4 Teilbarkeit in Ringen

In diesem Kapitel bezeichnet R einen Integritätsbereich.

4.1 Irreduzible und Primelemente

4.1.1 Definition: Betrachte Elemente $a, b \in R$.

(a) Gilt $\exists x \in R\colon ax = b$, so schreiben wir $a|b$ und sagen *a teilt b*, und nennen a einen *Teiler von b*, und b ein *Vielfaches von a*.

(b) Gilt $\exists x \in R^\times\colon ax = b$, so schreiben wir $a \sim b$ und nennen a und b *assoziiert*.

4.1.2 Proposition: Für alle $a, b, c, a', b', x_i, b_i \in R$ gilt:

(a) $1|a$ und $a|a$ und $a|0$.

(b) Aus $a|b$ und $b|c$ folgt $a|c$.

(c) Gilt $a|b_i$ für alle i, so auch $a \mid \sum_i x_i b_i$.

(d) Es ist $a \sim b$ genau dann, wenn $a|b$ und $b|a$.

(e) $\sim$ ist eine Äquivalenzrelation.

(f) Gilt $a \sim a'$ und $b \sim b'$, so ist $a|b$ genau dann, wenn $a'|b'$.

(g) Gilt $a|b$ und $b \in R^\times$, so ist auch $a \in R^\times$.

$1 \cdot a = a \cdot 1 = a$; $a \cdot 0 = 0$

$b = ax \wedge c = by$ mit $x, y \in R \Rightarrow c = axy$ mit $xy \in R$

$\forall i\colon b_i = a y_i$ mit $y_i \in R \Rightarrow \sum_i x_i b_i = a \cdot \sum_i x_i y_i$

$a \sim b \Rightarrow ax = b \Rightarrow a|b$ und $bx^{-1} = a \Rightarrow b|a$.

Sei $a|b$ und $b|a$. Das heißt: $\exists x, y \in R\colon ax = b \wedge by = a$

$\Rightarrow b = ax = by x$ ($b \cdot 1$ bzw. $b \cdot yx$)

$b \neq 0 \Rightarrow 1 = yx \Rightarrow x \in R^\times \Rightarrow a \sim b$.

$b = 0 \Rightarrow a = 0 \Rightarrow a = b \cdot 1 \Rightarrow a \sim b$.

$ax = b$ für $x \in R \Rightarrow ax b^{-1} = bb^{-1} = 1 \Rightarrow a \in R^\times$.

$ax = a'$, $by = b'$ mit $x, y \in R^\times$; $az = b$ mit $z \in R \Rightarrow a'zy$

$a \cdot (xb^{-1})$

$a'zy = axzy = xby = xb' \Rightarrow a'zyx^{-1} = b' \Rightarrow a' \mid b'$. Umgekehrt analog.

4.1.3 Definition: Ein Element $p \in R$ mit $p \neq 0$ und $p \notin R^\times$ heisst

(a) *irreduzibel* oder *unzerlegbar*, wenn gilt

$$\forall a, b \in R: \; p = ab \longrightarrow (a \in R^\times \text{ oder } b \in R^\times).$$

(b) *prim* oder ein *Primelement*, wenn gilt

$$\forall a, b \in R: \; p \mid ab \longrightarrow (p \mid a \text{ oder } p \mid b).$$

4.1.4 Proposition: Gilt $p \sim p'$, so ist p *irreduzibel* bzw. *prim* genau dann, wenn p' es ist.

Bew.: Sei $p' = px$ mit $x \in R^\times$.

$p \neq 0 \Rightarrow R \neq 0 \Rightarrow x \neq 0 \Rightarrow p' \neq 0$.

$p \notin R^\times \wedge p \mid p'$. Wäre $p' \in R^\times$, dann wäre auch $p \in R^\times$ nach (3). $\Rightarrow p' \notin R^\times$.

p unzerlegbar $\wedge\; p' = ab \Rightarrow p = a(bx^{-1}) \Rightarrow (a \in R^\times \vee bx^{-1} \in R^\times) \Rightarrow (a \in R^\times \vee b \in R^\times)$. Also ist p' unzerlegbar.

p prim $\wedge\; p' \mid ab \Rightarrow p \mid ab \Rightarrow (p \mid a \vee p \mid b) \Rightarrow (p' \mid a \vee p' \mid b)$. Also ist p' prim. qed.

4.1.5 Proposition: Jedes Primelement ist irreduzibel.

Bew.: p prim. Sei $p = ab$.

