10. Teilbarkeit in Ringen

Ein wichtiges Konzept in Ringen, das ihr für den Fall des Ringes $\mathbb{Z}$ bereits aus der Schule kennt, ist das von *Teilern* — also der Frage, wann und wie man ein Ringelement als Produkt von zwei anderen schreiben kann. Dies wollen wir jetzt in allgemeinen Ringen untersuchen, wobei die Polynomringe über Körpern letztlich neben $\mathbb{Z}$ die wichtigsten Anwendungsbeispiele sein werden. Um die Theorie dazu nicht zu kompliziert werden zu lassen, wollen wir uns dabei auf den Fall von Integritätsringen beschränken, also die Existenz von Nullteilern außer der 0 ausschließen.

Definition 10.1 (Teiler)**.** Es seien R ein Integritätsring und $a, b \in R$. Man sagt, dass b ein **Teiler** von a ist (in Zeichen: $b \mid a$), wenn es ein $c \in R$ gibt mit $a = b \cdot c$. In diesem Fall heißt a dann auch ein **Vielfaches** von b.

Beispiel 10.2.

(a) Die Teiler von 4 im Ring $\mathbb{Z}$ sind -4, -2, -1, 1, 2 und 4.

(b) Das Polynom $2t$ ist im Integritätsring $\mathbb{Q}[t]$ ein Teiler von t^2 (denn $t^2 = 2t \cdot \frac{1}{2} t$), nicht jedoch in $\mathbb{Z}[t]$.

Wie üblich wollen wir zuerst die wichtigsten Eigenschaften von Teilern untersuchen. Besonders wichtig ist dabei, dass sich die Teilbarkeitseigenschaft auch mit Hilfe von Idealen formulieren lässt.

Lemma 10.3 (Eigenschaften der Teilbarkeit)**.** *Es seien a, b, c Elemente in einem Integritätsring R.*

(a) *Gilt $c \mid b$ und $b \mid a$, so auch $c \mid a$ (Transitivität).*

(b) *Es ist $b \mid a$ genau dann, wenn $a \in \langle b \rangle$.*

(c) *Es gilt*

$$b \mid a \text{ und } a \mid b \quad \Leftrightarrow \quad \text{es gibt ein } d \in R^* \text{ mit } a = bd \quad \Leftrightarrow \quad \langle a \rangle = \langle b \rangle.$$

*Man sagt in diesem Fall auch, dass a und b zueinander **assoziiert** sind.*

Beweis.

(a) Gilt $c \mid b$ und $b \mid a$, also $b = cd$ und $a = be$ für gewisse $d, e \in R$, so ist auch $a = cde$, also $c \mid a$.

(b) Es gilt

$$b \mid a \quad \Leftrightarrow \quad \text{es gibt ein } c \in R \text{ mit } a = bc \quad \Leftrightarrow \quad a \in \{bc : c \in R\} \overset{8.8(a)}{=} \langle b \rangle.$$

(c) Wir zeigen die Äquivalenzen durch einen Ringschluss.

Es gelte zunächst $b \mid a$ und $a \mid b$, d. h. es gibt $d, e \in R$ mit $a = bd$ und $b = ae$. Setzt man dies ineinander ein, so ergibt sich $a = ade$ und $b = bde$. Sind nun a oder b ungleich 0, so folgt daraus mit der Kürzungsregel aus Lemma 7.8 (c) sofort $de = 1$, also $a = bd$ mit $d \in R^*$. Andernfalls ist $a = b = 0$, und damit natürlich auch $a = b \cdot 1$ mit $1 \in R^*$.

Nun sei $a = bd$ für ein $d \in R^*$. Dann ist auch $b = ad^{-1}$, nach Beispiel 8.8 (a) also $a \in \langle b \rangle$ und $b \in \langle a \rangle$. Nach Lemma 8.6 (b) bedeutet dies aber gerade $\langle a \rangle \subset \langle b \rangle$ und $\langle b \rangle \subset \langle a \rangle$, also $\langle a \rangle = \langle b \rangle$.

Ist schließlich $\langle a \rangle = \langle b \rangle$, also $a \in \langle b \rangle$ und $b \in \langle a \rangle$, so gilt $b \mid a$ und $a \mid b$ nach (b). □

Aufgabe 10.4. Man zeige:

(a) Eine natürliche Zahl ist genau dann durch 3 teilbar, wenn ihre Quersumme (also die Summe aller ihrer Ziffern) durch 3 teilbar ist.

(b) Für $a, b \in \mathbb{Z}$ gilt $17 \mid a + 3b$ genau dann, wenn $17 \mid b + 6a$.

Wie ihr vom Fall der ganzen Zahlen $\mathbb{Z}$ wisst, spielt bei der Untersuchung der Teilbarkeit vor allem der größte gemeinsame Teiler (und das kleinste gemeinsame Vielfache) von zwei gegebenen Zahlen eine große Rolle. Wir wollen ein derartiges Konzept daher auch in allgemeinen Integritätsringen einführen. Dabei haben wir jedoch zunächst das Problem, dass wir auf einem allgemeinen Integritätsring R keine „Ordnung“ haben, mit deren Hilfe wir sagen könnten, welchen gemeinsamen Teiler zweier Elemente von R wir als den *größten* ansehen wollen. Das folgende Beispiel zeigt, wie wir dieses Problem lösen können.

Beispiel 10.5. Betrachten wir die beiden ganzen Zahlen 12 und 30, so sind die gemeinsamen Teiler von ihnen -6, -3, -2, -1, 1, 2, 3 und 6. Von diesen ist 6 natürlich die größte Zahl — aber die 6 ist auch in dem Sinne „am größten“, dass jedes andere Element dieser Liste ein Teiler davon ist.

