Vorwort

Vorwort zur zweiten Auflage

In dieser zweiten Auflage habe ich auf Anraten einiger Leser und des Verlages den Titel des Buches von „Elementare Algebra und Zahlentheorie“ in „Einführung in Algebra und Zahlentheorie“ geändert, um Verwechslungen mit Texten für den Bereich „Elementarmathematik vom höheren Standpunkt“ von Lehramtsstudiengängen auszuschließen - im Sinne dieser Terminologie von Studiengängen gehört der Inhalt des Buches trotz seiner Beschränkung auf die elementareren Teile der Algebra und der Zahlentheorie in den Studienbereich „Höhere Mathematik“. Ferner habe ich eine Reihe Druckfehler und sonstige Fehler korrigiert sowie eine Reihe weiterer kleinerer Änderungen vorgenommen; ich danke S. Kühnlein, Karlsruhe, der mich auf die meisten der Fehler aufmerksam gemacht hat.

Schließlich habe ich, ebenfalls auf Anregung einiger Leser, zwei weitere ergänzende Abschnitte hinzugefügt. In Kapitel 12 wird der Hauptsatz der Galoistheorie formuliert und bewiesen sowie zum Beweis des hinreichenden Kriteriums für Konstruierbarkeit mit Zirkel und Lineal des regelmäßigen n-Ecks benutzt. In dem anderen neu hinzugekommenen ergänzenden Abschnitt 10.4 wird die algebraische Theorie der zyklischen fehlerkorrigierenden Codes vorgestellt, ohne aber auf die informationstheoretischen Grundlagen der Codierungstheorie einzugehen.

Wie auch die anderen ergänzenden Abschnitte des Buchs werden beide Abschnitte in der Regel nicht in den Rahmen einer einsemestrigen Vorlesung über Algebra und Zahlentheorie passen und sind zum Verständnis der anderen Teile des Buchs nicht notwendig; sie sollen interessierten LeserInnen zur Abrundung des Stoffes und als erster Einblick in fortgeschrittene Themen und in Anwendungen dienen.

Wie bisher bitte ich LeserInnen, die noch verbliebene Fehler finden, mir diese an `schulzep@math.uni-sb.de` zu melden, damit ich die Korrekturen auf mei-

ner homepage unter `www.math.uni-sb.de/ag/schulze/eazbuch.html` im Internet zugänglich machen kann. Dort sind auch die mir bekannten Fehler der ersten Auflage mit Korrekturen aufgelistet.

Saarbrücken, Mai 2008 *Rainer Schulze-Pillot*

Vorwort zur ersten Auflage

Dieses Buch ist aus dem Versuch entstanden, die Ausbildung der Studierenden in Algebra und Zahlentheorie an der Universität des Saarlandes in Saarbrücken an die durch die Einführung der Bachelor- und Masterabschlüsse und die anstehende Reform des Lehramtsstudiums veränderten Randbedingungen anzupassen.

Da algebraische und diskrete Strukturen ebenso wie einige grundlegende Ergebnisse und Methoden der Zahlentheorie in zunehmendem Umfang auch für Anwender relevant werden, erschien es sinnvoll, eine einsemestrige Vorlesung über Algebra und Zahlentheorie anzubieten, die auf einer Grundvorlesung über lineare Algebra aufbaut und sich unabhängig von der beabsichtigten Schwerpunktbildung für alle Studierenden eignet.
Eine erste Testversion dieser Vorlesung habe ich im Sommersemester 2005 gehalten. Auf dem Skript zu dieser Vorlesung basiert dieses Buch, das sich vor allem an Studierende der Mathematik ab dem dritten oder ggf. auch dem zweiten Semester in Bachelor- oder Lehramts-Studiengängen an Universitäten wendet.
Ebenso wie die Vorlesung kombiniert es Teile des Stoffes, der üblicherweise in einer Vorlesung über elementare Zahlentheorie behandelt wird, mit Teilen des Stoffes einer klassischen Algebra-Vorlesung.
Mit der Beschränkung auf die elementareren Teile des Gebiets und einer relativ ausführlichen Darstellung will das Buch eine breite Leserschaft ansprechen. Ich möchte aber nicht das Versprechen einer „sanften“ Einführung oder eines leicht verdaulichen anschaulichen und abstraktionsfreien „Mathe-light“-Kurses abgeben – wer eine Scheu vor abstrakten Konzepten hat, wird in der Regel ohnehin nicht Mathematik studieren und mit Sicherheit die Algebra meiden.

Das Buch enthält aus der Zahlentheorie einige Grundlagen der Primzahltheorie, den euklidischen Algorithmus, die Theorie der linearen diophantischen Gleichungen sowie des größten gemeinsamen Teilers und des kleinsten gemeinsamen Vielfachen, die Theorie der Kongruenzen mit dem chinesischen Restsatz, die Theorie der primen Restklassengruppe und der Potenzreste und das quadratische Reziprozitätsgesetz.
Aus der Algebra behandeln wir die Grundtatsachen über Gruppen und Ringe einschließlich der Operationen von Gruppen auf Mengen und der Behandlung

von Idealen und Restklassenringen, die Theorie der (endlich erzeugten) abelschen Gruppen und ihrer Charaktere sowie die Grundlagen der Körpertheorie unter besonderer Betonung der endlichen Körper.

Während in den Teilen des Stoffes, die aus der elementaren Zahlentheorie stammen, die zu Grunde liegenden abstrakten algebraischen Konzepte betont werden, werden die Teile, die aus der Algebra stammen, eng an die Behandlung (meist zahlentheoretischer) Beispiele angebunden.
Die Behandlung von Anwendungen ergibt sich dabei in natürlicher Weise; wir behandeln etwa das RSA-Verschlüsselungsverfahren, Primzahltests, Zahldarstellungen und modulares Rechnen im Computer sowie die diskrete Fourier-Transformation.

Wichtige Teile der klassischen Algebra-Vorlesung fallen bei dieser Vorgehensweise notwendigerweise unter den Tisch: Die Galoistheorie erscheint nur in ihrer einfachsten Form als Galoistheorie der endlichen Körper, die Theorie als solche und ihre Anwendungen für die Auflösung von Gleichungen durch Radikale bleiben ebenso einer weiterführenden Algebra-Vorlesung vorbehalten wie die Ausarbeitung der Gruppentheorie (Auflösbarkeit, Satz von Jordan-Hölder, freie Gruppen).
Die algebraische Behandlung der Konstruktionen mit Zirkel und Lineal führt nur bis zum notwendigen Kriterium, das immerhin erlaubt, die bekannten Sätze über Nicht-Konstruierbarkeit zu beweisen. Den Begriff des Zerfällungskörpers eines Polynoms und den Beweis seiner Eindeutigkeit behandeln wir in Abschnitt 9.4, haben aber die Theorie der endlichen Körper ohne deren Benutzung aufgebaut, so dass man diesen Abschnitt überspringen kann, wenn man möglichst rasch zu den endlichen Körpern kommen will.