Dann ist $p \mid ab \Rightarrow (p \mid a \vee p \mid b)$.

Ist $p \mid a$, so ist $a = px$ für ein $x \in R$.

$\Rightarrow p = ab = pxb \xrightarrow{p \neq 0} 1 = xb \Rightarrow b \in R^\times$

Analog: Ist $p \mid b$, so ist $a \in R^\times$

Also gilt $(b \in R^\times \vee a \in R^\times)$

qed.

4.1.6 Bemerkung: Eine *Primzahl* ist nach Definition eine natürliche Zahl $\geqslant 2$, welche ausser der 1 und sich selbst keine natürlichen Zahlen als Teiler hat. Nach obiger Definition bedeutet dies irreduzibel und positiv. In dem Ring $\mathbb{Z}$ ist irreduzibel aber äquivalent zu prim, und es hat sich herausgestellt, dass die Eigenschaft „prim“ die bessere Verallgemeinerung darstellt.

$\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$

$= 1 - i^2$

4.1.7 Beispiel: Im Ring $\mathbb{Z}$ ist 2 ein Primelement. In $\mathbb{Z}[i]$ gilt dagegen $2 = (1+i)(1-i)$ mit Nichteinheiten $1 \pm i$, also ist 2 nicht irreduzibel in $\mathbb{Z}[i]$. In $\mathbb{Z}[i\sqrt{5}]$ ist 2 zwar irreduzibel, aber nicht prim, denn es ist $2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$ und $2 \nmid 1 \pm i\sqrt{5}$.

$\| \quad \{a + bi\sqrt{5} \mid a, b \in \mathbb{Z}\}.$

$6 \quad = 1 - i^2 \cdot 5$

$2 \nmid 1 \pm i\sqrt{5}$

$\Rightarrow$ 2 nicht prim in $\mathbb{Z}[i\sqrt{5}]$.

4.2 Faktorielle Ringe

4.2.1 Definition: Ein Integritätsbereich, in dem jedes von 0 verschiedene Element ein Produkt von Einheiten und/oder Primelementen ist, heisst *faktoriell*.

4.2.2 Beispiel: Der Ring $\mathbb{Z}$ ist faktoriell.

4.2.3 Beispiel: Jeder Körper ist ein faktorieller Ring. (Er hat zwar keine Primelemente, aber auch nichts zu faktorisieren.)

Sei nun R beliebig faktoriell. Dann hat jedes Element von $R \smallsetminus \{0\}$ die Form

$$a \;=\; u \cdot p_1 \cdots p_m$$

für eine Einheit $u \in R^\times$, eine Zahl $m \geqslant 0$, und Primelemente $p_1, \ldots, p_m$.

Vorsicht: Die Eindeutigkeit dieser Zerlegung ist **nicht** Teil der Definition!

4.2.4 Satz: Diese *Primfaktorzerlegung* ist eindeutig bis auf Umordnung und Assoziiertheit, das heisst: Für jede weitere Zerlegung mit $v \in R^\times$ und Primelementen $q_1, \dots, q_n$

$$u \cdot p_1 \cdots p_m = a = v \cdot q_1 \cdots q_n$$

gilt $m = n$ und es existiert eine Permutation $\sigma \in S_m$ mit $\forall i\colon p_i \sim q_{\sigma i}$.

Bew.: Vertauschen $\rightsquigarrow$ OBdA $m \geq n$.

Induktion über m.

$m = 0 \Rightarrow n = 0$: klar.

Sei also $m > 0$. Dann ist $p_m \mid v q_1 \cdots q_n$

p_m prim $\Rightarrow p_m \mid v$ oder $\exists i: p_m \mid q_i$.

4.1.2(g) $\Downarrow$

$p_m \in R^\times \Rightarrow$ ↯

$p_m \cdot \kappa = q_i$ für $\kappa \in R$.

q_i prim $\Rightarrow q_i$ irred.

$\Rightarrow p_m \in R^\times$ oder $\kappa \in R^\times$.

$\Rightarrow \kappa \in R^\times$

$\Rightarrow p_m \sim q_i$

$$u p_1 \cdots p_m = v q_1 \cdots \hat{q_i} \cdots q_n \cdot q_i$$

$$p_m \cdot \kappa$$

$$\Rightarrow \underbrace{u p_1 \cdots p_{m-1}}_{R^\times} = \underbrace{(v\kappa)}_{\in R^\times} \cdot \underbrace{q_1 \cdots \hat{q_i} \cdots q_n}_{n-1}$$

$m-1$

IV $\Rightarrow m-1 = n-1$ und $p_1, \dots, p_{m-1}$

$\hat{=}$ $q_1, \dots, \hat{q_i}, \dots, q_n$ assoziiert bis auf Vertauschung.

ged.

