Lineare Algebra individuell
Online-Fassung, Ver. 0.42
Internes Material, **12.4.2004**

Kapitel 1

Erste algebraische Strukturen

Hier werden die grundlegenden Begriffe eingeführt; sie abstrahieren vom historisch entstandenen Zahlbegriff und erlauben uns, mit nicht allzu großem technischem Aufwand eine Reihe von Resultaten gleichzeitig zu gewinnen, die wir sonst Fall für Fall beweisen müssten. Andererseits ergibt sich ein Ansatz für nicht triviale Erweiterungen vertrauter Sätze über das Rechnen mit Zahlen.

1.2 Ringe und Körper

Wir beginnen mit einem Begriff, der alle uns vertrauten Zahlbereiche umfasst. Die folgende Bezeichnung wurde von D. Hilbert eingeführt und beinhaltet Rechenregeln, die z.B. für ganze, rationale, reelle Zahlen, aber auch für Polynome mit Koeffizienten aus solchen Zahlen gelten.

Definition. (*Ring*) 1/2/1

Ein *Ring* ist ein Tripel $(R,+,\cdot)$, bestehend aus einer Menge R und zwei Operationen $+$ (Addition) und $\cdot$ (Multiplikation) auf R, für die folgende Eigenschaften erfüllt sind:
(1) $(R,+)$ ist eine abelsche Gruppe.
(2) $(R,\cdot)$ ist ein Monoid.
(3) Für alle $a,b\in R$ gilt $a\cdot(b+c)=a\cdot b+a\cdot c$, $(a+b)\cdot c=a\cdot c+b\cdot c$.

Die letztgenannte Eigenschaft (*Distributivgesetz*) macht deutlich, dass die Kommutativität der Multiplikation im Allgemeinen nicht gefordert wird. In der Literatur wird der Begriff „Ring“ gelegentlich noch allgemeiner verwendet (d.h. es werden schwächere Forderungen gestellt).

Vereinbarungen.

- Das neutrale Element der Addition wird mit 0 bezeichnet (*Nullelement des Ringes*). $(R,+)$ heißt *additive Gruppe des Ringes* $(R,+,\cdot)$.
- Das neutrale Element der Multiplikation wird (meist) mit 1 bezeichnet (*Einselement des Ringes*).
- $a\cdot b+c\cdot d:=(a\cdot b)+(c\cdot d)$; wir sagen *Punktrechnung geht vor Strichrechnung* (diese Konvention erspart uns das Setzen gewisser Klammern). Genau genommen erhält die Eigenschaft (3) in der Definition dadurch erst einen Sinn.
- Der Ring $(R,+,\cdot)$ heißt *kommutativ*, falls das Monoid $(R,\cdot)$ kommutativ ist, d.h. für $a,b\in R$ gilt $a\cdot b=b\cdot a$.
- Anstelle von $(R,+,\cdot)$ schreiben wir meist R, wenn kein Zweifel über die Operationen besteht, mit denen die Menge R versehen werden soll. Ist es ausnahmsweise erforderlich darauf hinzuweisen, so schreiben wir

Hier stehen nur Dinge, die uns vom Rechnen mit ganzen Zahlen längst vertraut sind. Was fehlt: Eine Division, wie wir sie von den reellen oder rationalen Zahlen kennen.

m.a.W.: Die Multiplikation bindet stärker als die Addition.

auch 0_R für das Nullelement und 1_R für das Einselement sowie $+_R$ und $\cdot_R$ für die Operationen; R heißt dann die zugrundeliegende Menge des Ringes.

Satz. *Ist R ein Ring, $a, b \in R$, so gilt:* 1/2/2

(1) $0 \cdot a = 0 = a \cdot 0$.

(2) $(-1) \cdot a = -a = a \cdot (-1)$.

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

(4) *Für endliche Indexmengen I, J und Familien $(a_i)_{i \in I}$, $(b_j)_{j \in J}$ von Elementen aus R ist*
$$\Big(\sum_{i \in I} a_i\Big) \cdot \Big(\sum_{j \in J} b_j\Big) = \sum_{(i,j) \in I \times J} a_i \cdot b_j \quad (\textit{allgemeines Distributivgesetz}).$$

(5) *Für $a, b \in R$ mit $a \cdot b = b \cdot a$ ist* $(a+b)^n = \sum_{\nu=0}^{n} \binom{n}{\nu} a^\nu b^{n-\nu}$,

wobei $\binom{n}{\nu}$ (*der sog.* Binomialkoeffizient) *die Anzahl der Möglichkeiten bezeichnet, aus einer n-elementigen Menge eine ν-elementige auszuwählen* (binomischer Satz).

Es gilt $\binom{n}{\nu} = \dfrac{n!}{\nu!\,(n-\nu)!}$, diese Formel kann durch vollständige Induktion bewiesen werden.

Beweis. Wir zeigen z.B. (1). $0 + 0 = 0$, also gilt $(0 + 0) \cdot a = 0 \cdot a$, d.h. nach dem Distributivgesetz ist $0 \cdot a + 0 \cdot a = 0 \cdot a$, und addieren wir auf beiden Seiten der Gleichung dasjenige Ringelement, das in der Gruppe $(R, +)$ zu $0 \cdot a$ invers ist, so erhalten wir $0 \cdot a = 0$.
Die übrigen Eigenschaften werden zur Übung empfohlen. ❏

Beispiele.

1. $(\mathbb{Z}, +, \cdot)$, der *Ring der ganzen Zahlen* mit der üblichen Addition und Multiplikation.
2. $(\mathbb{R}, +, \cdot)$, die reellen Zahlen mit den aus der Analysis vertrauten Operationen.
3. M sei eine Menge, R ein Ring. Dann bildet die Menge $\mathrm{Abb}(M, R)$ der Abbildungen von M nach R einen Ring mit den folgenden Operationen: Für $f, g \in \mathrm{Abb}(M, R)$ sind $f + g$ und fg die durch
$$(f + g)(x) := f(x) + g(x), \quad (fg)(x) := f(x) \cdot g(x)$$
für $x \in M$ definierten Elemente aus $\mathrm{Abb}(M, R)$. (fg darf nicht mit der ebenfalls als Produkt bezeichneten Komposition von Abbildungen verwechselt werden).

Wir empfehlen, die Ringeigenschaften nachzurechnen.

Der für Gruppen eingeführte Begriff des Homomorphismus lässt sich analog auf den vorliegenden Fall übertragen. Eine Abbildung von Ringen wird *homomorph* genannt, wenn sie die relevanten Operationen und Elemente erhält. 1/2/3

Definition. (*Unterring, Ringhomomorphismus*)

$(R, +_R, \cdot_R)$ sei ein Ring.

(1) Eine Teilmenge $R' \subseteq R$ heißt *Unterring* von R, wenn $1_R \in R'$ ist, die Operationen $+_R$ und $\cdot_R$ von R Einschränkungen auf R' besitzen sowie R' mit diesen einen Ring bildet; gleich bedeutend nennen wir R einen *Erweiterungsring* von R'.

Was inhaltlich hinter diesen Begriffen der Algebra steht, haben Sie in Wirklichkeit schon lange verwendet. Wir benutzen sie insbesondere zur leichteren Formulierung von Rechenregeln.

(2) Ist $(S, +_S, \cdot_S)$ ein Ring, so heißt eine Abbildung $f: R \to S$ *Ringhomomorphismus,* wenn $f(1_R) = 1_S$ ist und für alle $x, y \in R$
$$f(x +_R y) = f(x) +_S f(y), \quad f(x \cdot_R y) = f(x) \cdot_S f(y).$$
(3) Ein Ringhomomorphismus $f : R \to S$ heißt (*Ring-*)*Isomorphismus,* wenn ein zweiseitig inverser Ringhomomorphismus $g : S \to R$ zu f existiert, d.h. für g gilt $f \cdot g = \mathrm{id}_S$ und $g \cdot f = \mathrm{id}_R$. Letztere Eigenschaft ist offenbar äquivalent dazu, dass der Homomorphismus f bijektiv ist.
(4) Das Symbol $\cong$ verwenden wir in diesem Zusammenhang um auszudrücken, dass ein (Ring-)Isomorphismus zwischen zwei Ringen existiert.

Die ganzen Zahlen bilden beispielsweise einen Unterring der reellen Zahlen, und die Inklusionsabbildung $\mathbb{Z} \to \mathbb{R}$ ist ein Ringhomomorphismus. Interessante Beispiele erfordern weitere Konstruktionen, denen wir uns nachfolgend zuwenden.

Bemerkungen.

1. Ein Ringhomomorphismus $f : R \to S$ induziert einen Homomorphismus $(R, +_R) \to (S, +_S)$ der zugehörigen abelschen Gruppen. Daher ist $f(0_R) = 0_S$ sowie $f(-x) = -f(x)$ für $x \in R$. Als *Kern von* f bezeichnen wir den Kern des zu f gehörigen Gruppenhomomorphismus, $\ker(f) = \{x \in R \mid f(x) = 0_S\}$.
   Es gilt genau dann $\ker(f) = \{0_R\}$, wenn f injektiv ist.
2. Das Bild $\mathrm{im}(f)$ eines Ringhomomorphismus $R \to S$ ist ein Unterring von S. Der Kern ist dagegen nur dann ein Unterring von R, wenn S einelementig (d.h. der „Nullring“) ist, denn 1_R wird durch f auf 1_S abgebildet, kann also nur dann im Kern liegen, wenn $1_S = 0_S$ ist.
3. Die identische Abbildung id_R eines Ringes R in sich ist ein Ringhomomorphismus. Sind $f : R \to S$ und $g : S \to T$ Ringhomomorphismen, so ist die Komposition $g \cdot f : R \to T$ ebenfalls ein Ringhomomorphismus.

Die Verifikation der Eigenschaften 2 und 3 erfordert nur ein formales Ausrechnen.

Vor der allgemeinen Beschreibung durch einen Homomorphiesatz werden zunächst wichtige Beispiele von Ringen und Homomorphismen bereitgestellt.

Integritätsbereiche und Körper

1/2/4

Definition. Ein Ring R heißt *Integritätsbereich* (auch *nullteilerfrei*), falls für $a, b \in R$ mit $a \cdot b = 0$ stets $a = 0$ oder $b = 0$ gilt.

Bemerkung.

1. $\mathbb{Z}$ und $\mathbb{R}$ sind Integritätsbereiche. Dagegen ist der Ring $\mathrm{Abb}(\{1, 2\}, \mathbb{R})$ kein Integritätsbereich, denn die Abbildungen $f, g : \{1, 2\} \to \mathbb{R}$ mit $f(1) = 0$, $f(2) = 1$ und $g(1) = 1$, $g(2) = 0$ haben als Produkt die Nullabbildung, sind aber beide von dieser verschieden (vgl. 1/2/2, Beispiel 3).
2. Integritätsbereiche erfüllen die *Kürzungsregel*
   $$ab = ac \text{ und } a \neq 0 \implies b = c,$$
   denn aus der Voraussetzung folgt $a(b - c) = 0$ und deshalb $a = 0$ oder $b - c = 0$.

Der nachfolgend erklärte Begriff des Körpers geht auf R. Dedekind zurück. Er beinhaltet unsere Vorstellung von den „vier Grundrechenarten“.

Definition. (*Körper, Unterkörper*) 1/2/5

Dass sich beispielsweise die Multiplikation $K \times K \to K$ auf $K' \subseteq K$ einschränken lässt, bedeutet $a, b \in K \Rightarrow a \cdot b \in K$.

(1) Ein kommutativer Ring $(K,+,\cdot)$ heißt *Körper,* falls die Multiplikation eine Einschränkung auf $K^* := K \setminus \{0\}$ besitzt und K^* mit dieser Operation eine Gruppe bildet.

(2) $K' \subseteq K$ heißt *Unterkörper* von $(K,+,\cdot)$, falls die Operationen des Körpers K Einschränkungen auf K' besitzen und K' mit diesen einen Körper bildet. Gleichbedeutend wird dann K auch *Erweiterungskörper* von K' genannt.

Bemerkung. Ein Körper K ist stets nullteilerfrei, denn sind $a, b \in K$ und $0 = ab$, so folgt aus $a \neq 0$ offensichtlich $0 = a^{-1}\cdot 0 = a^{-1}ab = 1\cdot b = b$. In Körpern gilt daher die Kürzungsregel.

