Lineare Algebra I

Woche 07

25.11.2025 und 27.11.2025

§ 9 Ringe

Ring (Modellbeispiel $\mathbb{Z}$)

Definition 9.1

typische Notation

Ein **Ring** $(R, +, \cdot)$ ist eine Menge R mit zwei Verknüpfungen $+$ und $\cdot$, die die folgenden Bedingungen erfüllen:

1. $(R, +)$ ist eine abelsche Gruppe. neutrales Element 0_R
   „Addition"
2. $(R, \cdot)$ ist eine Halbgruppe.
   „Multiplikation"
3. Es gelten die **Distributivgesetze**

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$
$$(a + b) \cdot c = (a \cdot c) + (b \cdot c)$$

} fallen zusammen für komm. Ringe

Ein Ring $(R, +, \cdot)$ heißt **kommutativ**, wenn $(R, \cdot)$ kommutativ ist.

Ein Ring $(R, +, \cdot)$ heißt ein **Ring mit Eins**, wenn $(R, \cdot)$ ein Monoid ist.

neutrales Element 1_R

Ring

Beispiel 9.2

1. $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ und $(\mathbb{C}, +, \cdot)$ sind kommutative Ringe mit Eins.

   $(\mathbb{Z}, +)$ ab. Gruppe, neutral ist 0
   $(\mathbb{Z}, \cdot)$ komm. Monoid, neutral ist 1

2. „Der“ **Nullring** ist der eindeutig bestimmte Ring mit nur einem Element, $R = \{0_R\}$.

   $0_R + 0_R = 0_R$
   $0_R \cdot 0_R = 0_R$
   } komm. Ring, Null. = Einsel. $= 0_R$

Ring

Beispiel 9.2

3. Für $m \in \mathbb{N}$ ist $(m\mathbb{Z}, +, \cdot)$ ein kommutativer Ring.

   $(m\mathbb{Z}, +)$ Ab. Gr., neutral ist 0

   $(m\mathbb{Z}, \cdot)$ komm. Halbgr. ohne Einsel. (falls $m \geq 2$)

   $= \{0, 1, \ldots, m-1\}$

4. Für $m \in \mathbb{N}$ ist $(\mathbb{Z}_m, +_m, \cdot_m)$ ein kommutativer Ring mit dem Einselement 1, der **Ring von $\mathbb{Z}$ modulo m**.

   $\mathbb{Z}_m$

   ~~$(m\mathbb{Z}, +)$~~

   ~~$(m\mathbb{Z}, \cdot)$~~

   $\mathbb{Z}_m$

Beispiel 9.2

5. Ist X eine Menge und $(R, +, \cdot)$ ein Ring, dann ist auch $(R^X, +, \cdot)$ ein Ring.

   Das Nullelement in $(R^X, +, \cdot)$ ist die **Nullfunktion** $x \mapsto 0_R$.

   Besitzt R das Einselement 1_R, dann ist die **Einsfunktion** $x \mapsto 1_R$ das Einselement von $(R^X, +, \cdot)$.

   Ist $(R, +, \cdot)$ kommutativ, dann ist auch $(R^X, +, \cdot)$ kommutativ.

Beispiel 9.2

6. Der **Endomorphismenring** $(\mathrm{End}(G), +, \circ)$ einer abelschen Gruppe $(G, +)$ ist

$$\mathrm{End}(G) := \{f \colon G \to G \mid f \text{ ist Endomorphismus}\}$$

mit den Verknüpfungen

punktweise

$$+ \colon \mathrm{End}(G) \times \mathrm{End}(G) \to \mathrm{End}(G) \quad \text{mit } (f, g) \mapsto f + g$$
$$\circ \colon \mathrm{End}(G) \times \mathrm{End}(G) \to \mathrm{End}(G) \quad \text{mit } (f, g) \mapsto f \circ g$$

Monoid mit id_G

$(\mathrm{End}(G), +, \circ)$ ist ein Ring mit dem Einselement id_G.

$(\mathrm{End}(G), +, \circ)$ ist i. A. nicht kommutativ.

$f \circ (g + h) = f \circ g + f \circ h$ weil f Endo ist

$(f + g) \circ h = f \circ h + g \circ h$ weil + pktweise def ist

Ring

Beispiel 9.2

7. Ist X eine Menge, dann ist $(\mathcal{P}(X), \triangle, \cap)$ ein kommutativer Ring mit dem Einselement X.

   $(\mathcal{P}(X), \triangle)$ ab Gruppe, Nullel. ist $\emptyset$
   $(\mathcal{P}(X), \cap)$ komm. Monoid mit Einsel. X
   Distr. $A \cap (B \triangle C) = (A \cap B) \triangle (A \cap C)$ ✔

8. $(\mathcal{P}(X), \triangle, \cup)$ ist jedoch kein Ring, da das Distributivgesetz nicht gilt.

   $(\mathcal{P}(X), \triangle)$
   $(\mathcal{P}(X), \cup)$

Rechenregeln in Ringen

Lemma 9.3

1. $0_R \cdot a = 0_R = a \cdot 0_R$
2. $a \cdot (-b) = -(a \cdot b) = (-a) \cdot b$

Beweis. ① $0_R + 0_R \cdot a = 0_R \cdot a = (0_R + 0_R) \cdot a$

$= 0_R \cdot a + 0_R \cdot a \Rightarrow 0_R = 0_R \cdot a$ (kürzen)

② $a \cdot (-b)$ ist add. Inv. zu $a \cdot b$:

$a \cdot (-b) + a \cdot b = a \cdot (-b + b) = a \cdot 0_R \overset{①}{=} 0_R$

Rechenregeln in Ringen

Lemma 9.3

3. $(-a)\cdot(-b) = a\cdot b$

4. Ist $(R,+,\cdot)$ ein Ring mit Einselement 1_R, aber nicht der Nullring, dann gilt $1_R \neq 0_R$.

Beweis. ③ $(-a)\cdot(-b) \overset{②}{=} -\big(a\cdot(-b)\big)$

$\overset{②}{=} -\big(-a\cdot b\big) = a\cdot b$

④ Annahme: $1_R = 0_R$. Es sei $a \in R$ beliebig.

