Kapitel 5

Integritätsbereiche und Teilbarkeit

5.1 Einfache Teilbarkeitsregeln

5.1.1 Definition. Sei $(I, +, 0, -, \cdot, 1)$ ein Integritätsbereich. Sind $a, b \in I$, dann heißt a durch b *teilbar* und b ein *Teiler* von a (b „teilt“ a, in Zeichen: $b|a$) $:\Leftrightarrow \exists c \in I : a = bc$.

Elementare Teilbarkeitsregeln:

1) $\forall a \in I : a|0$,

2) $\forall a \in I : 1|a$,

3) $\forall a \in I : a|a$,

4) $\forall a, b, c \in I : a|b$ und $b|c \Rightarrow a|c$,

5) $\forall a, b, c \in I : a|b \Rightarrow a|bc$,

6) $\forall a, b, c \in I : a|b$ und $a|c \Rightarrow a|b + c$,

7) $\forall a, b, c \in I, c \neq 0 : a|b \Leftrightarrow ac|bc$,

8) $\forall a, b, c, d \in I : a|b$ und $c|d \Rightarrow ac|bd$,

9) $\forall a, b \in I, n \in \mathbb{N} : a|b \Rightarrow a^n|b^n$.

5.1.2 Definition. Sei $(I, +, 0, -, \cdot, 1)$ ein Integritätsbereich. Jeder Teiler von 1 heißt *Einheit* von I. Sei $E(I)$ die Menge aller Einheiten von I. $a, b \in I$ heißen *assoziiert* (in Zeichen: $a \sim b$) $:\Leftrightarrow \exists e \in E(I) : a = be$.

5.1.3 Beispiele. 1) $I = \mathbb{Z}$: $E(I) = \{\pm 1\}$, also $a \sim b \Leftrightarrow a = \pm b$.

2) $I = K$ (K Körper): $E(I) = K \setminus \{0\}$, also $a \sim b \Leftrightarrow a, b \neq 0 \vee a = b = 0$.

3) $I = K[x]$ (K Körper): $E(I) = K \setminus \{0\}$ (wegen $\operatorname{grad} p(x)q(x) = \operatorname{grad} p(x) + \operatorname{grad} q(x)$), also gilt: $p(x) \sim q(x) \Leftrightarrow \exists a \in K \setminus \{0\} : p(x) = aq(x)$.

5.1.4 Satz. a) *$e \in I$ ist eine Einheit von $I \Leftrightarrow \exists f \in I : ef = 1$.*

b) *$(E(I), \cdot)$ ist eine abelsche Gruppe, genannt die* Einheitengruppe *von I.*

c) *$\sim$ ist eine Kongruenzrelation auf $(I, \cdot)$.*

d) *$\forall a, b \in I : a \sim b \Leftrightarrow a|b$ und $b|a$.*

Beweis. a) folgt unmittelbar aus der Definition.

b) $1 \in E(I)$; $e_1, e_2 \in E(I) \Rightarrow \exists f_1, f_2 : e_1 f_1 = e_2 f_2 = 1 \Rightarrow (e_1 e_2)(f_1 f_2) = 1 \cdot 1 = 1 \Rightarrow e_1 e_2 \in E(I)$; $e \in E(I) \Rightarrow \exists f : ef = 1 \Rightarrow f \in E(I)$, und f ist Inverses zu e. (Vgl. auch Übungsbeispiel 18.)

c) $a \sim a$, denn $a = a \cdot 1$; $a \sim b \Rightarrow a = be \Rightarrow b = ae^{-1}$ $(e, e^{-1} \in E(I)) \Rightarrow b \sim a$; $a \sim b$, $b \sim c \Rightarrow a = be$, $b = cf \Rightarrow a = c(ef) \Rightarrow a \sim c$ (wegen $ef \in E(I)$). Also ist $\sim$ eine Äquivalenzrelation. Weiters gilt: $a \sim b$, $c \sim d \Rightarrow a = be$, $c = df \Rightarrow ac = (bd)(ef) \Rightarrow ac \sim bd$.

d) $\Rightarrow$: $a \sim b \Rightarrow a = be$, $b = ae^{-1} \Rightarrow b|a$ und $a|b$.
$\Leftarrow$: $b|a$ und $a|b \Rightarrow a = bc$ und $b = ad \Rightarrow a = adc$. Für $a = 0$ ist auch $b = 0$. Für $a \neq 0$ ist $1 = dc$, also $d, c \in E(I)$, d.h., $a \sim b$. □

5.1.5 Beispiele. Äquivalenzklassen bezüglich $\sim$:

1) $I = \mathbb{Z}$: $\{0\}$, $\{\pm 1\}, \{\pm 2\}, \ldots, \{\pm n\}, \ldots$, $n \in \mathbb{N}$.

