§ 4 Teilbarkeit in Integritätsbereichen

In diesen Kapitel sind alle Ringe kommutativ !

1. Def Sei R ein kommutativer Ring, seien $a, b \in R$.

Wir nennen a ein Teiler von b, wenn es ein $x \in R$ gibt mit $ax = b$. Schreibe dafür kurz

$$a \mid b \quad (\text{"}a \text{ teilt } b\text{"})$$

Wenn a kein Teiler v. b ist, schreibe $a \nmid b$.

Klar: $1 \mid a$ und $a \mid 0$ gilt für alle $a \in R$.

Weiter $a \mid 1 \Leftrightarrow a$ Einheit

$a \mid b$ und $b \mid c \Rightarrow a \mid c$

Wenn a kein Nullteiler ist und wenn gilt

$a \mid b$ und $b \mid a$, so folgt: es gibt ein Einheit $u \in R^*$ mit $au = b$.

Denn: $b = ax$ $a = by \Rightarrow a = axy \Rightarrow 1 = xy$
↑ a kein Nullteiler.

Ist $u \in R^*$, so teilt stets $ua \mid a$.

Sind $b_1, \dots, b_n \in R$ und gilt

$a \mid b_1, \dots, a \mid b_n$, so folgt $a \mid b_1 + \dots + b_n$.

Def Sei R ein Integritätsbereich, seien $b_1, \dots, b_n \in R$.
Wir nennen a einen *größten gemeinsamen Teiler* von $b_1, \dots, b_n$, wenn gilt:

(1) $a \mid b_1, \dots, a \mid b_n$

(2) Ist $c \in R$ mit $c \mid b_1, \dots, c \mid b_n$, so folgt $c \mid a$.

Schreibweise $a \in ggT(b_1, \dots, b_n)$. (Der ggT ist im allgemeinen nicht eindeutig bestimmt: ist $u \in R^*$ und $a \in ggT(b_1, \dots, b_n)$, so folgt $au \in ggT(b_1, \dots, b_n)$.
(Über die Existenz eines ggT wird hier nichts behauptet.)

2. **Def** Sei R ein kommutativer Ring, seien $a_1, \dots, a_n \in R$.
Wir setzen $(a_1, \dots, a_n) = a_1 R + \dots + a_n R$ und nennen
(Übliche, aber etwas problematische Schreibweise – links steht also kein n-Tupel...).
Ist speziell $n = 1$, so heißt $(a_1) = a_1 R$ das von a_1 erzeugte *Hauptideal*.
Ein Integritätsring R heißt *Hauptidealbereich*
(*Hauptidealring*, engl. principal ideal domain PID)
wenn alle Ideale in R Hauptideale sind. ⊣

Bsp (a) Jeder Körper K ist ein Hauptidealbereich, denn $\{0\} = (0)$ und $K = (1)$ sind die einzigen Ideale

(b) $\mathbb{Z}$ ist Hauptidealbereich nach §3.8

3. Lemma Sei R ein Integritätsbereich, seien $b_1, \dots, b_n \in R$. Wenn gilt $(b) = (b_1, \dots, b_n)$, so ist b ein ggT von $b_1, \dots, b_n$.

Beweis Aus $b_j \in (b)$ folgt $b \mid b_j$ für $j = 1, \dots n$. Aus $b \in (b_1, \dots, b_n)$ folgt $b = r_1 b_1 + \dots + r_n b_n$ für $r_1, \dots, r_n \in R$. Ist also d ein Teiler von $b_1, \dots, b_n$, so folgt $d \mid b$. □

Korollar (Lemma von Bézout) Ist $b_1, \dots, b_n \in \mathbb{Z}$ so gibt es $r_1, \dots, r_n \in \mathbb{Z}$ mit $d = r_1 b_1 + \dots + r_n b_n$, wobei $d \in \mathrm{ggT}(b_1, \dots, b_n)$ □

4. Def Sei R ein Integritätsbereich, sei $r \in R$, $r \neq 0$, $r \notin R^*$.

(a) r heißt irreduzibel, wenn aus $r = x \cdot y$ für $x, y \in R$ folgt, dass $x \in R^*$ oder $y \in R^*$

(b) r heißt prim, wenn aus $r \mid xy$ für $x, y \in R$ folgt, dass $r \mid x$ oder $r \mid y$.