$a = a\cdot 1_R \overset{\text{Vor.}}{=} a\cdot 0_R \overset{①}{=} 0_R$, also ist R ein Nullring.

Charakteristik eines Ringes

Definition 9.4

Es sei $(R, +, \cdot)$ ein Ring mit Einselement 1_R.

Wenn $n\,1_R = 0_R$ für ein $n \in \mathbb{N}$ gilt, dann heißt

$$\min\{n \in \mathbb{N} \mid n\,1_R = 0_R\}$$

die **Chakteristik** von R, kurz $\operatorname{char}(R)$.
Andernfalls setzen wir $\operatorname{char}(R) = 0$.

Beispiel 9.5

1. $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ und $(\mathbb{C}, +, \cdot)$ haben die Charakteristik 0.
2. Der Nullring ist der einzige Ring mit Charakteristik 1.
3. $(\mathbb{Z}_m, +_m, \cdot_m)$ hat die Charakteristik m.

Restklassenring modulo m

Beispiel 9.6 (Begründung durch Satz 9.30)

Die Faktormenge $\mathbb{Z}/m\mathbb{Z}$ bildet mit den Verknüpfungen

$$[a] \mathbin{\tilde{+}} [b] = [a+b]$$
$$[a] \mathbin{\tilde{\cdot}} [b] = [a \cdot b]$$

den **Restklassenring modulo** m, kurz: $(\mathbb{Z}/m\mathbb{Z}, \tilde{+}, \tilde{\cdot})$.

$(\mathbb{Z}/m\mathbb{Z}, \tilde{+}, \tilde{\cdot})$ ist ein kommutativer Ring mit Einselement $[1]$.

Im Fall $m = 1$ ist $(\mathbb{Z}/m\mathbb{Z}, \tilde{+}, \tilde{\cdot})$ ein Nullring.

Restklassenring modulo 4

Beispiel 9.6

$\tilde{+}$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$
$[1]$	$[1]$	$[2]$	$[3]$	$[0]$
$[2]$	$[2]$	$[3]$	$[0]$	$[1]$
$[3]$	$[3]$	$[0]$	$[1]$	$[2]$

$\tilde{\cdot}$	$[0]$	$[1]$	$[2]$	$[3]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$
$[2]$	$[0]$	$[2]$	$[0]$	$[2]$
$[3]$	$[0]$	$[3]$	$[2]$	$[1]$

Produkt zweier Faktoren $\neq 0_{\mathbb{Z}}$ ist $0_{\mathbb{Z}}$.

Nullteiler, Integritätsring

Definition 9.7

Es sei $(R, +, \cdot)$ ein Ring.

1. $a \in R$ heißt **Linksnullteiler**, wenn es $b \neq 0_R$ gibt mit $a \cdot b = 0_R$.

   0_R ist Linksnullteiler (außer im Nullring)

2. $b \in R$ heißt **Rechtsnullteiler**, wenn es $a \neq 0_R$ gibt mit $a \cdot b = 0_R$.

   0_R ist Rechtsnullteiler (außer im Nullring)

3. $(R, +, \cdot)$ heißt **nullteilerfrei**, wenn es außer 0_R keine weiteren Links- oder Rechtsnullteiler gibt, wenn also gilt:

   $a \neq 0_R$ und $b \neq 0_R \Rightarrow a \cdot b \neq 0_R$

4. Ist $(R, +, \cdot)$
   - ein kommutativer Ring mit Eins,
   - nullteilerfrei
   - und ungleich dem Nullring,

   dann heißt $(R, +, \cdot)$ ein **Integritätsring** oder **Integritätsbereich**.

   (vgl. auch $(\mathbb{Z}, +, \cdot)$)

Integritätsring

Beispiel 9.9

kommt „nullteilerfrei" mit $1_R \neq 0_R$

1. $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ und $(\mathbb{C}, +, \cdot)$ sind Integritätsringe.

2. Es sei X eine Menge und $(R, +, \cdot)$ ein kommutativer Ring mit Eins.

   Dann ist $R^X = \{f \mid f : X \to R\}$ mit den punktweisen Verknüpfungen $+$ und $\cdot$ ein kommutativer Ring mit Eins.

   Es sei R nicht der Nullring, ($1_R \neq 0_R$) und X habe mindestens zwei Elemente.
   Dann ist $(R^X, +, \cdot)$ nicht nullteilerfrei!

Wähle $f(x) = \begin{cases} 0_R & \text{für } x = x_0 \\ 1_R & \text{sonst} \end{cases}$ $\quad g(x) = \begin{cases} 1_R & \text{für } x = x_0 \\ 0_R & \text{sonst} \end{cases}$

$\Rightarrow f \cdot g = 0_{R^X}$ Nullfkt.

Restklassenring modulo m

Satz 9.11

Es sei $m \in \mathbb{N}$. Dann sind äquivalent:

1. $(\mathbb{Z}\,/\,m\,\mathbb{Z}, \widetilde{+}, \widetilde{\cdot})$ ist ein Integritätsring.
2. m ist eine Primzahl.

Unterring

Definition 9.12

Es sei $(R, +, \cdot)$ ein Ring.

$U + U \subseteq U$
$U \cdot U \subseteq U$

1. Eine bzgl. $+$ und $\cdot$ abgeschlossene Teilmenge $U \subseteq R$ heißt ein **Unterring** von $(R, +, \cdot)$, wenn $(U, +, \cdot)$ selbst wieder ein Ring ist.

   D.h. $(U, +)$ ist UG von $(R, +)$
   $(U, \cdot)$ ist UHG von $(R, \cdot)$
   $\hookleftarrow U \cdot U \subseteq U$

2. Ist $(R, +, \cdot)$ ein Ring mit Einselement 1_R, dann fordern wir für einen **Unterring mit Eins** $(U, +, \cdot)$ zusätzlich, dass $1_R \in U$ liegt.

