

# Inhaltsverzeichnis

<b>1</b>	<b>Kommutative Ringe</b>	<b>2</b>
1.1	Ringe . . . . .	2
1.2	Einheiten, Teilbarkeit, Quotientenkörper (Seite 34) . . . . .	4
1.3	Ring der Polynome (Seite 41) . . . . .	6
1.4	Ideale und Faktorringe . . . . .	10
1.5	Charakteristik eines Körpers . . . . .	14
1.6	Primideale und Maximalideale . . . . .	14
1.7	Unterring . . . . .	16
1.8	Matrizen . . . . .	17
<b>2</b>	<b>Faktorisierungen von Ringen</b>	<b>19</b>
2.1	Euklidische Ringe . . . . .	19
2.2	Hauptidealring . . . . .	22
2.3	Faktorielle Ringe . . . . .	25
2.4	Einige algebraische Euklidische Ringe . . . . .	28
2.5	Polynomringe . . . . .	31
<b>A</b>	<b>Auswahlaxiom und das Zornsche Lemma</b>	<b>36</b>

# Kapitel 1: Kommutative Ringe

## 1.1 Ringe

**Definition.** Ein *Ring* ist eine Menge  $R$  ausgestattet mit Elementen  $0 \in R$ ,  $1 \in R$  und drei Abbildungen

$$\begin{cases} + : R \times R \rightarrow R \\ - : R \rightarrow R \\ \cdot : R \times R \rightarrow R \end{cases}$$

so dass folgende Axiome gelten.

$(R, +)$  ist eine abelsche Gruppe mit neutralem Element  $0$  und Inversem  $-$  d.h.

$$\begin{aligned} (a + b) + c &= a + (b + c) \\ 0 + a &= a \\ (-a) + a &= 0 \\ a + b &= b + a \end{aligned}$$

für alle  $a, b, c \in R$ .

$(R, \cdot)$ : Assoziativität  $(a \cdot b) \cdot c = a \cdot (b \cdot c)$  und Einselement  $1 \cdot a = a = a \cdot 1$ .

Distributivität:  $a(b + c) = ab + ac$  und  $(b + c)a = ba + ca$ .

Falls zusätzlich Kommutativität von  $\cdot$  gilt:  $ab = ba$ , dann sprechen wir von einem *kommutativen Ring*.

*Bemerkung.* •  $0$  ist eindeutig durch die Axiome bestimmt.

- Ebenso ist  $-a$  durch die Axiome für jedes  $a \in R$  eindeutig bestimmt.
- $0 \neq 1$  wurde nicht verlangt.
- $0 \cdot a = 0$  für jedes  $a \in R$  :

$$0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a \Rightarrow 0 = 0 \cdot a.$$

*Konvention.* • Klammern bei  $+$  (und ebenso bei  $\cdot$ ) lassen wir auf Grund der Assoziativität der Addition (Mult.) weg also  $a + b + c + d$ .

- Punktrechnung vor Strichrechnung, d.h.  $a \cdot b + c = (a \cdot b) + c$ .
- Den Multiplikationspunkt lässt man oft weg.

*Notation.*

$$\begin{aligned} 0 \cdot a &= 0 & 1 \cdot a &= a & 2 \cdot a &= a + a & 3 \cdot a &= a + a + a \\ (n + 1) \cdot a &= n \cdot a + a, & (-n) \cdot a &= -(n \cdot a) \text{ für } n \in \mathbb{N}. \end{aligned}$$

Dies definiert eine Abbildung  $\mathbb{Z} \times R \rightarrow R, (n, a) \mapsto n \cdot a$ . Diese erfüllt:  $(m + n) \cdot a = m \cdot a + n \cdot a$ ,  $n \cdot (a + b) = n \cdot a + n \cdot b$ .

Ebenso definieren wir

$$a^0 = 1_R \quad a^1 = a \quad a^2 = a \cdot a \quad a^{n+1} = a^n \cdot a \text{ für } n \in \mathbb{N}$$

Diese erfüllt

$$a^{m+n} = a^m + a^n \quad (a^m)^n = a^{m \cdot n} \quad (ab)^n = a^n b^n$$

in kommutativen Ringen.

**Definition.** Angenommen  $R, S$  sind Ringe und  $f : R \rightarrow S$  ist eine Abbildung. Wir sagen  $f$  ist ein *Ringhomomorphismus* falls

$$f(1_R) = 1_S \quad f(a+b) = f(a) + f(b) \quad f(a \cdot b) = f(a) \cdot f(b)$$

für alle  $a, b \in R$ . Falls  $f$  invertierbar ist, so nennen wir  $f$  einen *Ringisomorphismus*.

*Bemerkung.*  $f(0_R = 0_S)$  denn  $f(0_R) = f(0+0) = f(0) + f(0) \geq 0_S = f(0_R)$ .  
 $f(-a) = -f(a)$  für  $a \in R$  (ähnlicher Beweis).

**Definition.** Sei  $R$  ein Ring und  $S \subseteq R$  auch ein Ring. Wir sagen  $S$  ist ein *Unterring*, falls  $\text{id} : S \rightarrow R, s \mapsto s$  ein Ringhomomorphismus ist.

**Beispiel** (Ringe). (1)  $R = \{0\}$ . Hier ist  $0 = 1$ .

(2)  $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$  sind jeweils Unterringe.

(3) Sei  $V$  ein Vektorraum, dann ist

$$\text{End}(V) = \{f : V \rightarrow V \text{ linear}\}$$

ein Ring, wobei  $+$  punktweise definiert wird und  $\cdot$  die Verknüpfung ist.

(4)  $\text{Mat}_{n,n}(\mathbb{Q})$  bzw.  $\mathbb{R}, \mathbb{C}, \mathbb{Z}$ .

(5) Sei  $m \geq 1$ . Dann ist  $\mathbb{Z}_m = \mathbb{Z}/Z_m$  ein Ring. Wenn dies die Übersicht erhöht können wir die Restklasse  $[a]_{\equiv \text{ mod } m}$  einer Zahl  $a$  einfach mit  $\bar{a}$ . In dieser Notation haben wir

$$\bar{a} + \bar{b} = \overline{a+b} \quad \bar{a} \cdot \bar{b} = \overline{ab}.$$

(6)  $\mathbb{Z}$ -adjungiert- $i : \mathbb{Z}[i] = \{a + ib : a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$ .

$\mathbb{Z}$ -adjungiert- $\sqrt{2} : \mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\} \subseteq \mathbb{R}$ .

$$(a + b\sqrt{2})(c + d\sqrt{2}) = ac + 2bd + (ad + bc)\sqrt{2}.$$

(7) Sei  $X$  eine Menge und  $R = \mathbb{Z}^X = \{f : X \rightarrow \mathbb{Z}\}$  mit punktweise Operationen. Dies ist ein kommutativer Ring z.B.  $C([0, 1]) = \{f : [0, 1] \rightarrow \mathbb{C} \text{ stetig}\}$ .

Antibeispiel:  $C_0(\mathbb{R}) = \{f : \mathbb{R} \rightarrow \mathbb{C} \text{ stetig und } \lim_{|x| \rightarrow \infty} f(x) = 0\}$  ist kein Ring

**Beispiel** (Ringhomomorphismen). (1)  $R = \{0\} \xrightarrow{f} \mathbb{Z}, 0 \mapsto 0, 0_R = 1_R \mapsto f(1_R) = f(0_R) = 0_{\mathbb{Z}} \neq 1_{\mathbb{Z}}$

(2)  $R \rightarrow \{0\}, a \mapsto 0$  ist ein Ringhomomorphismus.

(3)  $\mathbb{Z} \rightarrow R, n \mapsto n \cdot 1_R$  ist ein Ringhomomorphismus.

(4)  $\mathbb{Z} \rightarrow \mathbb{Q} \rightarrow \mathbb{R} \rightarrow \mathbb{C}$  da Unterringe.

(5)  $\mathbb{R} \rightarrow \text{Mat}_{n,n}(\mathbb{R}), t \mapsto tI_n$ . Umgekehrt geht nicht.

(6)  $C([0, 1] \rightarrow \mathbb{C}, f \mapsto f(x_0)$  für ein festes  $x_0 \in [0, 1]$

(7)  $\mathbb{Z} \rightarrow \mathbb{Z}_m, a \mapsto \bar{a}$

(8)  $\text{Mat}_{n,n}(\mathbb{C}) \rightarrow \text{End}(\mathbb{C}^n), A \mapsto (x \in \mathbb{C}^n \mapsto Ax)$  ist ein Ringisomorphismus.

**Lemma.** Falls in einem Ring  $R$  gilt  $0 = 1$ , dann ist  $R = \{0\}$ .

*Beweis.* Sei  $a \in R$ . Dann gilt  $a = a \cdot 1 = a \cdot 0 = 0$

□

**Lemma** (Binomialformel). Sei  $R$  ein Ring und  $a, b \in R$  mit  $ab = ba$  (z.B. weil  $R$  kommutativ ist). Dann gilt für jedes  $n \in \mathbb{N}$   $(a+b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k}$ .

*Beweis.* Die Eigenschaften von  $\binom{n}{k}$  sind bekannt, und damit funktioniert der übliche Beweis.  $\square$

Falls  $n = 2$  ist und  $(a + b)^2 = a^2 + 2ab + b^2$  gilt. Dann folgt  $ab = ba$ .

$\triangle$  **Achtung.** Ab nun werden wir nur kommutative Ringe betrachten.

## 1.2 Einheiten, Teilbarkeit, Quotientenkörper (Seite 34)

**Beispiel.** In  $\mathbb{Z}_{15}$  gilt  $\overline{3} \cdot \overline{15} = \overline{15} = \overline{0}$  aber  $\overline{3} \neq \overline{0} \neq \overline{5}$ .

**Definition.** Sei  $R$  ein Ring. Ein Element  $a \in R \setminus \{0\}$  heißt ein Nullteiler falls es ein  $b \in R \setminus \{0\}$  mit  $ab = 0$  gibt.

**Definition.** Ein kommutativer Ring heißt ein Integritätsbereich falls  $0 \neq 1$  und falls aus  $ab = ac$  und  $a \neq 0$   $b = c$  folgt (Kürzen).

**Lemma.** Sei  $R$  ein kommutativer Ring mit  $0 \neq 1$ . Dann ist  $R$  ein Integritätsbereich gdw.  $R$  keine Nullteiler besitzt.

*Beweis.* Angenommen  $R$  ist ein Integritätsbereich und  $a \in R \setminus \{0\}, b \in R$  erfüllt  $a \cdot b = 0 \Rightarrow a \cdot b = a \cdot 0 \Rightarrow b = 0$ . Also kann es keine Nullteiler geben.

Angenommen  $R$  hat keine Nullteiler und  $a, b, c \in R, a \neq 0$  erfüllen  $ab = ac \Rightarrow ab - ac = 0, a(b - c) = 0 \Rightarrow b = c$ .  $\square$

**Beispiel.** 1.  $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$   
2. Antibeispiel:  $C([0, 1])$  ist kein Integritätsbereich.  
3. Wann ist  $\mathbb{Z}_m$  ein Integritätsbereich?

**Definition.** Sei  $R$  ein kommutativer Ring und  $a, b \in R$ . Wir sagen  $a$  teilt  $b$ ,  $a|b$  [in  $R$ ] falls es ein  $c$  in  $R$  gibt mit  $b = a \cdot c$ .

**Definition.** Wir sagen  $a \in R$  ist eine *Einheit* falls  $a|1 \Leftrightarrow \exists b$  mit  $ab = 1 \Leftrightarrow \exists a^{-1} \in R$ . Einheiten mit  $R^\times = \{a \in R \mid a|1\}$

*Bemerkung.*  $R^\times$  bildet eine Gruppe,  $1 \in R^\times$ ,  $a, b \in R^\times \Rightarrow (ab)(a^{-1}b^{-1}) = aa^{-1}bb^{-1} = 1 \Rightarrow ab \in R^\times$ .

**Beispiel.** 1.  $\mathbb{C}^\times = \mathbb{C} \setminus \{0\}$   
2.  $\mathbb{Z}^\times = \{\pm 1\}$   
3.  $\mathbb{Z}[i]^\times = \{1, -1, i, -i\}$   
4.  $\mathbb{Z}[\sqrt{2}]^\times = ?$ . Auf jedenfall enthält es  $(1 + \sqrt{2})(\sqrt{2} - 1) = 1$ .

**Definition.** Ein *Körper (field)*  $K$  ist ein kommutativer Ring in dem  $0 \neq 1$  und jede Zahl ungleich Null eine multiplikative Inverse besitzt.

**Lemma.** Ein Körper ist ein Integritätsbereich.

*Beweis.* Angenommen  $a \neq 0, b, c \in R$ .

$$ab = ac \xrightarrow{a^{-1}} a^{-1}ab = a^{-1}ac \Rightarrow b = c.$$

$\square$

**Proposition.** Sei  $m \geq 1$  eine natürliche Zahl. Dann ist  $\mathbb{Z}_m$  ein Körper genau dann wenn  $m$  eine Primzahl ist.

*Beweis.* Falls  $m = 1$  ist, dann ist  $\mathbb{Z}_1 = \{\bar{0}\}$  sicher kein Körper (da  $0 \neq 1$  gelten muss). Falls  $m = ab$  mit  $a, b < m$ , dann ist  $\bar{0} = \bar{m} = \bar{a}\bar{b}$  mit  $\bar{a} \neq 0 \neq \bar{b}$ . Also hat  $\mathbb{Z}_m$  Nullteiler, ist kein Integritätsbereich und kein Körper.

Sei nun  $m$  eine Primzahl und  $\bar{a} \neq 0$ . Sei  $d = \text{ggT}(m, a)$ . Nach Definition ist  $d \geq 1$  ein Teiler von  $m$ . Falls  $d = m$  wäre, dann folgt  $m|a \Rightarrow \bar{a} = \bar{0}$   $\nmid$ . Also ist  $d = 1$ . Nach dem Lemma vom letzten Mal folgt daraus, dass es  $k, l \in \mathbb{Z}$  mit  $1 = k \cdot m + l \cdot a$ . Modulo  $m$  ist die  $\bar{1} = \bar{l} \cdot \bar{a}$ . Dies zeigt, dass  $\bar{a} \neq 0$  die multiplikative Inverse  $l$  besitzt.  $\square$

**Satz** (Quotientenkörper (S.38)). *Sei  $R$  ein Integritätsbereich. Dann gibt es einen Körper  $K$ , der  $R$  enthält und so dass  $K = \{\frac{p}{q} : p, q \in R, q \neq 0\}$ . z.B. für  $R = \mathbb{Z}$  haben wir  $K = \mathbb{Q}$ .*

*Beweis.* Wir definieren die Relation  $\sim$  auf  $X = R \times (R \setminus \{0\})$  :

$$(a, b) \sim (p, q) \Leftrightarrow aq = pb \quad [\text{in } R] \quad [\text{versteckt wollen wir } \frac{a}{b} = \frac{p}{q}].$$

Äquivalenzrelation:

- $(a, b) \sim (a, b)$  denn  $ab = ab$ .
- $(a, b) \sim (p, q) \Rightarrow (p, q) \sim (a, b)$  denn  $aq = pb$  ist  $pb = aq$ .
- $(a, b) \sim (p, q)$  und  $(p, q) \sim (m, n)$ .  $aq = pb$  und  $pn = mq$ . Multipliziere erste mit  $n$  und zweite mit  $b$ .

$$aqn = pbn = pnb = mqb \Rightarrow aqn = mqb \xrightarrow{q \neq 0} an = mb.$$

und somit  $(a, b) \sim (m, n)$ .

Wir definieren  $K = X / \sim$  und die Elemente  $0_K = [(0, 1)]_\sim$  und  $1_K = [(1, 1)]_\sim$ . und die Operationen  $+$  und  $\cdot$ :

$$\begin{aligned} [(a, b)]_\sim + [(p, q)]_\sim &= [(aq + pb, bq)]_\sim \\ [(a, b)]_\sim \cdot [(p, q)]_\sim &= [(ap, bq)]_\sim. \end{aligned}$$

Diese Operationen sind wohldefiniert (für  $+$  siehe Buch).

Angenommen  $(a, b) \sim (a', b')$ ,  $(p, q) \sim (p', q')$  somit  $ab' = a'b$  und  $pq' = p'q$ . Schließlich multipliziere beide Gleichungen  $(ap)(b'q') = (a'p')(bq)$  und somit  $(ap, bq) \sim (a'p', b'q')$ .

Wir überprüfen Schritt für Schritt die Axiome eines Körpers:

- Kommutativität der Addition:

$$[(a, b)]_\sim + [(p, q)]_\sim = [(aq + pb, bq)]_\sim = [(pq + aq, qb)]_\sim = [(p, q)]_{\text{sim}} + [(a, b)]_\sim.$$

unter Verwendung der Kommutativität der Addition und Multiplikation in  $R$ .

$K$  ist sogar ein Körper.

$$[(0, 1)]_\sim \neq [(1, 1)]_\sim \text{ da } 0 \cdot 1 \neq 1 \cdot 1 \text{ in } R$$

Falls  $[(a, b)]_\sim \neq [(0, 1)]_\sim$ , dann ist  $[(a, b)]_\sim^{-1} = [(b, a)]_\sim$ , da

$$[(a, b)]_\sim \cdot [(b, a)]_\sim = [(ab, ab)]_\sim = [(1, 1)]_\sim$$

$\square$

Ab sofort schreiben wir  $\frac{a}{b} = [(a, b)]_\sim$ . Wir identifizieren  $a \in R$  mit  $\frac{a}{1} \in K$ . Hierzu bemerken wir, dass  $\iota : a \in R \mapsto \frac{a}{1} \in K$  ein injektiver Ringhomomorphismus ist.

*Beweis.* Angenommen  $a \neq 0$ , dann gilt  $\frac{a}{1} \neq \frac{0}{1}$ . Also gilt  $\text{Ker } \iota = \{0\}$  und  $\iota$  ist injektiv.

$$\iota(1) = \frac{1}{1} = 1_K \text{ und } \iota(a+b) = \frac{a+b}{1} = \frac{a}{1} + \frac{b}{1} = \iota(a) + \iota(b) \text{ sowie } \iota(ab) = \frac{a \cdot b}{1 \cdot 1} = \iota(a)\iota(b) \quad \square$$

**Definition.** Sei  $K$  ein Körper und  $L \subseteq K$  ein Unterring der auch ein Körper ist. Dann nennen wir  $L$  auch einen *Unterkörper*.

**Beispiel.** Verwenden sie SageMath um herauszufinden für welche  $p = 2, 3, \dots, 100$  es ein  $g \in (\mathbb{Z}/p\mathbb{Z})^X$  mit

$$(\mathbb{Z}/p\mathbb{Z})^X = \{g^k : k = 0, 1, \dots\}$$

gibt ( $k < p$  genügt)?

## 1.3 Ring der Polynome (Seite 41)

Im Folgenden ist  $R$  immer ein kommutativer Ring. Wir wollen einen neuen Ring, den Ring  $R[X]$  der Polynome in der Variablen  $X$  und Koeffizienten in  $R$  definieren.

**Beispiel.** Sei  $K = \mathbb{F}_2 = \{\bar{0}, \bar{1}\} = \mathbb{Z}/2\mathbb{Z}$ . Dann soll  $X^2 + X$  *nicht* das Nullpolynom sein, obwohl die zugehörige Polynomfunktion gleich 0 ist:

$$\begin{aligned} 0 \in \mathbb{F}_2 &\mapsto 0^2 + 0 = 0 \\ 1 \in \mathbb{F}_2 &\mapsto 1^2 + 1 = 1 + 1 = 0 \end{aligned}$$

Wir verwenden die Koeffizienten um Polynome zu definieren.

**Definition.** Sei  $R$  ein kommutativer Ring. Wir definieren den *Ring der formalen Potentreihen* (in einer Variable über dem Ring  $R$ ) als

1. die Menge aller Folgen  $(a_n)_{n=0}^\infty \in R^\mathbb{N}$
2.  $0 = (0)_{n=0}^\infty, 1 = (1, 0, 0, \dots)$
3.  $+: (a_n)_{n=0}^\infty + (b_n)_{n=0}^\infty = (a_n + b_n)_{n=0}^\infty$
4.  $\cdot: (a_n)_{n=0}^\infty \cdot (b_n)_{n=0}^\infty = (c_n)_{n=0}^\infty$  wobei

$$c_n = \sum_{i=0}^n a_i b_{n-i} = \sum_{\substack{i+j=n \\ i,j \geq 0}} a_i b_j.$$

Die Menge aller Folgen mit  $a_n = 0$  für alle hinreichend großen  $n \geq 0$  wird als der *Polynomring* (in einer Variable und über  $R$ ) bezeichnet.

