Folgen $(r_0, r_1, r_2, \ldots)$ von Elementen r_i aus R (§ 1.3). Wir könnten uns unter der Folge $(r_0, r_1, r_2, \ldots, r_n, r_{n+1}, \ldots)$ das Polynom $r_n x^n + r_{n-1}x^{n-1} + \ldots + r_0$ vorstellen, wenn alle r_ν mit $\nu > n$ Null wären. Also betrachten wir die Teilmenge $M \subset R^\infty$ aller derjenigen Folgen $(a_0, a_1, a_2, \ldots)$, in denen nur endlich viele a_ν ungleich Null sind. Aus dieser Menge M konstruieren wir $R[x]$.
Wir führen auf M nach dem Vorbild von (1) und (2) eine Addition und eine Multiplikation durch

$$(1') \quad (a_0, a_1, a_2, \ldots) + (b_0, b_1, b_2, \ldots) = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots),$$

$$(2') \quad (a_0, a_1, a_2, \ldots) \cdot (b_0, b_1, b_2, \ldots) = (p_0, p_1, p_2, \ldots) \quad \text{mit } p_\lambda = a_0 b_\lambda + a_1 b_{\lambda-1} + \ldots + a_\lambda b_0$$

ein; dabei hat man nachzuprüfen, daß die Ausdrücke rechter Hand wieder Elemente von M sind. Wir überlegen uns jetzt, daß wir eine Äquivalenzrelation auf M nicht einzuführen brauchen: Zwei Polynome $f(x)$ und $g(x)$ sind genau dann gleich, wenn ihr Differenzpolynom $f(x) - g(x)$ Null ist; nach (3) bedeutet das, daß $f(x)$ und $g(x)$ koeffizientenweise übereinstimmen müssen. Also müßte M bis auf die Schreibweise schon unser Ring $R[x]$ sein.
Ersichtlich ist M bezüglich der Addition eine abelsche Gruppe, weil R es ist. Ferner ist die Multiplikation kommutativ mit dem Einselement $(1, 0, 0, \ldots) \in M$. Rechnet man in

$$((a_0, a_1, a_2, \ldots) \cdot (b_0, b_1, b_2, \ldots)) \cdot (c_0, c_1, c_2, \ldots) = (r_0, r_1, r_2, \ldots)$$

die Komponente r_λ aus, so bekommt man

$$r_\lambda = \sum (a_i b_j) c_k \qquad (i + j + k = \lambda);$$

für den Fall, daß der zweite und der dritte Faktor linker Hand durch Klammern zusammengefaßt waren, bekommt man

$$r'_\lambda = \sum a_i (b_j c_k) \qquad (i + j + k = \lambda)$$

für die entsprechende Komponente des Ergebnisses. Es ist aber $r_\lambda = r'_\lambda$ wegen der Assoziativität der Multiplikation in R, die sich damit auf M überträgt. Eine letzte leichte Rechnung bestätigt noch das Distributivgesetz. Also ist M ein kommutativer Ring mit Einselement.
Nun kommen wieder die Änderungen der Schreibweise. Zunächst liefert die

Multiplikation eines Elements aus M mit $(0, 1, 0, 0, \ldots) \in M$ ein einfaches Resultat:

$$(a_0, a_1, a_2, \ldots) \cdot (0, 1, 0, 0, \ldots) = (0, a_0, a_1, a_2, \ldots).$$

Außerdem stellt man sofort fest, daß die Teilstruktur $T = \{(r, 0, 0, \ldots): r \in R\}$ von M isomorph R ist. Schreibt man nun für ein Element $(a_0, a_1, a_2, \ldots) \in M$ mit $a_\nu = 0$ für $\nu > n$ die Summe

$$(a_0, a_1, a_2, \ldots) = (a_0, 0, 0, \ldots) + (0, a_1, 0, \ldots) + \ldots + (0, 0, \ldots, 0, a_n, 0, \ldots)$$

und setzt $(0, 1, 0, 0, \ldots) = x$, so wird

$$(a_0, a_1, a_2, \ldots) = (a_0, 0, 0, \ldots) + (a_1, 0, 0, \ldots) \cdot x + \ldots + (a_n, 0, 0, \ldots) \cdot x^n.$$

Nach der Ersetzung von T durch R bekommen also die Elemente $(a_0, a_1, a_2, \ldots)$ von M die Gestalt $a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0$. Die Forderungen (3), (4), (5) sind offensichtlich erfüllt. Damit ist $R[x]$ konstruiert und Satz 1 bewiesen. Ziemlich selbstverständlich ist nun der

Satz 2: *Es seien R und $R^* \supset R$ kommutative Ringe mit demselben Einselement $1 \in R$; ferner sei x eine Unbestimmte über R und α ein Element von R^*. Dann wird durch $\varphi(f(x)) = f(\alpha)$ ein Homomorphismus φ von $R[x]$ auf $R[\alpha]$ definiert; dieser Homomorphismus ist ein Isomorphismus genau dann, wenn auch α eine Unbestimmte über R ist.*

Beweis: Die Abbildung φ ist surjektiv und sicher relationstreu, da man in (1) und (2) statt α auch x schreiben kann. Sie vermittelt einen Isomorphismus genau dann, wenn ihr Kern nur aus der Null allein besteht; das bedeutet aber: es gilt (3) mit α an Stelle von x, oder α ist Unbestimmte über R.
Die am häufigsten benutzte Konsequenz von Satz 2 ist der

Satz 3 (*Ersetzungssatz*): *Es seien R und $R^* \supset R$ kommutative Ringe mit demselben Einselement $1 \in R$; ferner sei x eine Unbestimmte über R und α ein Element von R^*. Dann geht eine auf den Verknüpfungen von $R[x]$ beruhende Identität in $R[x]$ in eine Identität in R^* über, wenn in ihr x durch α ersetzt wird.*

Beweis: Man wende den Homomorphismus φ von Satz 2 auf die betrachtete Identität aus $R[x]$ an.
Dieser Satz, der von vornherein klar ist, ist von großer Bedeutung; wir werden ihn oft benutzen.

25.3 Wir unterbrechen unsere Ausführungen durch einige Verabredungen und unmittelbar einsichtige Aussagen.
Sind R und $R^* \supset R$ kommutative Ringe mit demselben Einselement $1 \in R$ und ist α ein Element aus R^*, so ist $R[\alpha]$ der kleinste Ring, der R und α umfaßt; das gilt natürlich auch für den Spezialfall, daß α eine Unbestimmte über R ist. Man sagt auch, $R[\alpha]$ entsteht aus R durch *Ringadjunktion* von α. Sind x und y Unbestimmte über R, so gilt $R[x] \simeq R[y]$ nach Satz 2. Ist x eine Unbestimmte über R^*, so ist $R[x]$ ein Unterring von $R^*[x]$.
Hat $f(x) \in R[x]$ die Gestalt $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_0$ mit $a_n \neq 0$, so heißt a_n der höchste Koeffizient und a_0 das absolute Glied von $f(x)$. Ein

Polynom $f(x)$ heißt normiert, wenn sein höchster Koeffizient Eins ist. Buchstaben wie $x, y, \ldots$ werden vorwiegend für Ringerweiterungen durch Unbestimmte verwandt. Statt $f(x), g(x) \in R[x]$ schreibt man oft auch nur $f, g \in R[x]$. Spricht man von Polynomen über R, so meint man Polynome aus $R[x]$.
Für das Rechnen im Polynomring $R[x]$ weisen wir noch einmal auf die Unterschiede zur Analysis hin. Polynome sind keine Funktionen. Ein Polynom $f(x) \in R[x]$ in einer Unbestimmten x ist nach (3) nur Null, wenn es das Nullpolynom $0 \in R$ ist. Zwei Polynome $f(x), g(x) \in R[x]$ stimmen ebenfalls nach (3) genau dann überein, wenn sie koeffizientenweise übereinstimmen. Hierauf beruht die Methode des Koeffizientenvergleichs.
Schließlich gibt es auch Polynomringe ohne Einselement. Man betrachte etwa in $3[x]$ den Unterring $2\mathfrak{Z}[x]$ aller Polynome mit geraden ganzen Zahlen als Koeffizienten (vgl. auch in diesem Zusammenhang die Aufgabe 24.1).

25.4 Wir kommen zu einer weiteren

Definition: *Es sei $R[x]$ der Polynomring einer Unbestimmten x über R. Das Polynom $f(x) \in R[x]$ habe die Gestalt $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$ mit $a_n \neq 0$. Dann heißt n der Grad von $f(x)$.*

Die von Null verschiedenen Elemente aus R sind also Polynome vom Grad Null; für das Nullpolynom ist kein Grad definiert. Polynome vom Grad Eins bezeichnet man auch als lineare Polynome.
Sind $f(x)$, $g(x)$ und $f(x) + g(x)$ von Null verschiedene Polynome aus $R[x]$, so gilt

$$\text{Grad}\,(f(x) + g(x)) \leqq \text{Max}(\text{Grad}\, f(x), \text{Grad}\, g(x)). \tag{6}$$

Ist $f(x)g(x)$ nicht Null, so bekommt man

$$\text{Grad}\,(f(x)g(x)) \leqq \text{Grad}\, f(x) + \text{Grad}\, g(x), \tag{7}$$

und in dieser letzten Beziehung steht jedenfalls dann das Gleichheitszeichen, wenn R sogar ein Integritätsbereich ist.
Im Anschluß hieran stellen wir noch fest: Ist I ein Integritätsbereich mit Einselement, so ist auch $I[x]$ ein Integritätsbereich mit Einselement.

25.5 Wieder gehen wir von einem kommutativen Ring R mit Einselement aus; x sei eine Unbestimmte über R. Dann ist auch $R[x]$ ein kommutativer Ring mit Einselement; y sei eine Unbestimmte über $R[x]$. Man sieht, daß y erst recht Unbestimmte über R ist. Aber auch x bleibt Unbestimmte über $R[y]$, wie eine indirekte Überlegung sogleich zeigt. Sowohl $R[x][y]$ als auch $R[y][x]$ bestehen aus denselben Elementen, nämlich Summen von Ausdrücken der Gestalt $rx^m y^n$ ($r \in R$, $m \geqq 0$, $n \geqq 0$). Also gilt $R[x][y] = R[y][x]$, und man schreibt kurz $R[x, y]$.
Sind α, β beliebige Elemente eines kommutativen Oberringes $R^* \supset R$ mit demselben Einselement $1 \in R$, so gilt entsprechend $R[\alpha][\beta] = R[\beta][\alpha]$, und man schreibt wieder einfach $R[\alpha, \beta]$. Entsprechend bekommt man durch Adjunktion der Elemente $\alpha_1, \alpha_2, \ldots, \alpha_n \in R^*$ die Ringerweiterung $R[\alpha_1, \alpha_2, \ldots, \alpha_n]$ von R. Sollten die α_i sämtlich Unbestimmte über $R[\alpha_1, \alpha_2, \ldots, \alpha_{i-1}]$ sein, so spricht

man von *unabhängigen Unbestimmten* und schreibt etwas suggestiver etwa x_i statt α_i. Die Elemente von $R[\alpha_1, \alpha_2, \ldots, \alpha_n]$ sind Summen von Elementen der Gestalt $r\alpha_1^{\varrho_1}\alpha_2^{\varrho_2} \ldots \alpha_n^{\varrho_n}$ $(r \in R, \varrho_i \geqq 0)$.
Natürlich gelten die Verallgemeinerungen der Sätze 2 und 3; wir formulieren nur die letztere.

Satz 4: *Es seien R und $R^* \supset R$ kommutative Ringe mit demselben Einselement $1 \in R$; ferner seien $x_1, x_2, \ldots, x_n$ unabhängige Unbestimmte über R und $\alpha_1, \alpha_2, \ldots, \alpha_n$ Elemente von R^*. Dann geht eine auf den Verknüpfungen von $R[x_1, x_2, \ldots, x_n]$ beruhende Identität in $R[x_1, x_2, \ldots, x_n]$ in eine Identität in R^* über, wenn in ihr die x_i durch die α_i ersetzt werden.*

Da man in den Multiplikationsformeln (2) und (5) Elemente aus R kommutativ mit x multipliziert, wird der Ersetzungssatz natürlich falsch, wenn man auf die Kommutativität von R^* verzichtet.
Schließlich greifen wir noch einmal unsere letzte Feststellung im obigen Abschnitt 4 auf. Ihre wiederholte Anwendung führt zu dem

Satz 5: *Sind $x_1, x_2, \ldots, x_n$ unabhängige Unbestimmte über dem Integritätsbereich I mit Einselement, so ist auch $I[x_1, x_2, \ldots, x_n]$ ein Integritätsbereich mit Einselement.*

25.6 Ein wichtiges Hilfsmittel in der Theorie der Polynomringe ist der bereits aus der Schule bekannte Divisionsalgorithmus. Dabei gehen wir von einem Polynomring $K[x]$ über einem Körper K aus, wählen $f(x), g(x) \in K[x]$, $g(x) \neq 0$, und behaupten: Es gibt ein $q(x) \in K[x]$ und ein $r(x) \in K[x]$, so daß

$$f(x) = q(x)g(x) + r(x)$$

wird, wobei entweder $r(x) = 0$ oder Grad $r(x) <$ Grad $g(x)$ ist.
Der Beweis wird durch das übliche Verfahren geliefert, das Polynom $f(x)$ mit Rest durch das Polynom $g(x) \neq 0$ zu dividieren; es ist unverändert durchführbar, weil die Quotienten der Koeffizienten beliebiger Polynome aus $K[x]$ mit dem höchsten Koeffizienten von $g(x)$ wieder in K liegen. Das kann man auch in einen Induktionsbeweis nach dem Grad von $f(x)$ umschreiben: Für $f(x) = 0$ ist die Behauptung mit $q(x) = r(x) = 0$ richtig. Für Grad $f(x) = 0$ wähle man $q(x) = 0$ und $r(x) = f(x)$, falls Grad $g(x) > 0$ ist; bei Grad $g(x) = 0$ leisten $q(x) = \dfrac{f(x)}{g(x)} \in K$ und $r(x) = 0$ das Verlangte. Sowohl für $f(x) = 0$ als auch für Grad $f(x) = 0$ ist die Behauptung also richtig. Sie sei ferner für beliebige Polynome $f(x)$ von einem Grad kleiner als n und alle $g(x) = b_m x^m + b_{m-1}x^{m-1} + \ldots + b_0$, $b_m \neq 0$, bereits bewiesen. Ist dann $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$, $a_n \neq 0$, so können zwei Fälle eintreten. Bei $n < m$ wähle man einfach $q(x) = 0$ und $r(x) = f(x)$. Ist $n \geqq m$, so wird $f(x) = \dfrac{a_n}{b_m}x^{n-m}g(x) + h(x)$ mit einem $h(x) \in K[x]$, das entweder Null ist (und in diesem Fall ist man fertig) oder einen Grad $\leqq n - 1$ hat, also nach Voraussetzung in der Gestalt $h(x) = q^*(x)g(x) + r(x)$ mit $r(x) = 0$ oder Grad $r(x) <$ Grad $g(x)$ geschrieben

werden kann; das liefert dann aber $f(x) = q(x)g(x) + r(x)$ mit $q(x) = \frac{a_n}{b_m}x^{n-m} + q^*(x) \in K[x]$, womit der Induktionsbeweis abgeschlossen ist. Es gilt also der

Satz 6: *Es sei K ein Körper, $f(x), g(x) \in K[x]$ und $g(x) \neq 0$. Dann existieren $q(x), r(x) \in K[x]$ mit $f(x) = q(x)g(x) + r(x)$, wobei entweder $r(x) = 0$ oder Grad $r(x) <$ Grad $g(x)$ ist.*

Zusatz: Ist $g(x)$ normiert, der höchste Koeffizient also Eins, so kann in der Voraussetzung von Satz 6 der Körper K durch einen kommutativen Ring R mit Einselement ersetzt werden, weil in diesem Fall von selbst $\frac{a_n}{b_m} = a_n \in R$ ist.

Aufgabe 1: Am Beispiel des Endomorphismenringes R der additiven Gruppe von $\mathfrak{Q}[x]$ zeige man: Es gibt Ringe R mit Elementen $r \in R$, die unendlich viele Rechtsinverse, aber kein Linksinverses besitzen. (Vgl. Aufgabe 20.6, Aussage c).)

Aufgabe 2: Es sei R ein kommutativer Ring mit Einselement. Man konstruiere den Ring $R\langle x\rangle$ aller *formalen Potenzreihen* $\sum_{\nu=0}^{\infty} a_\nu x^\nu$, $a_\nu \in R$.

§ 26 Nullstellen von Polynomen

26.1 Wir betrachten wieder den Polynomring $R[x]$ über einem kommutativen Ring R mit $1 \in R$ und einen kommutativen Oberring $R^* \supset R$ mit demselben Einselement; α sei ein Element aus R^* und $f(x) \in R[x]$. Dann heißt α *Nullstelle* von $f(x)$ in R^*, wenn dort $f(\alpha) = 0$ gilt.

Beispiel 1. Das Polynom $x^2 - 4 \in \mathfrak{Z}[x]$ hat die Nullstellen $\pm 2 \in \mathfrak{Z}$; das Polynom $x^2 - 2 \in \mathfrak{Z}[x]$ hat die Nullstellen $\pm\sqrt{2} \in \mathfrak{R} \supset \mathfrak{Z}$ und $x^2 + 1 \in \mathfrak{Z}[x]$ die Nullstellen $\pm i \in \mathfrak{C} \supset \mathfrak{Z}$.