Auf einige für das weitere Verständnis nicht notwendige Themen wird in ergänzenden Bemerkungen oder in Abschnitten eingegangen, die in der Überschrift als Ergänzung gekennzeichnet sind. Bei einer einsemestrigen an dem Buch orientierten Vorlesung wird man auf die Behandlung der meisten dieser Ergänzungen in der Vorlesung verzichten müssen, ihre Lektüre will ich aber interessierten Studierenden, die ein wenig über das Grundwissen hinausgehen wollen, ausdrücklich ans Herz legen.

Die Übungsaufgaben habe ich meiner im Laufe der Jahre entstandenen Sammlung entnommen. Viele von ihnen stammen aus anderen Lehrbüchern, ohne dass ich die ursprünglichen Quellen noch zurück verfolgen kann; die Kollegen, die ihre Aufgaben hier wiederfinden, bitte ich um Verständnis für die fehlende Quellenangabe.

Abschließend möchte ich Christine Wilk-Pitz sowie Michael Bergau, Matthias Horbach und Alexander Rurainski danken, die Teile des Manuskripts als Skript zu der eingangs erwähnten Vorlesung bzw. zu früheren Vorlesungen in LaTeX geschrieben haben. Ferner danke ich Ute Staemmler, Markus

Zacharski und den HörerInnen meiner Vorlesung für etliche Fehlerkorrekturen. LeserInnen, die noch verbliebene Fehler finden, bitte ich, mir diese an `schulzep@math.uni-sb.de` zu melden, damit ich die Korrekturen auf meiner homepage unter `www.math.uni-sb.de/ag/schulze/eazbuch.html` im Internet zugänglich machen kann.

Saarbrücken, November 2006 *Rainer Schulze-Pillot*

0

Voraussetzungen aus den Grundvorlesungen

In den Grundvorlesungen über lineare Algebra werden zur Zeit allgemeine algebraische Grundbegriffe in sehr unterschiedlichem Ausmaß behandelt. In diesem Kapitel werden deshalb die für das Weitere benötigten Grundlagen zusammengestellt. Das meiste wird Leserinnen und Lesern vermutlich bereits bekannt sein.

0.1 Äquivalenzklassen, Gruppen, Ringe

Da dieses Buch sich hauptsächlich an Studierende im zweiten Studienjahr wendet, setzen wir Vertrautheit mit den grundlegenden Begriffen über Mengen und Abbildungen voraus. Auf die für uns besonders wichtigen Zahlenmengen $\mathbb{N}$ der natürlichen und $\mathbb{Z}$ der ganzen Zahlen gehen wir in Kapitel 1 noch näher ein, setzen sie aber für Beispiele in diesem Kapitel zunächst als bekannt voraus. Wie in der Zahlentheorie üblich gehört 0 nicht zu $\mathbb{N}$, wir schreiben $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$.
Auch die Begriffe *Äquivalenzrelation* und *Äquivalenzklasse* kennt die Leserin ebenso wie der Leser vermutlich bereits. Das in diesem Buch am häufigsten vorkommende Beispiel einer Äquivalenzrelation ist die Kongruenz modulo n:

Beispiel. Auf der Menge $\mathbb{Z}$ der ganzen Zahlen wird für $n \in \mathbb{N}$ (also insbesondere $n \neq 0$) eine *Kongruenz modulo n* genannte Äquivalenzrelation wie folgt definiert:
a ist genau dann *kongruent* zu b modulo n (Notation: $a \equiv b \bmod n$), wenn $a - b$ durch n teilbar ist. Eine äquivalente Bedingung ist, dass a und b bei Division durch n den selben Rest lassen. Die Äquivalenzklassen bezüglich dieser Relation sind die *Restklassen* modulo n. Ist also etwa $n = 2$, so sind genau die geraden Zahlen kongruent zu 0 modulo 2, die ungeraden Zahlen sind kongruent zu 1 modulo 2, die Menge $\mathbb{Z}$ zerfällt in zwei Äquivalenzklassen:
Die eine Klasse besteht aus den geraden Zahlen, die andere besteht aus den ungeraden Zahlen. Innerhalb einer Klasse sind alle Zahlen zueinander kongru-

ent modulo 2, zwei Zahlen aus verschiedenen Klassen sind nicht zueinander kongruent.
Ist $n = 3$, so besteht etwa die Äquivalenzklasse der 1 (d. h. die Menge aller zu 1 modulo 3 kongruenten ganzen Zahlen) aus den Zahlen

$$\ldots, -8, -5, -2, 1, 4, 7, \ldots.$$

Jede solche Äquivalenzklasse bezüglich der Kongruenz modulo n (d. h. die Menge aller zu einem festen $a \in \mathbb{Z}$ modulo n kongruenten Zahlen) nennt man auch eine *arithmetische Progression* modulo n, sie kann auch als $\{a + kn \mid k \in \mathbb{Z}\}$ charakterisiert werden.

Aus einer Vorlesung über Lineare Algebra im ersten Studienjahr sollte dem Leser darüber hinaus die Theorie der Vektorräume über einem (beliebigen) Körper vertraut sein.
In der Regel werden in einer solchen Vorlesung auch einige Grundtatsachen über Gruppen und über Ringe behandelt. Diese Grundtatsachen und -begriffe werden wir im Rahmen der ausführlicheren Behandlung von Gruppen und Ringen hier zwar erneut behandeln, wir wollen sie aber gelegentlich in Beispielen schon vorher benutzen können.
Wir listen daher kurz auf, was wir hierüber in solchen Beispielen voraussetzen wollen und verweisen für die gründlichere Behandlung dieser Dinge auf die entsprechenden Kapitel:

Definition 0.1. *Eine (nicht leere) Menge G mit einer Verknüpfung $\circ : (a, b) \longmapsto a \circ b$ (also einer Abbildung $G \times G \longrightarrow G$, die jedem Paar (a, b) von Elementen von G ein Element $c = a \circ b$ von G zuordnet) heißt Gruppe, wenn gilt:*

a) $a \circ (b \circ c) = (a \circ b) \circ c$ für alle $a, b, c \in G$ (Assoziativgesetz)
b) Es gibt ein (eindeutig bestimmtes) Element $e \in G$ mit $e \circ a = a \circ e = a$ für alle $a \in G$. (e heißt neutrales Element.)
c) Zu jedem $a \in G$ gibt es ein (eindeutig bestimmtes) Element a' (oder a^{-1}) in G mit $a' \circ a = a \circ a' = e$. ($a'$ heißt inverses Element zu a.)
d) Gilt überdies das Kommutativgesetz *$a \circ b = b \circ a$ für alle $a, b \in G$, so heißt die Gruppe* kommutativ *oder* abelsch *(nach Niels Henrik Abel, 1802–1829)*