2) $I = K$: $\{0\}, K \setminus \{0\}$.

3) $I = K[x]$: $\{0\}$, $\{ap(x) \mid a \in K \setminus \{0\}\}$, $p(x)$ normiert.

5.1.6 Definition. Sei $(I, +, 0, -, \cdot, 1)$ ein Integritätsbereich, $a \in I$.

Triviale Teiler von a: alle $e \in E(I)$ und alle b mit $b \sim a$.
Echte Teiler von a: alle b mit $b|a$ und $b \not\sim a$.

5.1.7 Definition. $a \in I \setminus E(I)$, $a \neq 0$, heißt *irreduzibel* $:\Leftrightarrow$ a hat nur triviale Teiler.

5.1.8 Beispiele. 1) $I = \mathbb{Z}$: $a \in I$ irreduzibel $\Leftrightarrow a = \pm p$, p Primzahl.

2) $I = K[x]$ (K Körper): Die irreduziblen Elemente heißen *irreduzible Polynome*. Z.B. ist ein lineares Polynom $ax + b$, $a \neq 0$, stets irreduzibel. In einem algebraisch abgeschlossenen Körper ist jedes irreduzible Polynom auch linear.

3) $I = \mathbb{R}[x]$: Irreduzibel sind hier alle linearen Polynome sowie alle Polynome $ax^2 + bx + c$ mit $a \neq 0$ und $b^2 - 4ac < 0$. (Aus dem Fundamentalsatz der Algebra folgt, dass es keine weiteren gibt.)

4) $I = K[x]$, K endlicher Körper: Zu jedem $n \in \mathbb{N}$ gibt es ein $p(x) \in K[x]$ mit $\operatorname{grad} p(x) = n$ und $p(x)$ irreduzibel. (Siehe Abschnitt 6.6 über endliche Körper.)

5.1.9 Definition. $p \in I \setminus E(I)$, $p \neq 0$, heißt *primes Element* oder *Primelement* $:\Leftrightarrow p|ab \Rightarrow p|a$ oder $p|b$.

5.1.10 Beispiel. Für $I = \mathbb{Z}$, $K[x]$ (K Körper) gilt: p irreduzibel $\Leftrightarrow$ p prim (folgt aus Abschnitt 5.3 und 5.4).

5.1.11 Anmerkungen. 1) a irreduzibel und $b \sim a \Rightarrow b$ irreduzibel.

2) p prim und $q \sim p \Rightarrow q$ prim.

3) p prim $\Rightarrow p$ irreduzibel, denn: $a|p \Rightarrow \exists b \in I : p = ab \Rightarrow p|ab \Rightarrow (p|a$ oder $p|b)$ und $a|p$ und $b|p$. Also gilt $p \sim a$ oder $p \sim b$. Im Falle $p \sim b$ ist $p = eb = ab$ für eine Einheit e. Wegen $p \neq 0$ ist $b \neq 0$ und daher $a = e$. Also ist in jedem Falle a ein trivialer Teiler von p. (Die Umkehrung von 3) gilt im allgemeinen nicht!)

5.2 ZPE-Ringe

5.2.1 Definition. Ein Integritätsbereich I heißt ein *ZPE-Ring* (Ring mit Primelementzerlegung, Ring mit eindeutiger Primelementzerlegung, Gauß'scher Ring, faktorieller Ring) :$\Leftrightarrow$ Zu jedem $a \in I \setminus E(I)$, $a \neq 0$, gibt es Primelemente $p_1, \ldots, p_r$ mit $a = p_1 \cdots p_r$.

5.2.2 Satz (Eindeutigkeit der Primelementzerlegung). *Sei I ein ZPE-Ring, $a \in I \setminus E(I)$, $a \neq 0$, $a = p_1 \cdots p_r = q_1 \cdots q_s$ mit Primelementen $p_1, \ldots, p_r, q_1, \ldots, q_s$. Dann ist $r = s$, und es gibt eine Permutation π von $\{1, \ldots, r\}$ mit $p_i \sim q_{\pi(i)}$, $i = 1, \ldots, r$.*