   Es reicht nicht, dass $(U, \cdot)$ irgendein neutrales Element hat!

3. Ein Unterring $(U, +, \cdot)$ von $(R, +, \cdot)$ heißt **echt**, wenn $U \subsetneq R$ gilt.

Unterringkriterium

Satz 9.13

Es sei $(R, +, \cdot)$ ein Ring und $U \subseteq R$.

Dann sind äquivalent:

1. $(U, +, \cdot)$ ist ein Unterring von $(R, +, \cdot)$.
2. $U \neq \emptyset$, und für alle $a, b \in U$ gilt $a - b \in U$ und $a \cdot b \in U$.

UG-Krit. für $(U, +)$ — UHG-Krit. für $(U, \cdot)$

Für UR mit Eins ist $1_R \in U$ zusätzlich zu prüfen.

Unterring

Beispiel 9.14

1. $(\mathbb{Z}, +, \cdot)$ ist ein Unterring mit Eins von $(\mathbb{Q}, +, \cdot)$.
   $(\mathbb{Q}, +, \cdot)$ ist ein Unterring mit Eins von $(\mathbb{R}, +, \cdot)$.
   $(\mathbb{R}, +, \cdot)$ ist ein Unterring mit Eins von $(\mathbb{C}, +, \cdot)$.

2. Für $m \in \mathbb{N}$ ist $(m\mathbb{Z}, +, \cdot)$ ein Unterring von $(\mathbb{Z}, +, \cdot)$.
   Im Fall $m \neq 1$ handelt es sich nicht um einen Unterring mit Eins.

3. Der Nullring $\{0_R\}$ und R selbst sind Unterringe in jedem Ring $(R, +, \cdot)$.

Unterring

Beispiel 9.14

4. Ist X eine Menge und $Y \subseteq X$, dann ist $(\mathcal{P}(Y), \triangle, \cap)$ ein Unterring von $(\mathcal{P}(X), \triangle, \cap)$.

   Im Fall $Y \subsetneq X$ handelt es sich nicht um einen Unterring mit Eins.

5. Das **Zentrum**

$$Z := \{z \in R \mid a \cdot z = z \cdot a \text{ für alle } a \in R\}$$

   eines Ringes $(R, +, \cdot)$ ist ein kommutativer Unterring.

   Wenn R ein Ring mit Eins ist, dann ist Z ein Unterring mit Eins.

Homomorphismus von Ringen

Definition 9.17

Es seien $(R_1, +_1, \cdot_1)$ und $(R_2, +_2, \cdot_2)$ zwei Ringe.

Eine Abbildung $f\colon R_1 \to R_2$ heißt **strukturverträglich** oder ein **Homomorphismus** von $(R_1, +_1, \cdot_1)$ in $(R_2, +_2, \cdot_2)$, wenn gilt:

$$f(a +_1 b) = f(a) +_2 f(b) \quad \text{für alle } a, b \in R_1$$
$$f(a \cdot_1 b) = f(a) \cdot_2 f(b) \quad \text{für alle } a, b \in R_1$$

Homo von Gruppen

Homo von HG

Besitzen beide Ringe ein Einselement 1_{R_1} bzw. 1_{R_2}, so wird für einen **Homomorphismus von Ringen mit Eins** zusätzlich $f(1_{R_1}) = 1_{R_2}$ gefordert.

Es reicht wieder zu zeigen: $f(1_{R_1})$ ist multipl. invertierbar.

analog: Endo, Iso, Auto

Komposition/Inverse von Homo-/Isomorphismen

Satz 9.18

Es seien $(R_1, +_1, \cdot_1)$, $(R_2, +_2, \cdot_2)$ und $(R_3, +_3, \cdot_3)$ drei Ringe.

1. Sind $f : R_1 \to R_2$ und $g : R_2 \to R_3$ Halbgruppenhomomorphismen, dann ist auch $g \circ f : R_1 \to R_3$ ein Halbgruppenhomomorphismus.
2. Ist $f : R_1 \to R_2$ ein Ringisomorphismus, dann ist auch $f^{-1} : R_2 \to R_1$ ein Ringisomorphismus.

Folgerung 9.19

Isomorphie von Ringen ist eine Äquivalenzrelation.

Bild und Kern eines Ringhomomorphismus

Definition 9.21

Es sei $f : (R_1, +_1, \cdot_1) \to (R_2, +_2, \cdot_2)$ ein Ringhomomorphismus.

Das **Bild** und der **Kern** von f sind definiert als

$$\text{Bild}(f) := \{f(a_1) \in R_2 \mid a_1 \in R_1\} = f(R_1) \quad \subseteq R_2$$
$$\text{Kern}(f) := \{a_1 \in R_1 \mid f(a_1) = 0_{R_2}\} = f^{-1}(\{0_{R_2}\}) \quad \subseteq R_1$$

Lemma 9.22

$\text{Bild}(f)$ ist ein Unterring von $(R_2, +_2, \cdot_2)$.
$\text{Kern}(f)$ ist ein Unterring von $(R_1, +_1, \cdot_1)$.

Homomorphismus von Ringen

Beispiel 9.23

1. Die Abbildung

$$f : (\mathbb{Z}, +, \cdot) \ni a \mapsto \overbrace{2\,a}^{a+a} = 2 \cdot a \in (\mathbb{Z}, +, \cdot)$$

ist kein Endomorphismus von Ringen.

$$f(a+b) = 2\cdot(a+b) = 2\cdot a + 2b = f(a) + f(b)$$
$$f(a\cdot b) = 2\cdot(a\cdot b)$$
$$f(a)\cdot f(b) = (2\cdot a)\cdot(2\cdot b) = 4\cdot a\cdot b$$

$\Big\}\neq$

Homomorphismus von Ringen

Beispiel 9.23 f^{-1} = „natürliche Repr. mit $\mathbb{Z}_m$"

