

## 2 Ringe

### 2.1 Grundlegende Definitionen und Eigenschaften

**Definition + Bemerkung 2.1.1** (a) Ein **Ring** ist eine Menge  $R$  mit Verknüpfungen  $+$  und  $\cdot$ , so dass gilt:

- (i)  $(R, +)$  ist abelsche Gruppe
- (ii)  $(R, \cdot)$  ist Halbgruppe
- (iii) Die Distributivgesetze gelten:

$$\left. \begin{aligned} x \cdot (y + z) &= xy + xz \\ (x + y) \cdot z &= xz + yz \end{aligned} \right\} \text{ für alle } x, y, z \in R$$

- (b)  $R$  heißt **Ring mit Eins**, wenn  $(R, \cdot)$  Monoid ist.
- (c)  $R$  heißt **kommutativer Ring**, wenn  $(R, \cdot)$  kommutativ ist.
- (d) Ein Ring  $R$  mit Eins heißt **Schiefkörper**, wenn  $R^\times = (R, \cdot)^\times = R \setminus \{0\}$ , dh. wenn jedes  $x \in R \setminus \{0\}$  invertierbar bzgl.  $\cdot$  ist.

**Beispiel:**

$$\mathbb{H} := \left\{ \begin{pmatrix} w & z \\ -\bar{z} & \bar{w} \end{pmatrix}, w, z \in \mathbb{C} \right\}$$

ist ein Schiefkörper, genannt die **Hamilton-Quaternionen**.

- (e) Ein kommutativer Schiefkörper heißt **Körper**.
- (f) In jedem Ring gilt:

$$\left. \begin{aligned} x \cdot 0 &= 0 = 0 \cdot x \\ x(-y) &= -(xy) = (-x)y \\ (-x)(-y) &= xy \end{aligned} \right\} \text{ für alle } x, y \in R$$

**Beweis:**  $x \cdot 0 = x \cdot (0 + 0) = x \cdot 0 + x \cdot 0$  (genauso für  $0 \cdot x$ )

$$x(-y) + xy = x(-y + y) = x \cdot 0 = 0$$

$$(-x)(-y) = -((-x)y) = -(-(xy)) = xy \quad \blacksquare$$

- (g) Ist  $R$  ein Ring mit Eins und  $R \neq \{0\}$ , so ist  $0 \neq 1$  in  $R$

**Beweis:** Wäre  $0 = 1$ , so gälte für jedes  $x \in R : x = x \cdot 1 = x \cdot 0 = 0$ , also doch  $R = \{0\}$  ■

### Definition 2.1.2

Sei  $(R, +, \cdot)$  ein Ring.

- (a)  $R' \subseteq R$  heißt **Unterring**, wenn  $(R', +, \cdot)$  Ring ist. Umgekehrt heißt  $R$  dann **Ring-erweiterung** von  $R'$ .
- (b)  $I \subseteq R$  heißt (zweiseitiges) **Ideal**, wenn  $(I, +)$  Untergruppe von  $(R, +)$  ist und  $rx \in I, xr \in I$  für alle  $x \in I, r \in R$ .

**Beispiel:** In  $R = \mathbb{Z}$  sind  $n\mathbb{Z}$  für jedes  $n \in \mathbb{Z}$  Ideale. In  $R = \mathbb{Q}$  dagegen sind diese für  $n \neq 0$  keine Ideale.

### Definition + Bemerkung 2.1.3

Sei  $R$  ein kommutativer Ring.

- (a) Für  $a$  ist  $(a) := a \cdot R = \{a \cdot r, r \in R\}$  ein Ideal in  $R$ .
- (b) Ein Ideal  $I$  in  $R$  heißt **Hauptideal**, wenn es ein  $a \in R$  gibt mit  $I = (a)$ .
- (c)  $R$  heißt **Hauptidealring**, wenn jedes Ideal in  $R$  ein Hauptideal ist.
- (d)  $\mathbb{Z}$  ist ein Hauptidealring.
- (e) Sei  $R$  ein kommutativer Ring mit Eins,  $R \neq \{0\}$ . Dann ist  $R$  ein Körper genau dann, wenn  $(0)$  und  $R$  die einzigen Ideale in  $R$  sind.

**Beweis:** " $\Rightarrow$ " Sei  $I \subset R$  Ideal,  $a \in I \setminus \{0\} \Rightarrow$  es gibt  $a^{-1} \in R \Rightarrow 1 = aa^{-1} \in I \Rightarrow I = R$  ( $x \in R \Rightarrow x = 1x$ )  
 " $\Leftarrow$ " Sei  $a \in R \setminus \{0\} \Rightarrow (a) = R \Rightarrow \exists b \in R : ab = 1$  ■

**Beispiel:**  $\mathbb{Z}/n\mathbb{Z}$  ist ein kommutativer Ring mit Eins für jedes  $n \in \mathbb{N}$ . Ist  $n = p$  für eine Primzahl  $p$ , so ist  $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$  ein Körper, und  $(\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z})^\times = \{\bar{a}, a \in \mathbb{Z}, \text{ggT}(a, p) = 1\}$ . In  $\mathbb{Z}/6\mathbb{Z}$  dagegen gilt  $\bar{2} \cdot \bar{3} = \bar{0}$ .

### Definition 2.1.4

Sei  $R$  ein kommutativer Ring.

- (a)  $x \in R$  heißt **Nullteiler**, wenn es ein  $y \in R \setminus \{0\}$  gibt mit  $xy = 0$ .
- (b)  $R \neq \{0\}$  heißt **nullteilerfrei**, wenn 0 der einzige Nullteiler in  $R$  ist. (Das heißt: Aus  $xy = 0$  folgt, dass  $x = 0$  oder  $y = 0$ .)

- (c)  $R$  heißt **Integritätsbereich** (engl. **integral domain**), wenn er nullteilerfrei und kommutativ ist sowie eine Eins besitzt.

**Definition + Bemerkung 2.1.5** (a) Eine Abbildung  $\varphi : R \rightarrow R'$  ( $R, R'$  Ringe) heißt **Homomorphismus von Ringen**, wenn  $\varphi : (R, +) \rightarrow (R', +)$  ein Homomorphismus von Gruppen und  $\varphi : (R, \cdot) \rightarrow (R', \cdot)$  ein Homomorphismus von Halbgruppen ist.

- (b) Sind  $R, R'$  Ringe mit Eins, so heißt ein Homomorphismus von Ringen  $\varphi : R \rightarrow R'$  ein **Homomorphismus von Ringen mit Eins**, wenn  $\varphi(1_R) = 1_{R'}$ .

- (c) Die Ringe bilden mit Ringhomomorphismus eine Kategorie

- (d) Die Ringe mit Eins bilden mit Homomorphismen von Ringen mit Eins eine Kategorie (echte Unterkategorie der Ringe)

- (e)  $(R, +, \cdot) \hookrightarrow (R, +)$  ist kovarianter Funktor: Ringe  $\rightarrow$  abelsche Gruppen.

- $(R, +, \cdot) \mapsto (R^\times, \cdot)$  ist kovarianter Funktor: Ringe mit Eins  $\rightarrow$  Gruppen.

**Beispiel:** Sei  $R$  ein kommutativer Ring mit Eins und  $R^{n \times n}$  der Ring der  $n \times n$ -Matrizen mit Einträgen in  $R$ . Für  $n \geq 2$  ist  $R^{n \times n}$  nicht kommutativ und nicht nullteilerfrei.

Die Eins in  $R^{n \times n}$  ist die Einheitsmatrix:

$$E_n := \begin{pmatrix} 1_R & & 0 \\ & \ddots & \\ 0 & & 1_R \end{pmatrix}$$

Die Einheiten in  $R^{n \times n}$  sind die invertierbaren Matrizen:  $(R^{n \times n})^\times = GL_n(R) = \{A \in R^{n \times n} : \exists B \in R^{n \times n} : A \cdot B = B \cdot A = E_n\} = \{A \in R^{n \times n} : \det A \in R^\times\}$ , denn für die Adjungierte  $A^\#$  von  $A$  gilt:  $A \cdot A^\# = \det(A) \cdot E_n$ .

( $A^\# = (b_{ij})$  mit  $b_{ij} = (-1)^{i+j} \det A_{ji}$ , wobei  $A_{ji}$  die Matrix  $A$  ohne die  $j$ -te Zeile und  $i$ -te Spalte ist.)

### Bemerkung 2.1.6

Sei  $\varphi : R \rightarrow R'$  Ringhomomorphismus. Dann gilt:

- (a)  $\text{Bild}(\varphi)$  ist Unterring von  $R'$

- (b)  $\text{Kern}(\varphi) := \varphi^{-1}(0)$  ist Ideal in  $R$

**Beweis:** Sei  $x \in \text{Kern}(\varphi)$ ,  $r \in R \Rightarrow \varphi(rx) = \varphi(r)\varphi(x) = \varphi(r)0 = 0 \Rightarrow rx \in \text{Kern}(\varphi)$  ■

## 2 Ringe

- (c) Ist  $R$  Schiefkörper,  $R'$  Ring mit Eins,  $\varphi$  Homomorphismus von Ringen mit Eins, so ist  $\varphi$  injektiv oder die Nullabbildung.

**Beweis:** Sei  $x \in R \setminus \{0\} \Rightarrow \varphi(x)\varphi(x^{-1}) = \varphi(1) \neq 0$ , sofern  $\varphi$  nicht die Nullabbildung  $\Rightarrow \varphi(x) \neq 0 \Rightarrow \text{Kern}(\varphi) = \{0\} \Rightarrow \varphi$  injektiv. ■

### Definition + Bemerkung 2.1.7

Sei  $R$  Ring mit Eins.