Beispiel 2. Nach Satz 23.2 hat das Polynom $x^2 + 1 \in \mathfrak{Z}_3[x]$ keine Nullstelle im Koeffizientenkörper $\mathfrak{Z}_3$. Aber nach Satz 23.1 existiert ein kleinster Oberkörper $E \supset \mathfrak{Z}_3$, in dem $x^2 + 1$ eine Nullstelle besitzt. Die Konstruktion im Beweis von Satz 23.1 zeigt noch, daß $|E| = 9$ ist.

Über die Nullstellen von Polynomen gelten einige ebenso einfache wie wichtige Sätze. Eine Konsequenz des Zusatzes zu Satz 25.6 ist zunächst der

Satz 1: *Es sei R ein kommutativer Ring mit Einselement, $f(x) \in R[x]$ und $\alpha \in R$ eine Nullstelle von $f(x)$. Dann gilt $f(x) = q(x) \cdot (x - \alpha)$ mit einem $q(x) \in R[x]$.*

Beweis: Es ist jedenfalls $f(x) = q(x)(x - \alpha) + r(x)$ mit einem $r(x) \in R[x]$, das entweder verschwindet oder den Grad Null hat. Das heißt $f(x) = q(x)(x - \alpha) + r$ mit einem festen $r \in R$. Ersetzen wir x durch α, so folgt $r = 0$.

Hieraus wiederum ergibt sich der

Satz 2: *Es sei I ein Integritätsbereich mit Einselement und $f(x) \in I[x]$ ein Polynom vom Grad n. Dann hat $f(x)$ in I höchstens n Nullstellen.*
Bemerkung: Das Polynom $f(x)$ hat also in keinem Integritätsbereich $I^* \supset I$ mit dem gemeinsamen Einselement $1 \in I$ mehr als n Nullstellen, da ja auch $f(x) \in I^*[x]$ gilt.

Beweis von Satz 2: Hat $f(x)$ die Nullstelle $\alpha_1 \in I$, so gilt nach Satz 1 zunächst $f(x) = (x - \alpha_1)q_1(x)$ mit einem $q_1(x) \in I[x]$. Hat $q_1(x)$ die Nullstelle $\alpha_2 \in I$, wobei die Möglichkeit $\alpha_2 = \alpha_1$ nicht ausgeschlossen ist, so wird weiter $f(x) = (x - \alpha_1)(x - \alpha_2)q_2(x)$ mit einem $q_2(x) \in I[x]$. Dieses Zerlegungsverfahren werde fortgesetzt; es bricht etwa nach m Schritten ab:

$$f(x) = (x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_m)q_m(x).$$

Dabei sind die α_i nicht notwendig verschiedene Nullstellen von $f(x)$ in I, und $q_m(x)$ hat keine Nullstelle in I. Mehr als diese m Nullstellen α_i hat $f(x)$ in I nicht; denn setzt man eine beliebige Nullstelle $\alpha \in I$ von $f(x)$ in die hingeschriebene Zerlegung ein, so muß wegen der Nullteilerfreiheit von I wenigstens einer der Faktoren $\alpha - \alpha_i$ verschwinden. Aus $m \leqq n$ folgt also die Behauptung.

Satz 2 bleibt demnach richtig, wenn mehrfach auftretende Nullstellen ihrer Vielfachheit entsprechend gezählt werden. Wir sagen in Zukunft, $f(x) \in I[x]$ habe die (genau) *k-fache Nullstelle* $\alpha \in I$, wenn $f(x) = (x - \alpha)^k q(x)$ mit einem $q(x) \in I[x]$, $q(\alpha) \neq 0$, gilt. Die Zahl $k \geqq 0$ ist definiert, weil $I[x]$ ein Integritätsbereich ist. Für das Nullpolynom wird der Begriff der Vielfachheit einer Nullstelle nicht erklärt. Satz 2 wird falsch, wenn die Nullteilerfreiheit des Koeffizientenringes nicht vorausgesetzt wird. Hierzu sehe man das

Beispiel 3. Das Polynom $f(x) = x^3 - x \in \mathfrak{Z}_6[x]$ hat alle sechs Elemente von $\mathfrak{Z}_6$ als Nullstellen.

Von vielfältigem praktischen Nutzen ist schließlich der

Satz 3: *Eine Nullstelle $\alpha \in \mathfrak{Q}$ des normierten Polynoms*

$$f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in \mathfrak{Z}[x]$$

ist eine ganze Zahl und Teiler von a_0.

Beweis: Ohne Beschränkung der Allgemeinheit sei $n \geqq 1$, $a_0 \neq 0$ und $\alpha = \frac{r}{s}$, $s \in \mathfrak{N}$, $r \in \mathfrak{Z}$, $(r, s) = 1$. Multiplikation von $f\left(\frac{r}{s}\right) = 0$ mit s^n liefert $r^n + a_{n-1}r^{n-1}s + \ldots + a_0 s^n = 0$ oder $r^n = ks$ mit einem $k \in \mathfrak{Z}$. Die natürliche Zahl s teilt r^n, hat aber keinen Primteiler mit r gemeinsam, muß also Eins sein. Daher ist α die ganze Zahl r, und aus $r(r^{n-1} + a_{n-1}r^{n-2} + \ldots + a_1) = -a_0$ ist zu sehen, daß a_0 durch r teilbar ist.

Als rationalzahlige Nullstellen des ganzzahligen normierten Polynoms $x^5 + x + 2$ kommen also nur ± 1 und ± 2 in Frage; demnach ist -1 die ein-

zige Nullstelle von $x^5 + x + 2$ in $\mathfrak{Q}$. Das Polynom $x^3 - x + 2$ hat überhaupt keine Nullstelle in $\mathfrak{Q}$.
Man sieht leicht, daß man Satz 3 auch zur Bestimmung der rationalzahligen Nullstellen nicht normierter ganzzahliger Polynome verwenden kann (Aufgabe 1). Daraus ergibt sich schließlich auch seine Anwendbarkeit bei der Suche nach allen rationalzahligen Nullstellen eines Polynoms $f(x) \in \mathfrak{Q}[x]$, das man ja nach Multiplikation mit dem Hauptnenner der Koeffizienten durch ein ganzzahliges Polynom ersetzen kann.

26.2 Im folgenden erklären wir in kommutativen Ringen mit Einselement eine formale Differentialrechnung.

Definition: *Es sei R ein kommutativer Ring mit Elementen $a, b, \ldots$ und $1 \in R$. Eine Abbildung $D\colon R \to R$ heißt eine Derivation oder Ableitung von R, wenn sie die beiden folgenden Bedingungen erfüllt:*
(1) $D(a + b) = D(a) + D(b)$,
(2) $D(ab) = aD(b) + bD(a)$.

Satz 4: *Es sei R ein kommutativer Ring mit Einselement und D eine Derivation von R. Dann ist $D(0) = D(1) = 0$, $D(-a) = -D(a)$, und für jedes $a \in R$ und jedes $n \in \mathfrak{N}$ gilt $D(a^n) = na^{n-1}D(a)$.*

Beweis: Aus $D(0) = D(0 + 0) = D(0) + D(0)$ folgt $D(0) = 0$. Ferner wird $D(1) = D(1 \cdot 1) = 1 \cdot D(1) + 1 \cdot D(1) = D(1) + D(1)$, also $D(1) = 0$. Es ist $0 = D(0) = D(a + (-a)) = D(a) + D(-a)$ und damit $D(-a) = -D(a)$. Die letzte Behauptung ergibt sich durch vollständige Induktion nach n.
Für Polynomringe betrachten wir nun eine spezielle, bereits aus der Analysis bekannte Ableitung.

Satz 5: *Es sei R ein kommutativer Ring mit Einselement und $R[x]$ der Polynomring in einer Unbestimmten x über R. Dann wird durch*

$$D(f(x)) = D(\sum_{\nu=0}^{n} a_\nu x^\nu) = \sum_{\nu=1}^{n} \nu a_\nu x^{\nu-1} =_{Df} f'(x)$$

eine Ableitung $D\colon R[x] \to R[x]$ definiert.

Beweis: Sofort zu sehen ist $D(f + g) = D(f) + D(g)$. Ferner gilt

$$D(a_\lambda x^\lambda \cdot b_\nu x^\nu) = D(a_\lambda b_\nu x^{\lambda+\nu}) = (\lambda + \nu) a_\lambda b_\nu x^{\lambda+\nu-1} = a_\lambda x^\lambda D(b_\nu x^\nu) + b_\nu x^\nu D(a_\lambda x^\lambda).$$

Zusammen mit (1) folgt hieraus noch

$$\begin{aligned} D(fg) &= D(\sum_{0}^{m} a_\lambda x^\lambda \cdot \sum_{0}^{n} b_\nu x^\nu) = D(\sum_{\lambda,\nu} a_\lambda x^\lambda \cdot b_\nu x^\nu) = \sum_{\lambda,\nu} D(a_\lambda x^\lambda \cdot b_\nu x^\nu) \\ &= \sum_{\lambda,\nu} a_\lambda x^\lambda D(b_\nu x^\nu) + \sum_{\lambda,\nu} b_\nu x^\nu D(a_\lambda x^\lambda) = \sum_{\lambda} a_\lambda x^\lambda D(\sum_{\nu} b_\nu x^\nu) + \sum_{\nu} b_\nu x^\nu D(\sum_{\lambda} a_\lambda x^\lambda) \end{aligned}$$

oder $D(fg) = fD(g) + gD(f)$, also (2).
Der folgende Satz wird oft gebraucht.

Satz 6: *Es sei I ein Integritätsbereich mit Einselement und n eine natürliche Zahl. Dann gelten die folgenden Aussagen.*

a) *Hat $f(x) \in I[x]$ die genau n-fache Nullstelle $\alpha \in I$, so hat entweder $f'(x)$ die mindestens $(n-1)$-fache Nullstelle $\alpha \in I$, oder $f'(x)$ ist das Nullpolynom. Ist zusätzlich die Charakteristik $\chi(I) = 0$, so hat $f'(x)$ die genau $(n-1)$-fache Nullstelle α.*
b) *Ist $f(x) \in I[x]$, $f(x) \neq 0$, $\alpha \in I$ und $f(\alpha) = f'(\alpha) = 0$, so ist α mindestens zweifache Nullstelle von $f(x)$.*

Beweis:
a) Unsere Voraussetzung ist $f(x) = (x-\alpha)^n q(x)$, $q(x) \in I[x]$, $q(\alpha) \neq 0$. Für eine beliebige Derivation $D: I[x] \to I[x]$ liefern (2) und die letzte Aussage von Satz 4

$$\begin{aligned} D(f(x)) &= (x-\alpha)^n D(q(x)) + q(x)D((x-\alpha)^n) \\ &= (x-\alpha)^n D(q(x)) + n(x-\alpha)^{n-1} q(x) D(x-\alpha); \end{aligned}$$

nach Satz 5 wird also speziell

$$f'(x) = (x-\alpha)^{n-1}[(x-\alpha)q'(x) + nq(x)].$$

Hieraus folgen die aufgestellten Behauptungen. Für $\chi(I) = 0$ ist ja $nq(\alpha) \neq 0$, und die eckige Klammer kann dann an der Stelle α nicht verschwinden.
b) Aus $f(x) = (x-\alpha)q(x)$, $q(x) \in I[x]$, folgt $f'(x) = (x-\alpha)q'(x) + q(x)$. Das liefert mit $f'(\alpha) = 0$ auch $q(\alpha) = 0$ und somit $q(x) = (x-\alpha)g(x)$, $g(x) \in I[x]$. Also wird $f(x) = (x-\alpha)^2 g(x)$.

Folgerung: Die Nullstelle $\alpha \in I$ von $f(x) \in I[x]$ ist genau dann einfach, wenn $f'(\alpha) \neq 0$ ist.

Aufgabe 1: Man bestimme alle rationalzahligen Nullstellen von
a) $x^5 - 2x^4 + 3x^3 - 6x^2 + 2x - 4$,
b) $3x^3 - 2x^2 + 6x - 4$,
c) $\frac{16}{3}x^5 - x^3 + x^2 + 2x - 7$.

Aufgabe 2: Es sei p eine Primzahl. Zeige: In $\mathfrak{Z}_p[x]$ gilt

$$x^p - x = \prod_{a \in \mathfrak{Z}_p} (x-a).$$

Wie folgt daraus die Wilsonsche Kongruenz (Satz 20.6)?

Aufgabe 3: Auf dem Integritätsbereich I sei eine Ableitung D definiert. Man zeige, daß sich D auf genau eine Weise auf den Quotientenkörper Q von I fortsetzen läßt: Es gibt genau eine Ableitung D^* von Q mit $D^*(a) = D(a)$ für jedes $a \in I$.

Aufgabe 4: Es sei p eine Primzahl. Man zeige: Die Kongruenz

$$a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0 \equiv 0 \bmod p \qquad (a_i \in \mathfrak{Z},\ p \nmid a_n)$$

hat höchstens n modulo p inkongruente Lösungen $x \in \mathfrak{Z}$.

Aufgabe 5: Ist $\alpha = a + bi \in \mathbb{C}$ $(a, b \in \mathfrak{R})$ Nullstelle des Polynoms $f(x) \in \mathfrak{R}[x]$ mit reellen Koeffizienten, so auch die konjugiert-komplexe Zahl $\bar{\alpha} = a - bi$. Beweis?

§ 27 Körpererweiterungen

27.1 Wir beginnen mit der

Definition: *Es sei K ein Körper. Eine Körpererweiterung oder ein Erweiterungskörper E von K ist ein Oberkörper $E \supset K$ von K.*

Es sei nun E eine Körpererweiterung von K. Dann gibt es in E und in K je ein Einselement, und diese Einselemente sind identisch, weil E ein Integritätsbereich ist (§ 25.1). Also ist auch $K[x]$ ein Unterring von $E[x]$ (§ 25.3).

Definition: *Es sei E eine Körpererweiterung von K und α ein Element von E. Wenn es ein vom Nullpolynom verschiedenes $f(x) \in K[x]$ mit $f(\alpha) = 0$ gibt, so heißt α algebraisch über K, andernfalls transzendent über K.*

Hiernach ist also eine Größe α genau dann algebraisch über dem Körper K, wenn zweierlei gilt: Es gibt einen Erweiterungskörper E von K, der α enthält, und es existiert ein $f(x) \in K[x]$, $f(x) \neq 0$, mit α als Nullstelle. Speziell ist jedes $\alpha \in K$ algebraisch über K. Die Zahlen $\sqrt{2}$ und i sind algebraisch über $\mathfrak{Q}$.
Nach § 25.2 können wir ferner sagen: Ist α transzendent (*Transzendente*) über K, so ist α eine Unbestimmte über K. Hiervon gilt auch die Umkehrung, weil eine Unbestimmte x über K Element des Quotientenkörpers E von $K[x]$ und E eine Körpererweiterung von K ist. Eine Transzendente über einem Körper K ist also dasselbe wie eine Unbestimmte über K.

27.2 Wir verabreden nun eine ständig auftretende Schreibweise.

Definition: *Es seien I und $I^* \supset I$ Integritätsbereiche mit demselben Einselement und $\alpha_1, \alpha_2, \ldots, \alpha_n$ Elemente aus I^*. Dann bezeichnen wir den Quotientenkörper von $I[\alpha_1, \alpha_2, \ldots, \alpha_n]$ mit $I(\alpha_1, \alpha_2, \ldots, \alpha_n)$.*

Wir bemerken dazu, daß $I[\alpha_1, \alpha_2, \ldots, \alpha_n] \subset I^*$ ein Integritätsbereich ist; der Körper $I(\alpha_1, \alpha_2, \ldots, \alpha_n)$ existiert also. Er besteht aus allen Brüchen $\frac{f}{g}$ mit $f, g \in I[\alpha_1, \alpha_2, \ldots, \alpha_n]$, $g \neq 0$. Speziell können die α_i unabhängige Unbestimmte über I sein.
Den Übergang von I zu $I[\alpha_1, \alpha_2, \ldots, \alpha_n]$ bezeichnet man als *Ringadjunktion*, den von I zu $I(\alpha_1, \alpha_2, \ldots, \alpha_n)$ als *Körperadjunktion* von $\alpha_1, \alpha_2, \ldots, \alpha_n$. Ersichtlich ist $I(\alpha_1, \alpha_2, \ldots, \alpha_n)$ der kleinste Körper, der I und die Elemente $\alpha_1, \alpha_2, \ldots, \alpha_n$ enthält; deshalb sagt man auch, er werde über I von den Elementen $\alpha_1, \alpha_2, \ldots, \alpha_n$ *erzeugt*. Aus den folgenden Beispielen sieht man unter anderem, daß Ringadjunktion und Körperadjunktion zu demselben Ergebnis führen können.

Beispiel 1. Es sei x eine Unbestimmte über dem Körper K. Dann gilt $K[x] \subset K(x)$, aber $K[x] \neq K(x)$; denn $x \in K[x]$ besitzt in $K[x]$ kein Inverses.

Beispiel 2. Es ist $\mathfrak{Q}[\sqrt{2}] = \mathfrak{Q}(\sqrt{2})$ (vgl. § 25.1 und § 20.3, Beispiel 6). Analog gilt $\mathfrak{Q}[\sqrt{3}] = \mathfrak{Q}(\sqrt{3})$, $\mathfrak{Q}[i] = \mathfrak{Q}(i)$, $\mathfrak{R}[i] = \mathfrak{R}(i) = \mathfrak{C}$.