*Beweis.* Wir überprüfen die Axiome welche die Multiplikation betreffen und überlassen die anderen dem Leser.

1.  $a \cdot b = b \cdot a$  gilt, denn  $\sum_{i+j=n} a_i b_j = \sum_{i+j=n} b_i a_j$ .
2.  $(1 \cdot a)_n = \sum_{i+j=n} 1_i a_j = a_n$ , da  $1_i = 0$  außer wenn  $i = 0$ .
3.  $\underbrace{(ab)c}_{=d} = a(bc)$  gilt, denn

$$d_n = \sum_{i+j=n} \underbrace{(ab)_i}_{=\sum_{k+l=i} a_k b_l} c_j = \sum_{i+j=n} a_i b_j c_k \quad c_i = \sum_{i+j+k=n} a_i b_j c_k$$

ohne Klammern wegen Assoziativität von  $\cdot$  in  $R$ . Rechts ergibt sich dieselbe Antwort.

4.

$$((a+b) \cdot c)_n = \sum_{i+j=n} \underbrace{(a+b)_i c_j}_{a_i c_j + b_i c_j} = \sum_{i+j=n} a_i c_j + \sum_{i+j=n} b_i c_j = (ac + bc)_n$$

Des Weiteren überprüfen wir, dass der Polynomring unter  $+$  und  $\cdot$  abgeschlossen ist:  
Angenommen  $a, b$  sind Polynome, so dass  $a_i = 0$  für  $i > I$  und  $b_j = 0$  für  $j > J$ . Daraus folgt

$$(a + b)_n = 0 \text{ für } n > \max(I, J) \quad (a \cdot b)_n = 0 \text{ für } n > I + J$$

denn  $(a \cdot b)_n = \sum_{i+j=n} \underbrace{a_i b_j}_{=0}$ . Falls  $a_i b_j \neq 0$  wäre, dann würde  $a_i \neq 0$  und  $b_j \neq 0$  folgen, was wiederum  $i \leq I, j \leq J$  und damit  $n = i + j \leq I + J$  impliziert.  $\square$

*Notation.* Wir führen ein neues Symbol, eine Variable, z.B.  $X$  ein und identifizieren  $X$  mit

$$X^0 = 1 = (1, 0, 0, \dots) \quad X^1 = (0, 1, 0, 0, \dots) \quad X^2 = (0, 0, 1, 0, \dots) \quad \dots$$

Allgemeiner: Sei  $a$  ein Polynom, dann ist

$$X \cdot a = (0, a_0, a_1, a_2, \dots)$$

denn  $(X \cdot a)_n = \sum_{i+j=n} X_i a_j = a_{n-1}$  da  $X = 0$  außer wenn  $i = 1$  ist.  $(X \cdot a)_0 = X_0 \cdot a_0 = 0$ .

Wir schreiben  $R[X] = \{\sum_{i=0}^n a_i X^i : n \in \mathbb{N}, a_0, \dots, a_n \in R\}$  ( $R$ -adjungiert- $X$ ) für den *Ring der Polynome in der Variablen  $X$*  und  $R[[X]] = \{\sum_{n=0}^{\infty} a_n X^n : a_0, a_1, \dots \in R\}$  für den *Ring der formalen Potenzreihen in der Variable  $X$*

**Definition.** Sei  $p \in R[X] \setminus \{0\}$ . Der Grad von  $p$   $\deg(p)$  ist gleich  $n \in \mathbb{N}$  falls  $p_n \neq 0$  ist und  $p_k = 0$  für  $k > n$ . In diesem Fall nennen wir  $p_n$  auch den *führenden Koeffizienten*.

Wir definieren  $\deg(0) = -\infty$ .

**Proposition.** Sei  $R$  ein Integritätsbereich. Dann ist  $R[X]$  auch ein Integritätsbereich. Des weiteren gilt für  $p, q \in R[X] \setminus \{0\}$

- $\deg(pq) = \deg(p) + \deg(q)$  und der führende Koeffizient von  $pq$  ist das Produkt der führenden Koeffizienten von  $p$  und  $q$ .
- $\deg(p + q) \leq \max(\deg(p), \deg(q))$
- Falls  $p \mid q$ , dann gilt  $\deg(p) \leq \deg(q)$ .

*Beweis.* Sei  $f = p \cdot q$ , also  $f_n = \sum_{i+j=n} p_i q_j$  für alle  $n \in \mathbb{N}$ .

- Angenommen  $n > \deg(p) + \deg(q) \Rightarrow p_i q_j = 0$  für alle  $i + j = n \Rightarrow f_n = 0$ .
- Angenommen  $n = \deg(p) + \deg(q)$ . Behauptung:  $f_n = p_{\deg(p)} q_{\deg(q)}$  (führende Koeffizienten  $\in R \setminus \{0\}$ ) da

$$f_n = \sum_{i+j=\deg(p)+\deg(q)} p_i q_j$$

Falls  $i < \deg(p)$  ist, so ist  $j > \deg(q) \Rightarrow q_j = 0$  und vice versa.

Somit ist  $f_n \neq 0$ , da  $R$  ein Integritätsbereich ist.

Diese beiden Punkte beweisen  $\deg(f) = \deg(p \cdot q) = \deg(p) + \deg(q)$  also die erste Behauptung in der Proposition.

Angenommen  $p \mid q$ , dann gibt es ein Polynom  $g$  so dass  $q = p \cdot g$  ist  $\deg(q) = \deg(p) + \underbrace{\deg(g)}_{\geq 0} \geq$

$\deg(p)$ . Beweise die dritte Aussage in der Proposition.

Angenommen  $p = \sum_{n=0}^{\deg(p)} p_n X^n, q = \sum_{n=0}^{\deg(q)} q_n X^n$ , dann ist

$$p + q = \sum_{n=0}^{\max(\deg(p), \deg(q))} (p_n + q_n) X^n.$$

Daraus folgt  $\deg(p + q) \leq \max(\deg(p), \deg(q))$ .  $\square$

**Definition.** Sei  $K$  ein Körper. Dann wird der Quotientenkörper von  $K[X]$  als der *Körper der rationalen Funktionen*  $K(X) = \{\frac{f}{g} : f, g \in K[x], g \neq 0\}$  bezeichnet.

Wenn wir obige Konstruktion (des Polynomrings) iterieren, erhalten wir den Ring der Polynome in mehreren Variablen

$$R[X_1, X_2, \dots, X_d] := (R[X_1])[X_2][X_3] \dots [X_d].$$

Falls  $R = K$  ein Körper ist, definieren wir auch

$$K(X_1, X_2, \dots, X_d) = \text{Quot}(K[X_1, \dots, X_d]).$$

*Bemerkung.* Auf  $R[X_1, \dots, X_d]$  gibt es mehrere Grad-Funktionen

$$\begin{aligned} \deg(x_1), \deg(x_2), \dots, \deg(x_d) \\ \deg_{\text{total}}(f) = \max\{m_1 + \dots + m_d \mid f_{m_1, \dots, m_d} \neq 0\} \end{aligned}$$

für  $f = \sum_{m_1, \dots, m_d} f_{m_1, \dots, m_d} X_1^{m_1} \dots X_d^{m_d}$ . z.B.

$$\deg_{\text{total}}(1 + X_1^3 + X_2 X_3) = 3 \quad \deg_{X_2}(1 + X_1^3 + X_2 X_3) = 1.$$

**Satz.** Seien  $R, S$  zwei kommutative Ringe. Ein Ringhomomorphismus  $\Phi$  von  $R[x]$  nach  $S$  ist eindeutig durch seine Einschränkung  $\varphi = \Phi|_R$  und durch das Element  $x = \Phi(X) \in S$  bestimmt. Des weiteren definiert

$$\Phi\left(\sum_{n=0}^{\infty} a_n X^n\right) = \sum_{n=0}^{\infty} \phi(a_n) x^n \quad (*)$$

einen Ringhomomorphismus falls  $\varphi : R \rightarrow S$  ein Ringhomomorphismus ist und  $x \in S$  beliebig ist.

*Beweis.* Sei  $\Phi : R[X] \rightarrow S$  ein Ringhomomorphismus,  $\varphi = \Phi|_R, x = \Phi(X) \in S$ . Dann gilt

$$\Phi\left(\sum_{n=0}^{\infty} a_n X^n\right) = \sum_{n=0}^{\infty} \Phi(a_n X^n) = \sum_{n=0}^{\infty} \varphi(a_n) x^n$$

wie im Satz behauptet. Dies zeigt bereits den ersten Teil des Satzes, da die rechte Seite der Formel nur  $\varphi$  und  $x = \Phi(X)$  benötigt.

Sei nun  $\varphi : R \rightarrow S$  ein Ringhomomorphismus und  $x \in S$  beliebig. Wir verwenden  $(*)$  um  $\Phi$  zu definieren  $\Phi : R[X] \rightarrow S$  ist nun definiert.

- $\Phi(1) = \phi(1_R) \underbrace{x^0}_{=1_S} = 1_S.$
- 

$$\begin{aligned} \Phi(a+b) &= \Phi\left(\sum_{n=0}^{\infty} (a_n + b_n) X^n\right) = \sum_{n=0}^{\infty} \varphi(a_n + b_n) x^n \\ &= \sum_{n=0}^{\infty} \varphi(a_n) x^n + \sum_{n=0}^{\infty} \varphi(b_n) x^n = \Phi(a) + \Phi(b) \end{aligned}$$



•

$$\begin{aligned}\Phi(a \cdot b) &= \Phi\left(\sum_{n=0}^{\infty} \left(\sum_{i+j=n} a_i b_j\right) X^n\right) = \sum_{n=0}^{\infty} \underbrace{\varphi\left(\sum_{i+j=n} a_i b_j\right)}_{\sum_{i+j=n} \varphi(a_i) \varphi(b_j)} X^n \\ &= \sum_{i,j} \varphi(a_i) \varphi(b_j) x^{i+j} = \left(\sum_i \varphi(a_i) x^i\right) \left(\sum_j \varphi(b_j) x^j\right) = \Phi(a) \Phi(b).\end{aligned}$$

Also ist  $\Phi$  in der Tat ein Ringhomomorphismus von  $R[X]$  nach  $S$ . □

*Notation.* Wir schreiben für zwei kommutative Ringe  $R, S$

$$\text{Hom}_{\text{Ring}}(R, S = \{\varphi : R \rightarrow S \mid \varphi \text{ ist ein Ringhomomorphismus}\})$$

in dieser Notation können wir obigen Satz in der Form

$$\text{Hom}_{\text{Ring}}(R[X], S) \cong \text{Hom}_{\text{Ring}}(R, S) \times S$$

schreiben. Dies kann iteriert werden:

$$\text{Hom}_{\text{Ring}}(R[x_1, \dots, x_d], S) \cong \text{Hom}_{\text{Ring}}(R, S) \times \underbrace{S \times \dots \times S}_{d\text{-mal}}.$$

**Beispiel.** Falls wir  $R = S$  und  $\varphi = \text{id}$  setzen, so erhalten wir für jedes  $a \in R$  die entsprechende Auswertungsabbildung

$$\text{ev}_a : f \mapsto f(a) = \sum_{n=0}^{\infty} f_n a^n.$$

Wenn wir  $a \in R$  variieren, ergibt sich auch eine Abbildung

$$\Psi : f \in R[X] \rightarrow \left( f(\cdot) : \begin{cases} R \rightarrow R \\ a \mapsto f(a) \end{cases} \right) \in R^R.$$

Wir statten  $R^R$  mit den punktweise Operationen aus, womit  $\Psi : R[X] \rightarrow R^R$  ein Ringhomomorphismus ist.

Falls  $|R| < \infty$  und  $R \neq \{0\}$ , so kann  $\Psi$  nicht injektiv sein.

**Beispiel.** Sei  $R = \mathbb{Z}$  und  $S = \mathbb{Z}/m\mathbb{Z}[X]$  für ein  $m \geq 1$ . Dann gibt es einen Ringhomomorphismus

$$f \in \mathbb{Z}[X] \mapsto \bar{f} = \sum_{n=0}^{\infty} (f_n \bmod m) X^n \in \mathbb{Z}/m\mathbb{Z}[X^n].$$

Hier ist  $\varphi : \mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}, a \mapsto a \bmod m$ .

**Beispiel.**  $R = \mathbb{C}, S = \mathbb{C}[X], \varphi(a) = \bar{a}, a \in \mathbb{C}$ .

$$f \in \mathbb{C}[X] \mapsto \sum_{n=0}^{\infty} \bar{f}_n X^n \in \mathbb{C}[X].$$

ist sogar ein Ringautomorphismus.

## 1.4 Ideale und Faktorringer

**Definition.** Sei  $R$  ein kommutativer Ring. Ein Ideal in  $R$  ist eine Teilmenge  $I \subseteq R$  so dass

- (i)  $0 \in I$
- (ii)  $a, b \in I \Rightarrow a + b \in I$
- (iii)  $a \in I, x \in R \Rightarrow xa \in I$

**Beispiel.** Seien  $R, S$  zwei kommutative Ringe und  $\varphi : R \rightarrow S$  ein Ringhomomorphismus. Dann ist

$$\text{Ker}(\varphi) = \{a \in R \mid \varphi(a) = 0\}$$

ein Ideal.

Beweis von (iii): Falls  $a \in \text{Ker}(\varphi), x \in R$  dann gilt  $\varphi(xa) = \varphi(x) \underbrace{\varphi(a)}_{=0} = 0 \Rightarrow xa \in \text{Ker}(\varphi)$ .

**Satz.** Sei  $R$  ein kommutativer Ring und  $I \subseteq R$  ein Ideal.

1. Die Relation  $a \sim b \Leftrightarrow a - b \in I$  ist eine Äquivalenzrelation auf  $R$ . Wir schreiben auch  $a \equiv b \pmod I$  für die Äquivalenzrelation und  $R/I$  für den Quotienten, den wir Faktoring nennen wollen.
2. Die Addition, Multiplikation, das Negative induzieren wohldefinierte Abbildungen

$$R/I \times R/I \rightarrow R/I \quad \text{bzw.} \quad R/I \rightarrow R/I.$$

3. Mit diesen Abbildungen,  $0_{R/I} = [0]_{\sim}, 1_{R/I} = [1]_{\sim}$  ist  $R/I$  ein Ring und die kanonische Projektion  $p : R \rightarrow R/I$  mit  $a \in R \mapsto [a]_{\sim} = a + I$  ist ein surjektiver Ringhomomorphismus.

*Beweis.* 1) :

1.  $a \sim a$  dann  $a - a = 0 \in I$ .
2.  $a \sim b \Rightarrow b \sim a$  denn  $b - a = \underbrace{(-1)}_{\in R} \underbrace{(a - b)}_{\in I} \in I$
3.  $a \sim b$  und  $b \sim c \Rightarrow a \sim c$  denn  $a - c = \underbrace{(a - b)}_{\in I} + \underbrace{(b - c)}_{\in I} \in I$

Also ist  $\sim$  eine Äquivalenzrelation und wir können den Quotienten  $R/\sim = R/I$  betrachten.

2) : Wir zeigen, dann  $+: R/I \times R/I \rightarrow R/I$  wohldefiniert ist:

$$[a]_{\sim} + [b]_{\sim} = [a + b]_{\sim}$$

über die Identifikation  $[a]_{\sim} \rightsquigarrow a, [b]_{\sim} \rightsquigarrow b$  und  $(a, b) \mapsto a + b \mapsto [a + b]_{\sim}$ .

Also müssen wir zeigen:  $a \sim a', b \sim b' \Rightarrow a + b \sim a' + b'$ . Dies gilt da  $a - a' \in I, b - b' \in I \Rightarrow (a + b) - (a' + b') \in I$  wegen Eigenschaft (ii) von Idealen.

Angenommen  $a \sim a', b \sim b' \Rightarrow ab \sim a'b'$ .

$$ab - a'b' = ab - a'b + a'b - a'b' = b \underbrace{(a - a')}_{\in I} + a' \underbrace{(b - b')}_{\in I} \in I.$$

wegen (iii) in der Def von Idealen Dies zeigt, dass die Multiplikation von Restklassen

$$[a]_{\sim} \cdot [b]_{\sim} = [a \cdot b]_{\sim}$$

wohldefiniert ist. Der Beweis für  $-a$  ist analog, oder ergibt sich aus der Multiplikation mit  $[-1]_{\sim}$ . Dies beweist 2).

3): Da die Ringaxiome nur Gleichungen enthalten, sind die Ringaxiome in  $R/I$  direkte Konsequenzen der Ringaxiome in  $R$ : z.B. Kommutativität von  $+$  in  $R/I$

$$[a] + [b] = [a + b] = [b + a] = [b] + [a]$$

wobei das zweite Gleich wegen der Kommutativität in  $R$  gilt.

Alle anderen Axiome folgen auf dieselbe Weise. Des Weiteren gilt für die Projektion  $p : R \rightarrow R/I, a \mapsto [a]_\sim$

$$\begin{aligned} p(0) &= [0]_\sim, p(1) = [1]_\sim \\ p(a + b) &= [a + b]_\sim = [a]_\sim + [b]_\sim = p(a) + p(b) \\ p(a \cdot b) &= [a \cdot b]_\sim = [a]_\sim \cdot [b]_\sim = p(a) \cdot p(b) \end{aligned}$$

Also ist  $p : R \rightarrow R/I$  ein Ringhomomorphismus. □

**Beispiel.** •  $I = \mathbb{Z}_m \subseteq \mathbb{Z}$  ist ein Ideal

•  $I = R, I = \{0\}$  (Nullideal) sind Ideale in einem beliebigen kommutativen Ring.

**Lemma.** Sei  $I \subseteq R$  ein Ideal in einem kommutativen Ring. Dann gilt

$$I = R \Leftrightarrow 1 \in I \Leftrightarrow I \cap R^X \neq \emptyset.$$

*Beweis.* „ $\Leftarrow$ “: Angenommen  $u = v^{-1} \in I$  und  $v \in R, a \in R$ . Dann gilt

$$a = a \cdot \underbrace{v \cdot u}_{=1} \in I.$$

Da  $a \in R$  beliebig war folgt also  $I = R$ . □

**Beispiel.** Welche Ideale gibt es in einem Körper? Nur  $\{0\}$  und  $K$ . Da jede andere Teilmenge von  $K$  eine Einheit besitzt (Lemma).

**Definition.** Sei  $R$  ein kommutativer Ring und seien  $a_1, \dots, a_n \in R$ . Dann wird

$$I = (a_1, \dots, a_n) = \{x_1 a_1 + x_2 a_2 + \dots + x_n a_n : x_1, \dots, x_n \in R\}$$

das von  $a_1, \dots, a_n$  erzeugte Ideal genannt.

Für  $a \in I$  wird  $I = (a) = Ra$  das von  $a$  erzeugte Hauptideal genannt.

**Lemma.** Sei  $R$  ein kommutativer Ring.

1)  $(a) \subseteq (b) \Leftrightarrow b \mid a$

2) Falls  $R$  ein Integritätsbereich ist, dann gilt  $(a) = (b) \Leftrightarrow \exists u \in R^X$  mit  $b = ua$

*Beweis.* Angenommen  $(a) \subseteq (b)$  wie in 1). Da  $a = 1 \cdot a \in (a)$  folgt  $a \in (b) = Rb$ . Also gilt  $a = x \cdot b$  für ein  $x \in R$ , also  $b \mid a$ .

Falls umgekehrt  $b \mid a$ , dann ist  $a \in (b) \Rightarrow (a) = Ra \subseteq (b)$ .

Die Implikation  $\Leftarrow$  in 2) folgt aus 1). Also nehmen wir nun an, dass  $(a) = (b)$ . Dies impliziert  $a = xb$  und  $b = ya$  für  $x, y \in R$ . Daraus folgt  $a = xb = xya$ .

Falls  $a = 0$  ist, so ist auch  $b = 0$  und wir setzen  $u = 1$ .