Beweis. Da $p_1 | q_1 \cdots q_s$, gibt es ein $\pi(1)$, $1 \leq \pi(1) \leq r$ mit $p_1 | q_{\pi(1)}$, d.h., $p_1 \sim q_{\pi(1)}$. Für eine geeignete Einheit e_1 gilt daher $e_1 p_2 \cdots p_r = q_1 \cdots q_{\pi(1)-1} \cdot q_{\pi(1)+1} \cdots q_s$. Durch wiederholte Anwendung dieser Überlegung erhält man schließlich die Behauptung. □

5.2.3 Satz (Teilerkettenbedingung). *Sei I ein ZPE-Ring. Dann gibt es keine unendliche Folge $(a_n)_{n \in \mathbb{N}}$ von Elementen von I, sodass für alle $n \in \mathbb{N}$ das Element a_{n+1} ein echter Teiler von a_n ist.*

Beweis. Es genügt, zu zeigen, dass es in $I \setminus \{0\}$ keine solche Folge geben kann. Nach dem gerade bewiesenen Satz gibt es zu jedem Element $a \in I \setminus \{0\}$ eine eindeutig bestimmte Zahl $r = r(a)$, sodass sich a als Produkt von r Primelementen schreiben lässt. (Für Einheiten a setzen wir $r(a) = 0$.)
Wenn b ein echter Teiler von a ist, dann ist $r(b) < r(a)$.
Wenn also $r(a_1) = k$ ist, dann kann es keine Folge $(a_n)_{n=1,\ldots,k+1,k+2}$ von Elementen von $I \setminus \{0\}$ geben, sodass für alle $n \leq k+1$ das Element a_{n+1} ein echter Teiler von a_n ist; erst recht kann es keine unendliche solche Folge geben. □

5.2.4 Beispiele. $\mathbb{Z}$ und $K[x]$ (K Körper) sind ZPE-Ringe (Beweis folgt aus Abschnitt 5.3 und 5.4).

5.2.5 Definition. Sei I Integritätsbereich, $a_1, \ldots, a_n \in I$.

1) $d \in I$ heißt ein *größter gemeinsamer Teiler* (ggT) von $a_1, \ldots, a_n \in I$:$\Leftrightarrow$ (i) $d | a_i$, $i = 1, \ldots, n$ und (ii) $\forall t \in I : t | a_i$, $i = 1, \ldots, n \Rightarrow t | d$.

2) $v \in I$ heißt ein *kleinstes gemeinsames Vielfaches* (kgV) von $a_1, \ldots, a_n \in I$:$\Leftrightarrow$ (i) $a_i | v$, $i = 1, \ldots, n$ und (ii) $\forall w \in I : a_i | w$, $i = 1, \ldots, n \Rightarrow v | w$.

5.2.6 Anmerkung. Sei d ein ggT von $a_1, \ldots, a_n$ und $d_1 \in I$. Dann gilt: d_1 ist ein ggT von $a_1, \ldots, a_n \Leftrightarrow d_1 \sim d$. Eine entsprechende Aussage gilt für das kgV.

5.2.7 Satz. *In einem ZPE-Ring I ist jedes irreduzible Element prim.*

Beweis. $a \in I$, a irreduzibel $\Rightarrow a \notin E(I)$, $a \neq 0 \Rightarrow a = p_1 \cdots p_r$ mit p_i prim $\Rightarrow p_1 | a$, $p_1 \notin E(I)$, d.h., $p_1 \sim a \Rightarrow a$ prim. □

Wir betrachten die Quotientenmenge $I/\!\sim = \{[a]_\sim \mid a \in I\}$ und denken uns aus jeder Klasse $[a]_\sim = \{b \in I \mid b \sim a\}$ ein festes Element $\mathbf{n}([a]_\sim)$ herausgegriffen (Auswahlaxiom!), d.h.,

$$\mathbf{n} : \begin{cases} I/\!\sim \to I \\ [a]_\sim \mapsto \mathbf{n}([a]_\sim) \in [a]_\sim. \end{cases}$$

Die Elemente der Menge $\mathbf{n}(I/\!\sim)$ heißen *normierte Elemente* (bezüglich $\mathbf{n}$).

Jede Klasse $[a]_\sim$ mit a prim besteht zur Gänze aus Primelementen. Die Elemente $\mathbf{n}([a]_\sim)$ mit a prim heißen *normierte Primelemente*.

5.2.8 Beispiele. 1) $I = \mathbb{Z}$, $\mathbf{n}([a]_\sim) = \mathbf{n}(\{\pm a\}) = |a|$.

2) $I = K[x]$, $\mathbf{n}(\{0\}) = 0$, $\mathbf{n}([p(x)]_\sim) = q(x)$, wobei $p(x) = a_n x^n + \cdots + a_1 x + a_0$, $a_n \neq 0$, $q(x) = (1/a_n)p(x)$. Wir wählen also aus jeder $\sim$-Klasse das Polynom mit höchstem Koeffizienten 1 aus.