Beispiel 3. Wir zeigen $\mathfrak{Q}(\sqrt{2}, \sqrt{3}) = \mathfrak{Q}(\sqrt{2} + \sqrt{3})$. Zunächst ist $\mathfrak{Q}(\sqrt{2} + \sqrt{3})$ der kleinste Körper, der $\mathfrak{Q}$ und $\sqrt{2} + \sqrt{3}$ enthält; da auch der Körper $\mathfrak{Q}(\sqrt{2}, \sqrt{3})$

das Element $\sqrt{2} + \sqrt{3}$ und ganz $\mathfrak{Q}$ enthält, folgt $\mathfrak{Q}(\sqrt{2}, \sqrt{3}) \supset \mathfrak{Q}(\sqrt{2} + \sqrt{3})$. Umgekehrt ist $\mathfrak{Q}(\sqrt{2}, \sqrt{3})$ der kleinste Körper, der $\mathfrak{Q}$ und die Elemente $\sqrt{2}, \sqrt{3}$ enthält. Wenn wir nachweisen können, daß $\sqrt{2}$ und $\sqrt{3}$ Elemente von $\mathfrak{Q}(\sqrt{2} + \sqrt{3})$ sind, so folgt entsprechend $\mathfrak{Q}(\sqrt{2}, \sqrt{3}) \subset \mathfrak{Q}(\sqrt{2} + \sqrt{3})$ und damit insgesamt die behauptete Gleichheit. Es gilt aber $(\sqrt{2} + \sqrt{3})^2 = 5 + 2\sqrt{6} \in \mathfrak{Q}(\sqrt{2} + \sqrt{3})$, also auch $\sqrt{6} \in \mathfrak{Q}(\sqrt{2}+\sqrt{3})$ und folglich $\sqrt{6}(\sqrt{2}+\sqrt{3}) = 3\sqrt{2}+2\sqrt{3} \in \mathfrak{Q}(\sqrt{2}+\sqrt{3})$; Subtraktion von $2(\sqrt{2} + \sqrt{3}) \in \mathfrak{Q}(\sqrt{2} + \sqrt{3})$ zeigt $\sqrt{2} \in \mathfrak{Q}(\sqrt{2} + \sqrt{3})$, und damit wird zuletzt auch $(\sqrt{2} + \sqrt{3}) - \sqrt{2} = \sqrt{3} \in \mathfrak{Q}(\sqrt{2} + \sqrt{3})$.

Später wird sich zeigen: Ist α algebraisch über K, so gilt $K[\alpha] = K(\alpha)$ (§ 53). In Beispiel 2 sind einige einfache Spezialfälle dieser Aussage notiert. In Beispiel 3 hat sich gezeigt, daß eine von zwei Elementen erzeugte Erweiterung auch von einem einzigen Element erzeugt werden konnte. Auch hierauf kommen wir noch zurück (§ 61).
Im Anschluß an die oben gegebene Definition machen wir schließlich noch eine Bemerkung: Ist Q der Quotientenkörper von I, so gilt $I(\alpha_1, \alpha_2, \ldots, \alpha_n) = Q(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Die Elemente rechter Hand sind ja Quotienten von Polynomen in den α_i mit Koeffizienten aus Q; erweitert man mit dem Hauptnenner aller dieser Koeffizienten, so ergeben sich Elemente aus $I(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Also ist $Q(\alpha_1, \alpha_2, \ldots, \alpha_n) \subset I(\alpha_1, \alpha_2, \ldots, \alpha_n)$, und die umgekehrte Enthaltenseinsbeziehung folgt aus $Q \supset I$.

27.3 Im folgenden betrachten wir ein Element α, das algebraisch über einem Körper K ist.

Satz 1: *Es sei α algebraisch über K. Dann existiert ein Polynom $f(x) \in K[x]$ mit folgenden Eigenschaften.*
(1) $f(x)$ ist normiert.
(2) Es ist $f(\alpha) = 0$.
(3) Ist $g(x) \in K[x]$ und Grad $g(x) <$ Grad $f(x)$, *so gilt $g(\alpha) \neq 0$.*
(4) Hat $f^*(x) \in K[x]$ die Eigenschaften (1), (2), (3), *so gilt $f^*(x) = f(x)$.*

Beweis: Die Menge der vom Nullpolynom verschiedenen Polynome aus $K[x]$ mit α als Nullstelle ist nach Definition von α nicht leer. Unter ihnen gibt es ein Polynom $h(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$, $a_n \neq 0$, kleinsten Grades $n > 0$, so daß für jedes $g(x) \in K[x]$ mit Grad $g(x) <$ Grad $h(x)$ gilt: $g(\alpha) \neq 0$. Das Polynom $f(x) = \frac{1}{a_n} h(x) \in K[x]$ hat dann, weil $h(\alpha) = 0$ war, die Eigenschaften (1), (2), (3). Schließlich hat das Polynom $d(x) = f(x) - f^*(x)$ auch die Nullstelle α; einen kleineren Grad als $f(x)$ kann es nach (3) nicht haben; andrerseits hat $d(x)$ keinen Grad größer oder gleich n, weil $f(x)$ und $f^*(x)$ normierte Polynome vom Grad n sind; also ist $d(x)$ das Nullpolynom (das nach unserer Definition aus § 25.4 keinen Grad hat), und es folgt $f^*(x) = f(x)$.
Die Eindeutigkeitsaussage (4) berechtigt zu der folgenden

Definition: *Es sei α algebraisch über dem Körper K. Dann heißt das Polynom $f(x)$ aus Satz 1 das Minimalpolynom oder das definierende Polynom von α über K.*

Weiter setzen wir das Folgende fest.

Definition: *Es sei I ein Integritätsbereich mit Einselement, $f(x) \in I[x]$ und* Grad $f(x) \geqq 1$. *Dann heißt $f(x)$ irreduzibel über I oder irreduzibel in $I[x]$, wenn aus $f(x) = g(x)h(x)$ mit $g(x), h(x) \in I[x]$ folgt: Entweder $g(x)$ oder $h(x)$ ist ein Element von I.*

Ein über I irreduzibles $f(x) \in I[x]$ läßt sich also höchstens durch Ausklammern eines Elementes aus I in Faktoren aus $I[x]$ zerlegen; andernfalls nennen wir $f(x)$ in $I[x]$ oder über I *reduzibel*. Von besonderem praktischen Interesse ist nun der

Satz 2: *Es sei α algebraisch über K. Dann gelten die folgenden Aussagen.*
a) *Das Minimalpolynom $f(x)$ von α über K ist irreduzibel in $K[x]$.*
b) *Hat das Polynom $P(x) \in K[x]$ die Eigenschaften (1), (2) und ist es in $K[x]$ irreduzibel, so ist es das Minimalpolynom $f(x)$ von α über K.*

Beweis:
a) Das Element α liegt in einem Erweiterungskörper E von K. Angenommen, es gäbe Polynome $g(x), h(x) \in K[x]$ mindestens vom Grad Eins mit $f(x) = g(x)h(x)$. Dann wird Satz 25.3 anwendbar; er liefert $g(\alpha)h(\alpha) = f(\alpha) = 0$. Das Produkt $g(\alpha)h(\alpha)$ ist in E nur Null, wenn einer der Faktoren verschwindet; da die Grade von $g(x)$ und $h(x)$ kleiner sind als Grad $f(x)$, liefert das einen Widerspruch zu (3).
b) Wir dividieren $P(x)$ mit Rest durch $f(x)$. Nach Satz 25.6 gibt es Polynome $q(x), r(x) \in K[x]$ mit

$$P(x) = q(x)f(x) + r(x),$$

wobei entweder Grad $r(x) <$ Grad $f(x)$ oder $r(x) = 0$ ist. Ersetzt man x durch α, so bekommt man $r(\alpha) = 0$; nach (3) muß also $r(x)$ das Nullpolynom sein. Da $f(x)$ mindestens den Grad Eins hat und $P(x)$ über K irreduzibel ist, muß weiter $q(x)$ ein Element von K sein. Schließlich sind $P(x)$ und $f(x)$ normiert; also ist sogar $q(x) = 1$ und damit $P(x) = f(x)$.
Dieser Satz gibt Veranlassung zu der

Definition: *Es sei α algebraisch über dem Körper K. Dann bezeichnen wir das Minimalpolynom $f(x) \in K[x]$ von α über K mit $f(x) =$ Irr (α, K). Wir sagen, α sei algebraisch vom Grad n über K, wenn* Grad Irr $(\alpha, K) = n$ *ist.*

Ist beispielsweise $\alpha \in K$, so wird Irr $(\alpha, K) = x - \alpha$; dann ist also α algebraisch vom Grad Eins über K. Zur Bestimmung von Minimalpolynomen stützt man sich in der Regel auf Satz 2. Wir betrachten einige einfache Beispiele.

Beispiel 4. Es sei $\alpha = \sqrt{2}$ und $K = \mathfrak{R}$. Dann gilt Irr $(\sqrt{2}, \mathfrak{R}) = x - \sqrt{2} \in \mathfrak{R}[x]$.

Beispiel 5. Es sei $\alpha = \sqrt{2}$ und $K = \mathfrak{Q}$. Das Polynom $P(x) = x^2 - 2 \in \mathfrak{Q}[x]$ hat dann die Eigenschaften (1), (2). Es ist ferner in $\mathfrak{Q}(x)$ irreduzibel. Um das zu zeigen, nehmen wir für den Augenblick das Gegenteil an. Dann gäbe es Polynome $g(x), h(x) \in \mathfrak{Q}[x]$ mit $P(x) = g(x)h(x)$ und Grad $g(x) = 1$, und wir dürfen ohne Beschränkung der Allgemeinheit zusätzlich annehmen, $g(x)$ sei bereits normiert: $g(x) = x - a$, $a \in \mathfrak{Q}$. Das ganzzahlige normierte Polynom $P(x) = x^2 - 2$ hätte demnach die Nullstelle $a \in \mathfrak{Q}$. Aus Satz 26.3 folgt sogar

$a \in \mathfrak{Z}$ und $a|2$; aber die Zahlen ± 1 und ± 2 sind keine Nullstellen von $x^2 - 2$. Die Annahme, $P(x)$ sei in $\mathfrak{Q}[x]$ reduzibel, war also falsch, und Satz 2 liefert nun $\mathrm{Irr}(\sqrt{2}, \mathfrak{Q}) = x^2 - 2$.

Beispiel 6. Nach dem Muster von Beispiel 5 sieht man ohne Rechnung $\mathrm{Irr}(\sqrt{3}, \mathfrak{Q}) = x^2 - 3$ und $\mathrm{Irr}(\sqrt[3]{2}, \mathfrak{Q}) = x^3 - 2$. Analog wird $\mathrm{Irr}(i, \mathfrak{Q}) = \mathrm{Irr}(i, \mathfrak{R}) = x^2 + 1$, weil $x^2 + 1$ keine reelle Nullstelle hat.

Beispiel 7. Es sei $\alpha = \frac{1}{\sqrt{2}}(1 + i)$ und $K = \mathfrak{Q}$. Wegen $\alpha^4 = -1$ hat das Polynom $P(x) = x^4 + 1 \in \mathfrak{Q}[x]$ die Eigenschaften (1), (2); wir behaupten $\mathrm{Irr}(\alpha, \mathfrak{Q}) = x^4 + 1$ und müssen dazu noch zeigen, daß $x^4 + 1$ irreduzibel über $\mathfrak{Q}$ ist. Wie in Beispiel 5 sieht man, daß $x^4 + 1$ keinen Faktor $g(x) \in \mathfrak{Q}[x]$ vom Grad Eins haben kann. Wir müssen also noch nachweisen, daß auch eine Zerlegung

$$x^4 + 1 = (x^2 + ax + b)(x^2 + cx + d) \qquad (a, b, c, d \in \mathfrak{Q})$$

in quadratische Faktoren aus $\mathfrak{Q}[x]$ unmöglich ist. Ausmultiplikation der Klammern rechter Hand und Koeffizientenvergleich ergibt zunächst $c = -a$ und, da $b \neq 0$ ist, $d = \frac{1}{b}$. Das führt weiter auf $a^2 = b + \frac{1}{b}$ und $\frac{a}{b} - ab = 0$ oder die möglichen Zerlegungen

$$\begin{aligned} x^4 + 1 &= (x^2 + i)(x^2 - i) \\ &= (x^2 + \sqrt{2}x + 1)(x^2 - \sqrt{2}x + 1) \\ &= (x^2 + i\sqrt{2}x - 1)(x^2 - i\sqrt{2}x - 1); \end{aligned}$$

doch die Faktoren liegen nicht in $\mathfrak{Q}[x]$. Also ist $x^4 + 1$ irreduzibel über $\mathfrak{Q}$ und $\mathrm{Irr}(\alpha, \mathfrak{Q}) = x^4 + 1$. Aber beispielsweise wird $x^4 + 1$ reduzibel über $\mathfrak{Q}(\sqrt{2})$ oder $\mathfrak{R}$ und $\mathrm{Irr}(\alpha, \mathfrak{Q}(\sqrt{2})) = \mathrm{Irr}(\alpha, \mathfrak{R}) = x^2 - \sqrt{2}x + 1$; die Zahl α ist also algebraisch vom Grad 4 über $\mathfrak{Q}$ und algebraisch vom Grad 2 über $\mathfrak{Q}(\sqrt{2})$ oder $\mathfrak{R}$.

27.4 Es fällt nicht leicht, ein $r \in \mathfrak{R}$ anzugeben, das transzendent über $\mathfrak{Q}$ ist. Gibt es derartige reelle Zahlen überhaupt? Diese Frage kann im Anschluß an den folgenden Satz beantwortet werden.

Satz 3: *Es sei R ein kommutativer Ring mit Einselement. Ist R abzählbar, so ist es auch der Polynomring $R[x]$.*

Beweis: Es sei R abzählbar und M_k die Menge aller Polynome $f(x) \in R[x]$ vom Grad k ($k \geqq 0$). Wir zeigen die Abzählbarkeit von $M = \bigcup_{k=0}^{\infty} M_k$; das ist $R[x]$ ohne das Nullpolynom. Nach Satz 4.2 genügt es zu zeigen, daß jedes M_k abzählbar ist. Bezeichnen wir wieder mit R_0 die Menge R ohne die Null, so läßt sich aber M_k eineindeutig auf $R_0 \times R \times R \times \ldots \times R$ ($k + 1$ Faktoren) abbilden, und dieses cartesische Produkt ist nach Satz 4.1 abzählbar, weil jeder der Faktoren es ist.

Als Beispiel betrachte man etwa den Fall $R = \mathfrak{Q}$: Die Menge aller Polynome mit rationalen Koeffizienten ist abzählbar.

Wir kommen nun auf die oben gestellte Frage zurück. Spricht man von transzendenten Zahlen schlechthin, so meint man in der Regel die reellen Zahlen r, die transzendent über $\mathfrak{Q}$ sind. Die Menge aller dieser Zahlen sei B, und es sei A die Menge aller über $\mathfrak{Q}$ algebraischen $r \in \mathfrak{R}$. Dann ist $A \cap B = \mathfrak{L}$ und $A \cup B = \mathfrak{R}$. Nun ist die Menge $\mathfrak{Q}[x]$ aller rationalzahligen Polynome abzählbar; jedes einzelne von ihnen hat nach der Bemerkung zu Satz 26.2 höchstens endlich viele, eventuell gar keine Nullstellen in $\mathfrak{R}$; die Menge A aller dieser Nullstellen ist demnach ebenfalls abzählbar. Da $\mathfrak{R} = A \cup B$ nicht abzählbar ist (§ 4), kann also B weder endlich noch abzählbar sein. Damit ist die Existenz überabzählbar vieler transzendenter Zahlen r nachgewiesen, ohne daß wir in der Lage sind, eine einzige von ihnen explizit anzugeben. Die Transzendenz etwa von e und π wird in der Zahlentheorie gezeigt.
Zuletzt notieren wir noch eine Konsequenz von Satz 3.

Satz 4: *Der Körper K sei höchstens abzählbar. Dann ist auch jede endlich erzeugte Erweiterung $K(\xi_1, \xi_2, \ldots, \xi_n)$ höchstens abzählbar.*

Beweis: Es genügt, $K(\xi_1, \xi_2, \ldots, \xi_n)$ abzuzählen unter der Annahme, K sei abzählbar und die Erzeugenden $\xi_1, \xi_2, \ldots, \xi_n$ seien unabhängige Unbestimmte über K. Mehrfache Anwendung von Satz 3 zeigt zunächst die Abzählbarkeit von $K[\xi_1, \xi_2, \ldots, \xi_n]$. Dann lassen sich aber nach dem Vorbild des Abzählbarkeitsbeweises für $\mathfrak{Q}$ auch die Elemente des Quotientenkörpers $K(\xi_1, \xi_2, \ldots, \xi_n)$ nach dem Paarschema abzählen (§ 4).

Aufgabe 1: Es sei K ein Körper. Man zeige: Mit α ist auch α^2 algebraisch über K und umgekehrt.

Aufgabe 2: Zeige, daß $\sqrt{2} + \sqrt{3} + \sqrt{5}$ algebraisch über $\mathfrak{Q}$ ist.

Aufgabe 3: Es sei d eine ganze Zahl. Man zeige:
a) Es ist $\mathfrak{Q}[\sqrt{d}] = \mathfrak{Q}(\sqrt{d})$.
b) Ist $\sqrt{d} \notin \mathfrak{Q}$, so wird durch $\varphi(a + b\sqrt{d}) = a - b\sqrt{d}$ ein Automorphismus φ von $\mathfrak{Q}(\sqrt{d})$ definiert $(a, b \in \mathfrak{Q})$.

