Algebra I (Variante mat200)
Skriptteil der Onlinelehre des SS2020
Universität Oldenburg

Prof. Dr. Anne Frühbis-Krüger
anne.fruehbis-krueger@uol.de

24. Juni 2020

Inhaltsverzeichnis

Kapitel 0

Vorbemerkungen

In diesem Semester finden wir uns alle durch die Pandemie-Situation in eine ganz anderen Lehr- bzw. Lernsituation versetzt als sonst. Die Entscheidung für einen Online-Kurs ist nicht aus didaktischen Gründen gefallen, sondern aus der Not geboren.

Wir werden Ihnen durch die verschiedenen Möglichkeiten der Wissensvermittlung, die uns ohne Präsenzlehre noch zur Verüfung stehen, den Stoff der Algebra I vermitteln und das vorliegende Skript ist ein wesentlicher Bestandteil davon, aber nicht der einzige. Es unterscheidet sich in der Darstellung deutlich von den meisten Skripten, die Sie bisher genutzt haben. In dem Skript werden Sie immer wieder Stellen (meist wichtige Definitionen, Sätze mit Beweis oder Beispiele) mit Verweisen auf kurze Videos lesen, die integraler Bestandteil der Lehrmaterialien sind und dann im StudIP abrufbar sind. Wir haben uns bewusst für gezielt eingesetzte kurze Videos statt einer Live-Vorlesung oder einzelner Vorlesungsvideos entschieden, da uns bewusst ist, dass nicht alle Studierenden über die technischen Voraussetzungen verfügen, um Lehrvideos in Spielfilmlänge konzentriert mitdenkend und ohne Verbindungsabbrüche verfolgen zu können. Darüberhinaus finden Sie gelegentlich Text in blauer Farbe, der dann zusätzliche Erläuterungen enthält. Diese würden in einer normalen Vorlesung als mündliche Ergänzung zum besseren Verständnis in informeller Weise vorkommen. Bitte beachten Sie, dass es sich hier nicht überall um mathematisch so exakte Formulierungen handelt, wie man sie in einem Lehrbuch oder Skript erwartet.

Uns ist selbstverständlich bewusst, dass ein reines Selbststudium an Hand

eines Skripts und flankierender Videos nicht der Betreuung entspricht, die wir alle an einer Präsenzuniversität erwarten. Daher wird es in diesem Semester zu den üblichen Vorlesungszeiten der Algebra I eine Online-Fragestunde im Stud-IP geben, in der ich jeweils auf die Fragen zum Skriptteil und den zugehörigen Videos eingehen werde. Hierbei handelt es sich um ein zusätzliches Angebot und nicht einen Pflichtbestandteil der Veranstaltung, da wir nicht davon ausgehen können, dass alle über ausreichend Bandbreite zur Teilnahme verfügen.

Der Übungsbetrieb wird ebenfalls so normal wie unter den Bedingungen möglich ablaufen mit wöchentlichen Übungsabgaben an den Tutor oder die Tutorin ihrer Übungsgruppe, Videos mit den Lösungen von Abgabe- und 'Präsenz'-aufgaben im StudIP (Übungsveranstaltung) sowie wöchentlichen Online-Meetings der einzelnen Übungsgruppen. Für die Übungsgruppeneinteilung verwenden Sie bitte – unabhängig davon, ob sie die Veranstaltung als Modul mat110 oder mat200 hören – im StudIP das Anmeldeverfahren/die Veranstaltung mit dem Namen mat110. Das Anmeldeverfahren ist ab 15.4. offen, eine Zuteilung zu den Übungsgruppen erfolgt durch Losverfahren unter automatischer Berücksichtigung Ihrer Terminwünsche am 22.4., Nachzügler können sich bis 1.5. noch in Restplätze eintragen oder sich durch die Lehrenden nachtragen lassen.

Ein Online-Kurs erfordert von den Studierenden mehr Disziplin im regelmäßigen Nacharbeiten des jeweils neuen Materials zur Vorbereitung der zugehörigen Online-Fragestunde. Während Sie im Präsenzbetrieb schon vieles durch Besuch der Vorlesung einmal gehört und gesehen haben, ehe sie es nacharbeiten, müssen Sie in diesem Semester selbst den Einstieg finden und sich durch das Material arbeiten. Umso wichtiger ist es, dass Sie kontinuierlich dran bleiben, keine Lücken aufreissen lassen und sich auch trauen, in der Fragestunde zur Vorlesung oder Übung zeitnah nach Dingen zu fragen,die Ihnen nicht klar geworden sind. Sie können sich sicher sein, dass Sie die betreffende Frage nicht als einziger haben!

Noch eine Anmerkung zum Schluß: Da Sie alle die Lineare Algebra bereits bei Frau Dr. Stein, bei mir oder auch bei Herrn Prof. Stein bereits gehört haben und wir dieselbe Notation verwenden, möchte ich für den Umgang mit Mengen, für die Quantorenschreibweise von Aussagen, für Beweistechniken und für grundlegende Eigenschaften von Abbildungen auf den Beginn der

jeweiligen Mitschriften oder Skripte verweisen.

Wir werden mit einer Betrachtung der ganzen Zahlen, die uns als Beispiel immer wieder begleiten werden, aus einer neuen, formaleren Perspektive beginnen. Dabei haben Sie auch gleich die Möglichkeit, den Umgang mit der neuen Situation und den Materialien auf einer inhaltlichen Basis zu erproben, die Ihnen noch nicht allzu fremd sein sollte.

Kapitel 1

Eigenschaften der ganzen Zahlen

Aus der Veranstaltung zur Linearen Algebra ist Ihnen bekannt, dass die ganzen Zahlen $\mathbb{Z}$ mit den üblichen Verknüpfungen der Addition und Multiplikation einen nullteilerfreien, kommutativen Ring bilden, der jedoch kein Körper ist.Ein multiplikatives Inverses besitzen nur die Elemente $\{1, -1\}$. Formaler fassen wir zusammen:

- $(\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring mit Eins.
- $(\mathbb{Z}, +, \cdot)$ besitzt keine Nullteiler.
- $\mathbb{Z}^* := \{a \in \mathbb{Z} \mid \exists b \in \mathbb{Z} : ab = ba = 1\} = \{1, -1\}$.
- $(\mathbb{Z}^*, \cdot)$ ist eine abelsche Gruppe.

Die ganzen Zahlen werden neben dem Polynomring in einer Variable über einem Körper ein grundlegendes Beispiel für viele Sachverhalte in dieser Vorlesung sein. Beim Nacharbeiten neu eingeführter Definitionen in späteren Kapiteln hilft es z.B. oft, sich zu fragen, wie das konkret für $\mathbb{Z}$ oder für $\mathbb{Q}[x]$ ausshe.

Auch die natürlichen Zahlen mit Null, $\mathbb{N}_0$ hatten wir in der Linearen Algebra kennengelernt. Hier sei insbesondere daran erinnert, dass wir das Wohlordnungsaxiom als gegeben annehmen:

Axiom 1.0.1 (Wohlordnungsaxiom) *Jede nicht-leere Teilmenge von* $\mathbb{N}_0$ *besitzt ein kleinstes Element.*

Das Wohlordnungsaxiom ist die Basis des Beweisprinzips der Vollständigen Induktion, die Sie ja bereits in der Linearen Algebra und in Mathematisches Problemlösen und Beweisen verwendet haben.

1.1 Division mit Rest

Satz 1.1.1 (Division mit Rest in $\mathbb{Z}$) *Seien $a \in \mathbb{Z}, b \in \mathbb{N}$. Dann existieren eindeutig bestimmte ganze Zahlen $q, r \in \mathbb{Z}$ mit*

$$a = q \cdot b + r \text{ und } 0 \leq r < b.$$

Die Aussage kennen sie zumindest für die natürlichen Zahlen schon aus der Grundschule. Dort wurde argumentiert, dass so lange immer b Steinchen vom Haufen mit a Steinchen weggenommen werden sollen, bis nicht mehr genug da sind. Der Grundgedanke bleibt derselbe, aber wir werden ihn im Beweis in strenger Formulierung aus dem Wohlordnungsaxiom ableiten.

Beweis:
Schritt 1: Finde einen vielversprechenden Kandidaten für r
Sei

$$M = \{a - c \cdot b \mid c \in \mathbb{Z} \text{ und } a - c \cdot b \geq 0\}.$$

M ist offensichtlich eine Teilmenge von $\mathbb{N}_0$ aufgrund der Nicht-Negativitätsbedingung. Ausserdem gilt für nicht-negative $a \in \mathbb{Z}$ einerseits

$$a = a - 0 \cdot b \in M$$

und für negative $a \in \mathbb{Z}$ andererseits

$$a - b \cdot a = \underbrace{(1-b)}_{\leq 0} \cdot \underbrace{a}_{<0} \in M,$$

weswegen M für beliebiges $a \in \mathbb{Z}$ nicht leer ist. Damit besitzt M nach dem Wohlordnungsaxiom 1.0.1 ein kleinstes Element, das wir mit r bezeichnen wollen.

Schritt 2: Zeige Eigenschaften von r und q
Für dieses r bleibt nun zu zeigen, daß $0 \leq r < b$, wobei die untere Schranke trivial erfüllt ist nach der Konstruktion von M. Würde aber $r \geq b$ gelten, so

wäre $r - b \geq 0$ und damit ein kleineres Element von M im Widerspruch zu der Wahl von r. Daher haben wir in der Tat unser gesuchtes r gefunden, das gesuchte q ist dann das c aus dem zugehörigen Ausdruck $a - c \cdot b = r$.

Schritt 3: Zeige Eindeutigkeit von (q, r)
Seien (r, q) und (r', q') nun zwei Paare, die die geforderten Eigenschaften des Satzes erfüllen und oBda $r \geq r'$. Dann gilt

$$r - r' = a - q \cdot b - (a - q' \cdot b) = (q' - q) \cdot b$$

und wegen $0 \leq r' \leq r < b$ muss damit $q' - q = 0$ gelten,was direkt $r = r'$ und $q = q'$ impliziert.

□

Korollar 1.1.2 *Seien $a, b \in \mathbb{Z}, b \neq 0$. Dann existieren eindeutig bestimmte ganze Zahlen $q, r \in \mathbb{Z}$ mit*

$$a = q \cdot b + r \text{ und } 0 \leq r < |b|.$$

Der Beweis bleibt den Studierenden als Übungsaufgabe überlassen. Ein guter Ausgangspunkt der Überlegungen ist die Division von $-a$ durch $-b$ für negatives b, aber dann muss man genau überlegen, wie man die Bedingung an r erfüllt.

Definition 1.1.3 *Das in Satz 1.1.1 eingeführte r heißt der* **Rest** *der Division von a durch b, kurz*

$$a \bmod b := r$$

das q heißt der **Quotient** *der Division von a durch b, kurz*

$$a \operatorname{div} b := q.$$

Definition 1.1.4 *Seien $a, b \in \mathbb{Z}, b \neq 0$. a heißt* **teilbar** *durch b, wenn der Rest der Division von a durch b null ist.*
Alternative Formulierungen: b **teilt** *a, b ist* **Teiler** *von a, $b \mid a$, a ist* **Vielfaches** *von b.*

Proposition 1.1.5 *Seien $a, b, c, d \in \mathbb{Z}$. Es gilt:*

a) $1 \mid a$, $a \mid a$ *und* $a \mid 0$

b) $0 \mid a \Longleftrightarrow a = 0$

c) $a \mid b$ *und* $b \mid c \Longrightarrow a \mid c$

d) $a \mid b$ *und* $c \mid d \Longrightarrow ac \mid bd$

e) $\forall c \neq 0 : (a \mid b \Longleftrightarrow ac \mid bc)$

f) $c \mid a$ *und* $c \mid b \Longrightarrow c \mid (ka + mb) \forall k, m \in \mathbb{Z}$

g) $a \mid b$ *und* $b \mid a \Longrightarrow a = (\pm 1)b$
(a *ist* **assoziiert** *zu* b*.)*

h) $a \mid b \Longrightarrow a \mid -b$

Beweis: Alle Behauptungen sind direkte Folgerungen aus der Definition der Teilbarkeit bzw. der Division mit Rest. Daher beweisen wir hier nur den Punkt d) exemplarisch und überlassen die anderen den Studierenden zur Übung:

$$\begin{aligned} (a \mid b \text{ und } c \mid d) &\Longrightarrow \exists k, m \in \mathbb{Z} : b = ka \text{ und } d = mc \\ &\Longrightarrow bd = (ka)(mc) \overset{(AG)}{=} kamc \overset{(KG)}{=} kmac \overset{(AG)}{=} (km)(ac) \\ &\Longrightarrow ac \mid bd \end{aligned}$$

□

Sollten Sie noch Kontakt zu Ihrem Abgabepartner aus der Linearen Algebra haben und mit diesem/dieser gut zusammengearbeitet haben, so empfiehlt es sich in der gegenwärtigen Situation, sich gegenseitig per Mail / StudIP / WhatsApp / Skype / o.ä. abwechselnd die Argumente der einzelnen Punkte zu erklären, damit Sie sich in das derzeit erzwungene mathematische Zusammenarbeiten auf elektronischem Weg einfinden.

Definition 1.1.6 *Seien* $a, b \in \mathbb{Z}$*.*

a) Gilt $c \mid a$ *und* $c \mid b$ *für ein* $c \in \mathbb{Z}$*, so heißt* c *ein* **gemeinsamer Teiler** *von* a *und* b*.*

b) $c \in \mathbb{Z}$ *heißt ein* **größter gemeinsamer Teiler** *von* a *und* b*, falls gilt:*

(i) $c \mid a$ *und* $c \mid b$

(ii) Für $d \in \mathbb{Z}$ gilt: $((d \mid a \text{ und } d \mid b) \Longrightarrow d \mid c)$

c) a und b heißen **teilerfremd**, *falls ± 1 die einzigen gemeinsamen Teiler von a und b sind.*

Notation 1.1.7 *Gerne spricht man auch von* **dem** *größten gemeinsamen Teiler von a und b statt von* **einem** *größten gemeinsamen Teiler von a und b. In diesem Fall wählt man aus der Menge der beiden größten gemeinsamen Teiler den positiven aus, was wir im Folgenden auch tun werden. Diesen bezeichnen wir mit* $\mathrm{ggT}(a, b)$.

Bisher haben wir den größten gemeinsamen Teiler definiert, aber noch nicht bewiesen, dass er auch existiert. Dies werden wir erst nach der Betrachtung erster Eigenschaften des ggT nachholen, da wir einige davon benötigen. Insbesondere sind zum jetzigen Zeitpunkt alle Aussagen der folgende Proposition zu lesen mit dem Zusatz 'unter der Voraussetzung, dass $\mathrm{ggT}(a, b)$ existiert, existieren auch die anderen angegebenen ggT'.

Proposition 1.1.8 (Eigenschaften des ggT**)** *Seien $a, b \in \mathbb{Z}$. Es gilt:*

a) $\mathrm{ggT}(b, a) = \mathrm{ggT}(a, b) = \mathrm{ggT}(|a|, |b|)$

b) $b \mid a \Longrightarrow \mathrm{ggT}(a, b) = |b|$

c) $\mathrm{ggT}(a, 0) = |a|$

d) $\mathrm{ggT}(a, b) = \mathrm{ggT}(a \bmod b, b)$

e) $\mathrm{ggT}\left(\frac{a}{\mathrm{ggT}(a,b)}, \frac{b}{\mathrm{ggT}(a,b)}\right) = 1$

Beweis: Hier nur ein Hinweis zum Beweis, jedoch keine Ausführung bis ins Detail: Alle Aussagen folgen direkt aus der Definition des ggT. Dabei nutzt man aus, dass bei Gleichheit der Mengen aller gemeinsamen Teiler zweier Zahlen auch der ggT übereinstimmt. In d) verwendet man zusätzlich die Definition der Division mit Rest, in e) die Tatsache, dass für jeden gemeinsamen Teiler d von $\frac{a}{\mathrm{ggT}(a,b)}$ und $\frac{b}{\mathrm{ggT}(a,b)}$ auch $d \cdot \mathrm{ggT}(a, b)$ gemeinsamer Teiler von a und b ist.

□

Satz 1.1.9 (Existenz des $\mathrm{ggT}(a,b)$**)** *Seien* $a, b \in \mathbb{Z}, b \neq 0$. *Dann existiert* $\mathrm{ggT}(a,b)$.

Diese Aussage kann man auf verschiedene Weise beweisen. Man kann über den Durchschnitt der Mengen der Teiler von a und b argumentieren oder einen algorithmischen Beweis führen, den wir später in allgemeinerem Kontext kennenlernen werden. Hier verwenden wir aus didaktischen Gründen einen Beweis, der nochmals das Wohlordnungsaxiom verwendet.

Beweis: Da Teiler einer ganzen Zahl nach 1.1.5 auch stets Teiler von deren additivem Inversen sind, reicht es im Beweis aus, sich auf nicht-negative a und b zu beschränken. Wir werden durch Widerspruchsbeweis zu unserem Ziel gelangen.
Nehmen wir also an, dass es Zahlenpaare $(a,b) \in \mathbb{N}_0 \times \mathbb{N}$ gibt mit $a < b$, für die es keinen ggT gibt. Nach Axiom 1.0.1 hat die nach Annahme nicht-leere Menge in solchen Paaren auftretender erster Einträge ein kleinstes Element a_0 und nochmals nach Axiom 1.0.1 die Menge aller in solchen Paaren mit erstem Eintrag a_0 auftretenden zweiten Einträge ein kleinstes Element b_0.
Da $\mathrm{ggT}(0, b_0) = |b_0|$ nach 1.1.8,c) und damit existent, ist $a_0 > 0$. Betrachten wir nun $\mathrm{ggT}(b_0 \bmod a_0, a_0)$. Wir wissen, dass nach 1.1.1 $(b_0 \bmod a_0) < a_0$. Damit kann $b_0 \bmod a_0$ nach der Minimalität von a_0 nicht in einem Paar auftreten, für das kein größter gemeinsamer Teiler existiert. Also existiert $\mathrm{ggT}(b_0 \bmod a_0, a_0)$. Jeder gemeinsame Teiler von $b_0 \bmod a_0$ und a_0 ist aber auch gemeinsamer Teiler von a_0 und b_0 und umgekehrt, aufgrund von

$$b_0 = (b_0 \operatorname{div} a_0) \cdot a_0 + (b_0 \bmod a_0).$$

Natürlich bleiben auch die Teilbarkeiten zwischen den gemeinsamen Teilern dabei unberührt, weswegen $\mathrm{ggT}(a_0, b_0)$ mit $\mathrm{ggT}(b_0 \bmod a_0, a_0)$ übereinstimmt und insbesondere existiert im Widerspruch zur Wahl von a_0 und b_0.

□

Bemerkung 1.1.10 *Betrachtet man mehr als* 2 *Zahlen, sagen wir* $a_1, \ldots, a_k \in \mathbb{Z}$ *so kann man sich auch die Fragen nach dem grössten gemeinsamen Teiler alle Zahlen stellen. Diesen kann man induktiv definieren als*

$$\mathrm{ggT}(a_1, \ldots, a_k) := \mathrm{ggT}(\mathrm{ggT}(a_1, \ldots, a_{k-1}), a_k).$$

Mit dieser Verallgemeinerung und ihren Eigenschaften werden Sie sich auf Übungsblatt 01 noch näher beschäftigen.

Satz 1.1.11 (Bézout-Identität, elementare Version) *Seien $a, b \in \mathbb{Z}, b \neq 0$. Dann existieren $x, y \in \mathbb{Z}$, so dass*

$$\mathrm{ggT}(a, b) = xa + yb.$$

Insbesondere ist $\mathrm{ggT}(a, b)$ die kleinste natürliche Zahl, die als $\mathbb{Z}$-Linearkombination von a und b dargestellt werden kann.

Beweis: Sei $M = \{c \in \mathbb{N} \mid \exists k, m \in \mathbb{Z} : c = ka + mb\}$. Die Menge ist nicht leer, da $|b| \in M$, so dass sie nach 1.0.1 ein minimales Element $d = xa + yb$ hat.
Schritt 1: d teilt a und b
Betrachte die Division a durch d:

$$a = q \cdot d + r \text{ für ein } q \in \mathbb{Z} \text{ und ein } 0 \leq r < d.$$

Dann ist

$$r = a - q \cdot (xa + yb) = (1 - qx)a + qyb \in M \cup \{0\}$$

und wegen der Minimalität von d in M gilt damit $r = 0$. Also gilt $d \mid a$ und wegen der Symmetrie der Situation auch $d \mid b$.
Schritt 2: $d = \mathrm{ggT}(a, b)$ Sei $c \in \mathbb{N}$ ein weiterer gemeinsamer Teiler von a und b, so gilt $c \mid xa + yb$, d.h. $c \mid d$, weswegen d größter gemeinsamer Teiler von a und b ist.

□

Bemerkung 1.1.12 *Der Satz 1.1.11 impliziert auch, dass alle $\mathbb{Z}$-Linearkombinationen von a und b selbst wieder Vielfache von $d = \mathrm{ggT}(a, b)$ sind. Denn gäbe es eine Linearkombination, die kein Vielfaches von d wäre, so ließe sich auch deren größter gemeinsamer Teiler mit d, der echt kleiner als d wäre, als Linearkombination aus a und b darstellen im Widerspruch zur Minimalität von d in M. Es gilt also:*

$$\{xa + yb \mid x, y \in \mathbb{Z}\} = \{zd \mid z \in \mathbb{Z}\}$$

Die bisher betrachteten Eigenschaften werden wir später in allgemeinerem Kontext wiedersehen und dort auch nochmals und dann mit konstruktiver Herangehensweise beweisen. Trotzdem ist es gut, die Überlegungen hier sorgfältig durchzudenken und die hier behandelten Tatsachen als Beispielvorrat für spätere Aussagen im Kopf zu behalten.

1.2 Ideale in $\mathbb{Z}$

Die in Bemerkung 1.1.12 aufgetauchte Menge ist ein erstes Beispiel einer neuer mathematischen Struktur, nämlich eines Ideals. Ideale können in beliebigen Ringen betrachtet werden. Allerdings haben Ideale in $\mathbb{Z}$ besonders schöne Eigenschaften, wie wir gleich sehen werden, so dass sie gut für den ersten Einstieg geeignet sind.

Definition 1.2.1 *Eine nicht-leere Teilmenge $I \subseteq \mathbb{Z}$ heißt* **Ideal** *in $\mathbb{Z}$, kurz $I \trianglelefteq \mathbb{Z}$, falls gilt:*

a) $\forall a, b \in I : a + b \in I$

b) $\forall a \in I, \forall r \in \mathbb{Z} : ar \in I$

Bemerkung 1.2.2 *Die Menge*

$$M = \{xa + yb \mid x, y \in \mathbb{Z}\} = \{zd \mid z \in \mathbb{Z}\}$$

ist ein Ideal, denn schon aus der jeder der beiden Beschreibungen der Menge wird klar, dass Summen und ganzzahlige Vielfache von Elementen von M wieder Elemente von M sind. Es handelt sich hierbei augenscheinlich um das kleinste Ideal, das a und b enthält, aber auch um das kleinste Ideal, das d enthält.

Definition 1.2.3 *Für $a_1, \ldots, a_n \in \mathbb{Z}$ heisst*

$$I := \langle a_1, \ldots, a_n \rangle := \{\sum_{i=1}^{n} k_i a_i \mid k_1, \ldots, k_n \in \mathbb{Z}\} \trianglelefteq \mathbb{Z}$$

das von $a_1, \ldots, a_n$ **erzeugte Ideal**, *$a_1, \ldots, a_n$ werden als* **Erzeuger** *von I bezeichnet.*

Definition 1.2.4 *Ein Ideal, das sich in der Form $I = \langle a_1 \rangle \trianglelefteq \mathbb{Z}$ schreiben läßt, wird als* **Hauptideal** *in $\mathbb{Z}$ bezeichnet.*

Bemerkung 1.2.5 *Wir werden später sehen, dass sich die Definition eines Ideals und auch die eines Hauptideals nahezu wörtlich auf beliebige kommutative Ringe mit 1 übertragen lassen. Ein kommutativer, nullteilerfreier Ring mit Eins, in dem jedes Ideal ein Hauptideal ist, wird als* **Hauptidealring** *bezeichnet werden. Mit diesem Ausblick sagt der folgende Satz aus, dass $\mathbb{Z}$ ein Hauptidealring ist.*

Satz 1.2.6 *Jedes Ideal $I \trianglelefteq \mathbb{Z}$ ist ein Hauptideal.*

Ehe wir diesen Satz beweisen, formulieren wir 1.1.11 neu in der Sprache der Ideale in $\mathbb{Z}$. Hierzu ist kein Beweis notwendig, da es sich lediglich um die Verwendung einer neuen Schreibweise für eine bereits bewiesene Tatsache handelt. Diese neue Schreibweise andererseits hilft uns, den obigen Satz in kompakter Form zu beweisen.

Satz 1.2.7 *Seien $a, b \in \mathbb{Z}, b \neq 0$. Dann gilt:*

$$\langle a, b\rangle = \langle \mathrm{ggT}(a, b)\rangle.$$

Beweis:(von Satz 1.2.6) Sei $I \trianglelefteq \mathbb{Z}$ ein beliebiges Ideal. Da I nicht leer ist, existiert mindestens ein $d_0 \in I$ und oBdA ist $d_0 \geq 0$. Ist $I = \langle d_0\rangle$, so ist I Hauptideal. Ansonsten ist $\langle d_0\rangle \subsetneq I$ und es existiert ein $a_0 \in I \setminus \langle d_0\rangle$. Damit ist $\langle d_0, a_0\rangle \subseteq I$, was nach 1.2.7 bedeutet, dass $\langle d_1\rangle \subseteq I$, wobei $d_1 = \mathrm{ggT}(d_0, a_0)$. Insbesondere ist aber wegen $d_1 \in I \setminus \langle d_0\rangle$ die positive ganze Zahl d_1 echt kleiner als d_0. Diese Konstruktion können wir nun iterieren: Ist im i-ten Durchlauf der Konstruktion $\langle d_i\rangle \subsetneq I$, so wird ein Element $a_i \in I \setminus \langle d_i\rangle$ sowie $d_{i+1} = \mathrm{ggT}(d_i, a_i)$ bestimmt, was eine Kette positiver ganzer Zahlen

$$d_0 > d_1 > \ldots > d_{i+1} > \ldots$$

erzeugt. Da aber nur endlich viele positive ganze Zahlen kleiner als d_0 sind, kann diese Kette irgendwann nicht mehr fortgesetzt werden, sagen wir bei einem d_n. Das bedeutet insbesondere, dass $I = \langle d_n\rangle$ erfüllt ist. I ist somit Hauptideal mit Erzeuger d_n.

□

Hier noch eine andere naheliegend erscheinende Aussage, die wir explizit beweisen werden. Sie stammt schon aus der griechischen Antike und dient uns hier als Übergang zu einer anderen zentralen Tatsache über die ganzen Zahlen, dem Fundamentalsatz der Arithemtik.

Lemma 1.2.8 (Euklid) *Seien $a, b, c \in \mathbb{Z}$ mit $a \neq 0$, $a \mid bc$ und $\mathrm{ggT}(a, b) = 1$. Dann gilt*

$$a \mid c.$$

Beweis: Ist $c = 0$, so ist die Aussage trivial, da jede ganze Zahl Null teilt. Wir beschränken uns ab jetzt also auf den Fall $c \neq 0$.
Nach Satz 1.1.11 impliziert $\mathrm{ggT}(a, b) = 1$ die Exisitenz von $x, y \in \mathbb{Z}$ mit

$$xa + yb = 1.$$

Multipliziert mit c liefert diese Gleichung:

$$xac + ybc = c.$$

Da a nun offensichtlich Teiler von xac ist und nach Voraussetzung Teiler von ybc, ist a auch Teiler von c.

□

Definition 1.2.9 *Eine Zahl $p \in \mathbb{N}$ heißt* **Primzahl**, *wenn sie genau zwei positive Teiler besitzt, nämlich 1 und p. Eine Zahl $n \in \mathbb{N}$ mit $n \geq 2$, die keine Primzahl ist, heißt* **zusammengesetzte Zahl**.

Bemerkung 1.2.10 *Ist n eine zusammengesetzte Zahl, so besitzt n noch mindestens einen Teiler $1 < n_1 < n$ und läßt sich daher als Produkt $n = n_1 \cdot \frac{n}{n_1}$ schreiben, wobei $\frac{n}{n_1}$ eine ganze Zahl ist.*

Korollar 1.2.11 *Sei p eine Primzahl und seien $a, b \in \mathbb{Z}$. Dann gilt:*

$$p \mid ab \Longrightarrow p \mid a \text{ oder } p \mid b.$$

Dies ist eine direkte Folgerung aus dem Lemma von Euklid und wird oft auch selbst als Lemma von Euklid bezeichnet.

Satz 1.2.12 (Fundamentalsatz der Arithmetik) *Jede natürliche Zahl $n \geq 2$ kann als Produkt von Primzahlen dargestellt werden, d.h. zu jedem $n \geq 2$ existieren $k \in \mathbb{N}$ sowie $p_1, \ldots, p_k$ (nicht notwendigerweise verschiedene) Primzahlen mit*

$$n = \prod_{i=1}^{k} p_i.$$

Die Faktorisierung ist bis auf Reihenfolge eindeutig.

Beweis: Wir führen den Beweis der Existenz der Zerlegung durch Induktion nach n:

Induktionsanfang: $n = 2$
$n = 2$ ist selbst Primzahl, so dass $n = p_1$ mit $p_1 = 2$ die gesuchte Zerlegung ist.

Induktionsvoraussetzung: n
Jede natürliche Zahl $2 \leq m \leq n$ besitzt eine Zerlegung in Primfaktoren.

Induktionsschritt: $n \mapsto n + 1$
Ist $n + 1$ Primzahl, so ist die Zerlegung in Primfaktoren bereits gefunden. Wir betrachten daher ab jetzt den Fall, dass $n + 1$ zusammengesetzt ist. Als zusammengesetzte Zahl hat $n + 1$ mindestens einen echten Teiler $1 < m_1 < n + 1$ und läßt sich daher schreiben als

$$n + 1 = m_1 \cdot m_2 \text{ mit } m_2 := \frac{n+1}{m_1} \in \mathbb{N}.$$

Für die natürlichen Zahlen $m_1, m_2 < n + 1$ existiert nach Induktionsvoraussetzung eine Zerlegung in Primfaktoren

$$m_1 = \prod_{i=1}^{k_1} p_{1,i} \text{ und } m_2 = \prod_{i=1}^{k_2} p_{2,i}$$

weswegen auch gilt

$$n + 1 = \prod_{j=1}^{2} \left(\prod_{i=1}^{k_j} p_{j,i} \right),$$

was die gesuchte Zerlegung von $n + 1$ in Primfaktoren liefert.

Es bleibt nun noch die Eindeutigkeit der Zerlegung bis auf Reihenfolge zu zeigen. Auch hier gehen wir wieder per Induktion nach n vor.

Induktionsanfang: $n = 2$
$n = 2$ ist als Primzahl ihre eigene Zerlegung, die offensichtlich eindeutig ist.

Induktionsvoraussetzung: n
Die Zerlegung jeder natürlichen Zahl $2 \leq m \leq n$ in Primfaktoren ist bis auf

Reihenfolge eindeutig.

Induktionsschritt: $n \mapsto n+1$
Seien nun

$$n+1 = \prod_{i=1}^{k} p_i \text{ und } n+1 = \prod_{j=1}^{r} q_j$$

zwei Zerlegungen von $n+1$ in Primfaktoren. Dann ist die Primzahl p_k nach dem Korollar zum Lemma von Euklid 1.2.11 ein Teiler eines der Primfaktoren q_j und damit $p_k = q_j$. Ohne Beschränkung der Allgemeinheit ist dieses $j = r$. Damit haben wir einen Primfaktor in der Zerlegung identifiziert und können ihn in beiden Produkten herausteilen;

$$\prod_{i=1}^{k-1} p_i = \frac{n+1}{p_k} = \prod_{j=1}^{r-1} q_j.$$

Ist $\frac{n+1}{p_k} = 1$, so war $n+1$ bereits eine Primzahl und es ist nichts mehr zu zeigen. Andernfalls die Zerlegung natürlichen Zahl $1 < \frac{n+1}{p_k} < n+1$ nach Induktionsvoraussetzung bis auf Reihenfolge eindeutig, so dass damit auch die Eindeutigkeit der Zerlegung von $n+1$ bis auf Reihenfolge bewiesen ist.

□

Kapitel 2

Ringe und Ideale

Gruppen, Ringe und Körper sind grundlegende Objekte der Algebra. Sie haben sie bereits in der Linearen Algebra kennengelernt, denn ohne deren Definition und grundlegende Eigenschaften sind selbst die Überlegungen der Theorie der Vektorräume nicht solide aufbaubar. Daher werden wir hier zuerst die Begriffe kurz und ohne Beweise wiederholen, ehe wir uns weiterführenden Begriffen, Eigenschaften und Sätzen zuwenden, die dann den Einstieg in die eigentliche Thematik der Algebra bilden.

2.1 Wiederholung: Gruppen, Ringe, Körper

In diesem Abschnitt wird es wegen des Wiederholungscharakters weder Beweise noch umfangreiche Überleitungstexte geben.

Definition 2.1.1 *Sei G eine nicht-leere Menge und*

$$\begin{array}{rcl} * : G \times G & \longrightarrow & G \\ (a, b) & \longmapsto & a * b \end{array}$$

eine zweistellige Operation auf G.

a) $(G, *)$ *heißt* **Halbgruppe**, *wenn das Assoziativgesetz in G bzgl. $*$ erfüllt ist:*
(AG) $\quad \forall a, b, c \in G : \quad (a * b) * c = a * (b * c).$

b) $(G, *)$ *heißt* **Monoid**, *wenn $(G, *)$ eine Halbgruppe ist, in der ein neutrales Element existiert:*
(NE) $\quad \exists e \in G : a * e = a = e * a \ \ \forall a \in G.$

c) $(G, *)$ *heißt* **Gruppe**, *wenn* $(G, *)$ *ein Monoid ist, in dem jedes Element ein inverses Element besitzt:*
$(IE) \qquad \forall a \in G \exists b \in G : a * b = e = b * a.$

d) Eine solche Struktur $(G, *)$ *heißt* **abelsch** *(oder* **kommutativ***), falls das Kommutativgesetz in* G *bzgl.* $*$ *erfüllt ist:*
$(KG) \qquad \forall a, b \in G : a * b = b * a.$

Lemma 2.1.2 *Sei* $(G, *)$ *eine Halbgruppe. Sind zusätzlich sowohl*
$(lNE) \qquad \exists e \in G : e * a = a \forall a \in G \quad$ *als auch*
$(lIE) \qquad \forall a \in G \exists b \in G : b * a = e$
erfüllt, so ist $(G, *)$ *bereits eine Gruppe.*

Lemma 2.1.3 *Sei* $(G, *)$ *eine Halbgruppe. Sind zusätzlich sowohl*
$(rNE) \qquad \exists e \in G : a * e = a \forall a \in G \quad$ *als auch*
$(rIE) \qquad \forall a \in G \exists b \in G : a * b = e$
erfüllt, so ist $(G, *)$ *bereits eine Gruppe.*

Satz 2.1.4 *In einem Monoid ist das neutrale Element eindeutig bestimmt. In einer Gruppe ist das inverse Element zu einem gegebenen Element eindeutig bestimmt.*

Notation 2.1.5 *Sehr häufig werden Gruppen in multiplikativer Notation, also als* $(G, \cdot)$*, mit den üblichen Schreibweisen für die Multiplikation notiert. Vor allem bei abelschen Gruppe ist auch die additive Notation, also* $(G, +)$*, mit den üblichen Schreibweisen der Addition gebräuchlich.*

Definition 2.1.6 *Sei* $(G, *)$ *eine Gruppe. Eine nicht-leere Teilmenge* $U \subseteq G$ *heißt* **Untergruppe** *von* G*, falls* $(U, *)$ *eine Gruppe ist.*

Proposition 2.1.7 *Sei* $(G, *)$ *eine Gruppe. Eine Teilmenge* $U \subseteq G$ *ist genau dann Untergruppe, wenn*

(U1) $U \neq \emptyset$

(U2) $\forall a, b \in U : a * b^{-1} \in U$

Definition 2.1.8 *Sei R eine nicht-leere Menge und seien*

$$\begin{aligned} + : R \times R &\longrightarrow R \\ (a,b) &\longmapsto a+b \\ \cdot : R \times R &\longrightarrow R \\ (a,b) &\longmapsto a \cdot b \end{aligned}$$

zwei zweistellige Operationen auf R.
$(R,+,\cdot)$ heißt **Ring**, *falls*

a) $(R,+)$ *abelsche Gruppe*

b) $(R,\cdot)$ *Halbgruppe*

c) die beiden Distributivgesetze gelten:
$\forall a,b,c \in R : (a+b)\cdot c = a\cdot c + b\cdot c$
$\forall a,b,c \in R : a\cdot(b+c) = a\cdot b + a\cdot c.$

Ein Ring $(R,+,\cdot)$ heißt **Ring mit 1**, *falls $(R,\cdot)$ Monoid ist.*
Ein Ring $(R,+,\cdot)$ heißt **kommutativ**, *falls $(R,\cdot)$ abelsch ist.*

Proposition 2.1.9 *Sei $(R,+,\cdot)$ ein Ring mit 1. Dann gilt:*

a) 0_R *und* 1_R *sind eindeutig bestimmt.*

b) $0_R \cdot a = 0_R = a \cdot 0_R \ \ \forall a \in R$

c) $(-a)\cdot b = -(a\cdot b) = a\cdot(-b) \ \ \forall a,b \in R$

d) $(-a)\cdot(-b) = a\cdot b \ \ \forall a,b \in R$

e) $(n\cdot a)\cdot b = n\cdot(a\cdot b) = a\cdot(n\cdot b) \ \ \forall a,b \in R \forall n \in \mathbb{N}$

Definition 2.1.10 *Sei $(R,+,\cdot)$ ein Ring mit 1. Ein Element $a \in R \setminus \{0\}$ heißt* **Nullteiler** *in R, falls*

$$\exists b \in R \setminus \{0\} : a\cdot b = 0 \ \textit{(Linksnullteiler)}$$

oder

$$\exists c \in R \setminus \{0\} : c\cdot a = 0 \ \textit{(Rechtsnullteiler).}$$

R heißt **nullteilerfrei**, *falls*

$$\forall a,b \in R : (a\cdot b = 0 \Longrightarrow (a=0) oder (b=0)).$$

Definition 2.1.11 *Ein nullteilerfreier, kommutativer Ring mit* $1 \neq 0$ *heißt* **Integritätsring** *(oder* **Integritätsbereich***).*

Die seltsame Bedingung $1 \neq 0$ stellt einfach sicher, dass wir es mit einem Monoid $(R \setminus \{0\}, \cdot)$ zu tun haben. Das beinhaltet eben auch, dass $R \setminus \{0\}$ nicht leer ist.