Beispiele.

- $(\mathbb{Q},+,\cdot)$, der uns schon vertraute *Körper der rationalen Zahlen* (Brüche), der anschließend exakt definiert wird.
- $(\mathbb{R},+,\cdot)$, der *Körper der reellen Zahlen*; die rationalen Zahlen bilden einen Unterkörper dieses Körpers.
- $(\mathbb{F}_2,+,\cdot)$, der zweielementige Körper, dessen Elemente mit $\overline{0}$, $\overline{1}$ bezeichnet werden; seine Operationen sind durch die nachfolgenden Tafeln bestimmt, die sich eindeutig daraus ergeben, dass $\overline{0}$ als neutrales Element der Addition gewählt wird.

Endliche Körper spielen in den Anwendungen eine wichtige Rolle, beispielsweise in der Kryptographie und der Codierungstheorie.

$+$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

$\cdot$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$

Es gibt wichtige Gründe, im späteren Kapitel über Vektorrechnung beliebige „Grundkörper“ zuzulassen, auch wenn der geometrische Sinn der Überlegungen nicht immer so evident ist wie für den Körper der reellen Zahlen.

Rationale Zahlen, Quotientenkörper

1/2/6

Wir betrachten die Menge $M := \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ und die Relation $\sim$ auf M, die durch die Bedingung

$$(a,b) \sim (c,d) \iff ad = bc$$

definiert ist. $\sim$ ist eine Äquivalenzrelation auf M. Mit $\mathbb{Q} := M/{\sim}$ bezeichnen wir die Menge der Äquivalenzklassen von M bezüglich $\sim$. Die Klasse eines Elements (a,b) wird a/b oder mit $\dfrac{a}{b}$ bezeichnet, sie heißt *Bruch.*

Bruchrechnung ist Ihnen natürlich längst bekannt – vielleicht wußten Sie nur noch nicht so genau, was ein Bruch eigentlich ist. Das soll hier präzisiert werden.

Nachfolgend sind n, a, b, a', b' ganze Zahlen sowie b, $b' \neq 0$.

(1) Auf $\mathbb{Q}$ existiert eine Operation $+_{\mathbb{Q}}$, für die $\dfrac{a}{b} +_{\mathbb{Q}} \dfrac{a'}{b'} = \dfrac{ab' + a'b}{bb'}$ gilt, und $\mathbb{Q}$ bildet mit dieser Operation eine abelsche Gruppe $(\mathbb{Q}, +_{\mathbb{Q}})$. Ihr neutrales Element ist der Bruch $\dfrac{0}{1}$.

(2) Auf $\mathbb{Q}$ existiert eine Operation $\cdot_{\mathbb{Q}}$, für die $\dfrac{a}{b} \cdot_{\mathbb{Q}} \dfrac{a'}{b'} = \dfrac{aa'}{bb'}$ gilt.
$(\mathbb{Q}, +_{\mathbb{Q}}, \cdot_{\mathbb{Q}})$ ist ein kommutativer Ring mit dem Einselement $\dfrac{1}{1}$.

(3) Die Abbildung $\mathbb{Z} \to \mathbb{Q}$, $n \mapsto \dfrac{n}{1}$ ist ein injektiver Ringhomomorphismus. Wir identifizieren die Elemente von $\mathbb{Z}$ mit ihren Bildern, schreiben also $n = \dfrac{n}{1}$.

Natürlich sind die Formeln unter (1), (2) als Definitionen für die Operationen $+_{\mathbb{Q}}$ und $\cdot_{\mathbb{Q}}$ geeignet. Zu prüfen ist allerdings, dass sie nicht von der Wahl der Repräsentanten abhängen.

(4) Der Ring $(\mathbb{Q}, +_{\mathbb{Q}}, \cdot_{\mathbb{Q}})$ ist ein Körper. Er heißt *Körper der rationalen Zahlen.*

Die Verifikation von (1) – (4) wird zur Übung empfohlen. Wir ersparen uns künftig die schwerfälligen Bezeichnungen für die Operationen in $\mathbb{Q}$ und verwenden die üblichen Symbole ($+$ bzw. $\cdot$).

Bemerkung. (*Quotientenkörper*)
Die eben ausgeführte Konstruktion lässt sich wörtlich auf einen beliebigen Integritätsbereich R übertragen. Wir erhalten den *Quotientenkörper* $Q(R)$, der aus allen Brüchen $\dfrac{a}{b}$ mit $b \neq 0$ besteht. Dabei wird der injektive Ringhomomorphismus

$$R \to Q(R), \quad a \mapsto \frac{a}{1}$$

wieder als Inklusion verstanden.

Dies ist ein allgemeines Verfahren, aus Integritätsbereichen Körper zu konstruieren. Beispiele bilden die sog. *Funktionenkörper.*

Komplexe Zahlen 1/2/7

Wir betrachten einen (zunächst beliebigen) Körper K. Auf der Menge $\mathrm{C}(K) := K \times K$ wird durch

$$(a_1, a_2) + (b_1, b_2) := (a_1 + b_1, a_2 + b_2)$$

eine Operation erklärt, die $(\mathrm{C}(K), +)$ zur abelschen Gruppe macht; neutrales Element ist $(0,0)$ (vgl. 1/1/4 (2)).

Satz.
(1) *Durch* $(a_1, b_1) \cdot (a_2, b_2) := (a_1a_2 - b_1b_2, a_1b_2 + a_2b_1)$ *erhält* $\mathrm{C}(K)$ *die Struktur eines kommutativen Ringes* $(\mathrm{C}(K), +, \cdot)$*, sein Einselement ist das Paar* $(1, 0)$.

(2) *Der Ring* $\mathrm{C}(K)$ *ist genau dann ein Körper, wenn* -1 *kein Quadrat in* K *ist.*

In unseren Anwendungen genügt die Implikation „$\Leftarrow$“.

Beweis. Die Verifikation der Ringeigenschaften bereitet keinerlei Schwierigkeiten, auch wenn die Definition der Multiplikation zunächst überraschend aussieht.
Zum Beweis für (2) nehmen wir an, -1 sei nicht das Quadrat eines Elements aus K. Dann besitzt $(a, b) \in \mathrm{C}(K)$ mit $(a, b) \neq (0, 0)$ ein multiplikatives Inverses: Zunächst gilt $a^2 + b^2 \neq 0$ (anderenfalls wäre $a^2 = -b^2$ und somit $-1 = a^2b^{-2}$ oder $-1 = b^2a^{-2}$, $\lightning$). Nun ist

$$\big((a^2 + b^2)^{-1}a, -(a^2 + b^2)^{-1}b\big) \cdot (a, b) = 1,$$

womit ein inverses Element gefunden ist.
Umgekehrt sei $-1 = c^2$ mit $c \in K$. Dann ist $(c, 1) \cdot (c, -1) = (0, 0)$, daher $\mathrm{C}(K)$ kein Integritätsbereich und erst recht kein Körper (vgl. 1/2/5). ❑

Bemerkung. Mit den obigen Bezeichnungen ist die Abbildung $K \to \mathrm{C}(K)$, die a auf $(a, 0)$ abbildet, ein injektiver Ringhomomorphismus. Wir identifizieren die Elemente von K mit ihren Bildern in $\mathrm{C}(K)$ und interpretieren diese Abbildung als Inklusion von Mengen, ähnlich wie wir das zuvor unter 1/2/6 (3) für die Abbildung $\mathbb{Z} \to \mathbb{Q}$ getan haben. Insbesondere werden so $0 \in K$ und $(0, 0) \in \mathrm{C}(K)$ bzw. $1 \in K$ und $(1, 0) \in \mathrm{C}(K)$ identifiziert. Für $x = (a, b) \in \mathrm{C}(K)$ ergibt sich dann $x = a + b \cdot (0, 1)$ mit eindeutig bestimmten Zahlen $a, b \in K$.

Wir beschränken uns von nun an auf den Spezialfall, dass $K = \mathbb{R}$ der Körper der reellen Zahlen ist.

Definition. (*komplexe Zahlen*)

Es sei $K = \mathbb{R}$. Dann ist der oben konstruierte Ring $\mathrm{C}(\mathbb{R})$ ein Körper; er heißt *Körper der komplexen Zahlen* und wird von nun an mit $\mathbb{C}$ bezeichnet. Für $(0,1) \in \mathbb{C}$ verwenden wir das Symbol i.

Sie sollten das Rechnen mit komplexen Zahlen anhand von Beispielen üben; die Aufgabensammlung gibt hierzu Gelegenheit.

Im Körper $\mathbb{C}$ gilt die (zunächst abenteuerlich anmutende) Beziehung $i^2 = -1$, was natürlich nur deshalb denkbar sein kann, weil wir $\mathbb{R}$ als Teilmenge von $\mathbb{C}$ auffassen, aber $i \in \mathbb{C} \setminus \mathbb{R}$ ist.

Bemerkung – Bezeichnung. (*komplexe Konjugation, Betrag*)

1. Jede komplexe Zahl α ist Summe $\alpha = a + bi$ mit eindeutig bestimmten reellen Zahlen a und b. $\mathrm{Re}(\alpha) := a$ heißt *Realteil* und $\mathrm{Im}(\alpha) := b$ *Imaginärteil* von α. Dadurch und durch die Bedingung $i^2 = -1$ lässt sich der Körper $\mathbb{C}$ „im Wesentlichen" eindeutig charakterisieren; wir hätten uns also die mühsame elementweise Konstruktion ersparen können, wäre nur von vornherein klar gewesen, dass überhaupt ein Körper mit den eben angegebenen Eigenschaften existiert.
2. Die durch $\alpha \mapsto \overline{\alpha}$ gegebene Abbildung $\mathbb{C} \to \mathbb{C}$, die α auf die komplexe Zahl $\overline{\alpha} := \mathrm{Re}(\alpha) - \mathrm{Im}(\alpha)\cdot i$ abbildet, heißt *komplexe Konjugation.* Sie ist ein Ringhomomorphismus von $\mathbb{C}$ in sich, dessen Quadrat die Identität ergibt. Für eine beliebige komplexe Zahl α gilt
$$\alpha + \overline{\alpha} = 2\cdot\mathrm{Re}(\alpha)\,, \quad \alpha - \overline{\alpha} = 2i\cdot\mathrm{Im}(\alpha),$$
und die Bedingung $\alpha = \overline{\alpha}$ ist äquivalent zu $\alpha \in \mathbb{R}$.
3. Die reelle Zahl $|\alpha| := \sqrt{\alpha\cdot\overline{\alpha}} = \sqrt{\mathrm{Re}(\alpha)^2 + \mathrm{Im}(\alpha)^2} \geq 0$ heißt *Betrag* von α. Die Bedingung $|\alpha| = 0$ ist äquivalent zu $\alpha = 0$, und nach 2. gilt allgemein $|\alpha\cdot\beta| = |\alpha|\cdot|\beta|$ für $\alpha, \beta \in \mathbb{C}$.

Den Beweis dieser trivialen Eigenschaften schreiben wir nicht auf.

Satz. (*Fundamentalsatz der Algebra*) 1/2/8

Sind $\alpha_0, \ldots, \alpha_n \in \mathbb{C}$ komplexe Zahlen, $n > 0$ und $\alpha_n \neq 0$, so existiert eine Zahl $x \in \mathbb{C}$ mit $\alpha_0 + \alpha_1 x + \ldots + \alpha_n x^n = 0$.

Dieser erstaunliche Satz wird (trotz seines Namens) hier nur zitiert; seine Beweise benutzen nichttriviale Eigenschaften der reellen Zahlen und sind auch in der Analysis gut aufgehoben.

Für den Körper der reellen Zahlen gilt die entsprechende Aussage nicht, da in $\mathbb{R}$ z.B. keine Zahl x mit $1 + x^2 = 0$ existiert.

Wir entnehmen aus dem Satz 1/2/7, dass sich der Körper $\mathbb{C}$ nicht durch eine analoge Konstruktion zu einem neuen Körper erweitern lässt (denn -1 ist ein Quadrat in $\mathbb{C}$).