4.2.5 Proposition: In jedem faktoriellen Ring ist irreduzibel äquivalent zu prim.

Bew.: prim $\Rightarrow$ irred.

$p \in R$ irred. Sei $p = u p_1 \cdots p_m$ mit $u \in R^\times$ und p_i prim.

$p \notin R^\times \Rightarrow m > 0$. Wäre $m > 1$, wäre $p = (u p_1) \cdot (p_2 \cdots p_m)$ eine Zerlegung mit Faktoren $\notin R^\times$.

Also ist $m = 1 \Rightarrow p = u p_1 \sim p_1 = p_i \Rightarrow p$ prim.

ged.

4.2.6 Proposition: Sei R faktoriell, und sei $\{p_i \mid i \in I\}$ ein Repräsentantensystem seiner Primelemente unter Assoziiertheit.

(a) Jedes Element von $R \setminus \{0\}$ kann man auf eindeutige Weise schreiben in der Form

$$a \;=\; u \cdot \prod_{i\in I}{}' p_i^{\mu_i}$$

für eine Einheit $u \in R^\times$ und Exponenten $\mu_i \in \mathbb{Z}^{\geqslant 0}$, fast alle gleich 0.

(b) Für $a = u \cdot \prod'_{i\in I} p_i^{\mu_i}$ und $b = v \cdot \prod'_{i\in I} p_i^{\nu_i}$ mit $u, v \in R^\times$ gilt $a|b$ genau dann, wenn für alle i gilt $\mu_i \leqslant \nu_i$.

(c) Jedes Element von $\mathrm{Quot}(R) \setminus \{0\}$ kann man auf eindeutige Weise schreiben in der Form

$$a \;=\; u \cdot \prod_{i\in I}{}' p_i^{\mu_i}$$

für eine Einheit $u \in R^\times$ und Exponenten $\mu_i \in \mathbb{Z}$, fast alle gleich 0.

Bew.: (a) $a = v \cdot q_1 \cdots q_n$, $q_j \sim p_{i_j}$, $v \in R^\times$
Jedes q_j ist zu genau einem p_i assoziiert.
$r_i := \#\{j \mid q_j \sim p_i\}$. eindeutig!

Nachtrag: $ax = b \iff v = uw \wedge \forall i: \nu_i = r_i + \lambda_i$
Also gilt $a|b \iff \exists w \in R^\times \; \exists \lambda_i \geq 0$: dies gilt
$\iff \forall i;\ \nu_i \geq r_i$.

(b) Sei $a = u \prod_i{}' p_i^{r_i}$
$x = w \cdot \prod_i{}' p_i^{\lambda_i} \in R \setminus \{0\}$
$w \in R^\times$
$\Rightarrow ax = (uw) \cdot \prod_i{}' p_i^{r_i+\lambda_i}$

(c) a, b wie in (b)
$\Rightarrow \frac{a}{b} = \underbrace{\frac{u}{v}}_{\in R^\times} \cdot \prod_i{}' p_i^{r_i - \nu_i}$
$\in \mathbb{Z}$
$f_3 + \mathbb{Z} = 0$

4.3 Grösster gemeinsamer Teiler

Sei R faktoriell.

4.3.1 Proposition-Definition: Betrachte Elemente $a_1, \ldots, a_n \in R$.

(a) Ein Element $b \in R$ mit $\forall i\colon b|a_i$ heisst ein *gemeinsamer Teiler von* $a_1, \ldots, a_n$.

(b) Es existiert ein gemeinsamer Teiler b von $a_1, \ldots, a_n$, so dass für jeden gemeinsamen Teiler b' von $a_1, \ldots, a_n$ gilt $b'|b$.

(c) Dieser *grösste gemeinsame Teiler von* $a_1, \ldots, a_n$ ist eindeutig bis auf Assoziiertheit. Wir bezeichnen jeden solchen mit $\mathrm{ggT}(a_1, \ldots, a_n)$.

Da der ggT nur eindeutig bis auf Assoziiertheit ist, sollte man ihn immer nur auf Assoziiertheit testen und nicht auf Gleichheit.