# Einführung in die Algebra

Vorlesung im
Sommersemester 2008
Technische Universität Berlin

gehalten von
Prof. Dr. M. Pohst

# Contents

CHAPTER 3

# Ringe

## 3.1. Definition

Eine nicht leere Menge $R$ mit zwei inneren Verknüpfungen $+$ (Addition), $\cdot$ (Multiplikation) heißt Ring $(R, +, \cdot)$, falls folgende drei Bedingungen erfüllt sind.

(i) $(R, +)$ ist abelsche Gruppe;
(ii) $(R, \cdot)$ ist eine Halbgruppe;
(iii) es gelten die Distributivgesetze:

$$\begin{aligned} x \cdot (y + z) &= (x \cdot y) + (y \cdot z), \\ (x + y) \cdot z &= (x \cdot z) + (y \cdot z) \quad \forall x,\, y,\, z \in R. \end{aligned}$$

Überdies heißt $R$ kommutativ, falls $x \cdot y = y \cdot x \ \forall x,\, y \in R$ gilt. $R$ heißt Ring mit Eins, falls $(R, \cdot)$ Monoid ist.

Bemerkung:
Statt $(R, x, \cdot)$ schreibt man oft kürzer $R$, statt $x \cdot y$ einfach $x\,y$. Vereinbarungsgemäß geht "Punktrechnung vor Strichrechnung". Das neutrale Element bzgl. $+$ wird als 0 geschrieben. Ein Einselement ist, falls es existiert, stets eindeutig bestimmt.

Beispiel:

(i) $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ sind kommutative Ringe mit Eins, jedoch auch $R = \{0\}$ (pathologischer Ring).
(ii) $(\mathbb{Z}/n\mathbb{Z})$ ist kommutativer Ring mit Eins $(n \in \mathbb{N})$.
(iii) Die Endomorphismen eines Vektorraums $V$ bilden einen Ring mit Einselement id. Dieser ist für $\dim V \geq 2$ nicht kommutativ.
(iv) $R^{n \times n}$ ist Matrizenring über $R$.

**3.1.1. Rechenregeln für Ringe.** Für $x,\, y \in R$ gilt (vergleiche Lineare Algebra I):

(i) $0\,x = x\,0 = 0$,
(ii) $(-x)\,y = -(x\,y) = x\,(-y)$,
(iii) $(-x)\,(-y) = x\,y$,
(iv) $(\mathbb{Z},\, R) \to R \ : \ (m,\, x) \mapsto mx = \underbrace{x + \ldots + x}_{m\text{-mal}}$,
$\mathbb{Z}$ operiert auf jedem Ring mittels $(n, x) \mapsto nx$.

Statt $x + (-y)$ schreibt man $x - y$.
Allgemein gilt für $x_i,\ y_j \in R\ (1 \leq i \leq n,\ 1 \leq j \leq m,\ n, m \in \mathbb{N})$:

$$x_1 + \ldots + x_n = \sum_{i=1}^{n} x_i; \qquad x_1 \cdot \ldots \cdot x_n = \prod_{i=1}^{n} x_i;$$

leere Summe $:= 0$; leeres Produkt $:= 1$, falls $1 \in R$;

$$\begin{aligned}
\left(\sum_{i=1}^{n} x_i\right)\left(\sum_{j=1}^{m} y_j\right) &= \sum_{i=1}^{n}\sum_{j=1}^{m} x_i y_j, \\
x^n &= \prod_{i=1}^{n} x, \\
x^{n+m} &= x^n \cdot x^m, \\
(x^n)^m = x^{nm}, & \\
(x+y)^n &= \sum_{i=0}^{n} \binom{n}{i} x^{n-i} y_i
\end{aligned}$$

in kommutativen Ringen mit 1.

### 3.2. Definition

Eine Teilmenge $S$ von $(R, +, \cdot)$ heißt Teilring (Unterring) von $R$, falls $(S, +, \cdot)$ selbst Ring ist. In diesem Fall heißt $R$ Oberring (Erweiterungsring) von $S$.

### 3.3. Hilfssatz

$R$ sei Ring und $\emptyset \neq S \subseteq R$. Dann sind äquivalent:

(i) $S$ Teilring von $R$,
(ii) $SS \subseteq S$ und $S + (-S) \subseteq S$.

Beweis:
(i) $\Rightarrow$ (ii): Klar. Beachte

$$\begin{aligned}
SS &= \{xy \mid x \in S,\ y \in S\}, \\
S + (-S) &= \{x - y \mid x,\ y \in S\}.
\end{aligned}$$

(ii) $\Rightarrow$ (i):

$$\begin{aligned}
S + (-S) \subseteq S &\Rightarrow (S, +) \text{ Gruppe}, \\
SS \subseteq S &\Rightarrow (S, \cdot) \text{ Halbgruppe},
\end{aligned}$$

denn die Rechenregeln übertragen sich von $R$.

□

Beispiele:

(i) Für $n \in \mathbb{N}$ ist $n\mathbb{Z}$ Unterring von $\mathbb{Z}$.
(ii) Die Diagonalmatrizen bilden einen Unterring von $R^{n\times n}$.

Bemerkung: Der Durchschnitt von Teilringen ist Teilring!

Wichtiger als Teilringe sind jedoch Ideale, die in gewisser Weise den Normalteilern in der Gruppentheorie entsprechen!

### 3.4. Definition

Es sei $R$ ein Ring. $\mathfrak{a} \subseteq R$ heißt Linksideal (bzw. Rechtsideal) von $R$, falls gilt:

(i) $\mathfrak{a}$ ist Untergruppe von $(R, +)$, d.h. $\mathfrak{a} \neq \emptyset$ und $\mathfrak{a} + (-\mathfrak{a}) \subseteq \mathfrak{a}$.
(ii) $\forall a \in \mathfrak{a} \ \forall x \in R \ : \ x\,a \in \mathfrak{a}$ (bzw. $ax \in \mathfrak{a}$), d.h. $R\,\mathfrak{a} \subseteq \mathfrak{a}$ (bzw. $\mathfrak{a} \supseteq \mathfrak{a}\,R$).

$\mathfrak{a} \subseteq R$ heißt Ideal, falls $\mathfrak{a}$ sowohl Links- als auch Rechtsideal ist.

Bemerkung:

(i) $\{0\}$, $R$ sind stets Ideale von $R$; Ideale sind Teilringe (Umkehrung i.a. falsch: $\mathbb{Z} \subset \mathbb{Q}$); für $R \ni 1$ und $1 \in \mathfrak{a}$ für ein Links- oder Rechtsideal $\mathfrak{a}$ von $R$ folgt sofort $\mathfrak{a} = R$.
(ii) Der Durchschnitt von (Links- bzw. Rechts-) Idealen ist wieder eins. Zu $A \subseteq R$ existiert folglich ein kleinstes Ideal, welches $A$ umfaßt, das sogenannte von $A$ erzeugte Ideal $(A)$.

Beispiel:
Es sei $\mathfrak{a}$ ein Ideal von $\mathbb{Z}$. Wegen $\mathfrak{a} \neq \emptyset$ und $(-\mathfrak{a}) \subseteq \mathfrak{a}$ gilt entweder $\mathfrak{a} = \{0\}$, oder $\mathfrak{a}$ enthält eine kleinste natürliche Zahl $m$. Gemäß Division mit Rest gilt, daß $m$ alle Zahlen von $\mathfrak{a}$ teilt. Also ist $\mathfrak{a} = \mathbb{Z}m = m\mathbb{Z}$.

### 3.5. Hilfssatz

Es sei $\emptyset \neq A \subseteq R$, $R$ Ring. Dann besteht $(A)$ aus allen endlichen Summen von Elementen der Form

$$n\,a,\ x\,a,\ a\,y,\ x\,a\,y \text{ mit } a \in A,\ x, y \in R,\ n \in \mathbb{Z}.$$

Beweis:

(i) Jedes Ideal $\mathfrak{a}$ mit $A \subseteq \mathfrak{a}$ enthält alle in (2.5) angegebenen Elemente.
(ii) Die Menge der in (2.5) angegebenen Elemente ist ein Ideal.

□

### 3.6. Korollar

Es sei $R$ ein Ring und $\emptyset \neq A \subseteq R$. Dann gilt:

(i) $(A) = \left\{ \sum_{\text{endl.}} x_i \cdot a_i \cdot y_i \;\middle|\; x_i,\ y_i \in R,\ a_i \in A \right\}$ für $R \ni 1$;

(ii) $(A) = \left\{ \sum_{\text{endl.}} x_i \cdot a_i + \sum_{\text{endl.}} m_j \cdot b_j \;\middle|\; x_i \in R,\ m_j \in \mathbb{Z},\ a_i, b_j \in A \right\}$ für $R$ kommutativ;

(iii) $(A) = \left\{ \sum_{\text{endl.}} x_i \cdot a_i \;\middle|\; x_i \in R,\ a_i \in A \right\}$ für $R$ kommutativ mit Eins.

Beweis: Unmittelbar klar nach (2.5)!

### 3.7. Definition

Ein Ideal $\mathfrak{a}$ eines Ringes $R$ heißt Hauptideal, falls $\mathfrak{a} = (a)$ für $a \in R$ gilt. $\mathfrak{a}$ heißt endlich erzeugbar, falls $\mathfrak{a} = (A)$ mit $\sharp A < \infty$ gilt.

Beispiel:
Alle Ideale in $\mathbb{Z}$ sind Hauptideale.

Bemerkungen:

(i) $R$ kommutativ $\Rightarrow\ (a) = Ra + \mathbb{Z}a$;
(ii) $R$ kommutativ mit Eins $\Rightarrow\ (a) = Ra$;
(iii) $R$ kommutativ ohne Eins: In $R = 2\mathbb{Z}$ ist $(2) = 4\mathbb{Z} + \mathbb{Z}2 = 2\mathbb{Z}$ von $2R = 4\mathbb{Z}$ verschieden;
(iv) $R \ni 1\ \Rightarrow\ (1) = R$.

**Arithmetik von Idealen:**

### 3.8. Definition

Die Summe zweier (Links- bzw. Rechts-) Ideale $\mathfrak{a}_1,\ \mathfrak{a}_2$ ist definiert durch:

$$\mathfrak{a}_1 + \mathfrak{a}_2 = \{a_1 + a_2 \mid a_1 \in \mathfrak{a}_1,\ a_2 \in \mathfrak{a}_2\}.$$

Bemerkung:
Die Summe endlich vieler (Links- bzw. Rechts-) Ideale ist wieder eins. Der Durchschnitt von Idealen ist wieder ein Ideal. Es gelten:

$$\mathfrak{a}_i \subseteq \mathfrak{a}_i + \ldots + \mathfrak{a}_n\ (1 \le i \le n), \quad \mathfrak{a}_i + \mathfrak{a}_i = \mathfrak{a}_i, \quad (A_1) + (A_2) = (A_1 \cup A_2).$$

Beispiel:
$R = \mathbb{Z}$:
$Ra + Rb = \{xa + yb \mid x, y \in \mathbb{Z}\} = c\mathbb{Z}$ mit $c = \text{ggT}\,(a, b)$,
$Ra \cap Rb = d\mathbb{Z}$ mit $d = \text{kgV}\,(a, b)$.

## 3.9. Definition

Das Produkt zweier (Links- bzw. Rechts-) Ideale $\mathfrak{a}_1$, $\mathfrak{a}_2$ ist definiert durch:

$$\mathfrak{a}_1 \cdot \mathfrak{a}_2 = \left\{ \sum_{\text{endl.}} a_{1i}\, a_{2i} \,|\, a_{1i} \in \mathfrak{a}_1,\ a_{2i} \in \mathfrak{a}_2 \right\}.$$

Bemerkung:
Das Produkt endlich vieler (Links- bzw. Rechts-) Ideale ist wieder eins. Es gelten die Rechenregeln:

$$\mathfrak{a}_1\,(\mathfrak{a}_2\mathfrak{a}_3) = (\mathfrak{a}_1\mathfrak{a}_2)\,\mathfrak{a}_3, \quad \mathfrak{a}_1\,(\mathfrak{a}_2 + \mathfrak{a}_3) = \mathfrak{a}_1\mathfrak{a}_2 + \mathfrak{a}_1\mathfrak{a}_3.$$

Ist $R$ kommutativ, so gilt $\mathfrak{a}_1\mathfrak{a}_2 = \mathfrak{a}_2\mathfrak{a}_1$. Sind $\mathfrak{a}_1$, $\mathfrak{a}_2$ Linksideale, so gilt $\mathfrak{a}_1\mathfrak{a}_2 \subseteq \mathfrak{a}_2$; sind $\mathfrak{a}_1$, $\mathfrak{a}_2$ Rechtsideale, so gilt $\mathfrak{a}_1\mathfrak{a}_2 \subseteq \mathfrak{a}_1$, $(A_1)\,(A_2) = (A_1A_2)$ für $R$ kommutativ.

Ist $R$ kommutativer Ring mit Eins und sind $a$, $b \in R$, so gilt

(i) $(a) + (b) = \{xa + yb \,|\, x,\, y \in R\} = Ra + Rb$.
(ii) $(a)\,(b) = (ab)$, $Ra\,Rb = R\,(Ra)\,b = Rab$.
(iii) $\mathfrak{a} \cap (\mathfrak{b} + \mathfrak{c}) \supseteq \mathfrak{a} \cap \mathfrak{b} + \mathfrak{a} \cap \mathfrak{c}$ mit Gleichheit für $\mathfrak{a} \supseteq \mathfrak{b} \vee \mathfrak{a} \supseteq \mathfrak{c}$.
(iv) für $\mathfrak{a} + \mathfrak{b} = R$ ist $\mathfrak{a} \cap \mathfrak{b} = \mathfrak{a}\mathfrak{b}$.

Beweis:

(i) klar.

(ii) klar.

(iii) $x \in \mathfrak{a} \cap \mathfrak{b},\ y \in \mathfrak{a} \cap \mathfrak{c} \ \Rightarrow\ x + y \in \mathfrak{a}, x + y \in \mathfrak{b} + \mathfrak{c}$.
Gilt oBdA $\mathfrak{a} \supseteq \mathfrak{b}$, so ist für $x \in \mathfrak{a} \cap (\mathfrak{b} + \mathfrak{c})$ zunächst $x = b + c$ mit $b \in \mathfrak{b},\ c \in \mathfrak{c}$.
Wegen $\mathfrak{a} \supseteq \mathfrak{b}$ ist auch $b \in \mathfrak{a}$ und damit $c \in \mathfrak{a}$, also $b \in \mathfrak{a} \cap \mathfrak{b},\ c \in \mathfrak{a} \cap \mathfrak{c}$.