(a)

$$\varphi_R : \mathbb{Z} \rightarrow R, n \mapsto \begin{cases} n \cdot 1_R = \underbrace{1_R + \dots + 1_R}_n & n \geq 0 \\ -((-n) \cdot 1_R) & n \leq 0 \end{cases}$$

ist Homomorphismus von Ringen mit Eins.

- (b) Ist  $\text{Kern}(\varphi_R) = n\mathbb{Z}$  ( $n \geq 0$ ), so heißt  $n$  die **Charakteristik** von  $R$ :  $n = \text{char}(R)$
- (c) Ist  $R$  nullteilerfrei, so ist  $\text{char}(R) = 0$ , oder  $\text{char}(R) = p$  für eine Primzahl  $p$ .
- (d)  $\text{Bild}(\varphi_R) \cong \mathbb{Z}/n\mathbb{Z}$ ,  $n = \text{char}(R)$
- (e) Ist  $K$  (Schief-)Körper der Charakteristik  $p > 0$ , so ist  $\text{Bild}(\varphi_K) \cong \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$  der kleinste Teilkörper von  $K$ . Er heißt **Primkörper**. Ist  $\text{char}(K) = 0$ , so lässt sich  $\varphi_K$  eindeutig fortsetzen zu einem injektiven Homomorphismus  $\tilde{\varphi}_K : \mathbb{Q} \rightarrow K$  mit  $\tilde{\varphi}_K(\frac{n}{m}) = \varphi_K(n) \cdot \varphi_K(m)^{-1}$ .

### Definition + Bemerkung 2.1.8

Sei  $R$  Ring. Dann gilt:

- (a) Ist  $J$  eine Indexmenge und sind  $I_j, j \in J$  Ideale in  $R$ , so ist  $\bigcap_{j \in J} I_j$  ein Ideal in  $R$ .
- (b) Sind  $I_1, I_2$  Ideale in  $R$ , dann ist  $I_1 + I_2 = \{a + b : a \in I_1, b \in I_2\}$  ein Ideal.
- (c) Sind  $I_1, I_2$  Ideale in  $R$ , dann ist  $I_1 \cdot I_2 = \{\sum_{i=1}^{<\infty} a_i b_i : a_i \in I_1, b_i \in I_2\}$  ein Ideal.
- (d) Sind  $I_1, I_2$  Ideale in  $R$ , dann ist  $I_1 \cdot I_2 \subseteq I_1 \cap I_2$  (aber im allgemeinen  $\neq$ !)
- (e) Sei  $R$  kommutativ mit Eins,  $X \subseteq R$ . Die Menge

$$(X) = \bigcap_{\substack{I \subseteq R \text{ Ideal} \\ X \subseteq I}} I = \left\{ \sum_{\text{endl.}} r_i x_i : r_i \in R, x_i \in X \right\}$$

heißt das von  $X$  erzeugte Ideal.

- (f) Sind  $I_1, I_2$  Ideale in einem kommutativen Ring  $R$  mit Eins, so ist  $I_1 + I_2 = (I_1 \cup I_2)$  und  $I_1 \cdot I_2 = (\{ab : a \in I_1, b \in I_2\})$ .

## 2.2 Polynomringe

### Definition + Bemerkung 2.2.1

Sei  $R$  ein kommutativer Ring mit Eins,  $R \neq \{0\}$ .

- (a) Ein **Polynom** über  $R$  ist eine Folge  $f = (a_i)_{i \in \mathbb{N}}$  mit einem  $n_0 \in \mathbb{N}$  so, dass  $\forall i > n_0 : a_i = 0$ .

Symbolische Schreibweise:  $f = \sum_{i=0}^n a_i X^i$

- (b) Die Menge  $R[X]$  der Polynome über  $R$  ist kommutativer Ring mit Eins mit den Verknüpfungen

$$\begin{aligned} (a_i)_{i \in \mathbb{N}} + (b_i)_{i \in \mathbb{N}} &= (a_i + b_i)_{i \in \mathbb{N}} \\ (a_i)_{i \in \mathbb{N}} \cdot (b_i)_{i \in \mathbb{N}} &= (c_i)_{i \in \mathbb{N}} \text{ mit } c_i = \sum_{k=0}^i a_k b_{i-k} \end{aligned}$$

- (c)  $R \rightarrow R[X]$ ,  $a \mapsto (a, 0, \dots)$  ist injektiver Ringhomomorphismus
- (d) Für  $f = \sum a_i X^i \in R[X]$ ,  $f \neq 0$ , heißt  $\text{Grad}(f) := \max\{i \in \mathbb{N}, a_i \neq 0\}$  der Grad von  $f$ .
- (e) Für  $f, g$  ist  $\text{Grad}(f + g) \leq \max(\text{Grad}(f), \text{Grad}(g))$ , falls  $f, g, f + g \neq 0$
- (f) Für  $f, g$  ist  $\text{Grad}(f \cdot g) \leq \text{Grad}(f) + \text{Grad}(g)$  für  $f, g, f \cdot g \neq 0$ .  
 $=$ , falls  $R$  nullteilerfrei

### Folgerung 2.2.2

Ist  $R$  Integritätsbereich, so ist  $R[X]$  ebenfalls Integritätsbereich und  $R[X]^\times = R^\times$

### Proposition 2.2.3

Sei  $R$  kommutativer Ring mit Eins.

- (a) Zu jedem  $x \in R$  gibt es genau einen Ringhomomorphismus  $\varphi_x : R[X] \rightarrow R$  mit  $\varphi_x|_R = \text{id}_R$  und  $\varphi_x(X) = x$ . Es ist  $\varphi_x(a_0, a_1, \dots) = \sum_{i \geq 0} a_i x^i$
- (b) Zu jedem Homomorphismus  $\alpha : R \rightarrow R'$  von Ringen mit Eins und jedem  $y \in R'$  gibt es genau einen Ringhomomorphismus  $\varphi_y : R[X] \rightarrow R'$ ,  $\varphi_y|_R = \alpha$  und  $\varphi_y(X) = y$ .  
 Explizit:  $\varphi_y(\sum a_i X^i) = \sum \alpha(a_i) y^i$ .

#### Beweis:

- (a) ist (b) für  $R' = R$  und  $\alpha = \text{id}_R$
- (b) Die angegebene Formel ist die einzig mögliche Definition dieses Ringhomomorphismus, weil  $\varphi_y(a_0, a_1, \dots) = \varphi_y(\sum_{i=0}^n a_i X^i) = \sum_{i=0}^n \varphi_y(a_i) \varphi_y(X)^i$  sein muß. ■

**Bemerkung 2.2.4**

Die vorangehende Folgerung bleibt richtig, wenn  $R'$  nicht kommutativ ist, solange  $\alpha(R) \subseteq Z(R)$  ist, also  $\alpha(a) \cdot b = b \cdot \alpha(a)$  für alle  $a \in R, b \in R'$  gilt.

**Bemerkung 2.2.5**

Die Zuordnung  $R \mapsto R[X]$  ist ein kovarianter Funktor: Ringe mit Eins  $\rightarrow$  Ringe mit Eins.

**Beweis:** Ist  $\alpha : R \rightarrow R'$  Ringhomomorphismus, so sei  $\Psi : R[X] \rightarrow R'[X]$  der Homomorphismus, der durch  $\alpha : R \rightarrow R' \xrightarrow[2.8(c)]{} R'[X]$  und  $X \mapsto X$  bestimmt ist. ■

**Definition + Bemerkung 2.2.6** (a)  $R[[X]] = \{(a_i)_{i \in \mathbb{N}} : a_i \in R\}$  ist mit  $+$  und  $\cdot$  wie im Polynomring ein kommutativer Ring mit Eins.  $R[[X]]$  heißt **Ring der (formalen) Potenzreihen** über  $R$ .  
Schreibweise (auch):

$$f = \sum_{i=0}^{\infty} a_i X^i$$

für  $f = (a_i)_{i \in \mathbb{N}}$

(b)  $R[X]$  ist Unterring von  $R[[X]]$ .

(c) Sei  $0 \neq f = \sum_{i=0}^{\infty} a_i X^i \in R[[X]]$ . Dann heißt  $o(f) := \min\{i \in \mathbb{N}, a_i \neq 0\}$  der **Untergrad** von  $f$ . Es gilt für alle  $f, g \in R[[X]] \setminus \{0\}$ :

$$o(f + g) \geq \min\{o(f), o(g)\} \text{ und } o(f \cdot g) \geq o(f) + o(g)$$

wobei in der Ungleichung für die Multiplikation Gleichheit gilt, wenn  $R$  nullteilerfrei ist.

**Proposition 2.2.7** (a) Ist  $R$  Integritätsbereich, so ist  $o(f \cdot g) = o(f) + o(g) \forall f, g \in R[[X]] \setminus \{0\}$  und es gilt:  $R[[X]]^\times = \{f = \sum_{i=0}^{\infty} a_i X^i \in R[[X]] : a_0 \in R^\times\}$

(b) Ist  $R = K$  Körper, so ist  $m := K[[X]] \setminus K[[X]]^\times = \{\sum a_i X^i : a_0 = 0\}$  Ideal in  $K[[X]]$ , und das einzige maximale.

**Beweis:** (a), (b), (d) ✓

(c) " $\subseteq$ ": Sei  $f = \sum a_i X^i \in R[[X]]^\times$ . Dann gibt es  $g = \sum b_i X^i \in R[[X]]$  mit  $1 = fg = a_0 b_0 + (a_1 b_0 + a_0 b_1)X + \dots \Rightarrow a_0 \in R^\times$

" $\supseteq$ ": Definiere  $g = \sum b_i X^i$  rekursiv durch  $b_0 = a_0^{-1}, b_i := a_0^{-1} \cdot \sum_{k=1}^i (-1)^k a_k b_{i-k}, i \geq 1$ . Dann ist  $fg = 1$  ■

**Beispiel:**  $i = 1 : b_i = a_0^{-1}(a_1 b_0)$

## 2.3 Faktorringe

Sei  $R$  ein kommutativer Ring mit Eins.