Es ist diese zweite Eigenschaft, die wir zur Definition eines größten gemeinsamen Teilers verwenden wollen und die so auch in jedem Integritätsring anwendbar ist. Wie in der folgenden Definition messen wir die Größe eines Teilers also ebenfalls wieder mit Hilfe der Teilbarkeit.

Definition 10.6 (ggT und kgV)**.** Es seien a,b zwei Elemente in einem Integritätsring R.

(a) Ein Element $g \in R$ heißt **größter gemeinsamer Teiler** von a und b, wenn gilt:

(1) $g \mid a$ und $g \mid b$ („g ist ein gemeinsamer Teiler“);

(2) ist $c \in R$ mit $c \mid a$ und $c \mid b$, so gilt auch $c \mid g$ („g ist der *größte* gemeinsame Teiler“).

Wir bezeichnen die Menge aller größten gemeinsamen Teiler von a und b mit $\operatorname{ggT}(a,b)$. Ist $1 \in \operatorname{ggT}(a,b)$, so heißen a und b **teilerfremd**.

(b) Ein Element $k \in R$ heißt **kleinstes gemeinsames Vielfaches** von a und b, wenn gilt:

(1) $a \mid k$ und $b \mid k$ („k ist ein gemeinsames Vielfaches“);

(2) ist $c \in R$ mit $a \mid c$ und $b \mid c$, so gilt auch $k \mid c$ („k ist das *kleinste* gemeinsame Vielfache“).

Wir bezeichnen die Menge aller kleinsten gemeinsamen Vielfachen von a und b mit $\operatorname{kgV}(a,b)$.

Beachte, dass durch unsere vielleicht etwas eigenwillig erscheinende Definition der „Größe“ eines Teilers bzw. Vielfachen zunächst einmal überhaupt nicht klar ist, ob größte gemeinsame Teiler und kleinste gemeinsame Vielfache überhaupt existieren, und ob sie im Fall der Existenz eindeutig sind. Wir haben $\operatorname{ggT}(a,b)$ und $\operatorname{kgV}(a,b)$ daher vorsichtshalber erst einmal als *Mengen* definiert (die auch leer sein oder mehr als ein Element enthalten können).

In der Tat wollen wir uns nun mit der Frage nach dieser Existenz und Eindeutigkeit von größten gemeinsamen Teilern beschäftigen (der Fall der kleinsten gemeinsamen Vielfachen wird sich in Folgerung 11.12 (c) dann relativ einfach daraus ergeben). Wir beginnen dabei mit der Eindeutigkeit, da deren Untersuchung deutlich einfacher ist als die der Existenz.

Beispiel 10.7 ((Nicht-)Eindeutigkeit des größten gemeinsamen Teilers)**.** Wir haben in Beispiel 10.5 schon festgestellt, dass -6, -3, -2, -1, 1, 2, 3 und 6 die gemeinsamen Teiler von 12 und 30 sind. Von diesen ist 6, aber auch -6 nach Definition 10.6 (a) ein größter gemeinsamer Teiler, denn alle diese acht Teiler von 12 und 30 sind auch Teiler von -6 und 6. Also ist

$$\operatorname{ggT}(12,30) = \{-6,6\}.$$

Insbesondere ist der größte gemeinsame Teiler also *nicht eindeutig*. Diese Nichteindeutigkeit besteht hier aber nur im Vorzeichen, also in der Möglichkeit, einen größten gemeinsamen Teiler noch mit der Einheit -1 von $\mathbb{Z}$ zu multiplizieren. Dies ist in der Tat ein allgemeines Phänomen, wie der folgende Satz zeigt.

Satz 10.8 ((Nicht-)Eindeutigkeit des größten gemeinsamen Teilers)**.** *Es sei g ein größter gemeinsamer Teiler zweier Elemente a,b in einem Integritätsring R. Dann ist $\operatorname{ggT}(a,b) = R^* g = \{cg : c \in R^*\}$ genau die Menge aller zu g assoziierten Elemente.*

Ein größter gemeinsamer Teiler zweier Elemente in einem Integritätsring ist also stets eindeutig bis auf Multiplikation mit Einheiten.

Beweis.

„$\subset$“: Es sei $g' \in \mathrm{ggT}(a,b)$. Damit sind g und g' größte gemeinsame Teiler von a und b. Wenden wir Teil (1) von Definition 10.6 (a) auf g' an, so sehen wir also, dass $g' \mid a$ und $g' \mid b$. Damit können wir dann Teil (2) mit $c = g'$ anwenden und erhalten $g' \mid g$. Durch Vertauschen der Rollen von g und g' ergibt sich genauso $g \mid g'$. Nach Lemma 10.3 (c) folgt damit $g' = cg$ für ein $c \in R^*$.

„$\supset$“: Es sei $g' = cg$ für ein $c \in R^*$. Dann folgt $g \mid g'$ und $g' \mid g$ nach Lemma 10.3 (c). Unter Benutzung der Transitivität der Teilbarkeitsrelation aus Lemma 10.3 (a) erfüllt daher mit g auch g' die beiden Eigenschaften aus Definition 10.6 (a):

(1) es gilt $g' \mid g \mid a$ und $g' \mid g \mid b$;

(2) ist $d \in R$ mit $d \mid a$ und $d \mid b$, so folgt $d \mid g \mid g'$.

Also ist auch g' ein größter gemeinsamer Teiler von a und b. □

Bemerkung 10.9. Der Beweis von Satz 10.8 lässt sich durch „Umkehren der Teilbarkeitsrelationen“ ganz analog auch für den Fall des kleinsten gemeinsamen Vielfachen führen.