5.2.9 Satz. *Ist I ein ZPE-Ring, $a \in I \setminus E(I)$, $a \neq 0$, dann gilt $a = ep_1^{e_1} \cdots p_r^{e_r}$, wobei $e \in E(I)$, $p_1, \ldots, p_r$ normierte, paarweise verschiedene Primelemente, $e_i \in \mathbb{N}$.* □

5.2.10 Lemma. *Sei I ein ZPE-Ring, $a, b \in I \setminus \{0\}$, $a = fp_1^{f_1} \cdots p_r^{f_r}$, $b = gp_1^{g_1} \cdots p_r^{g_r}$ (p_j prim, normiert und paarweise verschieden, $f_j, g_j \in \mathbb{N}_0$, $f, g \in E(I)$). Dann gilt: $a|b \Leftrightarrow f_j \leq g_j$ für $j = 1, \ldots, r$.*

Beweis. $a|b \Rightarrow \exists c \in I : b = ac \Rightarrow c = hp_1^{h_1} \cdots p_r^{h_r}$, $h_j \in \mathbb{N}_0$, $h \in E(I)$ (da I ZPE-Ring) $\Rightarrow f_j + h_j = g_j$, $j = 1, \ldots, r \Rightarrow f_j \leq g_j$, $j = 1, \ldots, r$.
Umkehrung: Ist $f_j \leq g_j$, $j = 1, \ldots, r$, so gilt mit $h_j := g_j - f_j \in \mathbb{N}_0$, $c := f^{-1}gp_1^{h_1} \cdots p_r^{h_r}$: $ac = b$, d.h., $a|b$. □

5.2.11 Satz. *Sei I ein ZPE-Ring, $a_1, \ldots, a_n \in I$, $a_i \neq 0$, $a_i = e_i p_1^{e_{1i}} \cdots p_r^{e_{ri}}$, $e_i \in E(I)$, p_j paarweise verschiedene normierte Primelemente, $e_{ji} \in \mathbb{N}_0$. Dann gilt:*

$$\mathrm{ggT}(a_1, \ldots, a_n) = p_1^{\min_{1 \leq i \leq n}(e_{1i})} \cdots p_r^{\min_{1 \leq i \leq n}(e_{ri})}$$

und

$$\mathrm{kgV}(a_1, \ldots, a_n) = p_1^{\max_{1 \leq i \leq n}(e_{1i})} \cdots p_r^{\max_{1 \leq i \leq n}(e_{ri})}.$$

Sind einige $a_i = 0$, so ist $\mathrm{ggT}(a_1, \ldots, a_n) = \mathrm{ggT}(a_i \mid a_i \neq 0)$, sind alle $a_i = 0$, so ist $\mathrm{ggT}(a_1, \ldots, a_n) = 0$. Sind einige $a_i = 0$, so ist $\mathrm{kgV}(a_1, \ldots, a_n) = 0$.

Beweis. Sei $d := p_1^{\min_{1 \leq i \leq n}(e_{1i})} \cdots p_r^{\min_{1 \leq i \leq n}(e_{ri})}$.
(i) $\min_i(e_{ji}) \leq e_{jk}$ für alle $k \in \{1, \ldots, n\} \Rightarrow d|a_k$, $k = 1, \ldots, n$.
(ii) $t|a_k$ für alle $k \in \{1, \ldots, n\} \Rightarrow t = fp_1^{f_1} \cdots p_r^{f_r}$ mit $f \in E(I)$, $f_j \leq e_{jk}$, $k = 1, \ldots, n$, $j = 1, \ldots, r \Rightarrow f_j \leq \min_i(e_{ji})$, $j = 1, \ldots, r \Rightarrow t|d$.
Die Sonderfälle (einige oder alle $a_i = 0$) sind trivial.
Die Aussage über das kgV beweist man analog zum ggT. □

5.2.12 Satz. *Sei I ein ZPE-Ring, und $\wedge, \vee$ auf $I/\sim = \{[a]_\sim \mid a \in I\}$ definiert durch*

$$[a]_\sim \wedge [b]_\sim := [\mathrm{ggT}(a, b)]_\sim, \qquad [a]_\sim \vee [b]_\sim := [\mathrm{kgV}(a, b)]_\sim.$$

Dann sind $\wedge$ und $\vee$ wohldefiniert (d.h., vom Repräsentanten unabhängig) und $(I/\sim, \wedge, \vee)$ ist ein Verband mit Nullelement $[1]_\sim = E(I)$ und Einselement $[0]_\sim = \{0\}$ („Teilerverband“). Die zugehörige Ordnung $\leq$ ist gegeben durch: $[a]_\sim \leq [b]_\sim :\Leftrightarrow a|b$.