In der Algebra werden dennoch interessante Erweiterungen des Körpers $\mathbb{C}$ untersucht, die z.B. nicht mehr kommutativ sind.

Polynome

Wir fixieren einen kommutativen Ring R, der hier gelegentlich *Grundring* genannt wird.

Polynome wurden ursprünglich bedenkenlos als Vielfachensummen der Potenzen X^n einer (nicht weiter erklärten) *Unbestimmten* X angesehen. Der folgende Satz ist die Existenzaussage für den anschließend definierten Begriff;

Wenn Sie sich das Rechnen mit „Unbestimmten" zutrauen und diesen Standpunkt übernehmen wollen, dann genügt es, sich lediglich die nachfolgenden Bezeichnungen anzueignen.

wer die Existenz eines „unbestimmten Elements" für selbstverständlich hält, kann ihn auch überspringen.

Satz. *Die Menge* $R^{[1]} := \{(a_i)_{i\in\mathbb{N}} \mid a_i \in R,\ \text{fast alle } a_i = 0\}$ *der Folgen im Ring* R, *deren Glieder* a_i *bis auf endlich viele verschwinden, bildet mit den Operationen* 1/2/9

$$(a_i)_{i\in\mathbb{N}} + (b_i)_{i\in\mathbb{N}} := (a_i + b_i)_{i\in\mathbb{N}}\,,$$

$$(a_i)_{i\in\mathbb{N}} \cdot (b_i)_{i\in\mathbb{N}} := (c_i)_{i\in\mathbb{N}} \quad \textit{mit} \quad c_i = \textstyle\sum_{j=0}^{i} a_j b_{i-j}$$

einen kommutativen Ring. Die auch mit 0 *bezeichnete Nullfolge* $(0,0,\ldots)$ *ist das neutrale Element der Addition, die auch mit* 1 *bezeichnete Folge* $(1,0,0,\ldots)$ *das neutrale Element der Multiplikation in* $R^{[1]}$.
Weiter gilt: Es gibt einen injektiven Ringhomomorphismus

$$\iota : R \to R^{[1]}, \quad \iota(a) := (a,0,0,\ldots).$$

Mittels ι *wird* R *künftig als Unterring von* $R^{[1]}$ *angesehen, insbesondere also* a *mit* $\iota(a)$ *identifiziert.*

Beweis. Wir überprüfen beispielsweise das Assoziativgesetz der Multiplikation: Sind $(a_i)_{i\in\mathbb{N}}$, $(b_i)_{i\in\mathbb{N}}$ und $(c_i)_{i\in\mathbb{N}}$ aus $R^{[1]}$, so folgt definitionsgemäß

So langweilige Beweise sollen die Ausnahme bleiben. Echte Ideen sind auch für die Verifikation der verbleibenden Eigenschaften nicht erforderlich.

$$(a_i)_{i\in\mathbb{N}} \cdot (b_i)_{i\in\mathbb{N}} = (d_i)_{i\in\mathbb{N}} \ \text{mit}\ d_i = \textstyle\sum_{j=0}^{i} a_j b_{i-j} \ \text{sowie}$$
$$(d_i)_{i\in\mathbb{N}} \cdot (c_i)_{i\in\mathbb{N}} = (e_i)_{i\in\mathbb{N}} \ \text{mit}$$
$$\begin{aligned} e_k &= \textstyle\sum_{i=0}^{k} d_i c_{k-i} = \sum_{i=0}^{k} \big(\sum_{j=0}^{i} a_j b_{i-j}\big) c_{k-i} \\ &= \textstyle\sum_{i=0}^{k} \sum_{j=0}^{i} a_j b_{i-j} c_{k-i} = \sum_{p,q,r\in\mathbb{N},\, p+q+r=k} a_p b_q c_r . \end{aligned}$$

Entsprechend ist

$$(b_i)_{i\in\mathbb{N}} \cdot (c_i)_{i\in\mathbb{N}} = (f_i)_{i\in\mathbb{N}} \ \text{mit}\ f_l = \textstyle\sum_{j=0}^{l} b_j c_{l-j} \ \text{sowie}$$
$$(a_i)_{i\in\mathbb{N}} \cdot (f_i)_{i\in\mathbb{N}} = (g_i)_{i\in\mathbb{N}} \ \text{mit}$$
$$\begin{aligned} g_k &= \textstyle\sum_{i=0}^{k} a_i f_{k-i} = \sum_{i=0}^{k} a_i \sum_{j=0}^{k-i} b_j c_{k-i-j} \\ &= \textstyle\sum_{i=0}^{k} \sum_{j=0}^{k-i} a_i b_j c_{k-i-j} = \sum_{p,q,r\in\mathbb{N},\, p+q+r=k} a_p b_q c_r \end{aligned}$$

und daher

$$\begin{aligned} \big((a_i)_{i\in\mathbb{N}} \cdot (b_i)_{i\in\mathbb{N}}\big) \cdot (c_i)_{i\in\mathbb{N}} &= (e_i)_{i\in\mathbb{N}} = (g_i)_{i\in\mathbb{N}} \\ &= (a_i)_{i\in\mathbb{N}} \cdot \big((b_i)_{i\in\mathbb{N}} \cdot (c_i)_{i\in\mathbb{N}}\big). \end{aligned}$$ ❑

Korollar – Definition. (*Polynomring*) 1/2/10

Der im Satz 1/2/9 konstruierte Erweiterungsring $R^{[1]}$ von R heißt *Polynomring*, seine Elemente *Polynome*. $R^{[1]}$ *enthält ein Element* X, *so dass für alle* $f \in R^{[1]}$ *gilt:*

Diese Eigenschaften sind es, die wir beim Rechnen mit Polynomen tatsächlich verwenden.

(1) *Es existieren* $n \in \mathbb{N}$ *und* $a_i \in R$, $0 \le i \le n$, *für die* $f = a_0 + a_1X + a_2X^2 + \ldots + a_nX^n$ *ist.*

(2) *Setzen wir unter* (1) *noch* $a_i = 0$ *für* $i > n$, *so ist die Folge* $(a_i)_{i\in\mathbb{N}}$ *durch* f *eindeutig bestimmt*, sie heißt *Koeffizientenfolge* von f bezüglich X.

Ein Ringelement X, das für alle Polynome $f \in R^{[1]}$ die Eigenschaften (1), (2) erfüllt, heißt eine *Unbestimmte*; wir verwenden dann auch die Bezeichnung $R^{[1]} =: R[X]$ (gelesen als R *adjungiert* X) und nennen $R[X]$ (genauer: das Paar $(R^{[1]}, X)$) den *Polynomring über* R *in der Unbestimmten* X.

Beweis. Für $r \in R$ und $(c_i)_{i\in\mathbb{N}} \in R^{[1]}$ ist (gemäß der Identifikation der Elemente von R und entsprechender Folgen aus $R^{[1]}$ mittels ι) offenbar $r \cdot (c_i)_{i\in\mathbb{N}} = (rc_i)_{i\in\mathbb{N}}$. Bezeichnet X die Folge mit dem Eintrag 1 an der Position 1 und 0 an allen anderen, d.h. $X = (0,1,0,0,\ldots)$, so gilt

$$X^i = (\underbrace{0, \ldots, 0}_{i}, 1, 0, \ldots)\,.$$

Wir wählen $f = (a_i)_{i\in\mathbb{N}} \in R^{[1]}$ beliebig und erhalten

$$f = \sum_{i\in\mathbb{N}} (\underbrace{0, \ldots, 0}_{i}, a_i, 0, \ldots) = \sum_{i\in\mathbb{N}} a_i X^i\,,$$

wobei die angegebenen unendlichen Summen nur endlich viele von 0 verschiedene Summanden enthalten und daher korrekt definiert sind. ❑

Werden Polynome $f \in R[X]$ von nun an gelegentlich als (formal unendliche) Summen $f = \sum_{i\in\mathbb{N}} a_i X^i$ mit $a_i \in R$ geschrieben, so ist dabei stets angenommen $a_i = 0$ für fast alle i (die Summe haben wir ohnehin nur für diesen Fall erklärt, vgl. 1/1/1).

Bemerkung. (*Prinzip des Koeffizientenvergleichs*)
Sind a_i, $b_i \in R$ und $f = \sum_{i\in\mathbb{N}} a_i X^i$, $g = \sum_{i\in\mathbb{N}} b_i X^i$ Polynome aus $R[X]$, so gilt genau dann $f = g$, wenn $a_i = b_i$ für alle $i \in \mathbb{N}$.

Bezeichnungen.

Vorsicht! Die Bezeichnungen *Term* und *Monom* werden in der Literatur nicht einheitlich verwendet.

(1) Ein Polynom $f = a_j X^j \in R[X]$ mit $j \in \mathbb{N}$, $a_j \in R \setminus \{0\}$ heißt *Term*; ist insbesondere $a_j = 1$, so sprechen wir auch von einem *Monom*.

(2) Für ein Polynom $f = a_0 + a_1X + a_2X^2 + \ldots + a_nX^n$ aus $R[X]$ mit $a_n \neq 0$ nennen wir $n =: \deg_X(f)$ (nachlässig auch $\deg(f)$) den *Grad des Polynoms* f; dem Nullpolynom wird ein (von nun an festgelegtes) Symbol $\deg_X(0) := -\infty \notin \mathbb{N}$ zugeordnet.

Bezüglich der nahe liegend definierten Ordnungsrelation auf $\{-\infty\} \cup \mathbb{N}$ ist $\deg(0) < \deg(f)$ für alle Polynome $f \neq 0$.
Die Bedingung $\deg(f) \leq 0$ ist äquivalent zu $f \in R$; in diesem Fall heißt das Polynom f *konstant.*

Gemeint ist hier natürlich die Ordnung auf $\{-\infty\} \cup \mathbb{N}$, die durch $-\infty < a$ für $a \in \mathbb{N}$ die vertraute Anordnung der natürlichen Zahlen erweitert.

Lemma. *Sind* f, $g \in R[X]$ *Polynome, dann gilt*:

Auf diesem Lemma basieren zahlreiche Beweise für Eigenschaften von Polynomen.

(1) $\deg_X(f + g) \leq \max\{\deg_X(f), \deg_X(g)\}$.
Ist $\deg_X(f) \neq \deg_X(g)$, *so besteht Gleichheit.*

(2) *Sind* f, $g \neq 0$, *so ist* $\deg_X(f\cdot g) \leq \deg_X(f) + \deg_X(g)$.
Für einen Integritätsbereich R *besteht Gleichheit.*

Beweis. (1) ergibt sich daraus, dass im Fall $\deg_X(f) > \deg_X(g)$ der höchste Koeffizient von $f + g$ mit dem von f übereinstimmt. Zum Beweis von (2) bemerken wir, dass der höchste möglicherweise von 0 verschiedene Koeffizient des Produkts $f\cdot g$ beider Polynome $f = a_0 + a_1X + \ldots + a_nX^n$ und $g = b_0 + b_1X + \ldots + b_mX^m$ der Koeffizient a_nb_m von X^{n+m} ist. Für einen Integritätsbereich R folgt weiter aus $a_nb_m = 0$, dass eines der Ringelemente a_n oder b_m selbst 0 sein muss, daher $a_nb_m \neq 0$, falls $n = \deg(f)$ und $m = \deg(g)$. ❑

Satz. *Ist* R *ein Integritätsbereich, dann ist der Polynomring* $R[X]$ *über* R *in der Unbestimmten* X *ebenfalls ein Integritätsbereich.* 1/2/11

Beweis. Wir wählen f, $g \in R[X]$ mit $0 = f\cdot g$. Es folgt $\deg_X(f\cdot g) = -\infty$. Ist keines der Polynome f, g das Nullpolynom, so ergibt sich nach dem Lemma $\deg_X(f\cdot g) = \deg_X(f) + \deg_X(g) \in \mathbb{N}$, $\lightning$. ❑

Algebren

Wir zeigen nun, wie die Vorstellung von dem Begriff der Unbestimmten durch die Forderung präzisiert werden kann, dass sich in eine polynomiale Identität ein beliebiges Element „einsetzen“ lässt.