Bemerkung.

a) Es reicht, in ii) die Existenz eines Elements $e \in G$ mit $e \circ a = a$ für alle $a \in G$ (also eines linksneutralen Elements von G) und in iii) für jedes $a \in G$ die Existenz eines $a' \in G$ mit $a' \circ a = e$ (also für jedes $a \in G$ die Existenz eines linksinversen Elements) zu verlangen. Beweis als Übung, genauso geht es natürlich mit rechts statt links. Dagegen erhält man etwas anderes (nicht besonders sinnvolles), wenn man die Existenz eines linksneutralen Elements und für jedes $a \in G$ die Existenz eines rechtsinversen Elements verlangt.

b) Nach Niels Henrik Abel (der in seiner kurzen Lebenszeit zahlreiche bedeutende Beiträge zur Algebra und zur Funktionentheorie geleistet hat) ist auch der seit 2003 jährlich als Analogon zum Nobelpreis in Oslo verliehene Abel-Preis mit einem Preisgeld von 6 Millionen Norwegischen Kronen (ca. 740000 Euro) benannt (bisherige Preisträger: 2003 Jean Pierre Serre, 2004 Michael Atiyah und Isadore Singer, 2005 Peter Lax, 2006 Lennart Carleson, 2007 Srinivasa Varadhan, 2008 John Thompson und Jacques Tits).

Satz 0.2. *Sei $(G, \circ)$ eine Gruppe. Dann gilt:*

(a) Für alle $a \in G$ ist $(a^{-1})^{-1} = a$.
(b) Für alle $a, b \in G$ ist $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$.
(c) Sind $a, b \in G$, so gibt es genau ein $x \in G$ mit $a \circ x = b$ und genau ein $y \in G$ mit $y \circ a = b$.
(d) Sind $a, x, y \in G$ mit $x \circ a = y \circ a$, so ist $x = y$.
(e) Sind $a, x, y \in G$ mit $a \circ x = a \circ y$, so ist $x = y$.

Definition 0.3. *Sei $(G, \circ)$ eine Gruppe mit neutralem Element e. Die Teilmenge $U \subseteq G$ heißt* Untergruppe*, wenn gilt:*

a) $e \in U$
b) $a, b \in U \implies ab \in U$
c) $a \in U \implies a^{-1} \in U$

Man schreibt dann auch $U \leq G$ oder $U < G$.

Definition 0.4. *Eine Menge R mit (Addition und Multiplikation genannten) Verknüpfungen $+, \cdot : R \times R \longrightarrow R$ heißt* Ring*, wenn gilt:*

a) $(R, +)$ ist kommutative Gruppe (mit neutralem Element 0).
b) Die Multiplikation $\cdot$ ist assoziativ: Für $a, b, c \in R$ gilt $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
c) Es gelten die Distributivgesetze

$$a \cdot (b + c) = a \cdot b + a \cdot c$$
$$(a + b) \cdot c = a \cdot c + b \cdot c \quad \text{für } a, b, c \in R$$

Falls es ein neutrales Element $1 \in R$ bezüglich der Multiplikation gibt, so heißt 1 das Einselement *des Ringes und R ein* Ring mit Einselement*.*
Ist die Multiplikation kommutativ, so heißt R ein kommutativer Ring*.*
Gibt es $a, b \in R$, $a \neq 0 \neq b$ mit $a \cdot b = 0$, so heißen a, b Nullteiler *in R, andernfalls heißt R* nullteilerfrei*.*
Ein kommutativer Ring $R \neq \{0\}$ mit Einselement, der nullteilerfrei ist, heißt Integritätsbereich*.*
Ein kommutativer Ring $R \neq \{0\}$ mit Einselement 1, in dem es zu jedem $a \neq 0$ ein multiplikatives Inverses a^{-1} gibt (also $aa^{-1} = a^{-1}a = 1$), heißt ein Körper; lässt man hier die Forderung der Kommutativität fort, so spricht man von einem Schiefkörper.

Bemerkung. a) Das Verknüpfungszeichen für die Multiplikation wird meistens fortgelassen: $ab := a \cdot b$.
b) In einem Ring gilt stets $a \cdot 0 = 0 \cdot a = 0$ für alle $a \in R$.
c) Gibt es im Ring R ein neutrales Element bezüglich der Multiplikation, so ist dieses eindeutig bestimmt.
d) Für den Rest dieses Buches haben alle Ringe ein Einselement. In der Literatur wird die Existenz des Einselements manchmal zur Definition des Begriffes Ring hinzugenommen, manchmal nicht.
e) Der Nullring $\{0\}$ ist von dieser Definition ebenfalls zugelassen, in ihm ist das einzige Element gleichzeitig Nullelement und Einselement.

Lemma 0.5. *Ein kommutativer Ring R ist genau dann nullteilerfrei, wenn in R die Kürzungsregel gilt, d. h., wenn für $a, b, c \in R, a \neq 0$ gilt:*

$$ab = ac \Leftrightarrow b = c.$$

Beweis. Sei R nullteilerfrei und seien $a, b, c \in R, a \neq 0$ mit $ab = ac$. Dann ist $0 = ab - ac = a(b - c)$ mit $a \neq 0$, also $b - c = 0$ nach Definition der Nullteilerfreiheit und daher $b = c$.
Gilt umgekehrt in R die Kürzungsregel und sind $a, b \in R, a \neq 0$ mit $ab = 0$, so ist $0 = ab = a0$ und nach der Kürzungsregel folgt $b = 0$, also ist R nullteilerfrei. □

Beispiele:

- $\mathbb{Z}$ ist ein Ring ohne Nullteiler.
- Ist K ein Körper, so ist K erst recht ein Ring (ohne Nullteiler).
- Ist K ein Körper, so ist die Menge $M_n(K)$ der $n \times n$- Matrizen mit Einträgen aus dem Körper K ein Ring, dessen Einselement die Einheitsmatrix E_n ist.
- Ist K ein Körper, V ein K-Vektorraum, so ist die Menge $\mathrm{End}(V)$ der linearen Abbildungen von V in sich ein Ring, dessen Einselement die identische Abbildung Id_V ist.
- Sei $C(\mathbb{R})$ die Menge der stetigen Funktionen von $\mathbb{R}$ nach $\mathbb{R}$. Dann ist $C(\mathbb{R})$ bezüglich der üblichen Operationen $(f + g)(x) = f(x) + g(x), (fg)(x) = f(x)g(x)$ ein kommutativer Ring, der nicht nullteilerfrei ist. Das Gleiche gilt, wenn man stattdessen die Menge aller Funktionen oder die Menge aller differenzierbaren Funktionen von $\mathbb{R}$ nach $\mathbb{R}$ betrachtet.