Aufgabe 4: Es sei d eine ganze Zahl. Man zeige: Die Menge G aller von Null verschiedenen Zahlen der Gestalt $x^2 + dy^2$ $(x, y \in \mathfrak{Q})$ ist eine multiplikative Untergruppe von $\mathfrak{Q}_0$.

Aufgabe 5: Man zeige:
a) Es ist $\mathfrak{Q}(\sqrt{2}, \sqrt{3}) = \mathfrak{Q}[\sqrt{2}, \sqrt{3}]$.
b) Der Körper $\mathfrak{Q}(\sqrt{2}, \sqrt{3})$ besteht aus allen reellen Zahlen der Gestalt

$$a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \qquad (a, b, c, d \in \mathfrak{Q}).$$

Aufgabe 6: Man gebe fünf Zwischenkörper K mit $\mathfrak{Q} \subset K \subset \mathfrak{Q}(\sqrt{2} + \sqrt{3})$ an.

Aufgabe 7: Man bestimme
a) $\mathrm{Irr}(3 + \sqrt{3}, \mathfrak{Q})$,
b) $\mathrm{Irr}(3 - \sqrt{3}, \mathfrak{Q})$,
c) $\mathrm{Irr}(\sqrt{2} + \sqrt{3}, \mathfrak{Q})$,

d) $\mathrm{Irr}(\sqrt[4]{2}+1, \mathbb{Q})$,
e) $\mathrm{Irr}(\sqrt[4]{2}+1, \mathbb{Q}(\sqrt{2}))$.

Aufgabe 8: Man löse noch einmal den Teil b) von Aufgabe 20.9.

Aufgabe 9: Für welche $a \in \mathbb{Z}$ ist $x^4 + ax^2 + 1$ reduzibel über $\mathbb{Q}$?

§ 28* Halbgruppenringe

28.1 Für das Folgende erinnern wir uns wieder an die Einführung des Ringes $R[x]$ aller Polynome in einer Unbestimmten x über dem kommutativen Ring R mit dem Einselement 1. In anderer Formulierung lautet Satz 25.1: Es seien ein kommutativer Ring R mit dem Einselement 1 und eine multiplikativ geschriebene Halbgruppe der Gestalt $H = \{e, x, x^2, x^3, \dots\}$ mit dem Einselement e vorgelegt. Dann gibt es einen eindeutig bestimmten kleinsten Oberring $R[H]$ von R, der auch H als Teilstruktur und wiederum 1 als Einselement enthält und in dem die Rechenregeln

$$(1) \qquad r_1h_1 + r_2h_2 + \dots + r_mh_m = 0 \Leftrightarrow r_1 = r_2 = \dots = r_m = 0 \quad (r_\nu \in R,\ h_\nu \in H,\ h_i \neq h_j \text{ für } i \neq j),$$

$$(2) \qquad rh = hr \text{ für alle } r \in R,\ h \in H$$

erfüllt sind.

Es ist nämlich $R[H] = R[x]$. Das Element e von H findet sich in $R[x]$ in der Gestalt 1, und die Bedingungen (1), (2) stehen an Stelle der Bedingungen (3), (5) aus § 25. Die Bedingung (4) aus § 25 steckt bereits in der Forderung, daß R und $R[H]$ dasselbe Einselement haben sollen. Die Bezeichnung $R[H]$ soll andeuten: Man hat ganz H zu R adjungiert.

Es seien nun wieder R ein kommutativer Ring mit dem Einselement 1 und diesmal H eine beliebige multiplikativ geschriebene Halbgruppe mit dem Einselement e. Unsere Frage lautet: Gibt es auch unter diesen schwächeren Voraussetzungen über H einen kleinsten Oberring von R, der H als Teilstruktur und 1 als Einselement enthält und in dem gemäß (1) und (2) gerechnet wird? Wenn wir sie mit ja beantworten und zeigen können, daß dieser Oberring eindeutig bestimmt ist, so dürfen wir ihn etwa mit $R[H]$ bezeichnen; er heißt der von R und H erzeugte *Halbgruppenring*.

Wie früher bei ähnlichen Fragestellungen (vgl. etwa § 13) wollen wir zunächst annehmen, daß es wenigstens einen Oberring S von R mit dem Einselement 1 gibt, der H als Teilstruktur enthält und in dem die Bedingungen (1), (2) erfüllt sind. Wir betrachten dann die Teilmenge $T \subset S$ aller endlichen Summen der Gestalt $r_1h_1 + r_2h_2 + \dots + r_mh_m$ ($r_\nu \in R$, $h_\nu \in H$, $h_i \neq h_j$ für $i \neq j$) und zeigen, daß T ein Unterring von S ist. Wählen wir zwei Elemente aus T, so können wir annehmen, daß sie aus denselben h_i zusammengesetzt sind; durch Hinzufügen endlich vieler Summanden der Gestalt $0h_i$ läßt sich das immer erreichen. Aus

$$(3) \qquad \begin{aligned}(r_1h_1 + r_2h_2 + \dots + r_mh_m) + (r'_1h_1 + r'_2h_2 + \dots + r'_mh_m)\\ = (r_1 + r'_1)h_1 + (r_2 + r'_2)h_2 + \dots + (r_m + r'_m)h_m\end{aligned}$$

ist nun zu sehen, daß T bezüglich der Addition eine abelsche Gruppe ist; sie hat das Nullelement $0e$, und das additive Inverse von $r_1h_1+r_2h_2+\ldots+r_mh_m\in T$ ist $(-r_1)h_1+(-r_2)h_2+\ldots+(-r_m)h_m$. Auch das Produkt zweier Elemente von T wird auf Grund von (2) wieder ein Element von T. Wir bekommen

$$(4a)\quad (r_1h_1+r_2h_2+\ldots+r_mh_m)(r_1'h_1+r_2'h_2+\ldots+r_m'h_m)=\sum_{h\in M} r(h)h:$$

hierin ist M die Menge aller Produkte h_ih_j und

$$(4b)\qquad r(h)=\sum r_i'r_j',$$

wobei über alle Indexpaare (i, j) summiert wird, für die $h_ih_j=h$ ist. Das Assoziativgesetz der Multiplikation und die Distributivgesetze gelten in S, also erst recht in T.

Der Ring T besteht aus allen endlichen Summen der Gestalt

$$(5)\qquad r_1h_1+r_2h_2+\ldots+r_mh_m\qquad (r_\nu\in R,\ h_\nu\in H,\ h_i\neq h_j \text{ für } i\neq j).$$

Wählt man $m=1$ und $r_1=1$, so sieht man $T\supset H$. Für $m=1$ und $h_1=e$ bekommt man eine Teilmenge R^* von T, von der man sofort sieht, daß sie ein isomorphes Bild des Ringes R ist; wir dürfen deshalb nach einer Ersetzung von R^* durch R auch sagen: $T\supset R$. Ist andrerseits $U\subset S$ ein Unterring von S, der H und R umfaßt, so muß er alle Elemente der Gestalt rh $(r\in R,\ h\in H)$ und damit auch alle Summen (5) enthalten: $T\subset U$. In S ist also T der kleinste Unterring, der R und H enthält; die Eins aus R ist Einselement auch von T.

Wären wir statt von S von einem anderen Oberring S^* von R ausgegangen, in dem die Bedingungen (1), (2) erfüllt sind und der 1 als Einselement und H als Teilstruktur enthält, so würde für den analog T erklärten Unterring T^* von S gelten: $T^*=T$. Dabei benutzt man (1) in der Form

$$(6)\quad r_1h_1+r_2h_2+\ldots+r_mh_m=r_1'h_1+r_2'h_2+\ldots+r_m'h_m \Leftrightarrow r_\nu=r_\nu' \ (\nu=1,2,\ldots,m).$$

Wüßten wir also die Existenz von T (oder auch nur die von S), so wäre alles bewiesen, und wir könnten sagen: Dies ist der eindeutig bestimmte kleinste Oberring $R[H]$ von R mit 1 als Einselement und H als Teilstruktur, in dem die Rechenregeln (1) und (2) gelten. Wegen der Gestalt (5) der Elemente von $R[H]$ nennt man $R[H]$ auch den *Halbgruppenring über H mit Koeffizienten aus R.*

Satz 1: *Es sei R ein kommutativer Ring mit dem Einselement 1 und H eine multiplikativ geschriebene Halbgruppe mit dem Einselement e. Dann existiert der Halbgruppenring $R[H]$. Er umfaßt R und H, enthält 1 als Einselement und besteht aus allen Elementen der Gestalt* (5). *Man rechnet in ihm nach den Regeln* (6), (3), (4).

Spezialfall: Ist H kommutativ, so ist $R[H]$ ein kommutativer Ring. Ist x eine Unbestimmte über R und $H=\{e, x, x^2, x^3, \ldots\}$, so gilt $R[H]=R[x]$.

Beweis von Satz 1: Wir konstruieren $R[H]=T$. Wir bemerken, daß sich das Konstruktionsverfahren aus dem Beweis von Satz 25.1 nicht übertragen läßt, da H nicht notwendig abzählbar zu sein braucht. Statt dessen gehen wir von einer gewissen Menge von Abbildungen $f: H\to R$ aus und haben dabei die Vorstellung, daß etwa dem Element $r_1h_1+r_2h_2+r_3h_3$ aus T

die Abbildung $f: H \to R$ mit $f(h_1) = r_1$, $f(h_2) = r_2$, $f(h_3) = r_3$ und $f(h) = 0$ für alle anderen $h \in H$ entsprechen möge. Es sei also A die Menge aller derjenigen Abbildungen $f: H \to R$, für die nur an endlich vielen Stellen $h \in H$ das Bild $f(h) \neq 0$ ist. Auf A erklären wir eine Addition und eine Multiplikation nach den Vorbildern (3) und (4). Es sei für $f, g \in A$

$$(3') \qquad (f + g)(h) = f(h) + g(h) \text{ für alle } h \in H;$$

auf diese Weise ist die Summe $f + g \in A$ erklärt, und A wird eine abelsche Gruppe bezüglich dieser Addition. Das Produkt von $f, g \in A$ im Sinn von § 3 ist gar nicht definiert; wir bezeichnen unser Produkt deshalb mit $f \circ g$ und erklären es durch

$$(4') \qquad (f \circ g)(h) = \sum f(h_i)g(h_j) \text{ für alle } h \in H,$$

wobei über alle diejenigen Indexpaare (i, j) summiert wird, für die $h_i h_j = h$ ist. Da $f(h_i)$ und $g(h_j)$ nur jeweils endlich oft ungleich Null sind, steht rechter Hand in (4') eine endliche Summe, also ein Element aus R; aus dem gleichen Grunde fällt außerdem diese Summe nur für endlich viele h von Null verschieden aus. Das Produkt $f \circ g$ der Elemente f, g von A liegt also wieder in A. Die so erklärte Multiplikation ist assoziativ, weil die Multiplikation in R es ist. Analog prüft man die Distributivgesetze nach. Also ist A ein Ring. Er enthält ein Einselement, nämlich die durch

$$\varepsilon(e) = 1, \ \varepsilon(h) = 0 \text{ für alle } h \in H, \ h \neq e$$

definierte Abbildung $\varepsilon \in A$.
Setzt man die Existenz des oben betrachteten Ringes T für den Augenblick voraus, so gilt gewiß $A \simeq T$. So haben wir die Konstruktion von A ja eingerichtet. Das bedeutet, daß wir nur noch die Schreibweise der Elemente von A ändern müssen, um $T = R[H]$ zu erhalten. Unser Beweis ist abgeschlossen.

28.2 Es sei wieder R ein kommutativer Ring mit Einselement. Beispiele für Halbgruppenringe sind dann etwa die Polynomringe $R[x]$, $R[x, y]$; zu $R[x, y]$ gehört die Halbgruppe H aller $x^m y^n$, $m \geqq 0$, $n \geqq 0$. Ein Halbgruppenring ist auch der Ring $R[x_1, x_2, x_3, \ldots]$ in abzählbar vielen unabhängigen Unbestimmten x_i über R.

§ 29* Der Quaternionenschiefkörper

29.1 Es sei G die Quaternionengruppe (vgl. § 18). Den in § 23 konstruierten komplexen Zahlkörper $\mathfrak{C} = \mathfrak{R}[i]$ könnte man auch wie folgt beschreiben: Er ist der eindeutig bestimmte kleinste Oberkörper von $\mathfrak{R}$, der auch das Element $i \in G$ enthält; dabei tritt als Verknüpfungsergebnis von i^2 die reelle Zahl —1 an die Stelle des Elementes $-1 \in G$.
Geht man von dieser etwas willkürlichen Deutung des Körpers $\mathfrak{C}$ aus, so kann man auch die Frage aufwerfen, ob man nicht in ähnlicher Weise die Elemente i, j, k aus G zu $\mathfrak{R}$ adjungieren kann. Zwar würde wegen $ij \neq ji$ die Multipli-

kation in der betreffenden Oberstruktur von $\mathfrak{R}$ nicht mehr kommutativ ausfallen; aber vielleicht ließe sich auf diese Weise der Körper $\mathfrak{R}$ der reellen Zahlen in einen Schiefkörper einbetten. Es ist etwas überraschend, daß dies in der Tat möglich ist. Die früher getroffene Wahl für die Bezeichnungen der Elemente von G erweist sich im folgenden noch einmal als besonders suggestiv. Wir nehmen zunächst wieder an, es gäbe einen Schiefkörper S, der $\mathfrak{R}$ als Teilstruktur und außerdem die Elemente $i, j, k \in G$ enthält. Etwa die Multiplikationsvorschriften $i^2 = -1$ und $ik = -j$ bedeuten in S: Es ist i^2 das additive Inverse von $1 \in S$ und ik das additive Inverse von $j \in S$. Die Einselemente von S und $\mathfrak{R}$ stimmen nach § 25.1 von selbst überein. In Analogie zu § 28, (2), möge für die Multiplikation in S außerdem noch

$$rs = sr \text{ für alle } r \in \mathfrak{R},\ s \in S \tag{1}$$

gelten. In S betrachten wir nun die Teilmenge T aller Elemente der Gestalt

$$a + bi + cj + dk \qquad (a, b, c, d \in \mathfrak{R};\ i, j, k \in G). \tag{2}$$

Die Formel

$$\begin{aligned}(a_1 + a_2 i + a_3 j + a_4 k) + (b_1 + b_2 i + b_3 j + b_4 k)\\ = (a_1 + b_1) + (a_2 + b_2)i + (a_3 + b_3)j + (a_4 + b_4)k\end{aligned} \tag{3}$$

für die Summe zweier Elemente aus T zeigt, daß T eine abelsche Gruppe bezüglich der Addition ist. Die Multiplikation zweier Elemente von T führt wegen (1) auf

$$\begin{aligned}(a + bi + cj + dk)(s + ti + uj + vk) = {} & (as - bt - cu - dv)\\ & + (at + bs + cv - du)i\\ & + (au + cs + dt - bv)j\\ & + (av + ds + bu - ct)k.\end{aligned} \tag{4}$$

Also ist T ein Unterring von S mit dem Einselement 1. Das Assoziativgesetz der Multiplikation und die Distributivgesetze gelten in S und damit erst recht in T; sie lassen sich aber auch leicht direkt nachprüfen. Tut man das, so benutzt man beim assoziativen Gesetz die Assoziativität der Multiplikation in der Quaternionengruppe G.

Der durch die Gestalt (2) seiner Elemente eindeutig bestimmte Ring T umfaßt $\mathfrak{R}$ und die Elemente i, j, k aus G, und er ist der kleinste Ring dieser Art, in dem die Multiplikationsvorschrift (1) gilt. Wir zeigen, daß T sogar ein Schiefkörper ist. Dazu sei $\alpha = a + bi + cj + dk$ ein Element aus T, dessen Koeffizienten a, b, c, d nicht sämtlich verschwinden, und $\bar{\alpha} = a - bi - cj - dk$. Mit (4) folgt

$$\alpha\bar{\alpha} = \bar{\alpha}\alpha = a^2 + b^2 + c^2 + d^2 \neq 0;$$

also ist

$$\alpha^{-1} = \frac{1}{a^2 + b^2 + c^2 + d^2}\,\bar{\alpha} \in T$$

das Inverse des von Null verschiedenen Elements α von T. Der Nachweis, daß T ein Schiefkörper ist, ist erbracht. Außerdem folgt, daß α nur Null sein

kann, wenn alle Koeffizienten verschwinden; gleichwertig damit ist

$$a_1 + a_2 i + a_3 j + a_4 k = b_1 + b_2 i + b_3 j + b_4 k \Leftrightarrow a_\nu = b_\nu \quad (\nu = 1, 2, 3, 4;\ a_\nu, b_\nu \in \mathfrak{R}). \tag{5}$$

Wieder bleibt die Frage nach der Existenz der Struktur T, und wieder können wir auf eine uns inzwischen geläufige Weise eine bejahende Antwort geben. Wir bilden die Menge $M = \mathfrak{R}^4$ aller Quadrupel (a, b, c, d) mit Komponenten aus $\mathfrak{R}$, stellen uns unter ihnen die Elemente (2) vor und definieren eine Addition und eine Multiplikation auf M nach den Vorbildern (3) und (4). Eine Äquivalenzrelation brauchen wir wegen (5) auf M nicht einzuführen. Es folgt der Nachweis, daß M ein Schiefkörper ist; abgesehen von der Bezeichnung der Elemente handelt es sich um den zu konstruierenden Schiefkörper T. Wir führen die einzelnen Schritte, die nach dem in § 23 gegebenen Muster ablaufen, nicht mehr durch.