Definition. (*R-Algebra*) 1/2/12

Q sei ein Ring, $\varphi : R \to Q$ ein Homomorphismus, für den die Bildelemente mit denen von Q kommutieren, d.h.

$$\varphi(r)\cdot q = q\cdot\varphi(r) \quad \text{für alle } r \in R \text{ und alle } q \in Q.$$

Dann heißt das Paar (Q, φ) eine *Algebra über* R, kurz *R-Algebra.*

Besteht kein Zweifel über den infrage kommenden Homomorphismus φ, so lassen wir ihn in den Notationen einfach weg und sprechen von der R-Algebra Q. Für $\varphi(r)$ schreiben wir kurz r, obwohl wir uns bewusst sind, dass hier im Allgemeinen ein Element eines anderen Ringes vorliegt. φ heißt auch *Struktur(homo)morphismus* der R-Algebra Q.

Was hier steht, ist wenig spektakulär. Sie haben z.B. die $\mathbb{Z}$-Algebrastruktur der reellen Zahlen schon immer verwendet, wenn Sie reelle Zahlen mit ganzen multiplizierten.

Beispiele.

1. Jeder Ring ist auf eindeutige Weise eine $\mathbb{Z}$-Algebra. Denn ist $\varphi : \mathbb{Z} \to Q$ ein Ringhomomorphismus, so muss notwendigerweise $\varphi(1) = 1_Q$ das Einselement von Q sein. Dann ist
$$\varphi(n) = \varphi(\underbrace{1 + \ldots + 1}_{n}) = \underbrace{\varphi(1) + \ldots + \varphi(1)}_{n} =: n \cdot 1_Q$$
und $(-n)\cdot 1_Q := -(n\cdot 1_Q)$ das Bild von $-n$ für $n \in \mathbb{N} \setminus \{0\}$. Weiter muss $0_Q =: 0 \cdot 1_Q$ das Bild der ganzen Zahl 0 sein. Existiert überhaupt ein Homomorphismus $\mathbb{Z} \to Q$, dann ist er durch
$$\mathbb{Z} \to Q\,, \quad m \mapsto m \cdot 1_Q \quad \text{für} \quad m \in \mathbb{Z}$$
eindeutig beschrieben. Umgekehrt ist leicht zu sehen, dass die Abbildung $m \mapsto m\cdot 1_Q$ stets ein Homomorphismus ist. Insbesondere sind die Körper $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$ auf eindeutige Weise $\mathbb{Z}$-Algebren.
2. $\mathbb{R}$ ist eine $\mathbb{Q}$ Algebra mittels der Inklusionsabbildung $\mathbb{Q} \to \mathbb{R}$.
3. Zusammen mit dem Homomorphismus, der das Ringelement $r \in R$ auf das ebenso bezeichnete konstante Polynom r abbildet, ist $R[X]$ eine R-Algebra. Sie wird von nun an immer mit diesem Strukturmorphismus versehen und heißt *Polynomalgebra über R in der Unbestimmten X.*

Definition. (*Homomorphismus von Algebren*) 1/2/13

Wir betrachten R-Algebren (Q, φ) und (Q', φ'). Ein *R-Algebrahomomorphismus* (auch *R-Homomorphismus*) $(Q, \varphi) \to (Q', \varphi')$ ist ein Ringhomomorphismus $\varPhi : Q \to Q'$ mit $\varPhi\cdot\varphi = \varphi'$. Das bedeutet, $\varPhi$ bildet mit den Strukturmorphismen ein kommutatives Diagramm:

Ein Algebrahomomorphismus ist also ein Ringhomomorphismus, der mit den gegebenen Strukturmorphismen verträglich ist.

$$\begin{tikzcd} Q \arrow[rr, "\varPhi"] & & Q' \\ & R \arrow[ul, "\varphi"] \arrow[ur, "\varphi'"'] & \end{tikzcd}$$

Für jede R-Algebra Q ist die Identität id_Q ein R-Homomorphismus, und das Produkt von R-Homomorphismen ist wieder ein R-Homomorphismus. $\varPhi$ heißt *Isomorphismus von R-Algebren* (auch *R-Isomorphismus*), wenn ein zweiseitig inverser R-Homomorphismus existiert, d.h. ein R-Homomorphismus $(Q', \varphi') \to (Q, \varphi)$, gegeben durch $\varPsi : Q' \to Q$, für den $\varPsi \cdot \varPhi = \mathrm{id}_Q$

und $\Phi \cdot \Psi = \mathrm{id}_{Q'}$ ist. Dies ist offenbar gleich bedeutend damit, dass der R-Homomorphismus Φ bijektiv ist.

Beliebige Ringhomomorphismen $S \to T$ sind stets auch $\mathbb{Z}$-Homomorphismen mit den eindeutig bestimmten Strukturen der Ringe S und T als Algebren über $\mathbb{Z}$.

Satz. (*Universaleigenschaft der Polynomalgebra*) 1/2/14

Q sei eine R-Algebra, $x \in Q$ und $R[X]$ die Polynomalgebra über R in der Unbestimmten X. Dann existiert ein eindeutig bestimmter Homomorphismus $\Phi : R[X] \to Q$ von R-Algebren mit $\Phi(X) = x$.

Dieser Satz gab Anlass, den Begriff der *Algebra* hier einzuführen.

Beweis. Die Eindeutigkeit des Homomorphismus Φ folgt aus

$$\begin{aligned}\Phi(a_0 + a_1X + a_2X^2 + \ldots + a_nX^n)&\\ &= a_0\Phi(1) + a_1\Phi(X) + a_2\Phi(X^2) + \ldots + a_n\Phi(X^n)\\ &= a_0 + a_1\Phi(X) + a_2\Phi(X)^2 + \ldots + a_n\Phi(X)^n\\ &= a_0 + a_1x + a_2x^2 + \ldots + a_nx^n.\end{aligned}$$

Zum Nachweis der Existenz ordnen wir dem Polynom $\sum_{i\in\mathbb{N}} a_iX^i \in R[X]$ die Koeffizientenfolge $(a_i)_{i\in\mathbb{N}}$ und dieser das Ringelement $\sum_{i\in\mathbb{N}} a_ix^i \in Q$ zu. Leicht ist nachzurechnen, dass dadurch ein R-Homomorphismus definiert wird, der X auf x abbildet. ❑

Der im Satz angegebene Homomorphismus heißt *Einsetzungshomomorphismus* (auch *Ersetzungshomomorphismus*), da er das Polynom $f = a_0 + a_1X + a_2X^2 + \ldots + a_nX^n \in R[X]$ mit $a_i \in R$ auf $f(x) := a_0 + a_1x + a_2x^2 + \ldots + a_nx^n \in Q$ abbildet.

Warnung. (*Polynome sind keine Funktionen*)

… ein beliebtes Missverständnis.

Als Beispiel betrachten wir die Abbildung $\Phi_f : \mathbb{F}_2 \to \mathbb{F}_2$, die durch ein Polynom $f \in \mathbb{F}_2[X]$ gegeben wird: $\Phi_f(a) := f(a)$, wobei $f(a)$ das Bild von f beim Einsetzungshomomorphismus $\mathbb{F}_2[X] \to \mathbb{F}_2$ mit $X \mapsto a$ bezeichnet. Ist z.B. $f = 1 + X + X^2 \in \mathbb{F}_2[X]$, dann ist die Abbildung

$$\Phi_f : \mathbb{F}_2 \to \mathbb{F}_2, \quad x \mapsto 1 + x + x^2$$

offensichtlich konstant (sie bildet jedes Element auf 1 ab). Für das konstante Polynom $g = 1 \in \mathbb{F}_2[X]$ gilt nun $\Phi_f = \Phi_g$. Ein Polynom ist also im Allgemeinen nicht durch die Funktion bestimmt, die wir durch Einsetzen von Elementen des Grundringes daraus bilden können. Wie sich später herausstellt, tritt dieser Effekt über einem unendlichen Grundkörper nicht mehr auf, so dass die manchmal für reelle Zahlen verwendete Interpretation von Polynomen als Funktionen eine gewisse Rechtfertigung erfährt. ❑

Satz. (*Eindeutigkeit der Polynomalgebra*) 1/2/15

P, P' seien Algebren über dem Grundring R sowie $X \in P$ und $X' \in P'$. Wir setzen voraus, dass für beide Paare (P, X) und (P', X') die folgende Universaleigenschaft *erfüllt ist:*

Für alle R-Algebren Q und alle Elemente $x \in Q$ existiert genau ein R-Homomorphismus $\Psi : P \to Q$ mit $\Psi(X) = x$ bzw. genau ein R-Homomorphismus $\Psi' : P' \to Q$ mit $\Psi'(X') = x$.

Dann ist der eindeutig bestimmte R-Homomorphismus $P \to P'$ mit $X \mapsto X'$ ein Isomorphismus von R-Algebren.

Universaleigenschaften charakterisieren Objekte bis auf einen eindeutig bestimmten Isomorphismus; diese (scheinbar) etwas vage Formulierung wird im vorliegenden Fall durch den angegebenen Satz präzisiert.

Beweis. Sind $\varPhi : P \to P'$ und $\varPhi' : P' \to P$ die eindeutig bestimmten Homomorphismen mit $X \mapsto X'$ bzw. $X' \mapsto X$, so ist $\varGamma := \varPhi' \cdot \varPhi : P \to P$ ein R-Homomorphismus mit $\varGamma(X) = X$ und durch diese Eigenschaft ebenfalls eindeutig bestimmt:

$$\begin{tikzcd}
& P' \arrow[dr, "\varPhi'"] & \\
P \arrow[ur, "\varPhi"] \arrow[rr, dotted, "\varGamma"] & & P \\
& R \arrow[ul] \arrow[ur] \arrow[uu] &
\end{tikzcd}$$

Da auch die Identität $\mathrm{id}_P : P \to P$ das Element $X \in P$ auf X abbildet, muss $\mathrm{id}_P = \varGamma$ sein. Entsprechend ergibt sich $\mathrm{id}_{P'} = \varPhi{\cdot}\varPhi'$, folglich ist $\varPhi$ ein Isomorphismus. ❑

Polynome in mehreren Unbestimmten 1/2/16

Analog zu 1/2/9 werden nun auf nahe liegende Weise Polynomringe in mehreren Unbestimmten definiert. Wieder ist die explizite Konstruktion für das Rechnen unwesentlich; die entscheidenden Eigenschaften sind in den nachfolgenden Bemerkungen zusammengefasst.

Wir erinnern daran, dass die Indexmenge $\mathbb{N}^n$ mit der komponentenweisen Addition ein Monoid bildet; neutrales Element ist $(0, \ldots, 0)$.

$n \geq 1$ bezeichnet eine natürliche Zahl. Wir setzen

$$R^{[n]} := \{(a_\nu)_{\nu \in \mathbb{N}^n} \mid a_\nu \in R,\ \text{fast alle } a_\nu = 0\}.$$

Dann ist $R^{[n]}$ mit den folgenden Operationen ein kommutativer Ring:

$$(a_\nu)_{\nu \in \mathbb{N}^n} + (b_\nu)_{\nu \in \mathbb{N}^n} := (a_\nu + b_\nu)_{\nu \in \mathbb{N}^n}\,,$$
$$(a_\nu)_{\nu \in \mathbb{N}^n} \cdot (b_\nu)_{\nu \in \mathbb{N}^n} := (c_\nu)_{\nu \in \mathbb{N}^n}\,, \qquad c_\nu := \textstyle\sum_{\lambda,\mu \in \mathbb{N}^n,\ \lambda+\mu=\nu} a_\lambda b_\mu .$$

Durch den Ringhomomorphismus $\iota : R \to R^{[n]}$, der $r \in R$ auf $(a_\nu)_{\nu \in \mathbb{N}^n}$ mit $a_{(0,\ldots,0)} = r$ und $a_\nu = 0$ für $\nu \neq (0, \ldots, 0)$ abbildet, erhält $R^{[n]}$ die Struktur einer R-Algebra. Sie heißt *Polynomalgebra in* n *Unbestimmten* über dem Ring R, ihre Elemente werden wieder Polynome genannt.

Nun sei $1 \leq i \leq n$. Wählen wir X_i als das Ringelement $(a_\nu)_{\nu \in \mathbb{N}^n}$ mit

$$a_\nu = \begin{cases} 1 & \text{für } \nu = (\underbrace{0, \ldots, 0, 1}_{i}, 0, \ldots, 0) \\ 0 & \text{sonst,} \end{cases}$$

dann sind die folgenden Eigenschaften erfüllt.