Definition 2.1.12 *Sei* $(R, +, \cdot)$ *ein Ring mit* 1*. Ein Element* $a \in R$ *heißt* **Einheit** *in* R*, falls*

$$\exists b \in R : a \cdot b = 1 = b \cdot a.$$

Die Menge der Einheiten in R *wird bezeichnet mit* R^**.*

Definition 2.1.13 *Ein Ring* $(R, +, \cdot)$ *mit* $1 \neq 0$ *heißt* **Schiefkörper***, falls* $R^* = R \setminus \{0\}$*.*
Ist R *zusätzlich kommutativer Ring, so heißt* R **Körper***.*

Bemerkung 2.1.14 $(R^*, \cdot)$ *ist eine Gruppe und wird als die* **Einheitengruppe** *von* R *bezeichnet.*

Korollar 2.1.15 *Sei* $K \neq \emptyset$ *und seien*

$$\begin{aligned} + : K \times K &\longrightarrow K \\ (a, b) &\longmapsto a + b \\ \cdot : K \times K &\longrightarrow K \\ (a, b) &\longmapsto a \cdot b \end{aligned}$$

zwei zweistellige Operationen auf K*.*
$(K, +, \cdot)$ *ist ein Körper genau dann, wenn*

a) $(K, +)$ *abelsche Gruppe*

b) $(K \setminus \{0\}, \cdot)$ *abelsche Gruppe*

c) das Distributivgesetz gilt:
$\forall a, b, c \in K : a \cdot (b + c) = a \cdot b + a \cdot c.$

2.2 Ergänzung: Integritätsring, Schiefkörper, Körper

Da die folgenden Aussagen nicht in der Linearen Algebra behandelt wurden und wir sie daher nicht ohne Beweis einfach zitieren können, grenze ich sie bewusst gegenüber den vorigen Aussagen ab. Thematisch könnten sie leicht in dasselbe Kapitel gepackt werden, aber mit dieser Aufteilung ist es für die Leserinnen und Leser des Skripts hoffentlich leichter, die neuen Inhalte von der Wiederholung abzugrenzen.

Satz 2.2.1 *Jeder Schiefkörper ist nullteilerfrei.*

Beweis: Sei $(R, +, \cdot)$ ein Schiefkörper und seien $a, b \in R$, $a \neq 0$, so daß $a \cdot b = 0$. Ein Nullteiler muss nach Definition selbst von Null verschieden sein ebenso wie der Faktor, mit dem er Null ergibt, so dass wir $a = 0$ nicht betrachten müssen und die Aussage bewiesen haben, sobald wir sehen, dass $b = 0$ gelten muss.
Wegen $a \neq 0$ existiert ein multiplikatives Inverses a^{-1} zu a, so dass gilt:

$$0 = a^{-1} \cdot 0 = a^{-1} \cdot a \cdot b = b,$$

weswegen a kein Nullteiler ist.

□

Korollar 2.2.2 *Jeder Körper ist ein Integritätsring.*

Beweis: Integritätsringe sind kommutative nullteilerfreie Ringe

□

Satz 2.2.3 *Jeder endliche Integritätsring R mit $1 \neq 0$ ist ein Körper.*

Beweis: Sei $(R, +, \cdot)$ ein endlicher Integritätsring. Wir werden zeigen, dass jedes Element $a \in R \setminus \{0\}$ ein multiplikatives Inverses hat. Anstatt diese Inverse jedoch explizit zu konstruieren, werden wir zeigen, dass es ein Inverses zu a geben muss, ohne dieses explizit anzugeben.

Schritt 1: Zeige $\phi : R \longrightarrow R, x \longmapsto a \cdot x$ injektiv
Seien $y_1, y_2 \in R$ mit $\phi(y_1) = \phi(y_2)$, dann gilt:

$$0 = a \cdot y_1 - a \cdot y_2 \overset{(DG)}{=} a \cdot (y_1 - y_2).$$

Da $a \neq 0$ und R nullteilerfrei ist, gilt damit $y_1 = y_2$.
Schritt 2: Zeige $\exists b \in R : a \cdot b = 1$
Da R endlich ist, ist ϕ wegen Injektivität auch surjektiv. Damit existiert $b \in R$, das auf die 1 abgebildet wird. Dies ist unser gesuchtes Inverses.

□

Generalvoraussetzung ab diesem Punkt:
Alle betrachteten Ringe besitzen eine $1 \neq 0$, sofern nicht ausdrücklich etwas anderes vorausgesetzt wird.

2.3 Ringhomomorphismen

In der Linearen Algebra beschäftigten wir uns nicht nur mit den dortigen Objekten – den Vektorräumen – sondern auch mit den mit der Vektorraumstruktur verträglichen Abbildungen zwischen diesen – den Vektorraum-Homomorphismen, die auch als Lineare Abbildungen bezeichnet werden. In der Algebra I wird unser Hauptaugenmerk auf Ringen liegen und auf Abbildungen, die diese Struktur respektieren, den Ringhomomorphismen.

Definition 2.3.1 *Seine* $(R, +_R, \cdot_R), (S, +_S, \cdot_S)$ *Ringe. Eine Abbildung* $\phi : R \longrightarrow S$ *heißt* **Ringhomomorphismus**, *falls gilt:*

a) $\forall a, b \in R : \phi(a +_R b) = \phi(a) +_S \phi(b)$

b) $\forall a, b \in R : \phi(a \cdot_R b) = \phi(a) \cdot_S \phi(b)$

c) $\phi(1_R) = 1_S$

Erinnern wir uns hier nochmals an die Generalvoraussetzung, dass alle Ringe ab Abschnitt 2.2 eine 1 haben, so könnte man sich fragen, wie die Definition für allgemeinere Ringe aussehen müsste. Für diese würde einfach Bedingung c) wegfallen. Zu beachten ist, dass Bedingung c) nicht aus den beiden anderen gefolgert werden kann, sondern tatsächlich die Verträglichkeit mit der Struktur des Ringes **mit** 1 erzwingt.

Bemerkung 2.3.2 *Analog zu den bei Vektorraumhomomorphismen eingeführten Begriffsbildungen, verwenden wir bei Ringhomomorphismen die Begriffe* **Ringmonomorphismus** *(oder auch* **Einbettung***) bei Injektivität,* **Ringepimorphismus** *bei Surjektivität sowie* **Ringisomorphismus** *bei Bijektivität. Ist* $R = S$*, so sprechen wir auch von einem* **Ringendomorphismus**. *Einen bijektiven Ringendomorphismus nennen wir* **Ringautomorphismus**.

Satz 2.3.3 *Seien* $(R, +_R, \cdot_R)$ *und* $(S, +_S, \cdot_S)$ *Ringe und* $\phi : R \longrightarrow S$ *ein Ringhomomorphismus. Dann gilt:*

a) $\forall n \in \mathbb{N}, \forall r \in R : \phi(r^n) = (\phi(r))^n$

b) $\forall r \in R^* : \phi(r) \in S^*$

c) $\forall n \in \mathbb{N}, \forall r \in R^* : \phi(r^{-n}) = (\phi(r))^{-n}$

Beweis: Aussage a) folgt direkt aus der n-fachen Anwendung von 2.3.1,b), ebenso wie c) nach Beweis von b).
Zum Beweis von b) seien $r, s \in R^*$ mit $r \cdot_R s = 1_R$. Dann gilt:

$$\phi(r) \cdot_S \phi(s) = \phi(r \cdot_R s) = \phi(1_R) = 1_S,$$

weswegen $\phi(r), \phi(s) \in S^*$.

□

Definition 2.3.4 *Seien $(R, +_R, \cdot_R), (S, +_S, \cdot_S)$ Ringe und sei $\phi : R \longrightarrow S$ ein Ringhomomorphismus. Dann heisst*

$$\ker(\phi) := \{x \in R \mid \phi(x) = 0_S\} = \phi^{-1}(\{0_S\})$$

der **Kern** *von ϕ. Das Bild von ϕ ist definiert als*

$$\mathrm{Im}(\phi) := \{y \in S \mid \exists x \in R : \phi(x) = y\} = \{\phi(x) \mid x \in R\}.$$

Definition 2.3.5 *Sei $(R, +_R, \cdot_R)$ ein Ring und $\emptyset \neq S \subseteq R$ eine Teilmenge. S heißt Unterring von R, kurz $S \leq R$, falls $(S, +_R, \cdot_R)$ ein Ring ist.*

Lemma 2.3.6 *Sei $(R, +_R, \cdot_R)$ ein Ring und $\emptyset \neq S \subseteq R$ eine Teilmenge. S ist Unterring von R, falls:*

a) $\forall s_1, s_2 \in S : s_1 +_R (-s_2) \in S$

b) $\forall s_1, s_2 \in S : s_1 \cdot_R s_2, s_2 \cdot_R s_1 \in S$

c) $1_R \in S$

Beweis: Die Voraussetzung $S \neq \emptyset$ zusammen mit Bedingung a) ist gerade das Untergruppenkriterium für S bzgl. der Addition, so dass wir daraus direkt schließen können, dass $(S, +_R)$ abelsche Gruppe ist.
Die Bedingung b) liefert uns die Abgeschlossenheit bzgl. der Multiplikation, bei der wir für zwei gegebene Elemente beide Reihenfolgen betrachten, da wir für R keine Kommutativität vorausgesetzt haben.[1] Daraus folgt bereits, dass $(S, \cdot_R)$ eine Halbgruppe ist, da die Assoziativität dann direkt aus der Assoziativität in R folgt. Weil nun nach Bedingung c) $1_R \in S$, ist diese Halbgruppe auch ein Monoid.
Die beiden Distributivgesetze gelten wiederum wegen der Abgeschlossenheit

[1] Natürlich reicht es, nur eine Reihenfolge zu fordern, da ja die Rollen von s_1 und s_2 bei einer Aussage "für alle s_1, s_2 "vertauscht werden können.

von $+_R$ und $\cdot_R$ in S und der Gültigkeit der Gesetze in R.
Damit wurde gezeigt, dass $(S, +_R, \cdot_R)$ ein Unterring von $(R, +_R, \cdot_R)$ ist.

□

Satz 2.3.7 *Seien $(R, +_R, \cdot_R)$ und $(S, +_S, \cdot_S)$ Ringe und $\phi : R \longrightarrow S$ ein Ringhomomorphismus. Dann gilt:*

a) $\mathrm{Im}(\phi)$ *ist Unterring von S.*

b) Ist $R_1 \leq R$ Unterring, so ist $\phi(R_1) = \{\phi(x) \mid x \in R_1\}$ Unterring von S.

c) Ist $S_1 \leq S$ Unterring, so ist $\phi^{-1}(S_1) = \{x \in R \mid \phi(x) \in S_1\}$ Unterring von R.

d) Ist R kommutativ, so auch $\phi(R)$.

e) ϕ ist genau dann injektiv, wenn $\ker(\phi) = \{0\}$.

Beweis: Die Beweise der Aussagen a),b) und c) sind direkte Anwendungen des Unterringkriteriums, weswegen deren Beweis eine gute Übung sein kann. Für den vorletzten Beweisteil d) betrachten wir einen kommutativen Ring R. Dann gilt im Unterring $\phi(R)$:

$$\forall r_1, r_2 \in R : \phi(r_1) \cdot_S \phi(r_2) = \phi(r_1 \cdot_R r_2) = \phi(r_2 \cdot_R r_1) = \phi(r_2) \cdot_S \phi(r_1),$$

was gerade die Kommutativität von $\phi(R)$ ist.
Ein Ringhomomorphismus ist insbesondere auch ein Gruppenhomomorphismus der zugrundeliegenden abelschen Gruppen $(R, +_R)$ und $(S, +_S)$, für den die Äquivalenz bereits in der Linearen Algebra bewiesen wurde. Sie erinnern sich sicher an die Argumente: Haben zwei unterschiedliche Elemente dasselbe Bild, so liegt ihre Differenz im Kern. Liegt zusätzlich zur Null ein weiteres Element im Kern, so haben die beiden Elemente dasselbe Bild.

□

Notation 2.3.8 *Ab jetzt werden wir die unteren Indizes bei den beiden Verknüpfungen in Ringen nur noch dort schreiben, wo eine echte Verwechslungsgefahr besteht.*

2.4 Charakteristik

Studierende, die bei mir im letzten Semester Lineare Algebra gehört haben, haben auf einem der Übungsblätter den Begriff der Charakteristik eines Ringes/Körpers gesehen. Formal eingeführt war er dort jedoch noch nicht. Daher holen wir das nun nach:

Definition 2.4.1 *Sei $(R, +, \cdot)$ ein Ring. Existiert eine positive Zahl $\ell \in \mathbb{N}$ mit*

$$\sum_{i=1}^{\ell} r = 0 \quad \forall r \in R,$$

so heißt die kleinste solche Zahl die **Charakteristik** *von R, kurz* $\mathrm{char}(R)$. *Existiert solch eine Zahl nicht, so definiert man* $\mathrm{char}(R) = 0$.

Die Beschreibung der Charakteristik in der obigen Definition ist offensichtlich etwas unhandlich. Statt alle $r \in R$ zu betrachten, reicht es völlig aus das kleinste ℓ zu wählen, für das

$$\sum_{i=1}^{\ell} 1 = 0.$$

(Klammern Sie einfach in der Summe der Definition r mittels Distributivgesetz aus.)
Aber auch nach dieser Vereinfachung erscheint insbesondere die Wahl von 0 im Falle der Nicht-Existenz eines ℓ noch nicht natürlich. Woher diese kommt, erklärt die folgende Interpretation der Charakteristik:

Bemerkung 2.4.2 *Betrachte die Abbildung*

$$\begin{aligned} \chi : \mathbb{Z} &\longrightarrow R \\ m &\longmapsto \chi(m) = m \cdot 1_R = \varepsilon(m) \cdot \sum_{i=1}^{|m|} 1_R, \end{aligned}$$

wobei die ad hoc Notation $\varepsilon(m)$ gerade das Vorzeichen von m codiert:

$$\varepsilon(m) = \begin{cases} 1_R & \text{für } m \geq 0 \\ -1_R & \text{für } m < 0 \end{cases}.$$

χ ist ein Ringhomomorphismus, wie sich direkt nachrechnen läßt. Das sollten Sie sich beim Nacharbeiten klarmachen und im Falle von Problemen nachfragen. Denken Sie daran, dass eine leere Summe $\sum_{i=1}^{0} 1_R$ gleich dem neutralen Element der Addition ist.
Offensichtlich existiert ein $\ell \in \mathbb{N}$ mit $\sum_{i=1}^{\ell} 1_R = 0$ genau dann, wenn $\ell \in \ker(\chi)$, was bedeutet:

$$\ker(\chi) = \{0\} \iff \operatorname{char}(R) = 0.$$

Gilt für zwei Zahlen $s, t \in \mathbb{Z}$

$$\chi(s) = \varepsilon(s) \cdot \sum_{i=1}^{|s|} 1_R = 0_R \text{ und } \chi(t) = \varepsilon(t) \cdot \sum_{i=1}^{|t|} 1_R = 0_R,$$

so gilt auch für jede $\mathbb{Z}$-Linearkombination von s und t:

$$\chi(as + bt) = \chi(a) \cdot_R \chi(s) +_R \chi(b) \cdot_R \chi(t) = \chi(a) \cdot_R 0_R +_R \chi(b) \cdot_R 0_R = 0_R.$$

Damit ist $\ker(\chi)$, welches wegen $0_R \in \ker(\chi)$ nicht leer ist, ein Ideal in $\mathbb{Z}$ und damit, wie wir aus dem vorigen Kapitel wissen, ein Hauptideal, erzeugt von seinem kleinsten positiven Element. Es gilt also:

$$\ker(\chi) = \langle m \rangle \iff \operatorname{char}(R) = m.$$

Satz 2.4.3 *Sei R ein Integritätsring. Dann ist R entweder von Charakteristik Null oder $\operatorname{char}(R)$ ist eine Primzahl.*

Beweis: Wir führen einen Widerspruchsbeweis:
Nehmen wir also an, dass die Charakteristik von R ein zusammengesetzte Zahl ist. Es ist daher $\operatorname{char}(R) = n_1 \cdot n_2$ für $n_1, n_2 \in \mathbb{N} \setminus \{1\}$. Da $n_1 \cdot n_2$ als Charakteristik nach Definition das kleinste Element ℓ ist, für das gilt $\chi(\ell) = 0_R$, wissen wir, dass gilt:

$$\chi(n_1) \neq 0_R \neq \chi(n_2), \text{ aber } \chi(n_1) \cdot_R \chi(n_2) = \chi(n_1 \cdot n_2) = 0_R.$$

Damit sind $\chi(n_1), \chi(n_2)$ Nullteiler in R im Widerspruch zu der Voraussetzung, dass R Integritätsring ist.

□

2.5 Ringe und noch mehr Ringe

In der Linearen Algebra sind Ihnen schon einige Ringe begegnet. Diese und weitere werden wir in dem Abschnitt nennen und einige besonders wichtige nochmals allgemeiner oder strenger einführen.

$\mathbb{Z}$ und $\mathbb{Z}_m$

Zusätzlich zum wohlbekannten Ring der ganzen Zahlen $(\mathbb{Z}, +, \cdot)$, mit dem Ihnen der Umgang bereits aus der Schule bekannt ist, wurde in der linearen Algebra noch ein weiterer, damit eng verwandter Ring eingeführt:

$$\mathbb{Z}_m = \{0, \ldots, m-1\} \quad \text{(Vorlesung SS2019)}$$

mit Addition und Multiplikation

$$\begin{aligned} + : \mathbb{Z}_m \times \mathbb{Z}_m &\longrightarrow \mathbb{Z}_m \\ (a, b) &\longmapsto (a + b) \bmod m \\ \cdot : \mathbb{Z}_m \times \mathbb{Z}_m &\longrightarrow \mathbb{Z}_m \\ (a, b) &\longmapsto (a \cdot b) \bmod m, \end{aligned}$$

bzw.

$$(\mathbb{Z}/m\mathbb{Z}, +, \cdot) \quad \text{(Vorlesung WS2019/20)}$$

mit Addition und Multiplikation

$$\begin{aligned} + : \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} &\longrightarrow \mathbb{Z}/m\mathbb{Z} \\ ([a]_m, [b]_m) &\longmapsto [a + b]_m \\ \cdot : \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} &\longrightarrow \mathbb{Z}/m\mathbb{Z} \\ ([a]_m, [b]_m) &\longmapsto [a \cdot b]_m. \end{aligned}$$

Diese beiden Ringe sind tatsächlich isomorph, aber mittels zweier verschiedener Zugänge eingeführt, wobei der im zweiten Fall gewählte Zugang einer allgemeinen Konstruktion entspricht, die wir in ein paar Wochen kennenlernen werden. Wenn hier im Moment eine Schreibweise verwendet wird und Sie in Ihrer Vorlesung die andere kennengelernt haben, dann dürfen Sie gefahrlos in der Ihnen bekannten weiterdenken, bis alle die allgemeine Konstruktion kennengelernt haben.

Bemerkung 2.5.1 *Der Ring $(\mathbb{Z}/m\mathbb{Z}, +, \cdot)$ ist, wie wir in der Linearen Algebra bereits gesehen haben, genau dann ein Körper, wenn m prim ist. Als Nullteiler hatten wir andererseits genau die Klassen $[a]_m$ mit $\mathrm{ggT}(a, m) \neq 1$ bestimmt und hatten festgestellt, dass jedes Element außer $[0]_m$ in $\mathbb{Z}/m\mathbb{Z}$ Nullteiler oder Einheit ist.*

Matrizenring und Vektorraumhomomorphismen

Ein ganz zentrales Objekt in der Linearen Algebra war der nicht-kommutative Ring mit 1 $(\mathrm{Mat}(n; K), +, \cdot)$ der $n \times n$-Matrizen mit Einträgen in einem Körper K und der Matrixaddition und Matrixmultiplikation als Verknüpfungen. Da in diesen Definitionen und im Verifizieren der Ringeigenschaften in der Linearen Algebra nirgends die Existenz eines multiplikativen Inversen in K verwendet wurde, läßt sich in gleicher Weise auch der Ring der $n \times n$ Matrizen $(\mathrm{Mat}(n; R), +, \cdot)$ über einem kommutativen Ring R mit 1 definieren.
Das Einselement im Ring $(\mathrm{Mat}(n; R), +, \cdot)$ ist die Diagnoalmatrix, deren Diagonaleinträge alle 1_R sind und die wir wieder als Einheitsmatrix bezeichnen. Wir schreiben dafür wie in der Linearen Algebra E_n.

Sei nun ein K-Vektorraum V über einem Körper K mit Basis $\mathcal{B}$ gegeben. Ein zentrales Ergebnis der Linearen Algebra waren die K-Vektorraum- und Ringisomorphismen

$$\begin{aligned} \Phi : End_K(V) &\longrightarrow Mat(n; K) \\ F &\longmapsto M_{\mathcal{B}}^{\mathcal{B}}(F) \\ \text{und} & \\ \Phi\,|_{Aut_K(V)} \colon Aut_K(V) &\longrightarrow GL(n; K) \\ F &\longmapsto M_{\mathcal{B}}^{\mathcal{B}}(F), \end{aligned}$$

wobei auf der Seite der Vektorraumendomorphismen die Ringoperationen gerade festgelegt sind als:

$$\begin{aligned} \forall x \in V : (f +_{End_K(V)} g)(x) &:= f(x) +_V g(x) \\ (f \cdot_{End_K(V)} g)(x) &:= (f \circ g)(x) \end{aligned}$$

Hier konnten wir die Verknüpfung $+_{End_K(V)}$ auf $End_K(V)$ einfach von der Verknüpfung $+_V$ im Wertebereich der Abbildung erben. Dabei ist es

kein Zufall, dass dann nicht nur die Operation selbst, sondern auch Assoziativität, neutrales und inverses Element sich direkt auf diejenigen von $(V, +)$ zurückführen lassen, wie wir bereits in der Linearen Algebra am Rande bemerkt hatten. Das werden wir im folgenden ausnutzen, um noch weitere Beispiele von Ringen kennenzulernen.

Ringe von Abbildungen und von Folgen

Legen wir zuerst ein wenig Notation fest, damit das folgende klar herausgearbeitet werden kann.

Die Menge der Abbildungen von einer nicht-leeren Menge A in eine nicht-leere Menge B bezeichnen wir mit

$$B^A = Abb(A, B) = \{f : A \longrightarrow B \mid f Abbildung\}.$$

Zwei Abbildungen $f, g \in Abb(A, B)$ sind gleich, wenn $f(a) = g(a)$ für alle $a \in A$.

Ist in dieser Notation nun B ein kommutativer Ring R mit 1, so ist auch $R^A = Abb(A, R)$ ein kommutativer Ring mit 1 mit Hilfe der ererbten Verknüpfungen

$$\begin{aligned} (f +_{Abb(A,R)} g)(x) &:= f(x) +_R g(x) \quad \forall x \in A \\ (f \cdot_{Abb(A,R)} g)(x) &:= f(x) \cdot_R g(x) \quad \forall x \in A. \end{aligned}$$

Betrachten wir nun zwei wichtige Spezialfälle:

- Ist $A = \{1, \ldots, n\} \subseteq \mathbb{N}$, so ist

$$\begin{aligned} R^A &= \{f : \{1, \ldots, n\} \longrightarrow R \mid f \text{ Abbildung}\} \\ &\cong \{(f(1), \ldots, f(n)) \mid f(i) \in R \ \forall 1 \leq i \leq n\} \\ &= \{(a_1, \ldots, a_n) \mid a_i \in R \ \forall 1 \leq i \leq n\} \\ &= R^n. \end{aligned}$$

  In diesem Fall ist R^A also gerade isomorph zur Menge aller n-Tupel von Einträgen aus R verknüpft mit kompomentenweiser Addition und Multiplikation.

- Ist $A = \mathbb{N}_0$, so erhalten wir

$$\begin{aligned} R^{\mathbb{N}_0} &= \{f : \mathbb{N}_0 \longrightarrow R \mid f \text{ Abbildung}\} \\ &\cong \{(a_i)_{i\in\mathbb{N}_0} \mid a_i \in R \ \ \forall i \in \mathbb{N}_0\} \\ &= \text{Menge aller Folgen mit Gliedern in } R, \end{aligned}$$

  wobei hier die gliedweise Addition und Multiplikation die Verknüpfungen sind.

Wir sehen also, dass es kein Zufall ist, dass die Menge aller R-Folgen einen kommutativen Ring bildet mit der konstanten Folge $(1)_{i\in\mathbb{N}_0}$ als neutralem Element der Multiplikation. Der Vollständigkeit halber sei explizit erwähnt, dass die Folge $(0)_{i\in\mathbb{N}_0}$ hier das neutrale Element der Addition ist.

Betrachten wir nun zum Abschluss noch eine unter gliedweiser Addition und gliedweiser Multiplikation abgeschlossene Teilmenge von $R^{\mathbb{N}_0}$, die allerdings keinen Ring mit 1 bildet und damit kein Unterring von $R^{\mathbb{N}_0}$ ist. Überlegen Sie, wo das Problem liegt.

Wir bezeichnen mit $R^{(\mathbb{N}_0)}$ die Menge derjenigen Folgen mit Gliedern in R, die nur endlich viele von 0_R verschiedene Glieder haben, d.h.

$$R^{(\mathbb{N}_0)} = \{(a_i)_{i\in\mathbb{N}_0} \mid a_i \in R \ \ \forall i \in \mathbb{N}_0 \text{ und } a_i = 0 \text{ für fast alle } i \in \mathbb{N}_0\}.$$

$R^{(\mathbb{N}_0)}$ bildet eine abelsche Gruppe unter der gliedweisen Addition und ist ein Untergruppe von $R^{\mathbb{N}_0}$.

Bemerkung 2.5.2 *Der Vergleich von Elementen in $R^{\mathbb{N}_0}$ und in $R^{(\mathbb{N}_0)}$ ist ein Vergleich von Abbildungen, wobei zwei Abbildungen gleich sind, wenn sie auf allen Elementen der Urbildmenge jeweils dasselbe Bild haben. Für die hier betrachteten Mengen von Folgen ist das genau der gliedweise Vergleich.*

Polynomring und Potenzreihenring

Polynome sind Ihnen bereits in der Schule begegnet, wo allerdings oft kein bewusster Unterschied zwischen Polynomen und Polynomabbildung gemacht wurde. In der Linearen Algebra jedoch haben wir diesen Unterschied bereits gemacht, indem wir Polynome als Elemente des Polynomringes betrachteten

und Polynomabbildungen mittels eines Polynoms und des Einsetzungshomomorphismus erzeugten. Dieser Unterschied wird sich auch in der nun folgenden strengen Einführung von Polynomringen über kommutativen Ringen widerspiegeln.

Der Einstieg ist dabei sehr formal und greift auf das eben Dargestellte zurück: Wir führen Potenzreihen und Polynome als Folgen ihrer Koeffizienten ein, d.h. wir bewegen uns weiter in den Mengen $R^{\mathbb{N}_0}$ bzw. $R^{(\mathbb{N}_0)}$. Dabei behalten wir aber nur die gliedweise Addition bei und definieren eine andere Multiplikation, was natürlich auch zu einem anderen neutralen Element der Multiplikation führt. wobei wir aber nicht die vorher betrachtete ererbte gliedweise Multiplikation verwenden, sondern diese Verknüpfung in anderer Weise festlegen. Das bedingt dann auch ein anderes neutrales Element

Satz 2.5.3 *Sei R ein kommutativer Ring mit 1 und seien $(R^{\mathbb{N}_0},+)$ und $(R^{(\mathbb{N}_0)},+)$ die eben eingeführten abelschen Gruppen. Mit der Multiplikation*

$$\begin{array}{rcl} \cdot : R^{\mathbb{N}_0} \times R^{\mathbb{N}_0} & \longrightarrow & R^{\mathbb{N}_0} \\ ((a_i)_{i\in\mathbb{N}_0},(b_i)_{i\in\mathbb{N}_0}) & \longmapsto & (\sum\limits_{k+m=i} a_k b_m)_{i\in\mathbb{N}_0} \end{array}$$

ist $(R^{\mathbb{N}_0},+,\cdot)$ ein kommutativer Ring mit Einselement $(e_i)_{i\in\mathbb{N}_0} = (1,0,\dots)$. Mit dieser Multiplikation ist $(R^{(\mathbb{N}_0)},+,\cdot)$ ein Unterring von $(R^{\mathbb{N}_0},+,\cdot)$.

Beweis: Zu zeigen ist hier zuerst die Assozitativität (AG) sowie das neutrale Element (NE) für den größeren Ring.

(AG) Seien $(a_i)_{i\in\mathbb{N}_0},(b_i)_{i\in\mathbb{N}_0},(c_i)_{i\in\mathbb{N}_0} \in R^{\mathbb{N}_0}$. Dann gilt

$$\begin{aligned} ((a_i)_{i\in\mathbb{N}_0}\cdot(b_i)_{i\in\mathbb{N}_0})\cdot(c_i)_{i\in\mathbb{N}_0} &= \left(\sum_{r+m=i}\left(\sum_{j+k=r} a_j b_k\right) c_m\right)_{i\in\mathbb{N}_0} \\ &= \left(\sum_{j+k+m=i} a_j b_k c_m\right)_{i\in\mathbb{N}_0} \\ &= \left(\sum_{j+r=i} a_j\left(\sum_{k+m=r} b_k c_m\right)\right)_{i\in\mathbb{N}_0} \\ &= (a_i)_{i\in\mathbb{N}_0}\cdot((b_i)_{i\in\mathbb{N}_0}\cdot(c_i)_{i\in\mathbb{N}_0}). \end{aligned}$$

(NE) Sei $(a_i)_{i\in\mathbb{N}_0} \in R^{\mathbb{N}_0}$. Dann gilt

$$\begin{aligned}(e_i)_{i\in\mathbb{N}_0}\cdot(a_i)_{i\in\mathbb{N}_0} &= \left(\sum_{j+k=i} e_j a_k\right)_{i\in\mathbb{N}_0}\\ &= (a_i)_{i\in\mathbb{N}_0}\\ &= \left(\sum_{j+k=i} a_j e_k\right)_{i\in\mathbb{N}_0}\\ &= (a_i)_{i\in\mathbb{N}_0}\cdot(e_i)_{i\in\mathbb{N}_0}\end{aligned}$$

Da wir wissen, dass der kleinere Ring eine abelsche Untergruppe des größeren Rings bzgl. der Addition ist und da $(e_i)_{i\in\mathbb{N}_0}$ offensichtlich im kleineren Ring enthalten ist, bleibt nur noch die Abgeschlossenheit der Multiplikation für die Anwendung des Unterringkriteriums übrig. Seien dazu $(a_i)_{i\in\mathbb{N}_0}, (b_i)_{i\in\mathbb{N}_0} \in R^{(\mathbb{N}_0)}$. Dann gibt es $i_0, j_0 \in \mathbb{N}_0$, so dass $a_i = 0$ und $b_j = 0$ für alle $i \geq i_0$ bzw. $j \geq j_0$. Damit ist

$$\sum_{i+j=m} a_i b_j = 0 \quad \text{für alle } m \geq i_0 + j_0,$$

was die Abgeschlossenheit unter Multiplikation zeigt.

□

Bemerkung 2.5.4 *Die Abbildung*

$$\begin{aligned}\varphi : R &\longrightarrow R^{(\mathbb{N}_0)}\\ a &\longmapsto (a, 0, \dots)\end{aligned}$$

ist ein injektiver Ringhomomorphismus, wie man direkt nachprüfen kann. Damit läßt sich R auffassen als Unterring von $R^{(\mathbb{N}_0)}$ und damit auch von $R^{\mathbb{N}_0}$.

Die gerade eingeführte Multiplikation erscheint auf den ersten Blick unnatürlich. Die Philosophie dahinter ist, dass zu dem m-ten Folgenglied des Produkts die Produkte all derjenigen Folgenglieder der Faktoren beitragen, deren Indizes in Summe gerade m ergeben. Wir können ein neues Symbol t wählen und den i-ten Eintrag einer Folge mit t^i markieren. Dann tragen zum

m-ten Glied des Produkts der Folgen $(a_i t^i)$ und $(b_j t^j)$ genau die Glieder bei, bei denen $t^i \cdot t^j = t^m$. Das erinnert doch schon sehr an das Produkt zweier Summen, wie wir es aus der Schule und den vorigen Semestern kennen. Deshalb kann man die folgen aus $R^{\mathbb{N}_0}$ und $R^{(\mathbb{N}_0)}$ auch mit Hilfe des neuen Symbols t als formale Summen schreiben und die oben definierte Multiplikation als Produkt der Summen auffassen.

Definition 2.5.5 *Sei R ein kommutativer Ring mit 1. Ein Element von $R^{\mathbb{N}_0}$ heißt* **formale Potenzreihe** *über R, ein Element von $R^{(\mathbb{N}_0)}$ heißt* **Polynom** *über R. Das i-te Folgenglied einer Potenzreihe oder eines Polynoms wird als i-ter* **Koeffizient** *bezeichnet. Das neutrale Element der Addition als das* **Nullpolynom**.
Für den Ring der formalen Potenzreihen über R schreiben wir

$$R[[t]] = \{f = \sum_{i=0}^{\infty} a_i t^i \mid (a_i)_{i\in\mathbb{N}_0} \in R^{\mathbb{N}_0}\}$$

mit einem neuen Symbol t und sagen der Ring der formalen Potenzreihen über R in der Variablen t, für den Ring der Polynome über R schreiben wir analog

$$R[t] = \{f = \sum_{i=0}^{\infty} a_i t^i \mid (a_i)_{i\in\mathbb{N}_0} \in R^{(\mathbb{N}_0)}\}.$$

Bemerkung 2.5.6 *Sei R ein kommutativer Ring mit 1 und sei $f = \sum_{i=0}^{\infty} a_i t^i \in R[t]$. Dann sind nur endlich viele Koeffizienten von f nicht Null und es existiert ein maximales $i \in \mathbb{N}_0$ mit $a_i \neq 0$.*

Definition 2.5.7 *Sei R ein kommutativer Ring mit 1. Die Abbildung*

$$\begin{aligned} \deg : R[t] \setminus \{0\} &\longrightarrow \mathbb{N}_0 \\ \sum_{i=0}^{\infty} a_i t^i &\longmapsto \max\{i \in \mathbb{N}_0 \mid a_i \neq 0\} \end{aligned}$$

heißt die **Gradabbildung**. *Für $f = \sum_{i=0}^{\infty} a_i t^i \in R[t]$ wird $\deg(f)$ als der* **Grad** *von f bezeichnet, $a_{\deg(f)}$ heißt der* **Leitkoeffizient** *von f, kurz $LC(f)$, $a_{\deg(f)} t^{\deg(f)}$ der* **Leitterm** *von f, kurz $LT(f)$.*
Wir setzen $\deg(0) := -\infty$.

Ist $\deg(f) = n$, so schreiben wir auch $\sum_{i=0}^{n} a_i t^i$ statt $\sum_{i=0}^{\infty} a_i t^i$.

Beobachtung 2.5.8

- *Ist R ein Körper, so ist $R[t]$ ein unendlich-dimensionaler Vektorraum mit Basis $(1, t, t^2, \dots)$.*
- *Seien $f = \sum_{i=1}^{n} a_i t^i, g = \sum_{i=1}^{m} b_i t^i \in R[t]$ mit $a_n \neq 0 \neq b_m$. Dann gilt*

$$\deg(f+g) \leq \max\{n, m\}$$

da für alle $j > \max\{n, m\}$ gilt: $a_j = 0 = b_j$ und damit auch $a_j + b_j = 0$. Gleichheit gilt in der Ungleichung offensichtlich, falls $n \neq m$ gilt oder bei $n = m$ dann $a_n \neq -b_n$.

- *Seien f und g wie zuvor. Dann gilt*

$$\deg(f \cdot g) \leq n + m,$$

da für jedes $j > n + m$ gilt, dass $k + r = j$ nur gelten kann, wenn mindestens eine der beiden Ungleichungen $k > n$ und $r > m$ erfüllt ist. (Beachten Sie, dass $-\infty + m = -\infty = n - \infty$.)

Lemma 2.5.9 *Sei R kommutativer Ring mit 1 und seien $f, g \in R[t]$. Dann gilt:*

a) Sind die Leitkoeffizienten von f und g keine Nullteiler in R , so gilt

$$\deg(f \cdot g) = \deg(f) + \deg(g).$$

b) $R[t]$ ist genau dann nullteilerfrei, wenn R nullteilerfrei ist.

c) Ist R Integritätsring, so gilt

$$(R[t])^* = \varphi(R^*)$$

mit dem injektiven Ringhomomorphismus aus Bemerkung 2.5.4.

Beweis: Seien $f = \sum_{i=1}^{n} a_i t^i, g = \sum_{i=1}^{m} b_i t^i$ mit $a_n \neq 0 \neq b_m$. Sind a_n und b_m nicht Nullteiler in R, dann gilt $a_n \cdot b_m \neq 0$ und damit $\deg(f \cdot g) = n + m$, was Behauptung a) beweist.
Besitzt R Nullteiler, so sind diese mittels des injektiven Ringhomomorphismus φ aus Bemerkung 2.5.4 auch Nullteiler in $R[t]$. Besitzt andererseits $R[t]$ Nullteiler $f = \sum_{i=1}^{n} a_i t^i$ und $g = \sum_{i=1}^{m} b_i t^i$ mit $a_n \neq 0 \neq b_m$ und $f \cdot g = 0$, so muss der $n + m$-te Koeffizient von $f \cdot g$, also $a_n \cdot b_m$, ebenfalls Null sein, was

uns Nullteiler in R liefert. Dies beweist die Äquivalenz b).
Ist R Integritätsring, so gilt nach a) und b) für alle Einheiten $f = \sum_{i=1}^{n} a_i t^i, g = \sum_{i=1}^{m} b_i t^i \in R[t]$ mit $a_n \neq 0 \neq b_m$ und $f \cdot g = 1_R$:

$$0 = \deg(1_r) = \deg(f \cdot g) = n + m,$$

und damit $n = m = 0$. Ausserdem muss gelten $a_0 \cdot b_0 = 1$, weswegen a_0 und b_0 bereits Einheiten in R sein müssen, was den Beweis abschließt.

