**Definition (9.1)**

Ein Ring ist ein Tripel $(R, +, \cdot)$ bestehend aus einer Menge $R$ und zwei Verknüpfungen $+ : R \times R \to R$ und $\cdot : R \times R \to R$, genannt Addition und Multiplikation, so dass die folgenden Bedingungen erfüllt sind:

(i) Das Paar $(R, +)$ ist eine abelsche Gruppe.

(ii) Das Paar $(R, \cdot)$ ist ein kommutatives Monoid.

(iii) Es gilt das Distributivgesetz $a(b + c) = ab + ac$ für alle $a, b, c \in R$.

# Definition der Ringhomomorphismen

## Definition (9.2)

Seien $(R, +_R, \cdot_R)$ und $(S, +_S, \cdot_S)$ Ringe. Eine Abbildung $\phi : R \to S$ heißt Ringhomomorphismus von $(R, +_R, \cdot_R)$ nach $(S, +_S, \cdot_S)$, wenn die Gleichung $\phi(1_R) = 1_S$ gilt und außerdem

$$\phi(a +_R b) = \phi(a) +_S \phi(b) \quad \text{und} \quad \phi(a \cdot_R b) = \phi(a) \cdot_S \phi(b)$$

für alle $a, b \in R$ erfüllt ist.

# Einheiten und Nullteiler

**Definition (9.4)**

Sei $R$ ein Ring.

(i) Ein Element $a \in R$ heißt Einheit, wenn ein $b \in R$ mit $ab = 1_R$ existiert. Die Menge der Einheiten von $R$ bezeichnen wir mit $R^\times$.

(ii) Man nennt es Nullteiler, wenn ein Element $b \in R$, $b \neq 0_R$ mit $ab = 0_R$ existiert.

Die Einheiten eines Rings $R$ bilden eine Gruppe $R^\times$, die sogenannte Einheitengruppe.

# Integritätsbereiche und Körper

**Definition (9.5)**

Ein Ring $R$ mit $0_R$ als einzigem Nullteiler heißt Integritätsbereich.
Gilt $R^\times = R \setminus \{0_R\}$, dann ist $R$ ein Körper.

# Die Charakteristik eines Rings

**Definition (9.8)**

Sei $R$ ein Ring. Die Charakteristik eines Rings $R$ ist definiert durch

$$\operatorname{char}(R) \quad = \quad \begin{cases} n & \text{falls } n \in \mathbb{N} \text{ minimal mit } n \cdot 1_R = 0_R \text{ ist,} \\ 0 & \text{falls } n \cdot 1_R \neq 0_R \text{ für alle } n \in \mathbb{N} \text{ gilt.} \end{cases}$$

**Proposition (9.9)**

Sei $R$ ein Integritätsbereich. Dann ist die Charakteristik $\operatorname{char}(R)$ entweder gleich Null oder eine Primzahl.

# Definition der Teilringe

**Definition (9.10)**

Sei $R$ ein Ring. Eine Teilmenge $S \subseteq R$ wird Teilring von $R$ genannt, wenn $1_R \in S$ gilt und mit $a, b \in S$ jeweils auch die Elemente $a - b$ und $ab$ in $S$ liegen.

Man bezeichnet einen Ring $R$ als Erweiterungsring eines anderen Rings $S$, wenn $S$ ein Teilring von $R$ ist. Das Paar $(S, R)$ bezeichnet man in diesem Fall als Ringerweiterung. Durch die Schreibweise $R|S$ wird ausgedrückt, dass $(S, R)$ eine Ringerweiterung ist.

# Teilringe sind Ringe

**Satz (9.11)**

Sei $(R, +, \cdot)$ ein Ring und $S \subseteq R$ ein Teilring. Dann ist die Menge $S$ unter den Verknüpfungen $+$ und $\cdot$ abgeschlossen. Bezeichnen wir mit $+_S$ und $\cdot_S$ die auf $S$ eingeschränkten Verknüpfungen, dann ist $(S, +_S, \cdot_S)$ ein Ring.

Beweis von Satz 9.11

geg. Ring $(R, +, \cdot)$, $S \subseteq R$ Teilring,
d.h. $1_R \in S$ und $\forall a, b \in S: a - b,\ a \cdot b \in S$

Beh.: $S$ ist abgeschlossen unter $+$ und $\cdot$
($\Rightarrow$ erhalte Verknüpfungen $+_S, \cdot_S$ auf $S$)

$1_R \in S \rightarrow 0_R = 1_R - 1_R \in S$

Für jedes $a \in S$ gilt $-a = 0_R - a \in S$.

Für alle $a, b \in S$ gilt somit $-b \in S$, und
daraus folgt $a + b = a - (-b) \in S$.

Die Abgeschlossenheit unter $\cdot$ gilt nach Voraussetzung.