Bezeichnungen – Bemerkungen.

(1) Die Elemente von $R^{[n]}$ sind Vielfachensummen von Potenzprodukten $X_1^{\nu_1} \cdot \ldots \cdot X_n^{\nu_n}$ (*Monomen*) mit Koeffizienten aus R.
Wir setzen $\boldsymbol{X} := (X_1, \ldots, X_n)$ und $\boldsymbol{X}^\nu := X_1^{\nu_1} \cdot \ldots \cdot X_n^{\nu_n}$ für $\nu = (\nu_1, \ldots, \nu_n) \in \mathbb{N}^n$. Dann ist jedes Polynom $f \in R^{[n]}$ von der Gestalt $f = \sum_{\nu \in \mathbb{N}^n} a_\nu \boldsymbol{X}^\nu$ ($a_\nu = 0$ für fast alle $\nu \in \mathbb{N}^n$), und die Koeffizienten $a_\nu \in R$ sind durch f eindeutig bestimmt (*Koeffizientenfamilie von* f *bezüglich* $\boldsymbol{X}$).
Ein n-Tupel $\boldsymbol{X} = (X_1, \ldots, X_n)$ von Polynomen aus $R^{[n]}$, das diese Eigenschaft besitzt, heißt Tupel von Unbestimmten. Wir schreiben dann auch $R^{[n]} =: R[X_1, \ldots, X_n] = R[\boldsymbol{X}]$ und nennen das Paar $(R^{[n]}, \boldsymbol{X})$ Polynomalgebra über R in den Unbestimmten $\boldsymbol{X}$.

Natürlich erhalten wir für $n = 1$ den schon bekannten Fall einer einzigen Unbestimmten, vgl. 1/2/9 ff.

(2) Ein Polynom $a_\nu X^\nu$ mit $a_\nu \in R \setminus \{0\}$ heißt *Term*; jedes Polynom $f \neq 0$ ist Summe von Termen.

(3) Für $f \in R[X_1, \ldots, X_n] \setminus \{0\}$ setzen wir

$$\deg_{\boldsymbol{X}}(f) = \deg_{(X_1, \ldots, X_n)}(f) := \max\{|\nu| \mid a_\nu \neq 0\},$$

wobei $|\nu| := \nu_1 + \ldots + \nu_n$ ist. $\deg_{\boldsymbol{X}}(f)$ heißt *vollständiger Grad* von f bezüglich $\boldsymbol{X} = (X_1, \ldots, X_n)$. Dem Nullpolynom ordnen wir als vollständigen Grad das Symbol $\deg_{\boldsymbol{X}}(0) := -\infty$ zu.
Ist $\deg_{\boldsymbol{X}}(f) \leq 0$, so heißt f wieder *konstant* (vgl. 1/2/10). Im Fall $\deg_{\boldsymbol{X}}(f) = 1$ wird f *linear* genannt.

Durch die angegebene Konstruktion entstehen aus dem kommutativen Ring R stets wieder kommutative Ringe $R^{[n]}$, so dass wir bei der Formulierung einer entsprechenden Universaleigenschaft in dieser Hinsicht vorsichtig sein müssen. Die folgende Eigenschaft reicht aus, die Polynomalgebra bis auf Isomorphie zu charakterisieren.

Satz. (*Universaleigenschaft von* $R[X_1, \ldots, X_n]$) 1/2/17

$R[X_1, \ldots, X_n]$ sei der Polynomring in den Unbestimmten $(X_1, \ldots, X_n)$ und Q eine R-Algebra sowie $x_1, \ldots, x_n \in Q$ mit $x_i x_j = x_j x_i$ für $i, j \in \{1, \ldots, n\}$. Dann existiert genau ein R-Homomorphismus $\Phi : R[X_1, \ldots, X_n] \to Q$ mit $\Phi(X_i) = x_i$ für $i = 1, \ldots, n$.
Die Abbildung Φ wird wieder *Einsetzungshomomorphismus*, auch *Ersetzungshomomorphismus* genannt.

Beweis. Es kann analog zum Satz 1/2/14 geschlossen werden. ❏

Alternativ bietet sich ein Induktionsschluss an.

Bemerkung. (*Adjunktion von Elementen*) 1/2/18

Der Einsetzungshomomorphismus gibt uns eine weitere Möglichkeit zur Konstruktion von Ringen. Dazu betrachten wir eine kommutative R-Algebra Q und $x_1, \ldots x_n \in Q$. Ist $f : R[X_1, \ldots, X_n] \to Q$ der durch $X_i \mapsto x_i$ bestimmte Einsetzungshomomorphismus, so bezeichnen wir den Unterring $\mathrm{im}(f)$ von Q mit $R[x_1, \ldots, x_n]$ und sagen, er sei durch *Adjunktion von* $x_1, \ldots, x_n$ zum Ring R entstanden; zusammen mit dem durch $R \to Q$ induzierten Strukturmorphismus heißt $R[x_1, \ldots, x_n]$ die *durch* $x_1, \ldots, x_n$ *erzeugte* R*-Algebra*. Beispielsweise gilt:

Hier als besonders einfaches Beispiel $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$.

1. In der $\mathbb{Z}$-Algebra $\mathbb{C}$ ist $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ (Ring der *ganzen gaußschen Zahlen*).
2. In der $\mathbb{Q}$-Algebra $\mathbb{R}$ ist
$\mathbb{Q}[\sqrt{2}, \sqrt{3}] = \mathbb{Q}[\sqrt{2} - \sqrt{3}] = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q}\}$.

Im ersten Fall ist Gleichheit leicht zu sehen, denn indem die Potenzen von i nach geraden und ungeraden Exponenten sortiert werden. Der andere Fall ist etwas interessanter und verbleibt als Übungsaufgabe.

Grundbegriffe der Teilbarkeitslehre 1/2/19

Wer sich mit Teilbarkeitseigenschaften ganzer Zahlen gut auskennt, wird diesen Abschnitt als recht trivial empfinden. Die Verallgemeinerung der Teilbarkeitslehre für $\mathbb{Z}$ auf eine größere Klasse von Ringen erweist sich später bei der Untersuchung von Polynomen als nützlich.

Wir fixieren einen zunächst beliebigen, kommutativen Integritätsbereich R.

Definition. (*Teilbarkeit, Assoziiertheit und Einheiten*)

Teilbarkeit wird hier so definiert, wie das anschaulich auch schon in der Schule geschah. Der Begriff der Einheit abstrahiert davon, dass in $\mathbb{Z}$ die Multiplikation mit ± 1 nichts an Teilbarkeitseigenschaften ändert.

(1) Sind $f, g \in R$ und existiert ein $q \in R$ mit $f = q \cdot g$, so sagen wir, g ist ein *Teiler* von f (kurz auch g *teilt* f) und schreiben dafür $g|f$. Ist diese Bedingung nicht erfüllt, so wird dafür das Symbol $g \nmid f$ verwendet. Falls $g|f$ und $f \nmid g$, so heißt g *echter Teiler* von f.

(2) $f, g \in R$ heißen *assoziiert,* wenn sie sich gegenseitig teilen, d.h. wenn $f|g$ und $g|f$. Wir schreiben dafür $f \sim g$.

(3) Ist $e \in R$ ein Teiler von 1, so heißt e eine *Einheit.* Da 1 jedes Element teilt, ist diese Bedingung äquivalent zu $e \sim 1$.

Teilbarkeit im zuvor angegebenen Sinn erlaubt es, in bestimmten Fällen einen Quotienten einzuführen. Für $f = q \cdot g$, $g \neq 0$ ist q im Integritätsbereich R durch f und g eindeutig bestimmt und wird gelegentlich mit $\dfrac{f}{g}$ oder f/g bezeichnet. Offensichtlich sind die Eigenschaften dieses Symbols mit denen des (definitionsgemäß ganz verschiedenen) verträglich, das in 1/2/6 ein *Bruch* genannt wurde.

Diese Anmerkung ist wohl etwas pedantisch; Sie hätten die Bezeichnung vermutlich ohnehin verwendet ...

Beispiele.

1. In $\mathbb{Z}$ ist 5 ein echter Teiler von -10, jedoch ist $-10 \sim 10$ und damit 10 ein Teiler, aber kein echter Teiler von -10.
2. Im Ring $\mathbb{R}[X]$ der Polynome in einer Unbestimmten X (vgl. 1/2/10) gilt $(X+1)|(X^2-1)$, und $X+1$ ist ein echter Teiler von X^2-1. Das Polynom $2X^2-2$ ist dagegen zu X^2-1 assoziiert und damit kein echter Teiler.

Satz. 1/2/20

(1) *Assoziiertheit ist eine Äquivalenzrelation auf* R.

(2) *Die Einheiten in* R *bilden mit der Ringmultiplikation eine Gruppe* R^*.

(3) $f \sim g$ *ist gleichbedeutend zur Existenz einer Einheit* $e \in R^*$, *für die* $f = e \cdot g$ *gilt.*

(4) f *sei Teiler von* g, *so ist* f *genau dann ein echter Teiler von* g, *wenn* f *und* g *nicht assoziiert sind.*

Im Gegensatz zum Ring $\mathbb{Z}$, für den echte Teiler als Teiler mit kleinerem Absolutbetrag definiert werden können, müssen wir uns im vorliegenden allgemeinen Fall auf eine Definition mittels Eigenschaften der Teilbarkeit beschränken.

Beweis. (1) ergibt sich unmittelbar aus der Definition der Assoziiertheit. Zum Beweis von (2) zeigen wir zunächst, dass die Multiplikation des Ringes R eine Einschränkung auf R^* besitzt: Sind $e, e' \in R^*$, so existieren definitionsgemäß $q, q' \in R$ mit $1 = qe$ und $1 = q'e'$. Multiplizieren wir diese Gleichungen miteinander, so folgt $1 = (qe) \cdot (q'e') = (qq') \cdot (ee')$, also ist ee' ein Teiler von 1 und daher $ee' \in R^*$. $1 \in R^*$ ist neutrales Element, die Assoziativität der Operation folgt aus dem Assoziativgesetz für R, und die Existenz von inversen Elementen ist Bestandteil der Definition.
(3), (4) verbleiben als Übungsaufgaben. ❑

Beispiele.

1. Im Polynomring $R = K[X]$ über dem Körper K ist $R^* = K \setminus \{0\}$ die Menge der Polynome vom Grad 0, denn aus $1 = q \cdot e$ folgt $q \neq 0$, $e \neq 0$ und $\deg_X(q) + \deg_X(e) = 0$.
   Für $K[X_1, \ldots, X_n]$ besteht die Gruppe der Einheiten entsprechend aus den Polynomen vom vollständigen Grad 0, ist also ebenfalls $K \setminus \{0\}$.
2. $\mathbb{Z}^* = \{1, -1\}$.
3. Für einen Körper K ist $K^* = K \setminus \{0\}$.

4. $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ bezeichne den Ring der ganzen gaußschen Zahlen (vgl. 1/2/18). Dann ist $\mathbb{Z}[i]^* = \{1, -1, i, -i\}$.

Der Nachweis unter 4. erfordert eine kleine Rechnung.

Definition. (*irreduzible Elemente*) 1/2/21

$p \in R \setminus \{0\}$ heißt *irreduzibel* (auch *unzerlegbar*), wenn p selbst keine Einheit ist und alle echten Teiler von p Einheiten sind.

Hier ist etwas Vorsicht geboten. Unter so allgemeinen Voraussetzungen dürfen wir den Begriff des irreduziblen Elements nicht mit dem des Primelements verwechseln.

Beispiele.

1. In $\mathbb{Z}$ sind die irreduziblen Elemente genau die zu Primzahlen assoziierten (vgl. 1/2/28).
2. Im Polynomring $K[X]$ über einem Integritätsbereich K ist das Polynom X irreduzibel.
3. In einem Körper gibt es keine irreduziblen Elemente, denn alle von 0 verschiedenen Elemente sind Einheiten.
4. In $\mathbb{R}[X]$ ist das Polynom $1 + X^2$ irreduzibel, als Element von $\mathbb{C}[X]$ ist es dagegen reduzibel: $1 + X^2 = (X + i)\cdot(X - i)$.
5. In $\mathbb{Z}[i]$ ist $1 + i$ irreduzibel, nicht jedoch $2 = (1 + i)\cdot(1 - i)$.