Nach der Eindeutigkeit kommen wir nun zur Existenz eines größten gemeinsamen Teilers. Mit der Vorstellung des Ringes $\mathbb{Z}$ im Hintergrund würden wir wahrscheinlich erwarten, dass zwei Elemente a und b eines Integritätsringes R stets einen größten gemeinsamen Teiler besitzen. Allerdings haben wir die „Größe“ der gemeinsamen Teiler in Definition 10.6 (a) ja wieder über die Teilbarkeit definiert, und es ist ja bereits im Ring $\mathbb{Z}$ so, dass zwei beliebige Zahlen bezüglich Teilbarkeit nicht unbedingt miteinander vergleichbar sein müssen: Für z. B. die ganzen Zahlen 2 und 3 gilt weder $2 \mid 3$ noch $3 \mid 2$. Daher könnte es natürlich passieren, dass zu a und b kein größter gemeinsamer Teiler existiert, weil es zwei gemeinsame Teiler gibt, zu denen kein größerer existiert, und die nicht miteinander vergleichbar sind. Im folgenden Beispiel ist dies der Fall:

Aufgabe 10.10 ((Nicht-)Existenz eines größten gemeinsamen Teilers)**.** Bestimme alle gemeinsamen Teiler von $2+2\sqrt{5}\mathrm{i}$ und 6 im Ring $\mathbb{Z}[\sqrt{5}\mathrm{i}]$ aus Aufgabe 7.24 und zeige so, dass es keinen größten gemeinsamen Teiler gibt.

Die Frage nach der Existenz eines größten gemeinsamen Teilers gestaltet sich also etwas schwieriger als erwartet. Zu ihrer Untersuchung ist es nützlich, die Idealschreibweise aus Lemma 10.3 zu verwenden und eine weitere Bedingung an die betrachteten Ringe zu stellen.

Definition 10.11 (Hauptidealringe)**.** Es sei R ein Integritätsring.

(a) Ein Ideal der Form $\langle a \rangle$ für ein $a \in R$ (also eines, das von nur einem Element erzeugt werden kann) nennt man ein **Hauptideal**.

(b) Man bezeichnet R als einen **Hauptidealring**, wenn jedes Ideal in R ein Hauptideal ist.

Beispiel 10.12. $\mathbb{Z}$ ist ein Hauptidealring, da alle Ideale in diesem Ring nach Beispiel 8.3 (a) von der Form $\langle n \rangle$ für ein $n \in \mathbb{N}$, also Hauptideale sind.

Satz 10.13 (Größte gemeinsame Teiler in Hauptidealringen)**.** *Es seien a und b zwei Elemente in einem Integritätsring R.*

(a) *Ist $g \in R$ mit $\langle a,b \rangle = \langle g \rangle$, so ist $g \in \mathrm{ggT}(a,b)$.*

Insbesondere existiert in einem Hauptidealring also stets ein größter gemeinsamer Teiler von a und b.

(b) *Ist R ein Hauptidealring, so gilt auch die Umkehrung: Ist $g \in \mathrm{ggT}(a,b)$, so ist $\langle a,b \rangle = \langle g \rangle$.*

*Insbesondere gibt es also in einem Hauptidealring zu jedem $g \in \mathrm{ggT}(a,b)$ Elemente $d,e \in R$ mit $g = da + eb$. Diese Aussage wird oft auch als **Lemma von Bézout** bezeichnet.*

Beweis.

(a) Wir überprüfen die beiden Bedingungen aus Definition 10.6:

(1) Nach Voraussetzung gilt $a \in \langle g \rangle$ und $b \in \langle g \rangle$, mit Lemma 10.3 (b) also $g \mid a$ und $g \mid b$.

(2) Es sei c ein gemeinsamer Teiler von a und b, also $c \mid a$ und $c \mid b$ bzw. $a \in \langle c \rangle$ und $b \in \langle c \rangle$. Nach Lemma 8.6 (b) ist dann auch $\langle g \rangle = \langle a,b \rangle \subset \langle c \rangle$, also $g \in \langle c \rangle$ und damit $c \mid g$.

11

(b) Da R ein Hauptidealring ist, gibt es ein $c \in R$ mit $\langle a,b \rangle = \langle c \rangle$. Dieses c ist nach (a) ebenfalls ein größter gemeinsamer Teiler von a und b. Nach Satz 10.8 sind c und g also assoziiert, und damit gilt $\langle a,b \rangle = \langle c \rangle = \langle g \rangle$ nach Lemma 10.3 (c).

Das Lemma von Bézout ergibt sich nun unmittelbar aus $g \in \langle a,b \rangle = \{da + eb : d,e \in R\}$ (siehe Definition 8.5). □

Beispiel 10.14.

(a) Wir haben in Beispiel 10.7 bereits gesehen, dass $6 \in \mathrm{ggT}(12,30)$ in $\mathbb{Z}$ gilt. Da $\mathbb{Z}$ nach Beispiel 10.12 ein Hauptidealring ist, muss sich 6 nach Satz 10.13 (b) also als Linearkombination von 12 und 30 schreiben lassen, was wir wegen $6 = -2 \cdot 12 + 1 \cdot 30$ hier natürlich auch direkt sehen können. Außerdem besagt der Satz auch, dass $\langle 12,30 \rangle = \langle 6 \rangle$ (was man ebenfalls auch direkt überprüfen könnte).

(b) Da in $\mathbb{Z}[\sqrt{5}\,\mathrm{i}]$ nach Aufgabe 10.10 im Allgemeinen kein größter gemeinsamer Teiler existiert, kann dieser Ring nach Satz 10.13 (a) kein Hauptidealring sein.