2. Für $m \in \mathbb{N}$ ist die Abbildung

$$f : (\mathbb{Z}_m, +_m, \cdot_m) \ni a \mapsto [a] = a + m\mathbb{Z} \in (\mathbb{Z}/m\mathbb{Z}, \tilde{+}, \tilde{\cdot})$$

ein Isomorphismus zwischen dem Ring $\mathbb{Z}$ modulo m und dem Restklassenring modulo m, beides kommutative Ringe mit Eins.

$$\begin{array}{lccccc} \text{in } (\mathbb{Z}/5\mathbb{Z}, \tilde{+}) & [-21] & \tilde{+} & [9] & = & [-12] \\ & \downarrow f^{-1} & & \downarrow & & \downarrow \\ \text{in } (\mathbb{Z}_5, +_5) & 4 & +_5 & 4 & = & 3 \end{array}$$

$$\begin{array}{lccccc} \text{in } (\mathbb{Z}/5\mathbb{Z}, \tilde{\cdot}) & [-21] & \tilde{\cdot} & [9] & = & [-189] \\ & \downarrow f^{-1} & & \downarrow & & \downarrow \\ \text{in } (\mathbb{Z}_5, \cdot_5) & 4 & \cdot_5 & 4 & = & 1 \end{array}$$

Homomorphismus von Ringen

Beispiel 9.23

3. Für Mengen X und $Y \subseteq X$ ist die Abbildung

$$f : (\mathcal{P}(X), \triangle, \cap) \ni A \mapsto A \cap Y \in (\mathcal{P}(Y), \triangle, \cap)$$

ein Homomorphismus von Ringen mit Eins.

$f(A \triangle B) = (A \triangle B) \cap Y$
$f(A) \triangle f(B) = (A \cap Y) \triangle (B \cap Y)$
} = nach Distributivgesetz

$f(A \cap B) = (A \cap B) \cap Y$
$f(A) \cap f(B) = (A \cap Y) \cap (B \cap Y)$
} =

$f(X) = X \cap Y = Y$

Homomorphismus von Ringen

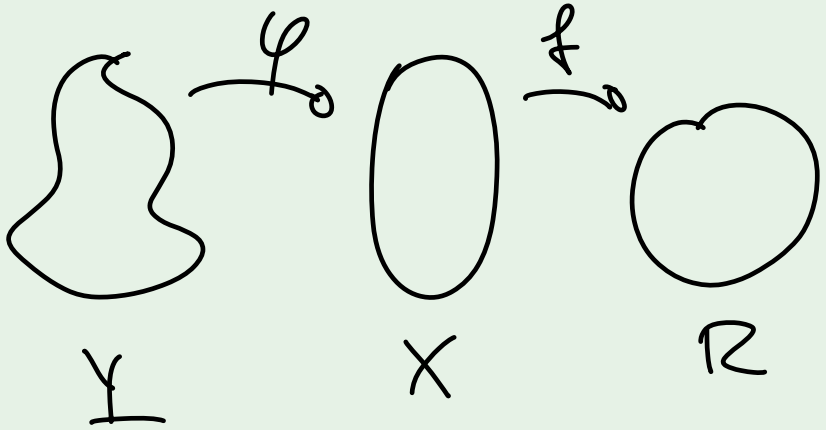
Beispiel 9.23

4. Es seien $(R, +, \cdot)$ ein Ring, X, Y Mengen und $\varphi\colon Y \to X$.

   φ induziert einen Ringhomomorphismus

   $$\varphi^*\colon (R^X, +, \cdot) \ni f \mapsto f \circ \varphi \in (R^Y, +, \cdot),$$

   genannt der **Pullback** φ^* von φ.



$\varphi^*(f+g) = (f+g)\circ\varphi$ (Addition in $(R^X,+)$)

$= (f\circ\varphi) + (g\circ\varphi)$ (Addition in $(R^Y,+)$)

$= \varphi^*(f) + \varphi^*(g)$

$\varphi^*(f\cdot g) = (f\cdot g)\circ\varphi$

$= (f\circ\varphi)\cdot(g\circ\varphi) = \varphi^*(f)\cdot\varphi^*(g)$

Injektivität eines Ringhomomorphismus

Lemma 9.24

Es seien $(R_1, +_1, \cdot_1)$ und $(R_2, +_2, \cdot_2)$ Ringe mit den Nullelementen 0_{R_1} bzw. 0_{R_2}. Für einen Homomorphismus $f : R_1 \to R_2$ sind äquivalent:

1. f ist injektiv.
2. $\mathrm{Kern}(f) = \{0_{R_1}\}$.
3. Die einzige Lösung der Gleichung $f(a) = 0_{R_2}$ ist $a = 0_{R_1}$.

§ 9.1 Ideale und Faktorringe

Ideal

Ideale sind bestimmte Unterringe, die dieselbe Funktion einnehmen wie Normalteiler in Gruppen.

Definition 9.25

Es sei $(R, +, \cdot)$ ein Ring.

1. Eine Teilmenge $J \subseteq R$ heißt ein **Ideal** von $(R, +, \cdot)$, wenn J ein Unterring von R ist und zusätzlich gilt:

$$R \cdot J \subseteq J \quad \text{und} \quad J \cdot R \subseteq J \qquad (*)$$

Zu zeigen: $(J, +)$ ist UG von $(R, +)$ sowie $(*)$,

denn: $(*) \Rightarrow J \cdot J \subseteq J$

2. Ein Ideal $(J, +, \cdot)$ von $(R, +, \cdot)$ heißt **echt**, wenn $J \subsetneq R$ gilt.

„ist Ideal von" ist nicht transitiv (keine Ordnungsrelation)

Kerne von Ringhomomorphismen sind Ideale

Lemma 9.27

Es seien $(R_1, +_1, \cdot_1)$ und $(R_2, +_2, \cdot_2)$ Ringe und $f : R_1 \to R_2$ ein Homomorphismus. Dann gilt:

1. Die Elemente von R_1, die denselben Funktionswert wie $a \in R_1$ haben, sind genau die Elemente der additiven Nebenklasse von $\operatorname{Kern}(f)$ zu a:

$$f^{-1}(\{f(a)\}) = a +_1 \operatorname{Kern}(f) = \operatorname{Kern}(f) +_1 a.$$

2. $\operatorname{Kern}(f)$ ist ein Ideal von R_1.

