

# Inhaltsverzeichnis

<b>1. Einführung</b>	<b>2</b>
1.1. Algebra . . . . .	2
1.2. Geschichtlicher Überblick . . . . .	2
1.3. Polynomielle Gleichungen . . . . .	3
1.4. Zahlentheorie . . . . .	4
1.4.1. Kurze Diskussion zu ggT . . . . .	5
1.5. Geometrie . . . . .	5
<b>2. Kommutative Ringe</b>	<b>6</b>
2.1. Ringe . . . . .	6
2.2. Einheiten, Teilbarkeit, Quotientenkörper (Seite 34) . . . . .	9
2.3. Ring der Polynome (Seite 41) . . . . .	11
2.4. Ideale und Faktorringe . . . . .	16
2.5. Charakteristik eines Körpers . . . . .	21
2.6. Primideale und Maximalideale . . . . .	22
2.7. Unterring . . . . .	24
2.8. Matrizen . . . . .	25
<b>3. Faktorisierungen von Ringen</b>	<b>27</b>
3.1. Euklidische Ringe . . . . .	27
3.2. Hauptidealring . . . . .	30
<b>A. Auswahlaxiom und das Zornsche Lemma</b>	<b>33</b>

# 1. Einführung

## 1.1. Algebra

### Was ist Algebra?

1. Gruppen und Wirkungen
2. Ringe und Module
3. Körpertheorie

**Wozu ist Algebra gut?** Zentrale Grundlage für die reine Mathematik.

**Was sind die möglichen Ziele dieser Vorlesung?** Grundlagen schaffen. Viele tolle Sätze und Zusammenhänge schaffen.

## 1.2. Geschichtlicher Überblick

Algebra vom Arabischen al-gabr, „das Zusammenfügen gebrochener Teile“ (Äquivalenzumformungen).

Epochen:

1. Babylonier ca. 2000 v.Chr.
2. Griechen 600 v. - 300 v.Chr.
3. Inder 5. - 7. Jhdt.
4. Araber 8. - 13. Jhdt.
5. Italiener 16. Jhdt.
6. Leibniz
7. Lineare Algebra
8. E. Galois
9. E. Noether ( $\sim$  1930)

## 1.3. Polynomielle Gleichungen

### Quadratische Gleichung

$$x^2 + px + q = 0 \Rightarrow x^2 + 2\frac{p}{2}x + \frac{p^2}{4} = \frac{p^2}{4} - q \Rightarrow (x + \frac{p}{2})^2 = \frac{p^2}{4} - q \Rightarrow x = -\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q}$$

### Kubische Gleichung $a, b, c$ gegeben.

$$x^3 + ax^2 + bx + c = 0$$

Wir setzen  $x = y - \frac{a}{3}$ , dann ist

$$x^3 = (y - \frac{a}{3})^3 = y^3 - 3\frac{a}{3}y^2 + 3(\frac{a}{3})^2y - (\frac{a}{3})^3$$

$$ax^2 = a(y - \frac{a}{3})^2 = a(y^2 - 2\frac{a}{3}y + (\frac{a}{3})^2)$$

$$bx = \dots$$

---

$$y^3 + py + q = 0$$

Ansatz:  $y = g + h$ .

$$g^3 + 4g^2h + 4gh^2 + h^3 + p(g + h) + q = 0$$

$$\underbrace{g^3 + h^3 + q}_{=0} + \underbrace{(3gh + p)(g + h)}_{=0} = 0$$

$$g^3 + h^3 = -q \quad \text{und} \quad gh = -\frac{p}{3}.$$

Sei  $G = g^3, H = h^3$ . Dann folgt  $G + H = -q$  und  $GH = -(\frac{p}{3})^3$ . Folgt  $G(-q - G) = -\frac{p^3}{27}$ . Dies können wir mit der Quadratischen Gleichung lösen. Die sich daraus ergebende Formel wird auch die Cardano-Formel genannt. Hat eine Kubischegleichung drei reelle Lösungen so verwendet jede Lösungsformel zur Berechnung dieser Komplexe Zahlen (Casus Irreduzibiles).

**Quadratische Gleichung** Diese wurde kurz danach von Ferrari gelöst. Herleitung siehe Buch.

**Gleichung 5. Grades** 1824 Abel: es kann keine Formel mit Wurzel ausdrücken geben.  
1830 Galois: Vollständige Erklärung und Erfindung der Gruppentheorie zu diesem Zweck.