Falls  $a \neq 0$ , so können wir kürzen und erhalten  $1 = xy$  also  $x, y \in R^X$  und wir setzen  $u = y$ . □

**Beispiel.** Sei  $R = C_{\mathbb{R}}([0, 3])$ .

$$a = \begin{cases} -x + 1 & \text{für } x \in [0, 1] \\ 0 & \text{für } x \in (1, 2) \\ x - 2 & \text{für } x \in [2, 3] \end{cases} \quad b = \begin{cases} x - 1 & \text{für } x \in [0, 1] \\ 0 & \text{für } x \in (1, 2) \\ x - 2 & \text{für } x \in [2, 3] \end{cases}.$$

Behauptung:  $(a) = (b)$  aber  $b \notin R^X a$ . Es gilt  $a \in (b)$ , denn  $a = b \cdot f$  und  $b = a \cdot f$  für

$$f = \begin{cases} -1 & \text{für } x \in [0, 1] \\ 2x - 3 & \text{für } x \in (1, 2) \\ 1 & \text{für } x \in [2, 3] \end{cases}$$

$b \notin R^X a$  folgt aus dem Zwischenwertsatz.

Falls  $I \subseteq R$  ein Ideal ist und  $a \in R$ , dann ist die Restklasse für Äquivalent modulo  $I$  gleich

$$[a]_N = \{x \in R : x \sim a\} = a + I.$$

**Satz** (Erster Isomorphiesatz). Angenommen  $R, S$  sind kommutative Ringe und  $\varphi : R \rightarrow S$  ist ein Ringhomomorphismus.

1. Dann induziert  $\varphi$  einen Ringisomorphismus

$$\bar{\varphi} : R/\text{Ker}(\varphi) \rightarrow \text{Im}(\varphi) = \varphi(R) \subseteq S$$

so dass  $\varphi = \bar{\varphi} \circ p$  wobei  $p : R \rightarrow R/\text{Ker}(\varphi)$  die kanonische Projektion ist (Diagramm links).

2. Sei  $I \subseteq \text{Ker}(\varphi)$  ein Ideal in  $R$ . Dann induziert  $\varphi$  einen Ringhomomorphismus  $\bar{\varphi} : R/I \rightarrow S$  mit  $\varphi = \bar{\varphi} \circ p_I$  (Diagramm rechts). Des weiteren gilt  $\text{Ker}(\bar{\varphi}) = \text{Ker}(\varphi)/I$  und  $\text{Im}(\bar{\varphi}) = \text{Im}(\varphi)$

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & S \\ \downarrow p & \nearrow \bar{\varphi} & \\ R/\text{Ker}(\varphi) & & \end{array} \quad \begin{array}{ccc} R & \xrightarrow{\varphi} & S \\ \downarrow p_I & \nearrow \bar{\varphi} & \\ R/I & & \end{array}$$

*Beweis.* Wir beginnen mit 2) und definieren  $\bar{\varphi}(x+I) = \varphi(x)$ . Dies ist wohldefiniert: Falls  $x+I = y+I$  ist, so ist  $x-y \in I \subseteq \text{Ker}(\varphi)$ . Daher gilt  $\varphi(x) - \varphi(y) = \varphi(x-y) = 0$ .

Da  $\varphi$  ein Ringhomomorphismus ist, gilt

$$\varphi(1_R) = 1_S \Rightarrow \bar{\varphi}(1+I) = 1_S$$

$$\varphi(x+y) = \varphi(x) + \varphi(y) \Rightarrow \bar{\varphi}(x+I + y+I) = \varphi(x+I) + \varphi(y+I)$$

$$\varphi(xy) = \varphi(x)\varphi(y) \Rightarrow \bar{\varphi}((x+I)(y+I)) = \bar{\varphi}(xy+I) = \varphi(xy) = \varphi(x)\varphi(y) = \bar{\varphi}(x+I)\bar{\varphi}(y+I)$$

$\varphi = \bar{\varphi} \circ p_I$  denn für  $x \in R$  gilt  $p_I(x) = x+I$ ,  $\bar{\varphi} \circ p_I(x) = \bar{\varphi}(x+I) = \varphi(x)$  nach Definition von  $\bar{\varphi}$ . Da dies für alle  $x \in R$  gilt ergibt sich obiges und das kommutative Diagramm.

$$\text{Ker}(\bar{\varphi}) = \{x+I : \underbrace{\varphi(x)}_{\bar{\varphi}(x+I)} = 0\} = \text{Ker}(\varphi/I)$$

$$\text{Im}(\bar{\varphi}) = \{\bar{\varphi}(x) : x \in R/I\} = \{\varphi(x) : x \in R\} = \text{Im}(\varphi)$$

Dies beweist 2) vom Satz.

Wir wollen nun 1) beweisen und wenden 2) für  $I = \text{Ker}(\varphi)$  an. Also ist  $\bar{\varphi}(x + \text{Ker}(\varphi)) = \varphi(x)$  für  $x + \text{Ker}(\varphi) \in R/\text{Ker}(\varphi)$  ein Ringhomomorphismus mit Bild  $\text{Im}(\varphi)$ .

Hier gilt  $\text{Ker}(\bar{\varphi}) = \text{Ker}(\varphi)/\text{Ker}(\varphi) = \{0 + \text{Ker}(\varphi)\}$ , also ist  $\bar{\varphi}$  injektiv. Daher ist  $\bar{\varphi}$  ein Ringhomomorphismus von  $R/\text{Ker}(\varphi)$  nach  $\text{Im}(\varphi)$  wie in 1) behauptet.  $\square$

*Bemerkung.* Sei  $I_0 \subseteq R$  ein Ideal in einem kommutativen Ring. Dann gibt es eine Korrespondenz (kanonische Bijektion) zwischen Idealen in  $R/I_0$  und Idealen in  $R$ , die  $I_0$  enthalten.

$$\begin{aligned} I \subseteq R, I_0 \subseteq I &\mapsto I/I_0 = \{x + I_0 : x \in I\} \subseteq R/I_0 \\ J \subseteq R/I_0 &\mapsto p_{I_0}^{-1}(J) \subseteq R \quad (p_{I_0} : \begin{cases} R \rightarrow R/I_0 \\ x \mapsto x + I_0 \end{cases}). \end{aligned}$$

**Definition.** Wir sagen zwei Ideale  $I, J$  in einem kommutativen Ring sind *coprim*, falls  $I + J = R$  ist. D.h.  $\exists a \in I, b \in J$  mit  $1 = a + b$ .

**Beispiel.**  $I = (p)$  und  $J = (q) \subseteq \mathbb{Z} = R$  falls  $p, q$  verschiedene (positive) Primzahlen sind.

**Proposition** (Chinesischer Restsatz). *Sei  $R$  ein kommutativer Ring und seien  $I_1, \dots, I_n$  paarweise coprime Ideale. Dann ist der Ringhomomorphismus  $\varphi : R \rightarrow R/I_1 \times \dots \times R/I_n$  mit  $x \mapsto (x + I_1, \dots, x + I_n)$  surjektiv mit  $\text{Ker}(\varphi) = I_1 \cap \dots \cap I_n$ .*

*Dies induziert einen Ringisomorphismus  $R/I_1 \cap \dots \cap I_n \rightarrow R/I_1 \times \dots \times R/I_n$ .*

*Beweis.* Dass der Kern  $\text{Ker}(\varphi)$  genau  $I_1 \cap \dots \cap I_n$  ist, ergibt sich aus den Definitionen. Wir zeigen, dass  $\varphi$  surjektiv ist. Hierfür wollen wir für jedes  $i \in \{1, \dots, n\}$  ein  $x_i \in R$  finden so dass

$$\varphi(x_i) = (0 + I_1, \dots, \underbrace{1 + I_i}_{i\text{-te Stelle}}, \dots, 0 + I_n).$$

Zur Vereinfachung der Notation betrachten wir den Fall  $i = 1$ .

**Behauptung:**  $I_1$  und  $I_2 \cap \dots \cap I_n$  sind coprime, d.h. es existieren  $a \in I_1$  und  $b \in I_2 \cap \dots \cap I_n$  so dass  $a + b = 1$ .

Aus der Behauptung folgt, dass  $x_1 = b$  erfüllt:

$$\varphi(x_1) = (b + I_1, b + I_2, \dots, b + I_n) = (1 + I_1, 0 + I_2, \dots, 0 + I_n)$$

wegen der Definition von  $b$  und  $a + b = 1$ .

Wir zeigen die Behauptung mittels Induktion nach  $n$ :

$n = 2$ :  $I_1$  und  $I_2$  sind coprime. Dies gilt nach Annahme in der Proposition.

Induktionsschritt ( $n - 1 \rightarrow n$ ): Wir nehmen an, dass  $I_1$  und  $I_2 \cap \dots \cap I_{n-1}$  coprime sind, d.h. es gibt  $a \in I_1, b \in I_2 \cap \dots \cap I_{n-1}$  mit  $a + b = 1$ . Des weiteren ist  $I_1$  coprime zu  $I_n$ , d.h. es gibt  $c \in I_1, d \in I_n$  mit  $c + d = 1$ .

$$\Rightarrow a + b(\underbrace{c + d}_{=1}) = 1 \Rightarrow \underbrace{a + bc}_{\in I_1} + \underbrace{bd}_{\in I_2 \cap \dots \cap I_{n-1} \cap I_n} = 1.$$

Folgt  $I_1$  ist coprime zu  $I_2 \cap \dots \cap I_n$ , Also haben wir die Behauptung mittels Induktion gezeigt.

Wir können  $x_1, \dots, x_n$  wie oben verwenden um die Surjektivität zu zeigen: Sei  $(a_1 + I_1, \dots, a_n + I_n) \in R/I_1 \times \dots \times R/I_n$  beliebig. Dann gilt

$$\varphi(a_1 x_1 + \dots + a_n x_n) = (a_1 x_1 + \dots + a_n x_n + I_1, \dots, a_1 x_1 + \dots + a_n x_n + I_n) = (a_1 + I_1, a_2 + I_2, \dots, a_n + I_n).$$

da  $x_i$  modulo  $I_i$  gleich 1 ist und ansonsten  $x_i \in I_j$  ( $j \neq i$ ) gilt und daher  $x_i$  modulo  $I_j$  gleich 0 ist.  $\square$

## 1.5 Charakteristik eines Körpers

Sei  $K$  ein Körper. Dann gibt es einen Ringhomomorphismus  $\varphi : \mathbb{Z} \rightarrow K$  mit

$$\begin{cases} n \in \mathbb{N} \mapsto \underbrace{1 + \dots + 1}_{n\text{-mal}} \\ -n \in \mathbb{N} \mapsto -\underbrace{(1 + \dots + 1)}_{n\text{-mal}} \end{cases}$$

Sei  $I = \text{Ker}(\varphi)$  so, dass  $\mathbb{Z}/I \equiv \text{Im}(\varphi) \subseteq K$ . Da  $K$  ein Körper ist, ist  $\text{Im}(\varphi)$  ein Integritätsbereich.

**Lemma.** Sei  $I \subseteq \mathbb{Z}$  ein Ideal. Dann gilt  $I = (m)$  für ein  $m \in \mathbb{N}$ . Der Quotient ist ein Integritätsbereich genau dann wenn  $m = 0$  oder  $m$  eine Primzahl ist.

*Beweis.* Falls  $I \cap \mathbb{N}_{>0} = \{\}$  ist, so ist  $I = (0)$ . Ansonsten können wir das kleinste Element  $m$  in  $I \cap \mathbb{N}_{>0}$  finden. Falls  $n \in I$  ist, so können wir Division mit Rest anwenden und erhalten  $\underbrace{n}_{\in I} = \underbrace{k \cdot m}_{\in I} + r$  für  $k \in \mathbb{Z}, r \in \{0, \dots, m-1\}$ . Folgt  $r \in I \Rightarrow r = 0$  da  $m$  das kleinste Element von  $I \cap \mathbb{N}_{>0}$  war. Da  $n \in I$  beliebig war, folgt  $I = (m)$ .

Falls  $m = a \cdot b$  für  $a, b < m$  ist, so ist  $\mathbb{Z}/(m)$  kein Integritätsbereich, da  $(a + (m))(b + (m)) = ab + (m) = 0 + (m)$  ist. Falls  $m > 0$  eine Primzahl ist, so ist  $\mathbb{Z}/(m)$  ein Körper und damit auch ein Integritätsbereich.  $\square$

**Definition.** Sei  $K$  ein Körper. Wir sagen, dass  $K$  Charakteristik 0 hat, falls  $\varphi : \mathbb{Z} \rightarrow K$  injektiv ist. Wir sagen, dass  $K$  Charakteristik  $p \in \mathbb{N}_{>0}$  hat falls  $\varphi : \mathbb{Z} \rightarrow K$  den Kern  $(p)$  hat.

**Beispiel.** Charakteristik 0:  $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \dots$  Wenn  $K$  Charakteristik 0 hat, dann enthält  $K$  eine isomorphe Kopie von  $\mathbb{Q}$ .

Charakteristik  $p : \mathbb{F}_p = \mathbb{Z}/(p), \mathbb{F}_p(X)$

**Proposition.** Sei  $K$  ein Körper mit Charakteristik  $p > 0$ . Dann ist die Frobeniusabbildung  $F : x \in K \rightarrow x^p \in K$  ein Ringhomomorphismus. Falls  $|K| < \infty$ , dann ist  $F$  ein Ringautomorphismus.

*Beweis.* Es gilt  $F(0) = 0^p, F(1) = 1^p = 1, F(xy) = (xy)^p = x^p y^p = F(x)F(y)$ . Wir müssen noch  $F(x+y) = F(x) + F(y)$  zeigen.

$$(x+y)^p = x^p + \underbrace{\binom{p}{1}}_{=p \cdot 1_K = 0} x^{p-1}y + \binom{p}{2} x^{p-2}y^2 + \dots + \binom{p}{p-1} xy^{p-1} + y^p = x^p + y^p \quad [\text{in } K].$$

**Behauptung:** Für  $0 < k < p$  gilt  $p \mid \binom{p}{k}$

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} = \frac{p(p-1)\dots(p-k+1)}{k!} \Rightarrow k! \binom{p}{k} = p(p-1)\dots(p-k+1) = 0 \mod p.$$

aber  $k! \mod p \neq 0$ . Da Rechnen modulo  $p$  einen Körper definiert, erhalten wir  $k! \not\equiv 0, k! \binom{p}{k} \equiv 0 \mod p \Rightarrow \binom{p}{k} \equiv 0 \mod p$ . Folgt  $p \mid \binom{p}{k}$ .

Wenn  $|K| < \infty$ , dann ist  $F$  auch surjektiv! Warum:  $\text{Ker}(f) \subseteq K$  ist ein Ideal  $\Rightarrow \text{Ker}(F) = \{0\}$  und  $F$  ist injektiv. Wenn  $|K| < \infty$ , folgt aus der Injektivität auch die Surjektivität.  $\square$

## 1.6 Primideale und Maximalideale

**Definition.** Sei  $R$  ein kommutativer Ring, und sei  $I \subseteq R$  ein Ideal. Wir sagen  $I$  ist ein *Primideal*, falls  $R/I$  ein Integritätsbereich ist. Wir sagen  $I$  ist ein *Maximalideal*, falls  $R/I$  ein Körper ist.

**Proposition.** Sei  $I \subseteq R$  ein Ideal in einem kommutativen Ring.

- 1) Dann ist  $I$  ein Primideal genau dann wenn  $I \neq R$  und für alle  $a, b \in R$  gilt  $ab \in I \Rightarrow a \in I$  oder  $b \in I$ .
- 2) Dann ist  $I$  ein Maximalideal genau dann wenn  $I \neq R$  und es gibt kein Ideal  $J$  mit  $I \subsetneq J \subsetneq R$ .

*Beweis.* 1)  $I$  ist ein Primideal  $\Leftrightarrow R/I \neq \{0 + I\}$  und  $([a][b] = 0 \Rightarrow [a] = 0 \text{ oder } [b] = 0 \Leftrightarrow I \neq R \text{ und } (ab \in I \Rightarrow a \in I \text{ oder } b \in I)$ .

- 2)  $I$  ist ein Maximalideal  $\Leftrightarrow R/I$  ist ein Körper  $\Leftrightarrow I \neq R$  und es gibt kein Ideal  $J \subseteq R$  mit  $I \subsetneq J \subsetneq R$ .

Letztes „genau dann wenn“:  $\Rightarrow$ : Sei  $J \subseteq R$  ein Ideal und  $I \subsetneq J$  und  $x \in J \setminus I$ . Dann ist  $x + I \in R/I \setminus \{0 + I\}$  ist invertierbar in  $R/I$ , also  $(x + I)^{-1} = y + I$ . Daraus folgt  $\underbrace{x}_{\in J} y - 1 \in I \subseteq J \Rightarrow 1 \in J$ ,

also  $J = R$ .

$\Leftarrow$ : Angenommen  $x + I \neq 0 + I$ , dann können wir  $J = (x) + I$  definieren. Dies ist ein Ideal  $I \subsetneq J \subseteq R$ . Also ist  $J = R$  und es gibt ein  $y \in R$  mit  $xy + I = 1 + I$   $\square$

**Beispiel.** In  $R = \mathbb{Z}$  gilt:

- $I = (m)$  ist ein Primideal  $\Leftrightarrow m = 0$  oder  $m = \pm p$  eine Primzahl ist.
- $I = (m)$  ist ein Maximalideal  $\Leftrightarrow m = \pm p$  eine Primzahl ist.

z.B.  $(0) \leq (2)$  mit  $(0)$  Primideal und  $(2)$  Prim- und Maximalideal.

**Beispiel.** Sei  $K$  ein Körper und  $a_1, \dots, a_n \in K$ . Wir definieren das Ideal

$$I = (X_1 - a_1, \dots, X_n - a_n) \subseteq K[X_1, \dots, X_n]$$

Dann ist  $I$  ein Maximalideal, und ist gleich dem Kern  $\text{Ker}(\text{ev}_{a_1, \dots, a_n})$  des Auswertungshomomorphismus

$$\text{ev}_{a_1, \dots, a_n}(f) = f(a_1, \dots, a_n).$$

*Beweis.*  $I \subseteq \text{Ker}(\text{ev}_{a_1, \dots, a_n})$  da  $\text{ev}(X_j - a_j) = a_j - a_j = 0$  für  $j = 1, \dots, n$ . Sei nun  $f \in \text{Ker}(\text{ev}_{a_1, \dots, a_n})$ .

$$f = \sum a_{(k_1, \dots, k_n)} X_1^{k_1} \dots X_n^{k_n}$$

Wir schreiben  $X_j^{k_j} = (a_j + X_j - a_j)^{k_j} = a_j^{k_j} + \underbrace{k_j a_j^{k_j-1} (X_j - a_j) + \dots}_{\in I}$

Also gilt  $X_j^{k_j} + I = a_j^{k_j} + I$

$$\Rightarrow f + I = \sum \underbrace{a_{(k_1, \dots, k_n)} a_1^{k_1} \dots a_n^{k_n}}_{f(a_1, \dots, a_n)=0} + I \in I$$

Weiters folgt  $I = \text{Ker}(\text{ev}_{a_1, \dots, a_n})$

$$\Rightarrow K[X_1, \dots, X_n]/I = K[X_1, \dots, X_n]/\text{Ker}(\text{ev}_{a_1, \dots, a_n}) \cong K$$

ist ein Körper  $\Rightarrow I$  ist ein Maximalideal.  $\square$

*Bemerkung.* Der Hilbert'sche Nullstellensatz besagt, dass jedes Maximalideal in  $\mathbb{C}[X_1, \dots, X_n]$  von dieser Gestalt ist.

**Satz.** Sei  $R$  ein kommutativer Ring, und  $I \subsetneq R$  ein Ideal. Dann existiert ein Maximalideal  $m \supseteq I$ . Insbesondere existiert in jedem Ring  $R \neq [0]$  ein Maximalideal.

*Beweis.* Wir werden das Zornsche Lemma verwenden. Hierzu definieren wir

$$X = \{J \subsetneq R \mid J \text{ ist ein Ideal und } I \subseteq J\}$$

und betrachten die Inklusion von Teilmengen als unsere Relation auf  $X$ . Wir müssen zeigen, dass jede Kette  $K$  in  $X$  eine obere Schranke besitzt. Falls  $K = \emptyset$ , dann ist  $I \in X$  eine obere Schranke. Sei nun  $K$  eine nichtleere Kette in  $X$ .