Beweis: ① folgt aus Lemma 8.18, da $f: (R_1, +_1) \to (R_2, +_2)$ ein Gruppenhomo ist. $\operatorname{Kern}(f)$ ist eine normale UG von $(R_1, +_1)$.

② Für $a \in R$ und $j \in \operatorname{Kern}(f)$ gilt:

$f(a \cdot_1 j) = f(a) \cdot_2 f(j) = f(a) \cdot_2 0_{R_2} = 0_{R_2} \Rightarrow a \cdot_1 j \in \operatorname{Kern}(f)$

analog: $j \cdot_1 a$

Ideal

Beispiel 9.29

1. In jedem Ring $(R, +, \cdot)$ sind die trivialen Unterringe $\{0\}$ (das **Nullideal**) und R (das **Einsideal**) Ideale.

2. Die Mengen der Form $m\mathbb{Z}$ mit $m \in \mathbb{N}$ sind genau die Ideale des Ringes $(\mathbb{Z}, +, \cdot)$.

3. Ist X eine Menge und $Y \subseteq X$, dann ist $(\mathcal{P}(Y), \triangle, \cap)$ ein Ideal von $(\mathcal{P}(X), \triangle, \cap)$. UG-Kriterium: $\mathcal{P}(Y) \neq \emptyset$ und

$$\underbrace{A}_{\subseteq Y} \triangle (-\underbrace{B}_{\subseteq Y}) = A \triangle B \subseteq Y$$

$$\underbrace{C}_{\subseteq X} \cap \underbrace{A}_{\subseteq Y} = A \cap C \subseteq Y$$

Faktorring bzgl. eines Ideals

Satz 9.30

Es sei $(R, +, \cdot)$ ein Ring und J ein Ideal. Dann gilt:

1. Die Faktormenge $R / J = \{[a] = a + J \mid a \in R\}$ mit

$$[a] \mathbin{\tilde{+}} [b] := [a + b] \quad \text{für } a, b \in R$$
$$[a] \mathbin{\tilde{\cdot}} [b] := [a \cdot b] \quad \text{für } a, b \in R$$

   ist ein Ring, genannt der **Faktorring von R nach J**. Das Nullelement ist $[0_R] = J$. Für die additiven Inversen gilt $\tilde{-}[a] = [-a]$.

2. Die **kanonische Surjektion** von R auf R / J

$$\pi : R \ni a \mapsto [a] \in R / J$$

   ist ein surjektiver Ringhomomorphismus. Es gilt $\operatorname{Kern}(\pi) = J$.

3. Wenn R ein kommutativer Ring ist, dann auch R / J.

Faktorring bzgl. eines Ideals

Satz 9.30

Es sei $(R, +, \cdot)$ ein Ring. Dann gilt:

4. Ist U irgendein Unterring und ist die Verknüpfung $\tilde{\cdot}$ auf der Menge der Nebenklassen $R \,/\, U$ wohldefiniert, dann ist U notwendigerweise ein Ideal von R.

Faktorring

Beispiel 9.32

1. Für $m \in \mathbb{N}$ ist der Faktorring $\mathbb{Z} / m\mathbb{Z}$ des Ringes $(\mathbb{Z}, +, \cdot)$ nach dem Ideal $m\mathbb{Z}$ der Restklassenring modulo m (Beispiel 9.6).

   Dieser ist isomorph zu $(\mathbb{Z}_m, +_m, \cdot_m)$, dem Ring von $\mathbb{Z}$ modulo m (Beispiel 9.23).

2. Ist X eine Menge und $Y \subseteq X$, dann ist der Faktorring $\mathcal{P}(X) / \mathcal{P}(Y)$ isomorph zum Ring $(\mathcal{P}(X \setminus Y), \triangle, \cap)$.

erzeugtes Ideal und Hauptideal

Definition 9.35

Es sei $(R, +, \cdot)$ ein Ring und $E \subseteq R$.

1. Dann heißt

   Durchschnitt von Idealen ist Idealen

   $$(E) := \bigcap \{ J \mid J \text{ ist Ideal von } R \text{ und } E \subseteq J \}$$

   das von E **erzeugte Ideal** in R.

2. Ist speziell $E = \{a\}$ für ein $a \in R$, so schreiben wir auch (a) statt $(\{a\})$ und nennen (a) das **von a erzeugte Hauptideal**.

   analog zur zykl. UG $\langle a \rangle$

3. Ein Ideal $(J, +, \cdot)$ heißt ein **Hauptideal**, wenn es ein $a \in R$ gibt, sodass gilt: $(a) = J$.

Darstellung des erzeugten Ideals

Satz 9.36

Es sei $(R, +, \cdot)$ ein Ring, $E \subseteq R$ und $a \in R$. Dann gilt

wie bei erzeugten UG

$$(E) = \left\{ \sum_{i=1}^{n} a_i \;\middle|\; \exists n \in \mathbb{N}_0 \; \forall i = 1, \ldots, n \; \left(a_i \in E \cup -E \cup R \cdot E \cup E \cdot R \cup R \cdot E \cdot R \right) \right\}$$

$$(a) = \left\{ \sum_{i=1}^{n} a_i \;\middle|\; \exists n \in \mathbb{N}_0 \; \forall i = 1, \ldots, n \; \left(a_i \in \{a\} \cup \{-a\} \cup Ra \cup aR \cup RaR \right) \right\}$$

Diese Darstellungen können vereinfacht werden, wenn R ein Einselement besitzt oder kommutativ ist.

erzeugtes Ideal

Beispiel 9.37

1. Der **Kommutator** der Elemente a, b eines Ringes $(R, +, \cdot)$ ist definiert als

$$[a, b] := a \cdot b - b \cdot a.$$

Das **Kommutatorideal** eines Ringes $(R, +, \cdot)$ ist das von Kommutatoren von R erzeugte Ideal, also

$$K := \left(\left\{[a, b] \,\middle|\, a, b \in R\right\}\right).$$

Ist $(R, +, \cdot)$ ein beliebiger Ring und K sein Kommutatorideal, dann ist der Faktorring $(R \,/\, K, \tilde{+}, \tilde{\cdot})$ kommutativ.