## 1.4. Zahlentheorie

$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$$

wobei  $\mathbb{N}$  die 0 enthält. In  $\mathbb{N}$  und in  $\mathbb{Z}$  gibt es Primzahlen.

**Satz.** Es gibt in  $\mathbb{Z}$  eine eindeutige Primfaktorzerlegung. Jede Zahl  $n \in \mathbb{Z} \setminus \{0\}$  lässt sich als Produkt

$$n = \varepsilon \cdot p_1^{k_1} \cdot \dots \cdot p_l^{k_l}.$$

schreiben, wobei  $\varepsilon = \pm 1$ ,  $l \in \mathbb{N}$ ,  $p_1, \dots, p_l > 0$  Primzahlen sind und  $k_1, \dots, k_l \in \mathbb{N}_{>0}$  sind. Diese Darstellung ist bis auf die Reihenfolge der Primzahlen eindeutig.

Welche Zahle in  $\mathbb{N}$  sind Summen von zwei Quadratzahlen? z.B. 3 geht nicht,  $5 = 4 + 1$

Was sind die Primzahlen in  $\mathbb{Z}[i] = \{a + ib : a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$ ? z.B.  $5 = (2 + i)(2 - i)$  ist keine Primzahl in  $\mathbb{Z}[i]$ , 3 ist eine.

Sehr nützlich für diese Frage ist:

**Definition.** Wir schreiben für  $a, b, m \in \mathbb{Z}$ , dass  $a \equiv b \pmod{m}$  falls  $m$  die Differenz  $b - a$  teilt (also falls es ein  $k \in \mathbb{Z}$  gibt mit  $b - a = km$ )

Dies definiert eine Äquivalenzrelation (für festes  $m \in \mathbb{Z}$ ). Der Quotientenraum wird mit

$$\mathbb{Z}_m = \mathbb{Z}/\mathbb{Z}_m = \{a + \mathbb{Z}_m : a \in \mathbb{Z}\}$$

bezeichnet.

**Lemma.** Addition und Multiplikation auf  $\mathbb{Z}$  definieren auch wohldefinierte Addition und Multiplikation auf  $\mathbb{Z}_m$ . D.h. für festes  $m$  gilt:  $a_1 \equiv a_2$  und  $b_1 \equiv b_2 \pmod{m} \Rightarrow a_1 + b_1 \equiv a_2 + b_2$  und  $a_1 \cdot b_1 \equiv a_2 \cdot b_2 \pmod{m}$ .

*Beweis.* Nach Annahme gilt

$$a_2 - a_1 = km$$

$$b_2 - b_1 = lm$$

---


$$(a_2 + b_2) - (a_1 + b_1) = (k + l)m$$

was bedeutet  $a_1 + b_1 \equiv a_2 + b_2 \pmod{m}$ . Multiplikation analog. □

**Lemma.** Die einzigen Quadratzahlen in  $\mathbb{Z}_4$  sind 0 und 1. Daher sind die Zahlen 3, 7, 11, 15, 19, ... keine Summen von zwei Quadratzahlen in  $\mathbb{N}$ .

*Beweis.*  $0^2 \equiv 0, 1^2 \equiv 1, 2^2 \equiv 0, 3^2 \equiv 1 \pmod{4}$ . Wenn  $n = k^2 + l^2$  dann gilt modulo 4, dass

$$n \equiv k^2 + l^2 \equiv \begin{cases} 0 \\ 1 \end{cases} + \begin{cases} 0 \\ 1 \end{cases} \equiv 0, 1, 2 \pmod{4}.$$

Also können die Zahlen  $3, 7, 11, \dots \equiv 3 \pmod{4}$  keine Summen von zwei Quadratzahlen sein. □

### 1.4.1. Kurze Diskussion zu ggT

**Proposition.** Für je zwei natürliche Zahlen  $a, b \in \mathbb{N}_{>0}$  gibt es einen größten gemeinsamen Teiler  $d > 0$ . Dieser erfüllt  $\mathbb{Z}a + \mathbb{Z}b = \mathbb{Z}d$ .