□

Ist K ein Körper, so besagt Aussage c) des obigen Lemmas gerade, dass die Einheiten des Polynomrings in einer Variable über K genau die von Null verschiedenen Körperelemente sind.

Ein Analogon zur Aussage a) des vorigen Lemmas macht im Potenzreihenring keinen Sinn. Aussage b) des vorigen Lemmas gilt auch für Potenzreihenringe, jedoch gibt es einen kleinen, aber wichtigen Unterschied im Beweis. (Achten Sie mal darauf, wenn Sie das hier nacharbeiten.) Aussage c) gilt nicht wie oben, sondern es gibt nur eine strikte Inklusion der Einheitengruppen, was zeigt, dass der Potenzreihenring mehr Einheiten besitzt als der Polynomring.

Lemma 2.5.10 *Sei R kommutativer Ring mit 1. Dann gilt:*

a) $R[[t]]$ ist genau dann nullteilerfrei, wenn R nullteilerfrei ist.

b) $(R[[t]])^* = \{f = \sum_{i=0}^{\infty} a_i t^i \in R[[t]] \mid a_0 \in R^*\}$.

Beweis: Besitzt R Nullteiler, so sind diese mittels des injektiven Ringhomomorphismus φ aus Bemerkung 2.5.4 und der Inklusion von Ringen $R[t] \leq R[[t]]$ auch Nullteiler in $R[[t]]$. Besitzt andererseits $R[[t]]$ Nullteiler $f = \sum_{i=0}^{\infty} a_i t^i$ und $g = \sum_{i=0}^{\infty} b_i t^i$ mit $f \cdot g = 0$, so gibt es wegen $f \neq 0 \neq g$ kleinste Indices[2] m, n mit $a_n \neq 0 \neq b_m$. Der $(n+m)$-te Koeffizient von $f \cdot g$ ist dann gerade $a_n \cdot b_m$ und muss wegen $f \cdot g = 0_{R[[t]}$ Null sein, was uns Nullteiler in R liefert. Dies beweist die Äquivalenz a).
Ist $f = \sum_{i=1}^{\infty} a_i t^i \in (R[[t]])^*$ und $g = \sum_{i=1}^{\infty} b_i t^i$ das zugehörige inverse Element, so gilt $f \cdot_{R[[t]]} g = 1_{R[[t]}$ und damit insbesondere $a_0 \cdot_R b_0 = 1_R$, weswegen a_0 eine Einheit sein muss. Ist andererseits $f = \sum_{i=0}^{\infty} a_i t^i$ und $a_0 \in R^*$, so gibt

[2] Das Wohlordnungsaxiom läßt hier grüßen.

es ein $b_0 \in R$ mit $a_0 \cdot b_0 = 1$. Nun machen wir einen Ansatz für ein mögliches Inverses zu f, nämlich eine Potenzreihe $g = \sum_{i=0}^{\infty} b_i t^i$, die bei diesem b_0 beginnt und deren weitere Koeffizienten noch unbekannt sind. Induktiv muss nun aber bei bereits bestimmten Koeffizienten $b_0, \ldots, b_{n-1}$ für den n-ten Koeffizienten von g gelten:

$$a_0 b_n + \sum_{j=1}^{n} a_j b_{n-j} = 0.$$

Dies bestimmt aber eindeutig den Koeffizienten b_n durch

$$b_n = -\sum_{j=1}^{n} \frac{a_j}{a_0} b_{n-j},$$

was die gesuchte Inverse g liefert.

□

Ihnen ist sicher aufgefallen, dass ich auf den letzten Seiten peinlich genau darauf geachtet habe, von *einem neuen Symbol t* zu sprechen und dieses nicht als eine Element eines geeigneten Ringes aufzufassen. Das hat einen guten Grund: Das Einsetzen eines Elements eines geeigneten Ringes in ein Polynom stellt selbst eine Abbildung vom Polynomring in den Ring dar. Diese muss aber nicht injektiv sein, was sie umso interessanter macht.

Definition 2.5.11 *(Einsetzungshomomorphismus) Sei S ein (nicht notwendigerweise kommutativer) Ring und R ein kommutativer Unterring von S. Ein Element $\alpha \in S$ heißt* **einsetzbar** *in Polynome über R, falls es mit jedem Element aus R kommutiert, d.h.*

$$r\alpha = \alpha r \quad \forall r \in R.$$

In diesem Fall definieren wir die Einsetzungsabbildung von α in Polynome über R als

$$\begin{array}{rcl} E_\alpha : R[t] & \longrightarrow & S \\ f = \sum_{i=0}^{n} a_i t^i & \longmapsto & f(\alpha) = \sum_{i=0}^{n} a_i \alpha^i \end{array}$$

Bitte beachten Sie, dass wegen der Kommutativität des Ringes R, alle Elemente aus R stets einsetzbar sind. Dennoch sind das meist nicht die einzigen Elemente aus S, die einsetzbar sind in Polynome über $R[t]$. Denken Sie etwa an das Einsetzen von reellen oder komplexen Zahlen in Polynome mit ganzzahligen Koeffizenten.

Satz 2.5.12 *Seien R, S und α wie in der vorigen Definition. Dann gilt:*

a) *E_α ist ein Ringhomomorphismus.*

b) *$R[\alpha] := \mathrm{Im}(E_\alpha) = \{f(\alpha) \mid f \in R[t]\}$ ist ein kommutativer Unterring von S.*

c) $\ker(E_\alpha) = \{f \in R[t] \mid f(\alpha) = 0\}$.

Beweis:

a) Zum Nachweis, dass E_α ein Ringhomomorphismus ist, sind drei Eigenschaften zu zeigen: Verträglichkeit mit Addition und Multiplikation sowie Abbildung des 1-Elements auf das 1-Element. Diese rechnen wir nun nach. Dazu seien $f = \sum_{i=0}^{n} a_i t^i$ und $g = \sum_{i=0}^{m} b_i t^i$ beliebige Elemente von $R[t]$. (Denken Sie daran, dass auch Koeffizienten jenseits des Grades definiert sind und den Wert 0 haben):

$$\begin{aligned} E_\alpha(f+g) &= E_\alpha\left(\sum_{i=0}^{\max\{n,m\}} (a_i + b_i)t^i\right) \\ &= \sum_{i=0}^{\max\{n,m\}} (a_i + b_i)\alpha^i \\ &= \left(\sum_{i=0}^{\max\{n,m\}} a_i\alpha^i\right) + \left(\sum_{i=0}^{\max\{n,m\}} b_i\alpha^i\right) \\ &= E_\alpha(f) + E_\alpha(g) \end{aligned}$$

$$\begin{aligned} E_\alpha(f \cdot g) &= E_\alpha\left(\sum_{i=0}^{n+m}\left(\sum_{j+k=i} a_j b_k\right) t^i\right) \\ &= \sum_{i=0}^{n+m}\left(\sum_{j+k=i} a_j b_k\right)\alpha^i \\ &\overset{\alpha r = r\alpha}{=} \left(\sum_{i=0}^{n} a_i \alpha^i\right)\cdot\left(\sum_{i=0}^{m} b_i \alpha^i\right) \\ &= E_\alpha(f)\cdot E_\alpha(g) \end{aligned}$$

$$\begin{aligned} E_\alpha(1_{R[t]}) &= E_\alpha(1_R) \\ &= 1_R \end{aligned}$$

b) Diese Aussage ist eine direkte Anwendung von 2.3.7,a) sowie für die Kommutativität von 2.3.7,d).

c) Diese Aussage ist die direkte Anwendung der Definition des Kerns.

□

Die obige Definition und der eben bewiesen Satz rechtfertigen das Einsetzen von Werten in Polynome, wie wir es schon zu Schulzeiten gemacht haben, ohne damals darüber nachzudenken. Mehr noch: die Überlegungen erlauben ein entsprechendes Vorgehen auch für Polynome über Ringen und klären, was einsetzbar ist. Schlampigerweise werden wir oft auch statt $E_\alpha(f)$ einfach wieder $f(\alpha)$ schreiben. Da Einsetzen ein Homomorphismus ist, gilt dann auch $(f+g)(\alpha) = f(\alpha) + g(\alpha)$ sowie $(f \cdot g)(\alpha) = f(\alpha) \cdot g(\alpha)$.

Die genauere Beschreibung des Kerns des Einsetzungshomomorphismus hat sie in anderer Sprechweise bereits in der Schule beschäftigt: Es ist die Frage nach Nullstellen von Polynomen. Ehe wir uns damit jedoch genauer beschäftigen können, müssen wir noch einen weiteren Begriff einführen, die Teilbarkeit von Polynomen:

Satz 2.5.13 *Sei R ein kommutativer Ring. Seien $f, g \in R[t]$ mit $LC(g) \in R^*$. Dann existieren eindeutige Polynome $q, r \in R[t]$, so daß*

$$f = q \cdot g + r \quad \textit{und } \deg(r) < \deg(g).$$

Beweis: Siehe Videoschnippsel DivMitRestPolynome.

□

Vergleichen sie die Struktur dieser Division mit Rest mit der in 1.1.1. Die verblüffende Ähnlichkeit ist kein Zufall, sondern beruht auf tieferen Gemeinsamkeiten der beiden Ringe, die wir in Abschnitt 2.7 noch allgemeiner untersuchen werden.

Bemerkung 2.5.14 *Die Zusatzbedingung $LC(g) \in R^*$ sichert im allgemeinen Fall auch, daß $g \neq 0$ gilt. Ist R ein Körper, so ist jedes Element außer Null eine Einheit und die Bedingung ist sogar äquivalent zu $g \neq 0$.*

Definition 2.5.15 *Sei R kommutativer Ring und seien $f, g \in R[t]$. f heißt teilbar durch g, falls es ein $q \in R[t]$ gibt mit $f = q \cdot g$.*
Sei S ein Ring, für den R ein Unterring ist. Ein einsetzbares $\alpha \in S$ heißt Nullstelle eines $f \in R[t]$, falls $f(\alpha) = 0$.

Blättern Sie einmal zurück zur Division mit Rest in den ganzen Zahlen. Bei der Definition der Teilbarkeit konnten wir dort auf die Division mit Rest zurückgreifen. Hier ist das schwieriger, weil auch ein Polynom f mit $LC(f) \notin R^*$ ein Teiler eines anderen Polynoms sein kann, dies aber vom Satz über die Division mit Rest nicht abgedeckt ist.

Proposition 2.5.16 *Sei R kommutativer Ring, $f \in R[t]$ und $\alpha \in R$. Dann existiert ein eindeutiges $q \in R[t]$ mit*

$$f = q \cdot (t - \alpha) + f(\alpha),$$

wobei $\deg(q) = \deg(f) - 1$.

Beweis:
Fall 1: $f_1 = a_n t^n$
Da $LC(t - \alpha) = 1_R$, können stets geeignete Vielfache von $t - \alpha$ von f_1 abziehen, so dass der Grad der Differenz kleiner als n ist. Dies werden wir nun induktiv für n ausführen: Ist $n = 0$, so ist f_1 konstant, $q = 0$ und $f_1(\alpha) = f_1(t)$, was den Induktionsanfang bildet. Sei nun als Induktionsvoraussetzung die Behauptung für Monome (d.h. Polynome mit nur einem von

Null verschiedenen Summanden) bis zum Grad n bewiesen. Im Induktionsschritt sei $f_1 = a_{n+1}t^{n+1}$ und wir rechnen:

$$f_1 = a_{n+1}t^{n+1} = a_{n+1}t^n(t-\alpha) + a_{n+1}\alpha t^n$$

Dann gibt es nach Induktionsvoraussetzung $q_1 \in R[t]$ mit $t^n = q_1(t-\alpha)+\alpha^n$, das wir in f_1 einsetzen können:

$$\begin{aligned} f_1 &= a_{n+1}(q_1(t-\alpha)+\alpha^n)(t-\alpha) + a_{n+1}\alpha(q_1(t-\alpha)+\alpha^n) \\ &= \underbrace{(a_{n+1}(q_1(t-\alpha)+\alpha^n) + a_{n+1}\alpha q_1)}_{:=q}(t-\alpha) + a_{n+1}\alpha^{n+1}, \end{aligned}$$

womit wir die gesuchte Darstellung gefunden haben.

Fall 2: $f \in R[t]$ beliebig
Auch diesen Fall behandeln wir mittels Induktion und verwenden dabei die Vorüberlegung aus Fall 1: Der Induktionsanfang bleibt derselbe wie im anderen Fall, da Polynome vom Grad Null Monome sind. Als Induktionsvoraussetzung sei die Behauptung bewiesen für $\deg(f) \leq n$. Im Induktionsschritt zerlegen wir f in seinen Leitterm und die anderen Terme $f = a_{n+1}t^{n+1}+f_2$, dann wissen wir nach Induktionsvoraussetzung und Fall 1, dass es $q_1, q_2 \in R[t]$ gibt mit

$$\begin{aligned} f_2 &= q_2(t-\alpha) + f_2(\alpha) \\ a_{n+1}t^{n+1} &= q_1(t-\alpha) + a_{n+1}\alpha^{n+1} \text{ und damit} \\ f &= q_1(t-\alpha) + a_{n+1}\alpha^{n+1} + q_2(t-\alpha) + f_2(\alpha) \\ &= \underbrace{(q_1+q_2)}_{:=q}(t-\alpha) + \underbrace{(a_{n+1}\alpha^{n+1} + f_2(\alpha))}_{=f(\alpha)}. \end{aligned}$$

Damit ist die Existenz gezeigt.
Für die Eindeutigkeit nehmen wir an, dass $q, s \in R[t]$ beide die Behauptung erfüllen:

$$q \cdot (t-\alpha) = f = s \cdot (t-\alpha).$$

Damit gilt:

$$(q-s)(t-\alpha) = 0.$$

Da aber $LC(t-\alpha) = 1$ und damit $(t-\alpha)$ kein Nullteiler sein kann, muss $q-s=0$ gelten, weswegen $q=s$ und damit die Eindeutigkeit gezeigt ist.

□

Korollar 2.5.17 *Sei R ein kommutativer Ring, $f \in R[t]$ und $\alpha \in R$. Dann gilt*

$$\alpha \text{ ist Nullstelle von } f \iff (t-\alpha) \mid f.$$

Beweis: α ist Nullstelle von f, genau dann wenn $f(\alpha) = 0$. Das bedeutet aber nach Proposition 2.5.16 genau, dass $f = q \cdot (t-\alpha)$, was nach Definition gerade $(t-\alpha) \mid f$ bedeutet.

□

Aus der Analysis sind wir darauf gepägt, nach mehrfachen Nullstellen zu suchen, indem wir die gemeinsamen Nullstellen einer Polynomfunktion und ihrer Ableitung zu betrachten. So würden wir natürlich auch für allgemeine Polynome vorgehen wollen, haben aber leider keine Ableitung, wie sie in der Analysis mittels einer Limes-Betrachtung definiert wurde, zur Verfügung. Stattdessen betrachten wir die Konstruktion, mit der die Ableitung eines Polynoms in der Analysis bestimmt werden konnte als Definition einer formalen Ableitung.

Definition 2.5.18 *Sei R ein Integritätsring und $f = \sum_{i=0}^{n} a_i t^i \in R[t]$. Dann ist die* **formale Ableitung** *von f das Polynom*

$$f' = \sum_{i=1}^{n} i a_i t^{i-1} \in R[t].$$

Proposition 2.5.19 *Sei R ein Integritätsring, seien $f, g \in R[t]$ und $\alpha \in R$. Dann gilt:*

a) $(\alpha f)' = \alpha f'$

b) $(f+g)' = f' + g'$

c) $(f \cdot g)' = f' \cdot g + f \cdot g'$

Beweis: Alle drei Eigenschaften lassen sich direkt mit der Definition nachrechnen. Die explizite Ausführung bleibt den Lesern überlassen.

□

Definition 2.5.20 *Sei R ein Integritätsring, $f \in R[t]$ und $\alpha \in R$ eine Nullstelle von f. α heißt m-**fache Nullstelle** von f, falls*

$$\exists g \in R[t] : f = (t-\alpha)^m \cdot g \quad \text{und} \quad g(\alpha) \neq 0$$

Proposition 2.5.21 *Seien $R \leq S$ Integritätsringe, $f \in R[t]$ und $\alpha \in S$ in f einsetzbar. Dann gilt:*

$$\alpha \text{ mehrfache Nullstelle von } f \iff f(\alpha) = 0 = f'(\alpha).$$

Bei diesem Beweis sollten Sie sich die Bedeutung einer mehrfachen Nullstelle nochmals vor Augen führen und an das obige Korollar zurückdenken. Der Beweis bleibt als Aufgabe für Übungsblatt 3.

Zum Abschluss dieses Abschnitts wenden wir uns nun einer Konstruktion zu, die Sie bereits für die ganzen Zahlen gesehen haben: Wir betrachten die Restklassen bzgl. eines Elements. Wie dort auch kann man zwei Zugänge wählen, die wir hier beide kurz skizzieren – vergleichen Sie beim Nacharbeiten mit der Konstruktion von $\mathbb{Z}_m$ bzw. $\mathbb{Z}/m\mathbb{Z}$ aus der Linearen Algebra und füllen Sie die fehlenden Details selbst.

Konstruktion 2.5.22 *Sei R ein kommutativer Ring und sei $d \in \mathbb{N}$.*

Variante 1: $R[t]_{\leq d}$
Wir setzen als Menge:

$$R[t]_{\leq d} := \{f \in R[t] \mid \deg(f) \leq d\} \subseteq R[t].$$

Sei $h \in R[t]$ mit $LC(h) \in R^*$ und $\deg(h) = d+1$. Dann ist Division mit Rest durch h definiert und wir können $R[t]_{\leq d}$ auch als die Reste der Division durch h auffassen und damit Rechenoperationen darauf definieren:

$$R[t]_{\leq d} = \{f \in R[t] \mid \deg(f) < \deg(h)\}$$

mit den Operationen

$$\begin{aligned} + : R[t]_{\leq d} \times R[t]_{\leq d} &\longrightarrow R[t]_{\leq d} \\ (f,g) &\longmapsto (f+g) \bmod h \\ \cdot : R[t]_{\leq d} \times R[t]_{\leq d} &\longrightarrow R[t]_{\leq d} \\ (f,g) &\longmapsto (f \cdot g) \bmod h \end{aligned}$$

Dann läßt sich analog zu $\mathbb{Z}_m$ *zeigen, dass* $(R[t]_{\leq d}, +, \cdot)$ *ein kommutativer Ring mit* 1 *ist und dass*

$$\begin{array}{rcl} \rho_h : R[t] & \longrightarrow & R[t]_{\leq d} \\ f & \longmapsto & f \bmod h \end{array}$$

ein Ringepimorphismus ist.

Variante 2: $R[t]/ < h >$
Sei $h \in R[t]$ *mit* $LC(h) \in R^*$ *und* $\deg(h) = d + 1$. *Definiere*

$$< h >:= \{ah \mid a \in R[t]\}.$$

Dann definiert $f \sim_h g :\Longleftrightarrow f - g \in < h >$ *eine Äquivalenzrelation auf* $R[t]$. *Die Menge* $R[t]/ < h >$ *ist ein kommutativer Ring mit* 1 *bzgl. der induzierten Addition und Multiplikation und*

$$\begin{array}{rcl} \rho_h : R[t] & \longrightarrow & R[t]/ < h > \\ f & \longmapsto & [f]_h \end{array}$$

ist ein Ringepimorphismus. In dieser Variante sind alle Konstruktionen analog zu $\mathbb{Z}/m\mathbb{Z}$.

2.6 Ideale

Der Begriff eines Ideals ist uns bereits für Ideale in $\mathbb{Z}$ bekannt, wo er half, sehr knapp und präzise Aussagen wie die Bezout-Identität zu formulieren. Diese Begriffsbildung würden wir gerne auch in beliebigen Ringen mit 1 vornehmen, müssen dabei allerdings etwas genauer auf Details achten, wie die folgende Definition im Vergleich zu Definition 1.2.1 zeigt.

Definition 2.6.1 *Sei R ein Ring. Eine Teilmenge $\emptyset \neq I \subseteq R$ heißt* **Linksideal** *in R, falls gilt:*

a) $\forall a, b \in I : \quad a + b \in I$

b) $\forall a \in I, \forall r \in R : \quad ra \in I$

Analog heißt eine Teilmenge $\emptyset \neq I \subseteq R$ heißt **Rechtsideal** *in R, falls gilt:*

a) $\forall a, b \in I : \quad a + b \in I$

b) $\forall a \in I, \forall r \in R : \quad ar \in I$

I heißt ein **Ideal** *(oder präziser* **zweiseitiges Ideal***) in R, falls es Rechts- und Linksideal ist.*

Bemerkung 2.6.2 *Wegen Bedingung b) enthält jedes Ideal das Element 0_R.*

Bemerkung 2.6.3 *Ist R ein kommutativer Ring, dann fallen die Begriffe Rechts- und Linksideal zusammen mit dem Begriff eines Ideals. Damit ist der Begriff eines Ideals in $\mathbb{Z}$, wie wir ihn aus Abschnitt 1.1 kennen, lediglich ein Spezialfall der allgemeinen Definition.*

Bemerkung 2.6.4 *Die beiden Bedingungen an ein Linksideal kann man zusammenfassen als*

$$\forall a, b \in I, \forall r, s \in R : \quad ra + sb \in I.$$

Ein Linksideal enthält also jede linksseitige R-Linearkombination von Elementen aus I. Für Rechtsideale und zweiseitige Ideale können die entsprechenden Bedingungen analog zusammengefasst werden.

Notation 2.6.5 *Wie schon im Fall des Ringes der ganzen Zahlen, so schreiben wir auch im allgemeinen Fall:*

$$\begin{aligned}\langle a_1,\dots,a_n\rangle_\ell &:= \{\sum_{i=1}^{n} r_i a_i \mid r_1,\dots,r_n \in R\}\\ \langle a_1,\dots,a_n\rangle_r &:= \{\sum_{i=1}^{n} a_i r_i \mid r_1,\dots,r_n \in R\}\\ \langle a_1,\dots,a_n\rangle &:= \{\sum_{i=1}^{n} r_i a_i s_i \mid r_1,\dots,r_n,s_1,\dots,s_n \in R\}\end{aligned}$$

für das Links- und Rechtsideal, das von $a_1,\dots,a_n \in R$ erzeugt wird. Analog schreiben wir im kommutativen Fall:

$$\langle a_1,\dots,a_n\rangle := \{\sum_{i=1}^{n} r_i a_i \mid r_1,\dots,r_n \in R\}$$

für das von $a_1,\dots,a_n \in R$ erzeugte Ideal.
Für unendliche Mengen $\emptyset \neq A \subseteq R$ schreiben wir:

$$\langle A\rangle_\ell := \{\sum_{i=1}^{n} r_i a_i \mid n \in \mathbb{N}, a_1,\dots,a_n \in A, r_1,\dots,r_n \in R\}$$

sowie die analogen Notationen für Rechtsideale und zweiseitige Ideale

Nicht jedes Ideal kann von endlich vielen Elementen erzeugt werden. Ein Ring, in dem jedes Ideal endlich erzeugt ist, heißt noetherscher Ring. Diesen Begriff werden wir in der Kommutativen Algebra näher studieren. In der Algebra I fehlt uns dafür die Zeit.

Notation 2.6.6 *Jeder Ring R enthält die Ideale $\langle 0_R\rangle = \{0_R\}$, das* **Nullideal**, *und $\langle 1_R\rangle = R$, das* **Einsideal** . *Wir bezeichnen diese beiden Ideale auch als die* **trivialen Ideale** *in R. Ein Ideal $I \subset R$ mit $\{0\} \subsetneq I \subsetneq R$ heißt ein* **echtes Ideal** *in R.*

Denken Sie an die Generalvoraussetzung, dass ab 2.3 alle Ringe eine $1 \neq 0$ haben.

Lemma 2.6.7 *Sei K kommutativer Ring. K ist genau dann ein Körper, wenn $\langle 0_K\rangle = \{0_K\}$ und $\langle 1_K\rangle = K$ die einzigen Ideale in K sind.*

Beweis: " $\Longrightarrow$ ":
Sei $I \subseteq K$ ein Ideal, das mindestens ein von Null verschiedenes Element a enthält. Dann existiert, da K Körper ist, auch ein multiplikatives Inverses a^{-1} zu a in K. Damit muss gelten, dass $1_K = a^{-1}a \in K$. Also ist I bereits der Körper K.
" $\Longleftarrow$ ":
Ist K kein Körper, so gibt es ein $a \in K \setminus \{0\}$, welches kein multiplikatives Inverses besitzt. Damit kann 1_K kein Vielfaches von a sein und es gilt:

$$\langle 0_K \rangle \subsetneq \langle a \rangle \subsetneq \langle 1_K \rangle,$$

was zu zeigen war.

□

Satz 2.6.8 *Seien R, S Ringe und sei $\varphi : R \longrightarrow S$ ein Ringhomomorphismus. Dann ist* $\ker(\varphi) \trianglelefteq R$ *ein Ideal in R. Da nach Generalvoraussetzung $1_R \neq 0_R$ ist* $\ker(\varphi)$ *eine echte Teilmenge von R.*

Beweis: Wir wissen, dass $\ker(\varphi) \neq \emptyset$, da $\varphi(0_R) = 0_S$ für jeden Gruppenhomomorphismus, als den sich die Abbildung φ bzgl. der zugrunde liegenden additiven Gruppen von R und S auffassen läßt.
Sind nun $a_1, a_2 \in \ker(\varphi)$ und $r_1, r_2 \in R$ beliebig. Dann gilt:

$$\begin{aligned} \varphi(r_1a_1 + r_2a_2) &= \varphi(r_1)\underbrace{\varphi(a_1)}_{=0_S} + \varphi(r_2)\underbrace{\varphi(a_2)}_{=0_S} = 0_S \\ \varphi(a_1r_1 + a_2r_2) &= \underbrace{\varphi(a_1)}_{=0_S}\varphi(r_1) + \underbrace{\varphi(a_2)}_{=0_S}\varphi(r_2) = 0_S. \end{aligned}$$

Somit liegt mit auch jede linksseitige und jede rechtsseitige R-Linearkombination von a_1 und a_2 in $\ker(\varphi)$, was damit ein Ideal in R ist.
Da wir mit Ringen mit $1 \neq 0$ arbeiten, ist eine der Bedingungen an den Ringhomomorphismus, dass $\varphi(1_R) = 1_S \neq 0_S$, weswegen $1_R \notin \ker(\varphi)$.

□

Korollar 2.6.9 *Sei R ein Ring mit $1 \neq 0$ und sei K ein Körper. Ist $\varphi : K \longrightarrow R$ ein Ringhomomorphismus, so ist φ injektiv.*

Beweis: Den Beweis finden Sie als Übungsaufgabe wieder.

□

Lemma 2.6.10 *Seien I, J Linksideale (bzw. Rechtsideale bzw. Ideale) in einem Ring R. Dann sind auch*

$$\begin{aligned} I + J &:= \{a + b \mid a \in I, b \in J\} \\ I \cap J &:= \{a \in R \mid a \in I \text{ und } a \in J\} \end{aligned}$$

Linksideale in R.

Der Beweis dieser Aussage besteht im Nachrechnen der Idealeigenschaften und bleibt den Studierenden überlassen.

Lemma 2.6.11 *Sei R ein Ring und $a \in R$. Dann gilt*

$$\langle a \rangle = \bigcap_{\substack{I \trianglelefteq R \\ a \in I}} I \trianglelefteq R.$$

Analoge Aussagen kann man für Links- bzw. Rechtsideal formulieren und beweisen, was im Vergleich zu zweiseitigen Idealen nur die offensichtlichen Änderungen erfordert.

Beweis: Offensichtlich ist $\langle a \rangle$ ein Ideal in R, das a enthält und damit ist die rechte Seite in der linken enthalten. Zu zeigen ist also nur die andere Inklusion.
Ist aber $a \in I$ für ein zweiseitiges Ideal I, so ist auch $ras \in I$ für alle $r, s \in R$ und damit $\langle a \rangle \subseteq I$. Damit ist $\langle a \rangle$ im Durchschnitt aller a enthaltenden Ideale enthalten.

□

Definition 2.6.12 *Sei R ein Ring und $I \trianglelefteq R$ ein Ideal (oder Linksideal oder Rechtsideal). Existiert ein $a \in I$, so dass $I = \langle a \rangle$ (bzw. $I = \langle a \rangle_\ell$ bzw. $I = \langle a \rangle_r$) , so heißt I* **Hauptideal** *(bzw.* **Linkshauptideal** *bzw.* **Rechtshauptideal***). Ist R ein Integritätsring und ist jedes Ideal in R ein Hauptideal, so heißt R* **Hauptidealring**.

Bemerkung 2.6.13 *Auch ein Ideal, das durch ein Erzeugersystem mit mehr als einem Erzeuger spezifiziert ist, kann ein Hauptideal sein. Man denke an $\langle 12, 15 \rangle \subseteq \mathbb{Z}$, was das von 3 erzeugte Hauptideal ist, oder an $\langle x^2 - 2x + 1, x^2 - 1 \rangle \subseteq \mathbb{Q}[x]$, welches von $x - 1$ erzeugt wird.*
Zwei Hauptideale $\langle a \rangle$ und $\langle b \rangle$ in einem Integritätsring R sind genau dann gleich, wenn es eine Einheit $c \in R^*$ gibt mit $a = cb$. Welches Argument brauchen Sie dafür?

Proposition 2.6.14 *$\mathbb{Z}[t]$ ist ein Integritätsring, jedoch kein Hauptidealring.*

Beweis: Da $\mathbb{Z}$ ein Integritätsring ist, ist nach 2.5.9,b) $\mathbb{Z}[t]$ ein Integritätsring. Betrachte andererseits $\langle 2, t\rangle \trianglelefteq \mathbb{Z}[t]$. Angenommen dieses Ideal ist ein Hauptideal $\langle a\rangle$. Dann gilt $a \neq 0$, $a \mid 2$ und $a \mid t$. Aus $a \neq 0$ und $a \mid 2$ können wir nach 2.5.9,a) schließen, dass $0 \leq \deg(a) \leq \deg(2) = 0$ gilt und damit $a \in \mathbb{Z}$. Wegen $a \mid t$ muss gelten $a = LC(a) \mid LC(t) = 1$, weswegen $a \in (\mathbb{Z}[t])^*$, das nach 2.5.9,c) gerade $\mathbb{Z}^* = \{1, -1\}$ ist. Andererseits gilt $1 \notin \langle 2, t\rangle$, was den gesuchten Widerspruch liefert. Also ist $\mathbb{Z}[t]$ kein Hauptidealring.

□

Proposition 2.6.15 *Sei R ein Integritätsring, aber kein Körper, so ist $R[t]$ kein Hauptidealring.*

Beweis: Dies finden Sie als Übungsaufgabe wieder.

□

2.7 Hauptidealringe und Euklidische Ringe

In Abschnitt 5 waren uns bereits frappierende Ähnlichkeiten zwischen $\mathbb{Z}$ und dem Polynomring über einem Körper aufgefallen. In diesem Abschnitt wollen wir die Gemeinsamkeiten nun in einen allgemeineren Kontext setzen.

Definition 2.7.1 *Ein Integritätsring R heißt* **euklidischer Ring**, *falls es eine Abbildung*

$$d : R \setminus \{0\} \longrightarrow \mathbb{N}_0$$

gibt, so dass für alle $a, b \in R$ mit $b \neq 0$ Elemente $q, r \in R$ existieren mit

$$a = qb + r \quad \text{mit} \quad (r = 0 \quad \text{oder } d(r) < d(b)).$$

Bemerkung 2.7.2 *Beachten Sie, dass im allgemeinen Fall keine Eindeutigkeitsaussage der Division mit Rest gefordert wird.*

Sobald wir Division mit Rest haben, können wir auch über größte gemeinsame Teiler sprechen. Dazu sollten wir allerdings unsere Definition von Teiler und größtem gemeinsamem Teiler auf diesen allgemeineren Fall erweitern, was aber keine inhaltlichen Schwierigkeiten bietet.

Definition 2.7.3 *Sei R ein Integritätsring und seien $a, b \in R$ mit $b \neq 0$. Dann ist b* **Teiler** *von a, falls es ein $q \in R$ gibt, so dass $a = qb$. In diesem Fall heisst a* **Vielfaches** *von b.*

Diese Begriffe sind uns im Fall der ganzen Zahlen schon aus Kapitel 1 bekannt. Ihre Verwendung wie auch das Symbol $b \mid a$ übernehmen wir auch in anderen Integritätsringen. Die Aussagen 1.1.5 gelten entsprechend mit Ausnahme von Aussage g). Diese finden wir hier in der allgemeinen Form wieder:

Definition 2.7.4 *Sei R ein Integritätsring, sei $\varepsilon \in R^*$ und seien $a, b \in R \setminus \{0\}$ mit $a = \varepsilon b$. Dann heissen a und b zueinander* **assoziiert**, *kurz $a \sim b$.*

Lemma 2.7.5 *Seien $a, b \in R$. Dann gilt:*

$$a \mid b \text{ und } b \mid a \implies a \sim b.$$

Die Beweisidee des vorigen Lemmas ist identisch mit der aus Kapitel 1.1. Der Unterschied in der Aussage beruht auf der Tatsache, dass $\mathbb{Z}^* = \{1, -1\}$, während in anderen Integritätsringen in der Regel viele mehr Einheiten existieren.

Bemerkung 2.7.6 *Die früher bereits betrachtete Gleichheit von Hauptidealen läßt sich nun auch formulieren als:*

$$\langle a \rangle = \langle b \rangle \Longleftrightarrow a \sim b.$$

In Hauptidealringen sind zwei Ideale also genau dann gleich, wenn sie von zueinander assoziierten Elementen erzeugt werden.

In Kapitel 1 folgte dann auf die Betrachtung der Teilbarkeit, der Begriff des größten gemeinsamen Teilers. Dieser Begriff läßt sind in Integritätsringen definieren.

Definition 2.7.7 *Sei R Integritätsring und seien $a, b \in R$ mit $b \neq 0$. Dann heißt eine Element $d \in R$* **ein größter gemeinsamer Teiler** *von a und b, falls*

a) d ist Teiler sowohl von a als auch von b

b) Jeder gemeinsame Teiler $c \in R$ von a und b ist auch Teiler von d.

Besonders einfach zu handhaben ist der Begriff eines größten gemeinsamen Teilers in euklidischen Ringen aufgrund der folgenden Beobachtung:

Bemerkung 2.7.8 *Ist R euklidischer Ring, so läßt sich die Bedingung in der Definition 2.7.3 auch schreiben als 'falls der Rest der Division von a durch b Null ist'.*

Der folgende Algorithmus, genannt Euklidischer Algorithmus, erlaubt uns die Bestimmung von größten gemeinsamen Teilern in euklidischen Ringen:

Algorithmus 2.7.9 *(Euklidischer Algorithmus)*

Voraussetzung:	*R euklidischer Ring*
Input:	*$a, b \in R$, $b \neq 0$*
Output:	*ein größter gemeinsamer Teiler von a und b*

- `WHILE` $(b \neq 0)$ $\{$
- $\quad r = a \bmod b$
- $\quad a = b$
- $\quad b = r\}$
- `RETURN`(a)

Der Algorithmus sieht erst einmal sehr abstrakt aus und Sie werden sich unter Umständen fragen, was da überhaupt geschieht. Ehe wir also die Korrektheit und die Terminierung des Algorithmus beweisen, betrachten wir dazu ein Beispiel. Das ist eigentlich immer eine gute Idee, wenn man mit einem Algorithmus oder einer Konstruktion konfrontiert ist und den Einstieg in das Erarbeiten nicht findet.

Bemerkung 2.7.10 *(mit Beispiel) Damit wir die Übersicht über die verschiedenen Durchläufe durch die* `WHILE`*-Schleife behalten, werden wir den auftretenden r jeweils einen Index geben, der beschreibt im wievielten Schleifendurchlauf sie entstanden sind. So starten wir mit $r_{-1} = a$ und $r_0 = b$ und erzeugen dann r_1,r_2 und so weiter. Damit liest sich die Rechnung des Algorithmus in induktiver Schreibweise für bereits bestimmte r_{i-1} und r_i wie folgt:*

$$r_{i+1} = r_{i-1} \bmod r_i.$$

In einem konkreten Beispiel haben wir dann für $a = 96$ und $b = 66$:

	a	b	*neuer Rest*	a *konkret*	b *konkret*	*neuer Rest*
Anfangswerte	r_{-1}	r_0	r_1	96	66	30
Durchlauf 1	r_0	r_1	r_2	66	30	6
Durchlauf 2	r_1	r_2	r_3	30	6	0

Damit wird wegen $r_3 = 0$ der Wert von r_2, also 6, vom Algorithmus zurückgegeben.

Beweis: (2.7.9) Terminierung:
Da r_{i+1} der Rest der Division von r_{i-1} durch r_i ist, gilt

$$d(r_0) > d(r_1) > \ldots d(r_i) > \ldots.$$

Es entsteht also eine strikt absteigende Sequenz von natürlichen Zahlen, die wegen der Endlichkeit der Menge $\{n \in \mathbb{N}_0 \mid n < d(r_0)\}$ nur endlich viele Elemente enthalten kann. Damit endet die Schleife nach endlich vielen Durchläufen, was bedeutet, dass zu diesem Zeitpunkt $r_n = 0$.