**Definition + Bemerkung 2.3.1** (a) Sei  $I$  Ideal in  $R$ . Durch die Verknüpfung  $\bar{x} \cdot \bar{y} := \overline{xy}$  wird die Faktorgruppe  $(R, +)/(I, +)$  ein kommutativer Ring mit Eins. Dieser Ring  $R/I$  heißt **Faktoring** oder **Quotientenring** von  $R$  und  $I$ . (Man verwechsle diesen Begriff des Quotientenrings nicht mit dem Quotientenkörper eines Integritätsbereiches, siehe weiter unten!)

- (b) Die Restklassenabbildung  $\pi : R \rightarrow R/I, x \mapsto \bar{x}$  ist surjektiver Ringhomomorphismus mit  $\text{Kern}(\pi) = I$ .
- (c) (UAE des Faktorrings:) Sei  $\varphi : R \rightarrow R'$  ein Ringhomomorphismus. Dann gibt es zu jedem Ideal  $I \subseteq R$  mit  $I \subseteq \text{Kern}(\varphi)$  einen eindeutig bestimmten Ringhomomorphismus  $\bar{\varphi} : R/I \rightarrow R'$  mit  $\varphi = \bar{\varphi} \circ \pi$
- (d) (Homomorphiesatz für Ringe:) Ist  $\varphi : R \rightarrow R'$  surjektiver Ringhomomorphismus, dann ist  $R' \cong R/\text{Kern}(\varphi)$ .

### Beweis:

- (a) **Wohldef. des Produkts:** Seien  $x', y' \in R$  mit  $\bar{x'} = \bar{x}, \bar{y'} = \bar{y}$ . Dann gibt es  $a, b \in I$  mit  $x' = x + a, y' = y + b$ .  $\Rightarrow x'y' = (x + a)(y + b) = xy + \underbrace{ay + bx + ab}_{\in I} \Rightarrow \bar{x'}\bar{y'} = \bar{xy}$ .  
Die restlichen Eigenschaften vererben sich dann von  $R$ .
- (b)  $\pi$  ist surjektiver Gruppenhomomorphismus mit  $\text{Kern}(\pi) = I$  nach Satz 1(a).  
 $\pi(xy) = \pi(x) \cdot \pi(y)$  nach Definition der Verknüpfung.
- (c) Nach Satz 1(d) gibt es einen eindeutig bestimmten Gruppenhomomorphismus  $\bar{\varphi} : R/I \rightarrow R'$  mit  $\varphi = \bar{\varphi} \circ \pi$ .  
Zeige also:  $\bar{\varphi}$  ist Ringhomomorphismus: Für  $x, y \in R$  ist  $\bar{\varphi}(\bar{xy}) = \varphi(xy) = \varphi(x)\varphi(y) = \bar{\varphi}(\bar{x})\bar{\varphi}(\bar{y})$
- (d) Folgt aus (c) und Satz 1(a) ■

**Definition 2.3.2** (a) Ein Ideal  $I \subsetneq R$  heißt **maximal**, wenn es kein Ideal  $I'$  in  $R$  gibt mit  $I \subsetneq I' \subsetneq R$ .

**Beispiel:** In  $R = K[X]$ ,  $K$  Körper, ist  $(X) = \{f = \sum_{i=0}^n a_i X^i, a_0 = 0\}$  maximal.

- (b) Ein Ideal  $I \subsetneq R$  heißt **Primideal**, wenn für  $x, y \in R$  mit  $xy \in I$  gilt:  $x \in I$  oder  $y \in I$ .

## 2 Ringe

### Beispiel:

- (1) Für  $p \in \mathbb{Z}$ ,  $p > 0$  gilt:  $p$  prim  $\Leftrightarrow p\mathbb{Z}$  ist Primideal in  $\mathbb{Z}$  (sogar maximal)
- (2)  $(X)$  ist Primideal in  $R[[X]] \Leftrightarrow R$  ist Körper.

(3)  $\{0\}$  ist Primideal in  $\mathbb{Z}$ .

**Bemerkung 2.3.3** (a)  $R$  ist nullteilerfrei  $\Leftrightarrow (0)$  ist Primideal.

(b)  $I \subsetneq R$  ist Primideal genau dann, wenn  $R/I$  nullteilerfrei ist.

### Beweis:

- (a)  $R$  ist nicht nullteilerfrei  $\Leftrightarrow \exists a, b \in R \setminus \{0\}: ab = 0 \Leftrightarrow (0)$  kein Primideal.
- (b) Seien  $x, y \in R$  mit  $x \cdot y \in I$ , also  $\bar{x} \cdot \bar{y} = 0$  in  $R/I$ .  $I$  Primideal  $\Leftrightarrow x \in I$  oder  $y \in I \Leftrightarrow \bar{x} = 0$  oder  $\bar{y} = 0 \Leftrightarrow R/I$  ist nullteilerfrei. ■

### Bemerkung 2.3.4

Sei  $I \subset R$  ein Ideal. Dann gilt:

- (a) Jedes maximale Ideal ist Primideal.
- (b)  $I$  ist maximales Ideal  $\Leftrightarrow R/I$  ist Körper.

### Beweis:

- (a) folgt aus (b) und Bemerkung 2.3.5.
- (b) Nach 2.1.3 (e) ist  $R/I$  genau dann Körper, wenn  $(0)$  und  $R/I$  die einzigen Ideale in  $R/I$  sind. Die Behauptung folgt dann aus:  $I \subsetneq J \subsetneq R$  in  $R \Leftrightarrow 0 \neq \bar{J} \neq R/I$  in  $R/I$  wobei  $\bar{J}$  das Bild von  $J$  in  $R/I$  ist. ■

### Bemerkung 2.3.5

Sei  $I$  ein Ideal in  $R$ . Dann entsprechen die Ideale in  $R/I$  bijektiv den Idealen in  $R$ , die  $I$  enthalten.

**Beweis:** Sei  $\pi : R \rightarrow R/I$  die Restklassenabbildung. Für jedes Ideal  $\bar{J}$  in  $R/I$  ist  $\pi^{-1}(\bar{J})$  ein Ideal in  $R$ . Es gilt  $\pi^{-1}(\bar{J}) \supseteq \pi^{-1}(0) = \text{Kern } \pi = I$ .

Sei umgekehrt  $J \subsetneq R$  ein Ideal mit  $I \subseteq J$ . Dann ist  $\bar{J} := \pi(J)$  ein Ideal in  $R/I$ , da  $\pi$  surjektiv ist.



Weiter ist  $\pi^{-1}(\pi(J)) = J$ , da  $\text{Kern } \pi \subseteq J$ , und  $\pi(\pi^{-1}(\bar{J})) = \bar{J}$ , da  $\pi$  surjektiv ist. ■

### Beispiel 2.3.6 (Algebraische Konstruktion der reellen Zahlen)

Sei  $C = \{(a_n)_{n \in \mathbb{N}} : (a_n) \text{ Cauchy-Folge, } a_n \in \mathbb{Q}\}$  (dh. für  $k \in \mathbb{N} \exists n \in \mathbb{N} : |a_i - a_j| < \frac{1}{k}$  für  $i, j \geq n$ )

$C$  ist Ring mit komponentenweiser  $+$  und  $\cdot$  (vornehm:  $C \subset \prod_{n \in \mathbb{N}} \mathbb{Q}$ ).

$N = \{(a_n) \in C : (a_n) \text{ Nullfolge}\}$  (dh. für  $k \in \mathbb{N} \exists n \in \mathbb{N} : |a_i| < \frac{1}{k} \forall i > n$ )

$N$  ist Ideal in  $C$ : ✓

**Beh.:**  $C/N$  ist Körper (bzw.  $N$  ist maximal)

**Beweis:** Sei  $a = (a_n)_{n \in \mathbb{N}} \in C \setminus N$ . zu zeigen:  $1 \in (N + (a))$ .

$(a_n) \notin N \Rightarrow a_n = 0$  nur für endlich viele  $n$ , dh.  $a_i \neq 0$  für  $i > n_0$ .

$$b_n := \begin{cases} 0 & , \quad a_i = 0 | i \leq n_0 \\ \frac{1}{a_i} & , \quad a_i \neq 0 | i > n_0 \end{cases}$$

$b = (b_n) \in C$ .

$$ab = (c_n), \quad c_n = \begin{cases} 0 & : \quad n < n_0 \\ 1 & : \quad n \geq n_0 \end{cases}$$

$$\Rightarrow 1 - ab = (d_n), \quad d_n = \begin{cases} 1 & : \quad n < n_0 \\ 0 & : \quad n \geq n_0 \end{cases}$$

$\Rightarrow (d_n) \in N \Rightarrow 1 = (d_n) + ba \in N + (a) \Rightarrow N$  maximal.