29.2 Diesen Schiefkörper, der aus allen Elementen der Gestalt (2) besteht und in dem nach den Regeln (3), (4) und (5) gerechnet wird, bezeichnen wir in Zukunft mit $\mathfrak{H}$; seine Elemente nennt man *Quaternionen*. Der Name Quaternionen stammt von dem englischen Mathematiker W. R. Hamilton (1805 — 1865); er hat sich ausführlich mit ihnen beschäftigt, nachdem schon Euler (1707—1783) mit ihnen gerechnet hatte. Der Quaternionenschiefkörper hat in verschiedenen Disziplinen der Mathematik eine gewisse Bedeutung erlangt; Anwendungen des Rechnens mit Quaternionen finden sich auch in der Mechanik (vgl. Blaschke [4]). Wir kommen im Rahmen der Algebra in § 55 noch einmal auf den Schiefkörper $\mathfrak{H}$ zurück, der dann eine interessante axiomatische Beschreibung erfährt.
Ist $\alpha = a + bi + cj + dk$ ein Element von $\mathfrak{H}$, so nennt man

$$\bar{\alpha} = a - bi - cj - dk \in \mathfrak{H}$$

die zu α *konjugierte Quaternion* und die reelle Zahl

$$N(\alpha) = \alpha\bar{\alpha} = a^2 + b^2 + c^2 + d^2$$

die *Norm* von α. Für sie gilt

$$N(\alpha)N(\beta) = N(\alpha\beta) \qquad (\alpha, \beta \in \mathfrak{H}). \tag{6}$$

Zum Beweis rechnen wir die linke Seite von (6) aus. Zunächst wird $N(\alpha)N(\beta) = (\alpha\bar{\alpha})(\beta\bar{\beta}) = \alpha(\beta\bar{\beta})\bar{\alpha} = (\alpha\beta)(\bar{\beta}\bar{\alpha})$; dabei wurde neben der Assoziativität der Multiplikation die Vertauschbarkeit der reellen Zahl $\beta\bar{\beta}$ mit $\bar{\alpha} \in \mathfrak{H}$ benutzt. Nun gilt weiter

$$\overline{\alpha\beta} = \bar{\beta}\bar{\alpha} \qquad (\alpha, \beta \in \mathfrak{H}), \tag{7}$$

wie man nach (4) feststellt. Also bekommen wir $N(\alpha)N(\beta) = \alpha\beta(\bar{\beta}\bar{\alpha}) = \alpha\beta\overline{\alpha\beta}$ $= N(\alpha\beta)$, wie es in (6) behauptet war.
Der Schiefkörper $\mathfrak{H}$ kann auch durch Adjunktion von $j \in G$ zu $\mathfrak{C}$ gewonnen werden. Dies sieht man, wenn man die Quaternion $\alpha = a + bi + cj + dk$ in

der Gestalt $\alpha = a + bi + (c + di)j = \alpha_1 + \alpha_2 j$ schreibt ($\alpha_\iota \in \mathbb{C}$, $j \notin \mathbb{C}$). Es gilt $\mathfrak{R} \subset \mathbb{C} \subset \mathfrak{H}$.

29.3 Ist K ein Körper, so gibt es nach Satz 26.2 höchstens zwei Elemente ξ in K mit der Eigenschaft $\xi^2 + 1 = 0$. Aber schon für den Quaternionenschiefkörper $\mathfrak{H}$, in dem $\pm i$, $\pm j$, $\pm k$ für ξ gewählt werden können, ist das nicht mehr richtig. Eben auf Grund von Satz 26.2 (vgl. auch § 23) ist es von vornherein unmöglich, ein $j \notin \mathbb{C}$ mit der Eigenschaft $j^2 = -1$ zu $\mathbb{C}$ zu adjungieren mit dem Ziel, einen Oberkörper von $\mathbb{C}$ zu erhalten. Man kann zwar $\mathfrak{H}$ als die Menge aller $\alpha_1 + \alpha_2 j$ ($\alpha_1, \alpha_2 \in \mathbb{C}$) auffassen, hat aber auf die Kommutativität der Multiplikation in $\mathfrak{H}$ verzichtet.
Als Beispiel für das Rechnen in $\mathfrak{H}$ zeigen wir noch die Existenz sogar unendlich vieler $\alpha \in \mathfrak{H}$ mit $\alpha^2 + 1 = 0$. Wird nämlich die Gleichung $a\xi^2 + b\xi + c = 0$ ($a, b, c \in \mathfrak{R}$) durch $\alpha \in \mathfrak{H}$ gelöst: $a\alpha^2 + b\alpha + c = 0$, so auch durch jede Quaternion $\beta\alpha\beta^{-1}$ ($\beta \in \mathfrak{H}$, $\beta \neq 0$); denn es gilt

$$\beta(a\alpha^2 + b\alpha + c)\beta^{-1} = a\beta\alpha^2\beta^{-1} + b\beta\alpha\beta^{-1} + c = a(\beta\alpha\beta^{-1})^2 + b(\beta\alpha\beta^{-1}) + c = 0.$$

Demnach ist etwa

$$(r + j)^{-1} i (r + j) = \frac{1}{r^2 + 1}(r - j) i (r + j) = \frac{r^2 - 1}{r^2 + 1} i + \frac{2r}{r^2 + 1} k$$

für jedes $r \in \mathfrak{R}$ eine Lösung der Gleichung $\xi^2 + 1 = 0$.

29.4 Wir betrachten für den Augenblick den Ring $\mathfrak{Z}[\sqrt{-d}]$, wobei d eine ganze Zahl und $\sqrt{-d} \notin \mathfrak{Z}$ sein soll. Ist $\alpha = a + b\sqrt{-d}$ ($a, b \in \mathfrak{Z}$) ein Element von $\mathfrak{Z}[\sqrt{-d}]$, so setzen wir $\bar{\alpha} = a - b\sqrt{-d}$ und bezeichnen die reelle Zahl $N(\alpha) = \alpha\bar{\alpha} = a^2 + db^2$ als die *Norm* von α. Auch für diese Norm gilt

$$N(\alpha)N(\beta) = N(\alpha\beta) \qquad (\alpha, \beta \in \mathfrak{Z}[\sqrt{-d}]). \tag{6'}$$

Um das nachzurechnen, beachten wir die Gültigkeit von

$$\overline{\alpha\beta} = \bar{\alpha}\,\bar{\beta} \qquad (\alpha, \beta \in \mathfrak{Z}[\sqrt{-d}]). \tag{7'}$$

Diese Beziehung rechnet man leicht direkt nach; sie gilt deswegen, weil wie in Aufgabe 27.3 durch $\varphi(\alpha) = \bar{\alpha}$ ein Automorphismus von $\mathfrak{Z}[\sqrt{-d}]$ definiert wird. Mit Hilfe von (7') wird dann $N(\alpha)N(\beta) = \alpha\bar{\alpha}\beta\bar{\beta} = \alpha\beta\bar{\alpha}\bar{\beta} = \alpha\beta\overline{\alpha\beta} = N(\alpha\beta)$, wie es in (6') behauptet war.
Schreibt man die Gleichung (6') mit $\alpha = a + b\sqrt{-d}$ und $\beta = s + t\sqrt{-d}$ aus ($a, b, s, t \in \mathfrak{Z}$), so lautet sie

$$(a^2 + db^2)(s^2 + dt^2) = (as - btd)^2 + d(at + bs)^2. \tag{8}$$

Das ist eine Identität, deren Gültigkeit man nachträglich für jeden kommutativen Ring bestätigt. Sie wird in der Zahlentheorie gebraucht (vgl. auch Aufgabe 27.4). Speziell beruht der Fall $d = 1$ auf dem Rechnen in $\mathfrak{Z}[i]$ oder $\mathbb{C}$.
Das Produkt von Zahlen der Form $x^2 + dy^2$ hat also wieder diese Gestalt. Eine

ähnliche Aussage liefert (6). Ausgeschrieben bekommt man nach (4) die Vierquadrateformel

$$\begin{aligned}(a^2+b^2+c^2+d^2)(s^2+t^2+u^2+v^2) = {} & (as-bt-cu-dv)^2 \\ & +(at+bs+cv-du)^2 \\ & +(au+cs+dt-bv)^2 \\ & +(av+ds+bu-ct)^2,\end{aligned}$$

die sich wieder in jedem kommutativen Ring als richtig erweist. Wenn man zeigen kann, und dies geschieht in der Zahlentheorie, daß sich jede Primzahl als Summe von vier Quadraten aus $\mathfrak{Z}$ schreiben läßt, so liefert die aufgeschriebene Formel den berühmten Satz von LAGRANGE (1736—1813), daß sich jedes Produkt von Primzahlen, also jede natürliche Zahl, als Summe von vier Quadraten aus $\mathfrak{Z}$ darstellen läßt.

§ 30* Duale Zahlen

Eine sogenannte *duale Zahl* hat die Gestalt $a + b\varepsilon$; dabei sind a, b reelle Zahlen, und es gilt $\varepsilon^2 = 0$:

(1) $a_1 + a_2\varepsilon = b_1 + b_2\varepsilon \Leftrightarrow a_\nu = b_\nu \qquad (\nu = 1, 2;\ a_\nu, b_\nu \in \mathfrak{R})$,

(2) $(a_1 + a_2\varepsilon) + (b_1 + b_2\varepsilon) = (a_1 + b_1) + (a_2 + b_2)\varepsilon$,

(3) $(a_1 + a_2\varepsilon) \cdot (b_1 + b_2\varepsilon) = a_1b_1 + (a_1b_2 + a_2b_1)\varepsilon$.

Diese Forderungen definieren den kommutativen Ring D der dualen Zahlen. Wir verzichten auf seine Konstruktion aus der Menge $M = \mathfrak{R}^2$ nach dem Vorbild von § 23.

Man sieht: Genau die Elemente der Gestalt $r\varepsilon$ ($r \in \mathfrak{R}$, $r \neq 0$) sind Nullteiler in D. Das Rechnen mit dualen Zahlen gestattet hübsche Anwendungen in der Geometrie, die auf den deutschen Mathematiker E. STUDY (1862—1930) zurückgehen (vgl. BLASCHKE [4]).

§ 31 Angeordnete Ringe

31.1 In den Ringen $\mathfrak{Z}, \mathfrak{Q}, \mathfrak{R}$ kann man sagen, ein gewisses Element sei positiv oder größer als ein anderes. Dieser Sachverhalt dient als Vorbild für die folgende

Definition: *Ein Ring $R \neq \{0\}$ mit Elementen $a, b, \ldots$ heißt angeordnet, wenn in R eine Relation $a > 0$ (lies: a größer Null, oder: a positiv) mit folgenden Eigenschaften erklärt ist:*

(1) Für jedes $a \in R$ gilt genau eine der Relationen $a > 0$, $a = 0$, $-a > 0$.

(2) Für $a > 0$, $b > 0$ gilt $a + b > 0$ und $ab > 0$.

Die Menge P aller positiven Elemente aus R heißt der *Positivbereich* von R. Eine Anordnung von R definiert also eine Partition $R = P \cup \{0\} \cup N$ von R; dabei ist N die Menge aller $r \in R$ mit $-r > 0$. Ist ein Ring R auf zwei Arten

angeordnet, so stimmen diese Anordnungen genau dann überein, wenn die zugehörigen Positivbereiche dieselben sind. Gleichheiten von Anordnungen werden so gezeigt.

Im Anschluß an die gegebene Definition treffen wir noch die folgenden weiteren Verabredungen. Es soll $a > b$ (a größer b) dasselbe heißen wie $a - b > 0$, und $a < b$ (a kleiner b) bedeute dasselbe wie $b > a$. An Stelle von $-r > 0$ können wir also auch $r < 0$ schreiben. Schließlich soll $a \geqq b$ bedeuten: Es ist entweder $a > b$ oder $a = b$. Entsprechend wird $a \leqq b$ erklärt. Für jedes Element r eines angeordneten Ringes R gilt also beispielsweise $r \geqq r$.

Sind a, b Elemente eines angeordneten Ringes R, so gilt nach (1) mindestens eine der Relationen $a \leqq b$ oder $b \leqq a$, und das gleichzeitige Bestehen von $a \leqq b$ und $b \leqq a$ ist gleichwertig mit $a = b$; aus $a \leqq b$ und $b \leqq c$, also $b - a \geqq 0$ und $c - b \geqq 0$, schließlich folgt vermöge (2) $(b - a) + (c - b) = c - a \geqq 0$ oder $a \leqq c$. Ein *angeordneter Ring* R ist also bezüglich der Relation $\leqq$ eine *geordnete Menge* (vgl. § 1.2).

Beispiele für angeordnete Ringe wurden schon genannt. Jeder Unterring eines angeordneten Ringes, etwa $\mathfrak{Q}[\sqrt{2}] \subset \mathfrak{R}$, ist angeordnet. Im allgemeinen sind für ein und denselben Ring R Anordnungen, wenn überhaupt, auf verschiedene Arten möglich. Man betrachte etwa $R = \mathfrak{Q}[x]$. Eine Anordnung von $\mathfrak{Q}[x]$ erhält man beispielsweise, wenn man jedes von Null verschiedene $f(x) \in \mathfrak{Q}[x]$ genau dann als positiv bezeichnet, wenn sein höchster Koeffizient ein positives Element von $\mathfrak{Q}$ ist. Eine ganz andere Anordnung von $\mathfrak{Q}[x]$ ergibt sich, wenn man ein $f(x) \neq 0$ genau dann positiv nennt, wenn $f(\pi)$ in $\mathfrak{R}$ positiv ist; beim Nachprüfen der Forderung (1) benutzt man, daß mit $f(x) \neq 0$ auch $f(\pi) \neq 0$ gilt, also die Transzendenz von π über $\mathfrak{Q}$.

Man kann aber auch leicht Ringe angeben, die sich nicht anordnen lassen. Man betrachte zunächst einen angeordneten Ring R und ein $r \in R$, $r \neq 0$; nach (1) gilt dann entweder $r > 0$ oder $-r > 0$, und beide Male liefert (2) $r^2 > 0$. Von Null verschiedene Quadrate sind also in angeordneten Ringen positiv. Ist speziell R ein angeordneter Ring mit Einselement, so folgt $1 = 1^2 > 0$ und $-1 < 0$. Eine Folge davon ist, daß beispielsweise $\mathfrak{C}$ nicht angeordnet werden kann; denn dazu müßte einerseits $1 > 0$ und andrerseits auch $-1 = i^2 > 0$ sein im Widerspruch zu (1).

Wir wenden uns nun dem Rechnen in angeordneten Ringen zu.

Satz 1: *Es sei R ein angeordneter Ring mit Elementen $a, b, c, d, \ldots$ Dann gelten die folgenden Regeln.*

a) *Aus $a > b$ und $c > d$ folgt $a + c > b + d$.*

b) *Aus $a > b$ und $c > 0$ folgt $ac > bc$ und $ca > cb$.*

c) *Ist R sogar ein Körper und $a > b > 0$, so folgt $b^{-1} > a^{-1} > 0$.*

Beweis:

a) Es ist $a - b > 0$, $c - d > 0$, nach (2) also $(a - b) + (c - d) = (a + c) - (b + d) > 0$ oder $a + c > b + d$.

b) Es ist $a - b > 0, c > 0$, nach (2) also $(a - b)c = ac - bc > 0$ oder $ac > bc$; analog wird $ca > cb$.

c) Man beachte, daß aus $c > 0$ auch $(c^{-1})^2 c = c^{-1} > 0$ folgt, und multipliziere $a > b > 0$ gemäß b) mit $a^{-1}b^{-1} > 0$.

Ist R ein angeordneter Ring, so definieren wir noch wie üblich den *Betrag* $|a|$ von $a \in R$; wir setzen $|a| = a$ für $a \geqq 0$ und $|a| = -a$ für $a < 0$. Es gelten dann die *Betragsrechenregeln* (Aufgabe 2)
(3) $|ab| = |a| \cdot |b|$,
(4) $|a + b| \leqq |a| + |b|$ (*Dreiecksungleichung*),
(5) $||a| - |b|| \leqq |a \pm b| \leqq |a| + |b|$.
Ziemlich evident ist ferner die Gültigkeit von

Satz 2: *Eine Anordnung eines Integritätsbereiches I läßt sich auf genau eine Weise zu einer Anordnung seines Quotientenkörpers Q fortsetzen.*

Beweis: Würde Q eine Anordnung gestatten, die auf der Teilstruktur $I \subset Q$ mit einer vorgegebenen Anordnung übereinstimmt, so müßte genau dann $\frac{a}{b} > 0$ sein ($a, b \in I$, $b \neq 0$), wenn $b^2 \cdot \frac{a}{b} = ab > 0$ in I ist; wenn es also eine Fortsetzung der Anordnung von I auf Q gibt, so nur diese. Ist aber

$$\frac{a}{b} > 0 \quad \Leftrightarrow \quad ab > 0$$

überhaupt eine Definition? Ja; denn aus $\frac{a}{b} = \frac{c}{d}$ oder $ad = bc$ folgt $abc^2 = a^2cd$; ist also ab positiv, so auch cd. Die gegebene Vorschrift definiert auch wirklich eine Anordnung auf Q: Die Forderung (1) ist erfüllt; aus $\frac{a}{c} > 0$ und $\frac{b}{c} > 0$ folgt $ac + bc = (a + b)c > 0$, also $\frac{a+b}{c} = \frac{a}{c} + \frac{b}{c} > 0$, und analog zeigt man $\frac{a}{c} \cdot \frac{b}{c} > 0$, insgesamt also (2). Und schließlich liegt eine Fortsetzung der Anordnung von I vor; ist nämlich $a \in I$ und a in I positiv, so ist es wegen $a = \frac{a^2}{a}$ positiv auch in Q.