Tatsächlich ist $(R \,/\, J, \tilde{+}, \tilde{\cdot})$ genau dann kommutativ, wenn das ausfaktorisierte Ideal J das Kommutatorideal von R enthält.

§ 9.2 Der Homomorphiesatz für Ringe

Homomorphiesatz für Ringe

Satz 9.38

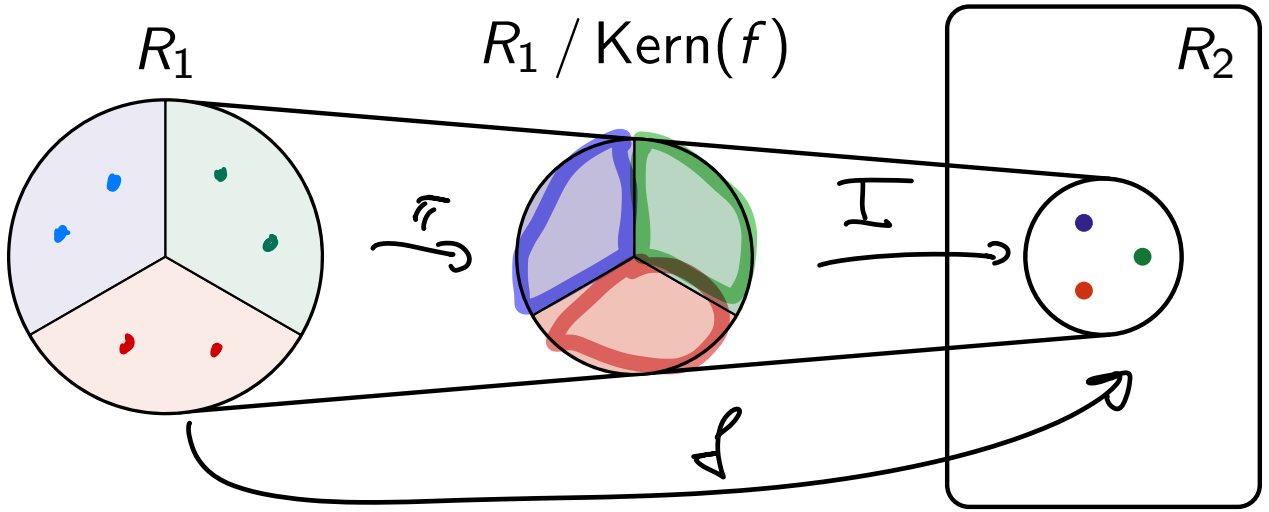
Es sei $f : (R_1, +_1, \cdot_1) \to (R_2, +_2, \cdot_2)$ ein Ringhomomorphismus.

Dann ist

$$\begin{aligned} I : R_1 / \operatorname{Kern}(f) &\longrightarrow \operatorname{Bild}(f) \\ a + \operatorname{Kern}(f) = [a] &\longmapsto f(a) \end{aligned}$$

$f|^{\operatorname{Bild}(f)} = I \circ \pi$

ein Ringisomorphismus.



§ 10 Körper

Körper

Definition 10.1

Ein **Körper** $(K, +, \cdot)$ ist eine Menge K mit zwei Verknüpfungen $+$ und $\cdot$, die die folgenden Bedingungen erfüllen:

1. $(K, +)$ ist eine abelsche Gruppe. Nullelement 0_K
2. $(K \setminus \{0_K\}, \cdot)$ ist eine abelsche Gruppe. Einselement 1_K
   Alle El., die multipl. invertierbar sind können, sind es auch.
   $0_K \cdot a = 0_K \quad \forall a \in K$
3. Es gelten die **Distributivgesetze**

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$
$$(a + b) \cdot c = (a \cdot c) + (b \cdot c)$$

} fallen zusammen

Ein Körper ist ein spezieller kommut. Ring mit $1_K \neq 0_K$

Körper

Beispiel 10.2

1. $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ und $(\mathbb{C}, +, \cdot)$ sind Körper.

   Nullel. 0 , Einsel. 1

2. $(\mathbb{Z}_2, +_2, \cdot_2)$ ist ein kleinstmöglicher Körper.

   bis auf Isomorphie eindeutig

3. Der Restklassenring $(\mathbb{Z}/4\mathbb{Z}, \tilde{+}, \tilde{\cdot})$ mit dem Nullelement [0] und dem Einselement [1] ist kein Körper.

   [2] ist nicht multipl. invertierbar.

Funktionen mit Werten in einem Körper

Beispiel 10.2

Es sei X eine Menge.

1. Ist $(H, +)$ eine Halbgruppe, dann ist auch $(H^X, +)$ Halbgruppe.
2. Ist $(M, +)$ ein Monoid, dann ist auch $(M^X, +)$ ein Monoid.
3. Ist $(G, +)$ eine Gruppe, dann ist auch $(G^X, +)$ eine Gruppe.
4. Ist $(R, +, \cdot)$ ein Ring, dann ist auch $(R^X, +, \cdot)$ ein Ring.
5. Ist $(K, +, \cdot)$ ein Körper, dann ist $(K^X, +, \cdot)$ i.A. kein Körper

wenn X mind. 2 El. hat

denn $K^X \setminus \{0\}$ enthält mit Funktionen, die an einer Nullfunktion

mind. einem $x \in X$ den Wert 0 annehmen, El., die nicht mult. invertierbar sind.

Körper und Integritätsringe

Satz 10.3

1. Jeder Körper $(K, +, \cdot)$ ist ein Integritätsring.
   (kommutativer, nullteilerfreier Ring mit Eins ungleich dem Nullring)

2. Jeder endliche Integritätsring $(R, +, \cdot)$ ist ein Körper.

Folgerung 10.4

Der Restklassenring $(\mathbb{Z}/m\mathbb{Z}, \tilde{+}, \tilde{\cdot})$ modulo m ist ein Körper genau dann, wenn $m \in \mathbb{N}$ eine Primzahl ist (Satz 9.11).