(c) Wir betrachten die beiden Elemente 2 und t im Polynomring $\mathbb{Z}[t]$: Nach der Gradformel aus Lemma 9.9 (a) sind Teiler von 2 nur konstante Polynome, also ± 1 und ± 2. Aber ± 2 ist wie in Beispiel 10.2 (b) kein Teiler von t. Damit sind ± 1 die einzigen gemeinsamen Teiler von 2 und t, und es folgt $\mathrm{ggT}(2,t) = \{1,-1\}$.

Beachte aber, dass es keine Linearkombination $f \cdot 2 + g \cdot t = 1$ mit $f,g \in \mathbb{Z}[t]$ geben kann, da der konstante Term des Polynoms auf der linken Seite dieser Gleichung in jedem Fall gerade, auf der rechten aber gleich 1 ist. Satz 10.13 (b) zeigt also, dass $\mathbb{Z}[t]$ kein Hauptidealring sein kann, bzw. dass das Ideal $\langle 2,t \rangle \trianglelefteq \mathbb{Z}[t]$ kein Hauptideal ist.

Um die Situation zu vereinfachen, wollen wir im Rest dieses Kapitels nun nur noch Hauptidealringe betrachten, so dass ein größter gemeinsamer Teiler g von zwei Elementen a und b nach Satz 10.13 also stets existiert und durch die Idealgleichung $\langle a,b \rangle = \langle g \rangle$ charakterisiert ist. Es bleiben dann noch zwei Fragen:

- Wie kann man erkennen, ob ein gegebener Integritätsring ein Hauptidealring ist?
- Wie kann man in einem Hauptidealring zu zwei gegebenen Elementen a und b konkret ein $g \in \mathrm{ggT}(a,b)$ finden, also ein g mit $\langle a,b \rangle = \langle g \rangle$?

In der Tat lassen sich beide Fragen gleichzeitig beantworten, indem man die folgende einfache Umformungsregel für Erzeuger von Idealen geschickt mehrfach anwendet.

Lemma 10.15. *Für alle a,b,q in einem Ring R gilt $\langle a,b \rangle = \langle a,b+qa \rangle$.*

Beweis. Es gilt $a \in \langle a,b+qa \rangle$ und $b = a \cdot (-q) + (b+qa) \in \langle a,b+qa \rangle$, und damit nach Lemma 8.6 (b) auch $\langle a,b \rangle \subset \langle a,b+qa \rangle$.

Analog ist $a \in \langle a,b \rangle$ und $b+qa = a \cdot q + b \in \langle a,b \rangle$ und damit auch $\langle a,b+qa \rangle \subset \langle a,b \rangle$. □

Beispiel 10.16. In $\mathbb{Z}$ können wir das Ideal $\langle 44,10 \rangle$ umformen als

$$\begin{aligned} \langle 44,10 \rangle &\overset{10.15}{=} \langle 44 - 4 \cdot 10, 10 \rangle = \langle 4,10 \rangle \\ &\overset{10.15}{=} \langle 4, 10 - 2 \cdot 4 \rangle = \langle 4,2 \rangle \\ &\overset{10.15}{=} \langle 4 - 2 \cdot 2, 2 \rangle = \langle 0,2 \rangle = \langle 2 \rangle. \end{aligned}$$

Damit haben wir $\langle 44,10 \rangle = \langle 2 \rangle$ als Hauptideal geschrieben; nach Satz 10.13 ist also insbesondere $2 \in \mathrm{ggT}(44,10)$.

Natürlich ist klar, welche Strategie wir hier angewendet haben: Wir haben die jeweils größere Zahl mit Rest durch die kleinere geteilt und konnten sie mit Hilfe von Lemma 10.15 dann durch den Rest dieser Division ersetzen. Da die beteiligten Zahlen bei dieser Vorgehensweise in $\mathbb{N}$ bleiben und immer kleiner werden, ist klar, dass letztlich einmal eine der Zahlen gleich Null werden und das Verfahren somit funktionieren muss.

Die entscheidende Idee bei diesem Verfahren ist also eine Division mit Rest. Eine solche existiert zwar nicht in jedem Integritätsring, aber doch in deutlich mehr Ringen als nur in $\mathbb{Z}$. Wir wollen die Existenz einer solchen Division mit Rest daher jetzt als Eigenschaft eines Ringes definieren. Wie wir sehen werden, wird sie uns sowohl sicherstellen, dass wir einen Hauptidealring haben, als auch ein konkretes Verfahren zur Bestimmung eines größten gemeinsamen Teilers liefern.

Definition 10.17 (Euklidische Ringe)**.** Ein Integritätsring R heißt **euklidischer Ring**, wenn es eine Abbildung $\delta\colon R\backslash\{0\} \to \mathbb{N}$ mit der folgenden Eigenschaft gibt: Für alle $a,b \in R$ mit $b \neq 0$ gibt es $q,r \in R$ mit $a = qb + r$, so dass $r = 0$ oder $\delta(r) < \delta(b)$ ist. (Es muss also eine Division mit Rest geben, wobei der Rest r — sofern er nicht Null ist — „gemessen mit der Funktion δ“ stets kleiner ist als das Element, durch das man geteilt hat.)

Eine Funktion δ mit dieser Eigenschaft wird als **euklidische Funktion** bezeichnet.

Beispiel 10.18. Der Ring $\mathbb{Z}$ ist mit der Funktion $\delta(n) := |n|$ ein euklidischer Ring.