(iv) Es ist

$$\begin{aligned}(\mathfrak{a} + \mathfrak{b})(\mathfrak{a} \cap \mathfrak{b}) &= \mathfrak{a}(\mathfrak{a} \cap \mathfrak{b}) + \mathfrak{b}(\mathfrak{a} \cap \mathfrak{b}) \subseteq \mathfrak{ab} \\ &\subseteq \mathfrak{a} \cap \mathfrak{b},\end{aligned}$$

also $(\mathfrak{a} + \mathfrak{b})(\mathfrak{a} \cap \mathfrak{b}) \subseteq \mathfrak{ab}$;
für $\mathfrak{a} + \mathfrak{b} = R$ gilt offenbar Gleichheit.

□

Bemerkung:
Ein Beispiel für $\mathfrak{a} \cap (\mathfrak{b} + \mathfrak{c}) \supset \mathfrak{a} \cap \mathfrak{b} + \mathfrak{a} \cap \mathfrak{c}$ wird im Anschluß an die Einführung von Polynomringen behandelt.

### 3.10. Satz

Es sei $R$ ein Ring mit Ideal $\mathfrak{a}$. Dann läßt sich $R/\mathfrak{a}$ mittels

$$(x + \mathfrak{a}) + (y + \mathfrak{a}) =: (x + y) + \mathfrak{a}, (x + \mathfrak{a})(y + \mathfrak{a}) := xy + \mathfrak{a} \quad \forall x, y \in R$$

zu einem Ring machen, dem Faktorring $R/\mathfrak{a}$ oder Restklassenring $R$ modulo $\mathfrak{a}$.

Beweis:
Zunächst ist $(\mathfrak{a}, +)$ additive Untergruppe von $(R, +)$, also $R/\mathfrak{a}$ eine additive Gruppe (vergleiche (1.17)). Wir zeigen: $(R/\mathfrak{a}, \cdot)$ ist Halbgruppe. Zunächst ist $\cdot$ innnere Verknüpfung. Dazu ist die Wohldefiniertheit nachzuweisen. Für

$$x + \mathfrak{a} = \tilde{x} + \mathfrak{a},\ y + \mathfrak{a} = \tilde{y} + \mathfrak{a} \quad \text{folgt} \quad x - \tilde{x},\ y - \tilde{y} \in \mathfrak{a}$$

und somit

$$xy - \tilde{x}\tilde{y} = (x - \tilde{x})\, y + \tilde{x}\,(y - \tilde{y}) \ \in \mathfrak{a},$$

da $\mathfrak{a}$ zweiseitiges Ideal ist. Also folgt $xy + \mathfrak{a} = \tilde{x}\tilde{y} + \mathfrak{a}$. Das Assoziativgesetz bzgl. $\cdot$ überträgt sich von $R$. Das gleiche gilt für die Distributivgesetze, da ja vertreterweise mit den Idealklassen gerechnet wird.

□

Bemerkung:

(i) Für $1 \in R$ ist $1 + \mathfrak{a}$ Einselement von $R/\mathfrak{a}$. $R$ kommutativ $\Rightarrow$ $R/\mathfrak{a}$ kommutativ.

(ii) Für $x - y \in \mathfrak{a}$ schreibt man $x \equiv y$ modulo $\mathfrak{a}$ ("kongruent"). Hierfür gelten die Regeln:

$$\left.\begin{array}{l} x \equiv y \text{ modulo } \mathfrak{a} \\ u \equiv v \text{ modulo } \mathfrak{a} \end{array}\right\} \Rightarrow x \overset{+}{\underset{\bullet}{}} u \equiv y \overset{+}{\underset{\bullet}{}} v \text{ modulo } \mathfrak{a}.$$

Für $R = \mathbb{Z}$ bedeutet die alte Schreibweise $x \equiv y \bmod n$ gerade $x \equiv y$ modulo $n\mathbb{Z}$, denn sämtliche Ideale von $\mathbb{Z}$ waren ja als Hauptideale nachgewiesen. Die spezielle Äquivalenzrelation $\equiv$ heißt Kongruenzrelation.

### 3.11. Definition

Es seien $R$, $S$ zwei Ringe. Unter einem Ringhomorphismus von $R$ nach $S$ versteht man eine Abbildung $f : R \to S$ mit

$$f(x+y) = f(x) + f(y),\ f(x \cdot y) = f(x) \cdot f(y) \quad \forall x, y \in R.$$

Bemerkung:

(i) Für Ringhomomorphismen $f : R \to S$ ist $\operatorname{Im} f = f(R)$ Unterring von $S$, $\ker f = f^{-1}(0)$ Ideal in $R$.

(ii) Ist $R$ ein Ring mit Ideal $\mathfrak{a}$, so ist $p : R \to R/\mathfrak{a} : x \mapsto x + \mathfrak{a}$ ein Ringepimorphismus, der sog. kanonische Epimorphismus. Es ist $\ker p = \mathfrak{a}$.

### 3.12. Hilfssatz

Eine Teilmenge $\mathfrak{a}$ eines Ringes $R$ ist genau dann ein Ideal, wenn $\mathfrak{a}$ Kern eines Ringhomomorphismus ist.

### 3.13. Hilfssatz

Es seien $R$, $S$ Ringe und $f : R \to S$ ein Ringhomomorphismus. Dann gilt:

(i) Ist $\mathfrak{b}$ ein Ideal in $S$, so ist $f^{-1}(\mathfrak{b})$ Ideal in $R$, $f^{-1}(\mathfrak{b}) \supseteq \ker f$.

(ii) Ist $\mathfrak{a}$ Ideal in $R$ und $f$ surjektiv, so ist $f(\mathfrak{a})$ Ideal in $S$.

Beweis:
Gemäß (1.16) gelten die Aussagen bzgl. $+$.

(i) Es sei $s = f(r) \in \mathfrak{b}$ und $x \in R$. Dann ist

$$f(xr) = f(x)\, f(r) \ \in \mathfrak{b},$$

also mit $r$ auch $xr \in f^{-1}(\mathfrak{b})$.

(ii) Es sei $y = f(x)$ mit $x \in \mathfrak{a}$ und $z \in S$. Dann ist $z = f(r)$ für ein $r \in R$ und somit

$$zy = f(r)\, f(x) = f(rx) \ \in f(\mathfrak{a}).$$

□

### 3.14. Satz

Es seien $R$, $S$ zwei Ringe.

(i) (Homomorphiesatz)
Ist $\varphi : R \to S$ ein Ringhomomorphismus, dann gilt
$$R/\ker\varphi \cong \varphi(R).$$

(ii) (Erster Isomorphiesatz)
Ist $U$ Unterring und $\mathfrak{a}$ Ideal von $R$, so gilt
$$(U+\mathfrak{a})/\mathfrak{a} \cong U/U\cap\mathfrak{a}.$$

(iii) (Zweiter Isomorphiesatz)
Für Ideale $\mathfrak{a}$, $\mathfrak{b}$ von $R$ mit $\mathfrak{a}\subseteq\mathfrak{b}$ ist $\mathfrak{b}/\mathfrak{a}$ Ideal von $R/\mathfrak{a}$, und es gilt
$$(R/\mathfrak{a})/(\mathfrak{b}/\mathfrak{a}) \cong R/\mathfrak{b}.$$

### 3.15. Hilfssatz

Es sei $\mathfrak{a}$ ein Ideal des Ringes $R$. Die Mengen
$$I(\mathfrak{a}) := \{\mathfrak{b} \mid \mathfrak{b} \text{ Ideal von } R \text{ mit } \mathfrak{b}\supseteq\mathfrak{a}\}$$
und
$$J(\mathfrak{a}) := \{\,\overline{\mathfrak{b}} \mid\ \overline{\mathfrak{b}} \text{ Ideal von } R\backslash\mathfrak{a}\}$$
werden dann mittels $\psi : I(\mathfrak{a}) \to J(\mathfrak{a}) : \mathfrak{b} \mapsto \mathfrak{b}/\mathfrak{a}$ bijektiv aufeinander abgebildet.

Beweis:
Für den kanonischen Epimorphismus $p : R \to R/\mathfrak{a}$ liefert $\psi$ eine Abbildung von $I(\mathfrak{a})$ in $J(\mathfrak{a})$. Für
$$\psi(\mathfrak{b}_1) = \psi(\mathfrak{b}_2) \quad \text{folgt} \quad \mathfrak{b}_1 = \mathfrak{b}_1+\mathfrak{a} = \mathfrak{b}_2+\mathfrak{a} = \mathfrak{b}_2,$$
also ist $\psi$ injektiv. Ist schließlich $\overline{\mathfrak{b}}$ Ideal von $J(\mathfrak{a})$, so ist $p^{-1}(\overline{\mathfrak{b}})$ ein Ideal von $R$, welches $\mathfrak{a}$ umfaßt, also in $I(\mathfrak{a})$ liegt. Hierfür gilt $\psi(p^{-1}(\overline{\mathfrak{b}})) = \overline{\mathfrak{b}}$ nach Konstruktion.

□

### 3.16. Definition

Es sei $R$ ein Ring. $0 \neq a \in R$ heißt linker (rechter) Nullteiler, falls $b \in R$ mit $a\,b = 0$ ($b\,a = 0$) für ein $0 \neq b \in R$ existiert. $x \in R$ heißt nilpotent, falls $m \in \mathbb{N}$ mit $x^m = 0$ existiert. Für $1 \in R$ heißt $e \in R$ Einheit (invertierbar), falls $e$ in $R$ ein Linksinverses und ein Rechtsinverses besitzt. $U(R) = R^\times$ bezeichnet die Menge der Einheiten von $R$.

Bemerkung:

(i) $e$ Einheit $\Rightarrow$ $e^{-1}$ existiert eindeutig.
Sei

$$ae = eb = 1 \quad \Rightarrow \quad a = a \cdot 1 = a\,(eb) = (ae)\,b = 1 \cdot b = b.$$

Für $ae = ea = 1$ und $be = eb = 1$ folgt

$$a = a \cdot 1 = a\,(eb) = (ae)\,b = 1 \cdot b = b.$$

(Vergleiche Gruppentheorie)

(ii) Die Elemente von $R$, welche keine Nullteiler sind, bilden eine Halbgruppe. Es seien $a$, $b$ keine Nullteiler; ist dann $x \in R$ mit $abx = 0$ so folgt

$$a\,(bx) = 0 \quad \Rightarrow \quad bx = 0 \quad \Rightarrow \quad x = 0.$$

(iii) Einheiten sind keine Nullteiler und bilden folglich eine multiplikative Untergruppe von $R$.

$$e \in R^\times,\ x \in R\ :\ ex = 0 \quad \Rightarrow \quad e^{-1}ex = 0 \quad \Rightarrow \quad 1 \cdot x = x = 0.$$

Beispiele:
Bestimme Einheiten, Nullteiler und nilpotente Elemente in
$\mathbb{Z}/12\mathbb{Z},\ \mathbb{Z},\ K^{n\times m},\ R = \{0\}$.

(i) $0 \neq x \in R$ nilpotent $\Rightarrow$ $x$ Nullteiler.
$0 = x^m = \left(x^{m-1}\right) x = x\left(x^{m-1}\right)$, wähle $m$ minimal!

(ii) $\mathbb{Z}/12\mathbb{Z} = \{\,\bar{i} \mid 0 \leq i \leq 11\}$
$\bar{j}^{\,m} \stackrel{?}{=} \bar{0} \ \Rightarrow\ j^m \equiv 0 \bmod 12\ \ (12 = 4 \cdot 3) \ \Rightarrow\ j = 0 \vee 6$
Nilpotente Elemente: $\bar{0}$, $\bar{6}$
Nullteiler: $\bar{6}$, $\bar{2}$, $\bar{4}$, $\bar{8}$, $\overline{10}$, $\bar{3}$, $\bar{9}$
Einheiten: $\bar{1}$, $\bar{5}$, $\bar{7}$, $\overline{11}$ $\ (\bar{1} = \bar{5}^2 = \bar{7}^2 = \overline{11}^2)$

(iii) $R = \mathbb{Z}$
Nilpotente Elemente: 0,
Nullteiler: keine,
Einheiten: $\pm 1$.

(iv) $K^{n\times n}$
Nilpotente Elemente sind z.B. alle oberen $\triangle$-Matrizen mit 0-Diagonale,
Nullteiler: alle singulären Matrizen,
Einheiten: $\mathrm{GL}\,(n,\, K)$.

## 3.17. Definition

Ein Ring $R$ mit $1 \neq 0$ heißt Schiefkörper, falls $R^\times = R\backslash\{0\}$ ist. Ist $R$ kommutativ, so heißt $R$ Körper.

### 3.18. Hilfssatz

Ein Ring $R$ ist genau dann ein Schiefkörper, wenn $(R\backslash\{0\}, \cdot)$ Gruppe ist.

Beweis:
$\Rightarrow$: per Definition

$\Leftarrow$:
$R\backslash\{0\}$ enthält Eins $e$ mit $0e = e0 = 0$. Also ist $R^\times = R\backslash\{0\}$.

□

Beispiele:

(i) Körper: $\mathbb{Q}$, $\mathbb{R}$, $(\mathbb{Z}/n\mathbb{Z})$ mit $n \in \mathbb{P}$.
(ii) Schiefkörper: $\mathbb{R}+\mathbb{R}i+\mathbb{R}j+\mathbb{R}k$ Quaternionen (als $\mathbb{R}$-Vektorraum)

Bemerkung:

(i) $R$ Ring mit Eins, $\mathfrak{a}$ Ideal von $R$ mit $\mathfrak{a} \cap R^\times \neq \emptyset$. Dann ist $\mathfrak{a} = R$; denn zu $a \in \mathfrak{a} \cap R^\times$ existiert $a^{-1} \in R$ und $a^{-1}a \in R\mathfrak{a} = \mathfrak{a}$, also $1 \in \mathfrak{a}$ und $R = R\,1 \subseteq \mathfrak{a}$.
(ii) Ein Schiefkörper $R$ enthält nur die Ideale $\{0\}$ und $R$.
(iii) Ist $K$ ein Schiefkörper und $\varphi : K \to R$ ein Ringhomomorphismus, so ist $\varphi = \mathcal{O}$ oder $\varphi$ injektiv.
(iv) Es gibt keine endlichen Schiefkörper! (ohne Beweis)

### 3.19. Hilfssatz

(i) Es sei $R$ ein Ring. Ist $a \in R$ kein Nullteiler, so gilt:

$$ax = ay \;\Rightarrow\; x = y; \quad xa = ya \;\Rightarrow\; x = y \quad \forall x, y \in R.$$

(ii) Ein endlicher nullteilerfreier Ring $R \neq \{0\}$ ist ein Schiefkörper.