$\Rightarrow C/N = \mathbb{R}$ ! ■

### Satz 7 (Chinesischer Restsatz)

Sei  $R$  kommutativer Ring mit Eins,  $I_1, \dots, I_n$  Ideale in  $R$  mit  $I_\nu + I_\mu = R$  für alle  $\nu \neq \mu$  (dann heißen  $I_\nu, I_\mu$  **relativ prim** oder **koprim**) Für  $\nu = 1, \dots, n$  sei  $\pi_\nu : R \rightarrow R/I_\nu$  die Restklassenabbildung. Dann gilt:

(a)  $\varphi : R \rightarrow R/I_1 \times \dots \times R/I_n$  ist surjektiv.  
 $x \mapsto (\pi_1(x), \dots, \pi_n(x))$

(b) Wegen dem Homomorphiesatz und  $\text{Kern}(\varphi) = \bigcap_{\nu=1}^n I_\nu$  gilt:

$$R/I_1 \times \dots \times R/I_n \cong R / \bigcap_{\nu=1}^n I_\nu$$

(c) (Simultane Kongruenzen:)

Für paarweise teilerfremde ganze Zahlen  $m_1, \dots, m_n$  und beliebige  $r_1, \dots, r_n \in \mathbb{Z}$  gibt es  $x \in \mathbb{Z}$  mit  $x \equiv r_\nu \pmod{m_\nu}$  für  $\nu = 1, \dots, n$  (Spezialfall von (a) für  $R = \mathbb{Z}$ )

**Beweis:** Es genügt z.z.:  $\bar{e}_\nu = (0, \dots, 0, \underbrace{1}_{\nu\text{-te Stelle}}, 0, \dots, 0) \in \text{Bild}(\varphi)$  für jedes  $\nu$ ,  
 dh. es gibt  $e_\nu \in R$  ( $\nu = 1, \dots, n$ ) mit  $e_\nu \in I_\mu$  für  $\nu \neq \mu$  und  $1 - e_\nu =: a_\nu \in I_\nu$  (Denn  
 für  $x = (\bar{x}_1, \dots, \bar{x}_n) \in R/I_1 \times \dots \times R/I_n$  sei  $e := \sum_{\nu=1}^n r_\nu e_\nu$  mit  $r_\nu \in p_\nu^{-1}(\bar{x}_\nu) \Rightarrow \varphi(e) = \sum p_\nu(r_\nu e_\nu) = x$ .)  
 Nach Voraussetzung gibt es für jedes  $\mu \neq \nu$   $a_\mu \in I_\nu, b_\mu \in I_\mu$  mit

$$\begin{aligned} a_\mu + b_\mu = 1 \Rightarrow 1 &= \prod_{\substack{\mu=1 \\ \mu \neq \nu}}^n (a_\mu + b_\mu) = \prod_{\substack{\mu=1 \\ \mu \neq \nu}}^n b_\mu + \underbrace{a_\nu}_{\in I_\nu} \\ &=: e_\nu \in \bigcap_{\substack{\mu=1 \\ \mu \neq \nu}}^n I_\mu \end{aligned}$$

$\Rightarrow 1 - e_\nu = a_\nu$  wie gewünscht. ■

## 2.4 Teilbarkeit

Sei  $R$  ein Integritätsbereich.

### Definition + Bemerkung 2.4.1

Seien  $a, b \in R \setminus \{0\}$ .

- (a)  $a$  **teilt**  $b$  (Schreibweise  $a \mid b$ )  $:\Leftrightarrow b \in (a)$  ( $\Leftrightarrow \exists x \in R : b = ax$ )
- (b)  $d \in R$  heißt **größter gemeinsamer Teiler** von  $a$  und  $b$ , (Schreibweise  $\text{ggT}(a, b)$ )  
 wenn gilt:
  - (i)  $d \mid a$  und  $d \mid b$  bzw.  $a \in (d), b \in (d)$
  - (ii) ist  $d' \in R$  auch Teiler von  $a$  und  $b$ , so gilt  $d' \mid d$  bzw.  $d \in (d')$
- (c) Ist  $d \in R$  ein ggT von  $a$  und  $b$  und  $e \in R^\times$ , so ist auch  $e \cdot d$  ein ggT. Sind  $d, d'$  beide ggT von  $a$  und  $b$ , so gibt es  $e \in R^\times$  mit  $d' = ed$ .

**Beweis:** Nach Definition gibt es  $x, y \in R$  mit  $d' = xd$  und  $d = yd' \Rightarrow d' = xyd' \Rightarrow d'(1 - xy) = 0 \xRightarrow{d' \neq 0} 1 = xy \Leftrightarrow x, y \in R^\times$  ■  
 $R$  nullteilerfrei

- (d) In analoger Weise wird das kleinste gemeinsame Vielfache definiert.

### Beispiel:

- (a) In  $\mathbb{Z}$  gibt es einen größten gemeinsamen Teiler.

- (b) In jedem nullteilerfreiem Hauptidealring  $R$  gibt es zu je zwei Elementen  $a, b$  einen größten gemeinsamen Teiler: Denn  $(a, b) = (a) + (b)$  ist ein Hauptideal, das heißt, es gibt ein  $d \in R$  mit  $(a, b) = (d)$ . Also gilt  $d \mid a$  und  $d \mid b$  und für jedes  $d' \in R$ , für das  $d' \mid a$  und  $d' \mid b$  gilt, gilt auch:  $(a) \subseteq (d')$ ,  $(b) \subseteq (d')$ , also  $(a, b) \subseteq (d')$  und somit  $(d) \subseteq (d')$ , also  $d' \mid d$ .

- (c) In  $\mathbb{Z}[\sqrt{-5}]$  gibt es zu 6 und  $4 + 2\sqrt{-5}$  keinen größten gemeinsamen Teiler.

### Definition 2.4.2

Ein Integritätsbereich  $R$  heißt **euklidisch**, wenn es eine Abbildung:  $\delta : R \setminus \{0\} \rightarrow \mathbb{N}$  mit folgender Eigenschaft gibt: zu  $f, g \in R, g \neq 0$  gibt es  $q, r \in R$  mit  $f = qg + r$  mit  $r = 0$  oder  $\delta(r) < \delta(g)$ .

**Beispiel:**  $\mathbb{Z}$  mit  $\delta(a) = |a|$ ,  $K[X]$  mit  $\delta(f) = \text{Grad}(f)$

### Bemerkung 2.4.3

Sei  $R$  euklidisch.

- (a) Für  $a, b \in R \setminus \{0\}$  gilt:
- (i) in  $R$  gibt es einen ggT von  $a$  und  $b$ , er heiße  $d$ .
  - (ii)  $(d) = (a, b) = (a) + (b)$
- (b) Jeder euklidische Ring ist ein Hauptidealring.

### Beweis:

- (a)  $\nexists$  sei  $\delta(a) \geq \delta(b)$ . Nach Voraussetzung gibt es  $q_1, r_1 \in R$  mit  $a = q_1 b + r_1$ ,  $\delta(r_1) < \delta(b)$  oder  $r_1 = 0$ .  
Ist  $r_1 = 0$ , so ist  $a \in (b) = (a, b)$  und  $\text{ggT}(a, b) = b$ . Sonst gibt es  $q_2, r_2 \in R$  mit  $b = q_2 r_1 + r_2$  und  $r_2 = 0$  oder  $\delta(r_2) < \delta(r_1)$ . usw...

$$\begin{array}{rcl} r_i & = & q_{i+2} r_{i+1} + r_{i+2} \\ \Rightarrow \quad \vdots & & \vdots \\ r_{n-2} & = & q_n r_{n-1} \end{array}$$

(da  $\delta(r_{i+2}) < \delta(r_{i+1})$ )

**Beh.:**  $d := r_{n-1}$  ist ggT von  $a$  und  $b$ .

**denn:**  $d \mid r_{n-2}$  (vorletzte Zeile:  $r_{n-3} = q_{n-1} r_{n-2} + r_{n-1} \Rightarrow d \mid r_{n-3}$ )

Induktion:  $d \mid r_i$  für alle  $i \Rightarrow d \mid b \Rightarrow d \mid a$

**umgekehrt:** Sei  $d'$  Teiler von  $a$  und  $b \Rightarrow d' \mid r_1 \xrightarrow{\text{Induktion}} d' \mid r_i \forall i \Rightarrow d' \mid d$ .

noch zu zeigen ist  $(d) = (a, b)$ :

" $\subseteq$ ":  $d \in (a, b)$  Nach Konstruktion ist  $r_{i+2} \in (r_i, r_{i+1}) \subset \dots \subset (a, b) \forall i$

" $\supseteq$ ":  $a \in (d), b \in (d)$  nach Definition.

- (b) Sei  $I \subseteq R$  Ideal,  $I \neq \{0\}$ . Wähle  $a \in I$  mit  $\delta(a)$  minimal. Dann gilt für jedes  $b \in I$ :  $b = qa + r$  mit  $r \in I$  und  $\delta(r) < \delta(a)$   $\nmid$  also  $r = 0 \Rightarrow I = (a)$  ■

### Definition + Bemerkung 2.4.4

Sei  $R$  kommutativer Ring mit Eins.

- (a)  $x, y \in R$  heißen **assoziert**, wenn es  $e \in R^\times$  mit  $y = xe$  gibt. "assoziert" ist eine Äquivalenzrelation.
- (b)  $x \in R \setminus R^\times$ ,  $x \neq 0$  heißt **irreduzibel** (unzerlegbar), wenn aus  $x = y_1 \cdot y_2$  mit  $y_1, y_2 \in R$  folgt:  $y_1 \in R^\times$  oder  $y_2 \in R^\times$ .
- (c)  $x \in R \setminus R^\times$  heißt **prim** (oder **Primelement**), wenn  $(x)$  ein Primideal ist, dh. aus  $x \mid y_1 y_2$  folgt  $x \mid y_1$  oder  $x \mid y_2$ .
- (d) Sind  $x, y \in R \setminus R^\times$  assoziiert, so ist  $x$  genau dann irreduzibel (bzw. prim), wenn  $y$  irreduzibel (bzw. prim) ist.
- (e) Ist  $R$  nullteilerfrei, so ist jedes von Null verschiedene Primelement irreduzibel.