Korrektheit:
Es bleibt zu zeigen, dass r_{n-1} ein größter gemeinsamer Teiler der beiden Eingabewerte ist.
Wir wissen:

$$r_{i-1} = q_i \cdot r_i + r_{i+1} \text{ für alle } 0 \leq i < n,$$

weswegen ein gemeinsamer Teiler zweier aufeinanderfolgender Reste r_{i-1} und r_i auch Teiler des darauffolgenden r_{i+1} und des vorausgehenden r_{i-2}, soweit deren Indizes noch zwischen 0 und $n-1$ liegen. Iterieren wir dieses Argument, so muss dieser Teiler gemeinsamer Teiler aller r_i sein.
Einerseits wissen wir ebenfalls:

$$r_{n-1} \mid r_{n-2} \text{ wegen } r_n = 0,$$

so dass r_{n-1} damit tatsächlich gemeinsamer Teiler von $r_{-1} = a$ und $r_0 = b$ sein muss. Andererseits muss aber auch jeder gemeinsame Teiler von $r_{-1} = a$ und $r_0 = b$ ein Teiler von r_{n-1}, weswegen r_{n-1} beide Bedingungen an einen größten gemeinsamen Teiler erfüllt.

□

Korollar 2.7.11 *(Bézout-Identität) Sei R ein euklidischer Ring und seien $a, b \in R$ mit $b \neq 0$. Sei ferner $d \in R$ ein größter gemeinsamer Teiler von a und b. Dann gilt*

$$\langle a, b \rangle = \langle d \rangle.$$

Überlegen Sie, wie man diese Aussage mit Hilfe der Schritte des euklidischen Algorithmus beweisen könnte. Hinweis: Alle r_i, die in Algorithmus 2.7.9 auftauchen, sind Linearkombinationen von a und b.

Bemerkung 2.7.12 *Bitte beachten Sie, dass wir im allgemeinen keine Eindeutigkeit für größte gemeinsame Teiler zweier Elemente eines euklidischen Rings fordern können. Alle zu einem gegebenen größten gemeinsamen Teiler assoziierten Elemente erfüllen ebenfalls beide Bedingungen an einen größten gemeinsamen Teiler.*

In $\mathbb{Z}$ hatten wir Eindeutigkeit erzwungen durch eine Positivitätsbedingung an den ggT*. Analog können wir in $K[t]$, dem Polynomring in einer Variable über einem Körper, Eindeutigkeit des* ggT *erzwingen durch* **Normieren** *des Polynoms, d.h. indem wir fordern, dass der Leitkoeffizient* 1 *ist.*

Satz 2.7.13 *Jeder euklidische Ring ist Hauptidealring.*

Verwenden Sie die Ideen aus dem Beweis von Satz 1.2.6 und passen Sie die (wenigen) Details an, die einer Änderung bedürfen.

Analog zum größten gemeinsamen Teiler können wir auch das kleinste gemeinsame Vielfache zweier Elemente eines Integritätsrings definieren:

Definition 2.7.14 *Sei R Integritätsring und seien $a, b \in R$ mit $b \neq 0$. Dann heißt $k \in R$ ein kleinstes gemeinsames Vielfaches von a und b, falls gilt:*

a) k ist Vielfaches sowohl von a als auch von b

b) Jedes gemeinsame Vielfaches $\ell \in R$ a und b ist auch Vielfaches von k.

Satz 2.7.15 *Sei R ein Hauptidealring und seien $a, b \in R$ mit $b \neq 0$. Dann gilt:*

a) Es gibt ein kleinstes gemeinsames Vielfaches $k \in R$ von a und b, für das gilt:

$$\langle a \rangle \cap \langle b \rangle = \langle k \rangle.$$

b) Mit dem k aus a) und einem größten gemeinsamen Teiler $d \in R$ von a und b gilt:

$$\langle a \cdot b \rangle = \langle k \cdot d \rangle.$$

Beweis:

a) $J = \langle a \rangle \cap \langle b \rangle$ ist nach Lemma 2.6.10 wieder ein Ideal. Da R ein Hauptidealring ist kann dieses von einem Element $k \in R$ erzeugt werden. Die Elemente von J sind jedoch genau die gemeinsamen Vielfachen von a und b, so dass k ein gemeinsames Vielfaches von a und b sein muss. Da k sogar Erzeuger von J ist, ist jedes andere gemeinsame Vielfache von a und b darüberhinaus auch Vielfaches von k. Damit ist k ein kleinstes gemeinsames Vielfaches von a und b.

b) Dies istÜbungsaufgabe. Denken Sie an HA3.2b.

□

Kapitel 3

Teilbarkeit

Nachdem der vorige Abschnitt bereits die Teilbarkeitstheorie aus Kapitel 1 erfolgreich verallgemeinern konnte, wenden wir uns nun dem Ziel einer Verallgemeinerung einer Primfaktorzerlegung zu. Dazu werden wir zuerst den Begriff einer Primzahl geeignet verallgemeinern, ehe wir dann auch eine Zerlegung in Primelemente bzw. irreduzible Elemente suchen.

3.1 Primelemente und irreduzible Elemente

In den ganzen Zahlen konnten wir eine Primzahl wahlweise dadurch charakterisieren, dass sie keine echten Teiler hat, oder dadurch, dass sie stets auch einen der Faktoren teilen muss, wenn sie ein Produkt teilt. In allgemeineren Ringen sind dies zwei verschiedene Eigenschaften, die zwar verwandt, aber nicht identisch sind.

Definition 3.1.1 *Sei R ein Integritätsring.*

a) Seien $a, b \in R$ mit $b \mid a$. Dann heißt b ein **echter** *(oder* **nicht-trivialer***)* **Teiler** *von a, falls*

- $b \notin R^*$
- $b \neq 0$
- $b \not\sim a$

Ist $b \neq 0$, aber kein nicht-trivialer Teiler, so heißt er **trivialer** *Teiler von a.*

b) Ein Element $c \in R \setminus (\{0\} \cup R^*)$ *heißt* **irreduzibel**, *wenn es keine nicht-trivialen Teiler besitzt, d.h.*

$$\forall a, b \in R \text{ mit } c = a \cdot b : (a \in R^* \text{ oder } b \in R^*)$$

c) Ein Element $p \in R \setminus (R^* \cup \{0\})$ *heißt* **prim** *(oder* **Primelement***), wenn*

$$\forall a, b \in R \text{ mit } p \mid a \cdot b : (p \mid a \text{ oder } p \mid b).$$

Bemerkung 3.1.2 *Ein Körper besitzt außer der* 0 *nur Einheiten, weswegen er weder Primelemente noch irreduzible Elemente enthalten kann.*

Satz 3.1.3 *Jedes Primelement eines Integritätsrings ist irreduzibel.*

Beweis: Sei $p \in R$ ein Primelement und sei $a \in R$ ein echter Teiler von p mit

$$p = a \cdot b$$

für ein geeignetes $b \in R$. Da p prim ist, muss damit p einen der Faktoren teilen. Teilt dabei p seinen Teiler a, so sind p und a zueinander assoziiert und a kein *echter* Teiler von p. Teilt p andererseits seinen Teiler a nicht, so gilt $p \mid b$, d.h. es gibt ein $c \in R$ mit $b = c \cdot p$ und

$$p = a \cdot c \cdot p,$$

weswegen dann a eine Einheit sein muss. Damit kann p keine nicht-trivialen Teiler besitzen und ist damit irreduzibel.

□

Von dem obigen Satz und der Intuition aus $\mathbb{Z}$ darf man sich aber nicht verleiten lassen, die Eigenschaften prim und irreduzibel gleichzusetzen, wie das folgende Beispiel zeigt:

Beispiel 3.1.4 *Betrachte* $R = \mathbb{Z}[i\sqrt{5}]$ *und darin*

$$3 \cdot 7 = (1 + 2i\sqrt{5})(1 - 2i\sqrt{5}).$$

Dann ist z.B. 3 *irreduzibel, aber nicht prim, wie Sie in einer Übungsaufgabe auf Blatt 4 nachrechnen werden.*

Lemma 3.1.5 *Sei R ein Hauptidealring, seien $a, b \in R$, so dass a irreduzibel und kein Teiler von b ist. Dann sind a und b teilerfremd.*

Beweis: Zu zeigen ist, dass

$$\langle a, b\rangle = \langle 1_R\rangle.$$

Da R Hauptidealring ist, wissen wir, dass es ein $c \in R$ gibt mit

$$\langle a, b\rangle = \langle c\rangle.$$

Damit enthält $\langle c\rangle$ insbesondere a und ist damit ein Teiler von a. Wegen der Irreduzibilität von a, kann c aber kein echter Teiler von a sein. Würde gelten $c \sim a$, so wäre b ein Vielfaches von a, was nach Voraussetzung ausgeschlossen war. Damit muss c eine Einheit sein, weswegen $\langle c\rangle = \langle 1_R\rangle$.

□

Satz 3.1.6 *Jedes irreduzible Element in einem Hauptidealring ist prim.*

Beweis: Sei R ein Hauptidealring und sei $a \in R$ irreduzibel. Seien ferner $b, c \in R$, so dass $a \mid bc$ und $a \nmid b$. Dann gilt nach dem vorstehenden Lemma, dass es $x, y \in R$ gibt mit $xa + yb = 1_R$ und damit folgt $xac + ybc = c \in \langle a, bc\rangle = \langle a\rangle$. Daher muss a Teiler von c sein. Somit ist a Primelement in R.

□

Der vorige Satz läßt sich auch formulieren als: In einem Hauptidealring stimmen die Begriffe *prim* und *irreduzibel* überein.

3.2 Faktorielle Ringe

Schon in der Schule wurden ganze Zahlen in Primfaktoren zerlegt. Der Fundamentalsatz der Arithmetik in Kapitel 1.2 lieferte dann die theoretische Basis dafür nach, nämlich die Existenz und die Eindeutigkeit einer Zerlegung (bis auf Reihenfolge) für ganze Zahlen ≥ 2. Damit existiert natürlich für jede ganze Zahl, die weder Null noch Einheit ist, eine solche Zerlegung in irreduzible Faktoren, die bis auf Reihenfolge und Vorzeichen der Faktoren eindeutig ist. Geht so etwas auch in anderen Ringen? Die Antwort darauf ist ja, wenn der Ring hinreichend gute Eigenschaften hat, die wir in diesem Abschnitt untersuchen werden.

Beginnen wir zuerst mit einer Aussage über eine Zerlegung in Primfaktoren:

Satz 3.2.1 *Sei R ein Integritätsring und sei $a \in R \setminus (\{0\} \cup R^*)$, so dass eine Zerlegung*

$$a = \prod_{i=1}^{r} p_i$$

für ein geeignetes $r \in \mathbb{N}$ und geeignete Primelemente $p_1, \ldots, p_r \in R$ existiert. Dann ist diese eindeutig bis auf Reihefolge der Faktoren und Multiplikation der Faktoren mit Einheiten.

Für a hatten wir einige Ringelemente im Satz nicht zugelassen. Deshalb sollten wir kurz innehalten und überlegen, ob uns das später Probleme machen kann. Dass wir hier die Null nicht zulassen, strt nicht, da diese bzgl. der Multiplikation ohnehin besondere Eigenschaften hat. Für Einheiten kann man eine Zerlegung niederschreiben, indem man die Einheit selbst mit dem leeren Produkt multipliziert. Somit deckt der obige Satz alle relevanten Fälle ab.

Bemerkung 3.2.2 *Die Aussage des Satzes läßt sich wie folgt konkretisieren: Sind*

$$\prod_{i=1}^{r} p_i = a = \prod_{i=1}^{s} q_i$$

zwei solche Zerlegungen, so gilt

- $r = s$

- *Es gibt eine Permutation* $\pi : \{1, \ldots, r\} \longrightarrow \{1, \ldots, r\}$*, so dass*

$$p_i \sim q_{\pi(i)} \quad \forall 1 \leq i \leq r$$

Das Vorgehen zum Beweis von 3.2.1 ist exakt analog zu dem in Kapitel 1 im Beweis von 1.2.12. Da wir aber in wesentlich allgemeinerem Kontext sind, führen wir es hier nochmals explizit aus.
Beweis: (3.2.1) Seien also

$$\prod_{i=1}^{r} p_i = a = \prod_{i=1}^{s} q_i$$

zwei Zerlegungen von a in Primfaktoren. Wir werden durch Induktion nach r die beiden in der vorigen Bemerkung genannten Eigenschaften zeigen.
Induktionsanfang: $r = 1$
In diesem Fall ist a selbst Primelement und muss daher einen der Faktoren $q_1, \ldots, q_s$ teilen, sagen wir o.B.d.A. q_s. Da a als Primelement in einem Integritätsring auch irreduzibel ist, sind alle anderen Faktoren $q_1, \ldots, q_{s-1}$ Einheiten und die Behauptung ist erfüllt.
Induktionsvoraussetzung: r
Die beiden Bedingungen aus der vorigen Bemerkung sind für Zerlegungen, bei denen mindestens eines der Produkte höchstens r Faktoren enthält.
Induktionsschritt: $r \longrightarrow r + 1$
Betrachte

$$\prod_{i=1}^{r+1} p_i = a = \prod_{i=1}^{s+1} q_i$$

Da p_{r+1} prim ist, teilt es einen der Faktoren $q_1, \ldots, q_{s+1}$, sagen wir (ggf. nach Permutation der Indizes) q_{s+1}. Da q_{s+1} selbst ebenfalls irreduzibel ist, muss gelten:

$$p_{r+1} \sim q_{s+1}.$$

Die Primfaktorzerlegungen von $\frac{a}{p_{r+1}}$ sind dann:

$$\prod_{i=1}^{r} p_i = \frac{a}{p_{r+1}} = \underbrace{\frac{q_{s+1}}{p_{r+1}}}_{\in R^*} \cdot \prod_{i=1}^{s} q_i.$$

Dies ist aber eine Primfaktorzerlegung mit r Faktoren, so dass die Induktionsvoraussetzung anwendbar ist und daher $r = s$ sowie die Eindeutigkeit der

Faktoren bis auf Reihenfolge und Assoziiertheit von Primelemente für diese erfüllt ist. Da diese Bedingungen auch für den auf beiden Seiten letzten verbleibenden Faktor der ursprünglichen Zerlegungen erfüllt waren, gilt damit auch $r+1 = s+1$ sowie die gesuchte Eindeutigkeitsaussage für die Faktoren.[1]

□

Damit wissen wir, dass die Zerlegung in Integritätsringen eindeutig ist, sofern sie existiert. Allerdings wissen wir noch nicht, ob bzw. unter welchen Bedingungen solch eine Zerlegung exisitert. Für die Beantwortung dieser Frage definieren wir zuerst einen Begriff, der die gewünschten Eigenschaften genau charakterisiert: faktorielle Ringe. In diesen gilt bereits nach Definition der verallgemeinerte Fundamentalsatz der Arithmetik.

Definition 3.2.3 *Sei R ein Integritätsring. R heißt* **faktorieller Ring** *(oder* **ZPE-Ring**[2] *oder englisch* **UFD**[3]*), falls*

$$\forall a \in R \setminus (\{0\} \cup R^*) \;\; \exists r \in \mathbb{N} \;\; \exists c_1, \ldots, c_r \in R \text{ prim:} \quad a = \prod_{i=1}^{r} c_i$$

Satz 3.2.4 *In einem faktoriellen Ring ist jedes irreduzible Element prim.*

Beweis: Sei R ein faktorieller Ring und sei $a \in R \setminus (\{0\} \cup R^*)$ irreduzibel. Dann besitzt a eine Zerlegung in ein Produkt aus Primelementen, das aber wegen der Irreduzibilität von a aus genau einem Faktor besteht. Damit ist a selbst prim.

□

Satz 3.2.5 *Sei R ein Integritätsring. Dann sind äquivalent:*

a) R ist faktoriell

b) In R gilt:

[1] Beachten Sie, dass wir nur für eine der beiden Zerlegungen, diejenige mit den p_i tatsächlich die Eigenschaft, prim zu sein, verwendet haben. Für die andere Seite reichte uns Irreduzibilität aus.

[2] **Z**erlegung in **P**rim-**E**lemente

[3] **U**nique **F**actorization **D**omain

(i) $\forall a \in R \setminus (\{0\} \cup R^*)\ \ \exists r \in \mathbb{N}\ \ \exists c_1, \ldots, c_r \in R$ *irreduzibel:* $a = \prod_{i=1}^{r} c_i$

(ii) Diese Zerlegung ist eindeutig bis auf Reihenfolge und Assoziiertheit.

c) In R gilt:

(i) $\forall a \in R \setminus (\{0\} \cup R^*)\ \ \exists r \in \mathbb{N}\ \ \exists c_1, \ldots, c_r \in R$ *irreduzibel:* $a = \prod_{i=1}^{r} c_i$

(ii) Jedes irreduzible Element von R ist prim.

Beweis: Wir zeigen: a) $\Longrightarrow$ b) $\Longrightarrow$ c) $\Longrightarrow$ a)

"a) $\Longrightarrow$ b)": Da jedes Primelement in R auch irreduzibel ist, erfüllt eine Zerlegung aus a) auch die Bedingung b)(i). Sie ist darüberhinaus eindeutig, da für eine Zerlegung in Primelemente und eine weitere irreduzible Zerlegung die Eindeutigkeit der Zerlegung aus Satz 3.2.1 mit Hilfe der dortigen Funote zum Beweis folgt, womit auch b)(ii) erfüllt ist.

"b) $\Longrightarrow$ c)":
Die Eigenschaften b)(i) und c)(i) sind wörtlich identisch. So bleibt zu zeigen, dass unter Voraussetzung der Eigenschaft b) auch jedes irreduzible Element von R prim ist. Sei also $u \in R$ irreduzibel und seien $a, b \in R$, so dass $u \mid ab$. Dann existiert ein $c \in R$, so dass $uc = ab$. Wir zerlegen nun a,b und c jedes für sich in irreduzible Faktoren mittels b) und bilden dann die entsprechenden Produkte als Zerlegung von $uc = ab$. Dann taucht u (bis auf Assoziiertheit) wegen der Eindeutigkeit der Zerlegung unter den irreduziblen Faktoren von ab auf. Diese setzen sich aber gerade aus den irreduziblen Faktoren von a und b zusammen. Damit ist u ein Faktor von a oder von b. Also ist u prim.

" c) $\Longrightarrow$ a)"
Da jedes irreduzible Element prim ist, ist auch jede Zerlegung in irreduzible Elemente eine Zerlegung in Primelemente.

□

Damit haben wir präzisiert, woran wir interessiert sind, aber noch haben wir keine Fortschritte dahingehend gemacht, dass uns bekannte Ringe diese Eigenschaft auch haben. Das ist unser nächstes Ziel: Die Faktorialität

von Hauptidealringen. Auf dem Weg dahin begegnen wir noch einer weiteren Eigenschaft: der Teilerkettenbedingung. Zusammen mit der für Hauptidealringe bereits gezeigten Eigenschaft, dass jedes irreduzible Element auch prim ist, wird die Teilerkettenbedingung eine weitere Charakterisierung der Faktorialität liefern.

Definition 3.2.6 *Sei R ein Integritätsring. Da genügt R der* **Teilerkettenbedingung**, *falls jede Folge $(a_n)_{n\in\mathbb{N}_0}$ mit $a_{n+1} \mid a_n$* **stationär** *wird, d.h.*

$$\exists n_0 \in \mathbb{N} : a_n \sim a_{n_0} \forall n \geq n_0$$

Teilbarkeit kann natürlich auch durch Enthaltensein von Idealen ausgedrückt werden, so dass man eine äquivalente Formulierung erhält:

Bemerkung 3.2.7 *Ein Integritätsring R erfüllt die Teilerkettenbedingung, falls für jede aufsteigende Kette*

$$\langle a_0\rangle \subseteq \langle a_1\rangle \subseteq \cdots \subseteq \langle a_n\rangle \subseteq \langle a_{n+1}\rangle \subseteq \ldots$$

von Hauptidealen in R ein $n_0 \in \mathbb{N}_0$ existiert mit

$$\langle a_n\rangle = \langle a_{n_0}\rangle \forall n \geq n_0.$$

Lemma 3.2.8 *Jeder Hauptidalring R erfüllt die Teilerkettenbedingung.*

Beweis: Sei $(\langle a_n\rangle)_{n\in\mathbb{N}_0}$ eine aufsteigende Folge von Hauptidealen in einem Hauptidealring R. Betrachte nun die Menge

$$I = \bigcup_{n=0}^{\infty} \langle a_n\rangle.$$

Offensichtlich ist $0 \in I$. Sind $a, b \in I$, so gibt es $n_1, n_2 \in \mathbb{N}_0$ mit $a \in \langle a_{n_1}\rangle$ und $b \in \langle a_{n_2}\rangle$. Damit gilt wegen der Inklusionen in der aufsteigenden Kette $a, b \in \langle a_{\max\{n_1,n_2\}}\rangle$, weswegen auch jede R-Linearkombination von a und b in $\langle a_{\max\{n_1,n_2\}} \subseteq I$ liegt. Daher ist I ein Ideal in R.
Da R ein Hauptidealring ist, gibt es ein $d \in R$ mit $I = \langle d\rangle$. Für dieses d gibt es nach Konstruktion von I ein $n_3 \in \mathbb{N}_0$, so dass $d \in \langle a_{n_3}\rangle$. Damit gilt

$$I = \langle d\rangle \subseteq \langle a_{n_3}\rangle \subseteq \bigcup_{n=0}^{\infty} \langle a_n\rangle = I.$$

Daher ist $I = \langle a_{n_3}\rangle$ und die aufsteigende Kette wird stationär.

□

Satz 3.2.9 *Ein Integritätsring, der die Teilerkettenbedingung erfüllt und in dem jedes irreduzible Elemente prim ist, ist faktoriell.*

Beweis: Sei M die Menge aller Elemente, die keine Zerlegung als Produkt endlich vieler Primelemente zulassen. Wir werden durch Widerspruchsbeweis zeigen, dass M leer ist. Nehmen wir dazu an, dass $M \neq \emptyset$. Dann existiert ein $a \in M$, das selbst nicht prim sein kann, da es sonst seine eigene Zerlegung wäre und damit $a \notin M$. Da in R nicht prim auch nicht irreduzibel impliziert, besitzt a also eine Zerlegung in $a = r \cdot s$ mit $r, s \in R \setminus (\{0\} \cup R^*)$. Mindestens eines der beiden Elemente r und s, sagen wir r, muss wieder in M liegen, da sonst auch a nicht in M läge. Daher ist $\langle a \rangle \subsetneq \langle r \rangle$.
Durch Iteration dieses Arguments erhalten wir eine strikt aufsteigende Kette von von Hauptidealen in R, was im Widerspruch zur Erfüllung der Teilerkettenbedingung in R steht. Somit war die Annahme $M \neq \emptyset$ falsch und wir haben bewiesen, dass R faktoriell ist.

□

Bemerkung 3.2.10 *Wir hatten bereits gesehen, dass in einem faktoriellen Ring die Begriffe irreduzible und prim sich gegenseitig implizieren. Weiterhin muss in jedem faktoriellen Ring auch die Teilerkettenbedingung gelten, da in solch einer Kette a_0 nur endlich viele bis auf Reihenfolge und Assoziiertheit eindeutig bestimmte prime Faktoren besitzt und damit in der aufsteigenden Kette von Idealen nur endlich viele Inklusionen strikt sein können. Somit stellen die beiden Bedingungen des vorigen Satzes noch eine weitere Charakterisierung von faktoriellen Ringen dar.*

Korollar 3.2.11 *Jeder Hauptidealring ist faktoriell.*

Beweis: Jedes irreduzible Elemente in einem Hauptidealring ist nach 3.1.6 prim. Nach Lemma 3.2.8 genügt jeder Hauptidealring der Teilerkettenbedingung. Damit ist jeder Hauptidealring nach Satz 3.2.9 ein faktorieller Ring.

□

Bemerkung 3.2.12 *Nicht jeder faktorielle Ring ist Hauptidealring. So ist etwa jeder Polynomring über einem faktoriellen Ring wieder faktoriell, wie*

wir nach Aufbau weiterer theoretischer Grundlagen in Kapitel 5 werden beweisen können.
Als Beispiele für faktorielle Ringe, die keine Hauptidealringe sind, können hier $K[x_1, \ldots, x_n]$ und $\mathbb{Z}[x]$ genannt werden, die wir bereits kennengelernt haben.

Ringe, Ringe, Ringe – wo ist der Überblick?

In dieser Vorlesung gingen wir bisher von den ganzen Zahlen und ihren Eigenschaften aus und fragten uns, welche Eigenschaften auch in anderen Objekten gelten und wie verschiedene dieser Eigenschaften zusammenhängen oder einander bedingen. Das führte uns zu einer Vielzahl von Eigenschaften nicht nur von Elementen, sondern auch von Ringen. Beim Nacharbeiten wird es daher leicht etwas verwirrend durch die vielen Begrifflichkeiten.

Informell gesprochen, war das Vorgehen bei vielen Eigenschaften so, dass wir eine Eigenschaft, die wir einmal bei $\mathbb{Z}$ gesehen hatten, herausgegriffen haben. Dann haben wir die Eigenschaft formalisiert durch Formulieren unter möglichst schwachen Voraussetzungen an den zugrundeliegenden Ring und schließlich die Menge aller Ringe mit dieser Eigenschaft benannt. Zusätzlich haben wir dann noch weitere Beispiele in dieser Menge zumindest angesprochen, um zu zeigen, dass die Eigenschaft tatsächlich für mehr Ringe als nur für die ganzen Zahlen erfüllt ist.

Wichtig für das Nacharbeiten der Inhalte ist es, eine Struktur in diese Begriffe hineinzubekommen. In diesem Sinne soll dieser Abschnitt Ihnen eine Hilfestellung bieten, wie Sie dabei vorgehen können, und Ihnen auch wichtige Beispiele an die Hand geben. Dabei führen wir diese Gedanken in der ersten Inklusionskette ausführlicher aus, während Ihnen Details in den weiteren Inhalten selbst überlassen werden.
Hier nun eine Übersicht über wichtige bisher behandelte Strukturen:

$$\text{Ringe} \supsetneq \text{Ringe mit 1} \supsetneq \text{Schiefkörper} \supsetneq \text{Körper}$$

Wir erinnern uns:
Ringe tragen die Struktur einer additiven Gruppe und einer multiplikativen Halbgruppe und genügen den distributiven Gesetzen. Ringe mit 1 besitzen zusätzlich ein neutrales Elemente bzgl. der Multiplikation, sind also multiplikative Monoide. Jeder Ring mit 1 ist auch ein Ring (durch vergessen der Bedingung der Existenz der 1), aber nicht jeder Ring ist ein Ring mit 1, so ist z.B. $2\mathbb{Z} = \{2a \mid a \in \mathbb{Z}\}$ ein (kommutativer) Ring, aber kein Ring mit 1. Ein nicht kommutatives Beispiel für einen Ring ohne 1 ist die Menge der rechten oberen Dreiecksmatrizen mit Diagonale Null in $Mat(3; K)$.
Existiert in einem Ring mit 1 zu jedem nicht-null Element ein multiplikatives Invererses, so ist dieser Ring ein Schiefkörper. Natürlich ist jeder Schiefkörper auch ein Ring mit 1, aber nicht umgekehrt. Beispiele für Ringe mit 1, die

keine Schiefkörper sind, sind z.B. der kommutative Ring mit 1 $\mathbb{Z}$ sowie der nicht-kommutative Ring mit 1 $Mat(2, K)$.
Gilt in einem Schiefkörper auch noch das Kommutativgesetz der Multiplikation, so handelt es sich um einen Körper. Natürlich ist jeder Körper damit Schiefkörper, aber nicht umgekehrt. Die Hamiltonschen Quaternionen aus der Übungsaufgabe 2.6 sind ein Beispiel eines Schiefkörpers, der kein Körper ist.

Ähnlich können wir auch weitere Inklusionsketten betrachten. Schauen wir uns z.B. folgende Inklusionskette an:

$$\text{Ringe} \supsetneq \text{kommutative Ringe} \supsetneq \text{komm. Ringe mit 1} \supsetneq \text{Körper}$$

Ein Beispiel eines nicht-kommutativen Ringes ohne 1 sind die oben schon genannten Dreiecksmatrizen mit Diagonale Null. Ein Beispiel eines kommutativen Rings ohne 1 ist $2\mathbb{Z}$. Ein Ring mit 1, der kein Körper ist, ist $\mathbb{Z}$.
Werfen wir nun einen genaueren Blick auf die Strukturen, die wir am Ende von Kapitel 2 und in diesem Kapitel kennengelernt haben:

$$\begin{aligned} \text{euklid. Ringe} &\subsetneq \text{Hauptidealringe} \subsetneq \text{faktorielle Ringe} \\ &\subsetneq \text{Integritätsringe} \subsetneq \text{komm. Ringe mit 1} \end{aligned}$$

Auch hier werfen wir einen Blick auf die abgrenzenden Beispiele: Leider sind Beispiele für Hauptidealringe, die nicht euklidisch sind, relativ aufwendig, so dass wir hier kein explizites Beispiel angeben. Beispiele faktorieller Ringe, die keine Hauptidealringe sind, sind $\mathbb{Z}[t]$ und $K[x_1, \ldots, x_n]$. Ein Beispiel eines Integritätsrings, der kein faktorieller Ring ist, ist $\mathbb{Z}[i\sqrt{5}]$, den wir bereits in einer Übungsaufgabe betrachtet haben. Ein anderes Beispiel eines Integritätsringes, der nicht faktoriell ist, ist $\mathbb{Q}[x, y]/\langle x^2 - y^3\rangle$, wo x^2 die Faktorisierungen $x \cdot x$ und $y^2 \cdot y$ besitzt. Solche Ringe werden wir in Kapitel 4 genauer kennenlernen; die Irreduzibilität von $x^2 - y^3$ werden wir nach Behandlung von Kapitel 5 formal nachweisen können, im Moment ahnt man aber auch schon, dass y^3 in $\mathbb{Q}[x, y]$ keine Quadratwurzel besitzen kann. Ein Beispiel eines kommutativen Rings mit 1, der nicht nullteilerfrei ist, ist $\mathbb{Z}/\langle 6\rangle$.

Kapitel 4

Äquivalenzrelationen und Faktorstrukturen

Nachdem wir in Kapitel 3 viele Strukturen aus dem ersten Kapitel wieder aufgegriffen und dabei verallgemeinert und formalisiert haben, ist es nun höchste Zeit, eine andere Bringschuld bei Ihnen abzutragen: Auch wenn $\mathbb{Z}_m \cong \mathbb{Z}/m\mathbb{Z}$ bzw. $K[t]_{\leq n} \cong K[t]/\langle h \rangle$ bereits aufgetaucht sind und sie einem Teil von Ihnen auch bereits als Restklassen bekannt sind, werden wir sie hier nochmals von Grund auf einführen. Dabei beginnen wir mit der Frage, was es eigentlich formal bedeuten soll, wenn wir zwei Elemente als äquivalent (bzgl. einer gewissen Eigenschaft) betrachten wollen. Das führt auf den Begriff einer Äquivalenzrelation. Im Kontext von Gruppen und Ringen untersuchen wir dann, darauf basierende Konstruktionen und können dann verschiedene Beispiele, die uns bereits begegnet sind, endlich einordnen.

Die zweite Hälfte des Kapitels ist dann grundlegenden theoretischen Resultaten gewidmet, die sich erst mit Hilfe von Restklassenstrukturen formulieren und beweisen lassen. Insbesondere gewinnen wir eine neue Perspektive auf Bilder von Homomorphismen und auf das Rechnen in $\mathbb{Z}_m$ und lernen darüberhinaus Konstruktionen neuer Körper kennen.

4.1 Äquivalenzrelationen

Vor der Definition einer Äquivalenzrelation sollten wir uns kurz an die Definition einer Relation erinnern:

Definition 4.1.1 *Sei X eine Menge. Eine* **Relation** *auf X ist eine Teilmenge $\rho \subseteq X \times X$, d.h. ein geordnetes Paar von zwei Elementen aus X. Für ein Paar $(x, y) \in \rho$ sagt man "x steht in Relation zu y", kurz $x \sim_\rho y$ oder $x \sim y$.*

Diese Definition ist sehr abstrakt und insbesondere die Schreibweise als Teilmenge der Menge aller Paare ist nicht ganz intuitiv. Daher auch die alternative Schreibeweise mit $x \sim y$ für "x steht in Relation zu y". Beide Arten der Schreibweise bestehen nebeneinander, ich nutze meist die letztere.

Beispiel 4.1.2 *Betrachten wir die Menge $\mathbb{Z}$, so sind die folgenden Beziehungen Relationen:*

a) x steht in Relation zu y, falls $x > y$.

b) x steht in Relation zu y, falls $x \geq y$.

c) x steht in Relation zu y, falls $x \mid y$.

d) x steht in Relation zu y, falls $x \mid y$ und $y \mid x$, d.h. falls x zu y assoziiert ist.

e) Sei $n \in \mathbb{N}$ fest. x steht in Relation zu y, falls $n \mid x - y$.

Definition 4.1.3 *Sei X eine Menge und ρ eine Relation auf X. ρ heißt*

a) **reflexiv**, *falls $x \sim_\rho x \;\; \forall x \in X$*

b) **symmetrisch**, *falls $(x \sim_\rho y \iff y \sim_\rho x) \;\; \forall x, y, \in X$*

c) **transitiv**, *falls $(x \sim_\rho y$ und $y \sim_\rho z \implies x \sim_\rho z) \;\; \forall x, y, z \in X$*

Eine reflexive, symmetrische und transitive Relation heißt **Äquivalenzrelation**.

Im vorigen Beispiel 4.1.2 erfüllen nicht alle Relationen alle drei Bedingungen. Es hilft sehr beim Verständnis des Begriffs, wenn man die Beispiele und alle drei Eigenschaften einmal in Ruhe durchdenkt oder noch besser mit seinem Abgabepartner durchspricht.

Beispiel 4.1.4 *Bei den Beispielen von oben sehen wir:*

a) $x > y$ *ist transitiv, aber weder reflexiv noch symmetrisch.*

b) $x \geq y$ *ist transitiv und reflexiv, aber nicht symmetrisch.*

c) $x \mid y$ *ist ebenfalls transitiv und reflexiv, aber nicht symmetrisch.*

d) x *assoziiert zu* y *ist transitiv, reflexiv und symmetrisch, also Äquivalenzrelation.*

e) Dies ist ebenfalls eine Äquivalenzrelation, denn $x - x = 0$ *ist durch jede natürliche Zahl teilbar, was die Reflexivität liefert,* $y - x = (-1) \cdot (x - y)$*, woraus die Symmetrie direkt ablesbar ist, und* $x - z = (x - y) + (y - z)$ *ergibt die Transitivität.*

Dazu nun noch zwei weitere Beispiele, bei denen Sie sich die drei Eigenschaften beim Nacharbeiten selbst überlegen sollten, um mit den Begriffen vertrauter zu werden.

f) $x \sim_{2^m} y \quad :\Longleftrightarrow \quad \exists m \in \mathbb{Z} : x = 2^m y.$

g) Seien $A, B \in Mat(n; K)$*.* A *und* B *heißen ähnlich, falls* $\exists P \in GL(n; K)$ *:* $B = P^{-1}AP$*. Ähnlichkeit von Matrizen ist eine Äquivalenzrelation.*

Sobald man zwei Elemente für äquivalent erklären kann, stellt sich auch die Frage nach allen zu einem Element äquivalenten Elementen und darauf gibt der Begriff der Äquivalenzklasse die Antwort:

Definition 4.1.5 *Sei* X *eine nicht-leere Menge,* $x \in X$ *und* ρ *eine Äquivalenzrelation auf* X*. Dann heißt*

$$[x] := \{y \in X \mid x \sim_\rho y\}$$

die **Äquivalenzklasse** *von* x*.*

Lemma 4.1.6 *Sei* X *eine nicht-leere Menge und* ρ *eine Äquivalenzrelation auf* X*. Dann liegt jedes* $x \in X$ *in genau einer Äquivalenzklasse.*

Beweis: Wir zeigen die Behauptung in zwei Schritten:
Schritt 1: $x \sim_\rho y \implies [x] = [y]$
Sei $z \in [x]$. Dann gilt

$$z \sim_\rho x \overset{x \sim_\rho y, \text{Trans.}}{\Longrightarrow} z \sim_\rho y,$$

weswegen $z \in [y]$ und damit $[x] \subseteq [y]$. Durch Vertauschen der Rollen von x und y folgt dann die andere Inklusion, womit $[x] = [y]$.

Schritt 2: $[x] \cap [y] \neq \emptyset \Longrightarrow [x] = [y]$
Sei $z \in [x] \cap [y]$. Dann gilt $x \sim_\rho z$ und $y \sim_\rho z$, was nach Schritt 1 $[x] = [z] = [y]$ liefert.

□

Bemerkung 4.1.7 *Sei X eine nicht-leere Menge und ρ eine Äquivalenzrelation auf X. Dann kann nach dem vorigen Lemma jede Äquivalenzklasse auf X bzgl. ρ eindeutig durch die Angabe eines Elements der Klasse benannt werden. In diesem Fall sagen wir, dass x ein* **Repräsentant** *der Klasse ist. Die Menge aller Äquivalenzklassen von X bzgl. ρ bezeichnen wir mit $X/\sim_\rho$.*
Die **kanonische** *Projektion von X bzgl. ρ ist die Abbildung*

$$\begin{array}{rcl} \pi : X & \longrightarrow & X/\sim_\rho \\ x & \longmapsto & [x]. \end{array}$$

π ist aufgrund des vorigen Lemmas wohldefiniert und darüberhinaus offensichtlich surjektiv. Eine Teilmenge $\mathcal{O} \subset X$ heißt ein **Repräsentantensystem** *von $X/\sim_\rho$, falls die Einschränkung $\pi\,|_{\mathcal{O}}$: $\mathcal{O} \longrightarrow X/\sim_\rho$ bijektiv ist, d.h. falls $\mathcal{O}$ genau einen Repräsentant jeder Klasse bzgl. ρ enthält.*

Notation 4.1.8 *Zwei Menge heißen* **disjunkt**, *wenn ihr Durchschnitt leer ist. Gilt für Mengen X, Y, Z nun $Z = X \cup Y$ und $X \cap Y = \emptyset$, so schreiben wir kurz $Z = X \dot\cup Y$ und nennen Z die disjunkte Vereinigung von X und Y. Eine Zerlegung einer Menge X in eine Vereinigung disjunkter Teilmengen wie im folgenden Korollar nennt man eine* **Partition** *von X.*

Korollar 4.1.9 *Sei X eine nicht-leere Menge, ρ eine Äquivalenzrelation auf X und $\mathcal{O}$ ein Repräsentantensystem bzgl. ρ. Dann gilt*

$$X = \dot{\bigcup_{x \in \mathcal{O}}} [x]$$

Jetzt haben wir formalisiert, was wir unter äquivalent verstehen wollen. Aber noch wissen wir nicht, wozu uns das nützlich sein könnte. Schauen wir uns dazu erst einmal an, was sich an Äquivalenzrelationen direkt anbietet, wenn die zugrundeliegende Menge eine algebraische Struktur trägt.