Die irreduziblen Polynome in $\mathbb{R}[X]$ und $\mathbb{C}[X]$ werden später angegeben.

Lemma. *Ist $p \in R \setminus \{0\}$ keine Einheit, dann sind die folgenden Eigenschaften äquivalent:*

(1) *p ist irreduzibel.*

(2) *Ist $p = f\cdot g$, so gilt $f \in R^*$ oder $g \in R^*$.*

(3) *Ist $p = f\cdot g$, so gilt $p \sim f$ oder $p \sim g$.*

Beweis. (1) $\Rightarrow$ (2): Es sei $p = f \cdot g$ und $f \notin R^*$. Dann ist voraussetzungsgemäß der Teiler f kein echter Teiler von p, also $p \sim f$. Mit der Kürzungsregel folgt aus 1/2/20 (3) leicht $g\,|1$.
(2) $\Rightarrow$ (3) ergibt sich ebenfalls aus 1/2/20 (3).
(3) $\Rightarrow$ (1): Ist f ein echter Teiler von p, so ist $p = fg$ für ein Element g von R und p nicht assoziiert zu f. Voraussetzungsgemäß muss daher $p \sim g$ sein, also existiert ein $e \in R^*$ mit $g = e\cdot p$, und aus $p = f\cdot e\cdot p$ sowie $p \neq 0$ folgt nach der Kürzungsregel $1 = f\cdot e$, daher $f \in R^*$. ❑

Mittels *Universaleigenschaften* definieren wir zwei Begriffe, die uns durch das Rechnen mit ganzen Zahlen vertraut sind.

Definition. (*größter gemeinsamer Teiler*) 1/2/22

Sind $f, g \in R$, dann heißt $d \in R$ *größter gemeinsamer Teiler* von f und g, falls

(1) $d|f$ und $d|g$;

(2) für $d' \in R$ mit $d'|f$ und $d'|g$ gilt stets $d'|d$.

Ist insbesondere 1 größter gemeinsamer Teiler von f und g, so heißen f und g *teilerfremd.*

Die Definition verwendet nur die Teilbarkeitsrelation. Allerdings wird nicht behauptet, dass stets ein größter gemeinsamer Teiler existiert.

Satz. (*Eindeutigkeit des größten gemeinsamen Teilers*) 1/2/23

Sind d_1 und d_2 größte gemeinsame Teiler von $f, g \in R$, so ist $d_1 \sim d_2$.

Ein größter gemeinsamer Teiler ist daher eindeutig bestimmt bis auf Multiplikation mit einer Einheit.

Beweis. d_1, d_2 seien größte gemeinsame Teiler von f und g, dann folgt nach der Eigenschaft (2) in 1/2/22 insbesondere $d_2|d_1$ und $d_1|d_2$, daher $d_1 \sim d_2$. ❑

Ganz ähnlich wird ein weiterer Begriff der Teilbarkeitslehre eingeführt.

Definition. (*kleinstes gemeinsames Vielfaches*) 1/2/24

Sind $f, g \in R$, dann heißt $c \in R$ *kleinstes gemeinsames Vielfaches* von f und g, falls

(1) $f|c$ und $g|c$;

(2) für $c' \in R$ mit $f|c'$ und $g|c'$ gilt stets $c|c'$.

Leicht ergibt sich der folgende

Satz. (*Eindeutigkeit des kleinsten gemeinsamen Vielfachen*) 1/2/25

Sind c und c' kleinste gemeinsame Vielfache von $f, g \in R$, so ist $c \sim c'$.

Beweis als Übungsaufgabe ...

Teilbarkeitslehre im Ring der ganzen Zahlen

Die zuvor eingeführten Begriffe der Teilbarkeitslehre werden nun auf den Ring $\mathbb{Z}$ der ganzen Zahlen angewendet. Insbesondere ergibt sich in diesem Fall die Existenz des größten gemeinsamen Teilers und des kleinsten gemeinsamen Vielfachen aus den nachfolgenden Überlegungen. 1/2/26

Wir beginnen mit einem klassischen Verfahren zur Bestimmung des größten gemeinsamen Teilers, es beruht auf der *Division mit Rest*:
Sind $f, g \in \mathbb{Z}$ und $g > 0$, so existieren ganze Zahlen $q, r \in \mathbb{Z}$ mit $0 \leq r < g$, für die $f = g \cdot q + r$ ist. Dafür schreiben wir gelegentlich auch

$$f : g = q \text{ Rest } r$$

und bezeichnen r als Rest von f bei Division durch g.

Diese Eigenschaft ganzer Zahlen lässt sich beweisen, indem für r das Minimum aller nicht negativen Zahlen gewählt wird, für die $f - s$ durch g teilbar ist.

Satz. (*euklidischer Algorithmus*)

Es sei $(f, g) \in \mathbb{Z}^2$ ein Paar ganzer Zahlen mit $f > g > 0$. Wir ordnen ihm eine endliche Folge

$$(f, g) = (f_0, g_0) \mapsto (f_1, g_1) \mapsto \ldots \mapsto (f_i, g_i) \mapsto (f_{i+1}, g_{i+1}) \mapsto \ldots \mapsto (f_l, g_l)$$

von Zahlenpaaren $(f_i, g_i) \in \mathbb{Z}^2$ zu mit $f_i > g_i > 0$ für $i > 0$, wobei $f_{i+1} = g_i$ und g_{i+1} der Rest von f_i bei Division durch g_i ist,

$$f_i = q_i g_i + g_{i+1}, \quad q_i, g_{i+1} \in \mathbb{Z}, \quad 0 < g_{i+1} < g_i.$$

Wegen $g > g_1 > \ldots > g_i > \ldots (> 0)$ bricht das Verfahren (Kettendivision) *nach endlich vielen Schritten ab; $d = g_l$ sei der letzte von 0 verschiedene Rest. Dann gilt*:

(1) *Es gibt Zahlen $p, q \in \mathbb{Z}$ mit $d = pf + qg$.*

(2) *d ist größter gemeinsamer Teiler von f und g.*

Obwohl die aus der Schule bekannte Methode zur Bestimmung des größten gemeinsamen Teilers mittels Primfaktorzerlegung recht anschaulich ist, gibt sie uns weniger Informationen als das hier angegebene Verfahren; überdies ist die Primfaktorzerlegung für große Zahlen schwer ausführbar.

Beweis. Die Eigenschaft (1) folgt durch schrittweises Einsetzen aus den angegebenen Gleichungen

$$f = qg + g_1, \quad g = f_1 = q_1 g_1 + g_2, \quad \ldots ,$$
$$f_i = q_i g_i + g_{i+1}, \quad \ldots ,$$
$$f_{l-1} = q_{l-1} g_{l-1} + g_l = q_{l-1} g_{l-1} + d.$$

Wir haben dafür lediglich induktiv zu prüfen, dass für $i \leq l$ gilt:

Sind f_i, g_i Vielfachensummen von f und g, so auch f_{i+1} und g_{i+1}.
Zu (2) bemerken wir zunächst, dass $g_{l-1} = f_l = q_l g_l$ ist ($q_l \in \mathbb{Z}$ geeignet gewählt). Einsetzen in die obige Kette von Gleichungen zeigt, dass $d = g_l$ dann sowohl f als auch g teilt.
Umgekehrt wissen wir nach (1), dass die Zahl d Vielfachensumme von f und g ist, also muss jeder Teiler von f und g auch d teilen. Folglich ist d größter gemeinsamer Teiler von f und g. ❏

Korollar – Bezeichnung. *$f, g \in \mathbb{Z}$ seien ganze Zahlen.*

(1) *Es existiert ein größter gemeinsamer Teiler d für f und g. Bis auf Assoziiertheit kann $d \geq 0$ gewählt werden und ist dadurch eindeutig bestimmt.* Wir bezeichnen diese Zahl mit $\mathrm{ggT}(f,g) := d$.

(2) *Es existieren $a, b \in \mathbb{Z}$ mit* $\mathrm{ggT}(f,g) = a\cdot f + b\cdot g$.

Beweis. Für $g = 0$ oder $f \sim g$ ist f größter gemeinsamer Teiler von f und g; die Aussagen (1), (2) sind in diesem Fall evident. Anderenfalls kann o.B.d.A. $f > g > 0$ gewählt werden, womit die Behauptung aus dem Satz folgt. ❏

Beispiele.

(1) Wir bestimmen $\mathrm{ggT}(30,22)$. Mit der Notation aus dem Satz gilt

Hier ist nur nach dem größten gemeinsamen Teiler gefragt.

$$(30,22) \mapsto (22,8) \mapsto (8,6) \mapsto (6,2) \text{ wegen}$$
$$30 = 1\cdot 22 + 8, \quad 22 = 2\cdot 8 + 6, \quad 8 = 1\cdot 6 + 2.$$

Daher folgt $\mathrm{ggT}(30,22) = 2$.

(2) Wir bestimmen den größten gemeinsamen Teiler von $f = 29$, $g = 17$ und stellen ihn als Vielfachensumme dieser Zahlen dar.
Wird mit r_i der Rest bei der i-ten Division bezeichnet, so ergibt sich:

$29 : 17 = 1$ Rest 12	$29 = 17\cdot 1 + 12$	$f - g = r_1$	
$17 : 12 = 1$ Rest 5	$17 = 12\cdot 1 + 5$	$g - r_1 = r_2$	$r_2 = -f + 2g$
$12 : 5 = 2$ Rest 2	$12 = 5\cdot 2 + 2$	$r_1 - 2r_2 = r_3$	$r_3 = 3f - 5g$
$5 : 2 = 2$ Rest 1	$5 = 2\cdot 2 + 1$	$r_2 - 2r_3 = r_4$	$r_4 = -7f + 12g$

Dieses Beispiel soll eine Anregung sein, beim „Rechnen mit der Hand“ die Zwischenschritte systematisch aufzuschreiben.

Die letzte Spalte der Tabelle entstand dabei durch Einsetzen aus der vorhergehenden. Mit $r_4 = 1$ erhalten wir den größten gemeinsamen Teiler als $1 = -7\cdot f + 12\cdot g$. ❏

Das zentrale Resultat über die Faktorzerlegung ganzer Zahlen beruht auf dem folgenden

Satz. (*Lemma von Euklid*) 1/2/27

Ist $p \in \mathbb{Z}$ irreduzibel, so gilt für beliebige Zahlen $f, g \in \mathbb{Z}$:

$$p|(f\cdot g) \implies p|f \ \vee \ p|g.$$

Beweis. O.B.d.A. sind $f, g \neq 0$. Ist $p \nmid f$, dann ist 1 größter gemeinsamer Teiler von p und f, denn ± 1 sind die einzigen echten Teiler von p. Nach dem vorigen Satz folgt $1 = a\cdot p + b\cdot f$ mit geeigneten Zahlen $a, b \in \mathbb{Z}$. Multiplikation dieser Gleichung mit g ergibt $g = a\cdot p\cdot g + b\cdot f\cdot g$, und die rechte Seite ist entsprechend der Voraussetzung durch p teilbar, also gilt $p|g$. ❑

Definition – Korollar. Es sei $p \in \mathbb{Z}$, $p > 1$. 1/2/28

(1) Die Zahl p heißt *Primzahl*, falls sie nur dann Teiler eines Produkts ist, wenn sie einen der Faktoren teilt: $p|fg \Rightarrow p|f \vee p|g$.

(2) *p ist genau dann Primzahl, wenn p irreduzibel ist, d.h. wenn in $\mathbb{Z}$ nur die Teiler ± 1, $\pm p$ existieren.*

Das Resultat aus dem Satz wird hier zur Definition des Begriffs *Primzahl* verwendet.

Beweis. Nach dem Satz bleibt noch zu zeigen, dass eine Primzahl p irreduzibel ist. Wir überprüfen die Eigenschaft (3) im Lemma aus 1/2/21: Es sei $p = f \cdot g$. Dann ist p insbesondere ein Teiler von $f \cdot g$, daher o.B.d.A. $p|f$. Wegen $f|p$ folgt $p \sim f$. ❑

Satz. (*Hauptsatz der Arithmetik*)

Jede ganze Zahl > 1 ist Produkt von Primzahlen. Diese sind bis auf Reihenfolge eindeutig bestimmt.