Beweis:

(i) $a\,(x - y) = 0 \;\Rightarrow\; x - y = 0 \;\Rightarrow\; x = y$; $\quad (x - y)\,a = 0 \;\Rightarrow\; x - y = 0 \;\Rightarrow\; x = y$.
(ii) Zeige: $(R\backslash\{0\}, \cdot)$ ist Gruppe.

Für $x \in R$, $x \neq 0$, betrachte $\varphi_x : R\backslash\{0\} \to R\backslash\{0\}$ : $a \mapsto xa$. $\varphi_x$ ist injektiv (nach (i)), also wegen $R$ endlich auch surjektiv. Dasselbe gilt für $\psi_x : a \mapsto ax$. Zu $a, b \in R\backslash\{0\}$ existieren folglich eindeutig $x, y \in R\backslash\{0\}$ mit $b = ax = ya$. Gemäß (1.5) ist $R^\times = R\backslash\{0\}$ Gruppe.

□

### 3.20. Definition

Es sei $R$ ein Ring mit $1 \neq 0$. Existiert dann eine kleinste natürliche Zahl $n$ mit $n\,1 = 0$, so heißt $n$ die Charakteristik $\chi(R)$ von $R$. Existiert kein solches $n$, setzt man die Charakteristik $\chi(R)$ zu 0 fest.

Beispiele:
$\chi(\mathbb{Z}) = 0,\ \chi(\mathbb{Z}/n\mathbb{Z}) = n.$

### 3.21. Satz

Die Charakteristik eines nullteilerfreien unitären ($R \ni 1 \neq 0$) Rings $R$ ist 0 oder eine Primzahl $p$. Im letzten Fall gilt $px = 0\ \forall x \in R$, sowie $kx = R(k,\, p)\, x$.

Beweis:
Es sei $R$ Ring mit $\chi(R) \neq 0$ und $n \in \mathbb{N}$ die kleinste natürliche Zahl mit $n1 = 0$, also speziell $n \geq 2$. Ist $n$ keine Primzahl, so gilt $n = pq$ mit $p,\, q \in \mathbb{Z}^{\geq 1},\ p < n,\ q < n$ und somit

$$0 = n1 = pq1 = (p1)\,(q1).$$

Da $R$ nullteilerfrei ist, erhält man $p1 = 0$ oder $q1 = 0$ im Widerspruch zur Minimalität von $n$. Nunmehr ist $0 = n1$, also auch

$$nx = n\,(1x) = (n1)\,x = 0x = 0 \quad \forall x \in R.$$

□

Bemerkung:
Der Durchschnitt von Schiefkörpern ist wieder einer. Also enthält jeder Schiefkörper einen kleinsten Teilkörper, den sogenannten Primkörper.

### 3.22. Satz

Der Primkörper eines Schiefkörper $K$ ist isomorph zu $\mathbb{Q}$ (für $\chi(K) = 0$) oder zu $\mathbb{Z}/Lp\mathbb{Z}$ für eine Primzahl $p$ (für $\chi(K) = p$).

Beweis:
In $K$ gilt $1 \neq 0$. Der Primkörper von $K$ umfaßt daher alle Elemente der Form $m1$ ($m \in \mathbb{Z}$). Für $\chi(K) = 0$ sind diese alle ungleich 0 für $m \neq 0$. Also existiert $(m1)^{-1}$ und damit $(m1)\,(n1)^{-1}$ im Primkörper. Setze

$$P := \{(m1)\,(n1)^{-1} \mid m \in \mathbb{Z},\ n \in \mathbb{Z},\ n \neq 0\}.$$

Es gilt:

$$(m1)\,(n1)^{-1} = (n1)^{-1}(m1) \text{ wegen } (n1)\,(m1) = (m1)\,(n1) = (mn)\,1,$$
$$(mn1)^{-1} = (m1)^{-1}(n1)^{-1}.$$

Also ist $P$ Körper, der im Primkörper enthalten ist, folglich gleich dem Primkörper.

$$\varphi\ :\ \mathbb{Q} \to P\ :\ \frac{m}{n} \mapsto (m1)\,(n1)^{-1}$$

ist dann ein Ringisomorphismus.
Für $\chi(K) = p$, $p$ Primzahl, ist $p1 = 0$. Für $x = k1$ $(1 \leq k < p)$ existiert (Euklidischer Algorithmus in $\mathbb{Z}$) ein $l \in \mathbb{Z}$ mit $k \cdot l \equiv 1 \bmod p$, also $(k1)(l1) = 1$ in $K$. Setze

$$P := \{k1 \mid 0 \leq k < p,\ k \in \mathbb{Z}\}.$$

Dies ist bereits der Primkörper von $K$.

$$\varphi : (\mathbb{Z}/p\mathbb{Z}) \to P : k + p\mathbb{Z} \mapsto k1$$

ist Ringisomorphismus! ($\varphi$ ist wohldefiniert wegen $(k + pm)\,1 = k1 + p1m1 = k1$.)

□

Wie bei Gruppen kann man für Ringe äußere Produkte (Summen) erklären.

Sind $R_1, \ldots, R_n$ Ringe, so wird $R_1 \times \ldots \times R_n =: \prod_{i=1}^{n} R_i = R$ zu einem Ring mittels

$$\begin{aligned}(x_1, \ldots, x_n) + (y_1, \ldots, y_n) &= (x_1 + x_2, \ldots, x_n + y_n),\\ (x_1, \ldots, x_n) \cdot (y_1, \ldots, y_n) &= (x_1 y_1, \ldots, x_n y_n).\end{aligned}$$

(Vergleiche Eigenschaften bei Gruppen, speziell ist $\varepsilon_i(R_i) = (0, \ldots, 0, R_i, 0, \ldots, 0)$ Ideal von $R$. Schreibweise: $R_1 \oplus \ldots \oplus R_n$.)
Ist andererseits $R$ ein Ring mit Idealen $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$, so heißt $R$ (innere) direkte Summe von $\mathfrak{a}_1, \ldots, \mathfrak{a}_n$, falls

$$R = \mathfrak{a}_1 + \ldots + \mathfrak{a}_n \quad \text{und} \quad R\mathfrak{a}_i \cap \sum_{\substack{j=1\\ j\neq i}}^{n} \mathfrak{a}_j = \{0\}$$

ist (vgl. (1.23)). (Schreibweise: $R = \mathfrak{a}_1 \dot{+} \ldots \dot{+} \mathfrak{a}_n$)
Ein Element $e \in R$ mit $e \neq 0$ und $e^2 = e$ heißt Idempotente von $R$.
Zwei Idempotente $e$, $f$ heißen orthogonal, falls $ef = fe = 0$ ist.

Beispiel:
$R = \mathbb{Z}/6\mathbb{Z}$. Es gilt: $R = <3 + 6\mathbb{Z}> \dot{+} <4 + 6\mathbb{Z}>$.
Hierin sind $e_1 = 3 + 6\mathbb{Z}$ und $e_2 = 4 + 6\mathbb{Z}$ Idempotente. Wir haben hier eine Zerlegung der Eins in orthogonale Idempotente: $1 + 6\mathbb{Z} = (3 + 6\mathbb{Z}) + (4 + 6\mathbb{Z})$.

Bemerkung:
Ringe $R$ mit $1 \in R$ haben mit einer Idempotenten $e \neq 1$ stets eine weitere: $1 - e$. Es gilt

$$\begin{aligned}1 &= e + (1 - e),\\ (1 - e)^2 &= 1^2 - 1 \cdot e - 1 \cdot e + e^2\\ &= 1 - e - e + e\\ &= 1 - e.\end{aligned}$$

$1-e$ und $e$ sind orthogonale Idempotente wegen

$$e\,(1-e) = e - e^2 = 0 = (1-e)\,e.$$

Somit gilt

$$R = R\,1 = R\,(e + (1-e))\& \subseteq \&R\,e\dot{+}R\,(1-e).\& \subseteq \&R$$

, also überall Gleichheit.

Beachte: Orthogonale Idempotente sind Nullteiler.

Es sei $R$ ein kommutativer Ring mit $1 \neq 0$. Zwei Ideale $\mathfrak{a}$, $\mathfrak{b}$ von $R$ mit $\mathfrak{a} + \mathfrak{b} = R$ heißen komaximal. Speziell existieren $e \in \mathfrak{a}$, $f \in \mathfrak{b}$ mit $e + f = 1$. (Allerdings wird nicht gefordert, daß $e$, $f$ orthogonale Idempotente sind.)

Beispiel: $R = \mathbb{Z}$, $m, n \in \mathbb{Z}$ teilerfremd $\Rightarrow$ $m\mathbb{Z} + n\mathbb{Z} = \mathbb{Z}$ und $mu + nv = 1$ für passende $u,\ v \in \mathbb{Z}$.

## 3.23. Hilfssatz

Es sei $R$ ein kommutativer Ring mit $1 \neq 0$. Dann gilt für Ideale $\mathfrak{a}, \mathfrak{a}_1, \ldots, \mathfrak{a}_n, \mathfrak{b}_1, \ldots, \mathfrak{b}_n$ mit $\mathfrak{a}_i + \mathfrak{a}_j = R (\mathfrak{a}_i,\ \mathfrak{a}_j$ komaxial$)(1 \leq i < j \leq n)$, $\mathfrak{a} + \mathfrak{b}_i = R\ (1 \leq i \leq n)$:

(i) $\mathfrak{a} + \mathfrak{b}_1 \cdot \ldots \cdot \mathfrak{b}_n = R$,

(ii) $\mathfrak{a}_1 \cdot \ldots \cdot \mathfrak{a}_n = \mathfrak{a}_1 \cap \ldots \cap \mathfrak{a}_n$.

Beweis:

(i)

$$\begin{aligned}
R &= R^n \\
&= \prod_{i=1}^{n} (\mathfrak{a} + \mathfrak{b}_i) \qquad \text{(wegen } 1 \in R\text{)} \\
&= \mathfrak{a}\,(\mathfrak{a}^{n-1} + \ldots) + \mathfrak{b}_1 \cdot \ldots \cdot \mathfrak{b}_n \qquad (R \text{ kommutativ}) \\
&\subseteq \mathfrak{a} + \mathfrak{b}_1 \cdot \ldots \cdot \mathfrak{b}_n \\
&\subseteq R,
\end{aligned}$$

also muß überall Gleichheit gelten.

(ii) Beweis per Induktion über $n$.

$n = 1$: Klar.

$n = 2$: vgl. Beweis zu Bem. (iv) auf Seite 45.

$n \to n+1$:

$$\begin{aligned}
\mathfrak{a}_1 \cdot \ldots \cdot \mathfrak{a}_{n+1} &= (\mathfrak{a}_1 \cdot \ldots \cdot \mathfrak{a}_n)\,\mathfrak{a}_{n+1} \\
&\overset{(*)}{=} (\mathfrak{a}_1 \cdot \ldots \cdot \mathfrak{a}_n) \cap \mathfrak{a}_{n+1} \\
&\overset{\text{Ind. Vor.}}{=} \bigcap_{i=1}^{n+1} \mathfrak{a}_i
\end{aligned}$$

$(*)$: Per Induktionsvoraussetzung für $n = 2$ und (i).

### 3.24. Chinesischer Restsatz

Es sei $R$ ein kommutativer Ring mit 1. Dann gilt für paarweise komaximale Ideale $\mathfrak{a}_i$ $(1 \le i \le n)$ (d.h. $\mathfrak{a}_i + \mathfrak{a}_j = R$ $(1 \le i < j \le n)$):

$$R/\mathfrak{a}_1 \cdot \ldots \cdot \mathfrak{a}_n \cong \prod_{i=1}^{n} R/\mathfrak{a}_i$$

Lösung simultaner Kongruenzen:

Suche alle $x$ mit

$$\begin{aligned} x &\equiv 2 \bmod 5, \quad \mathfrak{a}_1 = 5\mathbb{Z} \\ x &\equiv 4 \bmod 11, \quad \mathfrak{a}_2 = 11\mathbb{Z} \\ x &\equiv 7 \bmod 12, \quad \mathfrak{a}_3 = 12\mathbb{Z} \end{aligned}$$

oder "ewiger Kalender".

Beweis:
Betrachte Abbildung

$$\phi \,:\, R \to \prod_{i=1}^{n} R/\mathfrak{a}_i \,:\, x \mapsto (x + \mathfrak{a}_1, \ldots, x + \mathfrak{a}_n).$$

Offensichtlich ist $\phi$ ein Ringhomomorphismus mit $\ker \phi = \mathfrak{a}_1 \cap \ldots \cap \mathfrak{a}_n = \mathfrak{a}_1 \cdot \ldots \cdot \mathfrak{a}_n$. Es bleibt "$\phi$ surjektiv" zu zeigen, dann folgt die Behauptung aus dem Homomorphiesatz für Ringe (2.14)(i). Nach Voraussetzung existieren $e_{ij} \in \mathfrak{a}_i,\ e_{ji} \in \mathfrak{a}_j$ mit $1 = e_{ij} + e_{ji}$ $(1 \le i < j \le n)$. Setze

$$\tilde{e}_i := \prod_{\substack{j=1 \\ j \ne i}}^{n} e_{ji} \quad (1 \le i \le n).$$

$$\tilde{e}_i \equiv \begin{cases} 0 \bmod \mathfrak{a}_j \\ 1 \bmod \mathfrak{a}_i \quad (j \ne i). \end{cases}$$

Ist dann $(x_1 + \mathfrak{a}_1, \ldots, x_n + \mathfrak{a}_n) \in \prod_{i=1}^{n} R/\mathfrak{a}_i$ vorgelegt, so ist dies Bild von $x = \sum_{i=1}^{n} x_i\, \tilde{e}_i$. Denn für $\tilde{e}_i$ gilt $\tilde{e}_i \in \mathfrak{a}_j$ $(1 \le j \le n,\ j \ne i)$,

$$\tilde{e}_i \equiv \begin{cases} 1 \bmod \mathfrak{a}_i \\ 0 \bmod \mathfrak{a}_j \quad (j \ne i) \end{cases}.$$

□

$$R/(\mathfrak{a}_1 \cdot \ldots \cdot \mathfrak{a}_n) \;=\; \dot{+}_{i=1}^{n} \Big(R/(\mathfrak{a}_1 \cdot \ldots \cdot \mathfrak{a}_n)\Big)\tilde{e}_i \;\cong\; R/\mathfrak{a}_1 \oplus \ldots \oplus R/\mathfrak{a}_n.$$

Bemerkung:
Der Satz sagt aus, daß sich simultane Kongruenzen nach komaximalen Idealen stets lösen lassen. Er beschreibt die Lösungsmenge und gibt

sogar ein (konstruktives) Verfahren zu ihrer Bestimmung an. ("Zerlegung der Eins in orthogonale Idempotente").