Bsp In $\mathbb{Z}$ gilt: p irreduzibel $\Leftrightarrow \pm p$ Primzahl $\Leftrightarrow p$ prim
↑ Euklids Lemma LA I §1.11

Lemma Sei R Integritätsbereich, sei $r \in R$, $r \neq 0$, $r \notin R^*$.

Dann gilt: (i) r prim $\Rightarrow$ r irreduzibel

(ii) (r) ist Primideal genau dann, wenn r prim ist.

Beweis (i) Sei r prim. $r = xy \Rightarrow r \mid xy$

prim $\Rightarrow r \mid x$ oder $r \mid y$. Wenn $r \mid x \Rightarrow x = s \cdot r \Rightarrow r = s \cdot r \cdot y$

Kürzen $\Rightarrow 1 = sy \Rightarrow y \in R^*$. (Genauso, wenn $r \mid y$). □

(ii) Sei r prim, mit $xy \in (r) \Rightarrow r \mid xy \Rightarrow r \mid x$ oder $r \mid y \Rightarrow x \in (r)$ oder $y \in (r)$.

Sei (r) Primideal und $r \mid xy \Rightarrow xy \in (r)$ und $r \mid x$ oder $r \mid y$ weil $x \in (r)$ oder $y \in (r)$ □

5. Satz Sei R ein Hauptidealbereich, mit $r \in R$, $r \neq 0$ und $r \notin R^*$.

Dann sind äquivalent: (i) r ist prim

(ii) r ist irreduzibel (iii) (r) ist maximales Ideal

(iv) (r) ist Primideal.

Beweis Wir wissen schon:

$$(iii) \overset{\S 3.13}{\Rightarrow} (iv) \overset{\S 4.4}{\Leftrightarrow} (i) \overset{\S 4.4}{\Rightarrow} (ii)$$

Zu zeigen: (ii) $\Rightarrow$ (iii). Angenommen, $(r) \subseteq J = (a)$

$\Rightarrow a \mid r \Rightarrow r = ab$ für ein $b \in R$. Weil r irreduzibel ist, folgt $a \in R^*$ oder $b \in R^*$.

$a \in R^* \Rightarrow (a) = R$ Wegen $r \notin R^*$ ist $(r) \neq R$

$b \in R^* \Rightarrow (a) = (r)$ □

Im Spezialfall $R = \mathbb{Z}$ haben wir das in §3.15 gezeigt.

Beim Faktorisieren ganzer Zahlen ist die Primfaktorzerlegung wichtig. Wir betrachten das jetzt in Integritätsbereichen.

6. Def Ein Integritätsbereich R heißt faktoriell (Faktorieller Ring, Gauß'scher Ring, ZPE-Ring "zerlegbar in Primelement", engl. UFD unique factorization domain), wenn für jedes $r \in R$ mit $r \neq 0$, $r \notin R^*$ Primelemente $p_1, \dots, p_m$ existieren mit $r = p_1 \cdots p_m$.

Satz Jeder Hauptidealbereich ist faktoriell.

Beweis Voraussetzung (ÜA): Ist $a_0, a_1, \dots \in R$ mit $(a_0) \subseteq (a_1) \subseteq \dots$ so gibt es ein $m \in \mathbb{N}$ mit $(a_m) = (a_{m+k})$ für alle $k \geq 0$, d.h. jede aufsteigende Kette von Idealen wird irgendwann stationär ("Hauptidealbereiche sind noethersch").

Sei $S = \{ s \in R \mid s \neq 0, s \notin R^*, s$ kein Produkt von Primelementen $\}$

Zu zeigen: $S = \emptyset$. Angenommen, $S \neq \emptyset$. Dann gibt es $s \in S$ so, dass es kein $t \in S$ gibt mit $(t) \supsetneq (s)$ ($\rightarrow$ Voraussetzung!)