Dieser Satz ist uns natürlich vertraut. Danach kann beispielsweise der ggT als Produkt der maximalen Primzahlpotenzen bestimmt werden, die in zwei Zahlen auftreten.

Beweis. Wir zeigen zunächst die Existenz einer Faktorzerlegung: Bezeichnet $n > 1$ die kleinste Zahl, die kein Produkt von Primzahlen ist, so kann n selbst keine Primzahl sein, es gilt also $n = f \cdot g$ mit geeigneten Zahlen $1 < f < n$, $1 < g < n$. Nun sind f und g Produkte von Primzahlen, daher auch n, ↯.
Sind nun $p_1 \cdot \ldots \cdot p_m = q_1 \cdot \ldots \cdot q_n$ zwei Zerlegungen derselben Zahl in positive irreduzible Faktoren p_i bzw. q_j, so muss nach dem Lemma von Euklid p_1 eine der Zahlen q_j teilen. Da p_1 keine Einheit ist, folgt $p_1 = q_j$. So ergibt sich induktiv $m = n$ und nach Permutation der q_j auch $p_i = q_i$ für $i = 1, \ldots m$. ❑

Mit der hier dargestellten Methode ist es nicht schwer, einen entsprechenden Satz für den Polynomring $K[X]$ über einem Körper K zu beweisen. Im zweiten Kapitel wird das im Zusammenhang mit dem Studium der Nullstellenmengen von Polynomen ausgeführt.

Die (auch im Rahmen der Übungsaufgaben behandelte) Existenz eines kleinsten gemeinsamen Vielfachen für Zahlen $f, g \in \mathbb{Z}$ ergibt sich leicht aus dem Satz. Die dazu assoziierte nichtnegative Zahl wird mit $\mathrm{kgV}(f, g)$ bezeichnet.

Das Homomorphieprinzip für Ringe 1/2/29

Wir beginnen mit einem Beispiel. $R = \mathbb{Z}/m\mathbb{Z}$ sei die Faktorgruppe von $\mathbb{Z}$ nach der Untergruppe $m\mathbb{Z}$, $m \in \mathbb{N}$. Für $m = 0$ ist der kanonische Homomorphismus $\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ bijektiv, d.h. die Faktorgruppe R besitzt bereits eine Ringstruktur. Nun sei m beliebig. Wir definieren auf R eine Multiplikation durch

Dieses Beispiel dient der späteren Konstruktion einiger endlicher Körper.

$$(*) \qquad \overline{a} \cdot \overline{b} := \overline{a \cdot b} \quad \text{für } a, b \in \mathbb{Z},$$

wobei $\overline{x} := x + m\mathbb{Z}$ die Klasse des Elements x bezeichnet.
Die Vereinbarung $(*)$ ist nicht a priori sinnvoll, denn wir haben zur Definition des Produkts Repräsentanten der Klassen $\overline{a}$, $\overline{b}$ verwendet.

Es sei also $\overline{a} = \overline{a_1}$ und $\overline{b} = \overline{b_1}$. Dann ist $a = a_1 + q\cdot m$, $b = b_1 + r\cdot m$ mit geeigneten Zahlen $q, r \in \mathbb{Z}$. Multiplizieren wir beide Gleichungen miteinander, so erhalten wir $ab = a_1b_1 + c$ mit $c = (a_1r + b_1q + qrm)m \in m\mathbb{Z}$; die Klassen von ab und a_1b_1 stimmen daher überein.

$R = \mathbb{Z}/m\mathbb{Z}$ erfüllt mit der Multiplikation $(*)$ alle Eigenschaften eines kommutativen Ringes und heißt *Ring der Restklassen* modulo m. Die Gleichheit $\overline{x} = \overline{y}$ zweier Klassen wird auch durch die Notation $a \equiv b \mod (m)$ ausgedrückt.

Die in der Zahlentheorie übliche Notation $a \equiv b \mod (m)$ wird hier selten verwendet.

Wir bemerken, dass sich diese Konstruktion verallgemeinern lässt; in Analogie zur Faktorgruppe haben wir hier in einem Spezialfall den *Faktorring* konstruiert. Die Abbildung $\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$, die $n \in \mathbb{Z}$ auf die Klasse $\overline{n}$ abbildet, ist konstruktionsgemäß ein Ringhomomorphismus.

Allgemein können wir so vorgehen: Der bereits unter 1/2/3 definierte *Kern eines Ringhomomorphismus* $f : R \to S$ ist der Kern des zugehörigen Homomorphismus der additiven Gruppen, d.h. $\ker(f) = f^{-1}(0)$. Er ist bis auf Ausnahmen kein Unterring, erfüllt jedoch stets die folgende

$\ker(f)$ ist zwar stets eine Untergruppe von $(R,+)$, enthält aber nur dann 1_R, wenn $R = \ker(f)$. Es folgt $f(1_R) = 1_S = 0$, d.h. S ist der Nullring.

Definition. (*Ideal*) 1/2/30

Eine Untergruppe $\boldsymbol{a}$ der additiven Gruppe des Ringes R heißt (*zweiseitiges*) *Ideal,* falls für beliebige $r \in R$ und $x \in \boldsymbol{a}$ gilt $r\cdot x \in \boldsymbol{a}$ und $x\cdot r \in \boldsymbol{a}$.

Bemerkung. (*Rechnen mit Idealen*)

1. In einem Ring R gibt es wenigstens die *trivialen* Ideale $\mathbf{0} := \{0\}$ (*Nullideal*) und R (*Einsideal*).
2. Ein Körper besitzt nur die trivialen Ideale.
3. Der Durchschnitt einer Menge von Idealen im Ring R ist stets wieder ein Ideal.
4. Ist $F \subseteq R$ Teilmenge des Ringes R, so ist der Durchschnitt aller Ideale $\boldsymbol{a}$ aus R mit $F \subseteq \boldsymbol{a}$ ein Ideal (F), es heißt das von F *erzeugte Ideal.* (F) ist das kleinste Ideal, das F enthält.

   Insbesondere ergibt sich $\mathbf{0} = (0) = (\emptyset)$.

   Für einen kommutativen Ring R gilt
   $$(F) = \sum_{f\in F} fR := \Big\{ \sum_{f\in F} a_f f \,|\, a_f \in R,\ \text{fast alle } a_f = 0\Big\}.$$
   Im Fall einer endlichen Menge $F = \{f_1, \dots, f_s\}$ wird meist die Notation $(F) =: (f_1, \dots, f_s)$ verwendet.
5. Ist $\boldsymbol{a} = (f)$ für ein geeignetes Element $f \in R$, so wird $\boldsymbol{a}$ ein *Hauptideal* genannt. Das Nullideal und das Einsideal $(1) = R$ sind spezielle Hauptideale.
   Nach Satz 1/1/10 ist jedes Ideal im Ring $\mathbb{Z}$ ein Hauptideal, genauer: eines der Ideale $(m) = m\mathbb{Z}$, $m \in \mathbb{N}$.
   Mit der unter 4. eingeführten Bezeichnung gilt z.B. $(6, 4) = (2)$.
6. Die *Summe der Ideale* $\boldsymbol{a}$ *und* $\boldsymbol{b}$ des Ringes R ist
   $$\boldsymbol{a} + \boldsymbol{b} := (\boldsymbol{a} \cup \boldsymbol{b}) = \{a + b \,|\, a \in \boldsymbol{a}, b \in \boldsymbol{b}\};$$
   diese Operation ist kommutativ und assoziativ.
   Unter Verwendung der Bezeichnung aus 4. gilt beispielsweise
   $$(f_1, \dots, f_s) = (f_1) + \dots + (f_s).$$

Die angegebenen Eigenschaften sind mehr oder weniger offensichtlich.
3. folgt z.B. aus 1/1/8 und daraus, dass die Multiplikation mit Ringelementen nicht aus einem Ideal herausführt.

Warnung: Im Polynomring $K[X_1, X_2]$ ist dagegen $(X_1, X_2) = \{a_1X_1 + a_2X_2 \mid a_i \in K[X_1, X_2]\}$ kein Hauptideal, d.h. es existiert kein Polynom f mit der Eigenschaft $(X_1, X_2) = (f)$.

Satz – Definition. (*Faktorring*) 1/2/31

Dieser Satz und der nachfolgende Homomorphiesatz für Ringe sind nahezu identisch mit den entsprechenden Aussagen für Gruppen.

Ist $\boldsymbol{a}$ ein Ideal in dem Ring R, so besitzt die Faktorgruppe $R/\boldsymbol{a}$ eine eindeutig bestimmte Multiplikation, für die der kanonische Gruppenhomomorphismus $p : R \to R/\boldsymbol{a}$, $r \mapsto \overline{r}$ ein Ringhomomorphismus ist.

$R/\boldsymbol{a}$ heißt *Faktorring* von R nach $\boldsymbol{a}$ und p der *kanonische* (*Ring-*)*Homomorphismus* von R auf $R/\boldsymbol{a}$.

Beweis. Der Gruppenhomomorphismus p ist nur dann ein Ringhomomorphismus, wenn für $a, b \in R$ stets $p(a{\cdot}b) = p(a){\cdot}p(b)$ gilt. Folglich ist

$$(*) \qquad \overline{a} \cdot \overline{b} := \overline{a \cdot b} \quad \text{für } a, b \in R$$

(in diesem Fall) die einzig mögliche Definition einer Multiplikation auf $R/\boldsymbol{a}$. Wie im zuvor ausgeführten Beispiel 1/2/29 kann verifiziert werden, dass die Vorschrift $(*)$ nicht von der Wahl der Repräsentanten in den Klassen $\overline{a}$, $\overline{b}$ abhängt und daher auch sinnvoll ist. Die Ringeigenschaften sind unter Verwendung von $(*)$ leicht nachzurechnen. ❏

Wie im anfangs erläuterten Spezialfall heißt $R/\boldsymbol{a}$ auch Restklassenring von R modulo $\boldsymbol{a}$. Für $a, b \in R$ mit $\overline{a} = \overline{b}$ wird gelegentlich die Schreibweise $a \equiv b \bmod \boldsymbol{a}$ verwendet.

Satz. (*Homomorphiesatz für Ringe*) 1/2/32

$f : R \to R'$ sei ein Ringhomomorphismus, so existiert ein eindeutig bestimmter injektiver Ringhomomorphismus $j : R/\ker(f) \to R'$ mit $f = j{\cdot}p$, wobei p den kanonischen Homomorphismus $p : R \to R/\ker(f)$ bezeichnet.

Hier steht wieder das vertraute kommutative Diagramm, das wir im Zusammenhang mit dem Homomorphieprinzip für Gruppen kennen gelernt haben.

$$\begin{tikzcd} R \arrow[rr, "f"] \arrow[dr, "p"'] & & R' \\ & R/\ker(f) \arrow[ur, "j"'] & \end{tikzcd}$$

Es gilt insbesondere $\operatorname{im}(f) \cong R/\ker(f)$.

Beweis. Nach dem Homomorphiesatz für Gruppen (vgl. 1/2/26) existiert ein eindeutig bestimmter Gruppenhomomorphismus j, für den das angegebene Diagramm kommutiert. Aus 1/2/31 folgt unmittelbar, dass j mit der Multiplikation verträglich ist. ❏

Die Faktorisierung eines beliebigen Homomorphismus über den kanonischen Homomorphismus lässt sich ebenso für Algebren ausführen, d.h. wenn die Ringe R und R' mit Strukturmorphismen versehen sind, die mit f kommutieren. Das bereitet keinerlei Schwierigkeiten, hätte allerdings die Bezeichnungen unnötig kompliziert. Der Begriff des Faktorringes ist dann durch den der *Faktoralgebra* zu ersetzen, deren Strukturmorphismus durch Komposition des Strukturmorphismus von R mit dem kanonischen Homomorphismus entsteht. 1/2/33

Primkörper und Charakteristik 1/2/34

Wir wenden uns erneut den Faktorringen der ganzen Zahlen zu und betrachten als Beispiel $R = \mathbb{Z}/6\mathbb{Z}$. Hier gilt $\overline{2}{\cdot}\overline{3} = \overline{6} = \overline{0}$, und beide Faktoren sind von der Nullklasse verschieden. R ist daher kein Integritätsbereich.