Wir behaupten, dass  $\tilde{J} = \bigcup_{J \in K} J$  eine obere Schranke von  $K$  in  $X$  darstellt. Für jedes  $J \in K$  gilt  $J \subseteq \tilde{J}$  nach Definition von  $\tilde{J}$ . Weiters gilt:

- $\tilde{J} \neq R$  weil  $(J \in K \Rightarrow 1 \notin J)$  gilt  $1 \notin \tilde{J}$
- $\tilde{J} \supseteq I$ , weil  $K \neq \emptyset$ , also ein  $J \in K$  existiert, welches nach Definition von  $X \supseteq K$   $I$  enthalten muss.
- $\tilde{J}$  ist auch ein Ideal.
  - $0 \in \tilde{J}$  da  $0 \in I \subseteq \tilde{J}$
  - Sei  $x \in R$  und  $a \in \tilde{J}$ , dann gibt es ein  $J \in K$  mit  $a \in J$ . Dies impliziert  $xa \in J \subseteq \tilde{J}$ .
  - Sei nun  $a, b \in \tilde{J}$ , dann gibt es ein  $J_a \in K$  mit  $a \in J_a$  und  $J_b \in K$  mit  $b \in J_b$ . Da  $K$  eine Kette ist, gilt  $J_a \subseteq J_b$  oder  $J_a \supseteq J_b$  also entweder  $a, b \in J_b \Rightarrow a + b \in J_b \subseteq \tilde{J}$  oder  $a, b \in J_a \Rightarrow a + b \in J_a \subseteq \tilde{J}$ .

Somit ist  $\tilde{J}$  eine obere Schranke in  $X$ . Zusammenfassend folgt  $X$  ist induktiv geordnet, also existiert nach dem Zorn'schen Lemma ein maximales Element in  $X$ , d.h. es existiert ein Ideal  $m$ , welches  $I$  enthält, nicht gleich  $R$  ist und so sodass es zwischen  $m$  und  $R$  kein weiteres Ideal gibt.  $\square$

## 1.7 Unterring

**Definition.** Sei  $R$  ein Ring und  $S \subseteq R$  auch ein Ring. Wir sagen  $S$  ist ein *Unterring* falls  $\text{id} : S \rightarrow R, s \mapsto s$  ein Ringhomomorphismus ist.

**Alternativ Definition:** Sei  $R$  ein Ring und  $S \subseteq R$ . Dann ist  $S$  ein Unterring falls

1.  $0, 1 \in S$ .
2.  $a - b \in S$  für alle  $a, b \in S$ .
3.  $a \cdot b \in S$  für alle  $a, b \in S$ .

*Notation.* Sei  $S \subseteq R$  ein Unterring in einem Ring  $R$ . Seien  $a_1, \dots, a_n \in R$ . Wir definieren

$$S[a_1, \dots, a_n] = \bigcap_{\substack{T \subseteq R \text{ Unterring} \\ T \supseteq S \\ a_1, \dots, a_n \in T}} T.$$

genannt „s-adjungiert  $a_1, \dots, a_n$ “.

$$= \text{ev}_{a_1, \dots, a_n}(S[x_1, \dots, x_n]) = \left\{ \sum_{k_1, \dots, k_n \in M} c_{k_1, \dots, k_n} a_1^{k_1} \dots a_n^{k_n} \right\}.$$

mit  $|M| < \infty, M \subseteq \mathbb{N}^n, c_{k_1, \dots, k_n} \in S$ .

*Beweis von  $\subseteq$ .* Wir wissen aus der Serie, dass  $S[a_1, \dots, a_n]$  ein Unterring ist, der nach Definition  $S$  und  $a_1, \dots, a_n$  enthält. Auch wissen wir, dass  $\text{ev}_{a_1, \dots, a_n}(S[x_1, \dots, x_n])$  ein Unterring ist (da  $S[x_1, \dots, x_n]$  ein Ring ist und  $\text{ev}_{a_1, \dots, a_n}$  ein Ringhomomorphismus ist). Also tritt  $T = \text{ev}_{a_1, \dots, a_n}(S[x_1, \dots, x_n])$  als eine der Mengen im Durchschnitt auf und wir erhalten

$$S[a_1, \dots, a_n] \subseteq \text{ev}_{a_1, \dots, a_n}(S[x_1, \dots, x_n]).$$



□

*Beweis von  $\supseteq$ .* Wir wissen  $S[a_1, \dots, a_n]$  ist ein Unterring. Ebenso haben wir  $S$  und  $a_1, \dots, a_n$  sind in diesem Unterring enthalten. Folgt

$$\sum_{(k_1, \dots, k_n) \in M} \underbrace{c_{k_1, \dots, k_n}}_{\in S} a_1^{k_1} \dots a_n^{k_n} \subseteq S[a_1, \dots, a_n].$$

Durch variieren von  $M \subseteq \mathbb{N}^n, |M| < \infty$  und der Koeffizienten zeigt  $\supseteq$ . □

**Beispiel.** •  $\mathbb{Z}[\frac{1}{2}] = \{\frac{a}{2^n} : a \in \mathbb{Z}, n \in \mathbb{N}\} \subseteq \mathbb{Q}$ .

- $\mathbb{Z}[i] = \{a + ib : a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$ .
- $\mathbb{Z}[\sqrt{2}] = \{a + \sqrt{2}b : a, b \in \mathbb{Z}\} \subseteq \mathbb{R}$ .
- $\mathbb{Q}[\sqrt{2}] = \{a + \sqrt{2}b : a, b \in \mathbb{Q}\} \subseteq \mathbb{R}$  ist ein Körper:

$$\frac{a + \sqrt{2}b}{\underbrace{c + \sqrt{2}d}_{\neq 0}} = \frac{ac - 2bd + \sqrt{2}(ad - bc)}{c^2 - 2d^2}$$

mit Nenner in  $\mathbb{Q}$ .

## 1.8 Matrizen

Sei  $R$  ein kommutativer Ring,  $m, n \in \mathbb{N}_{>0}$ . Dann bezeichnen wir die Menge  $\text{Mat}_{mn}(R)$  als die Menge aller  $m \times n$ -Matrizen

$$\begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix}.$$

mit Koeffizienten oder Eintragungen  $a_{11}, \dots, a_{mn} \in R$ . Für  $m = n$  definieren wir auch auf  $\text{Mat}_{mm}(R)$  auf übliche Weise die Addition und Multiplikation. Dies definiert auf  $\text{Mat}_{mm}(R)$  gemeinsam mit dem Einselement  $I_m = (\delta_{ij})_{i,j}$  eine Ringstruktur. Sobald  $m > 1$  ist, ist dieser Ring nichtkommutativ.

Die Einheiten in  $\text{Mat}_{mm}(R)$  werden auch als invertierbare Matrizen bezeichnet. Die Menge wird auch die allgemeine lineare Gruppe vom Grad  $m$  über  $R$  genannt:

$$\text{Gl}_m(R) = \text{Mat}_{mm}(R)^\times = \{A \in \text{Mat}_{mm}(R) \mid \text{es existiert ein } B \in \text{Mat}_{mm}(R) \text{ mit } AB = BA = I_n\}.$$

**Proposition (Meta).** Jede Rechenregel für Matrizen über  $\mathbb{R}$  die nur  $+, -, \cdot, 0, 1$  beinhalten, gilt auch über einem beliebigen kommutativen Ring.

**Proposition.** Sei  $R$  ein kommutativer Ring

- $\text{Mat}_{mm}(R)$  erfüllt die Ringaxiome, also z.B.  $A(BC) = (AB)C$
- $\det(AB) = \det(A)\det(B)$
- $A\tilde{A} = \tilde{A}A = \det(A)I_m$ , wobei  $\tilde{A}$  die komplementäre Matrix

$$\tilde{A} = ((-1)^{i+j} \det(A_{ji}))_{i,j}.$$

- $\text{char}_A(A) = 0$  für das charakteristische Polynom  $\text{char}_A(X) = \det(XI_m - A)$  einer Matrix  $A$ .

*Bemerkung.*  $\det(A)$ , jeder Koeffizient von  $A(BC)$ ,  $(AB)C$ ,  $A\tilde{A}$ ,  $\tilde{A}A$ ,  $\det(A)I$ ,  $\text{char}_A(X)$ ,  $\text{char}_A(A)$  hängt polynomiell von den Eintragungen von  $A, B, C$  ab, wobei die Koeffizienten in  $\mathbb{Z}$  liegen z.B.

$$\det(A) = \sum_{\sigma \in S_n} \underbrace{\text{sgn}(\sigma)}_{\in \mathbb{Z}} a_{1\sigma(1)} a_{2\sigma(2)} \cdots a_{n\sigma(n)}$$

welche Monome in den Eintragungen von  $A$  sind.

**Lemma.** Wenn ein Polynom  $f \in \mathbb{R}[X_1, \dots, X_n]$  auf ganz  $\mathbb{R}^n$  verschwindet, dann ist  $f = 0$ .

*Beweis.* Sei  $f = \sum_{k_1, \dots, k_n} c_{k_1, \dots, k_n} X_1^{k_1} \cdots X_n^{k_n}$  ein Polynom für das die zugehörige Polynomfunktion  $f : \mathbb{R}^n \rightarrow \mathbb{R}$ ,  $(a_1, \dots, a_n) \mapsto f(a_1, \dots, a_n)$  verschwindet. Dies gilt dann auch für jede partielle Ableitung von  $f$ . Sei  $(l_1, \dots, l_n) \in \mathbb{N}^n$  mit  $k_i \geq l_i$  für  $i \in \{1, \dots, n\}$ . Dann gilt

$$\begin{aligned} 0 &= \partial_{x_1}^{l_1} \cdots \partial_{x_n}^{l_n} f(0) \\ &= \sum_{k_1, \dots, k_n} c_{k_1, \dots, k_n} k_1(k_1 - 1) \cdots (k_1 - l_1 + 1) x_1^{k_1 - l_1} \cdots k_n(k_n - 1) \cdots (k_n - l_n + 1) x_n^{k_n - l_n} \\ &= c_{l_1, \dots, l_n} l_1! \cdots l_n! \end{aligned}$$

Da dies für alle  $(l_1, \dots, l_n)$  gilt, folgt  $f = 0$ . □

*Bemerkung.* Das Lemma gilt analog für jeden Körper  $K$  mit  $|K| = \infty$ .

*Beweis der Proposition.* Wir bemerken zuerst, dass

- Jede Eintragung von  $A(BC) - (AB)C$  ein Polynom mit ganzzahligen Koeffizienten in den Variablen

$$a_{11}, \dots, a_{mm}, b_{11}, \dots, b_{mm}, c_{11}, \dots, c_{mm}$$

ist.

- $\det(AB) - \det(A)\det(B)$  ein Polynom mit ganzzahligen Koeffizienten in den Variablen  $a_{11}, \dots, a_{mm}, b_{11}, \dots, b_{mm}$  ist.
- jede Eintragung von  $A\tilde{A} - (\det(A))I_m$  (oder  $\tilde{A}A - (\det(A))I_m$ ) ein Polynom mit ganzzahligen Koeffizienten in den Variablen  $a_{11}, \dots, a_{mm}$  ist.
- jede Eintragung von  $\text{char}_A(A)$  ein Polynom mit ganzzahligen Koeffizienten in den Variablen  $a_{11}, \dots, a_{mm}$  ist.

Für  $R = \mathbb{R}$  wissen wir, dass diese Polynome ausgewertet an einer beliebigen Stelle gleich Null sind. D.h. mit dem Lemma sind bereits die Polynome gleich Null. Wenn wir den Ringhomomorphismus von  $\mathbb{Z}$  nach  $R$  auf die Koeffizienten anwenden, erhalten wir wieder das Nullpolynom.  $\Rightarrow$  All diese Gleichungen gelten auch für Matrizen über  $R$ . □

# Kapitel 2: Faktorisierungen von Ringen

*Buch Seiten 83-114.* Wir wollen in diesem Kapitel Ringe mit eindeutiger Primfaktorzerlegung betrachten. Im Folgenden ist  $R$  immer ein Integritätsbereich.

**Definition** (Wiederholung).  $a \mid b \Leftrightarrow \exists c$  mit  $b = ac$  für  $a, b \in R$ .  
 $a \in R^\times$  ist eine Einheit  $\Leftrightarrow a \mid 1$ .

**Definition.** Wir sagen  $p \in R \setminus \{0\}$  ist *irreduzibel*, falls  $p \notin R^\times$  und für alle  $a, b \in R$  gilt  $p = ab \Rightarrow a \in R^\times$  oder  $b \in R^\times$ .

**Definition.** Wir sagen  $p \in R \setminus \{0\}$  ist *prim* falls  $(p)$  ein Primideal ist, in anderen Worten falls  $p \notin R^\times$  und für alle  $a, b \in R$  gilt  $p \mid ab \Rightarrow p \mid a$  oder  $p \mid b$ .

**Lemma.** Sei  $R$  ein Integritätsbereich. Dann ist jedes prim  $p \in R$  auch irreduzibel.

*Beweis.* Angenommen  $p \in R \setminus \{0\}$  ist prim und angenommen  $p = ab$  (wie in der Definition von irreduzibel). Daraus folgt  $p \mid ab \Rightarrow p \mid a$  oder  $p \mid b$ .

Angenommen  $p \mid a$ , dann ist  $a = p \cdot c$  für ein  $c \in R$ . Folgt  $p = p \cdot c \cdot b \Rightarrow 1 = c \cdot b$  weil  $R$  ein Integritätsbereich ist, also  $b, c \in R^\times$ . Des Weiteren ist auch  $p \notin R^\times$ . Also ist  $p$  irreduzibel.  $\square$

*Bemerkung.* Die Umkehrung des Lemmas stimmt im Allgemeinen nicht. Wenn sie doch stimmt, so hilft dies für die Eindeutigkeit in einer Primfaktorzerlegung. Siehe später in 3.3.

## 2.1 Euklidische Ringe

**Definition.** Ein Integritätsbereich  $R$  heißt ein *Euklidischer Ring* falls es eine gradfunktion  $N : R \setminus \{0\} \rightarrow \mathbb{N}$  gibt, so dass die beiden folgenden Eigenschaften gelten:

- *Gradungleichung:*  $N(f) \leq N(fg)$  für alle  $f, g \in R \setminus \{0\}$ .
- *Division mit Rest:* Für  $f, g \in R$  mit  $f \neq 0$  gibt es  $q, r \in R$  mit  $g = q \cdot f + r$  wobei  $r = 0$  oder  $N(r) < N(f)$  ist. Wir nennen  $r$  den *Rest* (bei Division durch  $f$ ).

**Beispiel.** 0) z.B. erfüllt jeder Körper  $K$  mit  $N(f) = 0$  für alle  $f \in K$  diese Axiome (uninteressant, da es hier nur Einheiten und keine irreduziblen oder primen Elemente gibt).

- 1) Der  $R = \mathbb{Z}$  und  $N(n) = |n|$  für  $n \in \mathbb{Z}$  (erfüllt alle Eigenschaften auf Grund bekannter Eigenschaften von  $\mathbb{Z}$ ).
- 2) Sei  $K$  ein Körper,  $R = K[x]$  und  $N(f) = \deg(f)$  für  $f \in R \setminus \{0\}$ .
- 3) Sei  $R = \mathbb{Z}[i]$  der Ring der *Gausschen ganzen Zahlen* und  $N(a + ib) = |a + ib|^2$
- 4) Sei  $R = \mathbb{Z}[\sqrt{2}]$  und  $N(a + \sqrt{2}b) = |a^2 - 2b^2|$  für  $a + \sqrt{2}b \in R$  (algebraische Zahlentheorie betrachtet solche Beispiele).

*Beweis von Beispiel 2.*

- Gradungleichung: Seien  $f, g \in K[X] \setminus \{0\}$ . Dann gilt

$$N(fg) = \deg(fg) = \deg(f) + \underbrace{\deg(g)}_{\geq 0} \geq \deg(f) = N(f).$$

- Division mit Rest: Sei  $f \neq 0, g \in R = K[X]$ . Dann gibt es  $q, r \in K[X]$  mit  $g = fq + r$  und  $\deg(r) < \deg(f)$ .

*Beweis.* Falls  $\deg(g) < \deg(f)$ , dann setzen wir  $q = 0$   $r = g$ . Wir verwenden Induktion nach  $\deg(g)$ . Obiger Fall ist unser Induktionsanfang.

Sei  $m \in \mathbb{N}$  und angenommen wir haben Division mit Rest bereits für alle Polynome mit  $\text{Grad} < m$  bewiesen. Sei  $g \in K[X]$  mit  $\text{Grad } \deg(g) = m$ . Aufgrund des Induktionsanfangs haben wir  $m \geq \deg(f) =: n$ .

Sei  $g = g_m X^m + \dots$ ,  $f = f_n X^n + \dots$ . Wir definieren

$$\tilde{g} = g - \underbrace{g_m f_n^{-1} X^{m-n} f}_{\substack{\text{hat f\u00fchrenden Koeffizient } g_m \\ \text{und auch Grad } m \text{ (wie } g)}}.$$

womit  $\deg(\tilde{g}) < \deg(g) = m$ . Auf Grund der Induktionsvoraussetzung k\u00f6nnen wir  $\tilde{q}$  und  $\tilde{r}$  finden, so dass

$$\begin{aligned}\tilde{g} &= f\tilde{q} + \tilde{r} & \deg(\tilde{r}) < \deg(f) \\ g - g_m f_n^{-1} X^{m-n} f &= f\tilde{q} + \tilde{r} \\ g &= f \underbrace{(g_m f_n^{-1} X^{m-n} + \tilde{q})}_{=q} + \underbrace{\tilde{r}}_{=r}\end{aligned}$$

Dies beendet den Induktionsschritt. □

□

**Beispiel** (Bsp f\u00fcr Polynomdivision).  $g = x^6 + x^4 + 4x^3 + 2$ ,  $f = x^2 + 5$

$$\begin{array}{rcccccccl} x^6 + & 0x^5 + & x^4 + & 3x^3 + & 0x^2 + & 0x + & 2 & : & x^2 + 5 = x^4 - 4x^2 + 3x \\ -x^6 & & -5x^4 & & & & & & \\ \hline & & -4x^4 & +4x^3 & +0x^2 & & +2 & & \\ & & -4x^4 & & +20x^2 & & & & \\ \hline & & & 4x^3 & +20x^2 & +0x & +2 & & \\ & & & -3x^3 & & -15x & & & \\ \hline & & & & 20x^2 & -15x & +2 & & \\ & & & & -20x^2 & & -100 & & \\ \hline & & & & & -15x & -98 & = r & \end{array}$$

*Beweis von Beispiel 3.*  $R = \mathbb{Z}[i]$  der Ring der Gausschen ganzen Zahlen

$$\begin{aligned}N(a + ib) &= |a + ib|^2 \text{ f\u00fcr } a + ib \in \mathbb{Q}[i] \\ &\in \mathbb{N} \text{ f\u00fcr } a + ib \in \mathbb{Z}[i]\end{aligned}$$

$$N(z \cdot w) = N(z)N(w) \text{ f\u00fcr } z, w \in \mathbb{Q}[i]$$

$$N(z) = 0 \Leftrightarrow z = 0 \text{ multiplikativ}$$

**Normungleichung:** Sei  $z, w \in \mathbb{Z}[i] \setminus \{0\}$ . Dann gilt

$$N(zw) = N(z) \underbrace{N(w)}_{\geq 1} \geq N(z).$$

**Lemma.** Die Division mit Rest gilt in  $\mathbb{Z}[i]$ .

*Beweis.* Seien  $f, g \in \mathbb{Z}[i]$ ,  $f \neq 0$ . Wir definieren  $z = \frac{g}{f} \in \mathbb{Q}[i]$ ,  $z = a + ib$  f\u00fcr  $a, b \in \mathbb{Q}$ . Sei  $[r] =$

die beste Näherung von  $r \in \mathbb{Q}$  innerhalb von  $\mathbb{Z}$ . Definiere  $q = [a] + i[b] \in \mathbb{Z}[i]$ . Dann gilt

$$|z - q| \leq \sqrt{\underbrace{(a - [a])^2}_{\leq \frac{1}{2}} + \underbrace{(b - [b])^2}_{\leq \frac{1}{2}}} \leq \frac{1}{\sqrt{2}} \quad \text{und} \quad N(z - q) < 1$$

Definiere  $r = g - fq \Rightarrow g = fq + r$ . Dann gilt

$$N(r) = |r|^2 = |g - fq|^2 = |f|^2 \underbrace{|z - q|^2}_{< 1} < N(f).$$

□

□

*Beweis von Beispiel 4.* Der Ring  $R = \mathbb{Z}[\sqrt{2}] = \{a + \sqrt{2}b : a, b \in \mathbb{Z}\}$  ist ein euklidischer Ring. Wir definieren  $\phi : a + \sqrt{2}b \in \mathbb{Q}[\sqrt{2}] \mapsto \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} \in \text{Mat}_{22}(\mathbb{Q})$ . Dann ist  $\phi$  ein Ringhomomorphismus. In der Tat ist  $\phi$  auch  $\mathbb{Q}$ -linear,

$$\begin{aligned} \phi(1) &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2 \\ \phi(\sqrt{2}) &= \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}, \phi(\sqrt{2})^2 = \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}^2 = 2I_2 = \phi(\sqrt{2}^2) \end{aligned}$$

daraus folgt  $\phi(fg) = \phi(f)\phi(g)$  für  $f, g \in \mathbb{Q}[\sqrt{2}]$ . Wir definieren die Normfunktion

$$N(f) = |\det(\phi(f))| = \left| \det \left( \begin{pmatrix} a & 2b \\ b & a \end{pmatrix} \right) \right| = |a^2 - 2b^2|.$$

mit  $f = a + \sqrt{2}b \in \mathbb{Q}[\sqrt{2}]$ . Daher gilt  $N(fg) = N(f)N(g)$  für  $f, g \in \mathbb{Q}[\sqrt{2}]$ . Des weiteren gilt  $N(f) \geq 1$  für  $f \in \mathbb{Z}[\sqrt{2}]$ . Folgt die Normungleichung

$$N(fg) = N(f) \underbrace{N(g)}_{\geq 1} \geq N(f)$$

für  $g \in \mathbb{Z}[\sqrt{2}] \setminus \{0\}$ .