Der Beweis dieses Satzes folgt unschwer aus den Definitionen. □

5.2.13 Beispiel. $(\mathbb{Z}/\sim, \wedge, \vee) \cong (\mathbb{N}_0, \mathrm{ggT}, \mathrm{kgV})$.

5.2.A Charakterisierung von ZPE-Ringen

5.2.14 Satz. *Ein Integritätsbereich I ist genau dann ZPE-Ring, wenn die folgenden Bedingungen erfüllt sind:*

(a) *Jedes irreduzible Element ist prim.*

(b) *Teilerkettenbedingung: es gibt keine unendliche Folge $(a_n)_{n\in\mathbb{N}}$ von Elementen von I, sodass für alle $n \in \mathbb{N}$ das Element a_{n+1} ein echter Teiler von a_n ist.*

Beweis. Wir wissen bereits, dass jeder ZPE-Ring die Bedingungen (a) und (b) erfüllt. Zu zeigen ist die Umkehrung.
Sei also I ein Integritätsbereich, der die Bedingungen (a) und (b) erfüllt. Sei $a \in I$, $a \neq 0$, $a \notin E(I)$. Wir haben zu zeigen, dass a eine Primelementzerlegung besitzt.
Indirekt: Angenommen, es gibt keine Primelementzerlegung von a. Dann ist a kein Primelement, wegen (a) also nicht irreduzibel. Somit existiert ein nichttrivialer Teiler a_1 von a, d.h., $a = a_1b_1$, wobei a_1, b_1 beide echte Teiler sind. (Denn: $b_1 \sim a \Rightarrow b_1 = ae$, $e \in E(I) \Rightarrow a = a_1ae \Rightarrow 1 = a_1e \Rightarrow a_1 \in E(I)$, Widerspruch!)
Einer der beiden Teiler (o.B.d.A. a_1) hat keine Primelementzerlegung (sonst hätte ja a eine solche). Daher existiert ein echter Teiler a_2 von a_1, welcher ebenfalls keine Primelementzerlegung besitzt. Auf diese Weise wäre es möglich, eine unendliche echte Teilerkette $a, a_1, a_2, \ldots$ zu konstruieren, was der Bedingung (b) widerspricht. □

5.3 Hauptidealringe

5.3.1 Satz. *Sei R ein kommutativer Ring mit Einselement, $a \in R$, $(a) := \{ar \mid r \in R\}$. Dann ist (a) das kleinste Ideal von R, welches a enthält.*

Beweis. (a) ist Ideal: $0 = a0 \in (a)$; $ar_1, ar_2 \in (a) \Rightarrow ar_1 + ar_2 = a(r_1 + r_2) \in (a)$; $-ar_1 = a(-r_1) \in (a)$; für beliebiges $r \in R$ ist $r(ar_1) = a(rr_1) \in (a)$. Weiters ist $a = a \cdot 1 \in (a)$. Da jedes Ideal, welches a enthält, alle ar, $r \in R$, und damit (a) enthalten muss, ist (a) das kleinste Ideal, welches a enthält. □

5.3.2 Definition. (a) heißt das *von a erzeugte Hauptideal* von R. Ein Ideal heißt Hauptideal, wenn es von der Form (a) für ein $a \in R$ ist.

5.3.3 Definition. Ein Integritätsbereich I heißt *Hauptidealring* :⇔ Jedes Ideal von I ist ein Hauptideal.

5.3.4 Beispiele. 1) Jeder Körper ist ein Hauptidealring: $\{0\} = (0)$ und $K = (1)$ sind die einzigen Ideale, da K einfach ist.

2) $\mathbb{Z}$, $K[x]$ (K Körper) sind Hauptidealringe (siehe Abschnitt 5.4).

3) $\mathbb{Q}[x, y]$ ist kein Hauptidealring. Das von der Menge $\{x, y\}$ erzeugte Ideal (anders gesagt: der Kern des Homomorphismus $h : \mathbb{Q}[x, y] \to \mathbb{Q}$, der jedem Polynom seinen konstanten Term zuordnet) ist kein Hauptideal.

4) $\mathbb{Z}[x]$ ist kein Hauptidealring.