Da s nicht prim ist, gibt es $x, y \in R - R^*$ mit $s = xy$. Es folgt $(s) \subsetneq (x)$ und $(s) \subsetneq (y)$, also $x, y \notin S$. Folglich sind x, y Produkt von primen Elementen. Aber dann ist es $s = xy$ auch $\lightning$ □

7. Theorem Sei R ein Integritätsbereich. Dann sind äquivalent: (i) R ist faktoriell

(ii) jedes Element $r \in R$ mit $r \neq 0$, $r \notin R^*$ läßt sich als Produkt irreduzibler Elemente $p_1, \dots, p_m$ schreiben, $r = p_1 \cdots p_m$. Die p_j sind bis auf Reihenfolge und Multiplikation mit Einheiten eindeutig bestimmt.

Beweis (i) $\Rightarrow$ (ii) Weil prime Elemente irreduzibel sind, ist nur die Eindeutigkeit zu zeigen. Sei $r \in R$, $r \neq 0$, $r \notin R^*$, $r = p_1 \cdots p_m = q_1 \cdots q_n$, alle q_i prim, p_j irreduzibel.

$q_1 \mid r = p_1 \cdots p_m \Rightarrow$ es gibt ein j mit $q_1 \mid p_j$.
($\uparrow q_1$ prim)

OE $j = 1$, $q_1 \mid p_1$, d.h. $q_1 \cdot u_1 = p_1 \Rightarrow u_1 \in R^*$
($\uparrow p_1$ irred, $q_1 \notin R^*$)

$\Rightarrow q_2 \cdots q_n = u_1 p_2 \cdots p_m$

Jetzt genauso weiter machen wie $m = n$ und

$p_j = q_j \cdot u_j \quad u_j \in R^*$ (ev. nach Umsortieren der p_j)

(ii) $\Rightarrow$ (i) Es bleibt zu zeigen, dass jedes irreduzible Element in R auch prim ist. Sei $r \in R$ irreduzibel mit $r \mid x \cdot y$. Ist $x \in R^*$ oder $y \in R^*$, so folgt $r \mid y$ oder $r \mid x$. Ist weder x noch y eine Einheit $x = x_1 \cdots x_m$ x_i, y_j irreduzibel
$y = y_1 \cdots y_n$

Es folgt $r \cdot s = xy = x_1 \cdots x_m y_1 \cdots y_n$ für ein $s \in R$,
also $r = u \cdot x_i$ für ein i und $u \in R^*$ oder
$r = v \cdot y_j$ für ein j und $v \in R^*$
$\Rightarrow r \mid x$ oder $r \mid y$ □

Bemerkung

(a) In faktoriellen Integritätsbereichen sind "prim" und "irreduzibel" also äquivalent.

(b) Theorem §4.7 beinhaltet den "Hauptsatz der Arithmetik" (LA I §1.11): jede ganze Zahl $m \neq 0, \pm 1$ hat eine eindeutige Primfaktorzerlegung.

8. Beobachtg Isd R faktorielle Integritätsbereich und $r = p_1^{l_1} \cdots p_m^{l_m}$, p_i irreduzibel, $l_i \geq 0$, und gilt für $i<j$, dass $p_i \neq u p_j$ für alle $u \in R^*$, so sind die Teiler s von r genau von der Form

$$s = v \cdot p_1^{k_1} \cdots p_m^{k_m} \quad \text{mit } v \in R^*, \ 0 \leq k_j \leq l_j \text{ für alle } j.$$

Es folgt: Sind $a, b \in R$, so existiert stets ein größter gemeinsamer Teiler von a und b. Ist also $b_1, \ldots, b_n \in R$, so gibt es $d \in ggT(b_1, \ldots, b_n)$. #

9. Def Sei R ein Integritätsbereich.
Eine Abbildung $\delta: R \to \mathbb{N}$ heißt Gradfunktion, wenn gilt: für alle $a, b \in R$ mit $b \neq 0$ gibt es $q, r \in R$ mit $a = bq + r$ und $\delta(r) < \delta(b)$.
Ein Integritätsbereich mit Gradfunktion heißt euklidischer Bereich (euklidischer Ring)