### Newton-Verfahren

Eine explizite Berechnung des Urbildes von $(x_1 + \mathfrak{a}_1, \cdots, x_n + \mathfrak{a}_n)$ ist allerdings schneller möglich mit dem folgenden Verfahren, welches der Newton-Interpolation ähnelt.
Setze

$$e_i := \prod_{j=1}^{i-1} e_{ji} \quad (1 < i \leq n)$$

ähnlich zum Beweis sowie $y_1 = x_1$ und iterativ $y_{k+1} = y_k + (x_{k+1} - y_k)e_{k+1} \quad (1 \leq k < n)$.
Dann leistet $x = y_n$ das Gewünschte.

Beispiel:
Löse $x \equiv 2 \bmod 5,\ x \equiv 4 \bmod 11,\ x \equiv 7 \bmod 12$.
1. Lösungmöglichkeit: Raten.
2. Lösungmöglichkeit: per (2.38)!
$\mathfrak{a}_1 = 5\mathbb{Z},\ \mathfrak{a}_2 = 11\mathbb{Z},\ \mathfrak{a}_3 = 12\mathbb{Z},\ R = \mathbb{Z}$.
$\mathfrak{a}_i + \mathfrak{a}_j = R,\ e_{ij} + f_{ij} = 1$ mit $e_{ij} \in \mathfrak{a}_i$ und $f_{ij} \in \mathfrak{a}_j$.

| $i$ | 1 | 1 | 2 | 2 | 3 | 3 |
|---|---|---|---|---|---|---|
| $j$ | 2 | 3 | 1 | 3 | 1 | 2 |
| $e_{ij}$ | $-10$ | 25 | 11 | $-11$ | $-24$ | 12 |
| $f_{ij}$ | 11 | $-24$ | $-10$ | 12 | 25 | $-11$ |

$$\begin{array}{rcrcr} \tilde{e}_1 & = & f_{12}\, f_{13} & = & -264 \\ \tilde{e}_2 & = & f_{21}\, f_{23} & = & -120 \\ \tilde{e}_3 & = & f_{31}\, f_{32} & = & -75 \end{array}.$$

Gesucht sind $u, v$ mit $u \cdot 5 + v \cdot 11 = 1 \ \Rightarrow\ 1 = -2 \cdot 5 + (+11) = 5 \cdot 5 - 2 \cdot 12 = -11 + 12$.

$$\begin{aligned} x &= x_1\tilde{e}_1 + x_2\tilde{e}_2 + x_3\tilde{e}_3 \\ &= -2 \cdot 264 - 4 \cdot 120 - 7 \cdot 275 \\ &= -528 - 480 - 1925 \\ &= -2933; \end{aligned}$$

das Ergebnis ist modulo $5 \cdot 11 \cdot 12 = 660$ eindeutig, also ist die kleinste positive Lösung 367, die betraglich kleinste Lösung $-293$.
Gesamtlösung ist $367 + 660\mathbb{Z}$.

Nach dem Newton Verfahren verläuft die Berechnung wie folgt:
$e_1 = 1, e_2 = -10, e_3 = -275$,
$y_1 = 2, y_2 = 2 + (4 - 2)(-10) = -18$,
$y_3 = -18 + (7 - (-18))(-275) = -6893 \equiv -293 \bmod 660$.

### 3.25. Definition

Es sei $M$ eine nicht leere Menge. Eine Relation $\leq$ auf $M$ heißt Halbordnung, falls die Bedingungen

(i) $x \leq x$
(ii) $x \leq y \wedge y \leq x \;\Rightarrow\; x = y$
(iii) $x \leq y \wedge y \leq z \;\Rightarrow\; x \leq z$

$\forall x,\, y,\, z \in M$ erfüllt sind.

Beispiele:

(i) $(\mathbb{Z}, \geq 0)$, $(\mathbb{R}, \geq 0)$, lexikographische Ordung im $\mathbb{R}^n$;
(ii) $(\mathbb{C}, |\ |)$ erfüllt (i), (iii) aber nicht (ii);
(iii) $\mathfrak{P}(M)$ mit $\subseteq$:
$M = \{1, 2\}$ hat $\mathfrak{P}(M) = \{\emptyset, \{1\}, \{2\}, M\}$.
$\emptyset \subseteq \{1\} \subseteq M$, $\emptyset \subseteq \{2\} \subseteq M$. $\{1\}$ ist in $\{2\}$ nicht enthalten.

### 3.26. Definition

Es sei $M$ eine nicht leere Menge. Eine Halbordung $\leq$ auf $M$ heißt Ordnung, falls für alle $x,\, y \in M$ stets $x \leq y$ oder $y \leq x$ gilt. In diesem Fall heißt $M$ Kette.

Beispiel:
$(\mathbb{R}, \geq)$, nicht aber $(\mathbb{C}, |\ |)$.

### 3.27. Definition

Es sei $M \neq \emptyset$ und $\leq$ eine Halbordnung auf $M$. Für $A \subseteq M$ heißt $s(A) \in M$ obere Schranke von $A$, falls $x \leq s(A)\ \forall a \in A$ gilt. Für $A \subseteq M$ heißt $m(A) \in A$ maximales Element von $A$, falls aus $a \in A$ und $m(A) \leq a$ stets $a = m(A)$ folgt. Eine Teilmenge $X$ von $M$ heißt induktiv geordnet, falls jede Kette in $X$ eine obere Schranke in $X$ (!) besitzt.

Beispiel:
$A = \{\{1\}, \{2\}, \emptyset\} \subseteq \mathfrak{P}(\{1, 2\})$;
Es ist $s(A) = \{1, 2\}$; sowohl $\{1\}$ als auch $\{2\}$ sind maximale Elemente von $A$.

### 3.28. Zornsches Lemma

Jede nicht leere induktiv geordnete Menge besitzt ein maximales Element.

### 3.29. Definition

Es sei $R$ Ring mit Ideal $\mathfrak{a}$. $\mathfrak{a}$ heißt maximal, falls es kein Ideal $\mathfrak{b}$ mit $\mathfrak{a} \subset \mathfrak{b} \subset R$ gibt.

### 3.30. Satz

Es sei $V$ ein Vektorraum über dem Körper $K$ und $M \subseteq V$ linear unabhängig. Dann existiert eine Basis $B$ von $V$ mit $M \subseteq B$.

Beweis:
Es bestehe $Q \subseteq P(V)$ aus allen linear unabhängigen Teilmengen von $V$, die $M$ enthalten. Wegen $M \in Q$ folgt $Q \neq \emptyset$. Ist $K$ eine Kette in $Q$, so gilt

$$m(K) := \bigcup_{N \in K} N \ \in Q.$$

Denn sind $x_1, \ldots, x_n \in m(K)$, d.h. $x_i \in N_i \ (1 \leq i \leq n)$, so existiert ein maximaler Index $j$, mit $x_i \in N_j \ (1 \leq i \leq n)$, also sind $x_1, \ldots, x_n$ linear unabhängig.
Nach dem Zornschen Lemma existiert in $Q$ ein maximales Element $B$. Nach Voraussetzung ist $B$ linear unabhängig. Es bleibt $[B] = V$ zu zeigen.
Ist $x \in V \backslash [B]$, so gilt speziell $x \neq 0$, und $\tilde{B} := B \cup \{x\}$ ist linear abhängig. Also existieren $x_1, \ldots, x_r \in B$ und $\lambda_1, \ldots, \lambda_r, \ \lambda \in K$, nicht alle 0, mit

$$\sum_{i=1}^{r} \lambda_i x_i + \lambda\, x = 0.$$

Für $\lambda \neq 0$ folgt $x \in [B]$. Für $\lambda = 0$ folgt $B$ linear abhängig. Widerspruch!

□

Bemerkung:
Also folgt die Behauptung. Für $M = \emptyset$ liefert dies die Existenz einer Basis von $V$.

### 3.31. Satz

Es sei $R$ ein Ring mit $1 \neq 0$ und $\mathfrak{a} \neq R$ ein Ideal von $R$. Dann ist $\mathfrak{a}$ in einem maximalen Ideal $\mathfrak{m}$ von $R$ enthalten.

Bemerkung:
Für $\mathfrak{a} = \{0\}$ liefert dies die Existenz maximaler Ideale (in Ringen $R$ mit Eins).

Beweis:
Es sei $\mathfrak{M}$ die Menge aller Ideale $\mathfrak{b}$ von $R$ mit $R \supset \mathfrak{b} \supseteq \mathfrak{a}$, dann ist $\mathfrak{M} \neq \emptyset$ induktiv geordnet bzgl. $\subseteq$. (Die Vereinigungsmenge einer aufsteigenden Kette von Idealen ist wieder ein Ideal, welches in unserem Fall 1 nicht enthält.)
Nach dem Zornschen Lemma existiert ein maximales Element $\mathfrak{m}$ aus $\mathfrak{M}$. Wegen $1 \notin \mathfrak{m}$ ist $\mathfrak{m}$ maximales Ideal.

□

Bemerkung:

(i) In $\mathbb{Z}$ sind $p\mathbb{Z}$, $p$ Primzahl, genau die maximalen Ideale.
(ii) Ist $R$ Körper, so ist $\{0\}$ einziges maximales Ideal.

### 3.32. Satz

Es sei $R$ ein Ring mit Ideal $\mathfrak{m}$. Dann gilt:

(i) $\mathfrak{m} \neq R$ ist maximal $\Leftrightarrow$ $R/\mathfrak{m}$ enthält nur die Ideale $\mathfrak{m}$ und $R/\mathfrak{m}$.
(ii) Ist $R$ kommutativ mit $1 \neq 0$, so ist $\mathfrak{m}$ genau dann maximal, falls $R/\mathfrak{m}$ Körper ist.

Beweis:

(i) Gemäß (2.15).
(ii)

$$\begin{aligned} R/\mathfrak{m} \text{ Körper} &\Leftrightarrow \forall x \in R\backslash\mathfrak{m},\ \exists\, \lambda \in R :\ (x+\mathfrak{m})\,(\lambda+\mathfrak{m}) = 1+\mathfrak{m} \\ &\Leftrightarrow \forall x \in R\backslash\mathfrak{m},\ \exists \lambda \in R :\ \lambda x \equiv 1 \bmod \mathfrak{m} \\ &\Leftrightarrow \forall x \in R\backslash\mathfrak{m},\ \exists m \in \mathfrak{m},\ \exists \lambda \in R :\ \lambda x + m = 1 \\ &\Leftrightarrow Rx + \mathfrak{m} = R\ \ \forall x \in R\backslash\mathfrak{m} \\ &\Leftrightarrow \mathfrak{m} \text{ maximal.} \end{aligned}$$

□

### 3.33. Definition

Ein kommutativer Ring $R$ mit Eins heißt lokaler Ring, falls $R$ genau ein maximales Ideal besitzt.

### 3.34. Hilfssatz

$R$ kommutativ mit 1. $R$ lokaler Ring $\Leftrightarrow$ $R\backslash R^\times$ ist Ideal in $R$.

Beweis:
"$\Leftarrow$":
Jedes Ideal $\mathfrak{a}$ in $R$ mit $\mathfrak{a} \neq R$ beteht aus Nichteinheiten.

"$\Rightarrow$":
Für $x \in R,\ x \notin U(R)$, folgt $Rx = (x) \subseteq \mathfrak{m}$ für ein passendes maximales Ideal $\mathfrak{m}$ von $R$.

□

Beispiel:
$\dfrac{\mathbb{Z}}{\mathbb{Z}\backslash p\mathbb{Z}} = \left\{ \dfrac{r}{s} \in \mathbb{Q} \,\middle|\, r \in \mathbb{Z},\ p \nmid s \right\}$ ist lokaler Ring mit $\mathfrak{m} = \dfrac{p\mathbb{Z}}{\mathbb{Z}\backslash p\mathbb{Z}}$.

**Quotientenbildung bei kommutativen Ringen $R$.** Es sei $R$ ein kommutativer Ring und $S \subseteq R$ eine multiplikative Halbgruppe. Als "Brüche" (mit Nennern in $S$) definiert man die Menge $R \times S$ der geordneten Paare $(r,\, s)$. Wie bei der Konstruktion der rationalen aus den ganzen Zahlen bildet man auf $R \times S$ eine Äquivalenzrelation, deren Klassen dann die gewünschten Brüche bilden. Wegen der möglichen Existenz von Nullteilern muß man allgemeiner

$$(r,\, s) \sim (\tilde{r},\, \tilde{s}) \quad :\Leftrightarrow \quad \exists t \in S \,:\, t\,(r\tilde{s} - \tilde{r}s) = 0 \text{ definieren.}$$

Dies ist tatsächlich eine Äquivalenzrelation, denn Reflexivität und Symmetrie sind klar und bzgl. der Transitivität bemerken wir:

$$\begin{aligned}
&(r_1,\, s_1) \sim (r_2,\, s_2) \,\wedge\, (r_2,\, s_2) \sim (r_3,\, s_3)\\
&\Leftrightarrow\ \exists t_1,\, t_2 \in S \,:\, t_1\,(r_1 s_2 - r_2 s_1) = 0 = t_2\,(r_2 s_3 - r_3 s_2)\\
&\Rightarrow\ \exists t_1,\, t_2 \in S \,:\quad 0 \;=\; t_1 t_2 s_3\,(r_1 s_2 - r_2 s_1) + t_1 t_2 s_1\,(r_2 s_3 - r_3 s_2)\\
&\qquad\qquad\qquad\quad \;=\; t_1 t_2 s_2\,(s_3 r_1 - s_1 r_3)\\
&\qquad\qquad\qquad\quad \;=\; t\,(s_3 r_1 - s_1 r_3) \ \text{ für } \ t = t_1 t_2 s_2\\
&\Rightarrow\ \exists t \in S \,:\, t\,(s_3 r_1 - s_1 r_3) = 0\\
&\Leftrightarrow\ (r_1,\, s_1) \sim (r_3,\, s_3).
\end{aligned}$$

Die Äquivalenzklassen bilden Brüche:

$$K_{r,s} := \{(\tilde{r},\, \tilde{s}) \in R \times S \,|\, (r,\, s) \sim (\tilde{r},\, \tilde{s})\} =: \frac{r}{s}.$$

Setze

$$\begin{aligned}
K_{r_1,s_1} + K_{r_2,s_2} &= K_{r_1 s_2 + r_2 s_1,\, s_1 s_2},\\
K_{r_1,s_1} \cdot K_{r_2,s_2} &= K_{r_1 s_1,\, r_2 s_2}.
\end{aligned}$$

(Für die Äquivalenzklassen $\frac{r_1}{s_1}$, $\frac{r_2}{s_2}$ von $(r_1,\, s_1)$, $(r_2,\, s_2) \in R \times S$ definieren wir eine Addition und eine Multiplikation über die Vertreter:

$$\frac{r_1}{s_1} + \frac{r_2}{s_2} := \frac{r_1 s_2 + r_2 s_1}{s_1 s_2}, \quad \frac{r_1}{s_1} \cdot \frac{r_2}{s_2} := \frac{r_1 r_2}{s_1 s_2}.)$$