Beachte, dass die Division mit Rest im Sinne von Definition 10.17 in diesem Fall nicht eindeutig ist: Wollen wir z. B. $a = -5$ mit Rest durch $b = 2$ teilen, so wären sowohl $-5 = (-3)\cdot 2 + 1$ als auch $-5 = (-2)\cdot 2 - 1$ wegen $|1| = |-1| < |2|$ erlaubte Ergebnisse. Dies ist jedoch nicht weiter schlimm, denn eine Eindeutigkeit der Division mit Rest wird im Folgenden nicht benötigt (und wurde in Definition 10.17 ja auch nicht verlangt).

Ein zweites und sehr wichtiges Beispiel ist der Polynomring über einem beliebigen Körper, in dem mit der sogenannten Polynomdivision ebenfalls eine Division mit Rest existiert.

Satz 10.19 (**Polynomdivision**)**.** *Es sei K ein Körper. Dann ist der Polynomring $K[t]$ mit der Gradfunktion $\delta(f) := \deg f$ ein euklidischer Ring.*

Mit anderen Worten gibt es also zu je zwei Polynomen $f,g \in K[t]$ mit $g \neq 0$ stets Polynome $q,r \in K[t]$ mit $f = qg + r$ und $\deg r < \deg g$.

Beweis. Es seien $n = \deg f \in \mathbb{N} \cup \{-\infty\}$ und $m = \deg g \in \mathbb{N}$. Wir zeigen den Satz mit Induktion über n. Der Induktionsanfang ist dabei trivial, denn für $n < m$ können wir einfach $q = 0$ und $r = f$ setzen.

Es sei nun also $n \geq m$. Man kann f und g dann schreiben als

$$f = a_n t^n + \cdots + a_1 t + a_0 \quad \text{und} \quad g = b_m t^m + \cdots + b_1 t + b_0$$

mit $a_n, b_m \neq 0$. Wir dividieren nun die jeweils höchsten Terme von f und g durcheinander und erhalten

$$q' := \frac{a_n}{b_m} t^{n-m} \quad \in K[t]$$

(beachte, dass wir $\frac{a_n}{b_m}$ bilden können, weil K ein Körper ist, und t^{n-m}, weil wir $n \geq m$ vorausgesetzt haben). Dies wird unser erster Term im Ergebnis der Division. Subtrahieren wir nun $q'g$ von f, so erhalten wir

$$f - q'g = a_n t^n + \cdots + a_1 t + a_0 - \frac{a_n}{b_m} t^{n-m} \cdot (b_m t^m + \cdots + b_1 t + b_0).$$

Da sich der Term $a_n t^n$ in diesem Ausdruck weghebt, ist $\deg(f - q'g) < n$. Wir können also die Induktionsvoraussetzung auf $f - q'g$ anwenden und erhalten Polynome $q'', r \in K[t]$ mit $\deg r < \deg g$ und

$$f - q'g = q''g + r, \quad \text{also} \quad f = (q' + q'')g + r.$$

Setzen wir nun $q = q' + q''$, so erhalten wir offensichtlich genau den gewünschten Ausdruck. □

Beispiel 10.20. Der Beweis von Satz 10.19 ist konstruktiv, d. h. er gibt auch ein Verfahren an, mit dem man die Division von $f \in K[t]$ durch $g \in K[t]\backslash\{0\}$ konkret durchführen kann: Man muss einfach den höchsten Term von f durch den höchsten Term von g teilen, dies als ersten Teil q' des Ergebnisses hinschreiben, und das Verfahren dann mit $f - q'g$ fortsetzen — so lange, bis der Grad dieses Polynoms kleiner ist als der von g. Wollen wir z. B. in $\mathbb{R}[t]$ das Polynom $f = 2t^2 + 1$ durch $g = t - 2$ dividieren, so können wir dies wie folgt aufschreiben (wobei wir im ersten Schritt zur Verdeutlichung die Notationen von oben noch mit an die Rechnung geschrieben haben):

$$\begin{array}{rl} & (2t^2+1) \,:\, (t-2) \;=\; 2t+4 \\ q'g \longrightarrow & -\,\underline{(2t^2-4t)} \qquad\qquad \uparrow \\ & \qquad 4t+1 \qquad\qquad = \frac{2t^2}{t} =: q' \\ f - q'g \longrightarrow & -\,\underline{(4t-8)} \\ & \qquad\; 9 \end{array}$$

Das Ergebnis ist also $2t^2 + 1 = (2t+4)\cdot(t-2) + 9$ (d. h. $q = 2t+4$ und $r = 9$). Zur Kontrolle der Rechnung kann man diese Gleichheit durch Ausmultiplizieren natürlich auch direkt überprüfen.

Wie bereits angekündigt wollen wir nun sehen, dass euklidische Ringe stets Hauptidealringe sind.

Satz 10.21. *Jeder euklidische Ring ist ein Hauptidealring.*

Beweis. Es sei I ein Ideal in einem euklidischen Ring R. Ist $I = \{0\}$, so sind wir offensichtlich fertig, denn dann ist ja $I = \langle 0 \rangle$. Andernfalls wählen wir ein Element $g \in I\backslash\{0\}$, für das die euklidische Funktion δ minimal ist — ein solches Element existiert in jedem Fall, da δ ja nur natürliche Zahlen als Werte annimmt und jede nicht-leere Menge natürlicher Zahlen ein Minimum besitzt.