4.2 Faktorgruppen

Definition 4.2.1 *Sei $(G,+)$ eine abelsche Gruppe und $(U,+) \leq (A,+)$ eine Untergruppe. Die* **Kongruenzrelation** *$T \subset G \times G$ modulo U ist die Relation*

$$(a,b) \in T :\Longleftrightarrow a - b \in U.$$

Für $(a,b) \in T$ schreiben wir $a \equiv b (\mathrm{mod}\, U)$.

Satz 4.2.2 *Sei $(U,+)$ eine Untergruppe einer abelschen Gruppe $(G,+)$. Sei T die Kongruenzrelation modulo U. Dann gilt:*

a) T ist Äquivalenzrelation.

b) Eine Äquivalenzklasse bzgl. T ist von der Form

$$[a] = \{x \in G \mid x \equiv a \,\mathrm{mod}\, U\} = \{x \in G \mid x - a \in U\} =: a + U.$$

c) Bezeichnet G/U die Menge der Äquivalenzklassen modulo U, so ist $(G/U,+)$ eine abelsche Gruppe mit der Gruppenoperation

$$\begin{array}{rcl} + : G/U \times G/U & \longrightarrow & G/U \\ ([a],[b]) & \longmapsto & [a+b] \end{array}$$

Beweis:

a) Für alle $x \in G$ gilt $x - x = 0_G \in U$, weswegen die Kongruzenrelation modulo U reflexiv ist. Ist für $x, y \in G$ bereits $x - y \in U$ erfüllt, so ist auch $y - x = -(x - y) \in U$ da Untergruppen abgeschlossen sind bzgl. der Inversenbildung, womit die Symmetrie der Relation erfüllt ist. Gilt für $x, y, z \in G$ bereits $x - y \in U$ und $y - z \in U$, so ist wegen der Abgeschlossenheit einer Untergruppe bzgl. der Verknüpfung auch $x - z = (x - y) + (y - z) \in U$. Damit ist auch die Transitivität erfüllt und T ist eine Äquivalenzrelation.

b) Die ist lediglich eine explizite Formulierung des Begriffs Äquivalenzklasse in dem konkreten Kontext der Kongruenz modulo U.

c) Seien $[a], [b], [c] \in G/U$ repräsentiert durch $a, b, c \in G$. Aufgrund des Assoziativgesetzes in G muss gelten:

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

was genau das Assoziativgesetz in U/G liefert. Für alle $[a] \in G/U$, repräsentiert durch $a \in G$, muss gelten:

$$[0_G] + [a] = [0_G + a] = [a],$$

womit $[0_G]$ das neutrale Element in der abelschen Gruppe G/U ist. Für alle $a \in G/U$, repräsentiert durch $a \in G$ gilt weiterhin:

$$[a] + [-a] = [a - a] = [0_G],$$

womit auch die Existenz eines Inversen zu einem gegebenen $[a] \in G/U$ bewiesen ist. Daher ist $(G/U, +)$ eine Gruppe. Diese ist abelsch, da für alle $[a], [b] \in G/U$, reprsentiert durch $a, b \in G$ gilt:

$$[a] + [b] = [a + b] = [b + a] = [b] + [a].$$

□

Beachten Sie, dass wir in diesem Abschnitt nur ablesche Gruppen betrachtet haben. Würden wir auch nicht-abelsche Gruppen G zulassen, so müssten wir deutlich mehr Sorgfalt bei der Wahl von U walten lassen. Dies heben wir uns für die Algebra II auf.

Lemma 4.2.3 *Sei $(U, +)$ eine Untergruppe einer abelschen Gruppe $(G, +)$. Dann ist*

$$\begin{array}{rcl} \varphi : G & \longrightarrow & G/U \\ a & \longmapsto & [a] \end{array}$$

ein Gruppenepimorphismus mit Kern U.

Der Beweis bleibt den Lesern überlassen. Die Wohldefiniertheit von φ folgt bereits aus 4.1.6. Da die Gruppenstruktur auf G/U von der auf G nach Konstruktion induziert ist, folgt auch die Homomorphismuseigenschaft direkt. Die Surjektivität ist ebenfalls direkt nach Konstruktion von G/U gegeben. Bleibt einzig beim Nacharbeiten $ker(\varphi) = U$ nachzurechnen.

4.3 Restklassenringe

Geben wir nun der Menge X aus 4.1 noch etwas mehr Struktur und betrachten Ringe. Dabei helfen uns die bereits für Gruppen gezeigten Eigenschaften, da jeder Ring und jedes Ideal bzgl. der additiven Verknüpfung eine abelsche Gruppe ist. Wir behalten daher auch die dafür eingeführten Schreibweisen bei.

Satz 4.3.1 *Sei R ein Ring und $I \trianglelefteq R$ ein Ideal. Dann ist $(R/I, +, \cdot)$ ein Ring mit Einselement $[1_R]$ bzgl. der Verknüpfungen:*

$$\begin{aligned} + : R/I \times R/I &\longrightarrow R/I \\ ([a],[b]) &\longmapsto [a+b] \\ \cdot : R/I \times R/I &\longrightarrow R/I \\ ([a],[b]) &\longmapsto [ab] \end{aligned}$$

Beweis: Aus Satz 4.2.2 wissen wir bereits, dass $(R/I, +)$ eine abelsche Gruppe ist. Der Beweis der Assoziativität bzgl. $\cdot$ erfolgt nach demselben Schema wie bei der Addition: Seien $[a], [b], [c] \in R/I$, repräsentiert durch $a, b, c \in R$:

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

Ebenso sehen wir direkt das Einselement. Sei dazu $[a] \in R/I$ repräsentiert durch $a \in R$:

$$[a] \cdot [1_R] = [a \cdot 1_R] = [a] = [1_R \cdot a] = [1_R] \cdot [a]$$

Für die beiden distributiven Gesetze seien nun $[a], [b], [c] \in R/I$ repräsentiert durch $a, b, c \in R$ und es gilt:

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

und

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

Im Falle der Kommutativität von R rechnen wir außerdem für $[a], [b] \in R/I$,

repräsentiert durch $a, b, \in R$:

$$[a] \cdot [b] = [a \cdot b] = [b \cdot a] = [b] \cdot [a].$$

□

Definition 4.3.2 *Sei R ein Ring und $I \trianglelefteq R$ ein Ideal. Dann heißt $(R/I, +, \cdot)$ der* **Restklassenring** *(oder* **Faktorring** *von R modulo I.*

Korollar 4.3.3 *Sei R ein Ring und $I \trianglelefteq R$ ein Ideal. Dann ist die kanonische Projektion*

$$\begin{array}{rcl} \pi : R & \longrightarrow & R/I \\ a & \longmapsto & [a] \end{array}$$

ein Ringhomomorphismus mit Kern I.

Jedes Ideal in einem Ring R mit 1 taucht also als Kern eines Ringhomomorphismus auf. Andererseits hatten wir schon in Abschnitt 2.6 gesehen, dass der Kern eines Ringhomomorphismus ein Ideal ist. Einerseits zeigt das, dass Ideale wichtige und interessante Objekte sind. Andererseits sollte hinter diesem Zusammenhang von Idealen und Kernen auch noch mehr stecken. Was genau sehen wir in Abschnitt 4.5. Vorher jedoch werden wir noch ein paar konkrete Restklassenkonstruktionen betrachten.

4.4 Äquivalenzrelationen überall

Die Konstruktion von Äquivalenzrelationen und von Faktorstrukturen kann auf den ersten Blick sehr abstrakt und etwas abgehoben erscheinen, aber wir haben solche Strukturen schon mehrmals gesehen und darin gearbeitet. Andererseits bieten sie uns die Möglichkeit bestimmte Sachverhalte recht kompakt beschreiben zu können.

Der Ring $\mathbb{Z}/m\mathbb{Z}$

In Abschnitt 2.5 waren uns zwei Ringe begegnet:
Einerseits $\mathbb{Z}_m$, dessen Elemente natürliche Zahlen $\{0, 1, \ldots, m-1\}$ sind. Dieser besitzt eine Addition und Multiplikation, die von denen auf $\mathbb{Z}$ dadurch

induziert sind, dass zuerst die Operation in $\mathbb{Z}$ ausgeführt wird und dann der Rest der Division durch m gebildet wird.
Andererseits $\mathbb{Z}/m\mathbb{Z}$, dessen Elemente Restklassen bzgl. des Ideals $\langle m\rangle$ sind. Dieser besitzt eine Addition und Multiplikation die über die Konstruktion eines Restklassenringes induziert sind.
Nachdem wir zu Beginn des Kapitels den Begriff eines Repräsentantensystems kennengelernt habe, stellen wir fest, dass die Menge $\{0, 1, \ldots, m-1\}$ gerade ein Repräsentantensystem von $\mathbb{Z}/m\mathbb{Z}$ ist. Damit haben wir eine $1:1$ Zuordnung zwischen den Elementen der beiden Ringe.
Die Operationen in beiden Ringen werden von denselben Operationen in $\mathbb{Z}$ induziert; der Unterschied besteht lediglich darin, dass wir einmal mit zwei Klassen beginnen und die der Summe oder dem Produkt entsprechende Klasse als Bild erhalten und im anderen Fall mit zwei Repräsentanten starten und als Bild einen Repräsentanten der Klasse des Bildes erhalten. Wir haben uns also gerade in etwas informeller Form überlegt:

$$\begin{array}{rcl} \varphi : (\mathbb{Z}_m, +, \cdot) & \longrightarrow & (\mathbb{Z}/m\mathbb{Z}, +, \cdot) \\ a & \longrightarrow & [a] \end{array}$$

ist ein Isomorphismus von Ringen.

Der Ring $K[t]/\langle h\rangle$

Am Ende von Abschnitt 2.7 begegnete uns eine weiter Konstruktion, die wir in zwei Varianten ausführten:
Einerseits betrachteten wir $K[t]_{\leq n}$, bei dem Addition und Multiplikation von Polynomen vom Grad höchstens n im Polynomring erfolgten und dann durch Division mit Rest bzgl. eines Polynoms h vom Grad $n+1$ wieder auf ein Polynom vom Grad kleiner oder gleich n abgebildet wurden.
Andererseits betrachteten wir $K[t]/\langle h\rangle$ mit den induzierten Operationen als Restklassenring, ohne dies explizit formuliert zu haben.
Wie im vorigen Beispiel existiert eine Isomorphie dieser beiden Ringe (zum selben Polynom h), da die Elemente von $K[t]_{\leq n}$ gerade ein (diesmal in vielen Fällen unendliches) Repräsentantensystem vom $K[t]/\langle h\rangle$ darstellen.

Faktorräume

Nicht nur in Ringen stecken abelsche Gruppen als ein wichtiger Baustein. Schon in der Linearen Algebra haben wir uns mit Vektorräumen befasst,

die bzgl. der inneren Verknüpfung + ebenfalls die Struktur einer abelschen Gruppe tragen und darüberhinaus noch eine Skalarmultiplikation besitzen. Auch auf diese läßt sich die Faktorgruppenkonstruktion anwenden.

Satz 4.4.1 *Sei K ein Körper, V ein K-Vektorraum und U ein Untervektorraum von V. Dann ist V/U ein K-Vektorraum bzgl. der Verknüpfungen*

$$\begin{array}{rcl} +: V/U \times V/U & \longrightarrow & V/U \\ ([v],[w]) & \longmapsto & [v+w] \\ \cdot : K \times V/U & \longrightarrow & V/U \\ (\lambda,[v]) & \longmapsto & [\lambda v] \end{array}$$

Wie schon zuvor bei Restklassenringen, reicht es zum Beweis der Aussage die Faktorgruppenstruktur bzgl. + zu verwenden und lediglich die Eigenschaften explizit nachzurechnen, die die Skalarmultiplikation betreffen. Dies bietet keinerlei unerwartete Schwierigkeiten oder neue Einsichten und bleibt daher dem interessierten Leser als Teil des Nacharbeitens überlassen.

Korollar 4.4.2 *Sei K ein Körper, V ein K-Vektorraum und U ein Untervektorraum von V. Dann ist die kanonische Projektion*

$$\begin{array}{rcl} \pi : V & \longrightarrow & V/U \\ v & \longmapsto & [v] \end{array}$$

ein K-Vektorraumepimorphismus mit Kern U und es gilt:

$$\dim_K(V/U) = \dim_K(V) - \dim_K(U)$$

Der Beweis der ersten Aussage über den Vektorraumepimorphismus mit Kern U folgt direkt aus der Konstruktion der Abbildung und den bereits gezeigten Eigenschaften des zugrunde liegenden Homomorphismus abelscher Gruppen. Die zweite Aussage ist dann eine direkte Folge aus dem Satz über die Dimension des Kerns und des Bildes einer linearen Abbildung sowie aus dem Wissen um den Kern von π.

Eine kompakte Schreibweise in faktoriellen Ringen

Erinnern wir uns an den Abschnitt über faktorielle Ringe und die dort verwendete Schreibweise für Zerlegung in ein Produkt aus Primelementen:

Erinnerung 4.4.3 *Sei R faktorieller Ring und sei $a \in R \setminus (\{0\} \cup R^*)$. Dann existieren ein $r \in \mathbb{N}$ und Primelemente $c_1, \ldots, c_r \in R$, so dass*

$$a = \prod_{i=1}^{r} c_i.$$

Dabei war explizit nicht ausgeschlossen, dass es Indizes $j_1 \neq j_2$ geben kann mit $cj_1 \sim c_{j_2}$.
Im Fall der Primfaktorzerlegung in den ganzen Zahlen hatten wir daher bereits in der Schule eine etwas andere Formulierung vorgezogen: Sei $a \in \mathbb{Z} \setminus \{0, 1, -1\}$. Dann gibt es ein $s \in \mathbb{N}$, paarweise verschiedene Primzahlen $p_1, \ldots, p_s$ sowie natürliche Zahlen $e_1, \ldots, e_s$, so dass

$$a = \varepsilon(a) \prod_{i=1}^{s} p_i^{e_i},$$

wobei $\varepsilon(a) = \frac{a}{|a|}$ gerade das Vorzeichen von a ist.

Da stellt sich sofort die Frage, ob wir auch in allgemeineren faktoriellen Ringen zueinander assoziierte Faktoren zusammenfassen und die Zerlegung damit eleganter formulieren können.

Erinnerung 4.4.4 *Sei R faktorieller Ring. Dann ist die Assoziiertheit von Elementen nach 4.1.4,d) eine Äquivalenzrelation. Damit können wir für die Äquivalenzklassen ein Repräsentanensystem wählen.*

Nach diesen Überlegungen läßt sich auch die Zerlegung in Primelemente in einem faktoriellen Ring kompakter darstellen:

Bemerkung 4.4.5 *Sei R faktorieller Ring, $a \in R \setminus (\{0\} \cup R^*)$ und $\mathcal{P}$ ein Repräsentantensystem bzgl. Assoziiertheit in R. Dann existieren ein $n \in \mathbb{N}$, Primelemente $p_1, \ldots, p_n \in \mathcal{P}$, $e_1, \ldots, e_n \in \mathbb{N}$ sowie ein $\varepsilon \in R^*$, so dass*

$$a = \varepsilon \prod_{i=1}^{n} p_i^{e_i}.$$

Betrachten wir nun die Exponenten in der obigen Zerlegung noch etwas genauer. Für jedes $a \in R \setminus (\{0\} \cup R^*)$ und jedes Primelement $p \in \mathcal{P}$ läßt sich ein (maximales) $e \in \mathbb{N}_0$ finden, so dass

$$p^e \mid a, \quad \text{aber } p^{e+1} \nmid a.$$

Dieses bezeichnen wir als $v_p(a) := e$. Es beschreibt genau die Vielfachheit des Faktors p in der Zerlegung von a in Primelemente. Damit kann man die Zerlegung von a in Primelemente auch schreiben als:

$$a = \varepsilon \prod_{p \in \mathcal{P} \text{ prim}} p^{v_p(a)}.$$

Direkt fällt in der neuen Schreibweise auf, dass das Produkt möglicherweise unendlich viele Faktoren zu umfassen scheint. Dies täuscht jedoch, da zu einem gegebenen a der Exponent $v_p(a)$ nur für endlich viele Primelemente $p \in \mathcal{P}$ von Null verschieden ist.

Die Wahl der Schreibweise $v_p(a)$ ist kein Zufall. Sie suggeriert bereits, dass es sich hier um Abbildungen handelt.

Definition 4.4.6 *Sei R ein faktorieller Ring und $p \in R$ ein Primelement. Dann definiert*

$$\begin{array}{rcl} v_p : R \setminus \{0\} & \longrightarrow & \mathbb{N}_0 \\ a & \longmapsto & v_p(a) \end{array}$$

mit der oben bereits verwendeten Definition von $v_p(a)$ eine Abbildung.

Die folgenden Eigenschaften sind direkte Konsequenz der Definition der Abbildung v_p:

Lemma 4.4.7 *Sei R faktorieller Ring und $p \in R$ ein Primelement. Dann gilt für alle $a, b \in R \setminus \{0\}$:*

a) $v_p(ab) = v_p(a) + v_p(b)$

b) $v_p(a + b) \geq \min\{v_p(a), v_p(b)\}$

Lemma 4.4.8 *Sei R faktorieller Ring und seien $a, b \in R \setminus \{0\}$. Es gilt:*

a) $b \mid a \iff v_p(b) \leq v_p(a)\ \forall p \in \mathcal{P}$ *prim*

b) $a \in R^* \iff v_p(a) = 0\ \forall p \in \mathcal{P}$ *prim*

Dank der Abbildung v_p läßt sich nun in faktoriellen Ringen auch ein größter gemeinsamer Teiler bzw. ein kleinstes gemeinsames Vielfaches zu zwei von Null verschiedenen Nicht-Einheiten einfach niederschreiben:

Satz 4.4.9 *Sei R faktorieller Ring, $\mathcal{P}$ ein Repräsentantensystem bzgl. der Assoziiertheit in R und seien $a, b \in R \setminus (\{0\} \cup R^*)$. Dann existieren ein größter gemeinsamer Teiler d sowie ein kleinstes gemeinsames Vielfaches k von a und b und es gilt*

$$\begin{aligned} d &= \prod_{p \in \mathcal{P} \text{ prim}} p^{\min(v_p(a), v_p(b))} \\ k &= \prod_{p \in \mathcal{P} \text{ prim}} p^{\max(v_p(a), v_p(b))}. \end{aligned}$$

Ferner gilt: $dk \sim ab$.

Der Beweis beruht auf der Eindeutigkeit der Zerlegung in Primelemente in faktoriellen Ringen (bis auf Reihenfolge und Assoziiertheit). Nach Wahl eines Repräsentantensystems, müssen die primen Faktoren lediglich geeignet eingesammelt werden. Direktes Nachprüfen der Eigenschaften *eines* größten gemeinsamen Teilers bzw. *eines* kleinsten gemeinsamen Vielfachen liefert dann die Behauptung.

4.5 Isomorphiesätze

Wir hatten bereits gesehen, dass jedes Ideal als Kern eines Ringhomomorphismus auftritt und jeder Kern eines Ringhomomorphismus ein Ideal ist. Aber der Zusammenhang zwischen Idealen, Faktorringen und Ringhomomorphismen ist noch deutlich enger, wie wir in diesem Kapitel sehen werden.

Satz 4.5.1 *(Homomorphiesatz) Sei $\varphi : R \longrightarrow S$ ein Ringhomomorphismus. Dann gilt*

$$\begin{aligned} \psi : R/\ker(\varphi) &\longrightarrow \operatorname{Im}(\varphi) \\ [a] &\longmapsto \psi([a]) := \varphi(a) \end{aligned}$$

ist ein Ringisomorphismus.

Beweis:
Schritt 1: Zeige $R/\ker(\varphi)$, $\operatorname{Im}(\varphi)$ Ringe
Aus Satz 2.6.8 wissen wir, dass $\ker(\varphi) \trianglelefteq R$ ein Ideal ist und damit $(R/\ker(\varphi), +, \cdot)$ die von den Verknüpfungen auf R induzierte Ringstruktur trägt. Nach Satz

2.3.7,a) ist $\mathrm{Im}(\varphi)$ ebenfalls ein Ring (natürlich mit $1_{\mathrm{Im}(\varphi)} = 1_S$. Damit ist es überhaupt sinnvoll, über Ringhomomorphismen von $R/\ker$ nach $\mathrm{Im}(\varphi)$ zu sprechen.

Damit wir die Eigenschaften der Zuordnung ψ überhaupt als Abbildung diskutieren können, ist nun der erste Schritt zu zeigen, dass es sich um eine wohldefinierte Abbildung handelt. Erst danach können wir beginnen, zu zeigen, dass ψ ein bijektiver Ringhomomorphismus ist.

Schritt 2: Zeige ψ wohldefiniert
Sei also $[a] \in R/\ker(\varphi)$ eine beliebige Klasse in $R/\ker(\varphi)$ und seien $a_1, a_2 \in R$ zwei Repräsentanten dieser Klasse. Da beide aus der Klasse $[a]$ bzgl. $\ker(\varphi)$ stammen, existiert ein $u \in \ker(\varphi)$, so daß $a_2 = a_1 + u$. Damit rechnen wir:

$$\varphi(a_2) = \varphi(a_1 + u) = \varphi(a_1) + \underbrace{\varphi(u)}_{=0} = \varphi(a_1).$$

Damit ist bewiesen, dass die Wahl des Repräsentanten keinen Einfluß auf $\psi([a]) = \varphi(a_1) = \varphi(a_2)$ hat.

Schritt 3: Zeige ψ Ringhomomorphismus
Seien $a, b \in R$ beliebig. Dann gilt:

$$\begin{aligned} \psi([a] + [b]) = \psi([a + b]) &= \varphi(a + b) = \varphi(a) + \varphi(b) \\ &= \psi[a] + \psi[b] \\ \psi([a] \cdot [b]) = \psi([a \cdot b]) &= \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b) \\ &= \psi[a] \cdot \psi[b]. \end{aligned}$$

Außerdem ist

$$\psi(1_{R/\ker}) = \psi([1_R]) = \varphi(1_R) = 1_S.$$

Damit ist ψ ein Ringhomomorphismus.

Schritt 4: Zeige ψ injektiv
Seien $[a], [b] \in R/\ker(\varphi)$, repräsentiert durch $a, b \in R$ und gelte $\psi[a] = \psi[b]$. Dann gilt:

$$0_{\mathrm{Im}(\varphi)} = \psi([a]) - \psi([b]) = \varphi(a) - \varphi(b) = \varphi(a - b).$$

weswegen $a - b \in \ker(\varphi)$ und damit $[a - b] = [0_R]$, d.h. $[a] = [b]$.

Schritt 5: Zeige ψ surjektiv
Sei $s \in \mathrm{Im}(\varphi)$. Dann exisitiert ein $a \in R$ mit $\varphi(a) = s$. Damit gilt $\psi([a]) = \varphi(a) = s$ und s liegt im Bild von ψ.

Damit haben wir gezeigt, dass es sich bei ψ um einen bijektiven Ringhomomorphismus handelt, also wie behauptet um einen Ringisomorphismus.

□

Satz 4.5.2 *(1. Isomorphiesatz) Sei R ein Ring, $S \leq R$ ein Unterring und $I \trianglelefteq R$ ein Ideal. Dann ist*

$$\begin{array}{rcl} \psi : S/(I \cap S) & \longrightarrow & (I + S)/I \\ [a]_{I \cap S} & \longmapsto & [a]_I \end{array}$$

ein Ringisomorphismus.

Beweis: Auch hier beginnt der Beweis damit, dass zuerst gezeigt werden muss, dass strukturell die Behauptung überhaupt sinnvoll ist. Dazu sollten die beiden Mengen eine Ringstruktur tragen.

Schritt 1: Zeige $I \cap S \trianglelefteq S$ Ideal
Da $S \leq R$ ein Unterring ist und $I \trianglelefteq R$ ein Ideal, enthalten beide 0_R, womit der Schnitt nicht leer ist. Seien nun $a, b \in (I \cap S)$ und $\lambda, \mu \in S$. Dann ist $\lambda a + \mu b \in S$, wegen der Abgeschlossenheit eines Ringes unter Addition und Multiplikation. Andererseits sind λ und $\mu \in S \leq R$ und I ist ein Ideal in R. Daher ist $\lambda a + \mu b \in I$, so dass $\lambda a + \mu b \in I \cap S$. Also ist $I \cap S$ ein Ideal, weswegen dann $S/(I \cap S)$ der Faktorring von S bzgl. $I \cap S$ ist.

Schritt 2: Zeige $I + S \leq R$ Unterring
Da bereits I und S nicht leer sind, ist $I + S$ nicht leer. Seien nun $a + r, b + s \in I + S$. Wir rechnen mittels der Verknüpfungen in R:

$$(a + r) - (b + s) = a + r - b - s = \underbrace{(a - b)}_{\in I} + \underbrace{(r - s)}_{\in S} \in I + S$$

$$(a + r) \cdot (b + s) = \underbrace{ab + as + rb}_{\in I} + \underbrace{rs}_{\in S} \in I + S$$

Damit ist $I+S$ ein Unterring von R, der wegen $0_R \in S$ auch I als $(I+S)$-Ideal enthält. Daher ist $(I+S)/I$ der Faktorring von $I+S$ bzgl. des $(I+S)$-Ideals I.

Schritt 3: Zeige ψ Ringisomorphismus
Betrachte hierzu die beiden Ringhomomorphismen

$$\begin{array}{rcl} \varphi_1: \quad S & \longrightarrow & I+S \\ s & \longmapsto & 0_R + s \text{ und} \\ \varphi_2: I+S & \longrightarrow & (I+S)/I \\ a & \longmapsto & [a]_I. \end{array}$$

Hierbei ist φ_1 ein Ringmonomorphismus und φ_2 ein Ringepimorphismus mit $\ker(\varphi_2) = I \subset I+S$. Die Verkettung

$$\varphi = \varphi_2 \circ \varphi_1 : S \longrightarrow (I+S)/I$$

ist damit ein Ringhomomorphismus. Zum Nachweis der Surjektivität von φ sei $[b] \in (I+S)/I$ beliebig, dann existiert dazu ein Repräsentant $a+s \in I+S$ mit $a \in I$, $s \in S$ und $[a+s]_I = [b]_I$. Damit ist auch $[s]_I = [b]_I$, da wegen $a \in I$ $[a+s]_I = [(a+s)-a]_I = [s]_I$. Das bedeutet, dass gilt $[b]_I = \varphi(s)$. Damit ist φ surjektiv. Der Kern von φ besteht genau aus den Elementen $s \in S$, deren Bild $\varphi_1(s)$ unter der ersten Abbildung in I liegt. Dies sind genau die Elemente von $S \cap I$. Damit ist φ ein Ringepimorphismus mit $\ker(\varphi) = I \cap S$ und die Behauptung folgt mit dem Homomorphiesatz.

□

Satz 4.5.3 *(2. Isomorphiesatz) Sei R ein Ring und $I, J \trianglelefteq R$ Ideale mit $J \subseteq I$. Bezeichnet nun I/J das Bild des Ideals I unter der kanonischen Restklassenabbildung bzgl. J, dann ist*

$$\begin{array}{rcl} \psi: (R/J)\,/\,(I/J) & \longrightarrow & R/I \\ [\,[a]_J]_{I/J} & \longmapsto & [a]_I \end{array}$$

ein Ringisomorphismus.

Auch im Beweis des zweiten Isomorphiesatzes geht es um ein sorgfältige Vorbereitung der Anwendung des Homomorphiesatzes auf eine geeignete Abbildung. Der Beweis wird Ihnen als Übungsaufgabe wieder begegnen.

Auch wenn die Isomorphiesätze im Moment noch sehr technisch aussehen und etwas Zeit zum Verdauen der Beweise notwendig ist, so sind diese doch ganz zentrale Aussagen der Algebra. Sie verbinden Aussagen über Faktorringe mit Aussagen über Bilder von Ringhomomorphismen. In der Praxis ist es bisweilen wesentlich einfacher, einen Kern eines Homomorphismus auszurechnen als das Bild; aber dank des Homomorphiesatzes kennt man dann auch das Bild bis auf Isomorphie. Der erste Isomorphiesatz erleichtert das Arbeiten in Unterringen und deren Faktorringen oft wesentlich, während der zweite Isomorphiesatz den problemlosen Umgang mit Faktorringen von Faktorringen erlaubt.

4.6 Primideale und maximale Ideale

Im vorigen Kapitel hatten wir uns mit Primelementen und irreduziblen Elementen eines Ringes beschäftigt und dabei den Blick vor allem auf Hauptideale gelegt. Für die wichtige Klasse der Euklidischen Ringe und allgemeiner für Hauptidealringe konnten wir nach diesen Überlegungen dann auch Faktorialität zeigen. Entscheidend dabei war die Teilerkettenbedingung für *Hauptideale* sowie die Äquivalenz von *prim* und *irreduzibel* in Hauptidealringen.

Danach hatten wir explizite Restklassenkonstruktionen ($\mathbb{Z}/m\mathbb{Z}$, $K[t]/\langle h\rangle$) kennengelernt, bei denen die Äquivalenzrelation durch Hauptideale gegeben ist, und waren schließlich zu den Isomorphiesätzen gekommen, die Bilder von Abbildungen und Faktorringe verbinden. Allerdings ist bei weitem nicht jeder Ring ein Hauptidealring und daher können wir nicht erwarten, dass Kerne von Ringhomomorphismen sich immer als Hauptideale erweisen werden. Jenseits der Hauptideale würden wir uns daher eine Verallgemeinerung der Begriffe *prim* und *irreduzibel* wünschen, um Aussagen über Eigenschaften von Ringen der Form R/I treffen zu können.

Definition 4.6.1 *Sei R ein kommutativer Ring*[1]*. Ein echtes Ideal $\mathfrak{m} \trianglelefteq R$ heißt* **maximales Ideal**, *falls*

$$\forall I \trianglelefteq R \text{ mit } \mathfrak{m} \subseteq I \subseteq R: \quad (I = \mathfrak{m} \text{ oder } I = R).$$

Ein maximales Ideal ist als ein echtes Ideal, das maximal ist unter der Inklusion von Idealen.

[1] wie immer mit 1.

Lemma 4.6.2 *Sei R ein Hauptidealring und sei $c \in R \setminus (\{0\} \cup R^*)$. c ist irreduzibel genau dann, wenn $\langle c \rangle$ maximal ist.*

Beweis: "$\Longrightarrow$" Sei $I \trianglelefteq R$ ein Ideal mit $\langle c \rangle \subseteq I \subseteq R$. Da R ein Hauptidealring ist, existiert ein $d \in R$ mit $I = \langle d \rangle$. Wegen $\langle c \rangle \subseteq \langle d \rangle$ gilt aber $d \mid c$. Aus der Irreduzibilität von c folgt dann, dass $d \sim c$ oder $d \in R^*$. Im ersteren Fall ist $\langle d \rangle = \langle c \rangle$, im letzteren ist $\langle d \rangle = R$, womit die Maximalität von $\langle c \rangle$ gezeigt ist.
"$\Longleftarrow$" Sei umgekehrt $\langle c \rangle$ maximales Ideal in R und sei $d \in R$ ein Teiler von c. Dann gilt $\langle c \rangle \subseteq \langle d \rangle \subseteq R$, weswegen nach Maximalität gilt $\langle c \rangle = \langle d \rangle$, d.h. $c \sim d$, oder $\langle d \rangle = R$, d.h. $d \in R^*$. Damit ist die Irreduzibilität von c beweisen.

□

Bemerkung 4.6.3 *Schwächen wir die Bedingung 'Hauptidealring' ab zu 'Integritätsring', so läßt sich noch immer eine etwas schwächere Aussage treffen: $c \in R$ ist irreduzibel genau dann, wenn $\langle c \rangle$ maximal unter Inklusion von Hauptidealen ist. Das Vorgehen des Beweises bleibt dasselbe, die leichte Abschwächung der Aussage trägt lediglich solchen Situationen Rechnung, in denen $c \in R$ irreduzibel ist, es aber ein $d \in R$ gibt mit $\langle c \rangle \subsetneq \langle c, d \rangle \subsetneq R$.*

Definition 4.6.4 *Sei R ein kommutativer Ring. Ein echtes Ideal $\mathfrak{p} \trianglelefteq R$ heißt ein Primideal in R, falls*

$$\forall a, b \in R : (a \cdot b \in \mathfrak{p} \Longrightarrow (a \in \mathfrak{p} \text{ oder } b \in \mathfrak{p})).$$

Lemma 4.6.5 *Sei R ein Integritätsring und sei $p \in R \setminus (\{0\} \cup R^*)$. p ist prim genau dann, wenn $\langle p \rangle$ ein Primideal ist.*

Der Beweis dieses Lemmas folgt durch direkte Verwendung der Definitionen Primelement und Primideal – völlig analog dazu, wie wir es im vorigen Lemma mit den Definitionen irreduzibel und maximal gesehen haben. Der Beweis bleibt damit als Übungsaufgabe.

Korollar 4.6.6 *(zu den Definitionen) In einem kommutativen Ring ist jedes maximale Ideal prim.*

Beweis: Sei $\mathfrak{m} \trianglelefteq R$ ein maximales Ideal in einem kommutativen Ring R und seien $a, b \in R$ mit $a \cdot b \in \mathfrak{m}$. Betrachte das Ideal $\mathfrak{m} + \langle b \rangle$. Für dieses gilt

$$\mathfrak{m} \subseteq \mathfrak{m} + \langle b \rangle \subseteq R$$

und daher sind wegen der Maximalität von $\mathfrak{m}$ nur $\mathfrak{m} = \mathfrak{m} + \langle b \rangle$, d.h. $b \in \mathfrak{m}$, oder $\mathfrak{m} + \langle b \rangle = R$, d.h. $[b]_\mathfrak{m} \in (R/\mathfrak{m})^*$, möglich. Im letzteren Fall existiert aber eine Inverse $[c]_\mathfrak{m}$ zu $[b]_\mathfrak{m}$, d.h. es gibt ein $x \in \mathfrak{m}$ mit $x + b \cdot c = 1$. Aber dann ist

$$a = a \cdot (x + b \cdot c) = a \cdot \underbrace{x}_{\in \mathfrak{m}} + \underbrace{(a \cdot b)}_{\in \mathfrak{m}} \cdot c \in \mathfrak{m}.$$

Daher ist $\mathfrak{m}$ Primideal.

□

Korollar 4.6.7 *(zu den Definitionen und Satz 3.1.6) In einem Hauptidealring ist jedes Primideal, das nicht das Nullideal ist, maximal.*

Beweis: In einem Hauptidealring stimmen die Begriffe *irreduzibel* und *prim* überein. Die Lemmata 4.6.2 und 4.6.5 übertragen das gerade auf maximale Ideale und Primideale.

□

Satz 4.6.8 *Sei R kommutativer Ring und sei $I \trianglelefteq R$ ein echtes Ideal. Dann gilt:*

$$I \text{ ist Primideal} \iff R/I \text{ ist Integritätsring.}$$

Beweis: Vorab bemerken wir, dass $a \in I$ äquivalent zu $[a]_I = [0]_I$ ist nach der Definition von R/I. Die Bedingung I ist Primideal bedeutet gerade

$$\forall a, b \in R \text{ mit } a \cdot b \in I : (a \in I \text{ oder } b \in I).$$

Mit der gerade beobachteten Äquivalenz ist das dasselbe wie

$$\forall [a]_I, [b]_I \in R/I \text{ mit } [a \cdot b]_I = [0]_I : ([a]_I = [0]_I \text{ oder } [b]_I = [0]_I).$$

Das ist aber gerade die Aussage der Nullteilerfreiheit in R/I. Da R und damit R/I nach Voraussetzung kommutativ sind, ist das auch die Integritätsringeigenschaft von R/I.

□

Satz 4.6.9 *Sei R kommutativer Ring und sei $I \trianglelefteq R$ ein echtes Ideal. Dann gilt:*

$$I \text{ maximales Ideal} \iff R/I \text{ Körper.}$$

Beweis: Bezeichne mit $\pi : R \longrightarrow R/I$ den kanonischen Restklassenepimorphismus.
Ist I maximal, so gilt für jedes Element $a \in R \setminus I$: $I + \langle a \rangle = R$. Daher gilt auch

$$\langle \pi(a) \rangle = [0]_I + \langle \pi(a) \rangle = R/I.$$

Wegen der Surjektivität von π kann es in R/I also nur zwei Ideale geben, den ganzen Ring und das Nullideal. Damit ist R/I nach Lemma 2.6.7 ein Körper.
Ist andererseits $J \trianglelefteq R$ ein echtes Ideal mit $I \subsetneq J$, so ist $\langle [0]_I \rangle \subsetneq \pi(J) \subsetneq R/I$ und R/I damit nach Lemma 2.6.7 kein Körper.

□

Bemerkung 4.6.10 *Mit Hilfe der letzten beiden Sätze haben wir jetzt einen weiteren, viel einfacheren Beweis für Korollar 4.6.6: Jeder Körper ist Integritätsring, damit muss jedes maximale Ideal prim sein.*

Zum Abschluß der theoretischen Betrachtungen dieses Abschnitts fassen wir nochmals die verschiedenen Aussagen in neuer Weise zusammen:

Satz 4.6.11 *In einem Hauptidealring R sind für ein $a \in R \setminus \{0\}$ äquivalent:*

a) a ist Primelement

b) $R/\langle a \rangle$ ist Integritätsring

c) $R/\langle a \rangle$ ist Körper

Beweis: Dies ist die Zusammenstellung für den Fall eines Hauptidealrings von 4.6.7, 4.6.8 und 4.6.9.

□

Satz 4.6.12 *Sei R ein kommutativer Ring[2]. Dann sind äquivalent:*

a) R ist Körper

b) R hat keine echten Ideale

[2] mit $1 \neq 0$ wie üblich

c) $\forall I \trianglelefteq R$ *mit* $\langle 0_R\rangle \subseteq I \subseteq R : (I = \langle 0\rangle$ *oder* $I = R)$
(Wäre $\langle 0\rangle$ *echtes Ideal, so würde man sagen, dass* $\langle 0\rangle$ *maximales Ideal von* R *ist.)*

Beweis: Das ist die Zusammenstellung von 2.6.7 und 4.6.9 mit Blick auf Ideale in R.