Zur Multiplikation: Sind auch $(\tilde{r}_1,\, \tilde{s}_1) \in \frac{r_1}{s_1}$, $(\tilde{r}_2,\, \tilde{s}_2) \in \frac{r_2}{s_2}$, so ist $(r_1 r_2,\, s_1 s_2) \sim (\tilde{r}_1 \tilde{r}_2,\, \tilde{s}_1 \tilde{s}_2)$ wegen

$$\begin{aligned}
&(r_1,\, s_1) \sim (\tilde{r}_1,\, \tilde{s}_1) \,\wedge\, (r_2,\, s_2) \sim (\tilde{r}_2,\, \tilde{s}_2)\\
&\Leftrightarrow\ \exists t_1,\, t_2 \in S \,:\, t_1\,(r_1 \tilde{s}_1 - \tilde{r}_1 s_1) = 0 = t_2\,(r_2 \tilde{s}_2 - s_2 \tilde{r}_2)\\
&\Rightarrow\ \exists t_1,\, t_2 \in S \,:\, 0 = t_1 t_2\,(r_1 r_2 \tilde{s}_1 \tilde{s}_2 - \tilde{r}_1 r_2 s_1 \tilde{s}_2) + t_1 t_2\,(\tilde{r}_1 r_2 s_1 \tilde{s}_2 - \tilde{r}_1 \tilde{r}_2 s_1 s_2)\\
&\Rightarrow\ \exists t_1 t_2 \in S \,:\, 0 = t_1 t_2\,(r_1 r_2 \tilde{s}_1 \tilde{s}_2 - \tilde{r}_1 \tilde{r}_2 s_1 s_2)\\
&\Leftrightarrow\ (r_1 r_2,\, s_1 s_2) \sim (\tilde{r}_1 \tilde{r}_2,\, \tilde{s}_1 \tilde{s}_2);
\end{aligned}$$

für die Addition folgert man aus

$$\begin{aligned}
&\exists t_1,\, t_2 \in S \,:\, 0 = t_1\,(r_1 \tilde{s}_1 - \tilde{r}_1 s_1) = t_2\,(r_2 \tilde{s}_2 - s_2 \tilde{r}_2)\\
&\Rightarrow\ \exists t_1,\, t_2 \in S \,:\, 0 = t_1 t_2\,(r_1 \tilde{s}_1 s_2 \tilde{s}_2 - \tilde{r}_1 s_1 s_2 \tilde{s}_2 + r_2 \tilde{s}_2 s_1 \tilde{s}_1 - s_2 \tilde{r}_2 s_1 \tilde{s}_1)\\
&\Rightarrow\ \exists t_1,\, t_2 \in S \,:\, 0 = t_1 t_2\,((r_1 s_2 + r_2 s_1)\,\tilde{s}_1 \tilde{s}_2 - (\tilde{r}_1 \tilde{s}_2 + \tilde{r}_2 \tilde{s}_1)\, s_1 s_2)\\
&\Leftrightarrow\ (r_1 s_2 + r_2 s_1,\, s_1 s_2) \sim (\tilde{r}_1 \tilde{s}_2 + \tilde{r}_2 \tilde{s}_1,\, \tilde{s}_1 \tilde{s}_2).
\end{aligned}$$

Die Rechengesetze von $R$ übertragen sich über die Vertreter auf

$$R_S := \left\{ \frac{r}{s} \mid r \in R,\ s \in S \right\} \quad \text{für} \quad \frac{r}{s} = K_{r,s}.$$

Hierfür sind die Assoziativität von Addition und Multiplikation nachzurechnen. Neues Nullelement ist $K_{0,s}$, inverses Element zu $K_{r,s}$ ist $K_{-r,s}$.

Folglich bildet $R_S$ einen kommutativen Ring mit Einselement $\frac{s}{s}$ :

$$\frac{r}{s} \cdot \frac{s}{s} = \frac{r}{s} \quad \forall \frac{r}{s} \in R_S.$$

$R$ läßt sich homomorph in $R_S$ abbilden mittels

$$\iota \ : \ R \to R_S \ : \ r \mapsto \frac{rs}{s}$$

für ein beliebiges $s \in S$.
Im Fall, daß $S \neq 0$ keine Nullteiler enthält, ist $\iota$ sogar Monomorphismus, also Einbettung, d.h. $R_S$ läßt sich als Ringerweiterung von $R$ auffassen.

Spezialfälle:

(i) $S \ni 0 \ \Rightarrow \ R_S$ ist trivial.
(ii) $\emptyset \neq S$ besteht aus allen Nicht-Nullteilern $\neq 0$ von $R$. In diesem Fall heißt $R_S$ der (vollständige) Quotientenring $\mathfrak{Q}(R)$ von $R$. Sind speziell alle Elemente $\neq 0$ keine Nullteiler, so ist $\mathfrak{Q}(R)$ ein Körper.

Beispiel:

(i) $R = \mathbb{Z},\ S = \mathbb{Z}\backslash\{0\} \ \Rightarrow \ R_S \cong \mathbb{Q}$.
(ii) $R = \mathbb{Z},\ S = \{2^\nu \mid \nu \in \mathbb{Z}^{\geq 0}\} \ \Rightarrow \ R_S = \{\frac{a}{2^\nu} \mid \nu \in \mathbb{Z}^{\geq 0}\}$.
(iii) $R = \mathbb{Z},\ S = \mathbb{Z}\backslash p\mathbb{Z} \quad (p \in \mathbb{P}) \ \Rightarrow \ R_S = \mathbb{Z}_{(p)}$ ("$p$-Lokalisierung von $\mathbb{Z}$").

### 3.35. Definition

Es sei $R$ ein kommutativer Ring. Ein Ideal $R \supsetneq \mathfrak{p}$ von $R$ heißt Primideal, falls für $a,\ b \in R$ mit $ab \in \mathfrak{p}$ stets $a \in \mathfrak{p}$ oder $b \in \mathfrak{p}$ folgt.

Beispiele:

(i) $R = \mathbb{Z}$, alle Primideale sind von der Form $p\mathbb{Z}$ mit $p$ Primzahl.
(ii) $\{0\}$ ist Primideal, falls $R$ keine Nullteiler $\neq 0$ besitzt.

### 3.36. Satz (Charakterisierung von Primidealen)

Es sei $R$ ein kommutativer Ring und $\mathfrak{a} \subsetneq R$ ein Ideal in $R$. Dann sind äquivalent:

(i) $\mathfrak{a}$ Primideal,
(ii) $\forall a,\ b \in R$ mit $a \notin \mathfrak{a}$ und $b \notin \mathfrak{a} \ \Rightarrow \ ab \notin \mathfrak{a}$,
(iii) Für Ideale $\mathfrak{b}, \mathfrak{c}$ von $R$ mit $\mathfrak{bc} \subseteq \mathfrak{a}$ folgt $\mathfrak{b} \subseteq \mathfrak{a}$ oder $\mathfrak{c} \subseteq \mathfrak{a}$.

(iv) $R\backslash\mathfrak{a}$ ist multiplikative Halbgruppe,
(v) $R/\mathfrak{a}$ ist nullteilerfrei.

Beweis:
(i) $\Rightarrow$ (ii): nach Definition;

(ii) $\Rightarrow$ (iii): Wäre die Aussage falsch, existierten Elemente $b \in \mathfrak{b} \setminus \mathfrak{a},\ c \in \mathfrak{c} \setminus \mathfrak{a}$ mit $b \cdot c \in \mathfrak{a}$ im Widerspruch zur Voraussetzung.

(iii) $\Rightarrow$ (iv): Sind $a, b \in R \setminus \mathfrak{a}$, so folgt $(a) = Ra + \mathbb{Z}a,\ (b) = Rb + \mathbb{Z}b,\ (a)(b) = Rab + \mathbb{Z}ab = (ab)$. Wegen $(a) \not\subseteq \mathfrak{a}$ und $(b) \not\subseteq \mathfrak{a}$ muss $(ab) \not\subseteq \mathfrak{a}$ gelten, also $ab \notin \mathfrak{a}$.

(iv) $\Rightarrow$ (v): für $a + \mathfrak{a},\ b + \mathfrak{a}$, beide ungleich $\mathfrak{a}$, folgt $a,\ b \in R\backslash\mathfrak{a}$, damit $ab \in R\backslash\mathfrak{a}$ und

$$(a + \mathfrak{a})\,(b + \mathfrak{a}) = ab + \mathfrak{a} \neq \mathfrak{a};$$

(v) $\Rightarrow$ (i): es seien $a,\ b \in R$ mit $ab \in \mathfrak{a}$, also

$$\mathfrak{a} = ab + \mathfrak{a} = (a + \mathfrak{a})\,(b + \mathfrak{a})$$

und folglich $(a + \mathfrak{a} = \mathfrak{a} \ \Leftrightarrow\ a \in \mathfrak{a})$ oder $(b + \mathfrak{a} = \mathfrak{a} \ \Leftrightarrow\ b \in \mathfrak{a})$.

□

Bemerkung:

(i) In einem kommutativen Ring mit 1 ist jedes maximale Ideal ein Primideal, also ist jedes Ideal $\mathfrak{a} \subset R$ von $R$ in einem Primideal enthalten.

(ii) In einem kommutativen Ring $R$ mit Primideal $\mathfrak{p}$ bildet $R\backslash\mathfrak{p}$ eine multiplikative Halbgruppe $S$. Dann heißt

$$R_S = R_{R\backslash\mathfrak{p}} = \frac{R}{R\backslash\mathfrak{p}} =: R_{\mathfrak{p}}$$

Lokalisierung von $R$ bei $\mathfrak{p}$. $R_{\mathfrak{p}}$ ist ein lokaler Ring (siehe Übungsblatt 7).

(Falls $R \ni 1\ :\ R \to \frac{R}{R\backslash\mathfrak{p}}\ :\ r \mapsto \frac{r}{1}$ ist Ringmonomorphismus.)

Speziell: $R = \mathbb{Z},\ \mathfrak{p} = p\mathbb{Z}$ für $p \in \mathbb{P}$ :

$$R_{(p)} = \left\{ \frac{m}{n} \middle| \, m \in \mathbb{Z},\, n \in \mathbb{Z} \text{ mit } p \nmid n \right\}.$$

(iii) 0 Primideal $\Rightarrow$ $R$ nullteilerfrei.

(iv) $R \ni 1$, $\mathfrak{p}$ Primideal, $R/\mathfrak{p}$ nullteilerfrei:
$R/\mathfrak{p}$ endlich $\Rightarrow$ $R/\mathfrak{p}$ Körper
$\overset{2.29}{\Rightarrow}$ $\mathfrak{p}$ maximales Ideal.

Beispiele:

(i) $\mathfrak{p} = 2\mathbb{Z} \ \Rightarrow\ R_{\mathfrak{p}} = \left\{ \frac{a}{b} \middle| \ a,\, b \in \mathbb{Z},\ 2 \nmid b \right\}.$

(ii) $R = 2\mathbb{Z}, \mathfrak{a} = 4\mathbb{Z}$ :
$2 \cdot 2 \in \mathfrak{a}$, also ist $\mathfrak{a}$ kein Primideal. $\mathfrak{a}$ ist maximal, denn $x \in R \backslash \mathfrak{a}$ hat die Gestalt $2(2m+1)$,
$(\mathfrak{a}, x) \ni x - 4m = 2$.

### 3.37. Definition

Ein Ring $R$, in dem jedes Ideal endlich erzeugt ist, heißt noetherscher Ring.

Beispiel: $R = \mathbb{Z}$, dort ist jedes Ideal Hauptideal.

### 3.38. Satz (Charakterisierung noetherscher Ringe)

Für Ringe $R$ sind folgende Aussagen äquivalent:

(i) $R$ ist noethersch;
(ii) Jede aufsteigende Kette von Idealen $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \subseteq \ldots \subseteq \mathfrak{a}_k \subseteq \ldots$ wird stationär (bricht ab), d.h. es existiert $n \in \mathbb{N}$ mit $\mathfrak{a}_{n+i} = \mathfrak{a}_n \; \forall i \in \mathbb{N}$;
(iii) In jeder nicht leeren Menge von Idealen gibt es ein (bzgl. $\subseteq$) maximales Element.

Beweis:
(i) $\Rightarrow$ (ii):
Für eine vorgelegte Kette von Idealen ist deren Vereinigung $\mathfrak{a}$ wieder ein Ideal(!), welches etwa durch $a_1, \ldots, a_m$ erzeugt wird. Für $a_i \in \mathfrak{a}_{j_i}$ $(1 \leq i \leq m)$ gilt dann also $\mathfrak{a}_{j_0} \supseteq (a_1, \ldots, a_m) \supseteq \mathfrak{a}_{j_0}$, $a_i \in \mathfrak{a}_{j_0}$ $(1 \leq i \leq m)$ mit $j_0 := \max\{j_1, \ldots, j_m\}$, und wir erhalten etwa $n = j_0$, d.h. die Kette wird ab $\mathfrak{a}_{j_0}$ stationär.
(ii) $\Rightarrow$ (iii):
Es sei $\mathfrak{M} \neq \emptyset$ eine Menge von Idealen. Wähle $\mathfrak{a}_1 \in \mathfrak{M}$. Ist $\mathfrak{a}_1$ maximal, so sind wir fertig. Ist $\mathfrak{a}_1$ nicht maximal, so exitiert $\mathfrak{a}_2 \in \mathfrak{M}$, $\mathfrak{a}_2 \supset \mathfrak{a}_1$. Man erhält so eine aufsteigende Kette, die nach Voraussetzung stationär werden muß. Das diesbezügliche $\mathfrak{a}_n$ ist dann in $\mathfrak{M}$ maximal.
(iii) $\Rightarrow$ (i):
Es sei $\mathfrak{a}$ ein Ideal von $R$. Bilde

$$\mathfrak{M} := \{\mathfrak{b} \mid \mathfrak{b} \text{ endlich erzeugtes Ideal in } R \text{ mit } \mathfrak{b} \subseteq \mathfrak{a}\}.$$

Wegen $\{0\} \in \mathfrak{M}$ ist $\mathfrak{M} \neq \emptyset$. Sei $\mathfrak{m}$ maximales Element von $\mathfrak{M}$, etwa $\mathfrak{m} =< a_1, \ldots, a_k >$. Für beliebiges $a \in \mathfrak{a}$ ist $\tilde{\mathfrak{m}} := (a_1, \ldots, a_k, a)$ in $\mathfrak{M}$, also gleich $\mathfrak{m}$, also folgt $\mathfrak{a} = \mathfrak{m}$.