Dasselbe gilt für den zu $\mathbb{Z}/m\mathbb{Z}$ isomorphen Ring von $\mathbb{Z}$ modulo m $(\mathbb{Z}_m, +_m, \cdot_m)$.

In diesem Fall nennen wir diese auch **Restklassenkörper modulo m** bzw. **Körper von $\mathbb{Z}$ modulo m**.

Charakteristik eines Ringes

Bemerkung 10.5

Es sei $(K, +, \cdot)$ ein Körper mit Einselement 1_K.

Wenn $\underbrace{n\,1_K}_{1_K + \cdots + 1_K} = 0_K$ für ein $n \in \mathbb{N}$ gilt, dann heißt

$$\min\{n \in \mathbb{N} \mid n\,1_K = 0_K\}$$

die **Chakteristik** von K, kurz $\operatorname{char}(K)$. (kann wegen $1_K \neq 0_K$ nicht 1 sein)
Andernfalls setzen wir $\operatorname{char}(K) = 0$.

Beispiel

1. $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ und $(\mathbb{C}, +, \cdot)$ haben die Charakteristik 0.
2. Für $m \in \mathbb{N}$ prim hat der Körper $(\mathbb{Z}_m, +_m, \cdot_m)$ die Charakteristik m.

Fakt: $\operatorname{char}(K)$ ist Null oder prim.

Unterkörper

Definition 10.6

Es sei $(K, +, \cdot)$ ein Körper.

1. Eine bzgl. $+$ und $\cdot$ abgeschlossene Teilmenge $U \subseteq K$ heißt ein **Unterkörper** von $(K, +, \cdot)$, wenn $(U, +, \cdot)$ selbst wieder ein Körper ist.

   zu zeigen: $(U, +)$ ist UG von $(K, +)$ und $(U \setminus \{0_K\}, \cdot)$ ist UG von $(K \setminus \{0_K\}, \cdot)$

2. Ein Unterkörper $(U, +, \cdot)$ von $(K, +, \cdot)$ heißt **echt**, wenn $U \subsetneq K$ gilt.

Lemma 7.43: Das Nullelement 0_K von K ist auch das Nullelement von U. Das Einselement 1_K von K ist auch das Einselement von U.

Unterkörperkriterium

Satz 10.7

Es sei $(K, +, \cdot)$ ein Körper und $U \subseteq K$.

Dann sind äquivalent:

1. $(U, +, \cdot)$ ist ein Unterkörper von $(K, +, \cdot)$.
2. U besitzt mindestens zwei Elemente, und für alle $a, b \in U$ gilt $a - b \in U$ sowie $a \cdot b^{-1} \in U$, sofenr $b \neq 0_K$ ist.

Beispiel 10.8

1. $(\mathbb{Q}, +, \cdot)$ ist ein Unterkörper von $(\mathbb{R}, +, \cdot)$.
   $(\mathbb{R}, +, \cdot)$ ist ein Unterkörper von $(\mathbb{C}, +, \cdot)$.
2. Der Restklassenkörper $\mathbb{Z} / m\mathbb{Z}$ (mit $m \in \mathbb{N}$ prim) und der zu ihm isomorphe Körper $\mathbb{Z}_m$ besitzen keine echten Unterkörper.

Homomorphismus von Körpern

Definition 10.11

Es seien $(K_1, +_1, \cdot_1)$ und $(K_2, +_2, \cdot_2)$ zwei Körper.

Eine Abbildung $f\colon K_1 \to K_2$ heißt **strukturverträglich** oder ein **Homomorphismus** von $(K_1, +_1, \cdot_1)$ in $(K_2, +_2, \cdot_2)$, wenn gilt:

wie bei Ringen mit Eins

$$\begin{aligned} f(a +_1 b) &= f(a) +_2 f(b) \quad \text{für alle } a, b \in K_1 \\ f(a \cdot_1 b) &= f(a) \cdot_2 f(b) \quad \text{für alle } a, b \in K_1 \\ f(1_{K_1}) &= 1_{K_2} \end{aligned}$$

P

Es reicht aus, $f(1_{K_1}) \neq 0_{K_2}$ zu zeigen.

Körperhomomorphismen sind injektiv

Lemma 10.14

Es sei $f : (K_1, +_1, \cdot_1) \to (K_2, +_2, \cdot_2)$ ein Körperhomomorphismus.

Dann ist f injektiv.

Beweis. Es sei $a \neq b$, aber $f(a) = f(b)$.

$$1_{K_2} = f(1_{K_1}) = f\big(\underbrace{(a -_1 b)}_{\neq 0}{}^{-1} \cdot_1 \underbrace{(a -_1 b)}_{\neq 0}\big)$$

$$= f((a -_1 b)^{-1}) \cdot_2 f(a -_1 b)$$

$$= \text{---}\!\!*\!\!\text{---} \cdot_2 \underbrace{[f(a) -_2 f(b)]}_{=0_{K_2}}$$

$$= 0_{K_2} \quad \lightning$$

Körperhomomorphismen

Beispiel 10.15

1. Die Einbettungen (mit Abb.)

$$(\mathbb{Q}, +, \cdot) \ni x \mapsto x \in (\mathbb{R}, +, \cdot)$$
$$(\mathbb{R}, +, \cdot) \ni x \mapsto x \in (\mathbb{C}, +, \cdot)$$

   sind Körperhomomorphismen.

2. Die Körper $(\mathbb{Q}, +, \cdot)$ und $(\mathbb{R}, +, \cdot)$ besitzen außer der Identität keine weiteren Körperautomorphismen.

3. Die komplexe Konjugation $(\mathbb{C}, +, \cdot) \ni x \mapsto \overline{x} \in (\mathbb{C}, +, \cdot)$ ist ein Körperautomorphismus. Unter AoC gibt es viele weitere.