□

Damit dieser Stoff nicht so trocken bleibt, wie er auf den ersten Blick aussieht, wenden wir dies dann auch wieder auf die früher definierten Restklassenringe an:

Anwendung 4.6.13 *Aus Satz 4.6.11 sehen wir sofort:*

$$\mathbb{Z}/m\mathbb{Z} \text{ Körper} \iff m \text{ Primzahl}$$

sowie für einen Körper K*:*

$$K[t]/\langle h\rangle \text{ Körper} \iff h \text{ irreduzibles Polynom}$$

Anwendung 4.6.14 *Betrachten wir* $I = \langle 3, t^2+1\rangle \subset \mathbb{Z}[t]$*. Dies ist offensichtlich kein Hauptideal. Untersuchen wir* $\mathbb{Z}[t]/I$ *nun, indem wir zuerst den Restklassenring von* $\mathbb{Z}[t]$ *bzgl.* $\langle 3\rangle$ *bilden. Dieses Vorgehen ist abgedeckt durch den zweiten Isomorphiesatz, der sicherstellt, dass*

$$(\mathbb{Z}[t]/\langle 3\rangle)/(\langle 3, t^2+1\rangle/\langle 3\rangle) = \mathbb{Z}[t]/\langle 3, t^2+1\rangle.$$

Mit einem kurzen Blick auf die Definition eines Polynomrings als Folge von Elementen des Grundrings ist direkt klar, dass die Restklassenbildung sich rein in den Koeffizienten abspielt und damit $\mathbb{Z}[t]/\langle 3\rangle = (\mathbb{Z}/\langle 3\rangle)[t]$*. Wir sehen also einen Polynomring über dem Körper* $\mathbb{Z}/\langle 3\rangle$ *vor uns.* t^2+1 *besitzt keine Nullstellen im Körper* $\mathbb{Z}/\langle 3\rangle$ *und damit ist* $(\mathbb{Z}/\langle 3\rangle)[t]/\langle t^2+1\rangle$ *ein Körper. Daher ist* I *maximales Ideal.*
Der Körper $(\mathbb{Z}/\langle 3\rangle)[t]/\langle t^2+1\rangle$ *hat übrigens genau* 3^2 *Elemente. Überlegen Sie welche und warum.*

Bemerkung 4.6.15 *Sei* R *ein kommutativer Ring und sei* $g \in R\backslash(\{0\}\cup R^*)$*. Dann gilt für alle* $a, c, x \in R$*:*

$$[a]_g \cdot [x]_g = [c]_g \iff \exists y \in R : ax + gy = c.$$

Bemerkung 4.6.16 *Ist* R *ein euklidischer Ring, so folgt aus der vorigen Bemerkung für alle* $a \in R \setminus \{0\}$*:*

$[a]_g \in (R/\langle g\rangle)^* \iff 1$ *ist ein größter gemeinsamer Teiler von* a *und* g*.*

4.7 Chinesischer Restsatz

Bisher haben wir uns vor allem mit dem Fall von Restklassenringen nach Primidealen und maximalen Idealen befasst. Diese haben als Integritätsringe bzw. Körper natürlich sehr schöne Eigeneschaften, in ihnen läßt sich vor allem relativ problemlos rechnen. Aber dadurch sind bei weitem nicht alle Fälle abgedeckt. Daher wenden wir uns in diesem Abschnitt dem Chinesischen Restsatz zu, der es z.B. erlaubt, im Falle des Restklassenrings von $\mathbb{Z}$ bzgl. einer zusammengesetzten Zahl mit r paarweise verschiedenene Primfaktoren stattdessen in r verschiedenen Integritätsringen zu rechnen.

Wir werden den Chinesischen Restsatz zuerst in einer sehr allgemeinen Form beweisen, dann aber auch die wichtigen Spezialfälle in $\mathbb{Z}$ und $K[t]$ daraus folgern. Wie auch mit vielen anderen Begriffen, die wir für die ganzen Zahlen schon lange kennen und in den vergangenen Kapiteln auf größere Klassen von Ringen verallgemeinert haben, müssen wir auch hier erst einen Begriff neu definieren: Teilerfremdheit von Idealen.

Erinnerung 4.7.1 *Sei R ein faktorieller Ring. Elemente $a_1, \ldots, a_n \in R$ heißen teilerfremd (oder coprim), falls ihre einzigen gemeinsamen Teiler Einheiten in R sind, d.h. in der Sprache von Abschnitt 4.4 bei gegebenem Repräsentantensystem $\mathcal{P}$ von R bzgl. Assoziiertheit, dass*

$$\min\{v_p(a_1), \ldots, v_p(a_n)\} = 0 \quad \forall p \in \mathcal{P} \setminus [1_R].$$

Für die folgende Erinnerung müssen wir die betrachteten Ringe etwas weiter einschränken, da sie nicht nur von der Existenz eines größten gemeinsamen Teilers abhängt, sondern von der Bézout-Identität, die nur in Hauptidealringen gilt.

Erinnerung 4.7.2 *Sei R Hauptidealring. Sind $a, b \in R$ teilerfremd, so gilt:*

$$\langle a \rangle + \langle b \rangle = R.$$

In der Tat ist die letztere Eigenschaft für eine Verallgemeinerung des Begriffs der Teilerfremdheit auf Ideale besser geeignet, als die erstere, da sie bereits von Idealen handelt.

Definition 4.7.3 *Sei R ein Integritätsring. Zwei Ideale $I, J \trianglelefteq R$ heißen* **teilerfremd** *(oder* **coprim** *oder* **relativ prim***), falls:*

$$I + J = R.$$

Ideale $I_1, \ldots, I_n \trianglelefteq R$ heißen **paarweise teilerfremd**, *falls:*

$$I_i + I_j = R \ \forall 1 \leq i < j \leq n.$$

Betrachten wir nun ein Beispiel für das zentrale Problem dieses Kapitels und dessen Lösung:

Beispiel 4.7.4 *In seinem Handbuch zur Arithmetik schrieb Sun Zi vor mehr als 2000 Jahren bereits über ein Problem, das wir heute als eine Aufgabe in einem nicht nullteilerfreien Restklassenring auffassen würden:*

> *Wir haben eine gewisse Zahl von Dingen, wissen jedoch nicht genau wieviele. Wenn wir sie je drei zählen, so verbleiben zwei. Wenn wir sie je fünf zählen, so verbleiben drei. Wenn wir sie je sieben zählen, sind noch zwei übrig. Wieviele Dinge sind es?*

Zusätzlich möchten wir noch voraussetzen, dass die Zahl zwischen 100 und 200 liegt.
Im heutigen Formalismus der Algebra lautet dann die Aufgabe:
Finde eine Zahl $\tilde{x} \in \mathbb{N}_0$ mit $100 \leq \tilde{x} \leq 200$, so dass gilt:

$$\begin{aligned} \tilde{x} &\equiv 2 \bmod 3 \\ \tilde{x} &\equiv 3 \bmod 5 \\ \tilde{x} &\equiv 2 \bmod 7 \end{aligned}$$

Um diese zu lösen, bilden wir zuerst die folgenden Zahlen:

$$m_1 = 3, \quad m_2 = 5, \quad m_3 = 7, \quad m := 3 \cdot 5 \cdot 7 = 105.$$

Wichtig dabei ist, dass m kongruent Null modulo jeder der drei Zahlen m_1, m_2, m_3 ist. Nun bilden wir noch

$$N_1 = \frac{m}{m_1} = 35 \quad N_2 = \frac{m}{m_2} = 21 \quad N_3 = \frac{m}{m_3} = 15$$

Damit ist jedes der N_i teilerfremd zu dem entsprechenden m_i und kongruent Null zu den beiden anderen m_j. Insbesondere besitzt N_i damit ein multiplikatives Inverses y_i modulo m_i:

$$\begin{aligned} [N_1]_{m_1} = [35]_3 = [2]_3 &\implies [N_1]_3 \cdot [y_1]_3 = [2]_3 \cdot [2]_3 = [1]_3 \\ [N_2]_{m_2} = [21]_5 = [1]_5 &\implies [N_2]_5 \cdot [y_2]_5 = [1]_5 \cdot [1]_5 = [1]_5 \\ [N_3]_{m_3} = [15]_7 = [1]_7 &\implies [N_3]_7 \cdot [y_3]_7 = [1]_7 \cdot [1]_7 = [1]_7 \end{aligned}$$

Betrachten wir nun $x_0 = 2 \cdot N_1 \cdot y_1 + 3 \cdot N_2 \cdot y_2 + 2 \cdot N_3 \cdot y_3 = 233$*, so ergeben sich die gewünschten Kongruenzen (Nachrechnen!). Wir haben damit eine Lösung des Kongruenzsystems gefunden, aber es ist nicht die einzige und es ist nicht die gesuchte! Wir können aber zu* x_0 *genau beliebige Vielfache von* $m = 105$ *hinzuaddieren, ohne die drei Kongruenzen zu verändern. Damit ist die Lösungsmenge des Kongruenzsystems:*

$$\{233 + 105k \mid k \in \mathbb{Z}\}.$$

Für das konkrete Problem erhalten wir die Lösung $\tilde{x} = 233 - 105 = 128$*.*

Das obige Beispiel ist in einer Form aufgeschrieben, die bereits die Grundideen des Beweises des allgemeinen Satzes vorwegnimmt und daher beim Nacharbeiten als Leitfaden durch den Beweis verwendet werden kann. Doch es ist nicht absolut offensichtlich, die einzelnen Schritte zuzuordnen. Wer es nicht direkt hinbekommt, findet im Vergleich von Korollar 4.7.10 und Satz 4.7.5 Hinweise darauf, wie die einzelnen Fakten und Konstruktionen zusammenspielen.

Satz 4.7.5 *(Chinesischer Restsatz, allgemeine Formulierung) Sei* R *ein Integritätsring und seien* $I_1, \ldots, I_n$ *paarweise teilerfremde Ideale von* R*. Für jede gegebene Wahl von* $r_1, \ldots, r_n \in R$ *existiert ein* $b \in R$*, das die simultanen Kongruenzen*

$$\begin{aligned} b &\equiv r_1 \bmod I_1 \\ &\vdots \\ b &\equiv r_n \bmod I_n \end{aligned}$$

erfüllt. Die Lösung b *ist eindeutig modulo* $I_1 \cdot \cdots \cdot I_n = I_1 \cap \cdots \cap I_n$*.*

Da der Beweis etwas länglich und unübersichtlich werden kann, wenn man ihn in einem Stück ausführt, betrachten wir vorher mehrere Lemmata:

Lemma 4.7.6 *Sei* R *ein Integritätsring und seien* I_1, I_2 *teilerfremde Ideale in* R*. Dann existiert für jede Wahl von* $r_1, r_2 \in R$ *ein* $b \in R$*, das die simultanen Kongruenzen*

$$\begin{aligned} b &\equiv r_1 \bmod I_1 \\ b &\equiv r_2 \bmod I_2 \end{aligned}$$

erfüllt. Die Lösung b *ist eindeutig modulo* $I_1 \cdot I_2 = I_1 \cap I_2$*.*

Beweis: Da I_1 und I_2 coprim sind und damit $I_1 + I_2 = R$ gilt, existieren $x_1 \in I_1$ und $x_2 \in I_2$ mit $x_1 + x_2 = 1$. Insbesondere gilt dann

$$\begin{aligned} [x_2]_{I_1} &= [x_1 + x_2]_{I_1} = [1]_{I_1} \text{ und} \\ [x_1]_{I_2} &= [x_1 + x_2]_{I_2} = [1]_{I_2}. \end{aligned}$$

Betrachten wir nun

$$b = x_1 \cdot r_2 + x_2 \cdot r_1 \in R,$$

so gilt

$$\begin{aligned} [b]_{I_1} &= [r_1 x_2]_{I_1} = [r_1]_{I_1} \cdot [x_2]_{I_1} = [r_1]_{I_1} \\ [b]_{I_2} &= [r_2 x_1]_{I_2} = [r_2]_{I_2} \cdot [x_1]_{I_2} = [r_2]_{I_2}. \end{aligned}$$

Damit erfüllt b die Bedingungen des Satzes.
Für die Eindeutigkeit seien nun $b, c \in R$ zwei Lösungen des Kongruenzproblems. Dann gilt $[b]_{I_1} = [r_1]_{I_1} = [c]_{I_1}$ und $[b]_{I_2} = [r_2]_{I_2} = [c]_{I_2}$, weshalb $b - c \in I_1 \cap I_2$ gelten muss. Umgekehrt ändert das Hinzuaddieren eines Elements aus $I_1 \cap I_2$ die Restklassen modulo I_1 und I_2 nicht, womit gezeigt ist, dass die Lösungsmenge des Kongruenzsystems bei einer bekannten Lösung $b \in R$ genau die Menge

$$\{b + h \mid h \in I_1 \cap I_2\}$$

ist.

□

Lemma 4.7.7 *Sei R ein Integritätsring, seien $I_1, \ldots, I_n$ paarweise teilerfremde Ideale von R und sei $1 \leq i \leq n$ ein fester Index. Dann gilt*

$$I_i + \bigcap_{\substack{1 \leq j \leq n \\ j \neq i}} I_j = R.$$

Beweis: Da die Ideale paarweise teilerfremd sind, wissen wir, dass es zu jedem Paar von Indizes (i, j) mit $j \neq i$ Elemente $c_j \in I_i$ und $d_j \in I_j$ gibt mit $c_j + d_j = 1$. Wir rechnen:

$$1 = \prod_{\substack{1 \leq j \leq n \\ j \neq i}} (c_j + d_j) = f(\underline{c}, \underline{d}) + \prod_{\substack{1 \leq j \leq n \\ j \neq i}} d_j,$$

wobei im Ausdruck f jeder Summand durch mindestens ein c_j teilbar ist, weswegen $f(\underline{c}, \underline{d}) \in I_i$. Andererseits gilt offensichtlich

$$\prod_{\substack{1 \leq j \leq n \\ j \neq i}} d_j \in \bigcap_{\substack{1 \leq j \leq n \\ j \neq i}} I_j.$$

Damit sind f und das Produkt über die d_j die beiden gesuchten Summanden.

□

Mit Hilfe dieser beiden Lemmata ist der Beweis des Satzes dann ganz übersichtlich:

Beweis: (4.7.5)
Nach Lemma 4.7.6 ist die Aussage für $n = 2$ Ideale bewiesen, was wir als Induktionsanfang einer Induktion nach n verwenden. Nehmen wir als Induktionsvoraussetzung an, dass die Behauptung für $n - 1$ Ideale gilt. Im Induktionsschritt schließen wir nun von $n - 1$ auf n Ideale:
Sind $I_1, \ldots, I_n$ paarweise teilerfremde Ideale in R, so sind nach Lemma 4.7.7 auch $J = \bigcap_{1 \leq i \leq n-1} I_i$ und I_n teilerfremde Ideale. Für die simultane Kongruenz bzgl. der $n - 1$ Ideale $I_1, \ldots, I_{n-1}$ existiert ein b_1, das diese löst und modulo J eindeutig ist. Das liefert uns ein neues System simultaner Kongruenzen:

$$\begin{aligned} [b]_{I_n} &= [r_n]_{I_n} \\ [b]_J &= [b_1]_J, \end{aligned}$$

welches wieder nach Induktionsanfang eine modulo $J \cdot I_n$ eindeutige Lösung b besitzt.

□

Bemerkung 4.7.8 *Seien $R_1, \ldots, R_n$ Ringe. Dann bezeichnet $R_1 \times \cdots \times R_n$ die Menge aller n-Tupel aus Einträgen aus R_1 bis R_n. Auf dieser Menge lassen sich durch komponentenweise Addition und Multiplikation zwei Verknüpfungen definieren, bzgl. derer diese Menge wieder ein Ring ist. Die Überprüfung der Ringaxiome ist eine leicht längliche, explizite Rechnung, die keine Schwierigkeiten bietet und deshalb hier entfällt. Das Einselement des neuen Ringes ist $(1_{R_1}, \ldots, 1_{R_n})$.*

Korollar 4.7.9 *Sei R Integritätsring und seien $I_1, \ldots, I_n$ paarweise teilerfremde Ideale in R. Dann ist*

$$R \Big/ \left(\prod_{i=1}^{n} I_i \right) \cong (R/I_1) \times \cdots \times (R/I_n)$$

ein Ringisomorphismus, der $[r]_{(\prod_{i=1}^{n} I_i)}$ auf das Tupel der $[r]_{I_i}$ abbildet.

Beweis: Da jedes einzelne R/I_j ein Ring ist, ist auch die Menge auf der rechten Seite bzgl. der komponentenweisen Addition und Multiplikation ein Ring. Die Abbildung

$$\begin{array}{rcl} \varphi : R & \longrightarrow & (R/I_1) \times \cdots \times (R/I_n) \\ b & \longmapsto & ([b]_{I_1}, \ldots, [b]_{I_n}) \end{array}$$

ist komponentenweise aus Restklassenhomomorphismen zusammengesetzt, die (wie wir bereits wissen) jeweils Ringepimorphismen sind. Da die Verknüpfungen auf der rechten Seite ebenfalls komponenteweise definiert sind, ist auch φ ein Ringhomomorphismus (Nachrechnen!). Nach Satz 4.7.5 besitzt jedes System von simultanen Kongruenzen modulo I_1 bis I_n eine Lösung in R, so dass φ surjektiv ist. Ebenfalls nach 4.7.5 ist das Urbild der Null unter φ gerade das Produkt der Ideale $I_1 \cdots I_n$. Damit folgt die Aussage des Korollars aus dem Homomorphiesatz.

□

Den allgemeinen Satz können wir auch spezieller für Hauptidealringe oder noch konkreter für $\mathbb{Z}$ oder den Polynomring $K[t]$ über einem Körper K formulieren. Da es sich dabei lediglich um die direkte Anwendung des Satzes in einer konkretisierten Situation handelt, müssen wir diese Aussagen nicht beweisen.

Korollar 4.7.10 *(Chinesischer Restsatz für Hauptidealringe) Sei R ein Hauptidealring und seien $m_1, \ldots, m_n \in R$ paarweise teilerfremd. Zu gegebenen $r_1, \ldots, r_n \in R$ existiert dann ein $b \in R$, das das folgende System von simultanen Kongruenzen löst:*

$$[X]_{m_i} = [r_i]_{m_i} \quad \forall 1 \leq i \leq n.$$

Die Lösung ist modulo $m := m_1 \cdot \cdots \cdot m_n$ eindeutig und es gilt:

$$R/\langle m \rangle \cong (R/\langle m_1 \rangle) \times \cdots \times (R/\langle m_n \rangle)\,.$$

Korollar 4.7.11 *(Chinesischer Restsatz für Hauptidealringe, Version 2) Sei R ein Hauptidealring und sei $a \in R \setminus (\{0\} \cup R^*)$ mit Primfaktorzerlegung*

$$a = \varepsilon(a) \prod_{i=1}^{n} p_i^{e_i},$$

wobei $\varepsilon(a) \in R^*$ und $e_1, \ldots, e_n \in \mathbb{N}$ sowie $p_1, \ldots, p_n \in R$ paarweise nicht assoziierte Primelemente in R sind. Dann gilt

$$R/\langle a \rangle \cong (R/\langle p_1^{e_1} \rangle) \times \cdots \times (R/\langle p_n^{e_n} \rangle)\,.$$

Vergleichen Sie die beiden vorstehenden Korollare und bringen Sie die beiden Aussagen in Einklang. Wir spielen hier gerade mit verschiedenen Anwendungen desselben Satzes auf verschiedene Situationen und deren Formulierung. Unabhängig vom hier gewählten Kontext, in dem wir das gerade üben, ist die Fähigkeit, allgemeine Sätze auf konkrete Kontexte anwenden zu können, ohne sie jedesmal in einer neuen Situation wieder beweisen zu müssen, ein wichtiges Charakteristikum der Mathematik. Man begibt sich in einen recht allgemeinen Kontext (mit genau den Voraussetzungen, die man wirklich braucht), formuliert und beweist die gewünschte Aussage und wendet sie dann später in ganz verschiedenen Situationen an.

Bemerkung 4.7.12 *(Wie 'basteln' wir b konkret?)*
In der Situation des Satzes 4.7.10 wissen wir, dass die paarweise teilerfremden Ideale von der Form $I_i = \langle m_i \rangle$ sind. Wir definieren:

$$\begin{aligned} N &:= m_1 \cdots m_n \\ N_i &:= \prod_{\substack{1 \le j \le n \\ j \neq i}} m_j \end{aligned}$$

Dann gilt $\prod_{i=1}^{n} I_i = \langle N \rangle$ und $\prod_{\substack{1 \le j \le n \\ j \neq i}} I_j = \langle N_i \rangle$. Da m_i und N_i (für ein festes i) nach Konstruktion teilerfremd sind, ist N_i nach dem Satz von Bézout invertierbar in $R/\langle m_i \rangle$. Dieses Inverse nennen wir y_i. Damit kann man leicht explizit nachrechnen, dass

$$b = \sum_{i=1}^{n} r_i N_i y_i$$

das gewünschte System von simultanen Kongruenzen erfüllt.

Die folgende weitere Konkretisierung des Rings mit Formulierung der entsprechenden Aussage trägt den Namen 'Fundamentalsatz', ist aber mit unseren bisher bewiesenen Techniken nichts als ein direktes Korollar. Den Namen verdient der Satz wegen seiner großen Bedeutung in Theorie (als Strukturssatz) und Praxis. Eine recht naheliegende, aber auch wichtige Anwendung das sogenannte 'modulare' Rechnen in der Computeralgebra: In vielen Algorithmen mit Berechnungen über den ganzen Zahlen wachsen die betrachteten Zahlen zwischenzeitlich sehr schnell an, so dass die Rechnungen allein durch die großen Zahlen schon speicherintensiv und damit langsam werden können. Hat man vorab eine Abschätzung, wie groß die Zahlen, z.B. Koeffizienten eines polynomialen Ergebnisses, werden können, ist es statt der Rechnung über $\mathbb{Z}$ möglich über ausreichend vielen, verschiedenen Körpern $\mathbb{Z}/p\mathbb{Z}$ zu rechnen und das Ergebnis am Ende mit dem Chinesischen Restsatz zu bestimmen.

Satz 4.7.13 *(Fundamentalsatz für $\mathbb{Z}/m\mathbb{Z}$) Für alle $m \in \mathbb{N}$ mit teilerfremder Zerlegung $m = \prod_{i=1}^{n} m_i$ gilt*

$$\mathbb{Z}/m\mathbb{Z} \cong (\mathbb{Z}/m_1\mathbb{Z}) \times \cdots \times (\mathbb{Z}/m_n\mathbb{Z})\,.$$

Die Formulierung des Chinesischen Restsatzes für univariate Polynomringe über einem Körper werden Sie als Übungsaufgabe vorfinden.

4.8 Quotientenkörper und Lokalisierung

Viele der altbekannten Eigenschaften von $\mathbb{Z}$ haben wir schon in allgemeinen Kontext stellen können. Noch nicht betrachtet haben wir die Konstruktion der rationalen Zahlen $\mathbb{Q}$ aus den ganzen Zahlen $\mathbb{Z}$. Dies holen wir in dem folgenden recht kurzen Abschnitt nach. Für die 2-Fächer Bachelor ist lediglich die Konstruktion des Quotientenkörpers relevant, der allgemeinere Kontext der Lokalisierung ist nur für die Fachmathematiker verpflichtend.

Bemerkung 4.8.1 *Sei R ein Integritätsring und sei $S = R \times (R \setminus \{0\})$ die Menge aller Paare von Elementen aus R, bei denen das zweite nicht Null ist. Dann können wir auf S eine kommutative Ringstruktur definieren mittels der Verknüpfungen*

$$\begin{aligned} + : S \times S &\longrightarrow S \\ ((a,b),(c,d)) &\longmapsto (ad+bc, bd) \\ \cdot : S \times S &\longrightarrow S \\ ((a,b),(c,d)) &\longmapsto (ac, bd). \end{aligned}$$

Die Tatsache, dass es sich bei $(S, +, \cdot)$ tatsächlich um einen Ring handelt, läßt sich ohne Probleme direkt nachrechnen.

Satz 4.8.2 *Sei R ein Integritätsring. Dann ist durch auf der Menge $S = R \times (R \setminus \{0\})$ eine Äquivalenzrelation definiert durch*

$$(a, b) \sim (c, d) :\Longleftrightarrow ad - bc = 0.$$

$S/\sim$ ist ein Körper, der R enthält, der **Quotientenkörper** *von R, kurz $Quot(R)$.*

Beweis: $\sim$ ist offensichtlich reflexiv, da $ab - ab = 0$, und symmetrisch, da $bc - ad = -(ad - bc) = 0$. Für die Transitivität betrachten wir drei Paare $(a, b), (c, d), (e, f) \in S$, so dass $ad - bc = 0$ und $cf - de = 0$. Ist $c = 0$, so ist nach diesen Gleichungen, nach der Nullteilerfreiheit von R und nach der Voraussetzung $d \in R \setminus \{0\}$ auch $a = e = 0$, weshalb die gewünschte Gleichung $af - be = 0$ automatisch erfüllt ist. Bleibt der Fall $c \neq 0$ zu betrachten. Hierbei rechnen wir:

$$0 = e \cdot (ad - bc) + a \cdot (cf - de) = ade - bce + acf - ade = acf - bce.$$

Da aber R nullteilerfrei ist und da $c \neq 0$, muss damit gelten, dass $af - be = 0$, was uns die Transitivität von $\sim$ liefert. Damit ist $\sim$ eine Äquivalenzrelation auf S. $S/\sim$ ist wieder ein Ring (Nachrechnen!).
Zum Beweis, dass $S/\sim$ ein Körper ist, sei $0_{S/\sim} \neq s \in S/\sim$ beliebig und sei $(a, b) \in S$ ein Repräsentant von s. Dann ist insbesondere $a \neq 0$ und wir können das Paar $(b, a) \in S$ betrachten. Es gilt

$$(a, b) \cdot (b, a) = (ab, ab) \sim (1, 1),$$

d.h.

$$[(a, b)]_\sim \cdot [(b, a)]_\sim = 1_{S/\sim},$$

womit ein Inverses zu s bestimmt ist. Daher ist $S/\sim$ ein Körper. Wir betrachten jetzt die Komposition von Ringhomomorphismen:

$$\begin{array}{ccc} R & \hookrightarrow & S \longrightarrow S/\sim \\ r & \longmapsto & (r, 1) \longmapsto [(r, 1)]_\sim, \end{array}$$

wobei die erste Abbildung injektiv ist. Damit wir tatsächlich $R \subset S/\sim$ erhalten, muss auch die Verkettung der beiden Abbildungen injektiv sein.

Seien dazu $r_1 \neq r_2 \in R$, dann gilt $(r_1, 1) \neq (r_2, 1)$ und auch $[(r_1, 1)]_\sim \neq [(r_2, 1)]_\sim$ wegen $r_1 \cdot 1 - r_2 \cdot 1 = r_1 - r_2 \neq 0$. Daher ist die Komposition der beiden obigen Abbildungen injektiv und alle Behauptungen des Satzes sind gezeigt.

□

Erkennen Sie die Konstruktion? Die Addition und die Multiplikation sind gerade so definiert, wie es die Addition und Multiplikation von Brüchen, dargestellt als Paar (Zähler, Nenner), erfordert. Nehmen Sie als R die ganzen Zahlen $\mathbb{Z}$, dann ist die Äquivalenzrelation die Gleichheit nach Kürzen bzw. Erweitern und $S/\sim$ ist dann der Körper der rationalen Zahlen $\mathbb{Q}$.

Die obige Konstruktion ist ein Spezialfall einer allgemeineren Konstruktion der Lokalisierung. Diese werden wir in der kommutativen Algebra ausführlich besprechen. Hier geben wir lediglich die Definition an und nennen einige wichtige Eigenschaften im Vorgriff auf diese Veranstaltung.

Definition 4.8.3 *Eine Teilmenge $S \neq \emptyset$ eines kommutativen Ringes R heißt* **multiplikativ abgeschlossen**, *falls $1 \in S$ und für $a, b \in S$ auch $a \cdot b \in S$. Auf $R \times S$ definieren wir eine Relation durch*

$$(r, a) \sim (s, b) :\Longleftrightarrow \quad \exists v \in S : v(rb - sa) = 0$$

Bemerkung 4.8.4 *Hier könnte man noch fordern, dass $0 \notin S$. Damit würde man einen pathologischen Fall ausschliessen, denn wenn $0 \in S$, dann fallen alle Elemente beim Bilden von $S^{-1}R$ mit der Null zusammen und wir erhalten einen Ring mit nur einem Element. Ob man dies explizit ausschließen möchte oder nicht, ist Geschmacksache.*
Ist R nullteilerfrei oder enthält S keine Nullteiler von R, so ist die Bedingung $v(rb - sa) = 0$ gleichbedeutend mit $rb - sa = 0$. Einzig im Falle eines Nullteilers $v \in S$, kann es vorkommen, dass für zwei Paare (r, a) und (s, b) gilt $rb - sa \neq 0$, während $v(rb - sa) = 0$.

Satz 4.8.5 *Die Relation aus Definition 4.8.3 ist eine Äquivalenzrelation.*

Definition 4.8.6 *Sei R kommutativer Ring, $S \subseteq R$ multiplikativ abgeschlossene Teilmenge und $\sim$ die in 4.8.3 definierte Äquivalenzrelation. Für $(r, a) \in R \times S$ bezeichne die zugehörige Klasse von (r, a) durch*

$$\frac{r}{a} := [(r, a)]_\sim = \{(s, b) \in R \times S \mid (r, a) \sim (s, b)\}.$$

Die **Lokalisierung** *von R nach S ist dann die Menge der Äquivalenzklassen bzgl. $\sim$, kurz*

$$S^{-1}R := \{\frac{r}{a} \mid r \in R, a \in S\}.$$

Bemerkung 4.8.7 *Sei R kommutativer Ring. Ist R nullteilerfrei, so gilt*

$$(r, a) \sim (s, b) \Longleftrightarrow rb - sa = 0.$$

Satz 4.8.8 *Sei R ein kommutativer Ring und $S \subseteq R$ eine multiplikativ abgeschlossene Menge. Dann ist $(S^{-1}R, +, \cdot)$ ein kommutativer Ring mit $1_{S^{-1}R} = \frac{1}{1}$ und $0_{s^{-1}R} = \frac{0}{1}$, wobei die Addition und die Multiplikation analog zu den entsprechenden Operationen für Brüche definiert sind:*

$$\frac{r}{a} + \frac{s}{b} := \frac{rb + sa}{ab} \text{ und } \frac{r}{a} \cdot \frac{s}{b} := \frac{rs}{ab}.$$

Satz 4.8.9 *Sei R kommutativer Ring und $S \subseteq R$ eine multiplikativ abgeschlossene Teilmenge. Dann ist*

$$\begin{array}{rcl} \iota_S : R & \longrightarrow & S^{-1}R \\ r & \longmapsto & \dfrac{r}{1} \end{array}$$

ein Ringhomomorphismus mit $\mathrm{Im}(\iota_S \mid S) \subseteq (S^{-1}R)^*$ und $\ker(\iota_S) = \{r \in R \mid \exists s \in S \text{ mit } rs = 0\}$.

Bemerkung 4.8.10 *ι_S ist genau dann injektiv, wenn S weder die Null noch Nullteiler enthält.*
Die Konstruktion des Quotientenkörpers eines Integritätsringes R oben ist gerade die Lokalisierung von R an der multiplikativ abgeschlossenen Menge $S = R \setminus \{0\}$.

Kapitel 5

Irreduzibilität

Bereits im vorigen Kapitel hatten wir gesehen, dass Faktorringe, die durch Kongruenz bzgl. eines maximalen Ideals entstehen, Körper sind. Im Ring $\mathbb{Z}$ war es einfach maximale Ideal zu erkennen: sie werden von Primzahlen erzeugt und Primzahlen fühlen sich zumindest sehr vertraut an. Im Polynomring über einem Körper allerdings haben wir noch keine einfache Möglichkeit kennengelernt, wie wir maximale Ideale bzw. irreduzible Elemente erkennen können. Bilden wir einen Polynomring in einer Veränderlichen über einem Integritätsring, der kein Körper ist, so haben wir nicht einmal mehr einen euklidischen Ring vor uns und die Situation erscheint nochmals unübersichtlicher. Es ist also höchste Zeit, sich über Irreduzibilität Gedanken zu machen.

5.1 Nullstellen und Linearfaktoren

Tragen wir zuerst ein paar Aussagen zusammen, die wir bereits früher betrachtet hatten und die für den Umgang mit Irreduzibilität von Polynomen hilfreich sein können. Vergessen wir dabei nicht, dass wir schon einige Kenntnisse über Nullstellen und Linearfaktoren besitzen.

Erinnerung 5.1.1 *Seien R, S Integritätsringe mit $R \leq S$. Dann sind $R[t]$ und $S[t]$ Integritätsringe und es gilt $R[t]^* = R^*$ sowie $S[t]^* = S^*$.*
Ein Polynom $f \in R[t]$ kann stets auch als Polynom in $S[t]$ betrachtet werden. Es kann irreduzibel in $R[t]$, aber reduzibel in $S[t]$ sein, wie etwa $t^2 + 1 \in \mathbb{R}[t]$, das in $\mathbb{C}[t]$ in die Faktoren $t - i$ und $t + i$ zerfällt.

Beobachtung 5.1.2 *Ist $R = K$ ein Körper, so ist $f \in K[t] \setminus \{0\}$ genau dann reduzibel, wenn es eine Zerlegung $f = gh$ gibt mit $g, h \in K[t]$ und $0 < \deg(g), \deg(h) < \deg(f)$. Insbesondere ist jedes $f \in K[t]$ mit $\deg(f) = 1$ irreduzibel.*
Ist andererseits R kein Körper, so kann auch ein Polynom vom Grad 1 reduzibel sein (z.B. ist $4t + 6 \in \mathbb{Z}[t]$ reduzibel mit den nicht-trivialen Faktoren 2 und $2t+3$). Ist allerdings $f = at+b \in R[t]$ mit $a \in R^*$, so ist f irreduzibel, da wegen des Grades von f höchstens ein nicht-trivialer Faktor vom Grad 1 sein kann und der andere nicht-triviale Faktor dann ein Teiler jedes Koeffizienten ist. Einheiten haben jedoch keine nicht-trivialen Teiler.

Erinnerung 5.1.3 *Seien $R \leq S$ Ringe, wobei R kommutativ ist. Dann heißt $\alpha \in S$ eine* **Nullstelle** *von $f \in R[t]$, falls α einsetzbar in Polynome über R ist und $f(\alpha) = E_\alpha(f) = 0$.*

Hier wird uns hauptsächlich die Situation eines kommutativen S interessieren, so daß jedes Element von S einsetzbar ist in Polynome über R.

Erinnerung 5.1.4 *Seien $R \leq S$ kommutative Ringe, $f \in R[t]$ und $\alpha \in S$. Dann gilt:*

$$\alpha \text{ ist Nullstelle von } f \iff (t - \alpha) \mid f.$$

Satz 5.1.5 *Seien $R \leq S$ kommutative Ringe, $f \in R[t]$ ein Polynom vom Grad $\deg(f) = n$. Dann hat f höchstens n verschiedene Nullstellen in S.*

Beweis: Seien $\alpha_1, \ldots, \alpha_s \in S$ verschiedene Nullstellen von f. Dann gilt

$$\prod_{i=1}^{s} (t - \alpha_i) \mid f,$$

weswegen der Grad des Produktes höchstens n sein kann.

□

Beobachtung 5.1.6 *Ist $R = K$ ein Körper und ist $f \in K[t]$ ein Polynom vom Grad 2 oder 3, so ist f reduzibel über K genau dann, wenn f eine Nullstelle in K besitzt. Für Grad 4 gilt das nicht mehr. Überlegen Sie warum und finden Sie ein Beispiel!*
Ist andererseits R nullteilerfreier Ring, aber kein Körper, so gilt die obige Aussage noch immer für normierte Polynome bzw. deutlich allgemeiner für Polynome mit Leitkoeffizient in R^* bzw. für Polynome, von denen sich kein nicht-trivialer konstanter Faktor abspalten läßt.

5.2 Rationale Nullstellen

Betrachten wir nun die Situation, dass R ein faktorieller Ring ist und $S = Quot(R)$, etwas genauer.

Erinnerung 5.2.1 *Die folgenden Tatsachen wurden in früheren Kapiteln implizit oder explizit bereits gezeigt:*

- *In einem faktoriellen Ring R gibt es größte gemeinsame Teiler und kleinste gemeinsame Vielfache von je zwei Ringelementen.*
- *Sind $a, b \in R$ teilerfremd und gilt $a \mid b \cdot c$ für ein $c \in R$, so gilt $a \mid c$.*
- *Seien $a, b \in R$ und $d \in R$ ein größter gemeinsamer Teiler von a und b. Dann sind $A, B \in R$ mit $a = Ad$ und $b = Bd$ teilerfremd in R.*
- *Ist $\alpha \in Quot(R)$, so existieren teilerfremde $A, B \in R$ mit $\alpha = \frac{A}{B}$.*

Satz 5.2.2 *Sei R ein faktorieller Ring mit Quotientenkörper $K = Quot(R)$. Sei ferner $f = \sum_{i=0}^{n} a_i t^i \in R[t]$ ein Polynom vom Grad $n \geq 1$, d.h. insbesondere $a_n \neq 0$. Ist nun $\alpha = \frac{A}{B} \in K$ eine Nullstelle von f mit teilerfremden $A, B \in R$, $B \neq 0$, dann gilt:*

$$B \mid a_n \text{ und } A \mid a_0.$$

Beweis: Betrachte

$$0 = f(\alpha) = \sum_{i=0}^{n} a_i \left(\frac{A}{B}\right)^i.$$

Nach Multiplikation mit B^n (unschädlich, da R nullteilerfrei und $B \neq 0$) liefert das

$$0 = \sum_{i=0}^{n} a_i A^i B^{n-i} = \underbrace{a_n A^n}_{\text{Vielfaches von } A} + \underbrace{\sum_{i=1}^{n-1} a_i A^i B^{n-i}}_{\text{Vielfaches von } AB} + \underbrace{a_0 B^n}_{\text{Vielfaches von } B}.$$

Da jedes Element von R die Null teilt und damit A und B jeweils alle bis auf einen Summanden oben teilen, müssen sie jeweils auch den verbliebenen teilen. Da sie andererseits teilerfremd sind, müssen sie den jeweils verbleibenden Faktor teilen, was genau die Behauptung liefert.