*Beweis.* Wir bemerken zuerst, dass  $I = \mathbb{Z}a + \mathbb{Z}b = \{ka + lb : k, l \in \mathbb{Z}\}$  unter Addition und Multiplikation mit Elementen in  $\mathbb{Z}$  abgeschlossen ist. Da  $\mathbb{N}$  wohlgeordnet ist gibt es in  $I \cap \mathbb{N}_{>0}$  ein kleinstes Element  $d > 0$ . Sei nun  $m \in I$ . Dann können wir in  $\mathbb{Z}$  Division mit Rest verwenden, d.h.

$$\underbrace{m}_{\in I} = k \underbrace{d}_{\in I} + r \quad k \in \mathbb{Z}, r \in \{0, \dots, d-1\}.$$

Also ist auch  $k \cdot d$  in  $I$  und daher  $r = m - kd \in I$ ,  $r \geq 0$  und  $r < d$ . Folgt  $r = 0$  wegen der Definition von  $d \in I \cap \mathbb{N}_{>0}$  als das kleinste Element. Somit ist  $I \subseteq \mathbb{Z}d \subseteq I \Rightarrow I = \mathbb{Z}d$ . Wir überprüfen noch, dass  $d$  der größte gemeinsame Teiler von  $a$  und  $b$  ist.

$a \in I = \mathbb{Z}d \Rightarrow a = kd$ , also  $d|a$ .

$b \in I = \mathbb{Z}d \dots$ , also  $d|b$ .

Also ist  $d$  gemeinsamer Teiler. Angenommen  $f$  ist ein weiterer gemeinsamer Teiler von  $a$  und  $b$ . Da  $d \in I$  gibt es  $k, l \in \mathbb{Z}$  mit  $d = ka + lb$ . Folgt  $f|a$  und  $f|b$  und daher  $f|d$ , somit  $f \leq d$ .

□

## 1.5. Geometrie

Alte Griechen sahen Geometrie und Zahlentheorie getrennt.

Descartes (1596-1650): Kann man  $\sqrt[3]{2}$  oder  $20^\circ$  mit Zirkel und lineal konstruieren.

Klassifikation von Geometrie im Erlanger Programm Klein 1872

## 2. Kommutative Ringe

### 2.1. 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.**

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

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  $Z_m = \mathbb{Z}/Z_m$  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. □

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

**Achtung.** Ab nun werden wir nur kommutative Ringe betrachten.



## 2.2. 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  $a \neq 0, b, c \in R$ .

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

□

**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  $\bar{l}$  besitzt. □

**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  $b$ .

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

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:

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

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

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

□

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*.

**Übung.** 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)?

## 2.3. 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 Potenzreihen* (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

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

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  $j > J$ . Draus 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 vize 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  $\deg(p + q) \leq \max(\deg(p), \deg(q))$ . □

**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

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

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.

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

- 

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

•

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

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

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

Wir statteten  $R^R$  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.

## 2.4. 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.

- 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.
- Die Addition, Multiplikation, das Negative induzieren wohldefinierte Abbildungen

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

- 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) :

- $a \sim a$  dann  $a - a = 0 \in I$ .

$$2. \ a \sim b \Rightarrow b \sim a \text{ denn } b - a = \underbrace{(-1)}_{\in R} \underbrace{(a - b)}_{\in I} \in I$$

$$3. \ a \sim b \text{ und } b \sim c \Rightarrow a \sim c \text{ denn } a - c = \underbrace{(a - b)}_{\in I} + \underbrace{(b - c)}_{\in I} \in I$$



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

$$I = R \Leftrightarrow 1 \in I \Leftrightarrow I \cap R^{\times} \neq \emptyset.$$

*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  $(a) = (b) \Leftrightarrow \exists u \in R^\times$  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  $x, y \in R^\times$  und wir setzen  $u = y$ .  $\square$

**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  $b \notin R^\times a$ . Es gilt  $a \in (b)$ , denn  $a = b \cdot f$  und  $b = a \cdot f$  für

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

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

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

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

**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  $\text{Im}(\bar{\varphi}) = \text{Im}(\varphi)$

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

*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.

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

**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.  $\square$

## 2.5. 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  $\mathbb{Z}/I \cong \text{Im}(\varphi) \subseteq K$ . 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  $p \mid \binom{p}{k}$

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

aber  $k! \not\equiv 0 \pmod p$ . Da Rechnen modulo  $p$  einen Körper definiert, erhalten wir  $k! \not\equiv 0, k! \binom{p}{k} \equiv 0 \pmod p \Rightarrow \binom{p}{k} \equiv 0 \pmod p$ . 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.  $\square$

## 2.6. 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  $([a][b] = 0 \Rightarrow [a] = 0 \text{ oder } [b] = 0 \Leftrightarrow I \neq R$  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. □

**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 un  $a, b \in \tilde{J}$ , 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. □

## 2.7. 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:

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

mit Nenner in  $\mathbb{Q}$ .



## 2.8. 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  $R$  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.