**Lemma.** In  $\mathbb{Z}[\sqrt{2}]$  gilt die Division mit Rest.

*Beweis.* Seien  $f, g \in \mathbb{Z}[\sqrt{2}]$ ,  $f \neq 0$  und  $z = \frac{g}{f} = a + \sqrt{2}b \in \mathbb{Q}[\sqrt{2}]$  mit  $a, b \in \mathbb{Q}$ . Wir definieren  $q = [a] + \sqrt{2}[b] \in \mathbb{Z}[\sqrt{2}]$ . Dann gilt

$$N(z - q) = |(a - [a])^2 - 2(b - [b])^2| \leq \frac{1}{4} + 2\frac{1}{4} < 1.$$

Der restliche Beweis läuft analog zu  $\mathbb{Z}[i]$ .

□

□

**Satz.** In einem Euklidischen Ring ist jedes Ideal ein Hauptideal.

*Beweis.* Sei  $I \subseteq R$  ein Ideal in einem Euklidischen Ring  $R$ . Falls  $I = \{0\}$ , so ist  $I = (0)$  ein Hauptideal. Wir nehmen nun an, dass  $I \neq \{0\}$ . Wir definieren  $f \in I$  als ein Element mit

$$N(f) = \min \underbrace{\{N(g) : g \in I \setminus \{0\}\}}_{\subseteq \mathbb{N} \text{ nichtleer}}.$$

**Behauptung:**  $I = (f)$ . Da  $f \in I$  ist, gilt auch  $(f) \subseteq I$ . Für die Umkehrung nehmen wir an, dass  $g \in I$ . Nach Division mit Rest gibt es  $q, r \in R$  mit  $g = qf + r$  und  $r = 0$  oder  $N(r) < N(f)$ .

Falls  $r = 0$  ist, so ergibt sich  $g = qf \in (f)$ .

Falls  $r \neq 0$  ist, so ergibt sich

$$r = \underbrace{g}_{\in I} - q \underbrace{f}_{\in I} \in I$$

mit  $N(r) < N(f)$ . Aber dies widerspricht der Definition von  $f$ . Folgt  $I = (f)$  wie behauptet und dies ist der Satz.  $\square$

## 2.2 Hauptidealring

**Definition.** Sei  $R$  ein Integritätsbereich. Dann heißt  $R$  ein *Hauptidealring* falls jedes Ideal in  $R$  ein Hauptideal ist.

**Beispiel.** Jeder euklidische Ring ist ein Hauptidealring.

*Bemerkung.* Der Ring  $\mathbb{Z}[\frac{1}{2}(1 + i \cdot \sqrt{163})]$  ist ein Hauptidealring und kann nicht zu einem Euklidischen Ring gemacht werden.

**Proposition.** Sei  $R$  ein Hauptidealring. Für je zwei Elemente  $f, g \in R \setminus \{0\}$  gibt es einen größten gemeinsamen Teiler  $d$  mit  $(d) = (f) + (g)$ .

**Definition.** Seien  $f, g, d \in R \setminus \{0\}$ . Wir sagen  $d$  ist ein gemeinsamer Teiler von  $f$  und  $g$  falls  $d \mid f$  und  $d \mid g$ . Wir sagen  $d$  ist ein größter gemeinsamer Teiler falls  $d$  ein gemeinsamer Teiler ist und jeder gemeinsame Teiler  $t$  auch  $d$  teilt.

*Bemerkung.* Zwei ggT's unterscheiden sich um eine Einheit (wenn  $R$  ein Integritätsbereich ist).

*Beweis.* Da  $I = (f) + (g)$  ein Ideal ist und  $R$  ein Hauptidealring ist, gibt es ein  $d \in R$  mit  $I = (d) = (f) + (g)$ . Daraus folgt,  $(f) \subseteq (d)$  und damit  $d \mid f$ . Genauso  $(g) \subseteq (d)$  und damit  $d \mid g$ . Also ist  $d$  ein gemeinsamer Teiler. Falls  $t \in R$  ein weiterer gemeinsamer Teiler von  $f$  und  $g$  ist, so folgt  $(f) \subseteq (t)$ ,  $(g) \subseteq (t)$  und somit  $(d) = (f) + (g) \subseteq (t)$  und damit  $t \mid d$ . Also ist  $d$  ein größter gemeinsamer Teiler.  $\square$

In einem Euklidischen Ring kann man einen ggT von  $f, g \in R \setminus \{0\}$  durch den *euklidischen Algorithmus* bestimmen.

- 0) Falls  $N(f) > N(g)$ , so vertauschen wir  $f$  und  $g$ . Also dürfen wir annehmen, dass  $N(f) \leq N(g)$ .
- 1) Dividiere  $g$  durch  $f$  mit Rest:  $g = qf + r$
- 2) Falls  $r = 0$  ist, so ist  $f$  ein ggT und der Algorithmus stoppt.
- 3) Falls  $r \neq 0$  ist, so ersetzen wir  $(f, g)$  durch  $(r, f)$  und springen nach 1).

**Lemma.** Der Euklidische Algorithmus (wie oben beschrieben) endet nach endlich vielen Schritten und berechnet einen ggT.

*Beweis.* Nach Schritt 0) gilt  $\min(N(f), N(g)) = N(f)$ . Bei jedem Durchlauf von 1) – 3) wird diese natürliche Zahl echt kleiner. Nach endlich vielen Schritten müssen wir also im Fall 2) sein.

Im Schritt 0) ändern wir  $I = (f) + (g)$  nicht. In 1) erhalten wir  $q, r \in R$  mit  $r = g - qf \in I$ ,  $f \in I$ . Außerdem ist  $f \in I' = (r) + (f)$ ,  $g = qf + r \in I'$ . Dies impliziert  $(f) + (g) = I = I' = (r) + (f)$ . Also

ändert sich das Ideal  $I$  nicht während des Algorithmus. Nach endlich vielen Schritten erreichen wir Falls 2) im Algorithmus:

$$I = (f) + (g) = (a) + (b).$$

mit  $f, g$  den ursprünglichen Elementen und  $a, b$  denen nach endlich vielen Schritten. Nun gilt  $b = q \cdot a + \underbrace{0}_{r=0}$  und somit  $I = (f) + (G) = (a)$ . Mit dem Beweis von der Proposition folgt  $a$  ist ein ggt von  $f$  und  $g$  und  $a$  ist dann auch der Output vom Algorithmus.  $\square$

**Satz** (Prime Elemente). *Sei  $R$  ein Hauptidealring.*

- 1) *Dann ist  $p \in R \setminus \{0\}$  prim genau dann wenn  $p$  irreduzibel ist.*
- 2) *Jedes  $f \in R \setminus \{0\}$  lässt sich als Produkt einer Einheit und endlich vielen primen Elementen schreiben.*

*Beweis von 1)* . Wir wissen bereits, dass jedes prime Element irreduzibel ist (siehe Lemma in 3.0). Wir nehmen nun an, dass  $p \in R \setminus \{0\}$  irreduzibel ist. Wie nehmen weiters an, dass  $p \mid ab$  für  $a, b \in R$ . Falls  $p \mid a$ , so gibt es nichts zu beweisen. Also nehmen wir an, dass  $p \nmid a$ .

Sei  $d$  ein ggT von  $p$  und  $a$ , also insbesondere ist  $d \mid p = d \cdot e$ . Da  $p$  irreduzibel ist gilt  $d \in R^\times$  oder  $e \in R^\times$ . Angenommen  $e \in R^\times$  dann folgt  $d = pe^{-1}$  also  $p \mid d, d \mid a$  folgt  $p \mid a$  was unserer Annahme widerspricht.

Somit ist  $d \in R^\times$ .  $d = xp + ya$  für  $x, y \in R$  da dies nach der Proposition in einem Hauptidealring gilt. Multipliziert man dies  $bd^{-1}$  so erhält man

$$b = \underbrace{xbd^{-1}p}_{p \mid -'' -} + \underbrace{yd^{-1}ab}_{p \mid ab}.$$

Somit folgt  $p \mid b$ .  $\square$

**Satz.** *Sei  $R$  ein Hauptidealring und  $p \in R$  irreduzibel. Dann ist  $(p)$  ein Maximalideal. Insbesondere ist  $p$  prim.*

*Beweis.* Sei  $R$  ein Hauptideal Ring und  $p \in R$  irreduzibel. Sei  $J \subseteq R$  ein Ideal mit  $J \supsetneq (p)$ . Da  $R$  ein Hauptidealring ist, gibt es ein  $d \in R$  mit  $J = (d) \supsetneq (p)$ . Also gibt es ein  $c$  mit  $p = d \cdot c$ . Also folgt  $d \in R^\times$  oder  $c \in R^\times$  (da  $p$  irreduzibel ist).

Falls  $c \in R^\times$  ist, so ist  $d = p \cdot c^{-1} \in (p)$  und damit  $J = (d) = (p)$  - ein Widerspruch zur Annahme an  $J$ .

Also gilt  $d \in R^\times$  und  $1 = dd^{-1} \in (d) = J = R$ . Da  $J \subseteq R$  mit  $(p) \subsetneq J$  beliebig war, ist  $(p)$  ein Maximalideal.  $\square$

Für den Beweis vom Satz über Prime Elemente Eigenschaft 2 verwenden wir:

**Proposition.** *Sei  $R$  ein Hauptidealring und seien  $J_0 \subseteq J_1 \subseteq J_2 \subseteq \dots$  eine ansteigende Kette von Idealen in  $R$ . Dann gibt es ein  $n \in \mathbb{N}$  mit  $J_m = J_n$  für alle  $m \geq n$ .*

*Beweis.* Wir definieren  $J = \bigcup_{n \in \mathbb{N}} J_n$  und erhalten, dass  $J$  ein Ideal ist. Da  $R$  ein Hauptidealring ist, gibt es also ein  $d \in R$  mit  $J = (d)$ . Also gibt es ein  $n \in \mathbb{N}$  mit  $d \in J_n$ . Daraus folgt

$$J = \bigcup_{i \in \mathbb{N}} J_i = (d) \subseteq J_n \subseteq J_m \subseteq J = (d).$$

für alle  $m \geq n$ .  $\square$

*Beweis vom Satz über Prime Elemente Eigenschaft 2.* Sei  $f \in R \setminus \{0\}$ . Für diesen Beweis sagen wir, dass  $f$  zerlegbar ist. Falls sich  $f$  als ein Produkt einer Einheit und endlich vielen ( $n \in \mathbb{N}$ ) irreduziblen Elementen schreiben lässt. Falls  $f \in R^\times$  ( $n = 0$ ) oder  $f$  irreduzibel ( $n = 1$ ) ist, so ist  $f$  zerlegbar.

Wir beweisen die Aussage mit einem Widerspruchsbeweis und nehmen an  $f \in R \setminus \{0\}$  sei nicht zerlegbar. Also ist  $f$  nicht irreduzibel,  $f = f_0 = f_1 \tilde{f}_1$  wobei  $f_1, \tilde{f}_1 \notin R^\times$ . Falls  $f_1$  und  $\tilde{f}_1$  beider zerlegbar wären, so würde dies auch für  $f$  folgen.

O.B.d.A. dürfen wir also annehmen, dass  $f_1$  nicht zerlegbar ist. Wir iterieren dieses Argument und erhalten

$$f_0 = f_1 \tilde{f}_1 \quad f_1 = f_2 \tilde{f}_2 \quad f_2 = f_3 \tilde{f}_3 \dots$$

mit  $f_0, f_1, f_2, f_3, \dots$  nicht zerlegbar und  $\tilde{f}_1, \tilde{f}_2, \tilde{f}_3, \dots \notin R^\times$ .

Es gilt  $f_{n+1} \mid f_n$  und daher  $(f_n) \subseteq (f_{n+1})$  für alle  $n \in \mathbb{N}$ . Wir wenden also die Proposition von vorhin an und erhalten, dass es ein  $n \in \mathbb{N}$  mit  $(f_n) = (f_{n+1})$  gibt. Da  $R$  ein Integritätsbereich ist, folgt aus  $(f_n) = (f_{n+1})$ , dass sich  $f_n$  und  $f_{n+1}$  multiplikativ um eine Einheit unterscheiden. Also gilt

$$\frac{f_n}{f_{n+1}} = \widetilde{f_{n+1}} \in R^\times,$$

was den Konstruktion von  $f_n, \tilde{f}_n$  widerspricht. Dieser Widerspruch zeigt, dass jedes Element  $f \in R \setminus \{0\}$  wie im Satz formuliert zerlegbar ist.  $\square$

**Beispiel.** Einige Primzahlen in  $\mathbb{Z}[i]$ , z.B. sind  $1 \pm i, 3, 2 \pm i$  Primzahlen in  $\mathbb{Z}[i]$ .

2 ist keine Primzahl in  $\mathbb{Z}[i]$ , da  $2 = (1+i)(1-i)$ . 5 ist auch keine Primzahl in  $\mathbb{Z}[i]$ , da  $5 = (2+i)(2-i)$ .

Nach dem ersten folgenden Lemma ergibt sich nun, dass  $1 \pm i, 2 \pm i$  Primzahlen in  $\mathbb{Z}[i]$  sind. Nach dem zweiten Lemma sind 3, 7 Primzahlen in  $\mathbb{Z}[i]$ .

**Lemma.** Sei  $z \in \mathbb{Z}[i]$  so dass  $N(z) = p \in \mathbb{N}$  eine Primzahl in  $\mathbb{N}$  ist. Dann ist  $z$  irreduzibel (also prim) in  $\mathbb{Z}[i]$ .

*Beweis.* Angenommen  $z = u \cdot v$  ist ein Produkt von  $u, v \in \mathbb{Z}[i]$ . Dann ist  $p = N(z) = \underbrace{N(u)}_{\in \mathbb{N}} \cdot \underbrace{N(v)}_{\in \mathbb{N}}$  und daher  $N(u) = 1$  ( $u \in \mathbb{Z}[i]^\times$ ) oder  $N(v) = 1$  ( $v \in \mathbb{Z}[i]^\times$ ).  $\square$

**Lemma.** Angenommen  $p \in \mathbb{N}$  ist eine Primzahl in  $\mathbb{N}$ , die sich nicht als Summe zweier Quadratzahlen schreiben lässt. Dann ist  $p$  auch eine Primzahl in  $\mathbb{Z}[i]$ .

*Beweis.* Wir zeigen, dass  $p$  in  $\mathbb{Z}[i]$  irreduzibel ist. Also angenommen  $p = z \cdot w$  für  $z, w \in \mathbb{Z}[i]$ . Dann folgt  $N(p) = N(z)N(w) = p^2$  und damit  $N(z) \mid p^2$  in  $\mathbb{N}$ , womit  $N(z), N(w) \in \{1, p, p^2\}$  ist. Dabei ist aber  $N(z) = N(a+ib) = a^2 + b^2 = p$  nicht möglich. Also gilt  $N(z), N(w) \in \{1, p^2\}$  und es folgt  $N(z) = 1$  (und  $N(w) = p^2$ ) oder  $N(w) = 1$  (und  $N(z) = p^2$ ). Also ist  $z \in \mathbb{Z}[i]^\times$  oder  $w \in \mathbb{Z}[i]^\times$ .  $\square$

**Beispiel.** Im Ring der Polynome  $K[x]$  mit einer Variable über einem Körper  $K$  gibt es irreduzible Elemente:

Grad 1: jedes Polynom vom Grad 1 ist irreduzibel.

Grad 2: ein Polynom vom Grad 2 ist irreduzibel genau dann wenn es keine Nullstellen im Körper  $K$  hat.

Grad 3: selbes wie bei Grad 2.

Grad 4: das betrachten von Nullstellen ist nicht mehr ausreichend.



Dies hängt stark vom Körper  $K$  ab.

## 2.3 Faktorielle Ringe

**Definition.** Ein Integritätsbereich  $R$  heißt ein *faktorieller Ring* falls jedes  $a \in R \setminus \{0\}$  sich als ein Produkt von einer Einheit und endlich vielen Primelemente von  $R$  schreiben lässt:  $a = u \cdot p_1 \cdot \dots \cdot p_m$  für  $u \in R^\times, m \in \mathbb{N}, p_1, \dots, p_m \in R$  prim.

**Beispiel.** Jeder Euklidische und jeder Hauptidealring. Es gibt noch weitere Bsp, wir werden zeigen, dass z.B.  $\mathbb{Z}[x, y, z]$  ein faktorieller Ring ist.

**Proposition.** Sei  $R$  ein faktorieller Ring. Dann ist  $p \in R \setminus \{0\}$  irreduzibel gdw.  $p$  prim ist.

*Beweis.*  $\Leftarrow$ : ✓ schon gezeigt

$\Rightarrow$ : Sei also  $p$  irreduzibel. Dann ist  $p = u \cdot q_1 \cdot \dots \cdot q_n$  ein Produkt einer Einheit  $u \in R^\times$  und Primelementen  $q_1, \dots, q_n \in R$  nach Annahme an  $R$ . Da  $p$  irreduzibel ist folgt  $n = 1$  und  $(p) = (q_1)$ , womit  $(p)$  ein Primideal ist und  $p$  selbst ein Primelement ist.  $\square$

**Korollar.** Sei  $R$  ein Integritätsbereich. Dann ist  $R$  faktoriell gdw. jedes Element von  $R \setminus \{0\}$  eine Zerlegung als ein Produkt von einer Einheit und endlich vielen irreduziblen Elementen besitzt und jedes irreduzible Element auch ein Primelement ist.

**Definition.** Sei  $R$  ein kommutativer Ring und  $a, b \in R$ . Wir sagen  $a, b$  sind *assoziiert* und schreiben  $a \sim b$  falls es eine Einheit  $u \in R^\times$  gibt mit  $a = ub$ .

**Lemma.** Dies definiert eine Äquivalenzrelation auf  $R$ .

*Beweis.* •  $a \sim a$  da  $a = 1 \cdot a$  und  $1 \in R^\times$ .

•  $a \sim b \Rightarrow b \sim a$ : Gilt  $a = ub \Rightarrow b = u^{-1}a$  mit  $u^{-1} \in R^\times$ .

•  $a \sim b$  und  $b \sim c \Rightarrow a \sim c$ : Gilt  $a = ub$  und  $b = vc \Rightarrow a = (uv)c$  mit  $uv \in R^\times$ . Also  $a \sim c$ .  $\square$

**Lemma.** Sei  $R$  ein Integritätsbereich. Seien  $p, q \in R \setminus \{0\}$  irreduzibel und  $p \mid q$ . Dann gilt  $p \sim q$ .