**Beweis:** Sei  $(x)$  Primideal und  $x = y_1 y_2$ ,  $y_1, y_2 \in R \Rightarrow \exists: y_1 \in (x)$ , dh.  $y_1 = xa$  für ein  $a \in R$  ( $R$  nullteilerfrei,  $x \neq 0$ )  $\Rightarrow x = xay_2 \Rightarrow x(1 - ay_2) = 0 \xRightarrow{x \neq 0} ay_2 = 1 \Rightarrow y_2 \in R^\times$  ■

**Beispiel 2.4.5** (a) In  $\mathbb{Z}/6\mathbb{Z}$  ist 2 nicht irreduzibel:  $2 \cdot (-2) = 2$ .

- (b) In  $R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\} \subset \mathbb{C}$  ist  $(1 + \sqrt{-5})(1 - \sqrt{-5}) = 6 = 2 \cdot 3$ . In  $R$  ist 2 kein Primelement, weder  $1 + \sqrt{-5}$  noch  $1 - \sqrt{-5}$  sind durch 2 teilbar, **aber** 2 ist irreduzibel!.

**denn:** Sei  $2 = (a + b\sqrt{-5})(c + d\sqrt{-5}) \Rightarrow 4 = |2|^2 = (a + b\sqrt{-5})(a - b\sqrt{-5})(\dots) = (a^2 + 5b^2)(c^2 + 5d^2) = a^2 c^2 + \underbrace{5P}_{P \geq 0} \Rightarrow P = 0 \Rightarrow b = d = 0 \Rightarrow a^2 = 1, c^2 = 4$

### Proposition + Definition 2.4.6

Sei  $R$  ein Integritätsbereich.

- (a) Folgende Eigenschaften sind äquivalent:
- (i) Jedes  $x \in R \setminus \{0\}$  läßt sich eindeutig als Produkt von Primelementen schreiben.
  - (ii) Jedes  $x \in R \setminus \{0\}$  läßt sich "irgendwie" als Produkt von Primelementen schreiben.
  - (iii) Jedes  $x \in R \setminus \{0\}$  läßt sich eindeutig als Produkt von irreduziblen Elementen schreiben.

- (b) Sind diese drei Eigenschaften für  $R$  erfüllt, so heißt  $R$  **faktorieller Ring**. (Oder **ZPE-Ring** (engl.: UFD)). Dabei ist in (a) "eindeutig" gemeint, bis auf Reihenfolge und Multiplikation mit Einheiten. Präziser: Sei  $\mathcal{P}$  ein Vertretersystem der Primelemente ( $\neq 0$ ) bezüglich "assoziiert".

Dann heißt (i)  $\forall x \in R \setminus \{0\} \exists! e \in R^\times$  und für jedes  $p \in \mathcal{P}$  ein  $\nu_p(x) \geq 0 : x = e \prod_{p \in \mathcal{P}} p^{\nu_p}$ . (beachte  $\nu_p \neq 0$  nur für endlich viele  $p$ ).

**Beweis:**

(i)  $\Rightarrow$  (ii)  $\checkmark$

(ii)  $\Rightarrow$  (iii) Sei  $x \neq 0, x = ep_1 \cdot \dots \cdot p_r, p_i \in \mathcal{P}, e \in R^\times$ .

Sei weiter  $x = q_1 \cdot \dots \cdot q_s$  mit irreduziblem Element  $q_j$ .

Es ist  $x \in (p_1) \Rightarrow \exists j$  mit  $q_j \in (p_1)$ .  $\exists: j = 1$  dh.  $q_1 = \varepsilon_1 p_1$  mit  $\varepsilon_1 \in R^\times$  (da  $q_1$  irreduzibel)  $\Rightarrow \varepsilon_1 q_2 \cdot \dots \cdot q_s = ep_2 \cdot \dots \cdot p_r$ . Mit Induktion über  $r$  folgt die Behauptung.

(iii)  $\Rightarrow$  (i) Noch zu zeigen: Jedes irreduzible Element in  $R$  ist prim.

Sei  $p \in R \setminus R^\times$  irreduzibel,  $x, y \in R$  mit  $xy \in (p)$ , also  $xy = pa$  für ein  $a \in R$ . Schreibe  $x = q_1 \cdot \dots \cdot q_m, y = s_1 \cdot \dots \cdot s_n, a = p_1 \cdot \dots \cdot p_l$  mit irreduziblen Elementen  $q_i, s_j, p_k$ .

$\Rightarrow xy = q_1 \cdot \dots \cdot q_m s_1 \cdot \dots \cdot s_n = pa = p \cdot p_1 \cdot \dots \cdot p_l \xrightarrow{\text{Eindeutigkeit}} p \in \{q_1, \dots, q_m, s_1, \dots, s_n\}$  (bis auf Einheiten)

■

### Bemerkung 2.4.7

Ist  $R$  faktorieller Ring, so gibt es zu allen  $a, b \in R \setminus \{0\}$  einen ggT( $a, b$ ).

**Beweis:** Sei  $\mathcal{P}$  wie in 2.4.6 Vertretersystem der Primelemente.

$$a = e_1 \prod_{p \in \mathcal{P}} p^{\nu_p(a)}, b = e_2 \prod_{p \in \mathcal{P}} p^{\nu_p(b)} \Rightarrow d := \prod_{p \in \mathcal{P}} p^{\nu_p(d)}$$

mit  $\nu_p(d) = \min(\nu_p(a), \nu_p(b))$  ist ggT von  $a$  und  $b$ .

■

## Satz 8

Jeder nullteilerfreie Hauptidealring ist faktoriell.

**Beweis:**

- (1) Jedes  $x \in R \setminus \{0\}$  lässt sich als Produkt von irreduziblen Elementen schreiben.  
 (2) Jedes irreduzible  $p \in R \setminus \{0\}$  erzeugt ein maximales Ideal. Mit 2.4.6 folgt dann die Behauptung.

B(2) Sei  $p \in R \setminus \{0\}$  irreduzibel,  $I$  Ideal in  $R$  mit  $(p) \subseteq I \subset R$ .  
 Nach Voraussetzung gibt es  $a \in R$  mit  $I = (a)$ ,  $a \notin R^\times$ , da  $I \neq R$ .  
 Da  $p \in (p) \subseteq I = (a)$ , gibt es  $\varepsilon \in R$  mit  $p = a\varepsilon \xrightarrow{p \text{ irreduzibel}} \varepsilon \in R^\times \Rightarrow (p) = (a) = I$

B(1)  $x \in R \setminus \{0\}$  heie Strenfried, wenn  $x$  nicht als Produkt von irreduziblen Elementen darstellbar ist.  
 Sei  $x$  Strenfried. Dann ist  $x \notin R^\times$  und  $x$  nicht irreduzibel, also  $x = x_1 y_1$  mit  $x_1, y_1 \notin R^\times$ .  
 Sei  $x_1$  Strenfried (sonst ist  $x$  doch Produkt von irreduziblen Elementen). Also  $x_1 = x_2 y_2$ ,  $x_2, y_2 \notin R^\times$ .  
 Sei  $x_2$  Strenfried. Induktiv erhalten wir  $x, x_1, x_2, \dots$  alles Strenfriede mit  $(x) \subset (x_1) \subset (x_2) \subset \dots$ .  
 Sei nun  $I = \bigcup_{i \geq 1} (x_i)$ .  $I$  ist Ideal  $\checkmark \Rightarrow$   
 Es gibt  $a \in R$  mit  $I = (a) \Rightarrow \exists i$  mit  $a \in (x_i) \Rightarrow x_j \in (x_i)$  fr alle  $j > i$  ■

### Bemerkung 2.4.8

Sei  $R$  ein faktorieller Ring,  $\mathcal{P}$  ein Vertretersystem der Primelemente  $\neq 0$ . Fr  $x \in R \setminus \{0\}$  sei  $x = e \prod_{p \in \mathcal{P}} p^{\nu_p(x)}$  die eindeutige Darstellung, also  $e \in R^\times$ ,  $\nu_p(x) \in \mathbb{N}$ ,  $\nu_p(x) \neq 0$  nur fr endlich viele  $p \in \mathcal{P}$ . Dann gilt fr jedes  $p \in \mathcal{P}$ :

- (a)  $\nu_p(x) = n \iff p^n \mid x$  und  $p^{n+1} \nmid x$   
 (b) Die Abbildung  $\nu_p \rightarrow \mathbb{N}$  erfllt  
 (i)  $\nu_p(x \cdot y) = \nu_p(x) + \nu_p(y)$   
 (ii)  $\nu_p(x + y) \geq \min(\nu_p(x), \nu_p(y))$ , falls  $x + y \neq 0$   
 (c) Sei  $\rho \in \mathbb{R}$ ,  $0 < \rho < 1$ . Dann ist die Abbildung  $|\cdot|_\rho : R \rightarrow \mathbb{R}$ ,

$$|x|_\rho = \begin{cases} \rho^{\nu_p(x)}, & x \neq 0 \\ 0 & x = 0 \end{cases}$$

ein „nichtarchimedischer Betrag“ auf  $R$ , d.h.  $|x \cdot y|_\rho = |x|_\rho \cdot |y|_\rho$  und  $|x + y|_\rho \leq \max(|x|_\rho, |y|_\rho)$ .

- (d)  $d_\rho(x, y) = |x - y|_\rho$  ist eine Metrik auf  $R$ .

**Beispiel:**  $R = \mathbb{Z}$ ,  $\mathcal{P} = \{p \in \mathbb{N}_{>0}, p \text{ Primzahl}\}$ .  $\nu_p$  ist die  $p$ -adische Bewertung und  $|\cdot|_{\frac{1}{p}}$  ist der  $p$ -adische Betrag auf  $\mathbb{Z}$  (und  $\mathbb{Q}$ ).