Definition 0.6. *Sei R ein kommutativer Ring (wie stets mit Einselement 1). $a \in R$ heißt* Einheit *in R, wenn es $a' \in R$ gibt mit $aa' = 1$. Die Menge der Einheiten wird mit $R^\times$ bezeichnet.*

Beispiele:

- Die Einheiten in $\mathbb{Z}$ sind $+1, -1$.
- Die Einheiten im Ring $C(\mathbb{R})$ der stetigen reellen Funktionen sind die Funktionen, die keine Nullstelle haben.

- In einem Körper K sind alle Elemente außer 0 Einheiten, die Menge $K^\times$ der Einheiten von K ist also gleich $K \setminus \{0\}$.

Lemma 0.7. *Sei R ein kommutativer Ring (wie immer mit Einselement). Dann ist die Menge $R^\times$ der Einheiten von R unter der Multiplikation in R abgeschlossen; bezüglich der Multiplikation von R als Verknüpfung ist sie eine Gruppe, die* Einheitengruppe *von R.*

Beweis. Übung. □

Häufig vorkommende Abschwächungen des Gruppenbegriffs sind die beiden folgenden Begriffe, auf die wir aber in diesem Buch nicht näher eingehen:

Definition 0.8. *Eine Menge $H \neq \emptyset$ mit einer Verknüpfung $(a, b) \longmapsto a \cdot b$ heißt* Halbgruppe*, wenn die Verknüpfung assoziativ ist. Sie heißt* Monoid*, wenn es ein (notwendig eindeutig bestimmtes) Element $e \in H$ gibt mit*

$$ea = ae = a \text{ für alle } a \in H;$$

e heißt dann das neutrale Element *von H.*

Definition 0.9. *Sei K ein Körper. Eine K-*Algebra *ist ein K- Vektorraum A, auf dem zusätzlich eine Multiplikation $(a, b) \mapsto a \cdot b$ definiert ist und für den gilt:*

a) $(A, +, \cdot)$ ist ein (nicht notwendig kommutativer) Ring mit Einselement.
b) Für $a, b \in A, \lambda \in K$ gilt $\lambda(a \cdot b) = (\lambda a) \cdot b = a \cdot (\lambda b)$.

*Sind A und B zwei K-Algebren und $f : A \longrightarrow B$ eine lineare Abbildung mit $f(a_1 a_2) = f(a_1) f(a_2)$ für alle $a_1, a_2 \in A$ und $f(1_A) = 1_B$, so sagt man, f sei ein K-*Algebrenhomomorphismus *(oder ein* Homomorphismus von K-Algebren*). Ist f zudem bijektiv, so nennt man f einen* Isomorphismus *von Algebren.*

Beispiel. a) Ist K ein Körper und $L \supseteq K$ ein Oberkörper von K, so ist L eine K-Algebra.
b) Ist K ein Körper und $M_n(K)$ die Menge der $n \times n$-Matrizen über K, so ist $M_n(K)$ eine K-Algebra.
c) Ist K ein Körper, V ein K-Vektorraum, so ist $\mathrm{End}(V)$ eine K-Algebra.

0.2 Polynomring

In der Vorlesung über Lineare Algebra wird bei der Behandlung des charakteristischen Polynoms und des Minimalpolynoms einer Matrix meistens auch eine formale Definition des Polynomringes über einem beliebigen Körper vorgenommen, da über einem beliebigen Körper K die vom Grundkörper $\mathbb{R}$ gewohnte Behandlung von Polynomen als K-wertige Polynomfunktionen zu Problemen führt.

Die üblichste Art, diesen Polynomring einzuführen, ist die folgende, bei der wir zunächst einmal in einer Art Forderungskatalog festlegen, welche Eigenschaften wir vom Ring der Polynome in einer Variablen X mit Koeffizienten in dem Körper K erwarten:

Definition 0.10. *Sei K ein Körper. Ein* Polynomring *über K in einer Unbestimmten X ist ein kommutativer Ring A (mit Einselement) 1 und einem ausgezeichneten Element X, so dass gilt:*

a) A ist eine K-Algebra
b) Jedes Element $f \neq 0$ von A lässt sich eindeutig als

$$f = \sum_{i=0}^{n} a_i X^i \quad \text{mit } a_i \in K,\ a_n \neq 0$$

für ein $n \in \mathbb{N}$ schreiben.
Hat $f \neq 0$ diese Darstellung, so heißt f vom Grad n *und a_n der* Leitkoeffizient *von f, man schreibt $\deg(f) = n$. Dem Nullpolynom wird der Grad $-\infty$ (oder gar kein Grad) zugeordnet.*
Das Polynom f heißt normiert*, falls $a_n = 1$ gilt.*

Mit dieser Definition wissen wir zwar, was wir erreichen wollen, wir müssen uns aber den gewünschten Polynomring erst noch konstruieren.
Der nächstliegende Versuch ist zweifellos, den Polynomring als Ring von Funktionen zu definieren, die durch einen polynomialen Term gegeben sind, also als Menge aller Abbildungen $f : K \longrightarrow K$, für die es $a_0, \ldots, a_n \in K$ gibt, so dass

$$f(x) = \sum_{j=0}^{n} a_j x^j \quad \text{für alle } x \in K$$

gilt.
Die Leserin, die bereits Erfahrung im Umgang mit dem aus zwei Elementen 0 und 1 (mit $0+0=1+1=0, 0+1=1+0=1, 0\cdot 0=0\cdot 1=1\cdot 0=0, 1\cdot 1=1$) bestehenden Körper $\mathbb{F}_2$ hat, wird bemerken, dass dieser erste Versuch im Fall $K = \mathbb{F}_2$ fehlschlägt:
Für $K = \mathbb{F}_2$ gibt es genau vier Abbildungen $K \longrightarrow K$, während Teil b) der Definition impliziert, dass der Polynomring unendlich viele Elemente hat. Berücksichtigt man noch, dass $x^n = x$ für alle $n \in \mathbb{N} \setminus \{0\}$ und alle Elemente x von $\mathbb{F}_2$ gilt, so sieht man, dass jede dieser vier Abbildungen durch unendlich viele verschiedene Terme als polynomiale Abbildung gegeben werden kann.
Es ist aber auf Grund der Definition naheliegend, wie man bei der Konstruktion vorzugehen hat: Ein Polynom $f = \sum_{i=0}^{n} a_i X^i$ soll durch das $(n+1)$-Tupel seiner Koeffizienten $a_i \in K$ bestimmt sein, wobei $n = \deg(f) \in \mathbb{N}_0 = \mathbb{N} \cup \{0\}$ von f abhängt und beliebig groß sein kann. Ergänzen wir dieses $(n+1)$-Tupel durch unendlich viele Nullen zu einer unendlichen Folge $(a_j)_{j\in\mathbb{N}_0}$ von Elementen von K, so sind in dieser Folge offenbar nur endlich viele (nämlich