*Beweis.* Nach Annahme gibt es ein  $a \in R$  mit  $q = a \cdot p$ . Da  $q$  irreduzibel ist folgt  $a \in R^\times$  oder  $p \in R^\times$ . Da  $p$  irreduzibel ist, kann  $p \in R^\times$  nicht gelten. Also ist  $a \in R^\times$  und  $p \sim q$ .  $\square$

**Definition** (Wh.). Für  $n \in \mathbb{N}_{>0}$  sei  $S_n$  die *symmetrische Gruppe* auf der Menge  $\{1, \dots, n\}$ , d.h.

$$S_n = \{\sigma : \{1, \dots, n\} \rightarrow \{1, \dots, n\} \text{ bijektiv}\}.$$

**Satz** (Eindeutige Primfaktorzerlegung). Sei  $R$  ein faktorieller Ring, dann besitzt jedes nichttriviale Element von  $R$  eine bis auf Permutation und Assoziierung eindeutige Primfaktorzerlegung.

Genauer gilt also für jedes  $a \in R \setminus \{0\}$  gibt es eine Einheit  $u \in R^\times$ ,  $m \in \mathbb{N}$ , und Primelemente  $p_1, \dots, p_m$  mit  $a = up_1 \dots p_m$ .

Falls  $a = vq_1 \dots q_n$  eine weitere Zerlegung ist, wobei  $v \in R^\times$ ,  $n \in \mathbb{N}$  und  $q_1, \dots, q_n$  prim sind, dann gibt es  $\sigma \in S_n$  so dass  $q_j \sim p_{\sigma(j)}$  für  $j = 1, \dots, n$  und  $m = n$ .

Die Existenz der Zerlegung ist die Definition von „faktorieller Ring“. Wir nennen  $p_1, \dots, p_m$  die Primfaktorzerlegung von  $a$ .

*Beweis der Eindeutigkeit.* Angenommen  $a = up_1 \dots p_m = vq_1 \dots q_n$  mit  $u, v \in R^\times, m, n \in \mathbb{N}$  und  $p_1, \dots, p_m, q_1, \dots, q_n$  Primelemente in  $R$ . Falls  $n = 0$  ist, so ist  $a = v \in R^\times$ . Daraus folgt aber auch  $m = 0$  (Falls  $m > 0$  wäre, so folgt mit  $p_1 \mid a$  und  $a \mid 1$  dass  $p_1 \mid 1$  - ein Widerspruch zur Annahme an  $p_1$  prim).

Wir verwenden Induktion nach  $n$  und nehmen an, dass die Eindeutigkeit bereits gilt falls eine der beiden Zerlegungen weniger als  $n$  Faktoren besitzt. Wir nehmen an  $n > 0$ . Da  $a = up_1 \dots p_m = vq_1 \dots q_n$  gilt  $q_n \mid a$ . Da  $q_n$  ein Primelement von  $R$  ist, gibt es einen Index  $i = \sigma(n)$ , so dass  $q_n \mid p_{\sigma(n)}$ . Nach einem Lemma vom letzten Mal folgt daraus  $q_n \sim p_{\sigma(n)}$ . Wir verwenden nun die Induktionsannahme für

$$\frac{a}{q_n} = u \underbrace{\frac{p_{\sigma(n)}}{q_n}}_{\in R^\times} p_1 \dots p_{\sigma(n)-1} p_{\sigma(n)+1} \dots p_m = vq_1 \dots q_{n-1}.$$

Es folgt  $n - 1 = m - 1$  und es gibt eine Bijektion

$$\sigma : \{1, \dots, n-1\} \rightarrow \{1, \dots, \sigma(n)-1, \sigma(n)+1, \dots, m\}$$

so dass  $q_j \sim p_{\sigma(j)}$  für  $j = 1, \dots, n-1$ . Dies gilt auch für  $j = n$ . Dies beendet den Induktionsschritt.  $\square$

**Definition.** Sei  $R$  ein faktorieller Ring. Wir sagen  $P \subseteq R$  ist eine *Repräsentantenmenge* (der Primelemente) falls jedes  $p \in P$  ein Primelement in  $R$  ist und es zu jedem Primelement  $q \in R$  ein eindeutig bestimmtes  $p \in P$  gibt mit  $q \sim p$ .

**Beispiel.** Für  $R = \mathbb{Z}$  betrachten wir  $P = \{p \in \mathbb{Z} \text{ prim und positiv}\}$ . Für  $R = K[x]$  betrachten wir

$$P = \{f \in K[x] \text{ irreduzibel und } f \text{ normiert}\}.$$

Normiert: Der führende Koeffizient von  $f$  ist gleich 1.

Für  $R = \mathbb{Z}[i]$  verwenden wir  $P = \{a + ib : a, b \in \mathbb{Z}, a + ib \text{ prim und } -a < b \leq a\}$

**Lemma.** Sei  $R$  ein faktorieller Ring. Dann existiert eine Repräsentantenmenge.

*Beweis.* Wir verwenden das Auswahlaxiom für die Menge  $\{[p]_\sim : p \in R \text{ prim}\}$  und erhalten  $P$  als Bild der Auswahlfunktion.  $\square$

**Satz** (Eindeutige Primfaktorzerlegung). Sei  $R$  ein faktorieller Ring und  $P \subseteq R$  eine Repräsentantenmenge. Dann besitzt jedes  $a \in R \setminus \{0\}$  eine eindeutige Primfaktorzerlegung der Form

$$a = u \prod_{p \in P} p^{n_p} \left[ = u \prod_{\substack{p \in P \\ n_p > 0}} p^{n_p} \right]$$

wobei  $n_p = 0$  für alle bis auf endlich viele  $p \in P$ .

*Beweis der Existenz.* Falls  $a \in R^\times$  so setzen wir  $u = a$  und  $n_p = 0$  für alle  $p \in P$ . Ansonsten ist  $a = up_1 \dots p_n$ , wie in der Definition von faktoriellen Ringen. Zu jedem  $p_j$  gibt es ein eindeutig bestimmtes  $p \in P$  mit  $p_j \sim p$ . Damit erhalten wird

$$a = u \underbrace{p_1 \dots p_m}_{\in R^\times} \prod_{p \in P} p^{n_p}$$

wobei  $n_p = \#j$  mit  $p_j \sim p$ .  $\square$

*Beweis der Eindeutigkeit.* Angenommen  $a = u \prod_{p \in P} p^{n_p} = v \prod_{p \in P} p^{n'_p}$ . Falls  $n'_p = 0$  für alle  $p \in P$ , so ist  $a = v \in R^\times$  und  $n_p = 0$  für alle  $p \in P$  und  $a = u$ .

Ansonsten ist  $n'_p > 0$  für ein  $p_0 \in P$  und daher gilt  $p_0 \mid a = u \prod_{p \in P} p^{n_p}$ , was  $n_{p_0} > 0$  impliziert auf Grund der Eigenschaften der Repräsentantenmenge. Wir verwenden Induktion nach  $\sum_{p \in P} n'_p$ .  $\square$

**Lemma.** Sei  $R$  ein faktorieller Ring und  $P \subseteq R$  eine Repräsentantenmenge. Sei  $a = u \prod_{p \in P} p^{m_p}$  und  $b = v \prod_{p \in P} p^{n_p}$ . Dann gilt  $a \mid b$  gdw.  $m_p \leq n_p$  für alle  $p \in P$ .

*Beweis.* „ $\Rightarrow$ “:  $b = ac$  und  $c = w \prod_{p \in P} p^{k_p}$ . Dann folgt

$$v \prod_{p \in P} p^{n_p} = b = uw \prod_{p \in P} p^{m_p + k_p}$$

und daher  $n_p = m_p + k_p \geq m_p$  für alle  $p \in P$ .

„ $\Leftarrow$ “: Wir definieren  $c = vu^{-1} \prod_{p \in P} p^{n_p - m_p} \in R$ . Dann gilt

$$ac = u \prod_{p \in P} p^{m_p} \cdot vu^{-1} \prod_{p \in P} p^{n_p - m_p} = v \prod_{p \in P} p^{n_p} = b.$$

also  $a \mid b$ .  $\square$

**Proposition (ggT).** Sei  $R$  ein faktorieller Ring mit Repräsentantenmenge  $P$ . Dann existiert für jedes Paar  $a, b \in R$ , nicht beide 0, ein ggT. Falls  $a = u \prod_{p \in P} p^{m_p}, b = v \prod_{p \in P} p^{n_p}$  ist, so ist  $\prod_{p \in P} p^{\min(m_p, n_p)}$  ein ggT von  $a$  und  $b$ .

*Beweis.* Wir haben  $d \mid a$  und  $d \mid b$  auf Grund des Lemmas. Falls  $t = w \prod_{p \in P} p^{k_p}$  ein weiterer gemeinsamer Teiler von  $a$  und  $b$  ist, so folgt  $k_p \leq m_p, k_p \leq n_p$  und damit  $k_p \leq \min(m_p, n_p)$  für alle  $p \in P$ . Daraus folgt  $t \mid d$ .  $\square$

Wir können analog den ggT von mehreren Elementen  $a_1, \dots, a_l \in R$  definieren und die obige Proposition gilt analog.

**Definition.** Sei  $R$  ein faktorieller Ring. Wir sagen  $a_1, \dots, a_l \in R$  sind *coprim* falls 1 ein ggT von  $a_1, \dots, a_l$  ist, oder äquivalenterweise falls es zu jedem Primelement  $p$  in  $R$  ein  $a_j$  gibt so dass  $a_j$  nicht durch  $p$  teilbar ist.

**Korollar.** Sei  $R$  ein faktorieller Ring mit Quotientenkörper  $K$ . Dann hat jedes  $x \in K$  eine Darstellung  $x = \frac{a}{b}$  mit  $a, b \in R$  coprim,  $b \neq 0$ .

*Beweis.* Angenommen  $x = \frac{\tilde{a}}{\tilde{b}} \in K$  und sei  $d$  der ggT von  $\tilde{a}$  und  $\tilde{b}$ . Wir definieren  $a = \frac{\tilde{a}}{d}$  und  $b = \frac{\tilde{b}}{d}$  und erhalten, dass  $a, b$  coprim sind und

$$x = \frac{\tilde{a}}{\tilde{b}} = \frac{\frac{\tilde{a}}{d}}{\frac{\tilde{b}}{d}} = \frac{a}{b}.$$

$\square$

**Korollar.** Sei  $R$  faktoriell und  $K = \text{Quot}(R)$ . Dann hat jedes  $x \in K$  eine Darstellung der Form

$$x = u \prod_{p \in P} p^{n_p},$$

wobei  $n_p \in \mathbb{Z}$  und gleich 0 für alle bis auf endlich viele  $p \in P$  ist.

**Beispiel** (Ein Gegenbeispiel). Wir definieren  $R = \mathbb{Z}[i\sqrt{5}] \subseteq K = \mathbb{Q}[i\sqrt{5}] \subseteq \mathbb{C}$ . Also  $R = \{a + i\sqrt{5}b : a, b \in \mathbb{Z}\}$ . Zerlegungen der 6 :

$$6 = 2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5}).$$

1. Behauptung: 2, 3,  $1 \pm i\sqrt{5}$  sind alle irreduzibel in  $R$ .
2. Behauptung:  $2 \nmid 1 \pm i\sqrt{5}$  und  $3 \nmid 1 \pm i\sqrt{5}$ .

*Beweis der 2. Behauptung.*

$$\frac{1 \pm i\sqrt{5}}{2} = \frac{1}{2} \pm i\sqrt{5}\frac{1}{2} \notin R \quad \text{und} \quad \frac{1 \pm i\sqrt{5}}{3} = \frac{1}{3} \pm i\sqrt{5}\frac{1}{3} \notin R.$$

Folgt die 2. Behauptung. □

**2 ist irreduzibel:**

Angenommen  $2 = z \cdot w$ ,  $z, w \in R$ . Wir verwenden die Normfunktion  $N(a + i\sqrt{5}b) = |a + i\sqrt{5}b|^2 = a^2 + 5b^2$  für  $a + i\sqrt{5}b \in R$  hat diese Normfunktion Werte in  $\mathbb{N}$ .

$$\Rightarrow 4 = N(2) = N(z)N(w) \Rightarrow N(z), N(w) \in \{1, 2, 4\}.$$

2 kann nicht sein also  $\{N(z), N(w)\} = \{1, 4\}$ . Falls  $N(z) = 1$  ist, so ist  $z \pm 1$  eine Einheit in  $R$ . Analog für  $N(w) = 1$ .

**3 ist irreduzibel:**

Analog:  $N(z) = 3 = a^2 + 5b^2$  ist nicht möglich.

**Auch  $1 \pm i\sqrt{5}$  sind irreduzibel:**

$1 \pm i\sqrt{5} = zw \Rightarrow N(1 \pm i\sqrt{5}) = 6 = N(z)N(w) \Rightarrow N(z)N(w) \in \{1, 2, 3, 6\}$  Also ist  $z$  oder  $w$  eine Einheit in  $R$ .

Beispiele dieser Art führten zur Erfindung von „idealisierten Primfaktoren“ (heute Primideale).  
 $(6) = (2, 1 + i\sqrt{5})^2(3, 1 + i\sqrt{5})(3, 1 - i\sqrt{5})$

## 2.4 Einige algebraische Euklidische Ringe

Alle Beispiele, die wir hier betrachten wollen, leben in einem quadratischen Zahlkörper:  $K = \mathbb{Q}[\sqrt{d}] = \{a + b\sqrt{d} : a, b \in \mathbb{Q}\}$  mit  $d \in \mathbb{Z}$ , das kein Quadrat ist. Isomorph dazu  $\mathbb{Q}[x]/(x^2 - d)$ .

Wir definieren auf  $K$  die Konjugation  $\tau : K \rightarrow K, a + b\sqrt{d} \mapsto a - b\sqrt{d}$ . Dies definiert einen Körperautomorphismus.

*Beweis.* Wir definieren  $\text{ev}_{\sqrt{d}} : \mathbb{Q}[x] \rightarrow K, f \mapsto f(\sqrt{d})$ .  $\text{ev}_{\sqrt{d}}(x^2 - d) = 0$ . Da  $x^2 - d$  keine Nullstellen in  $\mathbb{Q}$  hat (Annahme an  $d$ ), ist  $x^2 - d$  irreduzibel/prim in  $\mathbb{Q}[x]$ . Daher folgt  $(x^2 - d)$  ist ein Maximalideal. Gemeinsam mit  $(x^2 - d) \subseteq \text{Ker}(\text{ev}_{\sqrt{d}})$ , erhalten wir  $(x^2 - d) = \text{Ker}(\text{ev}_{\sqrt{d}})$ . Der erste Isomorphiesatz ergibt nun

$$\mathbb{Q}[x]/(x^2 - d) = \mathbb{Q}[x]/\text{Ker}(\text{ev}_{\sqrt{d}}) \xrightarrow{\varphi_+} \mathbb{Q}[\sqrt{d}] = K.$$

Beweis Körperautomorphismus:

$$\begin{array}{ccccc} K & \xrightarrow{\varphi_+} & \mathbb{Q}[x]/(x^2 - d) & \xrightarrow{\varphi_-} & K \\ & & \searrow \tau & \nearrow & \\ \sqrt{d} & \longmapsto & X + (x^2 + d) & \longmapsto & -\sqrt{d} \end{array}$$

Wobei der Isomorphismus  $\varphi_+$  Auswertungen bei  $\sqrt{d}$  verwendet und analog dazu der Isomorphismus  $\varphi_-$  Auswertungen bei  $\sqrt{-d}$  verwendet.  $\square$

Auf  $K$  definieren wir die Normfunktion

$$N(a + b\sqrt{d}) = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - db^2$$

so dass  $N : K \rightarrow \mathbb{Q}$  multiplikativ ist, daher

$$N(zw) = (zw) \underbrace{\tau(zw)}_{\tau(z)\tau(w)} = N(z)N(w) \quad \text{für } z, w \in K.$$

Weiters  $N(z) = 0 \Leftrightarrow z = 0$  für alle  $z = a + b\sqrt{d} \in K$ .

Wir werden den Ring  $R = \mathbb{Z}[\sqrt{d}]$  betrachten und wollen  $\phi(z) = |N(z)|$  als Gradfunktion verwenden.

**Satz.** Für  $d = -1, -2, 2, 3$  ist  $R = \mathbb{Z}[\sqrt{d}]$  ein Euklidischer Ring, wobei wir  $\phi(z) = |N(z)|$  als Gradfunktion verwenden.

*Beweis.* Seien  $f, g \in R, f \neq 0$ . Wir definieren  $z = \frac{g}{f} \in \mathbb{Q}[\sqrt{d}] = a + b\sqrt{d}$  mit  $a, b \in \mathbb{Q}$ . Wir definieren  $q = \underbrace{[a]}_{\in \mathbb{Z}} + \underbrace{[b]}_{\in \mathbb{Z}} \sqrt{d} \in R$  als die beste Approximation. Dann gilt

$$\phi(z - q) = |N(z - q)| = \left| \underbrace{(a - [a])^2}_{\leq \frac{1}{2}} - d \underbrace{(b - [b])^2}_{\leq \frac{1}{2}} \right| \leq \frac{1}{4} + |d| \frac{1}{4} < 1 \quad (*)$$

für  $d = -1, -2, 2$ . Für  $d = 3$  gilt in (\*) Gleichheit, aber da die beiden Ausdrücke im Absolutbetrag verschiedene Vorzeichen haben, gilt auch hier  $\phi(z - q) < 1$ .

Wir definieren  $r = g - f \cdot q \in \mathbb{Z}[\sqrt{d}]$ , und erhalten  $g = fq + r$  und

$$\phi(r) = |N(r)| = |N(g - f \cdot q)| = |N(f)N(z - q)| < |N(f)| = \phi(f).$$

$\square$

Sei  $R = \mathbb{Z}[\sqrt{d}]$ .

**Lemma.** Es gilt  $u \in R^\times \Leftrightarrow N(u) = \pm 1$ .

**Lemma.** Falls  $z \in R$  eine Primzahl in  $\mathbb{Z}$  als Norm hat, so ist  $z$  in  $R$  irreduzibel.

**Lemma.** Falls  $p \in \mathbb{Z}$  eine Primzahl in  $\mathbb{Z}$  ist, so dass weder  $p$  noch  $-p$  eine Norm von einem Element in  $R$  ist, so ist  $p$  ein irreduzibles Element in  $R$ .

*Beweis von Lemma 1.* Sei  $u \in R^\times$ . Dann gibt es  $v \in R^\times$  mit  $uv = 1$ . Daraus folgt  $\underbrace{N(u)}_{\in \mathbb{Z}} \underbrace{N(v)}_{\in \mathbb{Z}} =$

$N(uv) = 1$  und daher  $N(u) = \pm 1$ .

Angenommen  $u \in R$  erfüllt  $N(u) = \pm 1$ . Dann gilt  $u \cdot (\pm \tau(u)) = \pm N(u) = 1$  also  $u^{-1} = \pm \tau(u)$ .  $\square$

*Beweis von Lemma 2.* Angenommen  $z \in R$  erfüllt  $N(z) = p$ , wobei  $p \in \mathbb{Z}$  eine Primzahl ist. Angenommen  $z = v \cdot w$  für  $v, w \in R$ . Dann folgt  $p = N(z) = N(v)N(w)$ . Da  $p \in \mathbb{Z}$  irreduzibel in  $\mathbb{Z}$  ist, folgt daraus  $\underbrace{N(v)}_{v \in R^\times} = \pm 1$  oder  $\underbrace{N(w)}_{w \in R^\times} = \pm 1$ .  $\square$

*Beweis von Lemma 3.* Sei  $p \in \mathbb{Z}$  prim und weder  $p$  noch  $-p$  eine Norm. Angenommen  $p = vw$  für  $v, w \in R$ . Dann folgt  $p^2 = N(p) = N(v)N(w)$ . Da  $p$  eine Primzahl ist folgt daraus  $N(v), N(w) \in \{\pm 1, \pm p, \pm p^2\}$ . Wobei  $\pm p$  nach Annahme nicht auftritt. Also gilt  $\underbrace{N(v) = \pm 1}_{v \in R^\times}$  (und  $N(w) = \pm p^2$ )

oder  $\underbrace{N(w) = \pm 1}_{w \in R^\times}$  (und  $N(v) = \pm p^2$ ). □

**Satz** (Gauss'sche ganze Zahlen). Sei  $R = \mathbb{Z}[i]$  der Ring der Gauss'schen ganzen Zahlen. Dann ist  $R$  ein Euklidischer Ring. Wir können in  $R$  die Repräsentantenmenge

$$P = \{z = a + ib \in R \mid z \text{ prim, } -a < b \leq a\}$$

verwenden. Diese Menge  $P$  enthält

- (Ramified):  $z = 1 + i$  mit  $2 = -i(1 + i)^2$
- (Inert):  $p \in \mathbb{N}$  prim mit  $p \equiv 3 \pmod{4}$ , z.B. 3, 7, 11, ...
- (Split):  $z = a \pm bi$  prim in  $R$ , wobei  $a, b \in \mathbb{N}, b < a$  und  $a^2 + b^2 = p \equiv 1 \pmod{4}$  mit  $p \in \mathbb{N}$  prim.  $p = (a + ib)(a - ib)$  z.B. 5, 13, ...