### Satz 9 (Irreduzibilitätskriterium für Polynome)

Sei  $R$  ein faktorieller Ring,  $p \in \mathcal{P}$ ,  $f = \sum_{i=0}^n a_i X^i \in R[X]$  mit  $a_n \neq 0$ ,  $\text{ggT}(a_0, \dots, a_n) = 1$ ,  $p \nmid a_n$ .

- (a) (Eisenstein) Ist  $n > 0$ ,  $p \mid a_i$  oder  $a_i = 0$  für  $i = 0, \dots, n-1$ ,  $p^2 \nmid a_0 \neq 0$ , so ist  $f$  irreduzibel.

**Beweis:** Sei  $f = gh$  mit  $g = \sum_{i=0}^r b_i X^i$ ,  $h = \sum_{i=0}^s c_i X^i$ ,  $b_r \neq 0 \neq c_s \Rightarrow n = r + s$ ,  $a_n = b_r c_s$ ,  $a_0 = b_0 c_0 \Rightarrow p \nmid b_r$ ,  $p \nmid c_s$

- (a)  $\exists p \mid b_0$ ,  $p \nmid c_0$ .

Sei  $t$  maximal mit  $p \mid b_i$  für  $i = 0, \dots, t$

Dann ist  $0 \leq t \leq r-1$  und

$$\underbrace{a_{t+1}}_{\notin (p)} = \underbrace{b_{t+1} \cdot c_0}_{\notin (p)} + \underbrace{\sum_{i=0}^t b_i c_{t+1-i}}_{\in (p)}$$

$\Rightarrow t+1 = n \Rightarrow r = n \Rightarrow s = 0 \Rightarrow f = c_0 \cdot g$ , nach Voraussetzung ist dann  $c_0 \in R^\times$ . ■

## 2.5 Brüche

**Ziel:** Verallgemeinere die Konstruktion von  $\mathbb{Q}$  aus  $\mathbb{Z}$ .

$$\mathbb{Q} = \left\{ \frac{m}{n} : m, n \in \mathbb{Z} \neq 0 \right\} / \sim$$

mit  $\frac{m}{n} \sim \frac{m'}{n'} \Leftrightarrow mn' = m'n$

### Definition + Bemerkung 2.5.1

Sei  $R$  kommutativer Ring mit Eins,  $S \subseteq (R, \cdot)$  ein Untermonoid.

- (a)  $S^{-1}R = R_S = (R \times S) / \sim$  mit der Äquivalenzrelation  $(a_1, s_1) \sim (a_2, s_2) \Leftrightarrow \exists t \in S : t(a_2 s_1 - a_1 s_2) = 0$  heißt **Ring der Brüche** von  $R$  mit Nennern in  $S$ . (oder **Lokalisierung** von  $R$  nach  $S$ ) Schreibweise:  $\frac{a}{s}$  sei eine Äquivalenzklasse von  $(a, s)$

## 2 Ringe

**Beweis:** z.z.:  $\sim$  ist Äquivalenzrelation:

reflexiv ✓

symmetrisch ✓

transitiv:  $\left. \begin{array}{l} (1) \quad a_2 s_1 = a_1 s_2 \\ (2) \quad a_3 s_2 = a_2 s_3 \end{array} \right\} \xRightarrow{?} a_3 s_1 = a_1 s_3$

$$a_3 s_2 s_1 \stackrel{(2)}{=} a_2 s_3 s_1 \stackrel{(1)}{=} a_1 s_3 s_2 \Rightarrow s_2(a_3 s_1 - a_1 s_3) = 0$$

(falls  $R$  nullteilerfrei und  $0 \notin S \Rightarrow a_3 s_1 = a_1 s_3$ )

Andernfalls sei nun mit  $t, t' \in S$   $\left. \begin{array}{l} t(a_2 s_1 - a_1 s_2) = 0 \\ t'(a_2 s_3 - a_3 s_2) = 0 \end{array} \right\} \Rightarrow t t' s_2(a_3 s_1 - a_1 s_3) = t(t' a_3 s_2 s_1 - t' a_1 s_3 s_2) \stackrel{(2)}{=} t(t' a_2 s_3 s_1 - t' a_1 s_3 s_2) = t s_3 t'(a_2 s_1 - a_1 s_2) \stackrel{(1)}{=} 0$  ■

(b) Mit  $\frac{a_1}{s_1} \cdot \frac{a_2}{s_2} = \frac{a_1 a_2}{s_1 s_2}$  und  $\frac{a_1}{s_1} + \frac{a_2}{s_2} = \frac{a_1 s_2 + a_2 s_1}{s_1 s_2}$  ist  $R_S$  ein kommutativer Ring mit Eins.

**Beweis:**  $\cdot$  wohldefiniert: Sei  $\frac{a'_1}{s'_1} = \frac{a_1}{s_1} \Rightarrow \exists t \in S : t(a'_1 s_1 - a_1 s'_1) = 0(*) \Rightarrow t(a'_1 a_2 s_1 s_2 - a_1 a_2 s_2 s'_1) \stackrel{(*)}{=} (t a_1 s'_1 a_2 s_2 - t a_1 a_2 s_2 s'_1) = 0$   
 $+$  wohldefiniert: Seien die  $\frac{a'_1}{s'_1}, \frac{a_1}{s_1}$  wie oben.  $\Rightarrow t(s'_1 s_2(a_1 s_2 + a_2 s_1) - s_1 s_2(a'_1 s_2 + a_2 s'_1)) = t s_2(a_1 s_2 s'_1 + a_2 s_1 s'_1 - a'_1 s_1 s_2 - a_2 s_1 s'_1) \stackrel{(\dots)}{=} 0$ . Die restlichen Eigenschaften vererben sich von  $R$  ■

### Definition + Bemerkung 2.5.2

Sei  $R$  Integritätsbereich,  $S = R \setminus \{0\}$ . Dann ist  $\text{Quot}(R) := R_S$  ein Körper, denn das Inverse zu  $\frac{b}{a}$  mit  $a \neq 0$  ist  $\frac{a}{b}$ . Er heißt der **Quotientenkörper** von  $R$ . (Dieser Begriff hat mit dem Quotientenring  $R/I$  von  $R$  modulo einem Ideal  $I$  nichts zu tun.)

#### Beispiel:

(a)  $R = \mathbb{Z}[X] \Rightarrow \text{Quot}(R) = \mathbb{Q}(X)$

(b)  $R = K[X_1, \dots, X_n]$ ,  $K$  Körper  $\Rightarrow \text{Quot}(R) = K(X_1, \dots, X_n)$  Körper der rationalen Funktionen in  $n$  Variablen.

### Beispiele 2.5.3 (a) Ist $0 \in S$ , so ist $R_S = 0$ .

(b)  $x \in R \setminus \{0\}$ ,  $S = \{x^n : n \geq 0\}$   $R_S =: R_x = \{\frac{a}{x^n} : a \in R, n \geq 0\}$   
 z.B.:  $R = \mathbb{Z}$ ,  $x = 2 \Rightarrow R_S = \mathbb{Z}[\frac{1}{2}] = \{\frac{m}{2^n} : m \in \mathbb{Z}, n \in \mathbb{N}\}$

(c) Sei  $\mathfrak{p} \subset R$  Primideal, dann ist  $S = R \setminus \mathfrak{p}$  Monoid.  
 $R_S =: R_{\mathfrak{p}}$  heißt Lokalisierung von  $R$  nach  $\mathfrak{p}$ .



**Beispiel:**

- a)  $R = \mathbb{Z}$ ,  $\mathfrak{p} = (2) \Rightarrow \mathbb{Z}_{(2)} = \left\{ \frac{m}{n} : m \in \mathbb{Z}, n \text{ ungerade} \right\}$
- b)  $\mathfrak{p} = (0)$ ,  $R$  nullteilerfrei, dann ist  $R_{\mathfrak{p}} = \text{Quot}(R)$ .
- c)  $R = K[X]$ ,  $\mathfrak{p} = (X)$ , dann ist  $R_{\mathfrak{p}} = \left\{ \frac{f}{g}, f, g \in K[X], g(0) \neq 0 \right\}$ .

(d)  $\mathfrak{p}R_{\mathfrak{p}} = \left\{ \frac{x}{y} : x \in \mathfrak{p}, y \in R \setminus \mathfrak{p} \right\}$  ist maximales Ideal in  $R_{\mathfrak{p}}$  und zwar das einzige.

**denn:** Sei  $\frac{z}{y} \in R_{\mathfrak{p}} \setminus \mathfrak{p}R_{\mathfrak{p}}$ , dh.  $z \in R \setminus \mathfrak{p}, y \in R \setminus \mathfrak{p} \Rightarrow \frac{y}{z} \in R_{\mathfrak{p}} \Rightarrow \frac{z}{y} \in (R_{\mathfrak{p}})^{\times}$ ,  
 typisches Beispiel:  $R = \mathbb{R}[X]$  (oder  $R = C^0([-1, 1])$ )  $\mathfrak{p} = \{f \in R : f(0) = 0\}$  ist  
 Primideal in  $R$ .  $R_{\mathfrak{p}} = \left\{ \frac{f}{g} : f, g \in R, g(0) \neq 0 \right\}$

**Bemerkung 2.5.4**

Sei  $R$  kommutativer Ring mit Eins,  $S \subset (R, \cdot)$  Monoid.