Bsp (a) $R = \mathbb{Z}$, $\delta(x) = |x|$ Absolutbetrag.
Mit Teilen mit Rest: ist $a, b \in \mathbb{Z}$, $b \neq 0$, so gibt es $q, r \in \mathbb{Z}$ mit $a = bq + r$, $0 \leq r < |b|$
(b) K Körper, $\delta(x) = \begin{cases} 1 & x \neq 0 \\ 0 & x = 0 \end{cases}$ ist Gradfunktion: $a = bq$ mit $q = ab^{-1}$ (Teilen ohne Rest)

10. Satz Jeder euklidische Bereich ist ein Hauptidealbereich.

Beis: Sei δ Gradfunktion auf R, sei $I \trianglelefteq R$.

Für $I = \{0\} = (0)$ ist I ein Hauptideal. Für $I \neq \{0\}$ wähle $b \in I - \{0\}$ so, dass $\delta(a)$ minimal ist. Ist $a \in I$ schon $a = bq + r$ mit $\delta(r) < \delta(b)$. Es folgt $r = a - bq \in I$, also $r = 0$ $\Rightarrow a \in (b) \Rightarrow I = (b)$ □

Gezeigt ist damit:

R Körper $\Rightarrow$ R euklid. Bereich $\Rightarrow$ R Hauptidealbereich $\Rightarrow$ R faktoriell.

(keiner der Pfeile ist umkehrbar!)

11. Lemma (Polynomdivision) Sei R ein Integritätsbereich, sei $g = a_0 + a_1 T + \dots + a_m T^m \in R[T]$ mit $\deg(g) = m \geq 0$ und $a_m \in R^*$ (Leithoeffizient).

Sei $f \in R[T]$. Dann gibt es eindeutig bestimmte Polynome $q, r \in R[T]$ mit $f = g \cdot q + r$ und $\deg(r) < m$.

Beis: Eindeutigkeit: $f = gq + r = g\tilde{q} + \tilde{r}$ mit $\deg(\tilde{r}) < m$

$\Rightarrow g(q - \tilde{q}) = \tilde{r} - r$. Da $a_m \in R^*$ folgt

$$\deg(g(q-\tilde{q})) = \underbrace{\deg(g)}_{=m} + \deg(q-\tilde{q}) = \underbrace{\deg(\tilde{r}-r)}_{<m}$$

also $\deg(q - \tilde{q}) = -\infty$ d.h. $q = \tilde{q}$ $\Rightarrow r = \tilde{r}$

Existenz: Induktion nach $\deg(f) = n$. Für $n < m$ setze $q = 0$ und $r = f$ — fertig. Sei jetzt $n \geq m \geq 0$, $f = b_0 + \dots + b_n T^n$. Setze $h = f - b_n a_m^{-1} T^{n-m} \cdot g$, es folgt $\deg(h) < n$. Also gibt es $\tilde{q}, r \in R[T]$ mit $h = g \cdot \tilde{q} + r$, $\deg(r) < m$. Es folgt

$$f = h + b_n a_m^{-1} T^{n-m} g = g\left(\tilde{q} + b_n a_m^{-1} T^{n-m}\right) + r \qquad \square$$

12. Korollar Sei K ein Körper. Dann ist der Polynomring $K[T]$ ein euklidischer Bereich und insbesondere faktoriell.

Beweis: Setze $\delta(f) = 2^{-\deg(f)}$, $2^{-\infty} = 0$

δ ist Gradfunktion nach §4.11 $\qquad \square$

Unser nächstes Ziel ist der Satz von Gauß: wenn R faktoriell ist, so ist auch $R[T]$ faktoriell.

Die Idee: betrachte $R \subseteq R[T] \subseteq Q[T]$, $Q = \mathrm{Quot}(R)$.
(R und $Q[T]$ faktoriell)

13. Sei R faktoriell Integritätsbereich.

(A) Es gilt $R[T]^* = R^*$. Ist $r \in R$ irreduzibel in R, so ist r auch irreduzibel in $R[T]$.