4. Realteil $(\mathbb{C}, +, \cdot) \ni x \mapsto \operatorname{Re} x \in (\mathbb{R}, +, \cdot)$ und Imaginärteil $(\mathbb{C}, +, \cdot) \ni x \mapsto \operatorname{Im} x \in (\mathbb{R}, +, \cdot)$ sind keine Körperhomomorphismen

   Sie sind nicht injektiv!

Bild und Kern eines Körperhomomorphismus

Definition 10.17

Es sei $f : (K_1, +_1, \cdot_1) \to (K_2, +_2, \cdot_2)$ ein Körperhomomorphismus.

Das **Bild** und der **Kern** von f sind definiert als

$$\text{Bild}(f) := \{f(a_1) \in K_2 \mid a_1 \in K_1\} = f(K_1) \quad \subseteq K_2$$
$$\text{Kern}(f) := \{a_1 \in K_1 \mid f(a_1) = 0_{K_2}\} = f^{-1}(\{0_{K_2}\}) \subseteq K_1$$

$\text{Bild}(f)$ ist ein Unterkörper von $(K_2, +_2, \cdot_2)$.
$\text{Kern}(f)$ ist kein Unterkörper von $(K_1, +_1, \cdot_1)$, denn $\text{Kern}(f) = \{0_{K_1}\}$

Ausfaktorisieren bei Körpern?

Gruppe modulo Normalteiler	G / N	Faktorgruppe
Ring modulo Ideal	R / J	Faktorring
Körper modulo Ideal ?	K / J	Faktorkörper ?

Würden wir für einen Körper K und einen Unterkörper U versuchen, auf der Faktormenge K / U die Verknüpfungen

$$[a] \mathbin{\tilde{+}} [b] = [a + b] \quad \text{und} \quad [a] \mathbin{\tilde{\cdot}} [b] = [a \cdot b]$$

einzuführen, um wieder eine Körperstruktur zu bekommen, dann könnten wir K auch als Ring betrachten und würden mit den obigen Verknüpfungen auf K / U auch eine Ringstruktur bekommen. Nach Satz 9.30 ist dafür aber notwendigerweise U ein Ideal des Ringes K. In einem Körper gibt es jedoch nur die beiden trivialen Ideale

$U_1 = \{0_K\}$ $\Rightarrow$ $K/U_1 \cong K$ kein neuer Körper

$U_2 = K$ $\Rightarrow$ $K/U_2 \cong \{0_K\}$ kein Körper

geordneter Körper

Definition 10.19

"Trennelement"

Es seien $(K, +, \cdot)$ ein Körper mit dem Nullelement 0_K und $\leqslant$ eine Totalordnung auf K.

1. Der Körper heißt **geordnet** bzgl. der Totalordnung $\leqslant$, wenn

$$\alpha \leqslant \beta \quad \Rightarrow \quad \alpha + \gamma \leqslant \beta + \gamma$$

Komp. mit +

$$\alpha \geqslant 0_K \text{ und } \beta \geqslant 0_K \quad \Rightarrow \quad \alpha \cdot \beta \geqslant 0_K$$

Komp. mit ·

für alle $\alpha, \beta, \gamma \in K$ gilt.

geordneter Körper

Definition 10.19

Es seien $(K, +, \cdot)$ ein Körper mit dem Nullelement 0_K und $\leqslant$ eine Totalordnung auf K.

2. $\alpha \in K$ heißt **nichtnegativ**, wenn $\alpha \geqslant 0_K$ ist.
3. $\alpha \in K$ heißt **positiv**, wenn $\alpha \geqslant 0_K$ und $\alpha \neq 0_K$ ist.
4. $\alpha \in K$ heißt **nichtpositiv**, wenn $\alpha \leqslant 0_K$ ist.
5. $\alpha \in K$ heißt **negativ**, wenn $\alpha \leqslant 0_K$ und $\alpha \neq 0_K$ ist.

Rechenregeln in geordneten Körpern

Lemma 10.20

Es sei $(K, +, \cdot)$ mit der Totalordnung $\leqslant$ ein geordneter Körper.
Dann gilt für $\alpha, \beta, \gamma, \delta \in K$:

1. $\alpha \geqslant 0_K \quad \Leftrightarrow \quad -\alpha \leqslant 0_K$
2. $\alpha \leqslant \beta$ und $\gamma \leqslant \delta \quad \Rightarrow \quad \alpha + \gamma \leqslant \beta + \delta$
3. $\alpha \leqslant \beta$ und $\gamma \geqslant 0_K \quad \Rightarrow \quad \alpha \cdot \gamma \leqslant \beta \cdot \gamma$
4. $\alpha \leqslant \beta$ und $\gamma \leqslant 0_K \quad \Rightarrow \quad \alpha \cdot \gamma \geqslant \beta \cdot \gamma$
5. $\alpha^2 \geqslant 0_K$
6. $\alpha \neq 0_K \quad \Rightarrow \quad \alpha^2 > 0_K$. Insbesondere gilt $1_K > 0_K$.
7. $\alpha > 0_K \quad \Rightarrow \quad \alpha^{-1} > 0_K$
8. $\beta > \alpha > 0_K \quad \Rightarrow \quad \alpha^{-1} > \beta^{-1} > 0_K$
9. $n\,1_K > 0_K$ für alle $n \in \mathbb{N}$.
   Insbesondere gilt notwendigerweise $\mathrm{char}(K) = 0_K$.

geordneter Körper

Beispiel 10.21

1. Die rationalen Zahlen $\mathbb{Q}$ mit der bekannten Totalordnung bilden einen geordneten Körper.

   einzig möglich

2. Die reellen Zahlen $\mathbb{R}$ mit der bekannten Totalordnung bilden einen geordneten Körper.

   einzig möglich

3. Die komplexen Zahlen $\mathbb{C}$ sind mit keiner Totalordnung ein geordneter Körper.

   $i^2 = -1 < 0$ $\lightning$ zu $\alpha^2 \geq 0 \quad \forall \alpha \in \mathbb{C}$