□

Beispiel 5.2.3 *Ein Spezialfall des vorigen Satzes ist die bereits aus der Schule (ohne Beweis) bekannte Aussage, dass jede ganzzahlige Nullstelle eines normierten Polynoms über $\mathbb{Z}$ den konstanten Term des Polynoms teilt.*

5.3 Satz von Gauß

Seien $R \leq S$ Integritätsringe. Die Frage nach Irreduzibilität von Polynomen über R bzw. über S ist recht subtil, wie wir zu Beginn des Kapitels bereits gesehen haben: Weder impliziert Irreduzibilität über R Irreduzibilität über S, noch umgekehrt. Unser Ziel in diesem Abschnitt wird sein, die Situation für den wichtigen Spezialfall $S = Quot(R)$ konkret zu beschreiben. Im Laufe des Kapitels werden wir auch die Aussage, dass ein Polynomring über einem faktoriellen Ring wieder faktoriell ist, endlich beweisen können.

Proposition 5.3.1 *Sei $\varphi : R \longrightarrow S$ ein Homomorphismus kommutativer Ringe. Dann ist auch*

$$\begin{array}{rcl} \Phi : R[t] & \longrightarrow & S[t] \\ \displaystyle\sum_{i=0}^{n} a_i t^i & \longmapsto & \displaystyle\sum_{i=0}^{n} \varphi(a_i) t^i \end{array}$$

ein Ringhomomorphismus.

Beweis: Offensichtlich handelt es sich um eine wohldefinierte Abbildung von Ringen, für die wegen $\varphi(1_R) = 1_S$ auch gilt

$$\Phi(1_{R[t]}) = \Phi(1_R t^0) = \varphi(1_R) t^0 = 1_S t^0 = 1_{S[t]}.$$

Für die Verträglichkeit mit Addition und Multiplikation betrachen wir zwei

Polynome $f = \sum_{i=0}^{n} a_i t^i, g = \sum_{i=0}^{m} b_i t^i \in R[t]$ und rechnen:

$$\begin{aligned}
\Phi(f+g) &= \Phi\left(\sum_{i=0}^{\max\{m,n\}} (a_i + b_i)t^i\right) \\
&= \sum_{i=0}^{\max\{m,n\}} \varphi(a_i + b_i)t^i \\
&= \sum_{i=0}^{\max\{m,n\}} (\varphi(a_i) + \varphi(b_i))t^i \\
&= \left(\sum_{i=0}^{n} \varphi(a_i)t^i\right) + \left(\sum_{i=0}^{m} \varphi(b_i)t^i\right) \\
&= \Phi(f) + \Phi(g) \\
\Phi(f \cdot g) &= \Phi\left(\sum_{k=0}^{n+m} \sum_{i+j=k} a_i b_j t^k\right) \\
&= \sum_{k=0}^{n+m} \left(\sum_{i+j=k} \varphi(a_i b_j)\right) t^k \\
&= \sum_{k=0}^{n+m} \sum_{i+j=k} \varphi(a_i)\varphi(b_j)t^k \\
&= \left(\sum_{i=0}^{n} \varphi(a_i)t^i\right) \cdot \left(\sum_{i=0}^{m} \varphi(b_i)t^i\right) \\
&= \Phi(f) \cdot \Phi(g)
\end{aligned}$$

Damit sind die Bedingungen an einen Ringhomomorphismus explizit nachgerechnet und die Behauptung damit bewiesen.

□

Satz 5.3.2 *Sei R ein kommutativer Ring, $I \trianglelefteq R$ ein Ideal und $J \trianglelefteq R[t]$, das von I in $R[t]$ erzeugte Ideal. Dann gilt*

a) $J \cap R = I$

b) Es gibt einen Isomorphismus

$$R[t]/J \cong (R/I)[t].$$

c) J ist genau dann Primideal, wenn I Primideal ist.

Beweis: Nach der Definition des von einer Menge erzeugten Ideals gilt

$$\begin{aligned} J &= \{\sum_{i=1}^{n} r_i a_i \mid n \in \mathbb{N}, a_1, \ldots, a_n \in I, r_1, \ldots, r_n \in R[t]\} \\ &= \{\sum_{j=0}^{m} b_j t^j \mid m \in \mathbb{N}_0, b_1, \ldots, b_m \in I\} \end{aligned}$$

Damit besteht J gerade aus den Polynomen, deren Koeffizienten in I liegen und von diesen sind genau die konstanten Polynome Elemente von R, was die Aussage a) liefert.
Für die Aussage b) betrachten wir die Restklassenabbildung $\varphi : R \longrightarrow R/I$ und die davon induzierte Abbildung $\Phi : R[t] \longrightarrow (R/I)[t]$ nach Proposition 5.3.1. Offensichtlich ist Φ surjektiv und ein Polynom liegt genau dann im Kern, wenn alle Koeffizienten auf Null abgebildet werden, d.h. wenn es in J liegt. Nach dem Homomorphiesatz erhalten wir damit den gewünschten Isomorphismus.
Mittels dieses Isomorphismus ist ausserdem klar, dass $R[t]/J$ genau dann Integritätsring ist, wenn $(R/I)[t]$ Integritätsring ist, was wiederum genau dann der Fall ist, wenn R/I selbst ein Integritätsring ist. Damit ist auch Aussage c) beweisen.

□

Korollar 5.3.3 *Sei R Integritätsring und $p \in R \setminus \{0\}$. p ist Primelement in R, genau dann wenn das konstante Polynom p Primelement in $R[t]$ ist.*

Beweis: Die Aussage ist äquivalent dazu, dass $\langle p \rangle \trianglelefteq R$ genau dann Primideal ist, wenn $\langle p \rangle \trianglelefteq R[t]$ Primideal ist. Das ist aber gerade Satz 5.3.2, c).

□

Proposition 5.3.4 *Sei R Integritätsring und sei $a \in R$ mit einer Zerlegung als Produkt $a = \prod_{i=1}^{n} f_i$, wobei $f_1, \ldots, f_n \in R[t]$. Diese ist genau dann eine Primfaktorzerlegung von a in $R[t]$, wenn sie eine Primfaktorzerlegung von a in R ist.*

Beweis: Wegen $a \in R$ und damit $\deg(a) = 0$ gilt auch $\deg(f_i) = 0$ für jeden einzelnen der Faktoren. Damit sind alle f_i bereits Elemente von R.
Nach dem vorigen Korollar ist somit jedes f_i genau dann prim in R, wenn es prim in $R[t]$ ist, was die gewünschte Aussage liefert.

□

Korollar 5.3.5 *Sei R Integritätsring. Ist $R[t]$ faktoriell, so auch R.*

Dies ist eine unmittelbare Folge der vorstehenden Proposition. Wir werden nach ein paar Vorarbeiten sehen, dass auch die umgekehrte Implikation gilt. Dafür müssen wir aber noch ein bisschen arbeiten.

Definition 5.3.6 *Sei R ein faktorieller Ring. Ein Polynom $f \in R[t] \setminus \{0\}$ heißt* **primitiv**, *falls die Koeffizienten von f teilerfremd sind.*

Bemerkung 5.3.7 *Ganz konkret formuliert, ist $f = \sum_{i=0}^{n} a_i t^i \in R[t] \setminus \{0\}$ primitiv, falls 1 ein größter gemeinsamer Teiler von $a_0, \ldots, a_n$ ist.*

Satz 5.3.8 *Sei R faktorieller Ring und seien $f, g \in R[t] \setminus \{0\}$ primitiv. Dann ist auch $f \cdot g$ primitiv.*

Beweis: Seien $f = \sum_{i=0}^{n} a_i t^i, g = \sum_{j=0}^{m} b_j t^j \in R[t]$ zwei primitive Polynome. Dann ist 1 ein größter gemeinsamer Teiler von $a_0, \ldots, a_n$ sowie ein gemeinsamer Teiler von $b_0, \ldots, b_m$.
Zum Nachweis der Primitivität von

$$f \cdot g = \sum_{k=0}^{m+n} \left(\sum_{i+j=k} a_i b_j \right) t^k$$

nehmen wir das Gegenteil an. Sei also $p \in R \setminus R^*$ ein Primelement, das ein gemeinsamer Teiler aller Koeffizienten

$$c_k = \sum_{i+j=k} a_i b_j, \quad 0 \leq k \leq n+m$$

des Produkts ist. Wegen der Primitivität von f und g teilt p mindestens ein a_i und mindestens ein b_j nicht. Bezeichne mit i_0 den kleinsten Index mit $p \nmid a_{i_0}$ und mit j_0 den kleinsten Index mit $p \nmid b_{j_0}$ und betrachte

$$\underbrace{c_{i_0+j_0}}_{\text{teilbar durch } p} = \underbrace{\sum_{\substack{i+j=i_0+j_0 \\ i<i_0}} a_i b_j}_{\text{teilbar durch } p} + a_{i_0} b_{j_0} + \underbrace{\sum_{\substack{i+j=i_0+j_0 \\ i>i_0}} a_i b_j}_{\text{teilbar durch } p}$$

Nach dieser Rechnung muss p auch Teiler des verbliebenen Summanden sein, was im Widerspruch steht dazu, dass p prim ist und weder Teiler von a_{i_0} noch von b_{j_0}. Damit ist $f \cdot g$ primitiv, was zu zeigen war.

□

Proposition 5.3.9 *Sei R faktorieller Ring und $K = Quot(R)$. Für jedes $f \in K[t]$ existieren $\alpha \in K$ und $g \in R[t]$ primitiv, so dass*

$$f = \alpha g.$$

Beweis: Sei $f = \sum_{i=0}^{n} \frac{a_i}{b_i} t^i \in K[t]$ mit $a_0, \ldots, a_n \in R, b_0, \ldots, b_n \in R \setminus \{0\}$. Dann gibt es ein kleinstes gemeinsames Vielfaches $k \in R$ der Nenner $b_0, \ldots, b_n \in R$,also einen Hauptnenner der Koeffizienten von f, und es ist $k \cdot f \in R[t]$. Schreiben wir

$$k \cdot f = \sum_{i=0}^{n} c_i t^i,$$

so existiert ein größter gemeinsamer Teiler $d \in R$ der Koeffizienten $c_0, \ldots, c_n \in R$ und es gilt

$$\frac{k}{d} \cdot f = \sum_{i=0}^{n} \frac{c_i}{d} t^i,$$

wobei 1 größter gemeinsamer Teiler der $\frac{c_0}{d}, \ldots, \frac{c_n}{d} \in R$ ist. Das Polynom $g := \frac{k}{d} \cdot f \in R[t]$ ist daher primitiv und es gilt mit $\alpha := \frac{d}{k}$:

$$f = \frac{d}{k} \cdot (\frac{k}{d} f) = \alpha \cdot g.$$

□

Bemerkung 5.3.10 *Ist f in der obigen Proposition bereits aus $R[t]$, so kann der erste Schritt des Beweises entfallen, da der Hauptnenner dann 1 ist und man erhält $\alpha = d$ und $f = \alpha \cdot (\frac{1}{d} f)$. In diesem Fall nennt man α (vor allem in der Computeralgebra) auch den* **Content** *von f.*

Lemma 5.3.11 *Sei R ein faktorieller Ring, $K = Quot(R)$, seien $f, g \in R[t] \setminus \{0\}$ primitiv, so dass $f = \alpha g$ für ein $\alpha \in K$, so ist $\alpha \in R^*$.*

Beweis: f und g sind primitive Polynome mit Koeffizienten in R. Schreiben wir $\alpha = \frac{\beta}{\gamma}$, wobei $\beta, \gamma \in R$ teilerfremd gewählt sind, so gilt $\gamma f = \beta g$ und der gemeinsame Teiler γ aller Koeffizienten von γf muss jeden Koeffizienten von βg und damit wegen der Teilerfremdheit von β und γ jeden Koeffizienten von g teilen. Damit muss γ wegen der Primitivität von g eine Einheit sein. Mit der analogen Argumentation muss auch β eine Einheit sein. Damit ist $\alpha = \frac{\beta}{\gamma} \in R^*$.

□

Satz 5.3.12 *Sei R faktorieller Ring und $K = Quot(R)$. Dann gilt für jedes nicht-konstante primitive Polynom $f \in R[t] \subseteq K[t]$:*

$$f \text{ irreduzibel in } R[t] \iff f \text{ irreduzibel in } K[t]$$

Bevor wir mit dem Beweis beginnen, erinnern wir uns nochmals, dass in faktoriellen Ringen, wie z.B. $K[t]$, die Begriffe *irredzuibel* und *prim* zusammenfallen. In Integritätsringen gilt die Äquivalenz der Begriffe nicht mehr, aber *prim* impliziert noch immer *irreduzibel*, so dass diese Richtung auch in $R[t]$ nutzbar ist. Das erlaubt es uns, in einer Richtung mittels der Eigenschaft *prim* statt *irreduzibel* zu argumentieren.

Beweis: Machen Sie sich beim Nacharbeiten klar, dass/warum wir das Richtige zeigen.

"reduzibel in $K[t]$ $\implies$ reduzibel in $R[t]$"
Sei $f \in K[t]$ reduzibel mit einer (echten) Zerlegung $f = g \cdot h \in K[t]$, wobei $\deg(g) \geq 1$ und $\deg(h) \geq 1$. Dann existieren kleinste gemeinsame Vielfache $a, b \in R \setminus \{0\}$ der Nenner der Koeffizienten der Polynome g bzw. h, so dass $ag, bh \in R[t]$. Damit besitzt abf in $R[t]$ eine Zerlegung

$$(ab)f = (ag) \cdot (bh).$$

Ist $(ab) \in R^*$, so ist bereits eine Zerlegung von f in $R[t]$ gefunden. Im anderen Fall muss jeder Primfaktor von $ab \in R$ das Produkt $(ag) \cdot (bh)$ und damit einen der beiden Faktoren teilen. In diesem Fall können wir die Gleichung durch den Primfaktor teilen, ohne $R[t]$ zu verlassen. Iterieren wir dieses Argument, indem wir nacheinander alle (Assoziiertheitsklassen von) Primfaktoren

der (wegen Faktorialität von R eindeutigen) Primfaktorzerlegung von ab abarbeiten, so wurde die Gleichung am Ende durch alle Primfaktoren von ab geteilt und wir haben eine Zerlegung

$$f = g_{neu} h_{neu} \in R[t]$$

erhalten mit $\deg(g_{neu}) = \deg(g)$ und $\deg(h_{neu}) = \deg(h)$. Es handelt sich daher um eine nicht-triviale Zerlegung von f in $R[t]$ und somit ist f reduzibel in $R[t]$.

"prim in $K[t]$ $\implies$ prim in $R[t]$"
Sei $f \in R[t]$ derart, dass es aufgefaßt als Element von $K[t]$ prim ist. Seien $g, h \in R[t]$, so dass das Produkt $g \cdot h \in R[t]$ von f geteilt wird.
Dann ist f offensichtlich auch Teiler dieses Produktes, aufgefaßt in $K[t]$. Da f prim in $K[t]$ ist, teilt f einen der beiden Faktoren, sagen wir g, d.h. es existiert ein $f_1 \in K[t]$ mit $f \cdot f_1 = g$. Dann existieren gemäß Lemma 5.3.9 $c, k \in K$ und $f_2, g_1 \in R[t]$, so dass f_2 und g_1 primitiv sind und $f_1 = k \cdot f_2$ sowie $g = c \cdot g_1$ gilt. Dabei ist insbesondere $c \in R$ nach 5.3.10, da $g \in R[t]$. Dann gilt

$$f \cdot f_2 \cdot \frac{k}{c} = g_1,$$

wobei $f \cdot f_2$ als Produkt zweier primitiver Polynome nach 5.3.8 wieder primitiv ist und damit $\frac{k}{c}$ nach 5.3.11 ein Element von R^*, Daher ist f in $R[t]$ Teiler von g_1 und dann (wegen $c \in R$) auch von $g = c \cdot g_1$.

□

Bemerkung 5.3.13 *Im vorangehenden Beweis haben wir für die Richtung "$\implies$" nur die Voraussetzung benutzt, dass f nicht konstant ist, nicht aber die Primitivität. Für die andere Richtung "$\impliedby$" haben wir dann die Primitivität verwendet, aber nicht die Voraussetzung, dass das Polynom nicht konstant ist. Die einzelnen Richtungen gelten also auch unter jeweils passend abgeschwächten Bedingungen.*

Satz 5.3.14 *(Lemma von Gauß) Ist R faktorieller Ring, so ist auch $R[t]$ faktoriell.*

An dieser Stelle erinnern wir uns noch kurz, dass Polynomringe in einer Variable über Körpern stets euklidische Ringe sind und als solche auch faktorielle Ringe. Dies nutzen wir im Beweis aus.

Beweis: Sei $g \in R[t] \setminus (\{0\} \cup R^*)$ und bezeichne K den Quotientenkörper $Quot(R)$. Zerlege nun mittels Bemerkung 5.3.10 g in ein Produkt

$$g = \alpha \cdot f$$

mit $\alpha \in R$ und $f \in R[t]$ primitiv. Dann besitzt f als Element des faktoriellen Ringes $K[t]$ eine Zerlegung in Primelemente

$$f = \prod_{i=1}^{s} q_i,$$

wobei $s \in \mathbb{N}$ und $q_1, \ldots, q_s \in K[t]$ prim. Für jeden Index i, $1 \leq i \leq s$, können wir nun nach Lemma 5.3.9 ein $c_i \in K$ und ein primitives Polynom $p_i \in R[t]$ mit $q_i = c_i \cdot p_i$ finden. Dabei sind q_i und p_i in $K[t]$ assoziiert, so dass auch p_i ein Primelement in $K[t]$ ist. Nach Satz 5.3.12 sind die p_i damit auch Primelemente in $R[t]$. Da die einzelnen p_i primitiv sind, ist es nach Lemma 5.3.8 auch ihr Produkt. In der Gleichung

$$f = \left(\prod_{i=1}^{s} c_i \right) \cdot \left(\prod_{i=1}^{s} p_i \right)$$

sind somit beiden Polynome primitiv, weswegen der Faktor $c := \prod_{i=1}^{s} c_i \in K$ nach Lemma 5.3.11 bereits in $R^* \subseteq R$ liegen muss. Damit besitzt c und dann auch $c \cdot \alpha$ ein Zerlegung als Produkt von Primfaktoren nach der Faktorialität von R, wobei jeder dieser Faktoren nach Korollar 5.3.3 auch prim als Element von $R[t]$ ist. Somit haben wir durch die beiden Primfaktorzerlegungen bereits eine Zerlegung von $g = \alpha \cdot f$ in Primfaktoren erhalten. $R[t]$ ist folglich ein faktorieller Ring.

□

Mit dieser Aussage ist die Bringschuld aus Bemerkung 3.2.12 nun abgetragen und wir haben endlich beweisen, dass z.B. $\mathbb{Z}[t]$ und $\mathbb{Q}[x_1, \ldots, x_n]$ faktorielle Ringe sind.

5.4 Irreduzibilitätskriterien

Auch wenn wir bereits wichtige Aussagen über Irreduzibilität und über Faktorialität in diesem Kapitel beweisen konnten, haben wir immer noch keine praxistaugliche Möglichkeit, die Irreduzibilität eines Polynoms zu überprüfen. Natürlich kann man in kleinen Graden einfach einen Ansatz (bzw. mehrere je nach möglichen Ausspaltungen des Grades des Polynoms) machen und dann durch Koeffizientenvergleich versuchen zu Ergebnissen zu kommen. Dieses Vorgehen 'mit der Brechstange' ist aber sehr umständlich und oft nicht zielführend. Daher betrachten wir nun Kriterien, die uns Irreduzibilität entscheiden lassen.

Sei in diesem Abschnitt stets R ein faktorieller Ring mit Quotientenkörper $K = Quot(R)$. Sei $p \in R$ ein Primelement und bezeichne $\pi_p : R \longrightarrow R/\langle p\rangle$ die kanonische Restklassenabbildung und 'by abuse of notation' auch die kanonische Restklassenabbildung $\pi_p : R[t] \longrightarrow (R/\langle p\rangle)[t]$. Beachten Sie dabei die Isomorphie aus 5.3.2,b). Vor diesem Hintergrund ist die doppelte Nutzung derselben Bezeichnung ungefährlich.

Satz 5.4.1 *(Reduktionskriterium) Seien R, K und p wie gerade beschrieben und sei $f \in R[t]$ ein primitives Polynom vom Grad $n \geq 1$ mit $p \nmid LC(f)$. Dann gilt:*

$$\pi_p(f) \text{ irreduzibel in } (R/\langle p\rangle)[t] \Longrightarrow f \text{ irreduzibel in } R[t].$$

Beweis: Ist $f \in R[t]$ reduzibel, so gibt es $g, h \in R[t]$ mit $f = g \cdot h$. Da f primitiv ist, kann weder g noch h vom Grad Null sein, so dass gilt $1 \leq \deg(g), \deg(h) < n$. Da p kein Teiler von $LC(f)$ ist und es sich bei π_p um einen Ringhomomorphismus handelt, gilt ausserdem

$$\deg(\pi_p(g)) + \deg(\pi_p(h)) = \deg(\pi_p(f)) = \deg(f) = \deg(g) + \deg(h),$$

so dass es sich bei $\pi_p(g)$ und $\pi_p(h)$ um echte Teiler von $\pi_p(f)$ vom gleichen Grad wie g bzw. h handeln muss. Daher ist auch $\pi_p(f)$ reduzibel, was die Behauptung beweist.

□

Satz 5.4.2 *(Transformationskriterium) Seien R und K wie zuvor, sei $f \in R[t]$ ein nicht-konstantes Polynom und sei $a \in R$. Dann gilt:*

$$f \text{ irreduzibel} \iff f(t+a) \text{ irreduzibel}.$$

Beweis: Offensichtlich ist

$$\begin{array}{rcl} \Phi_a : R[t] & \longrightarrow & R[t] \\ f(t) & \longmapsto & f(t+a) \end{array}$$

ein Ringisomorphismus mit Inverser Φ_{-a}. Daher bleibt Irreduzibilität unter der Abbildung sowie ihrer Inversen erhalten.

□

Satz 5.4.3 *(Kriterium von Eisenstein) Seien R und K wie zuvor und sei $f = \sum_{i=0}^{n} a_i t^i \in R[t]$ primitiv vom Grad $n \in \mathbb{N}$. Existiert ein Primelement $p \in R$ mit*

(i) $p \nmid a_n$

(ii) $p \mid a_i \ \ \forall 0 \leq i < n$

(iii) $p^2 \nmid a_0$,

dann ist f irreduzibel in $R[t]$.

Beweis: Beginnen wir den Beweis mit einer Erinnerung: In einem Produkt zweier Polynome in einem nullteilerfreien Ring ist der von Null verschiedene Term kleinsten Grades das Produkt der von Null verschiedenen Terme kleinsten Grades der Faktoren.
Nun beginnen wir mit dem Beweis: Angenommen ein primitives $f \in R[t]$ erfüllt die Bedingungen (i),(ii) und (iii), ist aber reduzibel mit der nichttrivialen Zerlegung $f = g \cdot h$, wobei wegen der Primitivität von f $1 \leq \deg(g), \deg(h) < n$.
Betrachten wir nun $[LC(f)]_p t^n \overset{(i),(ii)}{=} \pi_p(f) = \pi_p(g) \cdot \pi_p(h)$. Wegen der Nullteilerfreiheit von $R/\langle p \rangle$, wegen der Gestalt von $\pi_p(f)$ und wegen der Erinnerung zu Beginn des Beweises sind die Bilder von g und h unter der Restklassenabbildung von der Gestalt $\pi_p(g) = [LC(g)]_p t^m \neq [0]_p$ und $\pi_p(h) = [LC(h)]_p t^s \neq [0]_p$ für geeignete $m, s \in \{1, \ldots, n-1\}$ mit $n = m + s$. Insbesondere sind damit die konstanten Terme von g und h beide durch p teilbar, weswegen p^2 Teiler von a_0 ist im Widerspruch zu (iii). Die Annahme war also falsch und das Kriterium ist damit bewiesen.

□

Bemerkung 5.4.4 *Ist ein $f \in R[t]$ von positivem Grad irreduzibel, so ist es auch irreduzibel als Element in $K[t]$ nach Bemerkung 5.3.13. In diesem Sinne können die obigen Kriterien auch (durch einen Umweg über $R[t]$) als Kriterien für Irreduzibilität in $K[t]$ eingesetzt werden.*

Anwendung 5.4.5 *Für jede Primzahl $p \in \mathbb{N}$ ist das p-te* **zyklotomische Polynom** *(oder p-te* **Kreisteilungspolynom***)*

$$F_p = \frac{t^p - 1}{t - 1} = \sum_{i=0}^{p-1} t^i$$

in $\mathbb{Z}[t]$ irreduzibel und damit auch in $\mathbb{Q}[t]$.

Beweis: $R = \mathbb{Z}$ hat als Quotientenkörper $K = \mathbb{Q}$, so dass wir uns in der allgemeinen Situation dieses Abschnitts befinden.
Nun wissen wir nach dem Transformationskriterium, dass $F_p(t)$ genau dann irreduzibel in $\mathbb{Z}[t]$ ist, wenn auch $F_p(t+1)$ dies ist. Wir rechnen

$$F_p(t+1) = \frac{(t+1)^p - 1}{(t+1) - 1} = t^{p-1} + \sum_{i=1}^{p-2} a_i t^i + p,$$

wobei nach dem Binomischen Lehrsatz alle Koeffizienten außer $LC(F_p)$ durch p teilbar sind, aber der konstante Term nicht durch p^2 teilbar ist. Damit ist $F_p(t+1)$ irreduzibel in $\mathbb{Z}[t]$, was dann die Irreduzibilität von $F_p(t)$ in $\mathbb{Z}[t]$ und damit auch in $\mathbb{Q}[t]$ beweist.

□

Kapitel 6

Körpererweiterungen

In den vorigen Kapiteln hatten wir immer wieder gesehen, wie aus einem Ring weitere Ringe konstruiert wurden, etwa Polynomringe über Ringen und Körpern oder Faktorringe, aber auch die Konstruktion des Quotientenkörpers. In bestimmten Fällen entstanden durch diese Konstruktionen neue Körper, die andere Körper enthielten. In solche Situationen wird dieses Kapitel mehr Struktur bringen, etwa durch Begriffe wie algebraische und transzendente Körpererweiterungen oder Primkörper, die in vielen Kontexten (auch über diese Vorlesung hinaus) von Bedeutung sind.

6.1 Grundlegende Definitionen

Zu Beginn des Kapitels betrachen wir 'Unterkörper', die in der Regel als Teilkörper bezeichnet werden, aber strukturell in derselben Weise gebildet werden wie Untergruppen für Gruppen, Untervektorräume für Vektorräume und Unterringe für Ringe. Versuchen Sie einmal, ein Unterkörperkriterium selbst aufzustellen. Dann wissen Sie, ob Sie die allgemeine Idee hinter solchen Unterstrukturen und Unterstrukturkriterien verstanden haben.

Definition 6.1.1 *Sei $(K, +_K, \cdot_K)$ ein Körper und sei $k \subseteq K$ eine nichtleere Teilmenge von K. k heißt* **Teilkörper** *von K, falls $(k, +_K, \cdot_K)$ ein Körper ist. In diesem Fall heißt $K \supseteq k$ eine* **Körpererweiterung** *und K ein* **Erweiterungskörper** *von k.*

Bemerkung 6.1.2 *Ist $k \subseteq K$ eine Körpererweiterung, d.h. ist $(k, +_K, \cdot_K)$ ein Teilkörper von K, so trägt K in natürlicher Weise die Struktur eines k-*

Vektorraums. $(K, +_K)$ *ist wegen der Körpereigenschaften eine abelsche Gruppe, die Skalarmultiplikation ist die Einschränkung der multiplikativen Verknüpfung* $\cdot_K$ *des Körpers auf Elemente von* k *im ersten Argument. Die für einen Vektorraum zugrunde gelegten Eigenschaften der Skalarmultiplikation sind dann direkte Folge der Körpereigenschaften (Nachrechnen!).*
Betrachen wir genau, welche Eigenschaften des Körpers K *für die Vektorraumstruktur über* k *benötigt werden und welche nicht, so zeigt sich, dass bereits ein Integritätsring* R*, der einen Körper* k *enthält, in natürlicher Weise eine Vektorraumstruktur über* k *trägt.*

Definition 6.1.3 *Sei* $k \subseteq K$ *eine Körpererweiterung. Dann heißt die Zahl*

$$[K : k] := \dim_k(K) \in \mathbb{N} \cup \{\infty\}$$

der **Grad der Körpererweiterung** $K \supseteq k$*. Ist* $[K : k]$ *endlich, so spricht man von einer* **endlichen** *Körpererweiterung, andernfalls von einer* **unendlichen** *Körpererweiterung.*

Bemerkung 6.1.4 *Natürlich kann man Körpererweiterungen auch mehrfach nacheinander antreffen. Sind* $k \subseteq L \subseteq K$ *Körpererweiterungen, so nennt man* L *auch einen* **Zwischenkörper** *der Körpererweiterung* $k \subseteq K$*. Gilt sogar* $k \subsetneq L \subsetneq K$*, so spricht man von einem* **echten** *Zwischenkörper.*

Betrachtet man die obige Definition des Grades einer Körpererweiterung als Vektorraumdimension, so stellt sich relativ direkt die Frage, wie sich diese im Falle eines Körperturms wie in der Bemerkung verhält. Eigentlich ist das lediglich eine Anwendung von Linearer Algebra, aber aufgrund der Bedeutung des Satzes verdient er tatschlich den Namen 'Satz'.

Satz 6.1.5 *Sei* $k \subseteq K$ *eine Körpererweiterung mit Zwischenkörper* L*, d.h.* $k \subseteq L \subseteq K$*. Dann gilt:*

$$[K : k] = [K : L][L : k].$$

Insbesondere sehen wir in dem Satz, dass $[K : k]$ genau dann endlich ist, wenn $[K : L]$ und $[L : k]$ beide endlich sind.

Beweis: Zum Beweis der Dimensionsformel werden wir eine Basis von K als k-Vektorraum aus Basen von K als L-Vektorraum und L als k-Vektorraum

konstruieren. Damit folgt die gewünschte Dimensionsaussage direkt.

Schritt 1: Konstruktion eines Erzeugendensystems
Seien $(a_i)_{i\in I}$ eine Basis von L als k-Vektorraum und $(b_j)_{j\in J}$ eine Basis von K als L-Vektorraum. Sei außerdem $v \in K$ ein beliebiges Element von K. Dann gibt es ein $s \in \mathbb{N}_0$, $j_1, \ldots, j_s \in J$ und $\lambda_1, \ldots, \lambda_s \in L$, so dass

$$v = \sum_{i=1}^{s} \lambda_i b_{j_i}.$$

Für jedes $\lambda_i \in L$ gibt es ausserdem ein $r_i \in \mathbb{N}_0$, $m_1, \ldots, m_{r_i} \in I$ und $\mu_{i,1}, \ldots, \mu_{i,r_i} \in k$, so dass

$$\lambda_i = \sum_{t=1}^{r_i} \mu_{i,t} a_{m_t}.$$

Setzen wir diese in den Ausdruck für v ein, so erhalten wir:

$$v = \sum_{i=1}^{s} \left(\sum_{t=1}^{r_i} \mu_{i,t} a_{m_t} \right) b_{j_i} = \sum_{i=1}^{s} \sum_{t=1}^{r_i} \underbrace{\mu_{i,t}}_{\in k} \left(a_{m_t} b_{j_i} \right).$$

Damit lässt sich also jedes Element von K als k-Linearkombination von Elementen der Familie $(a_m b_j)_{j\in J, m\in I}$ schreiben. Diese Familie ist somit ein Erzeugendensystem von K als k-Vektorraum.

Schritt 2: Lineare Unabhängigkeit
Sei nun

$$\sum_{i\in I_0, j\in J_0} \lambda_{i,j} \left(a_i b_j \right) = 0$$

mit endlichen Teilmengen $I_0 \subseteq I$ und $J_0 \subseteq J$ sowie Koeffizienten $\lambda_{i,j} \in k$ eine k-Linearkombination der Null. Dann liefert eine andere Zusammenfassung der Summe:

$$0 = \sum_{j\in J_0} \underbrace{\left(\sum_{i\in I_0} \lambda_{i,j} a_i \right)}_{\in L} b_j,$$

so dass die lineare Unabhängigkeit der b_j über L sicherstellt, dass für jedes $j \in J_0$ gilt:

$$0 = \sum_{i\in I_0} \lambda_{i,j} a_i.$$

Für jede dieser Summen liefert aber die Lineare Unabhängigkeit der a_i über k, dass die Linearkombination trivial sein muss. Damit sind alle $\lambda_{i,j} = 0$, was für die Lineare Unabhängigkeit des in Schritt 1 gefundenen Erzeugendensystems zu zeigen war.

Schritt 3: Behauptung des Satzes
Die gefundene Basis $(a_i b_j)_{i \in I, j \in J}$ ist eine Familie, deren Indizes gerade die Paare $(i, j) \in I \times J$ sind. Sie besitzt also $\#I \cdot \#J$ Elemente, wie es die Behauptung des Satzes aussagt.

□

Direkt aus der Definition des Grades einer Körpererweiterung bzw. aus dem obigen Satz 6.1.5 kann man noch weitere wichtige Eigenschaften des Grades von Körpererweiterungen folgern:

Lemma 6.1.6 *Seien $k \subseteq L$ und $L \subseteq K$ Körpererweiterungen und sei $[K : k] < \infty$. Dann gilt:*

a) $[K : L] = 1 \iff K = L$

b) $[K : k] = [L : k] \iff K = L$

c) Ist $[K : k]$ prim, so gilt $K = L$ oder $L = k$.

Aussage c) des Lemmas genügt, um zu zeigen, dass es keinen echten Zwischenkörper von $\mathbb{R} \subseteq \mathbb{C}$ gibt. Warum?

Beweis:

a) Ist $[K : L] = 1$, so hat K eine einelementige Basis als L-Vektorraum und ist somit isomorph zu L^1. Da $L \subseteq K$ ein Teilkörper ist, kann $1_L = 1_K$ als dieses Basiselement gewählt werden. Sind umgekehrt die Körper gleich, so ist $K = L^1$ von L-Vektorraumdimension 1.

b) Nach dem obigen Satz 6.1.5 gilt $[K : k] = [K : L][L : k]$. Daher gilt (mittels Kürzen des gemeinsamen ganzzahligen Faktors in der Gleichung) $[K : k] = [L : k]$ genau dann, wenn $1 = [K : L]$, was nach a) genau für $K = L$ erfüllt ist.

c) Ist $[K : k] = p$ prim, so gilt auch hier nach dem Satz 6.1.5 $p = [K : k] = [K : L][L : k]$, wobei p einen der beiden Faktoren teilen muss. Der andere Faktor ist dann offensichtlich 1, womit gerade folgt, dass $K = L$ oder $L = k$.

□

Proposition 6.1.7 *Sei R ein Integritätsring, $K = Quot(R)$ und L ein beliebiger Körper mit $R \subseteq L$. Dann existiert ein injektiver Körperhomomorphismus $\varphi : K \longrightarrow L$ mit $\varphi(a) = a$ für alle $a \in R$.*

Beweis: Offensichtlich stimmt φ auf R mit der Inklusion $\iota : R \hookrightarrow L$ überein. Insbesondere sind damit $0_R = 0_L$ und $1_R = 1_L$.

Schritt 1: Definition von φ
Setze

$$\varphi(\frac{a}{b}) := \frac{\iota(a)}{\iota(b)}$$

für $a, b \in R$ mit $b \neq 0$. Zum Nachweis der Wohldefiniertheit der Abbildung betrachten wir zwei Repräsentanten $\frac{a}{b}, \frac{c}{d}$ mit $a, b, c, d \in R$, $b \neq 0 \neq d$, desselben Elementes $f \in K$. Es gilt also $ad - bc = 0_R$ und somit nach

$$\begin{aligned} 0_L &= \iota(0_R) \\ &= \iota(ad - bc) \\ &= \iota(a)\iota(d) - \iota(b)\iota(c) \\ &= \varphi(a)\varphi(d) - \varphi(b)\varphi(c). \end{aligned}$$

Daher repräsentieren auch $\frac{\varphi(a)}{\varphi(b)}$ und $\frac{\varphi(c)}{\varphi(d)}$ dasselbe Element von L, weswegen φ mit obiger Zuweisung wohldefiniert ist.

Schritt 2: Homomorphismuseigenschaft von φ
Da schon nach Voraussetzung $\varphi(1_R) = \iota(1_R) = 1_R = 1_L$ gilt, müssen wir lediglich die Verträglichkeit mit der Addition und Multiplikation betrachten: Seien $f, g \in K$ repräsentiert durch $f = \frac{a}{b}$ und $g = \frac{c}{d}$ mit $a, b, c, d \in R$,

$b \neq 0 \neq d$. Wir rechnen

$$\begin{aligned}
\varphi(f+g) &= \varphi(\frac{ad+bc}{bd}) \\
&= \frac{\iota(a)\iota(d)+\iota(b)\iota(c)}{\iota(b)\iota(d)} \\
&= \frac{\iota(a)}{\iota(b)} + \frac{\iota(c)}{\iota(d)} \\
&= \varphi(\frac{a}{b}) + \varphi(\frac{c}{d}) \\
&= \varphi(f) + \varphi(g) \\
\varphi(fg) &= \varphi(\frac{ac}{bd}) \\
&= \frac{\iota(a)\iota(c)}{\iota(b)\iota(d)} \\
&= \frac{\iota(a)}{\iota(b)} \cdot \frac{\iota(c)}{\iota(d)} \\
&= \varphi(\frac{1}{b})\varphi(\frac{c}{d}) \\
&= \varphi(f)\varphi(g)
\end{aligned}$$

Schritt 3: Injektivität von φ
Seien $f, g \in K$, repräsentiert durch $f = \frac{a}{b}$ und $g = \frac{c}{d}$ mit $a, b, c, d \in R$, $b \neq 0 \neq d$, zwei Elemente mit gleichem Bild unter φ. Dann gilt:

$$0_R = 0_L = \varphi(f-g) = \varphi(\frac{ad-bc}{bd}),$$

weswegen auch $ad - bc = 0_R$ gelten muss. Daher sind die beiden Brüche Repräsentanten derselben Klasse, d.h. $f = g$.