Will man den Ring $\mathfrak{Z}$ anordnen, so muß $1 > 0$ und nach (2) auch $1 + 1 = 2 > 0$, $1 + 1 + 1 = 3 > 0$ usw. gelten; $\mathfrak{Z}$ und wegen Satz 2 dann auch $\mathfrak{Q}$ gestatten also nur die eine bereits bekannte Anordnung. Ist R ein angeordneter Ring, so enthält er ein Element $a > 0$, und nach (2) ist niemals $na = 0$ ($n \in \mathfrak{N}$); die Ringelemente a, $a + a$, $a + a + a$, ... sind daher paarweise voneinander verschieden. Ein angeordneter Ring R ist also unendlich. Ist speziell $1 \in R$, so ist $1 > 0$, und R enthält, wie man in Analogie zu Aufgabe 20.10a) zeigt, einen zu $\mathfrak{Z}$ isomorphen Unterring T aller $m1$, $m \in \mathfrak{Z}$. Es hat also einen Sinn zu sagen, $\mathfrak{Z}$ sei *der kleinste angeordnete Ring mit* einem *Einselement*. Jeder angeordnete Körper umfaßt also $\mathfrak{Z}$ und damit auch $\mathfrak{Q}$, und $\mathfrak{Q}$ läßt sich axiomatisch bis auf Isomorphien eindeutig beschreiben als *der kleinste angeordnete Körper*.

31.2 Sind $0 < a < b$ Elemente eines angeordneten Ringes, so ist es nicht gesagt, daß ein $n \in \mathfrak{N}$ derart existiert, daß $na > b$ wird. Ein einfaches Beispiel

dieser Art ist etwa $\mathfrak{Q}[x]$ mit der bereits erwähnten Anordnung, daß ein $f(x) \neq 0$ genau dann positiv sein soll, wenn der höchste Koeffizient es ist; es gilt dann $0 < 1 < x$ und $n \cdot 1 < x$ für jedes $n \in \mathfrak{N}$. Solche Möglichkeiten werden in der folgenden Definition ausgeschlossen.

Definition: *Ein angeordneter Ring R mit Elementen $a, b, \ldots$ heißt archimedisch angeordnet, wenn aus $0 < a < b$ folgt: Es gibt ein $n \in \mathfrak{N}$ mit $na > b$.*

Archimedisch angeordnete Ringe sind etwa $\mathfrak{Z}$, $\mathfrak{Q}$, $\mathfrak{Q}[\sqrt{2}]$, $\mathfrak{R}$.
Es gibt viele angeordnete Körper. Beispielsweise läßt sich der Polynomring $\mathfrak{R}[x]$ wie eben beschrieben anordnen, und diese Anordnung kann nach Satz 2 zu einer Anordnung des Oberkörpers $\mathfrak{R}(x)$ von $\mathfrak{R}$ fortgesetzt werden. Aber für archimedisch angeordnete Körper gilt bereits der Satz: Ein archimedisch angeordneter Körper K ist einem Unterkörper von $\mathfrak{R}$ isomorph. Wir wollen den Beweis, obwohl er nicht schwierig ist, hier nicht ausführen.

Aufgabe 1: Läßt sich $\mathfrak{Z}_7(x)$ anordnen?

Aufgabe 2: Man beweise die Betragsrechenregeln (3), (4), (5).

Aufgabe 3: Der Körper $\mathfrak{R}$ läßt sich nur auf eine Weise anordnen. Beweis?

Aufgabe 4: Man bestimme alle Automorphismen von $\mathfrak{Q}$ und $\mathfrak{R}$.

Aufgabe 5: Ein angeordneter Ring R ist nullteilerfrei. Beweis?

Aufgabe 6: Ein archimedisch angeordneter Ring R ist ein Integritätsbereich. Beweis?

§ 32* Der Körper $\mathfrak{R}$ der reellen Zahlen

32.1 Im Rahmen unserer bisher durchgeführten Überlegungen haben wir zwar das Rechnen in den Strukturen $\mathfrak{Z}$, $\mathfrak{Q}$, $\mathfrak{R}$, $\mathfrak{C}$ als bekannt vorausgesetzt; aber unter der Annahme der Gültigkeit lediglich von Satz 2.1 ergaben sich als Folge allgemeiner Sätze auch Existenznachweise für die Strukturen $\mathfrak{Z}$ und $\mathfrak{Q}$ (§ 13, § 22), und in § 23 wurde der Körper $\mathfrak{C}$ aus $\mathfrak{R}$ gewonnen. Als Lücke blieb noch der Nachweis der Existenz des Körpers $\mathfrak{R}$ der reellen Zahlen. Die Schließung dieser Lücke erfordert einen gewissen Aufwand und unterscheidet sich wesentlich von den früher geübten Konstruktionsverfahren.
Schon anschaulich vollzieht sich der Übergang von $\mathfrak{Q}$ zu $\mathfrak{R}$ anders als etwa der von $\mathfrak{Z}$ zu $\mathfrak{Q}$. Damals wurden die Lösungen der Gleichungen $ax = b$ ($a, b \in \mathfrak{Z}$; $a \neq 0$) zu $\mathfrak{Z}$ adjungiert. Diesmal kann man sich die Elemente von $\mathfrak{Q}$ auf der Zahlengeraden markiert denken und will erreichen, daß umgekehrt auch jedem Punkt dieser Geraden ein Element r des Erweiterungskörpers $\mathfrak{R} \supset \mathfrak{Q}$ entspricht. Es gibt mehrere Möglichkeiten, diese Vorstellung mathematisch zu realisieren. Methodisch am ergiebigsten ist ein Verfahren, das durch den Konvergenzbegriff aus der Analysis nahegelegt wird und über die bloße Konstruktion des reellen Zahlkörpers $\mathfrak{R}$ hinaus eine allgemeine Bedeutung besitzt.

Es geht unter anderem auf G. CANTOR (1845—1918) zurück und besteht, kurz gesagt, in folgendem. Eine Folge rationaler Zahlen a_i, für die das Cauchysche Konvergenzkriterium erfüllt ist, hat immer einen Limes $a \in \mathfrak{R}$; aber a braucht nicht in $\mathfrak{Q}$ zu liegen. Umgekehrt gibt es zu jedem $a \in \mathfrak{R}$ eine (Cauchy-)Folge rationaler a_i mit a als Limes. Wir konstruieren nun $\mathfrak{R}$ als die Menge aller solcher Cauchy-Folgen aus rationalen a_i; zwei derartige Folgen werden äquivalent sein, wenn sie denselben Limes $a \in \mathfrak{R}$ haben. Dem wenden wir uns jetzt im einzelnen zu. Eine andere, für Beweiszwecke mitunter nützliche Konstruktion des Körpers $\mathfrak{R}$ durch sogenannte DEDEKINDsche Schnitte findet man etwa bei GRAUERT-LIEB [5].

32.2 Wir beginnen mit der

Definition: *Eine Folge* $(a_1, a_2, a_3, \ldots)$ *aus* $\mathfrak{Q}^\infty$ *heißt Cauchy-Folge, wenn zu jedem positiven* $\varepsilon \in \mathfrak{Q}$ *ein* $N(\varepsilon) \in \mathfrak{N}$ *derart existiert, daß* $|a_m - a_n| < \varepsilon$ *wird für* $m, n > N(\varepsilon)$. *Eine Folge* $(a_1, a_2, a_3, \ldots) \in \mathfrak{Q}^\infty$ *heißt Nullfolge, wenn zu jedem positiven* $\varepsilon \in \mathfrak{Q}$ *ein* $N_0(\varepsilon) \in \mathfrak{N}$ *derart existiert, daß* $|a_n| < \varepsilon$ *wird für* $n > N_0(\varepsilon)$.

Eine Nullfolge $(a_1, a_2, a_3, \ldots)$ ist also eine spezielle Cauchy-Folge; denn zu vorgegebenem $\varepsilon > 0$ aus $\mathfrak{Q}$ gelten für hinreichend große Indizes m, n die Ungleichungen $|a_m| < \frac{\varepsilon}{2}$ und $|a_n| < \frac{\varepsilon}{2}$, und aus ihnen folgt

$$|a_m - a_n| \leqq |a_m| + |a_n| < \varepsilon.$$

Eine Cauchy-Folge $(a_1, a_2, a_3, \ldots)$ ist beschränkt; das heißt, es gibt ein $q \in \mathfrak{Q}$ derart, daß $|a_n| \leqq q$ gilt für jeden Index n. Für $m, n > N(1)$ gilt ja $|a_m - a_n| < 1$, also für $m > N = N(1)$ die Abschätzung $|a_m| = |(a_m - a_{N+1}) + a_{N+1}| \leqq 1 + |a_{N+1}|$; man kann also $q = \mathrm{Max}(|a_1|, |a_2|, \ldots, |a_N|, 1 + |a_{N+1}|)$ setzen.

Es sei nun M die Menge aller Cauchy-Folgen aus $\mathfrak{Q}^\infty$; aus M konstruieren wir $\mathfrak{R}$. Elemente $(a_1, a_2, a_3, \ldots)$ und $(b_1, b_2, b_3, \ldots)$ aus M seien äquivalent, wenn $(a_1 - b_1, a_2 - b_2, a_3 - b_3, \ldots)$ eine Nullfolge ist. Man überzeugt sich, daß auf diese Weise wirklich eine Äquivalenzrelation auf M definiert wird. Ferner seien eine Addition und eine Multiplikation auf M durch

$$(a_1, a_2, a_3, \ldots) + (b_1, b_2, b_3, \ldots) = (a_1 + b_1, a_2 + b_2, a_3 + b_3, \ldots)$$

und

$$(a_1, a_2, a_3, \ldots) \cdot (b_1, b_2, b_3, \ldots) = (a_1 b_1, a_2 b_2, a_3 b_3, \ldots)$$

eingeführt; die rechten Seiten liegen wieder in M, was für die Summe aus

$$|(a_m + b_m) - (a_n + b_n)| = |(a_m - a_n) + (b_m - b_n)| \leqq |a_m - a_n| + |b_m - b_n|$$

und für das Produkt aus

$$\begin{aligned} |a_m b_m - a_n b_n| &= |a_m b_m - a_n b_m + a_n b_m - a_n b_n| \\ &= |b_m(a_m - a_n) + a_n(b_m - b_n)| \leqq |b_m| \cdot |a_m - a_n| + |a_n| \cdot |b_m - b_n| \end{aligned}$$

und der Beschränktheit der $|b_m|$ und $|a_n|$ folgt.
Ist unsere Äquivalenzrelation eine Kongruenzrelation ? Da wir mit den Klassen

rechnen wollen, müssen wir das nachprüfen. Für die Addition sieht man es sofort mit Hilfe der Dreiecksungleichung. Und sind

$(a_1, a_2, a_3, \ldots) \sim (a_1', a_2', a_3', \ldots)$ und $(b_1, b_2, b_3, \ldots) \sim (b_1', b_2', b_3', \ldots)$,

so wird auch $(a_1b_1, a_2b_2, a_3b_3, \ldots) \sim (a_1'b_1', a_2'b_2', a_3'b_3', \ldots)$ wegen

$|a_nb_n - a_n'b_n'| = |a_nb_n - a_n'b_n + a_n'b_n - a_n'b_n'| \leqq |b_n| \cdot |a_n - a_n'| + |a_n'| \cdot |b_n - b_n'|$,

was für hinreichend großes n kleiner als ein vorgegebenes $\varepsilon > 0$ aus $\mathfrak{Q}$ ausfällt. Es liegt also tatsächlich eine Kongruenzrelation vor.

Man sieht sofort, daß M ein kommutativer Ring ist. Das Nullelement in M ist $(0, 0, 0, \ldots)$; die dazu gehörende Klasse ist die Menge $\mathfrak{n} \subset M$ aller Nullfolgen, und nach Satz 21.2 ist $\mathfrak{n}$ ein Ideal von M. Die Menge A der Kongruenzklassen von M, von der wir ja erwarten, daß sie bis auf Isomorphien der Körper $\mathfrak{R}$ wird, ist nach § 21 dasselbe wie $M/\mathfrak{n}$; als homomorphes Bild des kommutativen Ringes M ist also auch A ein kommutativer Ring.

Wir wollen zeigen, daß A sogar ein Körper ist. Die Null in A ist die Klasse $\mathfrak{n}$; als Repräsentant kann $(0, 0, 0, \ldots)$ gewählt werden. Entsprechend ist $(1, 1, 1, \ldots) + \mathfrak{n}$ das Einselement. Ein von $\mathfrak{n}$ verschiedenes Element aus A enthält nur solche Folgen $(a_1', a_2', a_3', \ldots)$, für die ein $q \in \mathfrak{Q}$, $1 > q > 0$, existiert mit $|a_n'| > q$ für alle $n > N^*(q) \in \mathfrak{N}$; dabei hängen q und $N^*(q)$ von der vorgelegten Folge ab. Nur endlich viele a_i' einer solchen willkürlich dieser Klasse entnommenen Folge $(a_1', a_2', a_3', \ldots)$ sind also ihrem Betrage nach kleiner oder gleich q; ersetzen wir diese a_i' durch Einsen, so erhalten wir den Repräsentanten $(a_1, a_2, a_3, \ldots)$ derselben Klasse, und für ihn gilt $a_n \neq 0$ und $|a_n| > q$ für alle n. Der Nachweis, daß A ein Körper ist, ist erbracht, wenn wir gezeigt haben, daß $(a_1, a_2, a_3, \ldots) + \mathfrak{n}$ mit dem eben fixierten Repräsentanten $(a_1, a_2, a_3, \ldots)$ ein Inverses besitzt. Wir geben es an: $\left(\frac{1}{a_1}, \frac{1}{a_2}, \frac{1}{a_3}, \ldots\right) + \mathfrak{n}$; wir müssen nur noch nachweisen, daß $\left(\frac{1}{a_1}, \frac{1}{a_2}, \frac{1}{a_3}, \ldots\right)$ eine Cauchy-Folge ist. Das folgt aber daraus, daß $(a_1, a_2, a_3, \ldots)$ eine Cauchy-Folge ist und die Ungleichung

$$\left|\frac{1}{a_m} - \frac{1}{a_n}\right| = \frac{|a_m - a_n|}{|a_m a_n|} < \frac{1}{q^2}\,|a_m - a_n|$$

besteht.

32.3 Ist der so konstruierte Körper A nun auch das geworden, was wir haben wollten? Um das nachzuprüfen, orientieren wir uns an der Vorstellung, der Körper $\mathfrak{R} \supset \mathfrak{Q}$ sei die Menge aller Dezimalbrüche. Zunächst ist sicher die Teilstruktur $T = \{x\colon x \in A,\ x = (a, a, a, \ldots) + \mathfrak{n}\}$ aller durch konstante Folgen repräsentierbaren Klassen aus A isomorph $\mathfrak{Q}$. Von Isomorphien abgesehen ist also A ein Oberkörper von $\mathfrak{Q}$. Ferner definiert jeder Dezimalbruch, zum Beispiel der für π, eine Cauchy-Folge, hier

$$(3,\ 3{,}1,\ 3{,}14,\ 3{,}141,\ 3{,}1415, \ldots),$$

und wird so Repräsentant einer Klasse aus A. Schließlich sieht man auch umgekehrt, daß man für jede Klasse aus A genau einen Repräsentanten dieser Art

wählen kann. Wir dürfen A als die Menge aller Dezimalbrüche ansehen. Im folgenden stellen wir nun einige einfache Eigenschaften des in Abschnitt 32.2 konstruierten Körpers A fest, die, wie sich zum Schluß herausstellen wird, ihn axiomatisch eindeutig beschreiben.

32.4 Wir wollen A anordnen und wählen ein Element $(a_1, a_2, a_3, \ldots) + \mathfrak{n}$ von A, das nicht Null ist. Wir wissen bereits, daß dann ein $q \in \mathfrak{Q}$, $q > 0$, existiert, so daß $|a_n| > q$ wird für alle $n > N^*(q)$. Da nun $(a_1, a_2, a_3, \ldots)$ eine Cauchy-Folge ist, gilt ferner $|a_m - a_n| < 2q$ für alle $m, n > N(2q)$. Aus beidem zusammen folgt: Für $n > N = \mathrm{Max}(N^*(q), N(2q))$ haben alle a_n das gleiche Vorzeichen. Genau dann, wenn alle diese a_n positiv sind, sei $(a_1, a_2, a_3, \ldots) + \mathfrak{n} \in A$ positiv. Diese Vorschrift ist eine Definition, da ein anderer Repräsentant derselben Klasse sich lediglich um eine Nullfolge von $(a_1, a_2, a_3, \ldots)$ unterscheidet. Die Anordnungsaxiome aus § 31 sind ersichtlich erfüllt. Und schließlich wird die Anordnung von $\mathfrak{Q}$ fortgesetzt; denn $(a, a, a, \ldots) + \mathfrak{n} \in T \subset A$ wird genau dann positiv, wenn $a \in \mathfrak{Q}$ in $\mathfrak{Q}$ positiv ist.