(ÜA)

(B) Sei $f \in R[T]$ mit $\deg(f) = m \geq 1$, $f = a_0 + \dots + a_m T^m$. Sei $d \in \mathrm{ggT}(a_0, \dots, a_m)$, es folgt mit $a_i = d \cdot b_i$, dass $f = d(b_0 + \dots + b_m T^m)$ und $1 \in \mathrm{ggT}(b_0, \dots, b_m)$.

Man nennt ein Polynom $g \in R[T]$ mit $\deg(g) = m \geq 1$ primitiv, wenn $g = b_0 + \dots + b_m T^m$ und $1 \in \mathrm{ggT}(b_0, \dots, b_m)$.

Jedes Polynom $f \in R[T]$ mit $\deg(f) \geq 1$ lässt sich also schreiben als $f = d \cdot \tilde{f}$, mit $d \in R$ und $\tilde{f} \in R[T]$ primitiv. Diese Zerlegung ist eindeutig bis auf Multiplikation mit Einheiten, weil ggT bis auf Einheit eindeutig ist.

Irreduzible Polynome vom Grad ≥ 1 sind primitiv.

(C) Sei $Q = \mathrm{Quot}(R)$ und sei $f \in Q[T]$ mit $\deg(f) \geq 1$. Dann gibt es $\tilde{f} \in R[T]$ primitiv und $z \in Q$ mit $z \cdot \tilde{f} = f$. Bis auf Multiplikation mit einer Einheit in R^* ist $\tilde{f}$ eindeutig.

Beweis: Sei $m = \deg(f) \geq 1$, $f = \frac{a_0}{b_0} + \dots + \frac{a_m}{b_m} T^m$, $a_i, b_i \in R$

$b = b_0 \cdots b_m$.

Es folgt $b \cdot f \in R[T] \rightsquigarrow b \cdot f = d \cdot \tilde{f}$ mit $\tilde{f} \in R[T]$ primitiv, $d \in R \rightsquigarrow f = \frac{d}{b} \cdot \tilde{f}$. Ist $f = \frac{x}{y} \tilde{\tilde{f}}$ mit $\tilde{\tilde{f}} \in R[T]$ primitiv, $x, y \in R$, so folgt $yd \cdot \tilde{f} = x \cdot b \cdot \tilde{\tilde{f}} \overset{(B)}{\Rightarrow} \tilde{f} = u \cdot \tilde{\tilde{f}}$ für $u \in R^*$

14. Lemma (Gauß Lemma) Sei R faktoriell, seien $f, g \in R[T]$ primitiv, $\deg(f), \deg(g) \geq 1$.
Dann ist $h = f \cdot g$ primitiv.

Beweis Angenommen, das ist falsch. Dann existiert ein Elt $p \in R$, p prim, mit $h = p \cdot \tilde{h}$ $\tilde{h} \in R[T]$. Betrachte $\varphi : R \to R/(p)$ ← kanonisch, mit (p) Primideal
und $\varphi : R[T] \to R/(p)[T]$, $a_0 + \dots + a_n T^n \mapsto \varphi(a_0) + \dots + \varphi(a_n) T^n$.
Es folgt $\varphi(h) = 0$, aber $\varphi(f) \neq 0 \neq \varphi(g)$, weil p nicht alle Koeffizienten von f und g teilt ↯ □

15. Satz Sei R faktoriell und $f \in R[T]$ mit $\deg(f) \geq 1$.
Wenn f irreduzibel in $R[T]$ ist, so ist f auch irreduzibel in $Q[T]$, $Q = \mathrm{Quot}(R)$.