□

Korollar 6.1.8 *Seien R, K, L wie in der vorigen Proposition. Dann enthält L eine isomorphe Kopie von K. Insbesondere ist K bis auf Isomorphie der kleinste Körper, der R enthält.*

Beweis: Betrachte erneut die Abbildung φ aus dem Satz. Dann gilt nach dem Homomorphiesatz:

$$K = K/\ker(\varphi) \cong \mathrm{Im}(\varphi).$$

Die zweite Aussage ist dann offensichtlich, da jeder solche Körper eine isomorphe Kopie von K enthalten muss.

□

Definition 6.1.9 *Sei K ein Körper (mit mindestens 2 Elementen). Die Menge*

$$P_K := \bigcap_{\substack{T \subseteq K \\ T \text{ Teilkörper}}} T$$

heißt der **Primkörper** *von K.*

Haben Sie es gemerkt? In der Definition sind 2 Behauptungen versteckt, die bewiesen werden müssen: zuerst ist zu zeigen, dass P_K überhaupt ein Körper ist, danach muss geklärt werden, dass P_K bei gegebenem K eindeutig bestimmt ist. Das ist der Inhalt des folgenden Beweises:
Beweis: P_K ist nicht leer, da 0_K und $1_K \neq 0_K$ in jedem Teilkörper von K liegt.
Sind $a, b \in P_K$ so liegen sie in jedem der Teilkörper von K und damit liegen auch deren Summe, Produkt und Inverse bzgl. Addition sowie (für von Null verschiedene Elemente) auch die multiplikativen Inversen von a und b in jedem der Teilkörper. Damit liegen sie auch in P_K und P_K ist nach Untergruppenkriterium angewandt auf $(P_K, +_K)$ und $(P_K \setminus \{0\}, \cdot_K)$ ein Körper.
Sind P_1 und P_2 zwei Körper, die der Definition eines Primkörpers von K entsprechen, so muss für den Primkörper P_1 gelten $P_1 \subseteq P_2$ und umgekehrt für den Primkörper P_2 auch $P_2 \subseteq P_1$. Die beiden Körper sind also gleich, was die Eindeutigkeit des Primkörpers beweist.

□

Satz 6.1.10 *Sei K ein Körper (mit mindestens 2 Elementen) und sei $P_K \subseteq K$ der zugehörige Primkörper. Dann gilt*

a) $char(K) = p > 0 \iff P_K \cong \mathbb{Z}/\langle p \rangle$

b) $char(K) = 0 \iff P_K \cong \mathbb{Q}$

Beweis: Erinnern wir uns an die Definition der Charakteristik eines Integritätsrings (was natürlich auch jeder Körper ist): $char(R)$ ist nicht-negativer

Erzeuger des Ideals $\ker(\chi)$ für den Ringhomomorphismus $\chi : \mathbb{Z} \longrightarrow R$ mit $\chi(1) = 1_R$. Nach dem Homomorphiesatz gilt:

$$\mathbb{Z}/\ker(\chi) \cong \mathrm{Im}(\chi) \subseteq K.$$

Ist χ injektiv, so befinden wir uns in der Situation von Proposition 6.1.7 und K enthält wegen $\mathbb{Z} \subseteq K$ auch $Quot(\mathbb{Z}) = \mathbb{Q}$.
Ist χ nicht injektiv, so ist $\ker(\chi)$ wegen der Nullteilerfreiheit des Körpers K ein Primideal, d.h. es gibt ein $p \in \mathbb{Z}$, prim, mit $\ker(\chi) = \langle p \rangle$ und $char(K) = p$. Damit enthält K gerade den gewünschten Körper entsprechend der Charakteristik. Da jeder Teilkörper L von K die 1_K und damit auch alle Summen $\sum_{i=1}^{r} 1_k$ enthält, enthält er auch als Unterring $\mathbb{Z}$ (im Falle von Charakteristik Null) bzw. $\mathbb{Z}/\langle p \rangle$ (im Falle von Charakteristik p) und damit nach 6.1.7 auch den zugehörigen Quotientenkörper dieses Ringes, was zeigt, dass es sich bei diesen Körpern wegen Minimalität um Primkörper handelt.
Enthält K umgekehrt einen dieser Primkörper, so ist dadurch schon die Charakteristik bestimmt, da dann der Kern von χ bekannt ist.

□

Haben Sie bemerkt, dass der Satz auch aussagt, dass es außer $\mathbb{Z}/\langle p \rangle$ mit p prim und $\mathbb{Q}$ keine Primkörper gibt.

Satz 6.1.11 *Sei K ein Körper mit genau $q \in \mathbb{N}$ Elementen. Dann gibt es eine Primzahl $p \in \mathbb{Z}$ und eine natürliche Zahl d, so dass $char(K) = p$ und $q = p^d$.*

Beweis: Sei P_K der Primkörper von K. Da K nicht unendlich ist, muss auch P_K endlich sein, weswegen $char(K) = p$ für eine Primzahl p.
Auch $d = [K : P_K]$ muss endlich sein, da K nur endlich viele Elemente enthält. Als Vektorraum der Dimension d über einem Körper mit p Elementen hat K dann genau p^d Elemente.

□

Damit haben wir eine gute Vorstellung davon, welche Anzahlen von Elementen bei endlichen Körpern vorkommen können. Wir würden sie aber auch gerne explizit beschreiben oder sogar aus Primkörpern konstruieren können. Dafür sollten wir uns zuerst an den Einsetzungshomomorphismus für Polynome – zugeschnitten auf unsere Situation – erinnern.

Erinnerung 6.1.12 *Sei $k \subseteq K$ eine Körpererweiterung und $\alpha \in K$. Dann ist α einsetzbar in Polynome aus $k[t]$ und der Einsetzungshomomorphismus ist*

$$\begin{array}{rcl} E_\alpha : k[t] & \longrightarrow & K \\ f = \sum_{i=0}^{n} a_i t^i & \longmapsto & \sum_{i=0}^{n} a_i \alpha^i = f(\alpha). \end{array}$$

Dabei wird $\mathrm{Im}(E_\alpha)$ mit $k[\alpha]$ bezeichnet und ist als Bild eines Ringhomomorphismus selbst ein Ring.

Lemma 6.1.13 *Sei $k \subseteq K$ eine Körpererweiterung und $\alpha \in K$. Dann gilt*

$$k[\alpha] = \bigcap_{\substack{k \leq R \leq K \text{ als Unterringe} \\ \alpha \in R}} R.$$

$k[\alpha]$ ist also der kleinste Unterring von K, der α und k enthält.

Beweis: Da $k[\alpha]$ ein Unterring von K ist, der k als Unterring und α als Element enthält, taucht $k[\alpha]$ bei den Ringen R auf. Daher ist der Durchschnitt in $k[\alpha]$ enthalten. Jeder Unterring von K, der k und α enthält muss wegen der Abgeschlossenheit unter Addition und Multiplikation auch jeden polynomialen Ausdruck in α mit Koeffizienten in k enthalten, was genau $\mathrm{Im}(E_\alpha) = k[\alpha]$ ist. Damit ist $k[\alpha]$ im Durchschnitt und die Behauptung ist bewiesen.

□

Notation 6.1.14 *Man sagt auch, dass $k[\alpha]$ der* **durch Adjunktion von α an** *k erzeugte Unterring von K ist.*

Definition 6.1.15 *Sei $k \subseteq K$ eine Körpererweiterung und $\alpha \in K$. Dann definieren wir*

$$k(\alpha) := Quot(k[\alpha]).$$

Lemma 6.1.16 *Sei $k \subseteq K$ eine Körpererweiterung und $\alpha \in K$. Dann gilt*

$$k(\alpha) = \bigcap_{\substack{k \leq T \leq K \text{ als Teilkörper} \\ \alpha \in T}} T.$$

Beweis: Jeder Teilkörper T von K, der k und α enthält, ist auch ein Unterring von K mit diesen Eigenschaften und enthält damit nach Lemma 6.1.13 auch $k[\alpha]$. Nach Proposition 6.1.7 enthält T damit auch $k(\alpha) = Quot(k[\alpha])$. Andererseits taucht $k(\alpha)$ offensichtlich in der Liste solcher T auf, womit die Behauptung bewiesen ist.

□

Notation 6.1.17 *Allgemeiner kann man für beliebige Teilmengen $A \subseteq K$ auch $k[A]$ bzw. $k(A)$ definieren als kleinster Unterring bzw. kleinster Teilkörper, der k und A enthält, also*

$$k[A] := \bigcap_{\substack{k \leq R \leq K \text{ als Unterringe} \\ A \subseteq R}} R \quad \textit{und} \quad k(A) := \bigcap_{\substack{k \leq T \leq K \text{ als Teilkörper} \\ A \subseteq T}} T.$$

Im Fall einer endlichen Menge $A = \{\alpha_1, \ldots, \alpha_n\}$ schreibt man in Verallgemeinerung der Adjunktion eines Elements auf endlich viele auch gerne $k[\alpha_1, \ldots, \alpha_n]$ bzw. $k(\alpha_1, \ldots, \alpha_n)$.

Betrachten wir einmal $k = \mathbb{Q}$ und die Elemente $\alpha = \sqrt{2}$ und $\beta = \pi$. Dann sagt uns schon die Intuition, dass hierbei $k(\alpha)$, also die Adjunktion einer Quadratwurzel, also der Lösung einer quadratischen Gleichung, an den Körper k andere Eigenschaften haben dürfte als die Adjunktion von β, das keine polynomiale Gleichung über $\mathbb{Q}$ erfüllt, wie wir alle zumindest in der Schule schonmal in einer Randbemerkung gehört hatten. Aber was macht den Unterschied, sofern einer besteht, dann aus? Damit befasst sich der folgende Abschnitt.

6.2 Algebraische und transzendente Erweiterungen

In diesem Abschnitt werden wir vornehmlich solche Körpererweiterungen betrachten, die von einem Element erzeugt werden und dabei Eigenschaften des Elements mit Eigenschaften des durch dessen Adjunktion entstandenen Ringes oder Körpers verbinden. Generell läßt sich unsere Situation also wie folgt darstellen:

$$\underbrace{k}_{\text{Körper}} \subseteq \underbrace{k[\alpha]}_{\text{Integritätsring}} \subseteq \underbrace{k(\alpha)}_{\text{Körper}} \subseteq \underbrace{K}_{\text{Körper}},$$

wobei gerade die beiden mittleren Objekte im Fokus der Überlegungen stehen.

Definition 6.2.1 *Eine Körpererweiterung $k \subseteq K$ heißt* **einfach**, *falls es ein $\alpha \in K$ gibt mit $K = k(\alpha)$. In diesem Fall nennt man α ein* **primitives Element** *der Körpererweiterung.*

Definition 6.2.2 *Sei $k \subseteq K$ eine Körpererweiterung und $\alpha \in K$. Dann heißt α* **algebraisch** *über k, falls es ein $f \in k[t] \setminus \{0\}$ gibt mit $f(\alpha) = 0$, andernfalls heißt α* **transzendent** *über k.*

Betrachten wir die Körpererweiterung $\mathbb{Q} \subseteq \mathbb{R}$, so ist $\sqrt{2}$ algebraisch über $\mathbb{Q}$, da es die Gleichung $t^2 - 2 = 0$ erfüllt. Die Transzendenz von e über $\mathbb{Q}$ wurde erstmals von Charles Hermite 1873 beweisen, die von π über $\mathbb{Q}$ wurde erstmals von Ferdinand von Lindemann 1882 gezeigt. David Hilbert lieferte 1893 einen weiteren, eleganteren Beweis, der aber noch immer vom Umfang her den Rahmen eines Randkommentars einer Vorlesung Algebra I sprengen würde, so dass wir an dieser Stelle darauf verzichten müssen.

Definition 6.2.3 *Eine Körpererweiterung $K \supseteq k$ heißt* **algebraisch**, *falls jedes Element von K algebraisch über k ist. Existiert ein Element von K, das transzendent über k ist, so heißt die Körpererweiterung* **transzendent**.

Bemerkung 6.2.4 *Eine transzendente Körpererweiterung $K \supseteq k$ kann natürlich in K Elemente enthalten, die algebraisch über k sind. Allein die Existenz eines transzendenten Elementes macht die Körpererweiterung schon transzendent. Ist jedes Element von $K \setminus k$ transzendent über k, so sagt man auch, dass $K \supseteq k$ eine rein transzendente Erweiterung ist. Darauf werden wir aber hier in der Vorlesung nicht im Detail eingehen.*

Nun haben wir für den am Ende des letzten Abschnitts mit einem Beispiel angedeuteten Unterschied der beiden Situationen das nötige Vokabular und können uns der Charakterisierung der Situationen zuwenden.

Satz 6.2.5 *Sei $K \supseteq k$ eine Körpererweiterung und sei $\alpha \in K \setminus k$. Dann gilt:*

a) Ist α transzendent über k, so gilt

$$k[\alpha] \cong k[t] \quad \textit{und} \quad k(\alpha) \cong k(t),$$

wobei $k[t]$ hier den Polynomring in einer Variable bezeichnet und $k(t)$ dessen Quotientenkörper.

b) Ist α algebraisch über k, so gilt

$$k[\alpha] = k(\alpha)$$

und es gibt ein normiertes, irreduzibles Polynom $f_{\alpha,k} \in k[t] \setminus k$ mit

$$k[\alpha] \cong k[t]/\langle f_{\alpha,k}\rangle.$$

Definition 6.2.6 *Das soeben eingeführte Polynom $f_{\alpha,k}$ bezeichnet man als* **Minimalpolynom** *von α über k.*

Bemerkung 6.2.7 *In Fall a) des obigen Satzes ist $k[\alpha]$ ein Integritätsring, der kein Körper ist. In Fall b) ist $k[\alpha] = k(\alpha)$ dagegen ein Körper (und als solcher natürlich immer noch ein Integritätsring).*

Beweis: Betrachte $E_\alpha : k[t] \longrightarrow k[\alpha]$. Nach dem Homomorphiesatz gilt

$$k[t]/\ker(E_\alpha) \cong \mathrm{Im}(E_\alpha) = k[\alpha].$$

Da $k[t]$ ein Hauptidealring ist und $\ker(E_\alpha)$ ein Ideal in $k[t]$, existiert ein Polynom $f \in k[t]$ mit $\ker(E_\alpha) = \langle f\rangle$.
Ist E_α injektiv, so erfüllt α keine polynomiale Gleichung über k, d.h. ist transzendent, und $f = 0$, d.h. $k[t] \cong k[\alpha]$. Damit sind auch die zugehörigen Quotientenkörper isomorph, was bereits a) beweist.
Ist E_α nicht injektiv, so ist $\ker(E_\alpha) = \langle f\rangle$ für ein Polynome $f \in k[t] \setminus \{0\}$, da $k[t]$ Hauptidealring ist, und α erfüllt damit die polynomiale Gleichung $f(\alpha) = 0$. Damit ist α algebraisch über k und wir befinden uns in b). Da $\mathrm{Im}(E_\alpha)$ als Unterring eines Körpers insbesondere Integritätsring sein muss, ist auch der nach Homomorphiesatz dazu isomorphe Ring $k[t]/\langle f\rangle$ Integritätsring, was nach Satz 4.6.11 impliziert, dass $k[t]/\langle f\rangle \cong k[\alpha]$ ein Körper und f prim und damit irreduzibel ist. Daher ist $f_{\alpha,k} := \frac{1}{LC(f)} f$ ist das gesuchte irreduzible normierte Polynom.

□

Bemerkung 6.2.8 *Das Minimalpolynom ist zu gegebener Körpererweiterung $K \supseteq k$ und gegebenem $\alpha \in K$ eindeutig bestimmt, da das Ideal $\ker(E_\alpha)$ von einem Element einer eindeutig bestimmten Assoziiertheitsklasse in $k[t]$ erzeugt wird und durch Normierung ein eindeutiger Repräsentant der Klasse festgelegt wird. Jedes andere Polynom $g \in k[t]$ mit $g(\alpha) = 0$ liegt in $\ker(E_\alpha) = \langle f_{\alpha,k}\rangle$ und ist somit ein Vielfaches von $f_{\alpha,k}$.*

Korollar 6.2.9 *Sei $K \supseteq k$ eine Körpererweiterung und sei $\alpha \in K$ algebraisch über k mit Minimalpolynom $f_{\alpha,k}$ vom Grad n. Dann ist $(1, \alpha, \ldots, \alpha^{n-1})$ eine Basis des k-Vektorraums $k[\alpha]$.*
Insbesondere ist dann $[k[\alpha] : k] = n = \deg(f_{\alpha,k})$.

Beweis: Wir wissen aus dem vorigen Satz, dass $k[\alpha] \cong k[t]/\langle f_{\alpha,k}\rangle$ ein Körper ist, wobei nach Voraussetzung dieses Lemmas $f_{\alpha,k} = t^n + g$ für ein geeignetes $g \in k[t]$ von Grad höchstens $n-1$. Damit ist $(1, t, \ldots, t^{n-1})$ eine Basis von $k[t]/\langle f_{\alpha,k}\rangle$ und deren Bild $(1, \alpha, \ldots, \alpha^{n-1})$ (unter dem Isomorphismus) eine Basis von $k[\alpha]$. Der Rest der Aussage läßt sich dann direkt aus den Daten ablesen.

□

Betrachten wir nun den Umgang mit einem algebraischen Element $\alpha \in K \setminus k$ in den beiden folgenden Bemerkungen etwas genauer:

Bemerkung 6.2.10 *(Rechnen in $k[\alpha]$)*
Auch wenn wir bereits wissen, dass $k[\alpha]$ ein Körper ist, haben wir wegen der abstrakten Herangehensweise an den Beweis der Tatsache bisher noch nicht konkret beschrieben, wie ein Element $\beta \in k[\alpha] \setminus \{0\}$ invertiert werden kann. Auch dazu verwenden wir wieder den Isomorphismus $k[t]/\langle f_{\alpha,k}\rangle \cong k[\alpha]$ und verwenden für β dessen eindeutigen Repräsentanten g vom Grad $\leq n-1$. Dann sind wegen der Irreduzibilität von $f_{\alpha,k}$ und wegen des niedrigeren Grades von g die beiden Polynome $f_{\alpha,k}$ und g teilerfremd in dem euklidischen Ring $k[t]$, so dass es nach der Bézout-Identität Elemente $x, y \in k[t]$ gibt mit

$$x \cdot g + y \cdot f_{\alpha,k} = 1.$$

Damit repäsentiert x die Klassen des Inversen von g in $k[t]/\langle f_{\alpha,k}\rangle$ und dessen Bild ist die gesuchte Inverse in $k[\alpha]$.

Bemerkung 6.2.11 *(Ausnutzen von $k(\alpha) = k[\alpha]$)*
Ein Element von $k(\alpha)$ ist nach unseren Überlegungen stets auch ein Element von $k[\alpha]$ und kann somit in der Basis $(1, \ldots, \alpha^{n-1})$ dargestellt werden. Konkret findet man die Basisdarstellung über Koeffizientenvergleich wie in folgendem Ansatz mit gesuchtem $\sum_{i=0}^{n-1} x_i \alpha^i$ zu gegebenem $\gamma = \frac{g(\alpha)}{h(\alpha)} \in k(\alpha)$ mit geeigneten $g(\alpha), h(\alpha) \in k[\alpha]$:

$$g(\alpha) = h(\alpha) \left(\sum_{i=0}^{n-1} x_i \alpha^i \right).$$

Satz 6.2.12 *Sei $k \subseteq K$ eine Körpererweiterung und sei $\alpha \in K$. Dann sind äquivalent:*

a) α *algebraisch über* k

b) $[k[\alpha] : k] < \infty$

c) $k[\alpha]$ *Körper*

d) $k[\alpha] = k(\alpha)$

Dies ist eine Zusammenfassung der Ergebnisse der letzten Sätze, Lemmata und Bemerkungen und bleibt hier deswegen ohne Beweis. Es ist allerdings instruktiv, sich konkret zu überlegen, welche Argumente dabei für welche Implikation verwendet werden müssen.

Satz 6.2.13 *Jede endliche Körpererweiterung ist algebraisch.*

Beweis: Sei $K \supseteq k$ eine Körpererweiterung und sei $\beta \in K$ transzendent über k, so enthält K insbesondere den Integritätsring $k[\beta]$, der isomorph zu einem Polynomring $k[t]$ über k ist. Die k-Vektorraumdimension von $k[t]$ ist jedoch nicht endlich, da z.B. $(t^i \mid i \in \mathbb{N}_0)$ eine unendliche Basis von $k[t]$ ist. Damit kann auch $K \supseteq k$ keine endliche Körpererweiterung sein.

□

Korollar 6.2.14 *Sei $K \supseteq k$ eine Körpererweiterung und seien $\alpha, \beta \in K$ algebraisch über k. Dann ist $k(\alpha, \beta)$ eine endliche (und damit algebraische) Körpererweiterung.*

Beweis: Betrachte $k \subseteq k[\alpha] \subseteq k[\alpha, \beta]$. Da α algebraisch über k ist, ist die erste Körpererweiterung endlich, also insbesondere ein endlicher k-Vektorraum. Da β algebraisch über k ist, ist es auch algebraisch über $k[\alpha]$, da es ja noch immer Nullstelle derselben polynomialen Gleichung ist (auch wenn das Minimalpolynom vielleicht ein anderes ist). Somit ist $k[\alpha, \beta]$ ein endlich-dimensionaler $k[\alpha]$-Vektorraum und damit nach Linearer Algebra auch ein endlich-dimensionaler k-Vektorraum.

□

Bemerkung 6.2.15 *Durch Iteration des vorigen Korollars gilt die analoge Aussage auch für endlich viele algebraische Elemente von K.*

Satz 6.2.16 *Seien $k \subseteq L \subseteq K$ Körpererweiterungen. Dann gilt:*

$$K \supseteq k \text{ algebraisch } \Longleftrightarrow K \supseteq L \text{ und } L \supseteq k \text{ algebraisch.}$$

Beweis: Die Implikation "$\Longrightarrow$" ist offensichtlich, denn damit ist jedes Element von K bereits algebraisch über k und unter Verwendung derselben Gleichung auch über dem Zwischenkörper L. Ausserdem ist jedes Element des Zwischenkörpers L algebraisch über k, da es als Element von K eine polynomiale Gleichung mit Koeffizienten in k erfüllt.
Ist umgekehrt für die Implikation "$\Longleftarrow$" ein $\alpha \in K$ gegeben, so erfüllt α als algebraisches Element über L eine polynomiale Gleichung mit Koeffizienten in L. Diese Gleichung besitzt nur endlich viele Koeffizienten, sagen wir $\beta_1, \ldots, \beta_s$, die alle algebraisch über k sind. Damit ist nach den vorangegangenen Sätzen

$$\begin{array}{lcl} \dim_k(k[\alpha]) & \leq & \dim_k(k[\alpha, \beta_1, \ldots, \beta_s]) \\ & \overset{Gradformel}{=} & \dim_{k[\beta_1,\ldots,\beta_s]}(k[\alpha, \beta_1, \ldots, \beta_s]) \cdot \dim_k(k[\beta_1, \ldots, \beta_s]) \\ & < & \infty. \end{array}$$

Nach den äquivalenten Beschreibungen für die Eigenschaft algebraisch, ist damit α algebraisch über k.

□

Ende des Stoffs für das Modul mat200

Anhang A

Anhang

Die Inhalte des Anhangs sind zwar nicht klausurrelevant, können aber zum Verständnis des Stoffes bzw. seiner Tragweite beitragen, da sie eine ganz wichtige Anwendung der modernen Algebra, die Kryptologie, kurz anreissen.

A.1 Eulersche ϕ-Funktion

In diesem Anhang werden wir nicht so weit in die Tiefe gehen, wie in den Kapiteln des Skripts, jedoch möchte ich gerade für die Hörer des Moduls mat200 die Chance nicht verstreichen lassen, eine Anwendung der Algebra zu besprechen: die Verschlüsselung von Daten mittels RSA-Verfahren. Dazu sind allerdings einige Grundlagen aus der Theorie der Gruppen notwendig, die eigentlich erst in der Algebra II behandelt werden.

Satz A.1.1 *(Lagrange – kommutativer Fall) Sei G eine endliche abelsche Gruppe mit $|G| = n$ Elementen und sei $U \subseteq G$ eine Untergruppe. Dann gilt*

$$|G/U| \cdot |U| = n.$$

Beweis: Wir betrachten den Restklassenhomomorphismus

$$\pi : G \longrightarrow G/U,$$

dessen Kern gerade $\ker(\pi) = U$ ist. Sei nun $\mathcal{O}$ ein Repräsentantensystem von G/U, so ist die Anzahl der Restklassen $|G/U|$ gleich der Anzahl der Elemente von $\mathcal{O}$. Jede Äquivalenzklasse $[a]_U = a + U$ für ein $a \in \mathcal{O}$ hat andererseits genau $|U|$ Elemente. Damit gilt:

$$n = |G| = |G/U| \cdot |U|.$$

□

Korollar A.1.2 *Sei $(G, \cdot)$ eine endliche abelsche Gruppe mit $|G| = n$ Elementen. Dann gilt:*

$$\forall g \in G : \quad g^n = e_G.$$

Beweis: Betrachte zu einem beliebigen gegebenen $g \in G$ die Menge $U = \{g^i \mid i \in \mathbb{Z}\}$. Da $1_G = g^0 \in U$ und $g^i \cdot g^{-j} = g^{i-j} \in U$ für beliebige $i, j \in \mathbb{Z}$, erfüllt U das Untergruppenkriterium. Ausserdem muss es wegen der Endlichkeit von G und damit auch U ein kleinstes nicht-negatives r geben mit $g^r = g^0 = 1_G$. Nach den Rechenregeln für Gruppen impliziert das auch $g^i = g^{i \bmod r}$ für alle $i \in \mathbb{Z}$ und somit ist $|U| = r$. Nach Satz A.1.1 ist dann r Teiler von n und damit $g^n = g^0 = 1_G$.

□

Betrachten wir nun eine spezielle Klasse von Gruppen, die Einheitengruppen $(\mathbb{Z}/m\mathbb{Z})^*$ der Ringe $\mathbb{Z}/m\mathbb{Z}$:

Definition A.1.3 *Sei $m \in \mathbb{N}$. Dann ist die Eulersche ϕ-Funktion definiert als*

$$\begin{array}{rcl} \phi : \mathbb{N} & \longrightarrow & \mathbb{N} \\ m & \longmapsto & |\,(\mathbb{Z}/m\mathbb{Z})^*\,| = |\{1 \leq a \leq m \mid \mathrm{ggT}(a, m) = 1\}| \end{array}$$

Satz A.1.4 *(Euler) Sei $m \in \mathbb{N}$. Dann gilt*

$$a^{\phi(m)} \equiv 1 \bmod m \quad \forall a \in \mathbb{Z} \text{ mit } \mathrm{ggT}(a, m) = 1.$$

Beweis: Da $\phi(m)$ genau die Anzahl der Elemente in $(\mathbb{Z}/m\mathbb{Z})^*$ ist, ist dieser Satz ein direktes Korollar zu der Aussage direkt davor.

□

Satz A.1.5 *(Kleiner Satz von Fermat) Sei p eine Primzahl und $a \in \mathbb{Z}$. Dann gilt:*

$$a^p \equiv a \bmod p.$$

Ist $a \in \mathbb{Z}$ und p kein Teiler von a, so gilt insbesondere

$$a^{p-1} \equiv 1 \bmod p.$$

Beweis: Die zweite Aussage ist gerade der Satz von Euler, da jedes nicht durch p teilbare Element eine Restklasse aus $(\mathbb{Z}/p\mathbb{Z})^*$ repräsentiert.
Multipliziert man die zweite Aussage mit a, was nach Voraussetzung der zweiten Aussage nicht Null ist, so erhält man die erste Aussage für alle $a \in \mathbb{Z} \setminus p\mathbb{Z}$. Für Vielfache von p ist die Aussage trivial erfüllt.

□

Satz A.1.6 *Die Eulersche ϕ-Funktion besitzt folgende Eigenschaften:*

a) Für eine Primzahl p und ein $a \in \mathbb{N}$ gilt:

$$\phi(p^a) = p^a - p^{a-1} = p^a \cdot (1 - \frac{1}{p}).$$

b) Sind $n, m \in \mathbb{Z}$ teilerfremd, so gilt

$$\phi(mn) = \phi(m)\phi(n).$$

Beweis:

a) Es gibt genau p^a ganze Zahlen $0 \leq z < p^a$. Davon sind genau die Zahlen der Form $z = p \cdot m$ mit $0 \leq (p \cdot m) < (p \cdot p^{a-1})$ durch die Primzahl p teilbar, wobei dann für m offensichtlich $0 \leq m < p^{a-1}$ gilt. Also gibt es

$$p^a - p^{a-1} = p^a \cdot (1 - \frac{1}{p})$$

zu p teilerfremde Zahlen zwischen 0 und p^a ,was zu zeigen war.

b) Nach dem Chinesischen Restsatz wissen wir, dass

$$\mathbb{Z}/\langle mn \rangle \cong \mathbb{Z}/\langle m \rangle \times \mathbb{Z}/\langle n \rangle$$

und damit auch Isomorphie der zugehörigen Einheitengruppen gilt. Ein Element $([v]_m, [w]_n) \in \mathbb{Z}/\langle m \rangle \times \mathbb{Z}/\langle n \rangle$ ist somit genau dann Einheit, wenn $[v]_m \in (\mathbb{Z}/\langle m \rangle)^*$ und $[w]_n \in (\mathbb{Z}/\langle n \rangle)^*$. Damit ist die Anzahl der Elemente von $(\mathbb{Z}/\langle m \rangle \times \mathbb{Z}/\langle n \rangle)^*$ gerade $\phi(m) \cdot \phi(n)$.

□

Korollar A.1.7 *Ist* $m = \prod_{i=1}^{n} p_i^{e_i}$ *eine Primfaktorzerlegung der natürlichen Zahl* m *mit* $p_i \neq p_j$ *für* $i \neq j$*, so gilt:*

$$\phi(m) = m \prod_{i=1}^{n} (1 - \frac{1}{p_i}).$$

Der Beweis dieses Korollars ist eine direkte Anwendung des vorstehenden Satze und bleibt dem interessierten Leser überlassen.

A.2 Ver- und Entschlüsseln mit RSA

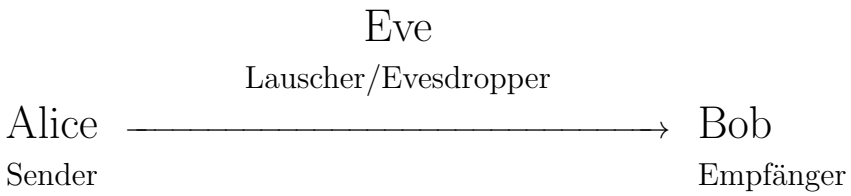
Möchten Alice und Bob miteinander auf einem öffentlichen Kanal (z.B. Internet) kommunizieren, ohne dass jemand anderes die Informationen abhören kann, so müssen sie diese verschlüsseln. Hier stellen wir ein recht grundlegendes Asymmetrisches Verschlüsselungsverfahren nach Rivest-Shamir-Adleman vor, das sogenannte RSA-Verfahren, das lange Zeit state-of-the-art war, bis die Weiterentwicklung der Computer und insbesondere Fortschritte auf dem Weg zum Quantencomputing es zumindest für viele praktische Anwendungen obsolet machten. Da es hier vorrangig um das Prinzip eines asymmetrischen Kryptoverfahrens geht und nicht um eine detaillierte Beleuchtung aller theoretischen und praktischen Aspekte, erhebt dieser Abschnitt auch keinerlei Anspruch, eine vollständige Einführung zu sein.

Sprechen wir hier von einem Asymmetrischen Kryptoverfahren, so ist damit gemeint, dass Alice und Bob nicht gegenseitig über dieselben Informationen zur Ver- und Entschlüsselung verfügen, sondern jeder einen öffentlichen Schlüssel besitzt, der allen zur Verfügung gestellt wird, sowie einen privaten Schlüssel, der aus dem öffentlichen Schlüssel nicht (bzw. hinreichend nicht leicht) errechnet werden kann und geheim gehalten wird.

Eine Nachricht ist für uns in diesem Kontext einfach eine Zahl $M \in \mathbb{Z}/N\mathbb{Z}$ für eine geeignete (und hinreichend große) zusammengesetzte Zahl N. Denken Sie etwa an recht offensichtliche Minibeispiele wie das Abzählen der Buchstaben des Alphabets oder den ASCII-Code zur Umsetzung der Buchstaben sowie Sonder- und Steuerzeichen in Zahlen.

Das Kommunikationsproblem

Alice möchte eine Nachricht an Bob schicken, die Eve als Lauscher an der Leitung nicht entschlüsseln kann.



Die Erzeugung der Schlüssel

Da Bob der Empfänger der Nachricht sein wird, muss das Geheimnis zur Entschlüsselung auf seiner Seite liegen. Es ist also an Bob, ein Schlüsselpaar zu erzeugen, von dem er den öffentlichen Schlüssel Alice zur Verfügung stellt.

RSA-Schlüsselerzeugung (Bob):

- Wähle/Erzeuge zwei Primzahlen p und q der Größenordnung von 2048 Bit ($=2^{2048}$) (die nicht zu dicht beieinander liegen und unabhängig erzeugt wurden – für Deutschland genauer spezifiziert in Bekanntmachung der Bundesnetzagentur vom 14.1.2014)

- $N = p \cdot q$ und damit $\phi(N) = (p-1) \cdot (q-1)$

- Wähle $e \in \mathbb{Z}$ mit $1 < e < \phi(N)$ und $\mathrm{ggT}(e, \phi(N)) = 1$, d.h. $[e]_{\phi(N)}$ ist Einheit in $\mathbb{Z}/\phi(N)\mathbb{Z}$.

- Berechne die Inversen $[d]_{\phi(N)}$ zu $[e]_{\phi(N)} \in (\mathbb{Z}/\phi(N)\mathbb{Z})^*$ und nenne den Repräsentanten mit $1 < d < \phi(N)$ nun d.
  Es gilt also:
  $$1 = ed - k\phi(N)$$
  für ein geeignetes $k \in \mathbb{Z}$.

- Publiziere (e, N) und halte $(d, p, q, \phi(N))$ geheim.

RSA-Verschlüsselung

Alice hat nun Bob's öffentlichen Schlüssel (N, e) erhalten und möchte ihre Nachricht m, die bereits als ganze Zahl $0 \leq M < N$ dargestellt ist, damit verschlüsseln. Dazu bedient sie sich der Multiplikation auf $\mathbb{Z}/N\mathbb{Z}$ und des erhaltenen Exponenten e.

Verschlüsselung (Alice):

- Suche Bob's Schlüssel (N, e) heraus
- Berechne $C = M^e \bmod N$
- Sende C an Bob

RSA-Entschlüsselung

Bob hat nun Alices Nachricht erhalten und verwendet seinen privaten Schlüssel sowie Gruppentheorie aus dem Abschnitt A.1, um die Nachricht zu entschlüsseln.

Entschlüsselung (Bob):

- Erhalte $C < N$ von Alice
- Rechne
$$C^d = M^{ed} = M^{1+k\phi(N)} \equiv M \bmod N.$$
(Denn $M^{\phi(N)} = 1$ nach dem Satz von Euler angewandt modulo N, falls $\mathrm{ggT}(M, N) = 1$.Im Fall $\mathrm{ggT}(M, N) = p$ (bzw. q) verwendet man unter Ausnutzung des Chinesischen Restsatzes dasselbe Argument oder den kleinen Satz von Fermat.)

RSA-Trapdoor-Einwegfunktion

Dieses Verschlüsselungsverfahren beruht im Grunde genommen darauf, dass es schwer ist zu C den Wert $C^{\frac{1}{e}}$ zu bestimmen, wenn man nur e und N kennt, nicht aber $p, q, d, \phi(N)$. Es gibt aber eine "Falltür", nämlich die Kenntnis von d, die das Unterfangen ganz einfach macht.

Gegeben: e, N wie oben mit $\mathrm{ggT}(e, N) = 1$

RSA-Trapdoor-Funktion:

$$f_{N,e}(M) := M^e \bmod N \text{ für } M \in \mathbb{Z}/N\mathbb{Z}$$

Es ist einfach $f_{N,e}$ zu evaluieren. Es sollte schwierig sein, $f_{N,e}$ zu invertieren (Einwegfunktion), aber durch die Falltür kann Bob trotzdem leicht M aus $f_{N,e}(M)$ bestimmen.

Einige Kommentare zum Brechen von RSA

- Mit 'Brechen von RSA' ist das Berechnen von $C^{\frac{1}{e}}$ zu gegebenem C gemeint.
- Das 'spezielle ganzzahlige Faktorisierungsproblem' ist das Problem der Ermittlung der beiden Primzahlen p und q aus $N = pq$.
- Ist es möglich das spezielle ganzzahlige Faktorisierungsproblem zu lösen, so kann man RSA leicht brechen, da aus der Kenntnis von p und q direkt die Kenntnis von $\phi(N) = (p-1)(q-1)$ folgt, womit dann mittels der Bézout-Identität modulo $\phi(N)$ direkt d bestimmt werden kann.
- Es ist nicht klar, ob das spezielle ganzzahlige Faktorisierungsproblem ebenfalls gelöst ist, sobald eine effektive Methode zum Brechen von RSA zur Verfügung steht.

Weiter werden wir an dieser Stelle nicht in die Tiefe oder in die Breite gehen, sondern überlassen dies z.B. einer Veranstaltung zur Kryptographie oder dem Selbststudium in einem Buch.
Es sei nur soviel gesagt, dass sie gerade mal einen ersten Eindruck von Kryptographie erhalten haben, aber nicht weiter in das Gebiet eingetaucht sind, als sie es z.B. mit dem Lösen linearer Gleichungssysteme in zwei Variablen in der Schule in die Lineare Algebra waren.
Für modernere Schlagworte zur Kryptographie möchte ich gerade noch die Stichworte "elliptische Kurven Kryptographie" sowie "Post-Quantum-Kryptographie" nennen, ohne jedoch auf deren Inhalt einzugehen.