□

Bemerkung:
Es sei $R$ ein noetherscher Ring und $f : R \to S$ ein Ringepimorphismus. Dann ist $S$ noethersch.
(Speziell: Ist $\mathfrak{a}$ ein Ideal von $R$, so ist $R/\mathfrak{a}$ noethersch.)

Beweis:
Es sei $\mathfrak{a}$ ein Ideal von $S$, dann ist etwa $f^{-1}(\mathfrak{a}) =< a_1, \ldots, a_k >$, und es folgt $\mathfrak{a} = (f(a_1), \ldots, f(a_k))$.

□

## Teilbarkeit in Ringen

Sinnvollerweise sind Nullteiler auszuschließen!
Ferner: $R \ni 1 \neq 0$ und $R$ sollte kommutativ sein.

### 3.39. Definition

Ein nullteilerfreier, kommutativer Ring $R \neq \{0\}$ heißt Integritätsring.

Bemerkung:
In Integritätsringen gilt die Kürzungsregel (2.19)(i), endliche Integritätsringe sind Körper (2.19)(ii). $R$ kommuativer Ring, $\mathfrak{a} \subset R$ Ideal: $\mathfrak{a}$ Primideal $\Leftrightarrow$ $R/\mathfrak{a}$ Integritätsring nach (2.33).

Beispiel: Alle Ideale $\neq \{0\}$ in $\mathbb{Z}$ und Körper sind Integritätsringe.

### 3.40. Definition

Es seien $R$ ein Integritätsring mit 1 und $a, b \in R$.
$a$ heißt Teiler von $b$ ($a$ teilt $b$, $b$ ist Vielfaches von $a$, $a|b$), falls $c \in R$ mit $b = ac$ existiert.
$a$ heißt assoziiert zu $b$ ($a \sim b$), falls $a|b$ und $b|a$ gilt.
$c \in R$ heißt größter gemeinsamer Teiler (ggT) von $a$, $b$, falls $c|a$ und $c|b$ und für alle $d \in R$ mit $d|a$, $d|b$ auch $d|c$ gilt.
$a$, $b$ heißen teilerfremd, falls $\mathrm{ggT}\,(a, b) \in U(R)$ ist.
$c \in R$ heißt kleinstes gemeinsames Vielfaches (kgV) von $a$, $b$, falls $a|c$, $b|c$ und für alle $d \in R$ mit $a|d$, $b|d$ auch $c|d$ gilt.
Ein Element $p \in R \backslash U(R)$, $p \neq 0$, heißt Primelement von $R$, wenn für alle $a$, $b \in R$ mit $p|ab$ stets $p|a$ oder $p|b$ folgt.
Ein Element $a \in R \backslash U(R)$, $q \neq 0$ heißt irreduzibel (unzerlegbar), wenn für alle $a$, $b \in R$ mit $ab = q$ stets $a \in U(R)$ oder $b \in U(R)$ folgt.

Beispiele:

(i) Übliche Definitionen in $\mathbb{Z}$; die zu $a \in \mathbb{Z}$ assoziierten Elemente sind $\pm a$ ($U(R) = \{\pm 1\}$), die Primzahlen sind die Primelemente und stimmen mit den irreduziblen Elemente überein.

(ii) Es sei $R = \mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$. Es gibt unendlich viele assoziierte Elemente $a\,(-1)^h\,(1 + \sqrt{2})^k$ ($h \in \{0, 1\}$, $k \in \mathbb{Z}$).

$$1+\sqrt{2} = \frac{(1+\sqrt{2})\,(1-\sqrt{2})}{1-\sqrt{2}} = \frac{-1}{1-\sqrt{2}} \quad \Rightarrow \quad \begin{array}{rcl} (1-\sqrt{2})^{-1} & = & -(1+\sqrt{2}), \\ (1+\sqrt{2})^{-1} & = & -(1-\sqrt{2}) \end{array}$$

$((1 + \sqrt{2})^k$ ($k \in \mathbb{Z}$) sind alle verschieden!)
$\sqrt{2}$ ist irreduzibel (und sogar Primelement!).

(Denn für $S := \mathbb{Z}[\sqrt{m}]$ $(m \in \mathbb{Z},\ \nexists a \in \mathbb{Z}^{\geq 2} : a^2 | m)$ ist

$$N : \mathbb{Z}[\sqrt{m}] \to \mathbb{Z} : a + b\sqrt{m} \mapsto a^2 - mb^2$$

eine multiplikativer Homomorphismus. Wäre nun $\sqrt{2} = xy$ in $\mathbb{Z}[\sqrt{2}]$, so folgte $N(\sqrt{2}) = -2 = N(x)\,N(y)$ in $\mathbb{Z}$, also $N(x) = \pm 1$ oder $N(y) = \pm 1$. Ist o.B.d.A. $N(x) = \pm 1$, so gilt für $x = u + v\sqrt{2}$ : $\pm 1 = (u + v\sqrt{2})\,(u - v\sqrt{2})$, d.h. $x \in U(R)$.)

Der Primelementnachweis verläuft ähnlich.

(iii) Es sei $R = \mathbb{Z}[\sqrt{-5}]$. Hierin ist $U(R) = \{\pm 1\}$ $(= U(\mathbb{Z}))$, wegen

$$N(a + b\sqrt{-5}) = a^2 + 5b^2 = 1 \quad \Leftrightarrow \quad b = 0,\ a = \pm 1.$$

Ferner ist $21 = 3 \cdot 7 = (4 + \sqrt{-5})\,(4 - \sqrt{-5}) = (1 + 2\sqrt{-5})\,(1 - 2\sqrt{-5})$.

Hierin sind die beteiligten Elemente offenbar (!) keine Primelemente, jedoch irreduzibel.

Beweis:

Es ist $N(3) = 9$, für $3 = xy$ mit $x,\ y \notin \{\pm 1\}$ folgt $N(x) = N(y) = 3$, jedoch ist $N(u + v\sqrt{-5}) = u^2 + 5v^2 = 3$ unlösbar in $\mathbb{Z}$. Also ist 3 irreduzibel. Der Nachweis für die anderen Elemente geht analog.

Bemerkung:
Jede Einheit teilt alle Elemente aus $R$; $x|x$ und $x|0$ für alle $x \in R$; $a \in R$ mit $a|1 \ \Rightarrow\ a$ ist Einheit $(a \in U(R))$; $a,\ b,\ x \in R$ und $a|b \ \Rightarrow\ ax|bx$; $a,\ r_i,\ x_i \in R$ $(1 \leq i \leq n)$ und $a|x_i$ $(1 \leq i \leq n) \ \Rightarrow\ a \Big| \sum_{i=1}^{n} r_i x_i$; $a,\ b,\ c \in R$ und $a|b,\ b|c \ \Rightarrow\ a|c$; $a,\ b \in R$ : $a|b \ \Leftrightarrow\ b \in Ra \ \Leftrightarrow\ Rb \subseteq Ra$; $a,\ b \in R$ :
$a \sim b \ \Leftrightarrow \exists e \in U(R) : b = ae \ \Leftrightarrow\ Ra = Rb$.
Jedes Primelement ist irreduzibel; dies ist eine Konsequenz des folgenden Hilfssatzes.

### 3.41. Hilfssatz

Es sei $R$ ein Integritätsring mit 1 und $a \in R \backslash U(R),\ a \neq 0$. Dann gilt:

(i) $a$ Primelement $\Leftrightarrow$ $Ra$ Primideal;
(ii) $a$ irreduzibel $\Leftrightarrow$ $Ra$ maximales Hauptideal von $R$.
($a$ reduzibel $\Leftrightarrow$ $Ra$ nicht maximal in der Menge der Hauptideale von $R$.)

Beweis:

(i)

$$\begin{aligned} a \text{ Primelement} &\Leftrightarrow (\forall x,\, y \in R :\ a|xy \ \Rightarrow\ a|x \vee a|y) \\ &\Leftrightarrow (\forall x,\, y \in R :\ xy \in Ra \ \Rightarrow\ x \in Ra \vee y \in Ra) \\ &\Leftrightarrow Ra \text{ Primideal.} \end{aligned}$$

(ii)

$$\begin{aligned} a \text{ irreduzibel} &\Leftrightarrow (\forall x,\, y \in R :\ a = xy \ \Rightarrow\ x \in U(R) \vee y \in U(R)) \\ &\Leftrightarrow (\forall x \in R :\ Ra \subseteq Rx \ \Rightarrow\ x \in U(R) \vee x \sim a) \\ &\Leftrightarrow (\forall x \in R :\ Ra \subset Rx \ \Rightarrow\ x \in U(R)) \\ &\Leftrightarrow Ra \text{ maximales Hauptideal von } R. \end{aligned}$$

□

### 3.42. Definition

Ein Integritätring mit 1, in dem jedes Ideal Hauptideal ist, heißt Hauptidealring.

Bemerkung:

(i) Hauptidealringe sind noethersch.
(ii) $\mathbb{Z}$ ist Hauptidealring, ebenso sind alle Körper Hauptidealringe.
(iii) Für Elemente $a \neq 0$ in Hauptidealringen gilt:

$a$ Primelement $\Rightarrow$ $a$ irreduzibel $\overset{(2.41)(ii)}{\Rightarrow}$ $Ra$ maximales Hauptideal $\Rightarrow$ $Ra$ Primideal $\overset{(2.41)(i)}{\Rightarrow}$ $a$ Primelement.

Merke: In Hauptidealringen stimmen irreduzible und Primelemente überein. Speziell ist also $\mathbb{Z}[\sqrt{-5}]$ kein Hauptidealring.

(iv) Es seien $d, a_1, \ldots, a_n$ aus einem Hauptidealring $R$. Dann gilt:

$$d = \mathrm{ggT}\,(a_1, \ldots, a_n) \quad \Leftrightarrow \quad (a_1, \ldots, a_n) = Rd.$$

Dies bedeutet, daß ein größter gemeinsamer Teiler von $a_1, \ldots, a_n$ sich als $d = \sum_{i=1}^{n} r_i\, a_i$ $(r_i \in R)$ darstellen läßt.

Beweis:
Für jeden gemeinsamen Teiler $\tilde{d}$ von $a_1, \ldots, a_n$ gilt:

$$a_i = b_i\, \tilde{d} \quad \Leftrightarrow \quad (a_1, \ldots, a_n) \subseteq R\tilde{d}.$$

Ferner ist $(a_1, \ldots, a_n)$ ein Hauptideal $Rd$, für das dann $\tilde{d}|d$ und damit $d = \mathrm{ggT}\,(a_1, \ldots, a_n)$ gelten muß.

□

### 3.43. Satz

In einem Hauptidealring $R$ läßt sich jedes $x \in R\backslash U(R),\ a \neq 0$, als Produkt von Primelementen darstellen.

Beweis:
Gemäß der vorrangehenden Bemerkung (iii) genügt es, eine Darstellung von $x$ als Produkt irreduzibler Elemente nachzuweisen.
Ist $x$ irreduzibel, sind wir fertig. Ansonsten existieren $x_1,\ x_2 \in R\backslash U(R)$ mit $x = x_1 x_2$, und es ist $(x) \subsetneqq (x_i)\ \ (1 \leq i \leq 2)$. Analog versuchen wir $x_1,\ x_2$ zu faktorisieren und erhalten so nach $n$ Schritten $x$ als Produkt von $y_1, \ldots, y_n \in R\backslash U(R)$. Dabei werden die Faktoren so angeordnet, daß im Falle nicht irreduzibler Faktoren diese die höchsten Indizes bekommen. Wegen

$$(x) \subsetneqq (y_2 \cdot \ldots \cdot y_n) \subsetneqq \ldots \subsetneqq (y_{n-1}\, y_n) \subsetneqq (y_n)$$

muß dieser Prozeß abbrechen ($R$ ist als Hauptidealring noethersch), d.h. nach endlich vielen Schritten wird $x$ ein Produkt irreduzibler Elemente.

□

### 3.44. Definition

Ein Integritätsring mit 1 heißt ZPE-Ring (Ring mit eindeutiger Primelementzerlegung, faktorieller Ring), falls sich jedes $x \in R\backslash U(R),\ x \neq 0$, bis auf Einheiten eindeutig als Produkt irreduzibler Elemente darstellen läßt.
(Aus $x = \varepsilon\, q_1 \cdot \ldots \cdot q_r = \tilde{\varepsilon}\, \tilde{q}_1 \cdot \ldots \cdot \tilde{q}_s$ mit $\varepsilon,\ \tilde{\varepsilon} \in U(R),\ q_i,\ \tilde{q}_j$ irreduzibel folgt $r = s$ und nach eventueller Umnumerierung $q_i \sim \tilde{q}_i\ (1 \leq i \leq r)$.)

### 3.45. Satz

Für Integritätsringe $R$ mit 1 sind äquivalent:

(i) $R$ ist ZPE-Ring;
(ii) jedes $x \in R\backslash U(R),\ x \neq 0$, ist Produkt irreduzibler Elemente, und jedes irreduzible Element von $R$ ist Primelement;
(iii) jedes $x \in R\backslash U(R),\ x \neq 0$, ist Produkt von Primelementen.

Beweis:
(i) ⇒ (ii):
Es bleibt zu zeigen, daß jedes irreduzible Element von $R$ ein Primelement ist. Es seien dazu $a,\ b \in R$ und $\pi \in R$ irreduzibel mit $\pi \mid ab$. Da $a,\ b$ sich eindeutig als Produkte irreduzibler Elemente schreiben lassen, ergibt sich die Zerlegung von $ab$ in irreduzible Elemente aus der von $a$ bzw. $b$. Nach Voraussetzung muß also ein zu $\pi$ assoziiertes Element in der Faktorisierung von $a$ oder $b$ auftreten, es folgt $\pi | a$ oder $\pi | b$.
(ii) ⇒ (iii): Trivial.
(iii) ⇒ (ii):

Ist $\pi$ irreduzibel, so besitzt $\pi$ eine Darstellung als Produkt von Primelementen. Diese besteht dann notwendig aus nur einem Faktor.

(ii) $\Rightarrow$ (i):
Es seien

$$x = \varepsilon\, q_1 \cdot \ldots \cdot q_r = \tilde{\varepsilon}\, \tilde{q}_1 \cdot \ldots \cdot \tilde{q}_s$$

mit $\tilde{\varepsilon}$, $\varepsilon \in U(R)$ und $q_i$, $\tilde{q}_j$ irreduzibel $(1 \leq i \leq r,\ 1 \leq j \leq s)$. Da $q_r$ Primelement ist, muß $q_r$ eins der $\tilde{q}_j$ teilen, also zu ihm assoziiert sein. Wir ordnen nun gegebenenfalls um, so daß $q_r | \tilde{q}_s$ gilt. Daraus folgt

$$\varepsilon\, q_1 \cdot \ldots \cdot q_{r-1} = \hat{\varepsilon}\, \tilde{q}_1 \cdot \ldots \cdot \tilde{q}_{s-1}$$

mit $\hat{\varepsilon} \in U(R)$. Nach $r$-maliger Anwendung folgt so $r = s$ und bei passender Numerierung $q_i \sim \tilde{q}_i$ $(1 \leq i \leq r)$.