Wir behaupten nun, dass $I = \langle g \rangle$ gilt und I somit ein Hauptideal ist. Die Inklusion $I \supset \langle g \rangle$ ist dabei wegen $g \in I$ klar nach Lemma 8.6 (b). Für die umgekehrte Inklusion $I \subset \langle g \rangle$ sei $a \in I$ beliebig. Wir dividieren a gemäß Definition 10.17 mit Rest durch g und erhalten

$$a = qg + r \qquad (*)$$

für gewisse $q, r \in R$ mit $r = 0$ oder $\delta(r) < \delta(g)$. Wegen $a \in I$ und $g \in I$ ist nun aber auch $r = a - qg \in I$ nach Definition 8.1. Da g ein Element mit minimaler euklidischer Funktion in I war, kann also nicht $\delta(r) < \delta(g)$ gelten. Damit ist notwendigerweise $r = 0$, und mit $(*)$ folgt $a = qg \in \langle g \rangle$. □

Beispiel 10.22. Neben $\mathbb{Z}$ ist nach Satz 10.19 also auch der Polynomring über einem Körper ein Hauptidealring. Dies sind sicher die beiden wichtigsten Beispiele für Hauptidealringe. Zwei weitere ergeben sich aus den folgenden beiden Aufgaben.

Aufgabe 10.23. Zeige, dass der Ring $\mathbb{Z}[\mathrm{i}] = \{a + b\,\mathrm{i} : a, b \in \mathbb{Z}\}$ (siehe Aufgabe 7.24 (a)) mit der Funktion $\delta(z) := |z|^2$ ein euklidischer Ring (und damit ein Hauptidealring) ist.

Aufgabe 10.24. Es sei K ein Körper. Zeige, dass jedes Ideal $I \trianglelefteq K[\![t]\!]$ mit $I \neq \langle 0 \rangle$ von der Form $\langle t^n \rangle$ für ein $n \in \mathbb{N}$ ist. Insbesondere ist $K[\![t]\!]$ also ein Hauptidealring.

Bemerkung 10.25. Man kann zeigen, dass es Hauptidealringe gibt, die nicht euklidisch sind. Eines der einfachsten Beispiele hierfür ist der Ring $\mathbb{Z}\left[\frac{1+\sqrt{19}\,\mathrm{i}}{2}\right]$ in der Notation aus Bemerkung 9.18 (b). Der Beweis dieser Tatsache ist jedoch recht aufwändig und soll hier nicht gegeben werden.

Ist I ein Ideal in einem Hauptidealring R, so besagt der Beweis von Satz 10.21 bereits, wie wir ein Element $g \in R$ mit $I = \langle g \rangle$ finden können: Wir können in $I\backslash\{0\}$ ein Element mit minimaler euklidischer Funktion suchen. Dies ist oftmals aber nur schwer durchführbar. Für Ideale der Form $I = \langle a, b \rangle$, die für die Bestimmung von $\mathrm{ggT}(a, b)$ benötigt werden, ist das folgende an Beispiel 10.16 angelehnte Verfahren deutlich einfacher.

Satz 10.26 (Euklidischer Algorithmus). *Es seien R ein euklidischer Ring und $a_1, a_2 \in R$.*

Wir konstruieren daraus nun wie folgt rekursiv eine (abbrechende) Folge $a_1, a_2, \dots, a_N$ in R: Sind $a_1, \dots, a_{n-1} \in R$ für ein $n \geq 3$ bereits bestimmt und ist $a_{n-1} \neq 0$, so teilen wir a_{n-2} wie in Definition 10.17 mit Rest durch a_{n-1} und erhalten so eine Darstellung

$$a_{n-2} = q_n a_{n-1} + r_n$$

für gewisse $q_n, r_n \in R$. Wir setzen dann $a_n := r_n = a_{n-2} - q_n a_{n-1}$.

Die so konstruierte Folge bricht nach endlich vielen Schritten ab, d. h. es ist $a_N = 0$ für ein $N \in \mathbb{N}$, und es gilt dann $\langle a_1, a_2 \rangle = \langle a_{N-1} \rangle$. Insbesondere ist das letzte Folgenglied a_{N-1}, das nicht Null ist, nach Satz 10.13 (a) also ein größter gemeinsamer Teiler von a_1 und a_2.

Beweis. Angenommen, die Folge $a_1, a_2, \dots$ würde nicht abbrechen, d. h. es wäre $a_n \neq 0$ für alle $n \in \mathbb{N}$. Nach der Definition eines euklidischen Ringes wäre dann $\delta(a_n) = \delta(r_n) < \delta(a_{n-1})$ für alle $n \geq 3$. Die Zahlen $\delta(a_n)$ müssten für $n \geq 2$ also eine unendliche, streng monoton fallende Folge natürlicher Zahlen bilden, was offensichtlich nicht möglich ist.

Nun gilt für alle $n \geq 3$

$$\langle a_{n-1}, a_n \rangle = \langle a_{n-1}, r_n \rangle = \langle a_{n-1}, a_{n-2} - q_n a_{n-1} \rangle \overset{10.15}{=} \langle a_{n-2}, a_{n-1} \rangle,$$

und daher mit Induktion über n

$$\langle a_1, a_2 \rangle = \langle a_2, a_3 \rangle = \dots = \langle a_{N-1}, a_N \rangle = \langle a_{N-1}, 0 \rangle = \langle a_{N-1} \rangle. \qquad \square$$

Algorithmus 10.27 (Erweiterter euklidischer Algorithmus). Satz 10.26 bestimmt zu zwei Elementen a_1, a_2 eines euklidischen Ringes R ein Element a_{N-1} mit $\langle a_1, a_2 \rangle = \langle a_{N-1} \rangle$. Wegen $a_{N-1} \in \langle a_1, a_2 \rangle$ lässt sich a_{N-1} dann also insbesondere als Linearkombination $a_{N-1} = d a_1 + e a_2$ der Ausgangselemente a_1 und a_2 mit geeigneten $d, e \in R$ schreiben.