**Beh.:** $(S, +_S, \cdot_S)$ ist ein Ring

zu überprüfen (1) $(S, +_S)$ ist abelsche Gruppe

(2) $(S, \cdot_S)$ ist abelsches Monoid

(3) Es gilt das Distributivgesetz.

Alle Rechenregeln werden von R „geerbt". Beispielsweise erhält man das Assoziativgesetz für alle $a, b, c \in S$ durch

$$(a +_S b) +_S c = (a + b) + c = a + (b + c) = a +_S (b +_S c)$$

↑ Assoziativgesetz in R

Für den Nachweis von (1) und (2) ist noch zu beachten, dass $0_R$ und $1_R$ in $S$ liegen (siehe oben), und dass für alle $a \in S$ auch $-a$ in $S$ liegt. □

# Durchschnitte von Teilringen sind Teilringe

**Lemma (9.12)**

Sei $(R, +, \cdot)$ ein Ring, und sei $(S_i)_{i \in I}$ eine Familie von Teilringen. Dann ist auch $S = \bigcap_{i \in I} S_i$ ein Teilring von $R$.

# Definition der Teilkörper

**Definition (9.13)**

Sei $K$ ein Körper. Eine Teilmenge $F \subseteq K$ wird Teilkörper von $K$ genannt, wenn $1_K \in F$ gilt, für alle $a, b \in F$ auch die Elemente $a - b$ und $ab$ in $F$ liegen und für jedes $a \in F$, $a \neq 0_K$ auch $a^{-1} \in F$ gilt.

- Es ist leicht zu sehen, dass der durch $F$ definierte Ring ein Körper ist.
- Die Begriffe Erweiterungskörper und Körpererweiterung sind in genauer Analogie zu den Ringen definiert.

# Definition des Primkörpers

**Lemma (9.14)**

Sei $K$ ein Körper und $(F_i)_{i \in I}$ eine beliebige Familie von Teilkörpern. Dann ist auch $F = \bigcap_{i \in I} F_i$ ein Teilkörper von $K$.

**Folgerung (9.15)**

Ist $K$ ein Körper und ist $(F_i)_{i \in I}$ die Familie aller Teilkörper von $K$, dann nennt man $P = \bigcap_{i \in I} F_i$ den Primkörper von $K$. Es handelt sich um den bezüglich Inklusion kleinsten Teilkörper von $K$.

- Es ist $\mathbb{Q}$ der gemeinsame Primkörper von $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$.
- Der Körper $\mathbb{F}_p$ ist jeweils sein eigener Primkörper.
- Wir werden später sehen, dass der Primkörper jedes Körpers isomorph zu $\mathbb{Q}$ oder zu $\mathbb{F}_p$ für eine Primzahl $p$ ist.

# Definition des erzeugten Teilrings

**Satz (9.16)**

Sei $\tilde{R}|R$ eine Ringerweiterung und $A \subseteq \tilde{R}$ eine beliebige Teilmenge. Dann gibt es einen eindeutig bestimmten Teilring $R[A]$ von $\tilde{R}$ mit den folgenden beiden Eigenschaften.

(i) Es gilt $R[A] \supseteq R \cup A$.

(ii) Ist $R'$ ein weiterer Teilring von $\tilde{R}$ mit $R' \supseteq R \cup A$, dann folgt $R' \supseteq R[A]$.

Damit ist $R[A]$ also der kleinste Teilring von $\tilde{R}$, der $R \cup A$ enthält. Man nennt ihn den von $A$ über $R$ erzeugten Teilring.

# Definition der komplexen Quadratwurzel

(U. Funktionentheorie)

$$\sqrt{z} = \begin{cases} 0 & \text{falls } z = 0 \\ e^{\frac{1}{2}\ln(z)} & \text{falls } z \neq 0 \end{cases}$$

Achtung: Nicht für alle $z, w \in \mathbb{C}$ gilt

$$\sqrt{zw} = \sqrt{z} \cdot \sqrt{w}$$

Beispiel: Für alle $d \in \mathbb{R}$ mit $d < 0$ gilt $\sqrt{d} = i\sqrt{|d|}$. Daraus folgt

z.B. $\sqrt{-3} \cdot \sqrt{-5} = (i\sqrt{3}) \cdot (i\sqrt{5}) = -\sqrt{15} \neq \sqrt{(-3)(-5)}$

# Beispiel: Quadratische Zahlringe

**Satz (9.17)**

Sei $d \in \mathbb{Z}$ und $\sqrt{d} \in \mathbb{C}$ wie oben definiert.

(i) Es gilt $\mathbb{Z}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$.

(ii) Ist $d \equiv 1 \mod 4$, dann gilt
$\mathbb{Z}[\frac{1}{2}(1 + \sqrt{d})] = \{\frac{1}{2}a + \frac{1}{2}b\sqrt{d} \mid a, b \in \mathbb{Z}, a \equiv b \mod 2\}$.