Zu 3) und 4) vgl. das allgemeinere Übungsbeispiel 84: Wenn R ein Integritätsbereich ist, und $a \in R$ kein multiplikatives Inverses hat, dann ist das von $\{a, x\}$ erzeugte Ideal kein Hauptideal.

5.3.5 Lemma. *Sei I ein Integritätsbereich, dann gilt:*

1) $a|b \Leftrightarrow (a) \supseteq (b)$.

2) $a \sim b \Leftrightarrow (a) = (b)$.

Beweis. Folgt aus den Definitionen. □

5.3.6 Definition. Sei R ein kommutativer Ring mit Einselement, $J \lhd R$ (d.h., J Ideal von R), $J \neq R$. Dann heißt J

1) *maximales Ideal* $:\Leftrightarrow \forall K\,(K \lhd R, J \subseteq K \subseteq R \;\Rightarrow\; K = J \text{ oder } K = R)$,

2) *Primideal* $:\Leftrightarrow (ab \in J \Rightarrow a \in J \text{ oder } b \in J)$.

5.3.7 Satz. *Sei R ein kommutativer Ring mit Einselement und $J \lhd R$, dann gilt:*

a) *R/J Körper $\Leftrightarrow$ J maximales Ideal,*

b) *R/J Integritätsbereich $\Leftrightarrow$ J Primideal.*

Beweis. Übungsbeispiele 86 und 87. □

5.3.8 Folgerung. Jedes maximale Ideal ist ein Primideal.

5.3.9 Satz. *Sei I ein Integritätsbereich, $p \in I$, $p \neq 0$, $p \notin E(I)$. Dann gilt:*

a) *(p) maximal in der Menge aller Hauptideale $\neq I \Leftrightarrow p$ irreduzibel,*

b) *(p) Primideal $\Leftrightarrow p$ prim.*

Beweis. a) $\Rightarrow$: $a|p \Rightarrow (a) \supseteq (p) \;\Rightarrow\; (a) = (p)$ oder $(a) = I = (1) \;\Rightarrow\; a \sim p$ oder $a \sim 1 \;\Rightarrow$ p irreduzibel.
$\Leftarrow$: analog.

b) $\Rightarrow$: $p|ab \Rightarrow ab \in (p) \Rightarrow a \in (p)$ oder $b \in (p) \Rightarrow p|a$ oder $p|b$.
$\Leftarrow$: analog. □

5.3.10 Folgerung. Sei I ein Hauptidealring, $p \in I$, $p \neq 0$, $p \notin E(I)$. Dann gilt:

a) p prim $\Leftrightarrow p$ irreduzibel,

b) $I/(p)$ Körper $\Leftrightarrow p$ irreduzibel.

5.3.11 Beispiel. $\mathbb{Z} = \mathbb{Z}/(n)$ ist Körper $\Leftrightarrow n = \pm p$, p Primzahl.

5.3.12 Satz. *Sei I Hauptidealring, $a_1, \ldots, a_n \in I$. Dann existiert* $\mathrm{ggT}(a_1, \ldots, a_n) =: d$, *und es gibt $x_1, \ldots, x_n \in I$ mit $d = a_1x_1 + \cdots + a_nx_n$.*

Beweis. Sei $M := \{a_1r_1 + \cdots + a_nr_n \mid r_i \in I\}$. Dann gilt $M \lhd I$ (analog wie für das Hauptideal (a) einzusehen). Somit gibt es ein $d \in I$ mit $M = (d)$. Wir zeigen: $d = \mathrm{ggT}(a_1, \ldots, a_n)$: wegen $a_1, \ldots, a_n \in M = (d)$ gilt $d|a_1, \ldots, d|a_n$; aus $t|a_1, \ldots, t|a_n$ folgt $t|a_1r_1 + \cdots + a_nr_n$, $\forall r_1, \ldots, r_n \in I$, und daraus $t|d$ (denn $d \in M$). □

5.3.13 Lemma (Teilerkettensatz). *Sei I Hauptidealring. Dann gibt es* keine *unendliche Folge $(a_n)_{n\in\mathbb{N}}$ von Elementen von I, sodass für alle $n \in \mathbb{N}$ das Element a_{n+1} ein echter Teiler von a_n ist.*