Oft möchte man auch diese Elemente d und e konkret berechnen. Dies ist durch eine kleine Erweiterung des Algorithmus aus Satz 10.26 möglich: Statt nur der Elemente a_n berechnen wir zeilenweise eine Tabelle mit Zeilen (a_n, d_n, e_n) für $n = 1, 2, \dots, N-1$, so dass in jeder Zeile $a_n = d_n a_1 + e_n a_2$ gilt. Dies ist sehr einfach: In die ersten beiden Zeilen können wir $(a_1, 1, 0)$ und $(a_2, 0, 1)$ schreiben, denn es ist ja $a_1 = 1 \cdot a_1 + 0 \cdot a_2$ und $a_2 = 0 \cdot a_1 + 1 \cdot a_2$. Berechnen wir nun a_n aus a_{n-2} und a_{n-1} als $a_n = a_{n-2} - q_n a_{n-1}$ wie in Satz 10.26, so führen wir die gleiche Rechnung in allen drei Spalten der Tabelle durch, setzen also auch $d_n = d_{n-2} - q_n d_{n-1}$ und $e_n = e_{n-2} - q_n e_{n-1}$. Dann folgt mit Induktion für alle n

$$a_n = a_{n-2} - q_n a_{n-1} = (d_{n-2} a_1 + e_{n-2} a_2) - q_n (d_{n-1} a_1 + e_{n-1} a_2) = d_n a_1 + e_n a_2,$$

und damit steht dann in der letzten Zeile $(a_{N-1}, d_{N-1}, e_{N-1})$ das gewünschte Ergebnis, so dass $a_{N-1} = d_{N-1} a_1 + e_{N-1} a_2$ gilt.

Die Tabelle unten zeigt dies konkret im Fall der beiden gegebenen Zahlen $a_1 = 11$ und $a_2 = 9$ in $\mathbb{Z}$. Für $n \geq 3$ entsteht der Eintrag a_n der ersten Spalte jeweils dadurch, dass man von a_{n-2} so oft wie möglich a_{n-1} abzieht, also den Rest der Division von a_{n-2} durch a_{n-1} hinschreibt. Dies ist durch die Pfeile auf der linken Seite der Tabelle angedeutet. In den anderen beiden Spalten machen wir (wie durch die Pfeile auf der rechten Seite angedeutet) exakt die gleichen Umformungen. Das gesuchte Ergebnis steht am Ende in der letzten Zeile, die nicht mit 0 beginnt: Im Beispiel unten ist dies $(1, -4, 5)$, und es besagt, dass $\langle 11, 9 \rangle = \langle 1 \rangle$ bzw. $1 \in \mathrm{ggT}(11, 9)$ gilt, und dass $1 = -4 \cdot 11 + 5 \cdot 9$ ist.

$11 - 1 \cdot 9 = 2$
$9 - 4 \cdot 2 = 1$
$2 - 2 \cdot 1 = 0$

a_n	d_n	e_n
11	1	0
9	0	1
2	1	-1
1	-4	5
0		

$(1,0) - 1 \cdot (0,1) = (1,-1)$
$(0,1) - 4 \cdot (1,-1) = (-4,5)$

12

Bemerkung 10.28. Das Verfahren aus Satz 10.26 lässt sich leicht auf mehr als zwei Elemente verallgemeinern: Sind $a_1,\dots,a_n$ Elemente in einem euklidischen Ring R und bestimmen wir mit Satz 10.26 ein $g \in \mathrm{ggT}(a_1,a_2)$, also mit $\langle a_1,a_2\rangle = \langle g\rangle$, so ist

$$\langle a_1,a_2,a_3,\dots,a_n\rangle = \langle g,a_3,\dots,a_n\rangle.$$

Auf diese Art können wir dann also rekursiv auch jedes Ideal, das von endlich vielen Elementen erzeugt wird, als Hauptideal schreiben: Man muss nur fortlaufend zwei Erzeuger durch einen größten gemeinsamen Teiler von ihnen ersetzen.

Bemerkung 10.29. Fassen wir die wichtigsten Ergebnisse dieses Kapitels zur Existenz und Eindeutigkeit von größten gemeinsamen Teilern zusammen, so sehen wir also:

> In einem Hauptidealring R existiert zu je zwei Elementen a und b stets ein größter gemeinsamer Teiler g, der bis auf Multiplikation mit Einheiten eindeutig bestimmt ist und sich als $g = da+eb$ mit $d,e \in R$ darstellen lässt.
>
> In euklidischen Ringen wie z. B. $\mathbb{Z}$ und Polynomringen über einem Körper können g sowie d und e mit dem (erweiterten) euklidischen Algorithmus berechnet werden.

Notation 10.30 (ggT und ggt)**.** In $\mathbb{Z}$ und $K[t]$ für einen Körper K können wir die Nichteindeutigkeit des größten gemeinsamen Teilers in Bemerkung 10.29 leicht durch eine Konvention beseitigen:

(a) Im Ring $R=\mathbb{Z}$ ist die Einheitengruppe $\mathbb{Z}^* = \{1,-1\}$. In diesem Fall besitzen zwei beliebige ganze Zahlen $m,n \in \mathbb{Z}$ also stets einen *eindeutigen nicht-negativen* größten gemeinsamen Teiler, den wir im Folgenden mit $\mathrm{ggt}(m,n) \in \mathbb{Z}$ bezeichnen werden — im Unterschied zur *Menge* $\mathrm{ggT}(m,n) = \{\mathrm{ggt}(m,n), -\mathrm{ggt}(m,n)\} \subset \mathbb{Z}$.