Betrachten wir R als $\mathbb{Z}$-Algebra, so erhält $\overline{2}{\cdot}\overline{3} = \overline{0}$ mit der Konvention aus 1/2/12 die Gestalt $2{\cdot}3 = 0$.

Nun soll untersucht werden, welche der Ringe $\mathbb{Z}/m\mathbb{Z}$ nullteilerfrei sind. Die Fälle $m = 0$, $m = 1$ sind recht einfach: $m = 0$ ergibt einen zu $\mathbb{Z}$

isomorphen Ring, der damit nullteilerfrei ist, und für $m = 1$ erhalten wir den Nullring. Nun nehmen wir an, $m > 1$ sei keine Primzahl. Dann ist m von der Form $m = a \cdot b$ mit geeigneten Zahlen a, b, $1 < a < m$ und $1 < b < m$. Daher ist $\overline{0}$ das Produkt der Klassen $\overline{a} \neq 0$ und $\overline{b} \neq 0$, also $\mathbb{Z}/m\mathbb{Z}$ kein Integritätsbereich.

Es verbleibt der Fall einer Primzahl m. Ist $\overline{0} = \overline{a} \cdot \overline{b}$, so muss m Teiler von $a \cdot b$ sein, teilt also eine der Zahlen a, b. Diese liegt dann in der Klasse $\overline{0}$ aus $\mathbb{Z}/m\mathbb{Z}$. Damit ist $\mathbb{Z}/m\mathbb{Z}$ im letzteren Fall ein Integritätsbereich. Da dieser Ring endlich ist, erhalten wir sogar noch mehr:

Satz. *Für jede Primzahl p ist $\mathbb{Z}/p\mathbb{Z}$ ein Körper.* Er wird von nun an mit dem Symbol $\mathbb{F}_p$ bezeichnet.

Die Körper $\mathbb{F}_p$ werden neben $\mathbb{R}$ und $\mathbb{C}$ die wichtigsten *Grundkörper* in späteren Rechenbeispielen bilden.

Beweis. Wie soeben gesehen, besitzt die Multiplikation des Ringes $R = \mathbb{Z}/p\mathbb{Z}$ eine Einschränkung auf die Menge M der von 0 verschiedenen Elemente. Es bleibt zu beweisen, dass für $x \in M$ bezüglich der Multiplikation stets ein Inverses existiert. Dazu betrachten wir die Abbildung $f : M \to M$ mit $f(a) := a \cdot x$. Sind $a_1, a_2 \in M$ mit $f(a_1) = f(a_2)$, so gilt in R die Gleichung $a_1 x = a_2 x$. Wegen $x \neq 0$ ergibt die Kürzungsregel $a_1 = a_2$. Damit haben wir eine injektive Abbildung f der endlichen Menge M in sich gefunden. Folglich ist f ist bijektiv, und das Urbild von 1 bezüglich f ist multiplikativ invers zu x. ❏

Die Existenz dieser Einschränkung ist nur eine andere Formulierung dafür, dass R Integritätsbereich ist.

Satz – Definition. (*Charakteristik eines Körpers*) 1/2/35

Jeder Körper K besitzt einen kleinsten Unterring. Er ist entweder isomorph zu $\mathbb{Z}$ oder zu genau einem der endlichen Körper $\mathbb{F}_p$, wobei p eine Primzahl bezeichnet. Im ersten Fall setzen wir $\operatorname{char}(K) := 0$, sonst $\operatorname{char}(K) := p$. Diese Zahl heißt *Charakteristik* von K.

Diese Einteilung liefert eine erste, grobe Klassifikation der Körper.

Beweis. Wir betrachten den Strukturmorphismus $f : \mathbb{Z} \to K$ der $\mathbb{Z}$-Algebra K, gegeben durch $f(n) = n \cdot 1$. Sein Bild liegt offenkundig in jedem Unterring von K.

$\ker(f)$ ist eines der Ideale $m\mathbb{Z}$, $m \in \mathbb{N}$ (vgl. 5. in 1/2/30 oder 1/1/10). Da ein Körper mindestens zwei verschiedene Elemente besitzt (0 und 1), kommt $m = 1$ nicht infrage. Falls $m \neq 0$ ist, muss $\operatorname{im}(f) \cong \mathbb{Z}/m\mathbb{Z}$ endlich sein (vgl. 1/2/32). Die Überlegungen unter 1/2/34 ergeben, dass m eine Primzahl ist (sonst hätte K Nullteiler). Das Bild $\operatorname{im}(f)$ ist daher zu einem der Körper $\mathbb{F}_p$ isomorph.
Es verbleibt nur noch der Fall $m = 0$. Dann ist $\ker(f) = \{0\}$, also f injektiv und daher $\mathbb{Z} \cong \operatorname{im}(f)$. ❏

Das Rechnen in den Körpern $\mathbb{F}_p$ mag ungewohnt sein, ist aber (insbesondere für kleine Primzahlen p) wenig aufregend.
Für $a \in \mathbb{Z}$ darf die Klasse $\overline{a} \in \mathbb{F}_p$ ebenfalls mit a bezeichnet werden, denn $\mathbb{F}_p$ ist eine $\mathbb{Z}$-Algebra. Mit dieser Konvention ergeben sich merkwürdig anmutende Identitäten wie z.B. $1 + 1 = 0$ oder $1 = 3$ in $\mathbb{F}_2$.
Das multiplikative Inverse eine Elements $\overline{a} \in \mathbb{F}_p \setminus \{\overline{0}\}$ lässt sich mittels einer Multiplikationstafel bestimmen. Es gibt jedoch die folgende Alternative: Wegen $\operatorname{ggT}(a, p) = 1$ finden wir mit dem euklidischen Algorithmus $b, c \in \mathbb{Z}$, für die $a \cdot b + c \cdot p = 1$ ist. Bilden wir die Klassen modulo p, so erhalten wir $\overline{a} \cdot \overline{b} = \overline{1}$ in $\mathbb{F}_p$.

Beispiel. Wir suchen das multiplikative Inverse für $17 \in \mathbb{F}_{29}$. Unter 1/2/26, Beispiel (2) haben wir mit dem euklidischen Algorithmus bereits ausgerechnet, dass in $\mathbb{Z}$ der größte gemeinsame Teiler der Zahlen 17 und 29 durch $1 = 12{\cdot}17 - 7{\cdot}29$ gegeben ist. Übergang zu den Restklassen modulo 29 ergibt $1 = 12\cdot 17$ in $\mathbb{F}_{29}$, d.h. $17^{-1} = 12$. ❑

Aus dem Beweis des Satzes ist zu entnehmen, dass die Charakteristik eines Körpers K auch so beschrieben werden kann:

Wir betrachten alle Vielfachen $n \cdot 1_K$ des Einselements von K mit $n \in \mathbb{N}$, so gibt es genau zwei mögliche Fälle:

(1) $n{\cdot}1_K \neq 0$ *für alle* $n > 0$, *dann ist* $\operatorname{char}(K) = 0$.

(2) *Es existiert ein* $n > 0$ *mit* $n{\cdot}1_K = 0$*; die kleinste dieser Zahlen* n *ist* $\operatorname{char}(K)$.

Für einen Körper K der Charakteristik 0 haben wir einen injektiven Homomorphismus $\iota : \mathbb{Z} \to K$ gefunden. Dieser lässt sich fortsetzen zu einem injektiven Homomorphismus

$$\mathbb{Q} \to K, \quad \frac{a}{b} \mapsto \frac{\iota(a)}{\iota(b)} \quad (a \in \mathbb{Z},\, b \in \mathbb{Z} \setminus \{0\}),$$

d.h. es gibt ein kommutatives Diagramm

$$\begin{tikzcd}
\mathbb{Z} \arrow[rr] \arrow[dr] & & K \\
& \mathbb{Q} \arrow[ur] &
\end{tikzcd}$$

injektiver Ringhomomorphismen.

Nebenstehende Überlegungen erklären den folgenden Satz 1/2/36. Der injektive Homomorphismus $\mathbb{Q} \to K$ wird künftig als Inklusion betrachtet.

Definition – Satz. (*Primkörper*) 1/2/36

Der kleinste Unterkörper eines Körpers heißt sein *Primkörper.* Er ist zu genau einem der Körper $\mathbb{Q}$ bzw. $\mathbb{F}_p$ isomorph, die auch als Primkörper der betreffenden Charakteristik 0 bzw. p bezeichnet werden.

$\mathbb{Q}$ und $\mathbb{F}_p$ spielen damit eine Sonderrolle unter allen Körpern.

Wir verfügen nun über Methoden, aus gegebenen Ringen neue zu konstruieren. Dazu gehören insbesondere die Erweiterung durch Polynome, die Faktorbildung und die Quotientenbildung. Im Zusammenhang mit dem Studium von Gleichungen lernen wir später noch algebraische Erweiterungen kennen. Die Elemente eines fixierten Grundkörpers, über dem wir alle unsere Rechnungen ausführen, werden wir künftig ganz unbefangen „Zahlen“ nennen.

Schwerpunkte zum gewählten Stoff

• Ringoperationen (elementare Eigenschaften, allgemeines Distributivgesetz, binomischer Satz)	[1/2/1 – 1/2/2]
• Erste Beispiele für Ringe	[1/2/2]
• Unterringe eines Ringes	[1/2/3]
• Ringhomomorphismen und Isomorphismen	[1/2/3]
• Elementare Eigenschaften von Ringhomomorphismen	[1/2/3]
• Nullteilerfreie Ringe (Integritätsbereiche)	[1/2/4]
• Kürzungsregel in Integritätsbereichen	[1/2/4]
• Körper und Unterkörper, Beispiele	[1/2/5]
• Konstruktion der rationalen Zahlen	[1/2/6]
• Verallgemeinerung der Konstruktion rationaler Zahlen (Konstruktion von Quotientenkörpern beliebiger Integritätsbereiche)	[1/2/6]
• Komplexe Zahlen (Realteil, Imaginärteil, Konjugation)	[1/2/7]
• Rechnen mit komplexen Zahlen	[1/2/7]
• Fundamentalsatz der Algebra (ohne Beweis)	[1/2/8]
• Der Polynomring in einer Unbestimmten (Definition)	[1/2/9 – 1/2/10]
• Prinzip des Koeffizientenvergleichs	[1/2/10]
• Grad eines Polynoms, Eigenschaften der Gradfunktion	[1/2/10]
• Ein Polynomring über einem Integritätsbereich ist wieder ein Integritätsbereich	[1/2/11]
• Begriff der Algebra über einem Ring, Strukturhomomorphismus	[1/2/12]
• Homomorphismen und Isomorphismen von Algebren	[1/2/13]
• Universaleigenschaft und Eindeutigkeit der Polynomalgebra	[1/2/14 – 1/2/15]
• Definition der Polynomalgebra $R^{[n]}$ in n Unbestimmten (Monome, Terme, vollständiger Grad)	[1/2/16]
• Universalität von $R^{[n]}$	[1/2/17]
• Adjunktion von Elementen	[1/2/18]
• Teilbarkeit einem kommutativen Integritätsbereich	[1/2/19]
• Assoziiertheit als Äquivalenzrelation	[1/2/20]
• Gruppe der Einheiten und irreduzible Elemente	[1/2/20 – 1/2/21]
• Größter gemeinsamer Teiler und kleinstes gemeinsames Vielfaches	[1/2/22 – 1/2/25]
• Der euklidische Algorithmus	[1/2/26]
• Lemma von Euklid, Primzahlen	[1/2/27]
• Hauptsatz der Arithmetik	[1/2/28]
• Ideale, durch Teilmengen eines Ringes erzeugte Ideale, Hauptideale	[1/2/30]
• Konstruktion von Faktorringen	[1/2/29 – 1/2/31]
• Homomorphiesatz für Ringe	[1/2/32]
• Die endlichen Körper $\mathbb{F}_p$ (p Primzahl)	[1/2/34 – 1/3/35]
• Der Primkörper eines Körpers	[1/2/36]

Sachverzeichnis