□

Bemerkung:

(i) Als direkte Konseqenz von (2.43) folgt, daß jeder Hauptidealring auch ZPE-Ring ist.

(ii) Wählt man aus jeder Klasse assoziierter Primelemente einen Vertreter aus und bezeichnet die Menge dieser Vertreter mit $P$ so läßt sich in ZPE-Ringen jedes $x \in R,\ x \neq 0$, eindeutig als

$$x = \varepsilon \prod_{p \in P} p^{\nu_p(x)}, \quad y = \eta \prod_{p \in P} p^{\nu_p(y)}$$

$(\nu_p(x) \in \mathbb{Z}^{\geq 0},\ \varepsilon,\ \eta \in U(R)$, nur endlich viele $\nu_p(x)$ ungleich Null, $\nu_p(x)$ ist der genaue Exponent, mit dem $p$ gerade $x$ teilt) schreiben. Für $x,\ y \in R \backslash \{0\}$ folgt dann insbesondere:

$$\begin{aligned} x\, y &= \varepsilon\, \eta \prod_{p \in P} p^{\nu_p(x) + \nu_p(y)}, \\ \mathrm{ggT}\,(x,\ y) &= \prod_{p \in P} p^{\min\{\nu_p(x),\, \nu_p(y)}, \\ \mathrm{kgV}\,(x,\ y) &= \prod_{p \in P} p^{\max\{\nu_p(x),\, \nu_p(y)}, \\ x \,|\, y &\Leftrightarrow \nu_p(x) \leq \nu_p(y)\ \ \forall p \in P. \end{aligned}$$

Ohne Euklidischen Algorithmus ist es i.a. ein schwieriges Problem, wie man in Hauptidealringen ein erzeugendes Element eines Ideals, etwa von $(a_1, \ldots, a_n)$, findet, d.h. einen ggT berechnet. Eine Faktorisierung in Primelemente ist meist zu aufwendig, etwa schon bei großen Zahlen in $\mathbb{Z}$.

### 3.46. Definition

Ein Integritätsring $R$ heißt euklidischer Ring, wenn es eine Abbildung $v : R\backslash\{0\} \to \mathbb{Z}^{\geq 0}$ gibt, derart daß für beliebige $a,\, b \in R,\; b \neq 0$, zwei Elemente $Q(a,\, b),\, R(a,\, b) \in R$ mit

$$a = Q(a,\, b)\, b + R(a,\, b) \quad \text{und} \quad R(a,\, b) = 0 \quad \text{oder} \quad v(R(a,\, b)) < v(b)$$

gibt.

Bemerkung:

(i) Euklidische Ringe sind Ringe mit Einselement.
Die Menge $\{v(x) \mid x \in R\backslash\{0\}\}$ enthält ein minimales Element $v(x_0)$. Hierfür ist notwendig $R(a,\, x_0) = 0 \;\forall a \in R$, also teilt $x_0$ alle $a \in R$. Ferner ist $0 \neq Q(x_0,\, x_0)$ Linkseins:

$$Q(x_0,\, x_0)\, y = Q(x_0,\, x_0)\, Q(y,\, x_0)\, x_0 = Q(y,\, x_0)\, Q(x_0,\, x_0)\, x_0 = Q(y,\, x_0)\, x_0 = y, \quad \forall y \in R.$$

Da $R$ kommutativ ist, ist $Q(x_0,\, x_0)$ Einselement von $R$.

(ii) $\mathbb{Z}$ mit $v = |\;\;|$ (Betragsfunktion) und $K[t]$ mit $v = \deg(\;\;)$ sind euklidische Ringe, es existiert der euklidische Algorithmus, der zur Berechnung eines ggT zweier Ringelemente dient. Jeder Körper ist ein euklidischer Ring.

Beispiel: (Übung)
$R = \mathbb{Z}[-1]$ (Gaußsche ganze Zahlen) mit $v : a + b\sqrt{-1} \mapsto a^2 + b^2$.

### 3.47. Satz

Jeder euklidische Ring $R$ ist Hauptidealring.

Beweis:
Es sei $\mathfrak{a} \neq \{0\}$ ein Ideal von $R$. Ferner sei $a \in \mathfrak{a}$ mit $v(a) = \min\{v(x) \mid x \in \mathfrak{a},\; x \neq 0\}$. Für $x \in a$ gilt dann $x = Q(x,\, a)\, a$, da notwendig $R(x,\, a)$ verschwinden muß. Also gilt $Ra \subseteq \mathfrak{a} \subseteq Ra$.

□

In this chapter we continue to study the structure of rings. We especially consider special types of rings, group rings, polynomial rings, Artinian and Noetherian rings. All these types of rings are important because of their widespread applicability, especially in the context of calculations with algebraic objects. Polynomials are used to generate algebraic extensions of fields, for defining curves and surfaces. They belong to the most important tools in algebra. Noetherian rings will frequently be used in calculations since their ideals have a finite number of generators, hence arithmetic can be done explicitly with those.

## 3.48. Group Rings and Polynomial Rings

The study of group rings is a relatively new topic of classical algebra. It was initiated by the idea that rings possess more structural properties than groups, hence, if one associates a suitable ring to a group then the structure of that so-called group ring should reveal structural aspects of the underlying group. We cannot cover this topic in full generality. Hence, we recommend that the reader concentrates on the applications to polynomial rings later in this section.

## 3.49. Definition

Let $S$ be a semigroup and $R$ be a ring. Then we define a **semigroup ring** $R[S]$ via

$$R[S] := \{f \,:\, S \to R \mid \; f(s) = 0 \text{ for almost all } s \in S\}$$

with operations

$$\begin{aligned} \text{addition} \;\; &: \;\; f+g \,:\, S \to R \,:\, s \mapsto f(s)+g(s) \;\;, \\ \text{multiplication} \;\; &: \;\; f\,g \,:\, S \to R \,:\, s \mapsto \sum_{\substack{t_1 t_2 = s \\ t_1, t_2 \in S}} f(t_1)\, g(t_2) \end{aligned}$$

for all $f$, $g \in R[S]$.

Whereas the definition of addition is straighforward the notion of multiplication seems to be kind of artificial at first glance. However, if we look at polynomials in one variable $t$ with coefficients in $R$ (for simplicity's sake let us assume that $R = \mathbb{R}$ as in highschool) then $S$ is just the semigroup $(\mathbb{Z}^{\geq 0}, +)$ and a map $f$ designs the coefficient $f(m)$ to the power $t^m$, i.e. the map $f$ stands for the polynomial $\sum_{i \geq 0} f(i) t^i$, where the formally infinite sum is actually finite because of the condition imposed on $f$. On the other hand, when we multiply two polynomials given in their usual representation, say $\sum_{i=0}^{n} a_i t^i$ and $\sum_{j=0}^{m} b_j t^j$, it is quite cumbersome to write down their product:

$$\sum_{k=0}^{n+m} (\sum_{l=0}^{k} a_l b_{k-l}) t^k \;\;,$$

where we must additionally require $a_l = 0 \;\; (l > n)$, $b_{k-l} = 0 \;\; (k - l > m)$. This shows why the notion of semigroup rings is advantageous. The advantages will become even more clear when we consider polynomials in several variables. Using the notion of semigroup rings we just choose $S = ((\mathbb{Z}^{\geq 0})^n, +)$ to obtain a polynomial ring over $R$ in $n$ variables. The usual problems, like showing that the order of variables does not matter, are no longer present, this becomes an easy consequence of the analogous property for the direct product of (semi) groups (shown in chapter 2.6).
We leave the verification of the ring axioms for $R[S]$ as an exercise to the reader. As a precedent we establish the law of associativity for

multiplication:
For arbitrary $s \in S$ we have

$$\begin{aligned}
(f\,(g\,h))\,(s) &= \sum_{t_1 t_4 = s} f(t_1)\,(g\,h)\,(t_4) \\
&= \sum_{t_1 t_4 = s} f(t_1) \sum_{t_2 t_3 = t_4} g(t_2)\,h(t_3) \\
&= \sum_{t_1 t_2 t_3 = s} f(t_1)\,g(t_2)\,h(t_3) \\
&= \sum_{t_5 t_3 = s} \left( \sum_{t_1 t_2 = t_5} f(t_1) g(t_2) \right) h(t_3) \\
&= \sum_{t_5 t_3 = s} (f g)\,(t_5)\,h(t_3) \\
&= ((f\,g)\,h)\,(s).
\end{aligned}$$

Next we consider the necessary premises for embedding $R$, $S$ into $R[S]$.

(i) Let $S$ be a monoid with unit element $e$. We put

$$\iota_R \,:\, R \to R[S] \,:\, r \mapsto f_r \quad \text{with} \quad f_r(s) = \left\{ \begin{array}{ll} r & \text{for } s = e \\ 0 & \text{otherwise} \end{array} \right\} \;.$$

Then $\iota_R$ is a ringmonomorphism because of

$$\begin{aligned}
f_{r+\tilde{r}}(s) &= \left\{ \begin{array}{ll} r + \tilde{r} & \text{for } s = e \\ 0 & \text{otherwise} \end{array} \right\} \\
&= \left\{ \begin{array}{ll} r & \text{for } s = e \\ 0 & \text{otherwise} \end{array} \right\} + \left\{ \begin{array}{ll} \tilde{r} & \text{for } s = e \\ 0 & \text{otherwise} \end{array} \right\} \\
&= f_r(s) + f_{\tilde{r}}(s) \;, \\
f_{r\tilde{r}}(s) &= \left\{ \begin{array}{ll} r\tilde{r} & \text{for } s = e \\ 0 & \text{otherwise} \end{array} \right\} \\
&= \sum_{t_1 t_2 = s} \left\{ \begin{array}{ll} r & \text{for } t_1 = e \\ 0 & \text{otherwise} \end{array} \right\} \left\{ \begin{array}{ll} \tilde{r} & \text{for } t_2 = e \\ 0 & \text{otherwise} \end{array} \right\} \\
&= (f_r\, f_{\tilde{r}})(s) \;,
\end{aligned}$$

and $\ker(\iota_R) = \{0\}$.

(ii) Let $R$ be a unital ring. We put

$$\iota_S \,:\, S \to R[S] \,:\, s \mapsto F_s \quad \text{with} \quad F_s(t) = \left\{ \begin{array}{ll} 1 & \text{for } t = s \\ 0 & \text{otherwise} \end{array} \right\} =: \delta_{ts} \;,$$

where $\delta_{ts}$ denotes the **Kronecker symbol** whose value is 1 if both indices coincide and otherwise 0.

$\iota_S$ is a homomorphism because of

$$\begin{aligned} F_{s\tilde{s}}(t) &= \delta_{t,s\tilde{s}} \\ &= \left\{ \begin{array}{ll} 1 & \text{for } s\tilde{s} = t \\ 0 & \text{otherwise} \end{array} \right\} \\ &= \sum_{t_1 t_2 = t} \delta_{t_1 s}\, \delta_{t_2 \tilde{s}} \\ &= \sum_{t_1 t_2 = t} \left\{ \begin{array}{ll} 1 & \text{for } t_1 = s \\ 0 & \text{otherwise} \end{array} \right\} \left\{ \begin{array}{ll} 1 & \text{for } t_2 = s \\ 0 & \text{otherwise} \end{array} \right\} \\ &= (F_s\, F_{\tilde{s}})(t) \ . \end{aligned}$$

Obviously, $\iota_S$ is injective and therefore a monomorphism.

If additionally $S$ is a monoid then $R[S]$ has a unit element with respect to multiplication, namely $F_e$:

$$\begin{aligned} (F_e\, f)(t) &= \sum_{t_1 t_2 = t} F_e(t_1)\, f(t_2) \\ &= \sum_{t_1 t_2 = t} \delta_{e t_1}\, f(t_2) \\ &= f(t) \quad \text{for all} \quad f \in R[S] \ . \end{aligned}$$

(iii) In case $R \ni 1$ we obtain

$$R[S] \ = \ \left\{ \sum_{s \in S} a_s\, F_s \ \middle| \ a_s \in R,\ a_s = 0 \text{ for almost all } s \in S \right\} \ .$$

If we identify $s \in S$ with its image $F_s = \iota_S(s)$ this becomes

$$R[S] \ = \ \left\{ \sum_{s \in S} a_s\, s \ \middle| \ a_s \in R,\ a_s = 0 \text{ for almost all } s \in S \right\} \ .$$

Then all calculations in $R[S]$ are easy:

$$\begin{aligned} \alpha \left( \sum_{s \in S} a_s\, s \right) &= \sum_{s \in S} (\alpha\, a_s)\, s \quad \forall \alpha \in R, \\ \sum_{s \in S} a_s\, s + \sum_{s \in S} b_s\, s &= \sum_{s \in S} (a_s + b_s)\, s, \\ \left( \sum_{s \in S} a_s\, s \right) \left( \sum_{t \in S} b_t\, t \right) &= \sum_{s,t \in S} a_s\, b_t\, s\, t \ = \ \sum_{u \in S} \left( \sum_{st = u} a_s\, b_t \right) u. \end{aligned}$$

**Examples**

(i) $S = \{ t^\nu \mid \nu \in \mathbb{Z}^{\geq 0} \} \cong \mathbb{Z}^{\geq 0}$, $R$ a unital commutative ring.

$$R[S] \ = \ \left\{ \sum_{\nu = 0}^{\infty} a_\nu\, t^\nu \ \middle| \ a_\nu \in R,\ a_\nu \neq 0 \text{ for only finitely many } \nu \right\} =: R[t]$$

is the polynomial ring in the variable $t$ over $R$. The elements of $R[t]$ are written as

$$f(t) = \sum_{i=0}^{\infty} a_\nu \, t^\nu$$

with $a_\nu \in R$, almost all $a_\nu = 0$. Polynomials in one varable are usually called **univariate** polynomials.