höchstens $\deg(f)+1$ viele) Folgenglieder von 0 verschieden. Umgekehrt erhalten wir jede Folge $(a_j)_{j\in\mathbb{N}_0}$ von Elementen von K, in der nur endlich viele Folgenglieder von 0 verschieden sind, als Fortsetzung des Koeffiziententupels eines Polynoms. Polynome im Sinne unserer Definition müssen also in Bijektion zu solchen Folgen stehen.
Da im Polynomring das Distributivgesetz gelten soll, ist ferner klar, dass das Produkt fg von zwei Polynomen $f=\sum_{i=0}^{n} a_iX^i$ und $g=\sum_{j=0}^{m} b_jX^j$ gleich $\sum_{k=0}^{n+m} c_kX^k$ mit $c_k=\sum_{i+j=k} a_ib_j$ sein muss, wenn es überhaupt möglich ist, den Polynomring wie gewünscht zu konstruieren.
Damit ist im Grunde vorgezeichnet, was wir zu tun haben:

Definition und Satz 0.11. *Sei K ein Körper. In*

$$A := K[X] := K^{(\mathbb{N}_0)} = \{a=(a_j)_{j\in\mathbb{N}_0} \mid a_j\in K,\ a_j=0 \text{ für fast alle } j\}$$

werde eine Verknüpfung (Multiplikation) definiert durch:

$$(a\cdot b)_n=\sum_{j=0}^{n} a_jb_{n-j},$$

ferner sei die Addition wie üblich durch

$$(a+b)_n=a_n+b_n$$

definiert. Dann gilt:

a) A mit $+$ und $\cdot$ ist eine kommutative K-Algebra
b) Die Elemente $e^{(i)}\in A$ seien für $i\in\mathbb{N}_0$ definiert durch

$$(e^{(i)})_n := \delta_{in}.$$

Dann ist $e^{(0)}$ das Einselement von A, und für $i,j\in\mathbb{N}_0$ gilt

$$e^{(i)}\cdot e^{(j)}=e^{(i+j)}.$$

Insbesondere gilt mit $X:=e^{(1)}$:

$$X^i=e^{(i)} \quad \text{für alle } i\in\mathbb{N}_0.$$

c) Ist $0\neq a\in A$ und $n:=\max\{j\in\mathbb{N}_0 \mid a_j\neq 0\}$, so ist

$$a=\sum_{j=0}^{n} a_jX^j.$$

d) Der Ring A ist ein Polynomring über K im Sinne von Definition 0.10. Jeder Polynomring A' in einer Unbestimmten X' über K ist zu A kanonisch isomorph durch

$$\sum_{i=0}^{n} a_iX^i \longmapsto \sum_{i=0}^{n} a_i(X')^i,$$

d.h., die angegebene Abbildung ist ein bijektiver Homomorphismus von K-Algebren.

e) $A = K[X]$ *ist nullteilerfrei und es gilt* $\deg(fg) = \deg(f) + \deg(g)$ *für von* 0 *verschiedene Polynome* f, g.
f) *Die Einheiten in* $K[X]$ *sind die konstanten Polynome* c *(Polynome vom Grad* 0*) mit* $c \in K^\times$.

Beweis. a) Dass $(A, +)$ eine abelsche Gruppe ist, ist klar. Die Assoziativität der Multiplikation müssen wir nachrechnen:
Sind $a, b, c \in A$, so ist der n-te Koeffizient $((ab)c)_n$ von $(ab)c$ gleich

$$\sum_{k=0}^{n}(\sum_{j=0}^{k}(a_j b_{k-j})c_{n-k} = \sum_{\substack{r,s,t \\ r+s+t=n}} a_r b_s c_t,$$

und den gleichen Wert erhält man, wenn man den n-ten Koeffizienten von $a(bc)$ ausrechnet.
Die Existenz des Einselements sehen wir in b), die Kommutativität ist klar, das Distributivgesetz und die Identität $\lambda(ab) = (\lambda a) \cdot b = a \cdot (\lambda b)$ für $\lambda \in K$, $a, b \in A$ rechnet man leicht nach.
b) Offenbar ist $(e^{(0)} \cdot a)_n = \sum_{j=0}^{n} e_j^{(0)} a_{n-j} = 1 \cdot a_n = a_n$ und daher $e^{(0)} \cdot a = a$ für beliebiges $a \in A$, $e^{(0)}$ ist daher neutrales Element bezüglich der Multiplikation in A.
Sind $i, j \in \mathbb{N}_0$, so hat man

$$(e^{(i)} \cdot e^{(j)})_n = \sum_{k=0}^{n} e_k^{(i)} e_{n-k}^{(j)} = \sum_{k=0}^{n} \delta_{ik}\delta_{j,n-k} = \begin{cases} 1 & \text{falls } i+j=n \\ 0 & \text{sonst} \end{cases},$$

also $e^{(i)} \cdot e^{(j)} = e^{(i+j)}$ wie behauptet. Mit vollständiger Induktion folgt daraus sofort $X^i := (e^{(1)})^i = e^{(i)}$.
c) folgt sofort aus b).
Der erste Teil von d) ist jetzt ebenfalls sofort klar. Hat man einen weiteren Polynomring A' über K in einer Unbestimmten X', so ist zunächst die Abbildung $\sum_{i=0}^{n} a_i X^i \longmapsto \sum_{i=0}^{n} a_i (X')^i$ bijektiv. Dass sie ein Homomorphismus von K-Algebren ist, rechnet man leicht nach.
e) folgt schließlich so: Sind $f = \sum_{i=0}^{m} a_i X^i, g = \sum_{j=0}^{n} b_j X^j \in A$ mit $a_m \neq 0, b_n \neq 0$, so ist

$$f \cdot g = \sum_{k=0}^{n+m} c_k X^k$$

mit $c_{m+n} = a_m b_n \neq 0$, da K ein Integritätsbereich ist.
Also gilt in A, dass aus $f \neq 0, g \neq 0$ folgt, dass $fg \neq 0$ ist und dass fg den Grad $n+m$ hat. Insbesondere erbt also der Polynomring A wie behauptet die Nullteilerfreiheit seines Grundrings K.
f) Übung □