Beweis. Angenommen, es gibt eine solche Folge $(a_n)_{n\in\mathbb{N}}$. Dann muss $(a_1) \subset (a_2) \subset \ldots \subset (a_n) \subset (a_{n+1}) \subset \ldots$ gelten, wobei alle auftretenden Inklusionen echt sind. Für $J := \bigcup_{n=1}^{\infty}(a_n)$ gilt dann $J \lhd I$, denn: $0 \in J$; $a, b \in J \Rightarrow \exists n, m \in \mathbb{N}$ (o.B.d.A. $n \geq m$): $a \in (a_n)$, $b \in (a_m) \Rightarrow a, b \in (a_n) \Rightarrow a + b, -a, ra \in (a_n)$, $r \in I$, $\Rightarrow a + b, -a, ra \in J$. Also gibt es ein $d \in I$ mit $J = (d)$. Wegen $d \in J$ ist $d \in (a_n)$ für ein $n \in \mathbb{N}$ und damit $(d) \subseteq (a_n) \subseteq (d)$, woraus $(a_n) = (a_{n+1}) = \ldots$ folgt. Widerspruch zur Annahme! □

5.3.14 Folgerung. Jeder Hauptidealring ist ein ZPE-Ring.

5.4 Euklidische Ringe

5.4.1 Definition. Ein Integritätsbereich I heißt ein *Euklidischer Ring* $:\Leftrightarrow$ Es gibt eine Abbildung $H : I \setminus \{0\} \to \mathbb{N}_0$ („Euklidische Bewertung“) mit folgender Eigenschaft: für alle $a \in I \setminus \{0\}$, $b \in I$ gibt es $q, r \in I$, sodass $b = aq + r$ mit $r = 0$ oder $H(r) < H(a)$ („Division mit Rest“).

5.4.2 Beispiele. 1) $\mathbb{Z}$ ist ein Euklidischer Ring mit $H(a) := |a|$. (Siehe 1.7.15.)

2) Jeder Körper ist ein Euklidischer Ring ($q = a^{-1}b$, $r = 0$).

5.4.3 Satz. *$K[x]$ (K Körper) ist ein Euklidischer Ring mit $H(p(x)) := \operatorname{grad} p(x)$, d.h., für $p(x) \neq 0$, $p_1(x)$ beliebig, gibt es Polynome $q(x)$ und $r(x)$ mit $p_1(x) = p(x)q(x) + r(x)$, wobei $r(x) = 0$ oder $\operatorname{grad} r(x) < \operatorname{grad} p(x)$.*

Beweis. Sei $p(x) = a_m x^m + \cdots + a_1 x + a_0$, $a_m \neq 0$, $m = \operatorname{grad} p(x)$, $p_1(x) = b_n x^n + \cdots + b_1 x + b_0$. Für $n < m$ kann $q(x) = 0$ und $r(x) = p_1(x)$ gewählt werden. Für $n \geq m$ sei $p_2(x) := p_1(x) - b_n a_m^{-1} x^{n-m} p(x)$. Wir haben $p_2(x) = c_k x^k + \cdots + c_1 x + c_0$ mit $k \leq n-1$. Für $k < m$ kann $q(x) = b_n a_m^{-1} x^{n-m}$ und $r(x) = p_2(x)$ gewählt werden. Für $k \geq m$ sei $p_3(x) := p_2(x) - c_k a_m^{-1} x^{k-m} p(x)$. Wir haben $p_3(x) = d_l x^l + \cdots + d_1 x + d_0$ mit $l \leq k-1$. Für $l < m$ kann $q(x) = b_n a_m^{-1} x^{n-m} + c_k a_m^{-1} x^{k-m}$ und $r(x) = p_3(x)$ gewählt werden. Für $l \geq m$ wird das Verfahren fortgesetzt, und man erhält nach endlich vielen Schritten ein Polynom $p_t(x)$ mit $p_t(x) = 0$ oder $\operatorname{grad} p_t(x) < m$. □

5.4.4 Satz. *Jeder Euklidische Ring I ist ein Hauptidealring.*

Beweis. Sei $J \lhd I$, $J \neq (0) = \{0\}$. Zu zeigen: $\exists a \in I : J = (a) = \{aq \mid q \in I\}$. Sei $a \in J \setminus \{0\}$ so gewählt, dass $H(a) = \min\{H(x) \mid x \in J \setminus \{0\}\}$. Wir behaupten, dass dann $J = (a)$ gilt. Trivialerweise gilt $(a) \subseteq J$. Sei umgekehrt $b \in J$. Wegen $a \neq 0$ gibt es $q, r \in I$ mit $b = aq + r$ und $r = 0 \vee H(r) < H(a)$. Es ist $r = b - aq \in J$ (wegen $J \lhd I$), woraus (wegen der Minimalität von $H(a)$) $r = 0$ und damit $b = aq \in (a)$ folgt. Somit gilt auch $J \subseteq (a)$, also $J = (a)$. □

5.4.5 Folgerung. Jeder Euklidische Ring ist ein ZPE-Ring.

5.4.A Euklidischer Algorithmus

Der Euklidische Algorithmus ist ein Algorithmus zur Berechnung des ggT in Euklidischen Ringen.