**Lemma.** Sei  $p \in \mathbb{N}$  prim. Dann ist  $(p - 1)! \equiv -1 \pmod{p}$ .

*Beweis.*

$$(p - 1)! = \prod_{k=1}^{p-1} k \stackrel{(*)}{=} 1 \cdot \left( \prod_{\substack{1 < a < p < p-1 \\ a \cdot b = 1 \pmod{p}}} (ab) \right) \cdot (p - 1) \equiv -1 \pmod{p}.$$

Wann gilt  $x = x^{-1}$  für  $x \in \mathbb{F}_p^\times$ ?

$$x = x^{-1} \Leftrightarrow x^2 = 1 \Leftrightarrow x^2 - 1 = 0 \Leftrightarrow (x + 1)(x - 1) = 0 \Leftrightarrow x = \pm 1$$

in  $\mathbb{F}_p$  ist. Dies beweist (\*). □

**Proposition.** Sei  $p \in \mathbb{N}$  kongruent 1 mod 4. Dann gibt es in  $\mathbb{F}_p$  zwei Lösungen der quadratischen Gleichung  $x^2 = -1$ .

**Beispiel.**  $p = 5, x = 2 \Rightarrow x^2 = 4 = -1$  in  $\mathbb{F}_5$ .

$p = 13, x = 5 \Rightarrow x^2 = 25 = -1$  in  $\mathbb{F}_{13}$ .

*Beweis.* Wir definieren  $x = \left(\frac{p-1}{2}\right)!$  in  $\mathbb{F}_p$ . Dann gilt

$$x^2 = 1 \cdot 2 \cdot 3 \cdot \dots \cdot \left(p - \frac{1}{2}\right) \cdot \underbrace{\left(\frac{p-1}{2}\right) \cdot \dots \cdot 3 \cdot 2 \cdot 1}_{\frac{p-1}{2} \text{-Faktoren}} \cdot (-1)^{\frac{p-1}{2}}.$$

und  $\frac{p-1}{2}$  ist gerade.

$$\begin{aligned} &= 1 \cdot 2 \cdot 3 \cdot \dots \cdot \left(\frac{p-1}{2}\right) \cdot \left(-\frac{p-1}{2}\right) \cdot \dots \cdot (-3) \cdot (-2) \cdot (-1) \\ &= 1 \cdot 2 \cdot 3 \cdot \dots \cdot \left(\frac{p-1}{2}\right) \cdot \left(\frac{p-1}{2} + 1\right) \cdot \dots \cdot (p-3) \cdot (p-2) \cdot (p-1) \\ &= (p-1)! = -1 \text{ in } \mathbb{F}_p. \end{aligned}$$

□

**Korollar.** Sei  $p \in \mathbb{N}$  kongruent  $1 \pmod{4}$ . Dann ist  $p$  keine Primzahl in  $\mathbb{Z}[i]$ .

*Beweis.* Wir betrachten  $\mathbb{Z}[i]/(p) \cong \mathbb{F}_p[x]/(x^2 + 1)$ ,  $a + ib + (p) \mapsto a + bX \pmod{p}$ . Aber  $x^2 + 1$  ist über  $\mathbb{F}_p$  nicht irreduzibel, da  $x^2 + 1$  zwei Nullstellen in  $\mathbb{F}_p$  hat (siehe Proposition). Also ist  $\mathbb{Z}[i]/(p)$  kein Integritätsbereich und  $p$  kein Primelement.  $\square$

*Alternativer Beweis.* Angenommen  $a \in \mathbb{Z}$  erfüllen  $a^2 \equiv -1 \pmod{p}$ . Insbesondere gilt damit  $p \mid (a^2 + 1) = (a^2 - i^2) = (a + i)(a - i)$ . Da aber  $a \in \mathbb{Z}$  ist, gilt  $p \nmid (a + i)$  und  $p \nmid (a - i)$ .  $\square$

*Beweis der Beschreibung der Primzahlen in  $\mathbb{Z}[i]$ .*  $N(1 + i) = 2$  und Lemma 2 zeigt, dass  $1 + i$  irreduzibel, also prim, ist. Angenommen  $p \in \mathbb{N}$  ist kongruent  $3 \pmod{4}$ . Dann gilt

$$p \nmid a^2 + b^2 \in \{0, 1, 2 \pmod{4}\}$$

für  $a, b \in \mathbb{Z}$  gilt  $a^2 \equiv 0, 1 \pmod{4}$ . Also ist  $p$  (und auch  $-p$ ) keine Norm  $N(a + ib) = a^2 + b^2 > 0$  eines Elements von  $\mathbb{Z}[i]$ . Lemma 3 zeigt also, dass  $p$  eine Primzahl in  $\mathbb{Z}[i]$  ist.

Sei nun  $p \in \mathbb{N}$  kongruent  $1 \pmod{4}$  und prim in  $\mathbb{Z}$ . Dann ist  $p$  keine Primzahl in  $\mathbb{Z}[i]$  wegen dem Korollar. Also kann Lemma 3 nicht angewendet werden und daher gibt es ein  $z \in \mathbb{Z}[i]$  mit  $\underbrace{N(z)}_{>0} = p$ . Anders formuliert haben wir also  $a, b \in \mathbb{Z}$  mit  $p = a^2 + b^2$  gefunden. O.B.d.A. dürfen wir  $a, b \in \mathbb{N}$  und  $b < a$  annehmen. Dann gilt  $a + ib, a - ib \in P$ ,  $p = (a + ib)(a - ib)$  und  $a \pm ib$  sind nicht assoziiert, da  $\pm 1, \pm i$  die einzigen Einheiten sind und der Winkel zwischen  $a + ib$  und  $a - ib$  echt kleiner als  $90^\circ$  ist.

Wir zeigen noch, dass obige drei Fälle alle Primzahlen in  $P \subseteq \mathbb{Z}[i]$  liefern. Angenommen  $z \in \mathbb{Z}[i]$  ist eine Primzahl. Dann ist  $n = N(z) = z\bar{z}$  eine natürliche Zahl. Sei  $p \in \mathbb{N}$  ein Primfaktor von  $n$ .

- $p = 2 \Rightarrow 2 = (1 + i)(1 - i) \mid n = z\bar{z} \Rightarrow (1 + i) \mid z\bar{z} \Rightarrow 1 + i \mid z$  oder  $1 + i \mid \bar{z}$ . Folgt  $1 - i \mid z$ . Also  $1 + i \sim z$  und  $1 + i \sim 1 - i \sim z$ .
- $p \equiv 3 \pmod{4}$ : Und  $p \mid z\bar{z}$  und  $p$  ist prim in  $\mathbb{Z}[i]$ . Also  $p \mid z$  oder  $p \mid \bar{z}$ . Und somit  $p \sim z$ .
- $p \equiv 1 \pmod{4}$ :  $(a + ib) \mid p = (a + ib)(a - ib) \mid z\bar{z}$ . Folgt  $a + ib \mid z \Rightarrow a + ib \sim z$  oder  $a + ib \sim \bar{z} \Rightarrow a - ib \mid z \Rightarrow a - ib \sim z$ .

$\square$

**Satz.** Im  $R_{falsch} = \mathbb{Z}[\sqrt{3}i]$  funktioniert Division mit Rest nicht wie in den obigen Fällen. Aber in  $R_{richtig} = \mathbb{Z}[\zeta] = \{a + b\zeta : a, b \in \mathbb{Z}\}$  für  $\zeta = \frac{1 + \sqrt{3}i}{2}$  funktioniert dies wieder.

*Beweis Skizze.*  $z = \frac{a}{f} = (a + \frac{1}{2}) + (b + \frac{1}{2})\sqrt{3}i$ ,  $a, b \in \mathbb{Z}$  hat Abstand 1 zu allen Elementen von  $\mathbb{Z}[\sqrt{3}i]$ . Beweis scheitert für  $R_{falsch}$ .

Aber in diesem Fall ist  $z \in R_{richtig}$  und deswegen hat es Abstand 0 zu sich selbst. Beweis klappt nun.  $\square$

## 2.5 Polynomringe

Seite 108

**Satz** (Gauss). Falls  $R$  ein faktorieller Ring ist, so ist auch  $R[x]$  ein faktorieller Ring.

**Korollar.** Der Ring  $\mathbb{Z}[x_1, \dots, x_n]$  und der Ring  $K[x_1, \dots, x_n]$  für einen Körper  $K$  sind faktoriell,

**Definition.** Sei  $R$  ein faktorieller Ring und  $f \in \mathbb{R}[x] \setminus \{0\}$ . Dann nennen wir den ggT der Koeffizienten von  $f$  den *Inhalt*  $I(f)$  von  $f$  (welcher bis auf Einheiten in  $R$  eindeutig bestimmt ist).

Wir sagen  $f$  ist *primitiv* falls  $I(f) \sim 1$ .

**Beispiel.** Sei  $R = \mathbb{Z}$ . Dann ist  $I(2x + 2) \sim 2$  und  $3x + 2$  ist primitiv.

### Beobachtungen

- Jedes normierte Polynom ist primitiv.
- Für  $a \in R \setminus \{0\}, f \in R[x] \setminus \{0\}$  gilt  $I(af) \sim aI(f)$ .
- Falls  $f \in R[x]$  irreduzibel ist, so ist entweder  $f \in R$  oder  $f$  ist primitiv. (Grad  $f = 0 \Rightarrow f \in R$ , Grad  $f > 0 \Rightarrow f = af^*, a \in R, f^*$  primitiv. Folgt  $a$  oder  $f^*$  ist eine Einheit  $\Rightarrow \deg(f^*) = \deg(f) > 0$  also  $f^*$  ist keine Einheit)

**Lemma.** Sei  $R$  ein faktorieller Ring und  $K = \text{Quot}(R)$ . Dann hat jedes  $f \in K[x] \setminus \{0\}$  eine Darstellung  $f = df^*$  wobei  $d \in K^\times$  und  $f^* \in R[x]$  ist primitiv. Diese Darstellung ist bis auf Assoziierung eindeutig:

Falls  $f = d_1 f_1^* = d_2 f_2^*, d_1, d_2 \in K^\times, f_1^*, f_2^* \in R[x]$  primitiv, dann ist  $d_1 \sim_R d_2, f_1^* \sim_R f_2^*$ .

Wobei  $\sim_R$  assoziiert über eine Einheit in  $R$  bedeutet.

*Beweis.* Sei  $f = \sum_{i=0}^n \underbrace{a_i}_{\in K} x^i \in K[x] \setminus \{0\}$  und  $a_i = \frac{b_i}{c_i}$  für  $b_i, c_i \in R, c_i \neq 0$  für  $i = 0, \dots, n$ . Wir definieren

$$g = \left( \prod_{i=0}^n c_i \right) f \in R[x]$$

Sei  $\underbrace{d}_{\in R} \sim I(g)$  ein ggT der Koeffizienten von  $g$ . Dann ist  $g = d'g^*$  für ein primitives  $g^* \in R[x]$ .

$$\Rightarrow f = \frac{d'}{\underbrace{\prod_{i=0}^n c_i}_d} \underbrace{g^*}_{f^*} \quad \text{mit} \quad d \in K^\times, f^* \in R[x] \text{ primitiv.}$$

Wir erhalten die Existenzaussage im Lemma.

Sei nun  $f = d_1 f_1^* = d_2 f_2^*$ . Wir schreiben  $\frac{d_1}{d_2} = \frac{a_1}{a_2}$  mit  $a_1, a_2 \in R$  coprim.

$$f_2^* = \frac{d_1}{d_2} f_1^* = \frac{a_1}{a_2} f_1^* \Rightarrow a_1 f_1^* = a_2 f_2^* \Rightarrow a_1 \sim I(a_1 f_1^*) \sim I(a_2 f_2^*) \sim a_2.$$

Aus  $a_1, a_2$  coprim folgt nun  $a_1 \sim 1 \sim a_2$ .

Wir haben also  $\frac{d_1}{d_2} \in R^\times$  gezeigt was genau  $d_1 \sim_R d_2$  und  $f_1^* \sim_R f_2^*$  bedeutet.  $\square$

**Definition.** Für  $f \in K[x] \setminus \{0\}$  nennen wir das  $d \in K^\times$  mit  $f = df^*, f^* \in R[x]$  primitiv, wieder den *Inhalt* von  $f$ .

**Proposition (Gauss).** Sei  $R$  faktoriell. Für  $f, g \in R[x]$  gilt  $I(fg) \sim I(f)I(g)$ . Insbesondere ist das Produkt von primitiven Elementen von  $R[x]$  wieder primitiv.

Im folgenden werden wir die „Reduktion der Koeffizienten“ verwenden: Für ein  $p \in R$  gibt es einen Ringhomomorphismus  $f \in R[x] \mapsto f \bmod p \in R/(p)[x], \sum_{i=0}^n a_i X^i \mapsto \sum_{i=0}^n (a_i + (p)) X^i$ . Dies folgt aus dem Satz von 4. VO (wobei  $\varphi(a) = a + (p)$  und  $\Phi(X) = X$ ).



*Beweis.* Wir zeigen zuerst die zweite Aussage der Proposition. Seien also  $f, g \in R[x]$  primitive Polynome. Sei  $p \in R$  ein Primelement. Dann gilt  $f \bmod p \neq 0$  und  $g \bmod p \neq 0$ . Da  $p$  ein Primelement ist, ist  $R/(p)$  ein Integritätsbereich. Daraus folgt, dass  $R/(p)[x]$  auch ein Integritätsbereich ist. Daher ist also

$$(fg) \bmod p = f \bmod p g \bmod p \neq 0.$$

Anders formuliert, sind also nicht alle Koeffizienten von  $fg$  durch  $p$  teilbar. Da  $p \in R$  ein beliebiges Primelement war, sehen wir, dass  $fg$  ein primitives Polynom ist.

Seien nun  $f, g \in K[x] \setminus \{0\}$  beliebig. Dann gilt  $f = af^*, g = bg^*$  für  $a \sim I(f), b \sim I(g), f^*, g^* \in R[x]$  primitiv.

$$\Rightarrow fg = ab \underbrace{f^* g^*}_{\in R[x]}$$

ist primitiv. Aus der Eindeutigkeit im Lemma folgt nun  $I(fg) \sim_R ab \sim_R I(f)I(g)$  □

**Satz (Gauss).** *Sei  $R$  ein faktorieller Ring. Dann ist auch  $R[x]$  faktoriell. Des Weiteren hat  $R[x]$  genau die beiden Typen von Primelementen:*

- $p \in R$  prim ist auch ein Primelement von  $R[x]$ .
- $f \in R[x]$  primitiv so dass  $f$  irreduzibel als Element von  $K[x]$  ist, ist ein Primelement von  $R[x]$ .

**Korollar.** *Sei  $f \in R[x]$  primitiv. Dann ist  $f$  irreduzibel als Element von  $R[x]$  gdw.  $f$  ist irreduzibel als Element von  $K[x]$ .*

*Beweis.* Wir zeigen zuerst, dass die beiden Typen von Primelementen im Satz tatsächlich Primelemente von  $R[x]$  sind.

- Sei  $p \in R$  ein Primelement. Dann ist

$$R[x]/(p)_{R[x]} \cong R/(p)_R[x]. \quad (*)$$

Warum:  $\Phi : R[x] \rightarrow R/(p)_R[x], f \mapsto f \bmod p$  ist ein Ringhomomorphismus. Der Kern von  $\Phi$  besteht aus allen  $f \in R[x]$  so dass  $p$  alle Koeffizienten teilt - oder aus  $\text{Ker}(\Phi) = (p)_{R[x]}$ . Also folgt (\*) aus dem ersten Isomorphiesatz.

Da  $R/(p)_R[x]$  ein Integritätsbereich ist, folgt, dass  $p \in R[x]$  ein Primelement ist.

- Sei  $f \in R[x]$  primitiv und als Element von  $K[x]$  irreduzibel. Wir wollen zeigen, dass  $f$  ein Primelement in  $R[x]$  ist.

Angenommen  $f \mid gh$  in  $R[x]$  für  $g, h \in R[x]$ . Folgt  $f \mid gh$  in  $K[x]$ , da  $gh = qf$  für  $q \in K[x] \subseteq K[x]$ . Da  $f \in K[x]$  irreduzibel/prim ist, folgt  $f \mid g$  oder  $f \mid h$ . O.B.d.A. nehmen wir an  $f \mid g$ . Dann existiert ein  $q \in K[x]$  mit  $g = qf$ . Aus der Proposition folgt

$$I(q) \sim_R I(q) \underbrace{I(f)}_{\sim_R 1} \sim_R I(qf) \sim_R I(g) \in R$$

also auch  $I(q) \in R$ . Da  $q \sim I(q)q^*$  folgt also  $q \in R[x]$ . Wir sehen also  $f \mid g$  in  $R[x]$ .

Also sehen wir, dass  $f$  ein Primelement von  $R[x]$  ist.

Als nächstes wollen wir zeigen, dass jedes irreduzible Element  $f \in R[x]$  ein Element vom Typ 1 oder Typ 2 wie im Satz ist. Da diese Elemente bereits als Primelemente in  $R[x]$  bekannt sind, folgt daraus insbesondere dass alle irreduziblen Elemente in  $R[x]$  auch Primelemente sind.

Sei also  $f \in R[x]$  irreduzibel.

- Falls  $\deg(f) = 0$  ist, so ist  $f \in R$  irreduzibel ( $R[x]^\times = R^\times$ ). Also ist  $f \in R$  prim nach Annahme an  $R$  und  $f$  ist vom Typ 1 und prim in  $R[x]$ .

- Sei nun  $\deg(f) > 0$ . Daraus folgt  $f$  ist primitiv. Wir müssen zeigen, dass  $f$  als Element von  $K[x]$  irreduzibel ist. Dann ist  $f$  vom Typ 2 und prim in  $R[x]$ .

Angenommen  $f = gh$  für  $g, h \in K[x]$ . Nach einem früheren Lemma gilt  $g = cg^*, h = dh^*$   $c, d \in K, g^*, h^* \in R[x]$  primitiv.  $\Rightarrow f = (cd)g^*h^*$ , wobei  $g^*, h^*$  primitiv ist (siehe frühere Proposition).  $I(f) \sim 1 \sim cd$ , womit  $cd \in R^\times$ . Also ist  $f = (cdg^*)h^*$  eine Zerlegung von  $f$  als Produkt von  $cdg^* \in R[x]$  und  $h^* \in R[x]$ . Da  $f$  in  $R[x]$  irreduzibel ist, ist  $cdg^*$  oder  $h^*$  eine Einheit in  $R[x]$ . Dies zeigt, dass  $f$  in  $K[x]$  irreduzibel ist.

Es bleibt zu zeigen, dass jedes  $f \in R[x] \setminus \{0\}$  ein endliches Produkt von endlich vielen Primelementen von  $R[x]$  ist. Auf Grund des früheren Lemmas gilt  $f = df^*$ , wobei  $d \in R \setminus \{0\}$  und  $f^* \in R[x]$  primitiv ist.  $d \in R \setminus \{0\}$  ist dabei ein endliches Produkt von Primelementen in  $R$  (welche Primelemente in  $R[x]$  vom Typ I sind und einer Einheit) - weil  $R$  faktoriell ist.  $f^* \in R[x]$  ist ein endliches Produkt von Primelementen vom Typ II und einer Einheit - wir können dies mittels Induktion nach dem Grad beweisen.