Bemerkung. a) Im Weiteren wird einfach von **dem** Polynomring $K[X]$ in einer Unbestimmten über K gesprochen, seine Elemente werden als $\sum_{i=0}^{n} a_i X^i$ geschrieben und auf die Definition durch Folgen wird kein Bezug mehr genommen. Die Elemente von $K[X]$ fasst man als formale Ausdrücke (polynomiale Terme) $\sum_{i=0}^{n} a_i X^i$ auf. Die konstanten Polynome (Polynome vom Grad 0) cX^0 mit $c \in K$ werden mit den Elementen von K identifiziert, man fasst also den Grundkörper K über diese Identifikation als Teilring des Polynomrings $K[X]$ auf.

b) Ist S irgendeine K-Algebra, so kann man (siehe das folgende Lemma) Elemente von S in Polynome aus $K[X]$ einsetzen: Ist $f = \sum_{i=0}^{n} a_i X^i \in K[X]$, $s \in S$, so ist

$$f(s) := \sum_{i=0}^{n} a_i s^i \in S.$$

Wenn dadurch kein Irrtum entstehen kann, so bezeichnet man (nicht völlig korrekt) auch die hierdurch gegebene Abbildung $s \mapsto f(s)$ von S nach S (die zu f gehörige *Polynomfunktion*) mit f, will man vorsichtiger sein, so kann man sie zur Unterscheidung von $f \in K[X]$ etwa mit $\bar{f}$ bezeichnen.
Wählt man hier $S = A$, so ergibt Einsetzen von X das Element $f(X) = \sum_{i=0}^{n} a_i X^i = f$ von A. Sie brauchen also an dieser Stelle nicht zwischen f und $f(X)$ zu unterscheiden, obwohl es Ihnen ja in der Analysis bereits ganz selbstverständlich geworden ist, zwischen der Funktion h und ihrem Funktionswert $h(x)$ in einem Punkt x sauber zu unterscheiden.
Die Situation ist hier scheinbar anders, weil ja ein Polynom gerade so definiert worden ist, dass es nicht eine Funktion ist, sondern ein Element der abstrakt konstruierten Algebra $K[X]$.

Lemma 0.12. *Sei K ein Körper, S eine K-Algebra und $s \in S$. Dann wird durch*

$$f \longmapsto f(s) \in S$$

ein Algebrenhomomorphismus $K[X] \longrightarrow S$ gegeben; der Einsetzungshomomorphismus *in s.*

Beweis. Man rechnet nach, dass auf Grund der Rechengesetze in S die Gleichungen $(f_1 + f_2)(s) = f_1(s) + f_2(s)$, $(f_1 f_2)(s) = f_1(s) f_2(s)$, $(cf)(s) = c \cdot f(s)$ und $1(s) = (1 \cdot X^0)(s) = 1 \cdot s^0 = 1_S$ gelten und die Abbildung daher in der Tat ein Homomorphismus von Algebren ist. □

Beispiel. In der linearen Algebra betrachtet man den Fall, dass $S = M_n(K)$ der Ring der $n \times n$-Matrizen über dem Körper K ist. Für $A \in M_n(K)$ besteht dann das Bild des Einsetzungshomomorphismus in A aus den Polynomen $\sum_{i=0}^{n} c_i A^i \in M_n(K)$ in A, und das Minimalpolynom von A ist das normierte Polynom f kleinsten Grades, das unter diesem Einsetzungshomomorphismus auf die Nullmatrix $0_n \in M_n(K)$ abgebildet wird.

Bemerkung. Man kann in der ganzen Diskussion den Grundkörper K auch durch einen beliebigen Integritätsbereich R ersetzen und so den Polynomring $R[X]$ über R konstruieren. Der einzige Punkt, bei dem man etwas vorsichtig sein muss, ist die Beschreibung der Einheiten: Im Polynomring $R[X]$ sind die Einheiten genau die konstanten Polynome $c = cX^0$ mit einer Einheit $c \in R^\times$ von R, zum Beispiel für $R = \mathbb{Z}$ also nur die konstanten Polynome ± 1. Die richtige Verallgemeinerung von $K^\times$ ist also hier die (ebenso notierte) Einheitengruppe des Rings R und nicht $R \setminus \{0\}$.
Wählt man als Grundring einen Ring mit Nullteilern, so enthält auch der Polynomring $R[X]$ Nullteiler und auch die Gleichung $\deg(fg) = \deg(f) + \deg(g)$ wird falsch. Sind nämlich $a, b \in R$ mit $ab = 0, a \neq 0 \neq b$, so gilt offensichtlich $(1 + aX^m) \cdot (bX^n) = bX^n$ für alle $m, n \in \mathbb{N}$, man hat also $\deg((1 + aX^m) \cdot (bX^n)) = n \neq m + n = \deg(1 + aX^m) + \deg(bX^n)$.

Vermutlich ist aus der Schule oder den Anfängervorlesungen bekannt, dass sich das Verfahren der Division mit Rest vom Ring $\mathbb{Z}$ (siehe Lemma 1.2 im nächsten Abschnitt) auf den Ring der reellen Polynome in einer Variablen übertragen lässt (Polynomdivision), wir formulieren und beweisen das jetzt für den Polynomring $K[X]$ über einem beliebigen Körper und erhalten damit die erste in einer Reihe von Aussagen, die zeigen werden, dass der Polynomring über einem Körper einige Ähnlichkeit mit dem Ring der ganzen Zahlen hat.