32.5 Ist A archimedisch angeordnet? Es seien $(a_1, a_2, a_3, \ldots) + \mathfrak{n}$ und $(b_1, b_2, b_3, \ldots) + \mathfrak{n}$ positive Elemente aus A. Dann gibt es positive rationale Zahlen q_1, q_2, r_1, r_2 derart, daß für alle hinreichend großen n gilt:

$$q_1 < a_n < q_2, r_1 < b_n < r_2.$$

Die Abschätzungen nach oben folgen daraus, daß $(a_1, a_2, a_3, \ldots)$ und $(b_1, b_2, b_3, \ldots)$ Cauchy-Folgen sind. Da $\mathfrak{Q}$ archimedisch angeordnet ist, gibt es ein $k \in \mathfrak{N}$ mit $kq_1 > r_2$. Dann ist aber erst recht $(ka_1, ka_2, ka_3, \ldots) + \mathfrak{n}$ größer als $(b_1, b_2, b_3, \ldots) + \mathfrak{n}$. Es ist also A ein archimedisch angeordneter Körper.

32.6 Wir wenden uns noch einmal der Definition zu Beginn von Abschnitt 32.2 zu und verallgemeinern sie, indem wir $\mathfrak{Q}$ durch einen angeordneten Körper K ersetzen.

Definition: *Es sei K ein angeordneter Körper. Eine Folge $(a_1, a_2, a_3, \ldots)$ aus K^∞ heißt Cauchy-Folge, wenn zu jedem positiven $\varepsilon \in K$ ein $N(\varepsilon) \in \mathfrak{N}$ derart existiert, daß $|a_m - a_n| < \varepsilon$ wird für $m, n > N(\varepsilon)$. Eine Folge $(a_1, a_2, a_3, \ldots) \in K^\infty$ heißt Nullfolge, wenn zu jedem positiven $\varepsilon \in K$ ein $N_0(\varepsilon) \in \mathfrak{N}$ derart existiert, daß $|a_n| < \varepsilon$ wird für $n > N_0(\varepsilon)$. Allgemeiner heißt die Folge $(a_1, a_2, a_3, \ldots) \in K^\infty$ in K konvergent mit dem Limes a, wenn es ein $a \in K$ gibt derart, daß zu jedem positiven $\varepsilon \in K$ ein $S(\varepsilon) \in \mathfrak{N}$ existiert mit $|a_n - a| < \varepsilon$ für $n > S(\varepsilon)$; man schreibt dann $\lim\limits_{\nu \to \infty} a_\nu = a$. Ein angeordneter Körper K heißt vollständig, wenn jede Cauchy-Folge $(a_1, a_2, a_3, \ldots) \in K^\infty$ in K konvergent ist.*

Nullfolgen sind also konvergent mit dem Limes Null.
Wir wissen, daß $\mathfrak{Q}$ nicht vollständig ist. Die in Abschnitt 32.3 aufgeschriebene Cauchy-Folge aus $\mathfrak{Q}^\infty$ beispielsweise ist nicht konvergent in $\mathfrak{Q}$, da sie keine rationale Zahl als Limes hat. Andererseits ist die betrachtete Cauchy-Folge nach dem Cauchyschen Konvergenzkriterium aus der Analysis jedenfalls in $\mathfrak{R}$ konvergent wie jede Cauchy-Folge aus $\mathfrak{R}^\infty$. Dort wird also behauptet: $\mathfrak{R}$ ist

ein vollständiger archimedisch angeordneter Körper. Unter dieser ständig benutzten Voraussetzung betreibt man dann reelle Analysis.
Wir wollen nun zeigen, daß der archimedisch angeordnete Körper A vollständig ist. Das ist nicht schwer, aber etwas umständlich aufzuschreiben.

Es sei eine Cauchy-Folge $(f_1 + \mathfrak{n}, f_2 + \mathfrak{n}, f_3 + \mathfrak{n}, \ldots) \in A^\infty$ von Elementen

$$\begin{array}{rcl} f_1 + \mathfrak{n} & = & (a_{11}, a_{12}, a_{13}, \ldots) + \mathfrak{n} \\ f_2 + \mathfrak{n} & = & (a_{21}, a_{22}, a_{23}, \ldots) + \mathfrak{n} \\ f_3 + \mathfrak{n} & = & (a_{31}, a_{32}, a_{33}, \ldots) + \mathfrak{n} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots & & \end{array} \tag{1}$$

aus A vorgelegt. Auf Grund unserer Definition und der in Abschnitt 32.4 vorgenommenen Anordnung von A hat das die folgende Bedeutung. Zu vorgegebenem $\varepsilon > 0$ aus $\mathfrak{Q}$ gibt es ein $N(\varepsilon) \in \mathfrak{N}$ mit nachstehender Eigenschaft. Sind r, s natürliche Zahlen größer als $N(\varepsilon)$, so existiert ein $\Lambda = \Lambda(r, s) \in \mathfrak{N}$ derart, daß für alle $\lambda > \Lambda$ gilt:

$$|a_{r\lambda} - a_{s\lambda}| < \varepsilon \qquad (r, s > N(\varepsilon); \lambda > \Lambda(r, s)). \tag{2}$$

Wir denken uns ferner die Repräsentanten in (1) noch in bestimmter Weise ausgesucht; wir wollen, daß die Komponenten der f_λ mit wachsendem λ immer weniger streuen: Lassen wir von einer Cauchy-Folge $(a_1, a_2, a_3, \ldots)$ die ersten k Komponenten weg, so wird auch $(a_{k+1}, a_{k+2}, a_{k+3}, \ldots)$ eine Cauchy-Folge, die dieselbe Klasse repräsentiert. Auf diese Weise können wir erreichen, daß in (1) für alle r, s gilt:

$$|a_{rs} - a_{rr}| < \frac{1}{r} \qquad (r, s \in \mathfrak{N}). \tag{3}$$

Eine beliebige Komponente der r-ten Folge f_r unterscheidet sich von der r-ten Komponente a_{rr} dieser Folge um weniger als $\frac{1}{r}$.
Unter diesen Voraussetzungen wollen wir zeigen: Die Folge

$$(f_1 + \mathfrak{n}, f_2 + \mathfrak{n}, f_3 + \mathfrak{n}, \ldots) \in A^\infty$$

ist in A konvergent mit dem Limes $f + \mathfrak{n} \in A$, wobei f die Diagonalfolge $(a_{11}, a_{22}, a_{33}, \ldots)$ des Schemas

$$\begin{array}{cccc} a_{11} & a_{12} & a_{13} & a_{14} \ldots \\ a_{21} & a_{22} & a_{23} & a_{24} \ldots \\ a_{31} & a_{32} & a_{33} & a_{34} \ldots \\ a_{41} & a_{42} & a_{43} & a_{44} \ldots \\ \ldots\ldots & \ldots\ldots & \ldots\ldots & \end{array}$$

bedeutet. Der Nachweis dafür ist gewiß dann erbracht, wenn wir das Folgende zeigen können. Zu vorgegebenem $\varepsilon > 0$ aus $\mathfrak{Q}$ existiert ein $S(\varepsilon) \in \mathfrak{N}$ derart, daß für alle $r, s > S(\varepsilon)$ gilt:

$$|a_{rs} - a_{ss}| < \varepsilon \qquad (r, s > S(\varepsilon)). \tag{4}$$

Das heißt speziell: Wird die Folge $(a_{r1}, a_{r2}, a_{r3}, \ldots)$ in dem angeschriebenen Schema nur hinreichend weit unten gewählt, so unterscheidet sich a_{rs} für $s \geqq r$ von der entsprechenden Komponente a_{ss} der Folge $(a_{11}, a_{22}, a_{33}, \ldots)$ dem Betrage nach um weniger als ε. Aus den Beziehungen (3) und (4) und der Ungleichung

$$|a_{rr} - a_{ss}| \leqq |a_{rr} - a_{rs}| + |a_{rs} - a_{ss}|$$

ergibt sich schließlich von selbst noch, daß f eine Cauchy-Folge, also $f + \mathfrak{n} \in A$ ist.

Der ausstehende Nachweis von (4) stützt sich auf (2) und (3). Für $r, s > N\left(\frac{\varepsilon}{2}\right)$ und hinreichend große $\lambda > \Lambda\,(r, s)$ gilt zunächst einmal

$$|a_{r\lambda} - a_{s\lambda}| < \frac{\varepsilon}{2} \tag{5}$$

auf Grund von (2). Die $a_{r\lambda}$ aus der r-ten Folge f_r unterscheiden sich aber nach (3) von a_{rr} um höchstens $\frac{1}{r}$, somit untereinander um höchstens $\frac{2}{r}$, und entsprechend unterscheiden sich die $a_{s\lambda}$ der s-ten Folge um höchstens $\frac{2}{s}$. An Stelle von (5) bekommen wir deswegen auch

$$|a_{r\lambda} - a_{s\lambda}| < \frac{\varepsilon}{2} + \frac{2}{r} + \frac{2}{s} \qquad \left(r, s > N\left(\frac{\varepsilon}{2}\right)\right), \tag{6}$$

diesmal für alle $\lambda \in \mathfrak{N}$. Hieraus ergibt sich (4) mit $\lambda = s$ und einem beliebigen $S(\varepsilon) \geqq \operatorname{Max}\left(N\left(\frac{\varepsilon}{2}\right), \frac{8}{\varepsilon}\right)$.

32.7 Es ist also A ein vollständiger archimedisch angeordneter Körper. Axiomatisch ist nun noch ein Punkt interessant: Zwei archimedisch angeordnete vollständige Körper K und L sind isomorph. Wenn wir das noch beweisen, so haben wir durch diese Angaben den Körper A sogar eindeutig beschrieben. Wir zeigen statt dessen: Ist K ein archimedisch angeordneter vollständiger Körper, so gilt $K \simeq A$.

Zunächst ist K angeordnet; nach § 31.1 dürfen wir also $\mathfrak{Q} \subset K$ voraussetzen. Weil K sogar archimedisch angeordnet ist, gibt es überdies zu jedem $a \in K$ ein $n \in \mathfrak{N}$ mit $n \cdot 1 = n > a$, und es folgt die Existenz ganzer Zahlen m, n mit $m < a < n$. Nun kann man eine Cauchy-Folge $(a_1, a_2, a_3, \ldots) \in \mathfrak{Q}^\infty$ konstruieren, die a als Limes hat; man wählt etwa $a_1 = m$ und halbiert das Intervall $[m, n]$ durch $\frac{m+n}{2}$; gilt dann noch $m \leqq a \leqq \frac{m+n}{2}$, so wählt man auch $a_2 = m$, andernfalls $a_2 = \frac{m+n}{2}$, und setzt das Verfahren der Intervallhalbierung fort.

Durch $f(a) = (a_1, a_2, a_3, \ldots) + \mathfrak{n} \in A$ wird nun eine Abbildung $f: K \to A$ definiert. Denn erstens ist $(a_1, a_2, a_3, \ldots)$ offenbar eine Cauchy-Folge, und zweitens bildet eine andere gegen a konvergierende Folge $(a_1', a_2', a_3', \ldots) \in \mathfrak{Q}^\infty$ auf Grund der Abschätzung

$$|a_n - a_n'| \leqq |a_n - a| + |a - a_n'|$$

nur einen anderen Repräsentanten derselben Klasse $(a_1, a_2, a_3, \ldots) + \mathfrak{n}$. Diese Abbildung $f: K \to A$ ist surjektiv, weil K vollständig ist. Sie ist auch injektiv; hätten nämlich die voneinander verschiedenen Elemente $a, b \in K$ dasselbe Bild $(a_1, a_2, a_3, \ldots) + \mathfrak{n} \in A$, so hätte die Folge $(a_1, a_2, a_3, \ldots)$ die beiden verschiedenen Limites a und b, was wegen

$$|a - a_n| + |a_n - b| \geqq |a - b|$$

nicht möglich ist.
Die Abbildung $f: K \to A$ ist also bijektiv. Sie ist auch relationstreu. Hierfür seien $(a_1, a_2, a_3, \ldots)$ und $(b_1, b_2, b_3, \ldots)$ Repräsentanten von Klassen aus A; nach Voraussetzung existieren in K die Limites $\lim\limits_{n\to\infty} a_n = a$ und $\lim\limits_{n\to\infty} b_n = b$. Zu zeigen sind dann die Regeln

$$\lim_{n\to\infty} (a_n + b_n) = \lim_{n\to\infty} a_n + \lim_{n\to\infty} b_n \tag{7}$$

und

$$\lim_{n\to\infty} a_n b_n = \lim_{n\to\infty} a_n \cdot \lim_{n\to\infty} b_n. \tag{8}$$

Ihr Nachweis verläuft nach dem aus der Analysis bekannten Muster und stützt sich auf die Ungleichungen

$$|(a_n + b_n) - (a + b)| \leqq |a_n - a| + |b_n - b| \tag{7'}$$

und

$$|a_n b_n - ab| \leqq |b_n| \cdot |a_n - a| + |a| \cdot |b_n - b|. \tag{8'}$$

Insgesamt gilt also $K \simeq A$.

32.8 Zuletzt ersetzen wir die in Abschnitt 32.3 betrachtete Teilstruktur $T = \{x: x \in A, x = (a, a, a, \ldots) + \mathfrak{n}\} \simeq \mathfrak{Q}$ von A durch $\mathfrak{Q}$; den dadurch aus A entstandenen Körper nennen wir den Körper $\mathfrak{R} \supset \mathfrak{Q}$ der reellen Zahlen. Wir fassen unsere Ergebnisse zusammen.

Satz 1: *Es gibt, von Isomorphien abgesehen, genau einen archimedisch angeordneten vollständigen Körper, den Körper $\mathfrak{R}$ der reellen Zahlen.*

Ergänzend wiederholen wir: Der Ring $\mathfrak{Z}$ der ganzen Zahlen ist eindeutig bestimmt als der kleinste angeordnete Ring mit Einselement; der Körper $\mathfrak{Q}$ ist eindeutig bestimmt als der kleinste angeordnete Körper (§ 31). Andere axiomatische Beschreibungen von $\mathfrak{Z}$ und $\mathfrak{Q}$ hatten wir in § 13.2 und § 22.2 kennengelernt.

§ 33* Bewertete Körper

33.1 In einem angeordneten Körper K mit Elementen $a, b, \ldots$ gelten nach § 31.1 die Betragsrechenregeln $|ab| = |a| \cdot |b|$ und $|a + b| \leqq |a| + |b|$. Ihre Bedeutung für die Analysis kann gar nicht hoch genug eingeschätzt werden.

Wir haben sie zum Beispiel bereits bei der Konstruktion des Körpers $\mathfrak{R}$ in typischer Weise gebraucht. Am Anfang der Analysis, etwa in $\mathfrak{R}$, steht der Limesbegriff, und die Theorie besteht aus den Sätzen, die sich über ihn ergeben. Es seien beispielsweise a_n, b_n reelle Zahlen mit $\lim\limits_{n\to\infty} a_n = a$ und $\lim\limits_{n\to\infty} b_n = b$; dann gilt $\lim\limits_{n\to\infty} a_n b_n = ab$. Der Beweis beruht auf der Abschätzung (8′) aus § 32,

$$|a_n b_n - ab| = |b_n(a_n - a) + a(b_n - b)| \leqq |b_n| \cdot |a_n - a| + |a| \cdot |b_n - b|,$$

die sich ihrerseits auf die beiden Betragsrechenregeln stützt. Will man zeigen, daß das Produkt stetiger Funktionen wieder stetig, das Produkt differenzierbarer Funktionen wieder differenzierbar ist, so benutzt man das gleiche Beweisschema.

Nun wissen wir aus § 31.1, daß der Körper $\mathfrak{C}$ sich nicht anordnen läßt. Trotzdem kann man in ihm mit großem Erfolg Analysis betreiben, und die zitierten Limes-Sätze gelten auch hier. Dazu definiert man den Betrag $|z|$ einer komplexen Zahl $z \in \mathfrak{C}$ als die nichtnegative reelle Wurzel aus $z\bar{z} \geqq 0$ und hat damit einen reellen „Wert" von z; für komplexe Zahlen $z_1, z_2, \ldots$ soll dann $\lim\limits_{n\to\infty} z_n = z$ bedeuten, daß der „Wert" von $z_n - z$ mit wachsendem n immer kleiner wird: Zu vorgegebenem reellen $\varepsilon > 0$ existiert ein $S(\varepsilon) \in \mathfrak{N}$ derart, daß $|z_n - z| < \varepsilon$ ist für $n > S(\varepsilon)$. Entscheidend ist nun, daß auf diese Weise die Betragsrechenregeln $|ab| = |a| \cdot |b|$ und $|a + b| \leqq |a| + |b|$ auch für komplexe Zahlen a, b ihre Gültigkeit behalten (vgl. Anhang). Als Folge davon kann man die erwähnten Sätze auch für komplexe Folgen oder Funktionen aussprechen und die alten Beweise, die auf diesen Regeln beruhen, übernehmen.

Dieses Beispiel zeigt, daß es sich lohnt, den Begriff der Anordnung eines Körpers K in folgender Weise zu verallgemeinern.

Definition: *Ein Körper K mit Elementen $a, b, \ldots$ heißt bewertet, wenn eine Abbildung $\varphi\colon K \to W$ von K in einen angeordneten Körper W (meist $W = \mathfrak{R}$) mit folgenden Eigenschaften vorhanden ist:*

(1) $\varphi(0) = 0$; $\varphi(a) > 0$ *für alle* $a \in K$, $a \neq 0$.
(2) $\varphi(ab) = \varphi(a) \cdot \varphi(b)$ *für alle* $a, b \in K$.
(3) $\varphi(a + b) \leqq \varphi(a) + \varphi(b)$ *für alle* $a, b \in K$.