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

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  $f = \sum_{k_1, \dots, k_n} c_{k_1, \dots, k_n} X_1^{k_1} \dots X_n^{k_n}$  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

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

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  $R$ . □

# 3. 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.

## 3.1. 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

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

womit  $\deg(\tilde{g}) < \deg(g) = m$ . Auf Grund der Induktionsvoraussetzung können 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 für Polynomdivision).  $g = x^6 + x^4 + 4x^3 + 2, f = x^2 + 5$

$$\begin{array}{r} x^6 + 0x^5 + x^4 + 3x^3 + 0x^2 + 0x + 2 : x^2 + 5 = x^4 - 4x^2 + 3x \\ \underline{-x^6} \phantom{+ 0x^5} \phantom{+ x^4} \phantom{+ 3x^3} \phantom{+ 0x^2} \phantom{+ 0x} \phantom{+ 2} \\ \phantom{x^6 + } 0x^5 + \phantom{x^4} - 5x^4 + 3x^3 + 0x^2 + 0x + 2 \\ \phantom{x^6 + } \underline{-4x^4} \phantom{+ 3x^3} \phantom{+ 0x^2} \phantom{+ 0x} \phantom{+ 2} \\ \phantom{x^6 + } \phantom{0x^5 + } -4x^4 + 3x^3 + 0x^2 + 0x + 2 \\ \phantom{x^6 + } \phantom{0x^5 + } \underline{-4x^4} \phantom{+ 3x^3} \phantom{+ 0x^2} \phantom{+ 0x} \phantom{+ 2} \\ \phantom{x^6 + } \phantom{0x^5 + } \phantom{-4x^4 + } 4x^3 + 20x^2 + 0x + 2 \\ \phantom{x^6 + } \phantom{0x^5 + } \phantom{-4x^4 + } \underline{-3x^3} \phantom{+ 20x^2} \phantom{+ 0x} \phantom{+ 2} \\ \phantom{x^6 + } \phantom{0x^5 + } \phantom{-4x^4 + } \phantom{4x^3 + } 20x^2 - 15x + 2 \\ \phantom{x^6 + } \phantom{0x^5 + } \phantom{-4x^4 + } \phantom{4x^3 + } \underline{-20x^2} \phantom{- 15x} \phantom{+ 2} \\ \phantom{x^6 + } \phantom{0x^5 + } \phantom{-4x^4 + } \phantom{4x^3 + } \phantom{20x^2 - } -15x - 98 = r \end{array}$$

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

$$\begin{aligned} N(a + ib) &= |a + ib|^2 \text{ für } a + ib \in \mathbb{Q}[i] \\ &\in \mathbb{N} \text{ für } a + ib \in \mathbb{Z}[i] \\ N(z \cdot w) &= N(z)N(w) \text{ für } z, w \in \mathbb{Q}[i] \\ N(z) &= 0 \Leftrightarrow z = 0 \text{ multiplikativ} \end{aligned}$$

**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  $z = \frac{g}{f} \in \mathbb{Q}[i], z = a + ib$  für  $a, b \in \mathbb{Q}$ . 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  $t = g - fq \Rightarrow g = fq + r$ . 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. □

## 3.2. 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  $\mathbb{Z}[\frac{1}{2}(1+i\sqrt{163})]$  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  $p \mid b$ . □



# 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.

...

$\Rightarrow$  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

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

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

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

**Beispiel.**  $K_{\min} = \emptyset, \hat{K}_{\min} = X$  ist eine *f-Kette*, die in jeder anderen *f-Kette* enthalten ist.

$K_1 = \{f(\hat{K}_{\min})\} = K_{\min} \cup \{f(\hat{K}_{\min})\}$  ist eine weitere *f-Kette*, die in jeder anderen nicht-leeren *f-Kette* enthalten ist.

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

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

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

- Falls  $\widehat{C} \cap K \neq \emptyset$  ist, so gilt  $C \subseteq K$ ,  $f(\widehat{C}) \in K$  und  $f(\widehat{C})$  ist ein minimales Element von  $\widehat{C} \cap K$  (da  $K$  eine  $f$ -Kette ist). Damit ist aber auch  $f(\widehat{C}) \in K_{neu}$  und  $f(\widehat{C})$  ist ein minimales Element von  $\widehat{C} \cap K_{neu}$  (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  $f(\widehat{C}) = f(\widehat{K}) \in K_{neu}$  eine minimale obere Schranke von  $C$  in  $K_{neu}$ .
- Falls  $f(\widehat{K}) \in C$ , so ist  $\widehat{C} \cap K_{neu} = \emptyset$  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. □

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