Die Ringe dieser Form bezeichnen wir als quadratische Zahlringe.

Beweis von Satz 9.17, neu (i)

geg: $d \in \mathbb{Z}$, $S = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$

Beh: $\mathbb{Z}[\sqrt{d}] = S$

Überprüfe, dass $S$ die definierenden Eigenschaften von $\mathbb{Z}[\sqrt{d}]$, d.h. im Einzelnen

(1) $S$ ist Teilring von $\mathbb{C}$ (2) $S \supseteq \mathbb{Z} \cup \{\sqrt{d}\}$

(3) Ist $S'$ ein beliebiger Teilring von $\mathbb{C}$ mit $S' \supseteq \mathbb{Z}[\sqrt{d}]$, dann folgt $S' \supseteq S$.

zu (1) Das Einselement 1 von $\mathbb{C}$ ist in $S$ enthalten, da $1 = 1 + 0 \cdot \sqrt{d}$ und $1, 0 \in \mathbb{Z}$.

Seien $\alpha, \beta \in S$. zu zeigen: $\alpha - \beta, \alpha\beta \in S$

$x \in S \Rightarrow \exists a, b \in \mathbb{Z}$ mit $x = a + b\sqrt{d}$

$\beta \in S \Rightarrow \exists u, v \in \mathbb{Z}$ mit $\beta = u + v\sqrt{d}$

$\Rightarrow x - \beta = (a + b\sqrt{d}) - (u + v\sqrt{d}) =$

$(a-u) + (b-v)\sqrt{d} \in S$ weg. $a-u, b-v \in \mathbb{Z}$

ebenso: $x\beta = (a + b\sqrt{d})(u + v\sqrt{d}) =$

$au + bu\sqrt{d} + av\sqrt{d} + bv\sqrt{d}\sqrt{d} =$

$(au + bvd) + (bu + av)\sqrt{d} \in S$, da

$au + bvd \in \mathbb{Z}$, $bu + av \in \mathbb{Z}$

zu (2) Für jedes $a \in \mathbb{Z}$ gilt $a = a + 0 \cdot \sqrt{d} \in S$.

ebenso $\sqrt{d} = 0 + 1 \cdot \sqrt{d} \in S$.

zu (3) Sei $S'$ ein Teilring von $\mathbb{C}$ mit $S' \supseteq \mathbb{Z} \cup \{\sqrt{d}\}$

z.Zg: $S \subseteq S'$ Sei $\alpha \in S$. $\Rightarrow \exists a, b \in \mathbb{Z}$

mit $\alpha = a + b\sqrt{d}$. $\mathbb{Z} \subseteq S' \Rightarrow a, b \in S'$

$b, \sqrt{d} \in S'$, $S'$ Teilring von $\mathbb{C} \Rightarrow b\sqrt{d} \in S'$

$a \in S'$, $b\sqrt{d} \in S'$, $S'$ Teilring von $\mathbb{C} \Rightarrow \alpha = a + b\sqrt{d} \in S'$.

□

$-3)(-5)$

# Von einem Element erzeugte Teilringe

**Proposition (9.18)**

Sei $\tilde{R} \mid R$ eine Ringerweiterung und $c \in \tilde{R}$. Dann gilt

$$R[c] = \left\{ f(c) \;\middle|\; f \in R[x] \right\}.$$

**Definition (10.1)**

Sei $R$ ein Ring. Ein Ideal in $R$ ist eine Teilmenge $I \subseteq R$ mit den Eigenschaften

(i) $0_R \in I$

(ii) Für alle $a, b \in I$ und $r \in R$ gilt $a + b \in I$ und $ra \in I$.

# wichtiger Spezialfall: Hauptideale

**Proposition (10.2)**

- Ist $R$ ein Ring und $b \in R$, dann ist die Menge der Vielfachen $\{ab \mid a \in R\}$ von $b$ ein Ideal in $R$. Man nennt ein solches Ideal ein Hauptideal und bezeichnet es mit $(b)$.
- Ein Hauptidealring ist ein Integritätsbereich, in dem jedes Ideal ein Hauptideal ist.
- In jedem Ring $R$ ist das Nullideal $(0_R) = \{0_R\}$ das kleinste und das Einheitsideal $(1_R) = R$ das bezüglich Inklusion größte Ideal.

# Definition der Teilerrelation

**Definition (10.3)**

Seien $R$ ein Ring und $a, b \in R$. Wir sagen, dass $a$ ein Teiler von $b$ ist und schreiben $a|b$, wenn ein $c \in R$ mit $b = ac$ existiert. Gilt sowohl $a|b$ als auch $b|a$, dann sagt man, die Elemente $a$ und $b$ sind assoziiert zueinander.