- (a) Die Abbildung  $i_S : R \rightarrow R_S, a \mapsto \frac{a}{1}$  ist Ringhomomorphismus
- (b)  $i_S$  ist injektiv genau dann, wenn  $S$  keinen Nullteiler von  $R$  enthält. ( $0 \notin S$ )

**Beweis:**  $\frac{a}{1} = 0 = \frac{0}{1}$  in  $R_S \Rightarrow \exists s \in S$  mit  $s(a1 - 01) = 0$  ■

(c)  $i_S(S) \subset (R_S)^{\times}$

**Beweis:**  $\left(\frac{s}{1}\right)^{-1} = \frac{1}{s}$  ■

(d) (UAE) Zu jedem Homomorphismus  $\varphi : R \rightarrow R'$  von Ringen mit Eins mit  $\varphi(S) \subset (R')^{\times}$  gibt es genau einen Homomorphismus  $\tilde{\varphi} : R_S \rightarrow R'$  mit  $\varphi = \tilde{\varphi} \circ i_S$

**Beweis:**  $\tilde{\varphi}\left(\frac{a}{s}\right) = \tilde{\varphi}\left(a \frac{1}{s}\right) = \tilde{\varphi}\left(\frac{a}{1} \left(\frac{s}{1}\right)^{-1}\right) = \varphi(a)\varphi(s)^{-1}$  ■

**2.6 Der Satz von Gauß**

Sei  $R$  faktorieller Ring,  $\mathcal{P}$  Vertretersystem der von Null verschiedenen Primelemente in  $R$ .

**Bemerkung 2.6.1**

Für jedes  $p \in \mathcal{P}$  lässt sich  $\nu_p$  fortsetzen zu einer Abbildung  $\nu_p : \text{Quot}(R) \setminus \{0\} \rightarrow \mathbb{Z}$ , die die Eigenschaften von 2.4.8 b) erfüllt. Dabei gilt für  $a, b \in R \setminus \{0\} : \nu_p\left(\frac{a}{b}\right) = \nu_p(a) - \nu_p(b)$ .

**Beispiel:**

- (a)  $R = \mathbb{Z}$ ,  $\mathcal{P} = \{p \in \mathbb{N}, p \text{ Primzahl}\}$ .  $\nu_p$  ist die  **$p$ -adische Bewertung** auf  $\mathbb{Q}$ . Die Vervollständigung von  $\mathbb{Q}$  wie in Beispiel 2.3.6 ergibt den Körper  $\mathbb{Q}_p$  der  $p$ -adischen Zahlen.
- (b)  $R = \mathbb{C}[X]$ ,  $\mathcal{P} = \{X - a, a \in \mathbb{C}\}$ . Für  $p = X - a \in \mathcal{P}$ ,  $f \in \mathbb{C}[X]$  ist  $\nu_p(f) = \text{ord}_a(f)$  die Nullstellenordnung der Nullstelle  $a$ .

### Definition + Proposition 2.6.2

Sei  $R$  faktorieller Ring,  $\mathcal{P}$  Vertretersystem der von Null verschiedenen Primelemente in  $R$ ,  $p \in \mathcal{P}$  und  $K = \text{Quot}(R)$ .

- (a) Für  $f = \sum_{i=0}^n a_i X^i \in K[X] \setminus \{0\}$  sei  $\nu_p(f) := \min\{\nu_p(a_i), i = 0, \dots, n\}$ .
- (b)  $f \in K[X] \setminus \{0\}$  heißt **primitiv**, wenn  $\nu_p(f) = 0$  für alle  $p \in \mathcal{P}$  ist.
- (c) (Gauß) Für  $f, g \in K[X] \setminus \{0\}$  gilt:  $\nu_p(f \cdot g) = \nu_p(f) + \nu_p(g)$  für alle  $p \in \mathcal{P}$ .

**Beweis:** Sei  $f = \sum_{i=0}^n a_i X^i$ ,  $g = \sum_{j=0}^m b_j X^j$ ,  $f \cdot g = \sum_{k=0}^{m+n} c_k X^k$ , also  $c_k = \sum_{i+j=k} a_i b_j$ .

**1. Fall:** Sei  $m = 0$ . Dann ist  $c_k = a_k b_0$  für  $k = 0, \dots, n$  und

$$\begin{aligned} \nu_p(f \cdot g) &= \min_{i=0}^n (\nu_p(a_i b_0)) \\ &= \min_{i=0}^n (\nu_p(a_i) + \nu_p(b_0)) \\ &= \min_{i=0}^n (\nu_p(a_i)) + \nu_p(b_0) = \nu_p(f) + \nu_p(g) \end{aligned}$$

**2. Fall:** Sei  $f, g \in R[X]$  und primitiv, also  $\nu_p(f) = \nu_p(g) = 0$ . Sei  $i_0 := \min_{i=0}^n \{i : p \nmid a_i\}$  und  $j_0 := \min_{j=0}^m \{j : p \nmid b_j\}$ . Es ist:

$$c_{i_0+j_0} = \underbrace{a_{i_0} b_{j_0}}_{p \nmid} + \sum_{i=0}^{i_0-1} \underbrace{a_i}_{p \mid} b_{i_0+j_0-i} + \sum_{j=0}^{j_0-1} a_{i_0+j_0-j} \underbrace{b_j}_{p \mid}$$

also gilt  $p \nmid c_{i_0+j_0}$  und damit  $\nu_p(f \cdot g) = 0$ .

**3. Fall:**  $f, g$  sind beliebig. Es gibt  $c, d \in K \setminus \{0\}$ , so dass  $\tilde{f} = c \cdot f$ ,  $\tilde{g} = d \cdot g$  primitiv sind. Dann folgt aus Fall 1 und Fall 2, dass:

$$\begin{aligned}\nu_p(f \cdot g) &= \nu_p\left(\frac{1}{c} \tilde{f} \cdot \frac{1}{d} \tilde{g}\right) \\ &= \nu_p\left(\frac{1}{c}\right) + \nu_p\left(\frac{1}{d}\right) + \nu_p(\tilde{f} \cdot \tilde{g}) \\ &= \nu_p\left(\frac{1}{c}\right) + \nu_p(\tilde{f}) + \nu_p\left(\frac{1}{d}\right) + \nu_p(\tilde{g}) \\ &= \nu_p(f) + \nu_p(g)\end{aligned}$$

■

### Satz 10 (Gauß)

Ist  $R$  faktorieller Ring, so ist  $R[X]$  faktoriell.

**Beweis:** Sei  $K = \text{Quot}(R)$ . Dann ist  $K[X]$  faktoriell (sogar euklidisch), und  $R[X] \subseteq K[X]$  ist ein Unterring. Sei  $\mathcal{P}$  Vertretersystem der von Null verschiedenen Primelemente in  $K[X]$ . O.B.d.A. ist jedes Primpolynom in  $\mathcal{P}$  ein primitives Polynom in  $R[X]$ . Sei weiter  $\tilde{\mathcal{P}}$  ein Vertretersystem der von Null verschiedenen Primelemente in  $R$ . Sei nun  $f \in R[X] \setminus \{0\}$ . Schreibe  $f = c \cdot f_1 \cdots f_n$  mit  $f_i \in \mathcal{P}$  und  $c \in (K[X])^\times = K \setminus \{0\}$ .

Es ist  $c \in R$ , denn: für  $p \in \tilde{\mathcal{P}}$  ist nach 2.6.2

$$\underbrace{\nu_p(f)}_{\geq 0} = \nu_p(c) + \sum_{i=1}^n \underbrace{\nu_p(f_i)}_{=0},$$

also ist  $\nu_p(c) \geq 0$ .

Schreibe also  $c = e \cdot p_1 \cdots p_m$  mit  $e \in R^\times$  und  $p_i \in \tilde{\mathcal{P}}$ .

**Behauptung 1:** Jedes  $p_i \in \tilde{\mathcal{P}}$  ist auch prim in  $R[X]$ :

Sei  $(p) := p \cdot R[X]$  das von  $p$  in  $R[X]$  erzeugte Ideal. Es genügt zu zeigen:  $R[X]/(p)$  ist nullteilerfrei (nach 2.3.3 b)). Sei  $\bar{R} := R/(p \cdot R)$ .  $\bar{R}$  ist nullteilerfrei, da  $p \in \tilde{\mathcal{P}}$  ist, also ist auch  $\bar{R}[X]$  nullteilerfrei.

Die Restklassenabbildung  $\pi : R \rightarrow \bar{R}$  ist surjektiv und induziert einen surjektiven Ringhomomorphismus  $\tilde{\pi} : R[X] \rightarrow \bar{R}[X]$ . Es ist Kern  $\pi = \{f = \sum_{i=0}^n a_i X^i \in R[X], p \mid a_i, i = 0, \dots, n\} = p \cdot R[X]$ , also ist  $\bar{R}[X] \cong R[X]/(p)$ .

**Behauptung 2:** Jedes  $f_i \in \mathcal{P}$  ist auch prim in  $R[X]$ :

Seien  $g, h \in R[X]$  mit  $g \cdot h \in (f_i) := f_i \cdot R[X]$ . Da  $f_i$  prim in  $K[X]$  ist, ist o.B.d.A:  $g \in f_i \cdot K[X]$ , also  $g = f_i \cdot \tilde{g}$  für ein  $\tilde{g} \in K[X]$ . Für jedes  $p \in \tilde{\mathcal{P}}$  ist  $0 \leq \nu_p(g) = \nu_p(f_i) + \nu_p(\tilde{g}) = \nu_p(\tilde{g})$ , also ist  $\tilde{g} \in R[X]$  und damit  $(f_i)$  ein Primideal in  $R[X]$ . ■

### Beispiel 2.6.3

$f(X) = X^{p-1} + X^{p-2} + \dots + X + 1 \in \mathbb{Q}[X]$ ,  $p$  Primzahl. Beh.:  $f$  ist irreduzibel.