(b) Im Polynomring $R=K[t]$ über einem Körper K ist $K[t]^* = K^* = K\backslash\{0\}$ nach Lemma 9.9 (c), d. h. der größte gemeinsame Teiler zweier Polynome ist eindeutig bis auf Multiplikation mit einer Konstanten ungleich 0. In diesem Fall existiert zu zwei Polynomen $f,g \in K[t]$, die nicht beide gleich Null sind, also stets ein *eindeutiger normierter* größter gemeinsamer Teiler, den wir wieder mit $\mathrm{ggt}(f,g) \in K[t]$ bezeichnen.

Eine sehr wichtige Anwendung des erweiterten euklidischen Algorithmus ist, dass wir mit seiner Hilfe multiplikative Inverse in Faktorringen wie z. B. $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ konkret berechnen können. Bisher hatten wir hierzu ja nur in Satz 7.10 gesehen, dass in $\mathbb{Z}_n$ für eine Primzahl n *jedes* Element ungleich 0 ein multiplikatives Inverses besitzt — wir wussten aber noch nicht, wie wir dieses ohne Ausprobieren bestimmen können.

Folgerung 10.31 (Inversenberechnung in Faktorringen)**.** *Es seien a und b Elemente eines Hauptidealringes R und $b \notin R^*$ (so dass also $R/\langle b\rangle$ nicht der Nullring ist). Dann gilt*

$$\overline{a} \text{ ist eine Einheit in } R/\langle b\rangle \quad\Leftrightarrow\quad a \text{ und } b \text{ sind teilerfremd.}$$

Schreiben wir dann $da+eb=1$ für gewisse $d,e \in R$ wie in Satz 10.13 (b), so ist $\overline{a}^{-1} = \overline{d}$ in $R/\langle b\rangle$.

Beweis. Es gilt

$$\begin{aligned}
&\overline{a} \text{ ist eine Einheit in } R/\langle b\rangle \\
\Leftrightarrow\ &\text{es gibt ein } d \in R \text{ mit } \overline{d}\,\overline{a} = \overline{1} \text{ in } R/\langle b\rangle \\
\Leftrightarrow\ &\text{es gibt ein } d \in R \text{ mit } 1-da \in \langle b\rangle \\
\Leftrightarrow\ &\text{es gibt } d,e \in R \text{ mit } da+eb=1 && \text{(Beispiel 8.8 (a))} \\
\Leftrightarrow\ &\langle a,b\rangle = \langle 1\rangle = R \\
\Leftrightarrow\ &1 \in \mathrm{ggT}(a,b) && \text{(Satz 10.13),}
\end{aligned}$$

und in diesem Fall ist dann offensichtlich $\overline{a}^{-1} = \overline{d}$. □

Beispiel 10.32.

(a) Die Einheiten von $\mathbb{Z}_{10}$ sind nach Folgerung 10.31 die Klassen aller zu 10 teilerfremden Zahlen, also $\mathbb{Z}_{10}^* = \{\overline{1}, \overline{3}, \overline{7}, \overline{9}\}$.

(b) Aus der Gleichung $1 = -4 \cdot 11 + 5 \cdot 9$ im Beispiel von Algorithmus 10.27 erhalten wir sofort $\overline{5}^{-1} = \overline{9}$ in $\mathbb{Z}_{11}$.

Aufgabe 10.33. Bestimme $\operatorname{Im} f$ für den Gruppenhomomorphismus

$$f \colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z},\ (m,n) \mapsto 693m + 483n,$$

und gib für jedes $a \in \operatorname{Im} f$ explizit ein Urbild in $f^{-1}(\{a\})$ an.

Aufgabe 10.34. Es seien $f = t^5 + \overline{2}t^3 - t$ und $g = \overline{2}t^3 + t^2 + \overline{1}$ in $\mathbb{Z}_5[t]$.

(a) Berechne alle größten gemeinsamen Teiler von f und g und stelle einen von ihnen in der Form $df + eg$ mit $d, e \in \mathbb{Z}_5[t]$ dar.

(b) Liegt das Polynom $t^3 + t^2 + \overline{1}$ im Ideal $\langle f, g \rangle$?

(c) Ist $\overline{t^{1000}}$ eine Einheit in $\mathbb{Z}_5[t]/\langle f, g \rangle$?

Aufgabe 10.35. Zeige, dass für alle $q, m, n \in \mathbb{N}_{>0}$ mit $q \neq 1$ gilt, dass

$$\operatorname{ggt}(q^m - 1, q^n - 1) = q^{\operatorname{ggt}(m,n)} - 1.$$

Aufgabe 10.36. Es sei $I_0 \subset I_1 \subset I_2 \subset \cdots$ eine Folge von Idealen in einem Ring R, von denen jedes im nächsten enthalten ist (man spricht in diesem Fall auch von einer aufsteigenden Kette von Idealen).

(a) Zeige, dass die Vereinigung $\bigcup_{n \in \mathbb{N}} I_n$ aller dieser Ideale wieder ein Ideal in R ist.

(b) Ist R ein Hauptidealring, so zeige man, dass die Kette von Idealen ab einem gewissen Glied konstant ist, d. h. dass es ein $n_0 \in \mathbb{N}$ gibt mit $I_n = I_{n_0}$ für alle $n \geq n_0$.

(c) Gib ein Beispiel für einen Ring R und eine aufsteigende Idealkette in R an, die nicht ab einem gewissen Glied konstant ist.

Aufgabe 10.37. Es sei $I_0 \supsetneq I_1 \supsetneq I_2 \supsetneq \cdots$ eine unendliche Folge von Idealen in $\mathbb{R}[t]$. Zeige, dass $\bigcap_{n=0}^{\infty} I_n = \{0\}$.