Es ist klar: Jeder angeordnete Körper K besitzt die durch $W = K$ und $\varphi(a) = |a|$ definierte *Betragsbewertung*. Der Körper $\mathfrak{C}$ läßt sich durch $\varphi(z) = +\sqrt{z\bar{z}} \in \mathfrak{R}$ bewerten. Eine *triviale Bewertung* schließlich hat jeder Körper K: Man setze $\varphi(0) = 0$ und $\varphi(a) = 1$ für jedes $a \in K$, $a \neq 0$. Zwei Be-

wertungen $\varphi_1 : K \to W$ und $\varphi_2 : K \to W$ wird man genau dann als äquivalent ansehen, wenn für alle $a, b \in K$ gilt:

$$\varphi_1(a) < \varphi_1(b) \quad \Leftrightarrow \quad \varphi_2(a) < \varphi_2(b).$$

Folgerungen aus (1) und (2) sind $\varphi(1) = 1$, $\varphi(-1) = 1$ und $\varphi(-a) = \varphi(a)$. Damit läßt sich wie in § 31, (5), die Dreiecksungleichung (3) in der Gestalt

$$|\varphi(a) - \varphi(b)| \leqq \varphi(a \pm b) \leqq \varphi(a) + \varphi(b)$$

verallgemeinern. Schließlich bekommt man aus (3) auch noch

$$\varphi(a_1 + a_2 + \ldots + a_n) \leqq \varphi(a_1) + \varphi(a_2) + \ldots + \varphi(a_n).$$

33.2 Eine Folge $(a_1, a_2, a_3, \ldots)$ von Elementen a_ν eines durch φ bewerteten Körpers K heißt *Cauchy-Folge* oder *Fundamentalfolge*, wenn zu jedem positiven $\varepsilon \in W$ ein $N(\varepsilon) \in \mathfrak{N}$ derart existiert, daß $\varphi(a_m - a_n) < \varepsilon$ wird für $m, n > N(\varepsilon)$. Entsprechend überträgt man den Konvergenzbegriff. Ein Rückblick auf die Konstruktion, die in § 32 von $\mathfrak{Q}$ zu $\mathfrak{R}$ geführt hat, zeigt, daß auch sie sich ohne wesentlichen zusätzlichen Aufwand verallgemeinern läßt. Am Ende steht das Ergebnis: Jeder bewertete Körper K besitzt einen minimalen bewerteten Oberkörper E derart, daß die Bewertung von E eine Fortsetzung der Bewertung von K und jede Cauchy-Folge aus E^∞ in E konvergent ist; der Körper E ist bis auf Isomorphien eindeutig bestimmt und heißt die *vollständige Hülle* von K bezüglich der Bewertung φ. In § 32 handelte es sich um den Spezialfall $K = \mathfrak{Q}$, $E = \mathfrak{R}$, $\varphi(a) = |a|$.
Wir wollen auf Einzelheiten nicht weiter eingehen, weisen aber noch auf folgendes hin. Sind a, b Elemente eines bewerteten Körpers K, so darf man sich unter $\varphi(a - b)$ ihre „Entfernung" $d(a, b)$ vorstellen. Wir präzisieren das.

Definition: *Eine Menge M von Elementen $a, b, c, \ldots$ heißt ein metrischer Raum, wenn eine Abbildung $d: M \times M \to A$ des cartesischen Produktes $M \times M$ in einen angeordneten Körper A (meist $A = \mathfrak{R}$) mit folgenden Eigenschaften erklärt ist:*
(1) $d(a, b) = 0$ *für* $a = b$; $d(a, b) > 0$ *für* $a \neq b$.
(2) $d(a, b) = d(b, a)$.
(3) $d(a, c) \leqq d(a, b) + d(b, c)$.

Diese Forderungen an die Entfernung oder *Metrik* $d(x, y)$ haben plausible anschauliche Bedeutungen; insbesondere bezieht die *Dreiecksungleichung* (3) ihren Namen hierher. Ist nun K durch φ bewertet, so definiert ersichtlich $d(a, b) = \varphi(a - b)$ eine Metrik auf K.

33.3 Welche Bewertungen gestattet beispielsweise $\mathfrak{Q}$? Wir kennen bislang die triviale und die Betragsbewertung. Weitere Bewertungen von $\mathfrak{Q}$ erhält man wie folgt.

Es sei $p \in \mathfrak{N}$ eine feste Primzahl und das positive $q \in \mathfrak{Q}$ in der Gestalt $\frac{m}{n} p^k$ mit zu p und untereinander teilerfremden natürlichen Zahlen m, n geschrieben; wir setzen dann $\varphi_p(0) = 0$ und

$$\varphi_p(q) = \varphi_p(-q) = p^{-k}.$$

Dies definiert eine Bewertung $\varphi_p: \mathfrak{Q} \to \mathfrak{Q}$ von $\mathfrak{Q}$. Die Forderungen (1), (2) aus 33.1 sind trivialerweise erfüllt, und sind m, n, r, s ganz und teilerfremd zu p, so folgt für $k \leqq l$ und von Null verschiedener Summe in der folgenden Klammer

$$\varphi_p\left(\frac{m}{n} p^k + \frac{r}{s} p^l\right) = \varphi_p\left(\frac{ms + nrp^{l-k}}{ns} p^k\right) = p^{-\varkappa}, \qquad \varkappa \geqq k,$$

oder $\varphi_p(a+b) \leqq \operatorname{Max}(\varphi_p(a), \varphi_p(b)) \leqq \varphi_p(a) + \varphi_p(b)$, also (3).
Dies nennt man eine *p-adische Bewertung* von $\mathfrak{Q}$. Etwas nachlässig gesagt, ist ein $q \in \mathfrak{Q}$ klein, wenn es durch eine hohe Potenz von p teilbar ist. Jede Wahl von p liefert eine andere derartige Bewertung, und entgegen dem ersten Augenschein spielen diese Bewertungen eine große Rolle (vgl. etwa HASSE [6]). Weitere Bewertungen von $\mathfrak{Q}$ gibt es, wie man zeigen kann, nicht.

§ 34 Symmetrische Polynome

34.1 Wir wenden uns noch einmal Polynomringen $R[x_1, x_2, \ldots, x_n]$ in n Unbestimmten über einem kommutativen Ring R mit Einselement zu. Ein Polynom $f(x_1, x_2, \ldots, x_n) \in R[x_1, x_2, \ldots, x_n]$ heißt *symmetrisch*, wenn es bei jeder Permutation der x_i unverändert bleibt, wenn also für jedes $\pi \in \mathfrak{S}_n$ gilt:

$$f(x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(n)}) = f(x_1, x_2, \ldots, x_n).$$

Beispiele solcher Polynome sind etwa $x_1 + x_2 + \ldots + x_n$, $x_1^2 + x_2^2 + \ldots + x_n^2$ oder Ringelemente $r \in R$.
Weitere symmetrische Polynome, die besonders häufig auftreten, erhält man wie folgt. Man wähle eine weitere Unbestimmte x über $R[x_1, x_2, \ldots, x_n]$ und betrachte das Polynom $g(x) = (x - x_1)(x - x_2)\ldots(x - x_n) \in R[x_1, x_2, \ldots, x_n][x]$. Wir multiplizieren aus und setzen

$$g(x) = x^n - \sigma_1 x^{n-1} + \sigma_2 x^{n-2} - + \ldots + (-1)^n \sigma_n.$$

Jede Permutation der x_i läßt $g(x)$ und damit auch die $\sigma_i \in R[x_1, x_2, \ldots, x_n]$ fest; sie heißen die *elementarsymmetrischen Polynome* der $x_1, x_2, \ldots, x_n$ und haben die Gestalt

$$\sigma_1 = \sum_i x_i, \ \sigma_2 = \sum_{i<j} x_i x_j, \ \ldots, \ \sigma_n = x_1 x_2 \ldots x_n.$$

Gegenstand unserer Erörterungen ist der folgende *Hauptsatz über symmetrische Polynome.*

Satz 1: *Jedes symmetrische Polynom* $f(x_1, x_2, \ldots, x_n) \in R[x_1, x_2, \ldots, x_n]$ *läßt sich als Polynom in den elementarsymmetrischen Polynomen* σ_i *schreiben:*

$$f(x_1, x_2, \ldots, x_n) \in R[\sigma_1, \sigma_2, \ldots, \sigma_n].$$

Beweis: Das Polynom $f(x_1, x_2, \ldots, x_n)$ ist eine Summe von Ausdrücken der Gestalt $r x_1^{\lambda_1} x_2^{\lambda_2} \ldots x_n^{\lambda_n}$, $r \in R$, $r \neq 0$, $\lambda_i \geqq 0$; wir schreiben diese Summe

so auf, daß $ax_1^{\alpha_1}x_2^{\alpha_2}\dots x_n^{\alpha_n}$ vor $bx_1^{\beta_1}x_2^{\beta_2}\dots x_n^{\beta_n}$ steht, wenn die erste nicht verschwindende unter den Differenzen $\alpha_1-\beta_1,\ \alpha_2-\beta_2,\ \dots,\ \alpha_n-\beta_n$ positiv ist. Wir nehmen an, $f(x_1, x_2, \dots, x_n)$ habe den Grad m; das soll heißen, daß für wenigstens einen der Summanden $\lambda_1+\lambda_2+\dots+\lambda_n = m$ wird und die Exponentensumme sonst immer $\leqq m$ ausfällt. Der triviale Fall $f(x_1,x_2,\dots,x_n) = 0$ ist dabei ausgeschlossen.

Der erste Summand von $f(x_1, x_2, \dots, x_n)$ heiße $ax_1^{\alpha_1}x_2^{\alpha_2}\dots x_n^{\alpha_n}$. Weil nun $f(x_1, x_2, \dots, x_n)$ symmetrisch ist, gilt $\alpha_1 \geqq \alpha_2 \geqq \dots \geqq \alpha_n$. Denselben ersten Summanden hat das Polynom

$$a\sigma_1^{\alpha_1-\alpha_2}\sigma_2^{\alpha_2-\alpha_3}\dots\sigma_n^{\alpha_n} \in R[x_1, x_2, \dots, x_n]$$

vom Grad

$$(\alpha_1-\alpha_2)+2(\alpha_2-\alpha_3)+\dots+(n-1)(\alpha_{n-1}-\alpha_n)+n\alpha_n = \alpha_1+\alpha_2+\dots+\alpha_n \leqq m.$$

Wir subtrahieren es von $f(x_1, x_2, \dots, x_n)$ und betrachten die Differenz

$$d(x_1, x_2, \dots, x_n) = f(x_1, x_2, \dots, x_n) - a\sigma_1^{\alpha_1-\alpha_2}\sigma_2^{\alpha_2-\alpha_3}\dots\sigma_n^{\alpha_n}.$$

Es ist entweder $d(x_1, x_2, \dots, x_n) = 0$, und in diesem Fall sind wir fertig, oder das symmetrische Polynom $d(x_1, x_2, \dots, x_n)$ hat einen Grad $\leqq m$ und einen ersten Summanden $bx_1^{\beta_1}x_2^{\beta_2}\dots x_n^{\beta_n}$, der bei der verabredeten Reihenfolge nur einer der möglichen Nachfolger von $ax_1^{\alpha_1}x_2^{\alpha_2}\dots x_n^{\alpha_n}$ sein kann. Solche Nachfolger gibt es unter Polynomen vom Grad $\leqq m$ nur endlich viele. Setzt man daher das Subtraktionsverfahren fort, so bricht es nach endlich vielen Schritten mit einer Differenz Null ab, und Satz 1 ist bewiesen.

Dieser Beweis ist konstruktiv; er ermöglicht es, zu vorgelegtem symmetrischen $f(x_1, x_2, \dots, x_n)$ die gewünschte Darstellung als Polynom in den elementarsymmetrischen Polynomen $\sigma_i(x_1, x_2, \dots, x_n)$ auch wirklich aufzufinden, selbst wenn die Rechnung im einzelnen mühsam sein mag.

34.2 Eine der häufigsten Anwendungen von Satz 1 beruht darauf, daß auch das Polynom

$$D(x_1, x_2, \dots, x_n) = \prod_{i<k}(x_i - x_k)^2 \in R[x_1, x_2, \dots, x_n]$$

symmetrisch ist, also eine Polynomdarstellung durch die $\sigma_i(x_1, x_2, \dots, x_n)$ gestattet.

Es sei K ein Körper und $f(x) = x^n + a_1x^{n-1} + a_2x^{n-2} + \dots + a_n \in K[x]$; es gebe einen Erweiterungskörper E von K, in dem $f(x)$ die n nicht notwendig paarweise voneinander verschiedenen Nullstellen $\xi_1, \xi_2, \dots, \xi_n$ besitzt. Später wird sich zeigen, daß ein derartiger Körper E immer existiert (§ 58). Nach dem Beweis von Satz 26.2 gilt dann in $E[x]$

$$f(x) = (x-\xi_1)(x-\xi_2)\dots(x-\xi_n).$$

Unter der *Diskriminante* $D(f)$ von $f(x)$ versteht man die Zahl

$$D(f) = \prod_{i<k}(\xi_i - \xi_k)^2.$$

Man betrachte nun die Polynomdarstellung von $D(x_1, x_2, \ldots, x_n)$ durch die $\sigma_i(x_1, x_2, \ldots, x_n)$ und ersetze in ihr die x_i durch die ξ_i. Wegen

$$\sigma_j(\xi_1, \xi_2, \ldots, \xi_n) = (-1)^j a_j$$

folgt, daß $D(f)$ ein Polynom in den a_j, also $D(f) \in K$ ist. Wir beachten dabei, daß wir die Koeffizienten von $f(x)$ so bezeichnet haben, daß sie bis aufs Vorzeichen dem Polynom $g(x)$ aus dem vorigen Abschnitt entsprechen.
Die Darstellung der Diskriminante $D(f)$ durch die Koeffizienten a_j von $f(x)$ erfordert einige Rechnung, die unter anderem nach dem Muster des Beweises von Satz 1 durchgeführt werden kann. Wir geben zwei Resultate an:

$$D(x^2 + px + q) = p^2 - 4q; \tag{1}$$

$$D(x^3 + a_1x^2 + a_2x + a_3) = a_1^2a_2^2 - 4a_2^3 - 4a_1^3a_3 - 27a_3^2 + 18a_1a_2a_3. \tag{2}$$

34.3 Die Bedeutung der Diskriminante $D(f) \in K$ des Polynoms $f(x) \in K[x]$ beruht auf den Informationen, die sie über die Nullstellen $\xi_i \in E$ von $f(x)$ vermittelt. Sie ist genau dann Null, wenn $f(x)$ in E wenigstens eine mehrfache Nullstelle hat. Wir sehen uns noch zwei Beispiele an.
Das quadratische Polynom $x^2 + px + q \in \Re[x]$ hat entweder zwei konjugiert-komplexe oder nur reelle Nullstellen ξ_1, ξ_2; der letzte Fall tritt genau dann ein, wenn $(\xi_1 - \xi_2)^2 = D(x^2 + px + q) = p^2 - 4q \geqq 0$ ist, was auch die übliche Auflösung der quadratischen Gleichung ergibt.
Das kubische Polynom $f(x) = x^3 + a_1x^2 + a_2x + a_3 \in \Re[x]$ besitzt entweder eine reelle und zwei konjugiert-komplexe oder drei reelle Nullstellen, ihrer Vielfachheit entsprechend gezählt; ein Polynom ungeraden Grades mit reellen Koeffizienten hat ja, wie wir aus der Analysis wissen, mindestens eine reelle Nullstelle. Sind alle drei Nullstellen reell, so ist sicher $D(f) \geqq 0$. Umgekehrt: Sind die Nullstellen ξ_1, ξ_2 nicht reell und $\xi_3 \in \Re$, so sind $(\xi_1 - \xi_3)^2$ und $(\xi_2 - \xi_3)^2$ von Null verschiedene konjugiert-komplexe Zahlen, also $(\xi_1 - \xi_3)^2(\xi_2 - \xi_3)^2 > 0$, und mit $(\xi_1 - \xi_2)^2 < 0$ folgt $D(f) = (\xi_1 - \xi_2)^2(\xi_1 - \xi_3)^2(\xi_2 - \xi_3)^2 < 0$. So ergibt sich der mitunter gebrauchte

Satz 2: *Das kubische Polynom $x^3 + a_1x^2 + a_2x + a_3 \in \Re[x]$ hat genau dann drei reelle Nullstellen, wenn die Diskriminante*

$$a_1^2a_2^2 - 4a_2^3 - 4a_1^3a_3 - 27a_3^2 + 18a_1a_2a_3 \geqq 0$$

ist.

Aufgabe 1: Es sei K ein Körper und

$$f(x) = x^n + a_1x^{n-1} + a_2x^{n-2} + \ldots + a_n \in K[x].$$

In dem Erweiterungskörper E von K habe $f(x)$ die Nullstellen $\xi_1, \xi_2, \ldots, \xi_n$. Man beweise die Formel

$$D(f) = (-1)^{\frac{n(n-1)}{2}} f'(\xi_1)f'(\xi_2) \ldots f'(\xi_n). \tag{3}$$

Literatur: v. d. Waerden [16].