Satz 0.13. *Sei K ein Körper, seien $f, g \in K[X], g \neq 0$. Dann gibt es eindeutig bestimmte Polynome $q, r \in K[X]$ mit*

$$f = qg + r, \quad r = 0 \text{ oder } \deg(r) < \deg(g).$$

Beweis. Wir beweisen diese Aussage durch vollständige Induktion nach dem Grad $\deg(f)$ von f, beginnend bei $\deg(f) = 0$. Der Induktionsanfang $\deg(f) = 0$ ist trivial. Wir schreiben $f = \sum_{i=0}^{m} a_i X^i, g = \sum_{i=0}^{n} b_i X^i$ mit $a_m \neq 0, b_n \neq 0, m \geq 1$ und nehmen an, die Aussage sei für $\deg(f) < m$ bereits bewiesen. Ist $\deg(f) < \deg(g)$, so ist die Aussage (mit $q = 0, r = f$) trivial, wir können also $n \leq m$ annehmen. Dann ist der Grad von

$$\begin{aligned} f_1 &:= f - (\frac{a_m}{b_n} X^{m-n})g \\ &= (a_m X^m - (\frac{a_m}{b_n} X^{m-n}) b_n X^n) + \sum_{i=0}^{m-1} c_i X^i \\ &= \sum_{i=0}^{m-1} c_i X^i \end{aligned}$$

(mit gewissen $c_i \in K$, die hier nicht weiter interessieren) offenbar kleiner als m, wir können also nach Induktionsannahme

$$f_1 = q_1 g + r \text{ mit } r = 0 \text{ oder } \deg(r) < \deg(g)$$

schreiben und erhalten

$$f = (q_1 + \frac{a_m}{b_n} X^{m-n})g + r,$$

was mit $q = q_1 + \frac{a_m}{b_n} X^{m-n}$ die gewünschte Zerlegung $f = qg + r$ für f liefert. Hat man zwei Zerlegungen $f = qg + r = q'g + r'$, so ist $(q - q')g = r' - r$, also ist $q - q' = 0$ oder $\deg(g) \leq \deg(q - q') + \deg(g) = \deg(r - r') < \deg(g)$, was unmöglich ist. Wir haben also $q = q'$ und daher auch $r = r'$. □

Beispiel. Durch den üblichen Prozess der Polynomdivision erhält man etwa:

$$(X^4 - 1) = (X^2 + 2X + 1)(X^2 - 2X + 3) + (-4X - 4).$$

Bemerkung. Im Beweis benutzt man Division durch den Leitkoeffizienten $b_n \neq 0$ von $g = \sum_{i=0}^{n} b_i X^i$; das Verfahren der Division mit Rest lässt sich daher nicht ohne weiteres auf den Polynomring $R[X]$ über einem Ring R übertragen (siehe Übung 0.3).

Eine wichtige Anwendung der Division mit Rest ist die Möglichkeit, für eine Nullstelle $a \in K$ eines Polynoms aus $K[X]$ einen Faktor $X - a$ aus dem Polynom herauszuziehen:

Definition und Korollar 0.14. *Sei K ein Körper.*

a) Sei $f \in K[X]$, $f \neq 0$, $a \in K$ mit $f(a) = 0$. Dann gibt es ein eindeutig bestimmtes $q \in K[X]$ mit $f = (X - a)q$.

b) Sind $\beta_1, \ldots, \beta_r$ verschiedene Nullstellen von $0 \neq f \in K[X]$, so gibt es eindeutig bestimmte $e_i \in \mathbb{N} \setminus \{0\}$, $g \in K[X]$ mit

$$f = \prod_{i=1}^{r} (X - \beta_i)^{e_i} g \text{ und } g(\beta_i) \neq 0 \text{ für } 1 \leq i \leq r.$$

Der Exponent e_i in dieser Darstellung heißt die Vielfachheit *der Nullstelle β_i des Polynoms f, ist $e_i = 1$, so spricht man von einer* einfachen Nullstelle*, sonst von einer* mehrfachen*.*

c) Seien $f, g \in K[X]$ mit $n > \max(\deg(f), \deg(g))$, seien $a_1, \ldots, a_n \in K$ paarweise verschieden mit $f(a_i) = g(a_i)$ für $1 \leq i \leq n$.
Dann ist $f = g$.
Insbesondere gilt: Hat K unendlich viele Elemente, so folgt aus $f(a) = g(a)$ für alle $a \in K$, dass $f = g$ gilt.

d) Hat K unendlich viele Elemente, so ist der Polynomring $K[X]$ isomorph zum Ring der Abbildungen $f : K \longrightarrow K$, die durch polynomiale Terme gegeben sind.

Beweis. a) Wir teilen f mit Rest durch $X - a$. Wäre der Rest hierbei nicht 0, so hätte er wegen $\deg(X - a) = 1$ Grad 0, wäre also gleich einer Konstanten $c \in K$. Setzen wir in die Polynomgleichung $f = (X - a)q + c$ den Wert $a \in K$ ein, so erhalten wir

$$0 = f(a) = (a-a)q(a) + c,$$

also $c = 0$.

b) Zunächst ist klar, dass man eine Darstellung

$$f = \prod_{i=1}^{r}(X-\beta_i)^{e_i} g \text{ und } g(\beta_i) \neq 0 \text{ für } 1 \leq i \leq r.$$

erhält, indem man a) so oft iteriert, bis der verbleibende Faktor g in keinem der β_i verschwindet. Hat man zwei derartige Darstellungen $f = \prod_{i=1}^{r}(X-\beta_i)^{e_i} g = f = \prod_{i=1}^{r}(X-\beta_i)^{e_i'} g'$ und ist etwa $e_1 \geq e_1'$, so kann man, da $K[X]$ nullteilerfrei ist, den Faktor $(X-\beta_1)^{e_1'}$ in der rechten Gleichung dieser Kette kürzen und erhält

$$(X-\beta_1)^{e_1-e_1'} \prod_{i=2}^{r}(X-\beta_i)^{e_i} g = \prod_{i=2}^{r}(X-\beta_i)^{e_i'} g'.$$

Einsetzen von β_1 in diese Gleichung liefert dann $e_1 - e_1' = 0$, da sonst die linke Seite 0 ergäbe und die rechte nicht. Das iteriert man für die anderen Faktoren $(X-\beta_i)$ und erhält am Ende $g = g'$.

c) In b) sehen wir, dass $f = \prod_{i=1}^{r}(X-\beta_i)^{e_i} g$ Grad $\deg(g) + \sum_{i=1}^{r} e_i$ hat, insbesondere muss $r \leq n$ für die Anzahl r der verschiedenen Nullstellen eines Polynoms $f \neq 0$ vom Grad n gelten. Anders gesagt: Nimmt ein Polynom $f \neq 0$ in n verschiedenen Stellen $a_1, \ldots, a_n$ den Wert 0 an, so muss $\deg(f) \geq n$ gelten.
Da in der Situation von c) $\deg(f-g) < n$ gilt und $f-g$ in den n verschiedenen Stellen $a_1, \ldots, a_n$ den Wert 0 annimmt, ist $f - g = 0$, also $f = g$.

d) Aus c) folgt, dass die (offenbar surjektive) Abbildung, die jedem $f \in K[X]$ die Funktion $a \mapsto f(a)$ zuordnet, für unendliches K injektiv ist. Da sie offenbar ein Algebrenhomomorphismus ist, ist sie ein Isomorphismus.