Beobachte:

$$f(X) = \frac{X^p - 1}{X - 1}$$

( $f$  heißt "p-tes Kreisteilungspolynom" (Zeichnung fehlt))

**Trick:**  $g(X) = f(X + 1)$  ist genau dann irreduzibel, wenn  $f(X)$  irreduzibel ist.

$$g(X) = \frac{(X+1)^p - 1}{X} = \sum_{k=1}^p \binom{p}{k} X^{k-1}, \quad (n = p-1), \quad \binom{p}{p} = 1 = a_{p-1}, \quad \binom{p}{1} = p = a_0$$

Noch zu überlegen:  $\binom{p}{k}$  ist durch  $p$  teilbar für  $k = 1, \dots, p-1$ , bekannt:  $\binom{p}{k} = \frac{p!}{k!(p-k)!} \Rightarrow \binom{p}{k}$  ist durch  $p$  teilbar. Mit Eisenstein folgt die Behauptung.

## 2.7 Maximale Ideale

### Proposition 2.7.1

Sei  $R$  ein kommutativer Ring mit Eins. Dann gibt es zu jedem echten Ideal  $I \subsetneq R$  ein maximales Ideal  $\mathfrak{m}$  mit  $I \subseteq \mathfrak{m}$ .

### Lemma von Zorn

Sei  $M$  eine nicht leere, geordnete Menge. Hat jede total geordnete Teilmenge von  $M$  eine obere Schranke in  $M$ , so besitzt  $M$  ein maximales Element.

Zur Erinnerung:

- $\leq$  heißt **Ordnung** wenn  $\leq$  reflexiv, transitiv und antisymmetrisch ist.
- $N \subset M$  ist **total geordnet**, falls für  $x, y \in N$  gilt:  $x \leq y$  oder  $y \leq x$ .
- $x \in M$  ist eine **oberere Schranke** für  $N$  wenn für alle  $y \in N$  gilt:  $y \leq x$ .
- $m \in M$  heißt **maximal**, wenn für alle  $x \in M$  aus  $m \leq x$  folgt, dass  $x = m$  ist.

**Beweis:** (der Proposition) Sei  $M$  die Menge aller echten Ideale in  $R$ , die  $I$  enthalten.  $I \in M$ , also  $M \neq \emptyset$ .  $M$  ist durch  $\subseteq$  geordnet.

**Behauptung:**  $n = \bigcup_{J \in N} J$  ist obere Schranke für  $N \subseteq M$ . Nach Zorn enthält  $M$  dann ein maximales Element  $\mathfrak{m}$ .  $\mathfrak{m}$  ist ein maximales Ideal in  $R$ . ■

**Beweis:** (der Behauptung)

- $n$  ist ein Ideal: Seien  $x, y \in n$ , also  $x \in J_1, y \in J_2$ . O.B.d.A.A.  $J_1 \subseteq J_2$ , also  $x \in J_2$  und damit auch  $x + y \in J_2 \subseteq n$ . Auch gilt für alle  $a \in R$ :  $a \cdot x \in J \subseteq n$ .
- $I \subseteq n$  ✓
- $n$  ist eine obere Schranke von  $N$ . ✓
- $n \neq R$ , denn sonst wäre  $1 \in n$ , also  $1 \in J$  für ein  $J \in N$ , im Widerspruch zu  $J \in M$ .

## 2.8 Moduln

Sei  $R$  kommutativ mit Eins.

**Definition + Bemerkung 2.8.1** (a) Eine abelsche Gruppe  $(M, +)$  zusammen mit einer Abbildung  $\bullet : R \times M \rightarrow M$  heißt **R-Modul**, wenn für alle  $a, b \in R, x, y \in M$  gilt:

- (i)  $a(x + y) = ax + ay$
- (ii)  $(a + b)x = ax + bx$
- (iii)  $(ab)x = a(bx)$
- (iv)  $1x = x$

**Beispiel:**

- (1)  $R$  ist  $R$ -Modul. (mit  $\cdot$  als Ringmultiplikation)
- (2) Ist  $R$  ein Körper, so ist  $R$ -Modul =  $R$ -Vektorraum.
- (3)  $R = \mathbb{Z}, M = \mathbb{Z}/2\mathbb{Z} = \{\bar{0}, \bar{1}\}$  ist  $\mathbb{Z}$ -Modul durch  $n \cdot \bar{0} = \bar{0}, n \cdot \bar{1} = \bar{n}$ . Jede abelsche Gruppe  $A$  ist  $\mathbb{Z}$ -Modul durch  $nx = \underbrace{x + \dots + x}_{n\text{-mal}}$  und  $(-n)x = n(-x)$  für  $n \in \mathbb{N}_1, x \in A$
- (4) Jedes Ideal in  $R$  ist  $R$ -Modul.

- (b) Eine Abbildung  $\varphi : M \rightarrow M'$  von  $R$ -Moduln heißt **R-Modulhomomorphismus** (oder **R-linear**), wenn  $\varphi$  Gruppenhomomorphismus ist und für alle  $x \in M, a \in R$  gilt:  $\varphi(ax) = a\varphi(x)$

## 2 Ringe

- (c)  $\text{Hom}_R(M, M') := \{\varphi : M \rightarrow M' : \varphi \text{ } R\text{-linear}\}$  ist  $R$ -Modul durch
- $$\left. \begin{aligned} (\varphi_1 + \varphi_2)(x) &:= \varphi_1(x) + \varphi_2(x) \\ (a\varphi)(x) &:= a\varphi(x) \end{aligned} \right\} \forall \varphi_1, \varphi_2 \in \text{Hom}_R(M, M'), a \in R, x \in M$$

(d) Die  $R$ -Moduln bilden mit den  $R$ -linearen Abbildungen eine Kategorie

(e) Die Kategorien  $\mathbb{Z}\text{-Mod.}$  und **Abelsche Gruppen** sind isomorph. denn:

$$\dots \varphi(nx) = \varphi(x + \dots + x) = \varphi(x) + \dots + \varphi(x) = n\varphi(x)$$

( $\varphi : A \rightarrow A'$  Gruppenhomomorphismus,  $x \in A$ ,  $n \in \mathbb{N}$ )  $\Rightarrow$  Jeder Gruppenhomomorphismus von abelschen Gruppen ist  $\mathbb{Z}$ -linear.

### Definition + Bemerkung 2.8.2

Sei  $M$  ein  $R$ -Modul.

- (a) Eine Untergruppe  $U$  von  $(M, +)$  heißt  **$R$ -Untermodul** von  $M$ , wenn  $R \cdot U \subseteq U$  ist, dh. wenn  $U$  selbst  $R$ -Modul ist.
- (b) Ist  $\varphi : M \rightarrow M'$   $R$ -linear, so sind  $\text{Kern}(\varphi)$  und  $\text{Bild}(\varphi)$  Untermoduln von  $M$  bzw.  $M'$  (denn  $\varphi(x) = 0 \Rightarrow \varphi(ax) = 0 \forall \dots$  und  $a\varphi(x) = \varphi(ax) \forall \dots$ )
- (c) Sei  $U \subseteq M$  Untermodul.  
Dann wird  $M/U$  zu einem  $R$ -Modul durch  $a\bar{x} := \overline{ax}$  (denn: Ist  $x' \in \bar{x}$ , also  $x - x' \in U$ , so ist  $ax' - ax = a(x' - x) \in U$ )  
Die Restklassenabbildung  $p : M \rightarrow M/U$ ,  $x \mapsto \bar{x}$  ist dann  $R$ -linear ( $p(ax) = \overline{ax} = a\bar{x} = ap(x)$ )

### Definition + Bemerkung 2.8.3 (a) Für $X \subseteq M$ heißt

$$\langle X \rangle := \bigcap_{\substack{U \text{ Untermodul von } M \\ X \subseteq U}} U$$

der von  $X$  erzeugte Untermodul.

- (b)  $\langle X \rangle = \left\{ \sum_{i=0}^n a_i x_i, a_i \in R, x_i \in X, n \in \mathbb{N} \right\}$ .

- (c) Eine Teilmenge  $B \subseteq M$  heißt **linear unabhängig**, wenn  $0 = \sum_{b \in B} a_b b$  mit  $a_b \in R$  (wobei  $a_b = 0$  für alle bis auf endlich viele  $b \in B$  gelten soll, damit die Summe  $\sum_{b \in B} a_b b$  wohldefiniert ist) nur möglich ist mit  $a_i = 0 \forall i$ .

- (d) Eine Teilmenge  $B \subseteq M$  heißt **Basis**, wenn jedes  $x \in M$  eindeutig als Linearkombination  $0 = \sum_{b \in B} a_b b$  mit  $a_b \in R$  (wobei  $a_b = 0$  für alle bis auf endlich viele  $b \in B$  gelten soll) darstellbar ist.  
äquivalent:  $B$  linear unabhängig und  $\langle B \rangle = M$

(e)  $M$  heißt **frei**(er  $R$ -Modul), wenn  $M$  eine Basis besitzt.

**Beispiel:**

- (1)  $R$  ist freier  $R$ -Modul mit Basis 1 (oder einer anderen Einheit)
- (2) Für jedes  $n \in \mathbb{N}$  ist  $R^n = R \oplus \cdots \oplus R$  freier  $R$ -Modul mit Basis  $e_1, \dots, e_n$ ,  $e_i = (0, \dots, 0, 1, 0, \dots, 0)$  (hier steht die 1 an der  $i$ -ten Stelle).
- (3) Ist  $I \subseteq R$  Ideal, so ist  $M := R/I = \langle \{\bar{1}\} \rangle$ . Für  $I \neq \{0\}$  ist  $R/I$  **nicht** frei. denn: Sei  $\bar{x} \in M$ ,  $a \in I \setminus \{0\} \Rightarrow a\bar{x} = \overline{ax} = \bar{0} \Rightarrow$  in  $M$  gibt es kein linear unabhängiges Element (oder, um formal zu sein, keine linear unabhängige einelementige Teilmenge).