Beweis Angenommen, es gibt $g, h \in Q[T]$ mit $\deg(g), \deg(h) \geq 1$ und $f = g \cdot h$ (Skalare sind Einheit in $Q[T]$). Schreibe $g = a\tilde{g}$, $h = b \cdot \tilde{h}$ mit $\tilde{g}, \tilde{h} \in R[T]$ primitiv $\Rightarrow f = ab \cdot \underbrace{(\tilde{g}\tilde{h})}_{\text{primitiv}}$. Andererseits $f = d \cdot \tilde{f}$ mit $\tilde{f}$ primitiv. Schreibe $ab = \frac{x}{y}$ mit $x, y \in R$ $\quad y \cdot d \cdot \tilde{f} = x \cdot (\tilde{g} \cdot \tilde{h}) \Rightarrow \tilde{f} = u \cdot \tilde{g} \cdot \tilde{h}$
für ein $u \in R^*$ und §4.13 (B) ↯

□

16. Theorem (Satz von Gauß) Wenn R faktorieller Integritätsbereich ist, so ist auch $R[T]$ faktoriell.

Beweis: Wir wenden Theorem §4.7 an.

Sei zuerst $f \in R[T]$ mit $\deg(f) \geq 1$ primitiv. Wenn f nicht irreduzibel ist, gibt es $g, h \in R[T]$ mit $f = g \cdot h$, $g, h \notin R[T]^* = R^*$. Weil f primitiv ist, folgt $\deg(g), \deg(h) \geq 1$ und g, h sind ebenfalls primitiv. Induktiv folgt

$$f = q_1 \cdots q_m \qquad q_i \in R[T] \text{ primitiv, irreduzibel, } \deg(q_i) \geq 1.$$

Angenommen, $\tilde{q}_1, \ldots, \tilde{q}_n \in R[T]$ sind ebenfalls irreduzibel mit $f = \tilde{q}_1 \cdots \tilde{q}_n$. Es folgt (weil f primitiv) $\deg(\tilde{q}_j) \geq 1$ und $\tilde{q}_j$ primitiv. Nach Satz §4.11 sind die $\tilde{q}_j, q_i$ irreduzibel in $Q[T]$. Da $Q[T]$ faktoriell ist, folgt $n = m$ und nach Umsortieren

$$\tilde{q}_i = a_i q_i, \quad a_i = \frac{x_i}{y_i} \in Q \qquad x_i, y_i \in R.$$ Wegen

$y_i \tilde{q}_i = x_i q_i$ folgt $a_i \in R^*$ (wie vorher)

$\Rightarrow$ die Zerlegung $f = q_1 \cdots q_n$ ist eindeutig bis auf Einheiten in R^*.

Sei jetzt $f \in R[T]$, $f \neq 0$, $f \notin R[T]^* = R^*$.

Wenn $\deg(f) = 0$, so ist $f \in R$ und hat eindeutige Zerlegung in R (weil R faktoriell) also auch in $R[T]$ nach §4.13 (A). Ist $\deg(f) \geq 1$ schreibe $f = d \cdot \tilde{f}$ mit $\tilde{f} \in R[T]$ primitiv und

$$f = c_1 \cdots c_k g_1 \cdots g_e$$

$c_i \in R$ irreduzibel
$g_j \in R[T]$ primitiv, irreduzibel, $\deg(g_j) \geq 1$

Ist $f = \tilde{c}_1 \cdots \tilde{c}_{\tilde{k}} \tilde{g}_1 \cdots \tilde{g}_{\tilde{e}}$ eine zweite Zerlegung in Primitive Elemente, mit $\tilde{c}_i \in R$, $\deg(\tilde{g}_j) \geq 1$, so sind die $\tilde{g}_j$ primitiv (weil irreduzibel). Es folgt

$$\tilde{c}_1 \cdots \tilde{c}_{\tilde{k}} = c_1 \cdots c_k \cdot u \qquad u \in R^*$$

$$\tilde{g}_1 \cdots \tilde{g}_{\tilde{e}} = g_1 \cdots g_k \cdot u^{-1}$$

und damit $k = \tilde{k}$, $l = \tilde{l}$ und (nach Umsortieren)

$$\tilde{c}_i = u_i c_i \qquad u_i \in R^*$$

$$\tilde{g}_j = v_j g_j \qquad v_j \in R^*$$

□

#