(ii)

$$S = \prod_{i=1}^{n} \{t_i^{\nu_i} \in \mathbb{Z}^{\geq 0}\} \cong (\mathbb{Z}^{\geq 0})^n \,, \; R \text{ a unital commutative ring } .$$

The elements of $S$ can be written in the form $\mathbf{t}^{\underline{\nu}} := t_1^{\nu_1} \cdot \ldots \cdot t_n^{\nu_n}$ with $\underline{\nu} \in (\mathbb{Z}^{\geq 0})^n$. Then

$$R[S] \;=\; \left\{ \sum_{\underline{\nu} \in (\mathbb{Z}^{\geq 0})^n} a_{\underline{\nu}} \mathbf{t}^{\underline{\nu}} \;\middle|\; a_{\underline{\nu}} \in R, a_{\underline{\nu}} \neq 0 \text{ for only finitely many } \underline{\nu} \right\} =: R[\mathbf{t}]$$

is the polynomial ring in $n$ variables $t_1, \ldots, t_n$ over $R$ with elements

$$f(\mathbf{t}) = \sum_{\underline{\nu} \in (\mathbb{Z}^{\geq 0})^n} a_{\underline{\nu}} \mathbf{t}^{\underline{\nu}} \quad (a_{\underline{\nu}} \in R, \text{ almost all } a_{\underline{\nu}} = 0) \;\; .$$

Polynomials in several variables ($n \geq 2$) are usually called **multivariate** polynomials.

(iii) $S$ a group, $R$ a unital ring. $R[S]$ is called **group ring**. Knowledge about the group ring yields information about the group itself. We cite without proof a result of Higman: If $G$, $H$ are finite abelian groups with $\mathbb{Z}[G] \cong \mathbb{Z}[H]$ then $G$ and $H$ are isomorphic.

As we already mentioned important results on polynomial rings immediately follow from the properties of the semigroup used for their construction.
For example, we get

$$\begin{aligned} R[t_1, ..., t_n, t_{n+1}] &\cong R[t_1, ..., t_n]\,[t_{n+1}], \\ R[t_1, ..., t_n] &\cong R[t_{\pi(1)}, ..., t_{\pi(n)}] \quad \forall \pi \in \mathfrak{S}_n \end{aligned}$$

as an immediate consequence of the corresponding statements for direct products of (semi) groups.

For the elements of the monoid $(\mathbb{Z}^{\geq 0})^n$ we can introduce an ordering via

$$\mathbf{t}^{\underline{\nu}} \geq \mathbf{t}^{\underline{\mu}} \quad \Leftrightarrow \quad \underline{\nu} \geq \underline{\mu} \;\; .$$

There are various possibilities. We just mention the two most popular ones:

(i) lexicographic ordering
We put $\underline{\nu} \geq \underline{\mu}$ if and only if there exists an index $i \in \{1, ..., n\}$ with $\nu_j = \mu_j \ \ (j < i)$ and $\nu_i > \mu_i$. This means that for the smallest index $i$ for which the coordinates of $\underline{\nu}$ and $\underline{\mu}$ differ the $i$-th coordinate of $\underline{\nu}$ is larger than that of $\underline{\mu}$.
(ii) graded lexicographic ordering
We put $\underline{\nu} \geq \underline{\mu}$ if either $\sum_{i=1}^{n} \nu_i^2 > \sum_{i=1}^{n} \mu_i^2$ or, in case both sums are equal, $\underline{\nu}$ is lexicographically greater than $\underline{\mu}$ (including the case $\underline{\nu} = \underline{\mu}$). Here we first compare the Euclidean lengths of $\underline{\nu}$ and $\underline{\mu}$ and only if they are equal we make use of lexicographic ordering.
For a thorough study of (multivariate) polynomials we need to introduce a few definitions which will be mostly familiar from high school arithmetic.

### 3.50. Definition

Let

$$f(\mathbf{t}) = \sum_{\underline{\nu} \in (\mathbb{Z}^{\geq 0})^n} a_{\underline{\nu}} \mathbf{t}^{\underline{\nu}}$$

be an element of the polynomial ring $R[\mathbf{t}]$. The single summands $a_{\underline{\nu}} \mathbf{t}^{\underline{\nu}}$ are called **monomials**. The **degree** of a non-zero monomial is defined as the sum of its exponents: $\nu_1 + \ldots + \nu_n$. The **degree** $\deg(f)$ of a non-zero polynomial $f$ is the maximum of the degrees of its monomials. The degree of $0$ (as monomial or as polynomial) is formally defined to be $-\infty$. If we have a total ordering on the exponents - and therefore on the monomials - the coefficient of the largest monomial is called **leading coefficient** $l(f)$, sometimes also **headterm**. In case $l(f) = 1$ the polynomial $f$ is called **monic**.

We shortly consider the behavior of the degree function with respect to the addition and multiplication of polynomials. Comparing the degrees of the occuring monomials we immediately see that

$$\begin{aligned} \deg(f+g) &\leq \max\{\deg(f), \deg(g)\} \\ \deg(f\,g) &\leq \deg(f) + \deg(g) \ . \end{aligned}$$

The last inequality becomes an equation, if $l(f)$, $l(g)$ are no zero divisors.
Hence, the degree of the product of two polynomials equals the sum of their degrees over entire rings $R$. The property to be entire is therefore transfered from $R$ to $R[\mathbf{t}]$:

$$R[\mathbf{t}] \text{ entire ring } \Leftrightarrow \ R \text{ entire ring } \ .$$

Because of the behavior of the degree function mentioned above we also obtain the result that the units of $R$ and of $R[t]$ coincide:

$$f \in U(R[\mathbf{t}]) \ \Leftrightarrow \ f \in U(R) \ .$$

We will consider further properties of rings with respect to whether they transfer from $R$ to $R[\mathbf{t}]$.

**Theorem** (**Hilbert's Basis Theorem**) Let $R$ be a unital commutative ring. If $R$ is noetherian then also $R[t]$ is noetherian.

**Proof** Let $\mathbf{A}$ be an ideal of $R[t]$. Then we consider the polynomials of $\mathbf{A}$ of degree $i \in \mathbb{Z}^{\geq 0}$ and put

$$\mathbf{a}_i := \{x \in R \mid x = \mathrm{lc}(f) \text{ for an } f \in \mathbf{A} \text{ with } \deg(f) = i\} \cup \{0\} \ .$$

The $\mathbf{a}_i$ are ideals in $R$ because of

(i) for $f, g \in \mathbf{A}$ with $\deg(f) = \deg(g) = i$ we either have $\mathrm{lc}(f + g) = \mathrm{lc}(f) + \mathrm{lc}(g) \neq 0$ or $\deg(f + g) < i$ and the coefficient of $t^i$ of $f + g$ is zero,

(ii) for $a = \mathrm{lc}(f) \in \mathbf{a}_i,\ r \in R$ we have $ra = 0$ or $rf \in \mathbf{A}$ with $\deg(rf) = i$ and $\mathrm{lc}(rf) = ra \in \mathbf{a}_i$ .

Since we can multiply elements of $\mathbf{A}$ by $t$ we obtain

$$\mathbf{a}_0 \subseteq \mathbf{a}_1 \subseteq \ldots \subseteq \mathbf{a}_r \subseteq \ldots \ .$$

Since $R$ is noetherian this chain becomes stationary. Let $r \in \mathbb{Z}^{\geq 0}$ be minimal with $\mathbf{a}_r = \mathbf{a}_{r+k}\ \forall k \in \mathbb{N}$. Since $R$ is noetherian each ideal $\mathbf{a}_i$ has finitely many generators $a_{i1}, \ldots, a_{in_i}$ $(n_i \in \mathbb{N})$ for $0 \leq i \leq r$. We fix elements $f_{ij} \in \mathbf{A}$ with $\deg(f_{ij}) = i$ and $\mathrm{lc}(f_{ij}) = a_{ij}$ for $0 \leq i \leq r,\ 1 \leq j \leq n_i$. We will show that $\mathbf{A} = \mathbf{B}$ for

$$\mathbf{B} \ := \ \langle f_{ij} \mid 0 \leq i \leq r\,,\ 1 \leq j \leq n_i \rangle \ .$$

Clearly, $\mathbf{B}$ is contained in $\mathbf{A}$. On the other hand, let $f \in \mathbf{A}$ with $\deg(f) = d$. The proof of $f \in \mathbf{B}$ is carried out by induction on $d$. For $d = 0$ there is nothing to show since $f$ is contained in $\mathbf{a}_0 \subseteq \mathbf{B}$. We let therefore be $d > 0$ and assume that all elements of $\mathbf{A}$ of degree less than $d$ belong to $\mathbf{B}$. We need to consider two cases.

(i) For $d > r$ we have

$$\mathbf{a}_d = \langle \mathrm{lc}(t^{d-r} f_{r1}), \ldots, \mathrm{lc}(t^{d-r} f_{rn_r}) \rangle \ ,$$

there exist $\gamma_1, \ldots, \gamma_{n_r} \in R$ such that

$$g \ := \ f - \sum_{i=1}^{n_r} \gamma_i t^{d-r} f_{ri}$$

is a polynomial of $\mathbf{A}$ with $\deg(g) < d$.

(ii) For $d \leq r$ we analogously obtain a polynomial

$$g \ := \ f - \sum_{i=1}^{n_d} \tilde{\gamma}_i f_{di}$$

of degree less than $d$ in $\mathbf{A}$.

According to our induction assumption in both cases the difference polynomial $g$ belongs to the ideal $\mathbf{B}$, hence the polynomial $f$ itself. This finishes the proof of $\mathbf{A} = \mathbf{B}$, the ideal $\mathbf{A}$ is finitely generated and therefore $R[t]$ noetherian.

□

Applying the preceding theorem $n$ times we obtain that for noetherian rings $R$ the polynomial ring in $n$ variables $R[\mathbf{t}]$ is noetherian, too.

A similar discussion whether the properties of a ring $R$ to be a principal ideal ring or a factorial ring transfer to $R[t]$ (and therefore to $R[\mathbf{t}]$) is postponed to the next section.

## 3.51. Univariate Polynomials

Univariate polynomials play a predominant role among all polynomials. This is mainly due to the fact that polynomial rings in one variable over a field have nicer properties than those with several variables. Also, polynomial rings in $n > 1$ variables could be considered as polynomial rings in one variable over a polynomial ring in $n - 1$ variables as base ring. This is usually not the appropriate approach, however, and therefore we shall consider univariate and multivariate polynomials in separate sections.
We begin with basic properties which will be of importance later on.

## 3.52. Definition

Let $\Lambda$ be a unital overring of $R$, i.e. $1_\Lambda = 1_R$, then for every $x \in \Lambda$ the mapping

$$\Phi_x \,:\, R[t] \to \Lambda \,:\, f(t) \mapsto f(x)$$

is a ring homomorphism with $\Phi_x|_R = \mathrm{Id}_R$. Hence, it leaves every element of $R$ invariant and is therefore called an **$R$-homomorphism**. Since $\Phi_x$ maps a polynomial to a ring element it is also called a **specialization** of the polynomial $f(t)$ to its value $f(x)$.

That $\Phi_x$ is indeed a ring homomorphism can be easily verified and is left as an exercise to the reader.

## 3.53. Definition

Let $\Lambda$, $R$ be as in the previous definition. An element $x \in \Lambda$ is called **zero** of $f(t) \in R[t]$, if $f$ is in the kernel of $\Phi_x$. This is clearly tantamount to the more familiar version that $f(t)$ specializes to 0 at $x$.

Proposition 1. *Let $R$ be a unital entire ring. An $R$-homomorphism $\varphi \,:\, R[t] \to R[t]$ is an isomorphism exactly for $\varphi(t) = at + b$ with $a \in U(R)$, $b \in R$.*

Before we actually proof this we emphasize that every $R$-homomorphism $\varphi \,:\, R[t] \to \Lambda$ is uniquely determined by the image $\varphi(t)$. This is because of

$$\varphi\left(\sum_{i=0}^{n} a_i\, t^i\right) \;=\; \sum_{i=0}^{n} \varphi(a_i\, t^i) \;=\; \sum_{i=0}^{n} \varphi(a_i)\, \varphi(t)^i \;=\; \sum_{i=0}^{n} a_i\, \varphi(t)^i \quad .$$

**Proof** For $\varphi(t) = at + b$ with $a \in U(R),\ b \in R$ the inverse mapping is given by $\varphi^{-1}(t) = a^{-1}(t - b)$ satisfying $\varphi \circ \varphi^{-1} = \mathrm{Id}_{R[t]}$. On the other hand, if $\varphi$ is an $R[t]$-isomorphism then $\varphi$ maps $t$ onto some polynomial of $R[t]$, say $\varphi(t) = g(t) := \sum_{i=0}^{n} a_i t^i \in R[t]$ and $\varphi$ being surjective there exists $f(t) = \sum_{j=0}^{m} b_j t^j \in R[t]$ with $t = \varphi(f(t))$. This yields

$$t = \varphi(f(t)) = \varphi(\sum_{j=0}^{m} b_j t^j) = \sum_{j=0}^{m} b_j \varphi(t)^j = \sum_{j=0}^{m} b_j g(t)^j = f(g(t))$$

and comparing degrees we obtain

$$1 = \deg(t) = \deg(f(g(t)) = \deg(g)\deg(f)\ .$$

The latter is possible only for $\deg(f) = \deg(g) = 1$, hence $g(t) = at + b,\ f(t) = ct + d\ \ (a,\, b,\, c,\, d \in R)$. From

$$\begin{aligned} t &= f(g(t)) \\ &= c\,(at + b) + d \\ &= cat + bc + d \end{aligned}$$

we deduce $1 = ac$, $0 = bc + d$ and therefore $a \in U(R)$.
□

# Bibliography


[1] Bewersdorff, Jörg, *Algebra für Einsteiger*,Vieweg, 2002.
[2] Birkhoff, Bartee, *Modern Applied Algebra*.
[3] S. Bosch, *Algebra*, Springer, 1993.
[4] N. Bourbaki, *Algebre*, Hermann, Paris 1962.
[5] J. H. Davenport, Y. Siret, E. Tournier, *Computer algebra*, Acad. Press, 1989.
[6] G. Fischer, *Lehrbuch der Algebra*, Vieweg 2008.
[7] I. N. Herstein, *Topics in Algebra*, Xerox Coll. Pub., 1964.
[8] Th. W. Hungerford, *Algebra*, 1974.
[9] N. Jacobson, *Lectures in Abstract Algebra*, Springer GTM, 1974.
[10] R. Kochendörffer, *Einführung in die Algebra*, Dt.Verl.d. Wissenschaften, 1974.
[11] S. Lang, *Algebra*, Addison-Wesley, 1971.
[12] A. Leutbecher, *Zahlentheorie*, Springer, 1996.
[13] F. Lorenz, *Algebra I, II*, BI Wissenschaftsverlag, 1987/90.
[14] K. Meyberg, *Algebra I, II*, Carl Hanser Verlag, 1975.
[15] Mignotte, *Mathematics for Computer Algebra*, Springer, 1992.
[16] E. Scholz, *Geschichte der Algebra*, BI Wissenschaftsverlag, 1990.
[17] G. Stroth, *Algebra*, de Gruyter, 1998.
[18] B. L. van der Waerden, *Algebra I, II*, Springer, 1966/87.
[19] Weber, *Lehrbuch der Algebra*, Vieweg, 1895.