Sei I Euklidischer Ring und $a, b \in I$. Für $a = b = 0$ ist $\operatorname{ggT}(a, b) = 0$. Sei o.B.d.A. $a \neq 0$.

$$
\begin{aligned}
&\Rightarrow \exists q_1, r_1 \in I : b = aq_1 + r_1,\ r_1 = 0 \text{ oder } H(r_1) < H(a),\\
\text{falls } r_1 \neq 0 &\Rightarrow \exists q_2, r_2 \in I : a = r_1 q_2 + r_2,\ r_2 = 0 \text{ oder } H(r_2) < H(r_1),\\
\text{falls } r_2 \neq 0 &\Rightarrow \exists q_3, r_3 \in I : r_1 = r_2 q_3 + r_3,\ r_3 = 0 \text{ oder } H(r_3) < H(r_2),\\
&\ \ \vdots\\
&\text{allgemein:}\\
\text{falls } r_i \neq 0 &\Rightarrow \exists q_{i+1}, r_{i+1} \in I : r_{i-1} = r_i q_{i+1} + r_{i+1},\ r_{i+1} = 0 \text{ oder } H(r_{i+1}) < H(r_i).\\
&\qquad \text{(Dabei ist } a = r_0 \text{ und } b = r_{-1} \text{ zu setzen.)}
\end{aligned}
$$

Nach endlich vielen Schritten (wegen $H(a) = H(r_0) > H(r_1) > H(r_2) > \ldots$) erhält man ein k mit $r_k = 0$ und $r_{k-1} \neq 0$. Wir zeigen nun: $r_{k-1} = \mathrm{ggT}(a, b)$. Wir haben:

$$\begin{aligned} r_{k-2} = r_{k-1}q_k + 0 &\Rightarrow r_{k-1} | r_{k-2}, \\ r_{k-3} = r_{k-2}q_{k-1} + r_{k-1} &\Rightarrow r_{k-1} | r_{k-3}, \\ r_{k-4} = r_{k-3}q_{k-2} + r_{k-2} &\Rightarrow r_{k-1} | r_{k-4}, \\ &\vdots \\ r_1 = r_2 q_3 + r_3 &\Rightarrow r_{k-1} | r_1, \\ a = r_1 q_2 + r_2 &\Rightarrow r_{k-1} | a, \\ b = a q_1 + r_1 &\Rightarrow r_{k-1} | b, \end{aligned}$$

also gilt $r_{k-1}|a$ und $r_{k-1}|b$. Gilt umgekehrt $t|a$ und $t|b$, dann folgt analog: $t|r_1$, $t|r_2$, $t|r_3$, $\ldots$, $t|r_{k-1}$.

Wir haben für Hauptidealringe gezeigt: $\mathrm{ggT}(a, b) = ax + by$ mit $x, y \in I$. In Euklidischen Ringen kann man x, y berechnen:

$$\begin{aligned} \mathrm{ggT}(a,b) &= r_{k-1} = r_{k-3} + r_{k-2}(-q_{k-1}) = r_{k-3} + (r_{k-4} - r_{k-3}q_{k-2})(-q_{k-1}) = \\ &= r_{k-4}\underbrace{(-q_{k-1})}_{\in I} + r_{k-3}\underbrace{(1 + q_{k-2}q_{k-1})}_{\in I} = \ldots = ax + by. \end{aligned}$$

5.4.6 Anmerkung. 1) In jedem ZPE-Ring gibt es zu beliebigen Elementen a, b immer einen größten gemeinsamen Teiler; diesen kann man nach 5.2.11 bestimmen, wenn man die Primzerlegung der Elemente a und b kennt.

2) Wenn R Hauptidealring ist, weiß man überdies (siehe 5.3.12), dass sich der größte gemeinsame Teiler von a und b in als R-Linearkombination von a und b schreiben lässt.

3) Wenn schließlich R euklidischer Ring ist, dann haben wir sogar einen expliziten Algorithmus, der den ggT sowie diese Linearkombination findet. (Für den Fall $R = \mathbb{Z}$ ist dieser Algorithmus weit schneller als das Finden der Primfaktorzerlegung.)