**Lemma (10.4)**

Ist $R$ ein Integritätsbereich, so sind $a, b \in R$ genau dann zueinander assoziiert, wenn ein $\varepsilon \in R^\times$ mit $b = \varepsilon a$ existiert.

Beweis von Lemma 10.4

geg: Integritätsbereich $R$, $a, b \in R$

Beh.: $a, b$ sind assoziiert (d.h. $a \mid b$ und $b \mid a$) $\iff \exists \varepsilon \in R^* : b = \varepsilon a$

„$\Leftarrow$" Aus $b = \varepsilon a$ folgt $a \mid b$.

$b = \varepsilon a \Rightarrow \varepsilon^{-1} b = \varepsilon^{-1} \varepsilon a = 1_R \, a = a$

Daraus folgt $b \mid a$.

„$\Rightarrow$" $a \mid b \Rightarrow \exists c \in R$ mit $b = ca$

$b \mid a \Rightarrow \exists d \in R$ mit $a = db$

einsetzen $\Longrightarrow a = dca \Rightarrow 1_R \cdot a = dc \cdot a$

R Int.-Ber.

$\Longrightarrow$ Kürzungsregel $1_R = dc \Rightarrow c \in R^\times$ Es gilt also

$b = \varepsilon a$ mit $\varepsilon \in R^\times$ gg. durch $\varepsilon = c$ $\square$

# Definition des größten gemeinsamen Teilers

**Definition (10.5)**

Sei $R$ ein Ring mit $a_1, ..., a_n \in R$. Wir sagen, ein Element $d \in R$ ist ein größter gemeinsamer Teiler (kurz $\mathrm{ggT}$) von $a_1, ..., a_n$, wenn gilt

(i) $d|a_i$ für $1 \leq i \leq n$

(ii) Ist $b \in R$ mit $b|a_i$ für $1 \leq i \leq n$, dann folgt $b|d$.

Wir nennen die Elemente $a_1, ..., a_n$ teilerfremd, wenn $1_R$ ein $\mathrm{ggT}$ der Elemente ist.

# Definition des kleinsten gemeinsamen Vielfachens

**Definition (10.6)**

Sei $R$ ein Ring mit $a_1, ..., a_n \in R$. Ein Element $e \in R$ heißt kleinstes gemeinsames Vielfaches (kurz $\mathrm{kgV}$) von $a_1, ..., a_n$, wenn gilt

(i) $a_i | e$ für $1 \leq i \leq n$

(ii) Ist $b \in R$ mit $a_i | b$ für $1 \leq i \leq n$, dann folgt $e | b$.

# Eindeutigkeit von $\mathrm{ggT}$ und $\mathrm{kgV}$

**Lemma (10.7)**

Sei $R$ ein Ring und $d \in R$ ein größter gemeinsamer Teiler der Ringelemente $a_1, ..., a_n$. Ein weiteres Element $d' \in R$ ist genau dann ein $\mathrm{ggT}$ von $a_1, ..., a_n$, wenn $d$ und $d'$ zueinander assoziiert sind. Dieselbe Aussage gilt auch für das kleinste gemeinsame Vielfache.

# Idealtheoretische Charakterisierung von $\mathrm{ggT}$ und $\mathrm{kgV}$

**Satz (10.8)**

Sei $R$ ein Ring, und seien $a, b \in R$.

(i) Es gilt $(a) \subseteq (b)$ genau dann, wenn $b$ ein Teiler von $a$ ist.

(ii) Ist $d \in R$ mit $(d) = (a, b)$, dann ist $d$ ein $\mathrm{ggT}$ von $a$ und $b$.

(iii) Ist $e \in R$ mit $(e) = (a) \cap (b)$, dann ist $e$ ein $\mathrm{kgV}$ von $a$ und $b$.

Ist $R$ ein Hauptidealring, dann gilt auch von (ii) und (iii) die Umkehrung.

Anmerkung zu Satz 10.8:

$(a,b)$ ist eine Kurzschreibweise für die Menge $\{ra+sb \mid r,s \in R\}$.

Es ist leicht zu sehen, dass diese Menge ein Ideal ist.

Beweis von Teil ii):

Seien $a,b \in R$. z.zg.: $a \mid b \Leftrightarrow (a) \supseteq (b)$

„$\Leftarrow$" $b = 1_R \cdot b \in (b) \overset{(b)\subseteq(a)}{\Rightarrow} b \in (a)$

$\Rightarrow \exists r \in R$ mit $b = r\,a \Rightarrow a \mid b$

„$\Rightarrow$" $a \mid b \Rightarrow \exists r \in R$: $b = r\,a$

$\Rightarrow b \in (a)$ Weil $(a)$ ein Ideal ist, liegt damit auch jedes Vielfache von $b$ in $(a)$. $\rightarrow (b) \subseteq (a)$ $\square$