$\deg(f^*) = 0 \Rightarrow f^* \in R^*$  (Produkt ohne Primfaktoren)

$\deg(f^*) = 1 \Rightarrow f^*$  ist selbst irreduzibel, da  $f^*$  primitiv ist und als Element von  $K[x]$  irreduzibel ist.

Falls die Aussage für alle primitiven Elemente vom Grad kleiner als  $\deg(f^*)$  von bekannt ist, so unterscheiden wir die Fälle

- $f^*$  ist irreduzibel  $\checkmark$ .
- $f^* = gh$  für  $g, h \in R[x]$  (automatisch primitiv) beide nicht Einheiten.

Nach Induktionsannahme sind daher sowohl  $g$  als auch  $h$  endliche Produkte von Primelementen, womit dies auch für  $f^*$  gilt.  $\square$

**Lemma.** Sei  $K$  ein Körper und  $a \in K$ . Dann gilt für jedes  $f \in K[x]$

$$f(x) = (x - a)g(x) + r \quad \text{für} \quad g(x) \in K[x], r \in K.$$

Daher gilt  $f(a) = 0 \Leftrightarrow (x - a) \mid f(x)$ .

**Proposition.** Sei  $K$  ein Körper. Dann sind lineare Polynome der Form  $x - a$  für  $a \in K$  irreduzibel als Elemente von  $K[x]$ . Für quadratische ( $\deg(f) = 2$ ) und kubische ( $\deg(f) = 3$ ) Polynome  $f \in K[x]$  gilt

$$f \text{ ist irreduzibel} \Leftrightarrow f \text{ hat keine Nullstelle } (\forall a \in K \text{ gilt } f(a) \neq 0)$$

*Beweis.*  $\Leftarrow$ : Falls  $\deg(f) \in \{2, 3\}$  und  $f = gh$ ,  $g, h \notin K[x]^\times$ , dann gilt  $\deg(f) = \deg(g) + \deg(h)$  und daher ist mindestens ein Faktor von Grad 1. Falls  $\deg(g) = 1$  ist, so hat  $g$  eine Nullstelle und  $f(x) = g(x)h(x)$  ebenso.

$\Rightarrow$ : Falls  $f$  irreduzibel ist, so kann  $f$  wegen dem Lemma keine Nullstelle haben.  $\square$

**Satz** (Fundamentalsatz der Algebra). Jedes Polynom  $f \in \mathbb{C}[x]$  mit  $\deg(f) > 0$  hat eine Nullstelle in  $\mathbb{C}$ .

Die irreduziblen Elemente von  $\mathbb{C}[x]$  sind genau die linearen Polynome. Insbesondere hat jedes  $f \in \mathbb{C}[x]$  eine Faktorisierung in Linearfaktoren

$$f(x) = a \prod_{j=1}^{\deg(f)} (x - z_j).$$

für gewisse  $a \in \mathbb{C} \setminus \{0\}$  und  $z_1, \dots, z_{\deg(f)} \in \mathbb{C}$ .

**Korollar** (Fundamentalsatz für  $\mathbb{R}$ ). Ein Polynom in  $\mathbb{R}[x]$  ist irreduzibel gdw. entweder  $\deg(f) = 1$  ist oder  $\deg(f) = 2$  ist und  $f$  keine Nullstellen in  $\mathbb{R}$  besitzt.

*Beweis.* Wir müssen  $\Rightarrow$  beweisen. Nach obigem Satz gibt es für jedes  $f \in \mathbb{R}[x]$  mit  $\deg(f) > 0$  eine Nullstelle  $z \in \mathbb{C}$ . Falls  $z = a \in \mathbb{R}$  ist, so folgt  $(x - a) \mid f(x)$  also  $f(x) \sim (x - a)$ . Falls  $z \notin \mathbb{R}$  ist, so folgt  $0 = \overline{0} = \overline{f(z)} = f(\bar{z})$ . Daher hat  $f(x)$  in  $\mathbb{C}[x]$  die Teiler  $x - z$  und  $x - \bar{z}$ .

$$\Rightarrow (x - z)(x - \bar{z}) = (x^2 - \underbrace{(z + \bar{z})x}_{2 \operatorname{Re}(z)} + \underbrace{\bar{z}z}_{|z|^2}) \mid f(x) \text{ in } \mathbb{C}[x]$$

und auch in  $\mathbb{R}[x]$  z.B. wegen der Polynomdivision. Daher gilt  $f(x) \sim (x^2 - (2 \operatorname{Re}(z)x + |z|^2))$  und  $\deg(f) = 2$ ,  $f$  hat keine reellen Nullstellen.  $\square$

**Proposition.** Sei  $R$  ein faktorieller Ring. Sei  $f \in R[x]$  und  $\frac{a}{b} \in K$  mit  $b \neq 0, (a, b)$  coprime. Falls  $f(\frac{a}{b}) = 0$  ist, so ist  $b$  ein Teiler von führenden Koeffizienten von  $f$  und  $a$  ein Teiler vom konstanten Term von  $f$ .

*Beweis.* Wir nehmen an  $f(\frac{a}{b}) = 0$  an. Also gilt  $(x - \frac{a}{b}) \mid f(x)$  in  $K[x]$ . Und auch  $(bx - a) \mid f(x)$  in  $K[x]$ . Dann gilt sogar  $(bx - a) \mid f(x)$  in  $R[x]$ .

Denn: Angenommen  $f(x) = (bx - a)h(x)$  für  $h(x) \in K[x]$ . Für den Inhalt der Polynome gilt daher  $I(f) \in R$ .

$$I(f) = I((bx - a)h(x)) \sim I(bx - a)I(h) \sim I(h) \in R(h = ch^*, c \sim I(h)).$$

Also folgt  $h(x) \in R[x]$  und daher  $(bx - a) \mid f(x)$  in  $R[x]$ .

Also  $f(x) = (bx - a)h(x)$  für  $h(x) \in R[x]$ .  $\Rightarrow$  führender Koeffizient von  $f = b \cdot$  (führender Koeffizient von  $h$ ). Und Konstanter Term von  $f = -a \cdot$  (konstanter Term von  $h$ ).  $\square$

**Beispiel.** Für welche  $a \in \mathbb{Z}$  ist  $f_a(x) = x^2 + ax + 1 \in \mathbb{Z}[x]$  irreduzibel?

Wegen der Proposition ist eine Nullstelle von  $f_a(x)$  in  $\mathbb{Q}$  automatisch  $\pm 1$  ( $f_a(\frac{p}{q}) = 0 \Rightarrow p \mid 1, q \mid 1 \Rightarrow \frac{p}{q} = \pm 1$ ).

$$f_a(1) = 2 + a1 = 0 \Leftrightarrow a = -2 \quad f_a(-1) = 2 - a = 0 \Leftrightarrow a = 2.$$

Hier ist  $f_a$  reduzibel. Für  $a \in \mathbb{Z} \setminus \{\pm 2\}$  ist  $f_a \in \mathbb{Z}[x]$  irreduzibel ( $f_a$  ist primitiv und  $f_a \in \mathbb{Q}[x]$  ist irreduzibel da  $f_a$  keine Nullstellen hat).

**Beispiel.** Sei  $K$  ein Körper. Dann ist  $f(x, y) = y^3 - x^5 \in K[x, y]$  irreduzibel. In diesem Fall wollen wir das Diskutierte für  $R = K[x]$  verwenden und den Polynomring  $R[y]$ . Wir bemerken zuerst, dass  $f \in R[y]$  primitiv ist (da  $f$  als Polynom in  $y$  normiert ist und Koeffizienten in  $K[x]$  besitzt). Daher (Korollar von Satz von Gauss) ist  $f \in R[y]$  irreduzibel gdw.  $f$  als Element von  $\underbrace{\operatorname{Quot}(R)}_{K[x]}[y]$  irreduzibel ist.

Wir nehmen an,  $f$  ist nicht irreduzibel als Element von  $K(x)[y]$ . Also muss  $f$  eine Nullstelle in  $K(x)$  besitzen. Seien  $p, q \in K[x]$  coprime,  $q \neq 0$  mit  $f(\frac{p}{q}) = 0$ . Folgt  $q \mid 1$ . Also o.B.d.A.  $q = 1$  und  $f(p) = 0$ ,  $f(y) = y^3 - x^5 \Rightarrow p(x)^3 = x^5$  in  $K[x]$ . Insbesondere  $p(x) \mid x^5$ , also  $p(x) = ax^k \Rightarrow p(x)^3 = a^3 x^{3k} = x^5$  ist unmöglich. Dieser Widerspruch zeigt, dass  $f(y)$  keine Nullstelle in  $K(x)$  hat. Folgt  $f(y)$  ist irreduzibel als Element von  $K(x)[y]$  und primitiv in  $(K[x])[y]$  und daher irreduzibel in  $K[x, y]$ .

# Anhang A: Auswahlaxiom und das Zornsche Lemma

**Auswahlaxiom** (in der Mengenlehre)

Sei  $I$  eine nichtleere Menge und seien  $X_i$  für  $i \in I$  nichtleere Mengen. Dann ist  $\prod_{i \in I} X_i \neq \emptyset$ , d.h. es existiert eine Funktion

$$f : I \rightarrow \bigcup_{i \in I} X_i$$

mit  $f(i) \in X_i$  für alle  $i \in I$ .

*Bemerkung.* • unabhängig von den anderen ZF-Axiomen der Mengenlehre

- kritisiert wegen der Nichtkonstruktivität des Axioms und mancher scheinbar paradoxen Folgerung
- notwendig für einen großen Teil der Mathematik

Häufig wird nicht das Auswahlaxiom sondern ein dazu äquivalentes Lemma, das Zornsche Lemma, verwendet. Für dieses benötigen wir etwas mehr Begriffe:

**Definition.** Sei  $X$  eine Menge. Eine *Ordnung* auf  $X$  ist eine Relation  $\leq$  so dass

- 1) reflexivität:  $x \leq x$
- 2) antisymmetrie:  $x \leq y$  und  $y \leq x$
- 3) transitivität:  $x \leq y$  und  $y \leq z \Rightarrow x \leq z$  für alle  $x, y, z \in X$ .

Die Ordnung heißt *total* oder *linear* falls zusätzlich

- 4) linearität:  $x \leq y$  oder  $y \leq x$

gilt. Ansonsten heißt sie *partiell*.

**Beispiel.** •  $\leq$  in  $\mathbb{R}$  ist total

- $|$  in  $\mathbb{Z}$  partiell, da  $2X3$  und  $3X2$ .
- $\subseteq$  auf  $\mathcal{P}(A) = \{B \subseteq A\}$

**Definition.** Sei  $\leq$  eine Ordnung auf einer Menge  $X$ . Ein Element  $x \in X$  heißt *maximal* falls für alle  $y \in X$  gilt  $x \leq y \Rightarrow x = y$ . Ein Element  $m \in X$  ein *Maximum* falls  $x \leq m$  für alle  $x \in X$  gilt.

**Definition.** Sei  $\leq$  eine Ordnung auf einer Menge  $X$  und sei  $A \subseteq X$ . Ein Element  $x \in X$  heißt eine *obere Schranke* von  $A$  falls  $a \leq x$  für alle  $a \in A$ . Analog definiert man *untere Schranke* von  $A$ .

**Definition.** Sei  $\leq$  eine Ordnung auf einer Menge  $X$ . Eine Teilmenge  $K \subseteq X$  heißt eine *Kette* falls für alle  $x, y \in K$  gilt  $x \leq y$  oder  $y \leq x$ . Wir sagen die Ordnung  $\leq$  sei *induktiv* falls jede Kette in  $X$  eine obere Schranke besitzt.

**Satz** (Zornsches Lemma). *Sei  $\leq$  eine induktive Ordnung auf einer Menge  $X$ . Dann existiert ein maximales Element in  $X$ .*

**Typische Anwendung:** Jeder Vektorraum über  $K$  hat eine Hamel-Basis.

*Beweisidee.* Ausgehend von der leeren Menge (die eine Kette darstellt) wollen wir Elemente einer immer Länger werdenden Kette finden, wobei wir immer wieder eine obere Schranke hinzufügen

wollen - sofern dies möglich ist.

...

⇒ eine Art Induktion

**Problem:** Die Vereinigung von Ketten muss keine Kette sein. □

Vorerst einige Definitionen und Lemmata:

**Definition.** Für eine Teilmenge  $C \subseteq X$  definieren wir

$$\widehat{C} = \{x \in X \setminus C \mid x \text{ ist eine obere Schranke}\}.$$

Um die Beweisidee umzusetzen verwenden wir eine *Auswahlfunktion* auf der Menge  $\{\widehat{C} : C \subseteq X \text{ s.d. } \widehat{C} \neq \emptyset\}$

**Definition.** Eine Teilkette  $K \subseteq X$  heißt eine *f-Kette* falls für jede Teilmenge  $C \subseteq K$  mit  $\widehat{C} \cap K \neq \emptyset$  das Element  $f(\widehat{C})$  zu  $K$  gehört und eine minimale obere Schranke von  $C$  in  $K$  ist, also  $f(\widehat{C}) \leq y$  für alle  $y \in \widehat{C} \cap K$  gilt. Dies vermeidet „unnötige Zwischenschritte“, die zu Problemen bei einer Vereinigung von Ketten führen würde.

**Beispiel.**  $K_{\min} = \emptyset$ ,  $\widehat{K}_{\min} = X$  ist eine *f-Kette*, die in jeder anderen *f-Kette* enthalten ist.  $K_1 = \{f(\widehat{K}_{\min})\} = K_{\min} \cup \{f(\widehat{K}_{\min})\}$  ist eine weitere *f-Kette*, die in jeder anderen nichtleeren *f-Kette* enthalten ist.

- $\widehat{\emptyset} = X \Rightarrow f(x) \in X$  ist definiert
- $K_{\min}$  ist eine *f-Kette*:  $C = \emptyset$  und  $f(\widehat{\emptyset}) \in K_{\min}$  ist minimal  $C = K_{\min}$  erfüllt  $\widehat{C} \cap K_{\min} = \emptyset$
- Falls  $K$  eine *f-Kette* ist, so können wir  $C = \emptyset$  in der Definition verwenden und erhalten  $f(\widehat{\emptyset}) \in K$ , also  $K_{\min} \subseteq K_1 \subseteq K$ .

**Lemma** (Verlängerung). Falls  $K$  eine *f-Kette* ist und  $\widehat{K} \neq \emptyset$  ist, so ist  $K_{\text{neu}} = K \cup \{f(\widehat{K})\}$  wieder eine *f-Kette*.

*Beweis.* Sei  $C \subseteq K_{\text{neu}}$ .

- Falls  $\widehat{C} \cap K \neq \emptyset$  ist, so gilt  $C \subseteq K$ ,  $f(\widehat{C}) \in K$  und  $f(\widehat{C})$  ist eine minimales Element von  $\widehat{C} \cap K$  (da  $K$  eine *f-Kette* ist). Damit ist aber auch  $f(\widehat{C}) \in K_{\text{neu}}$  und  $f(\widehat{C})$  ist ein minimales Element von  $\widehat{C} \cap K_{\text{neu}}$  (da  $f(\widehat{K})$  eine obere Schranke von  $K$  ist).
- Falls  $C \subseteq K$  und  $\widehat{C} \cap K = \emptyset$ , dann ist  $\widehat{C} = \widehat{K}$ , da  $K$  eine Kette ist gilt  $\widehat{C} \supseteq \widehat{K}$ . Sei  $x \in \widehat{C}, k \in K \Rightarrow k \neq \widehat{C}$ , also existiert ein  $c \in C$  mit  $k \leq c \leq x \Rightarrow x$  ist eine obere Schranke von  $K$  und  $x \notin K$  also  $x \in \widehat{K}$  und somit  $\widehat{C} \in \widehat{K}$ .  
Folglich ist  $f(\widehat{C}) = f(\widehat{K}) \in K_{\text{neu}}$  eine minimale obere Schranke von  $C$  in  $K_{\text{neu}}$ .
- Falls  $f(\widehat{K}) \in C$ , so ist  $\widehat{C} \cap K_{\text{neu}} = \emptyset$  und es gibt nichts zu beweisen.

□

**Lemma** (Zwei *f-Ketten*). Angenommen  $K, K'$  sind zwei *f-Ketten* und  $K' \setminus K \neq \emptyset$ . Dann ist  $K \subseteq K'$  und es gilt  $x \leq x'$  für alle  $x \in K$  und  $x' \in K' \setminus K$ .

Informell: „ $K$  ist eine Anfangsabschrift von  $K'$ “.

*Beweis.* Sei  $x' \in K' \setminus K$ . Wir definieren

$$C = \{x \in K \cap K' : x \leq x'\} \subseteq K' \cap K$$

und verwenden, dass  $K'$  eine *f-Kette* ist. Da  $x' \in \widehat{C} \cap K'$  ist, folgt  $f(\widehat{C}) \in K'$  und  $f(\widehat{C}) \leq x'$ . Falls  $\widehat{C} \cap K \neq \emptyset$  wäre, so wäre  $f(\widehat{C}) \in K$  (da  $K$  eine *f-Kette* ist) womit aber  $f(\widehat{C}) \in C \cap \widehat{C}$  der Definition von  $\widehat{C}$  widerspricht.

Also ist  $\widehat{C} \cap K = \emptyset$ . In anderen Worten bedeutet dies, dass es zu jedem  $x \in K$  ein  $c \in C$  mit

$x \leq c$  geben muss. Nach Definition von  $C$  folgt daher  $x \leq c \leq x'$ . Also  $x \leq x'$  für alle  $x \in K$ . Unsere Annahmen an  $K$  und  $K'$  war bloss, dass es  $x' \in K' \setminus K$  gibt. Daraus folgt nun auch  $K \subseteq K'$ , denn ansonsten könnten wir die Rollen von  $K$  und  $K'$  vertauschen.  $\square$

**Lemma** (Vereinigung). *Wir definieren  $K_{max} = \bigcup_{f\text{-Kette}} K$ . Dann ist  $K_{max}$  eine  $f$ -Kette.*

*Beweis.* Da für je zwei Ketten  $K, K'$   $K \subseteq K'$  oder  $K' \subseteq K$  gilt, sehen wir, dass  $K_{max}$  wieder eine Kette ist. Wir müssen noch zeigen, dass  $K_{max}$  eine  $f$ -Kette ist und nehmen hierzu eine Teilmenge  $C \subseteq K_{max}$  mit  $\widehat{C} \cap K_{max} \neq \emptyset$ . Sei  $x' \in \widehat{C} \cap K_{max}$  und sei  $K'$  eine  $f$ -Kette mit  $x' \in K'$ .

**Behauptung:**  $C \subseteq K'$ .

Sei also  $x \in C$ , dann existiert eine  $f$ -Kette  $K$  mit  $x \in K$ . Nach obigem Lemma gilt  $K \subseteq K'$  ( $\Rightarrow x \in K' \checkmark$ ) oder  $K' \subseteq K$ . Woraus folgt  $K'$  enthält wegen obigem Lemma alle Elemente von  $K$  unterhalb von  $x'$ . Da  $x' \in \widehat{C}$  und  $x \in C$  folgt  $x \leq x'$  und  $x \in K'$ .

Da  $C \subseteq K'$ ,  $c \in \widehat{C} \cap K'$  und da  $K'$  eine  $f$ -Kette ist, folgt nun  $f(\widehat{C}) \in K' \subseteq K_{max}$  und  $f(\widehat{C}) \leq x'$ . Da  $x' \in \widehat{C} \cap K_{max}$  beliebig war, sehen wir, dass  $f(\widehat{C}) \in K_{max}$  ein minimales Element von  $\widehat{C} \cap K_{max}$  ist. Dies zeigt aber, dass  $K_{max}$  eine  $f$ -Kette ist.  $\square$

*Beweis vom Zornschen Lemma.*  $K_{max}$  ist nach Definition eine größte  $f$ -Kette in  $X$ . Insbesondere ist also das erste Lemma nicht anwendbar, d.h.  $\widehat{K}_{max} = \emptyset$ .

Des Weiteren ist aber  $K_{max}$  eine Teilkette, die nach Annahme an  $\leq$  eine obere Schranke  $x_{max}$  besitzen muss. Es folgt also  $x_{max} \in K_{max}$  ist ein Maximum von  $K_{max}$  und auch, dass  $x_{max}$  ein maximales Element von  $X$  ist.  $\square$