□

Bemerkung. a) Sind $f \in K[X]$ und $a, c \in K$ mit $f(a) = c$ und hat $f - c$ in a eine e-fache Nullstelle, so sagt man auch, f nehme in a den Wert c mit der Vielfachheit e an.

b) Nimmt das Polynom f vom Grad n in den verschiedenen Elementen $a_1, \ldots, a_r$ von K die Werte $c_1, \ldots, c_r$ mit den Vielfachheiten $e_1, \ldots, e_r$ an, so betrachte man das Polynom

$$f_1 = \sum_{i=1}^{r} c_i \prod_{\substack{j=1 \\ j\neq i}}^{r} \frac{(X-a_j)^{e_j}}{(a_i-a_j)^{e_j}}$$

vom Grad $n_1 < \sum_{i=1}^{r} e_i$ (das *Lagrange'sche Interpolationspolynom* für die vorgegebenen Werte und Vielfachheiten). Offenbar nimmt auch f_1 die

Werte c_i in den Stellen a_i mit den Vielfachheiten e_i an. Ist auch $n = \deg(f) < \sum_{i=1}^{r} e_i$, so sieht man genauso wie in c) des vorigen Korollars, dass $f_1 = f$ gilt. Man hat also nicht nur die Eindeutigkeitsaussage aus Teil c) des Korollars, sondern kann das eindeutige Polynom vom Grad $n_1 < \sum_{i=1}^{r} e_i$ mit der gegebenen Werteverteilung explizit angeben. Wir kommen auf dieses Beispiel in Kapitel 4 zurück.

0.3 Ergänzung: Formale Potenzreihen

Ganz ähnlich wie den Polynomring kann man auch den Ring der formalen Potenzreihen über einem Körper K oder allgemeiner über einem kommutativen Ring mit 1 definieren, ohne sich irgendwelche Gedanken über Konvergenz machen zu müssen. Das spielt für den weiteren Verlauf des Buches keine Rolle, ist aber so interessant und einfach, dass es hier kurz durchgeführt werden soll:

Definition und Satz 0.15. *Sei R ein kommutativer Ring mit Einselement 1. In*

$$B := R[[X]] := R^{\mathbb{N}_0} = \{a = (a_j)_{j\in\mathbb{N}_0} \mid a_j \in R\}$$

werde eine Verknüpfung (Multiplikation) definiert durch:

$$(a \cdot b)_n = \sum_{j=0}^{n} a_j b_{n-j},$$

ferner sei die Addition wie üblich durch

$$(a + b)_n = a_n + b_n$$

definiert. Dann gilt:

a) B mit den Verknüpfungen $+$ und $\cdot$ ist eine kommutative R-Algebra mit Einselement $(1, 0, 0, \ldots)$; sie heißt der Ring der formalen Potenzreihen *in einer Variablen X über R.*

b) Die Elemente $e^{(i)} \in B$ seien für $i \in \mathbb{N}_0$ definiert durch

$$(e^{(i)})_n := \delta_{in}.$$

Dann ist $e^{(0)}$ das Einselement von B, und für $i, j \in \mathbb{N}_0$ gilt

$$e^{(i)} \cdot e^{(j)} = e^{(i+j)}.$$

Insbesondere gilt mit $X := e^{(1)}$:

$$X^i = e^{(i)} \quad \text{für alle } i \in \mathbb{N}_0.$$

c) Ist $0 \neq b \in B$, so schreibt man (formal, also ohne unendliche Summen zu definieren)

$$b = \sum_{j=0}^{\infty} b_j X^j.$$

d) Ist R ein Integritätsbereich, so ist auch $B = R[[X]]$ nullteilerfrei.
e) Die Einheiten in $R[[X]]$ sind die Potenzreihen $b = \sum_{j=0}^{\infty} b_j X^j$ mit $b_0 \in R^\times$.

Beweis. Die Aussagen a),b) sowie d) werden genauso wie für den Polynomring bewiesen. Für e) sei $b = \sum_{j=0}^{\infty} b_j X^j$ mit $b_0 \in R^\times$ gegeben. Wir setzen $c_0 := b_0^{-1}$ und definieren für $n \geq 1$ rekursiv

$$c_n := -b_0^{-1}(c_0 b_n + c_1 b_{n-1} + \cdots + c_{n-1} b_1).$$

Die Definition der Multiplikation für formale Potenzreihen impliziert dann $b \cdot c = 1_B$. □

Übungen

0.1. Zeigen Sie, dass in einem Ring R stets $a\,0 = 0$ für alle $a \in R$ gilt.

0.2. Zeigen Sie, dass in einem Ring R mit Einselement die Menge $R^\times$ der Einheiten in R stets eine Gruppe bezüglich der Multiplikation im Ring ist.

0.3. (Division mit Rest im Polynomring über einem Ring) Sei R ein kommutativer Ring mit 1, seien $f, g \in R[X], f \neq 0, g = \sum_{j=0}^{n} c_j X^j$ mit $c_n \in R^\times$. Zeigen Sie: Es gibt eindeutig bestimmte Polynome $q, r \in R[X]$ mit

$$f = qg + r, \quad r = 0 \text{ oder } \deg(r) < \deg(g).$$

Finden Sie für $R = \mathbb{Z}$ ein Beispiel mit $f, g \in R[X], g = \sum_{j=0}^{n} c_j X^j \neq 0$ aber mit $c_n \notin \{0, 1, -1\}$, in dem die Division mit Rest nicht möglich ist!

0.4. Sei R ein Integritätsbereich. Zeigen Sie für $f, g \in R[X]$:

a) $\deg(f+g) \leq \max\{\deg(f), \deg(g)\}$
b) $\deg(f+g) = \max\{\deg(f), \deg(g)\}$ falls $\deg(f) \neq \deg(g)$

0.5. Definieren Sie für ein Element $a = \sum_{j=0}^{\infty} a_i X^i \neq 0$ des Rings $R[[X]]$ der formalen Potenzreihen über dem Integritätsbereich R den *Untergrad* $\operatorname{ldeg}(a)$ durch

$$\operatorname{ldeg}(a) := \min\{j \in \mathbb{N}_0 \mid a_j \neq 0\}$$

sowie $\operatorname{ldeg}(0) = \infty$. Zeigen Sie für $a, b \in R[[X]]$:

a) $\operatorname{ldeg}(a+b) \geq \min\{\operatorname{ldeg}(a), \operatorname{ldeg}(b)\}$
b) $\operatorname{ldeg}(a+b) = \min\{\operatorname{ldeg}(a), \operatorname{ldeg}(b)\}$ falls $\operatorname{ldeg}(a) \neq \operatorname{ldeg}(b)$.
c) $\operatorname{ldeg}(ab) = \operatorname{ldeg}(a) + \operatorname{ldeg}(b)$