Lineare Algebra I

Woche 06

21.11.2023 und 23.11.2023

Normalteiler

Die Untergruppe $(U, \star)$ einer Gruppe $(G, \star)$ induziert die zwei Äquivalenzrelationen $\sim^U$ und ${}^U\!\sim$ auf G mit den Äquivalenzklassen

$$[a]_{\sim^U} = a \star U \quad \text{bzw.} \quad [a]_{{}^U\!\sim} = U \star a.$$

Definition

$N \trianglelefteq G$

Eine Untergruppe $(N, \star)$ heißt eine **normale Untergruppe** oder **Normalteiler** von $(G, \star)$, wenn gilt:

$a \star N = N \star a$ für alle $a \in G$. ↓ Gleichheit von Mengen, nicht notwendigerweise $an = na$

Beispiel

- $\{e\}$ und G sind immer Normalteiler.
- Ist G abelsch (kommutativ), dann ist jede Untergruppe ein Normalteiler.

Kerne von Gruppenhomomorphismen sind Normalteiler

Lemma

Es sei $f : (G_1, \star) \to (G_2, \square)$ ein Gruppenhomomorphismus.

Dann gilt

$$\boxed{f^{-1}(\{f(a)\})} = a \star \mathrm{Kern}(f) \overset{b}{=} \mathrm{Kern}(f) \star a,$$

Elemente in G_1 mit demselben Bild wie a

analog

für alle $a \in G_1$

also ist $\mathrm{Kern}(f)$ ein Normalteiler von G_1.

Beweis. • $f^{-1}(\{f(a)\}) \subseteq a * \mathrm{Kern}(f)$:

Es sei $b \in f^{-1}(\{f(a)\})$, also $f(b) = f(a)$.

$e_2 = f(a)' \square f(b) = f(a') \square f(b) = f(a' * b)$, also

$a' * b \in \mathrm{Kern}(f)$, d.h. $b \in a * \mathrm{Kern}(f)$.

• $a * \mathrm{Kern}(f) \subseteq f^{-1}(\{f(a)\})$:

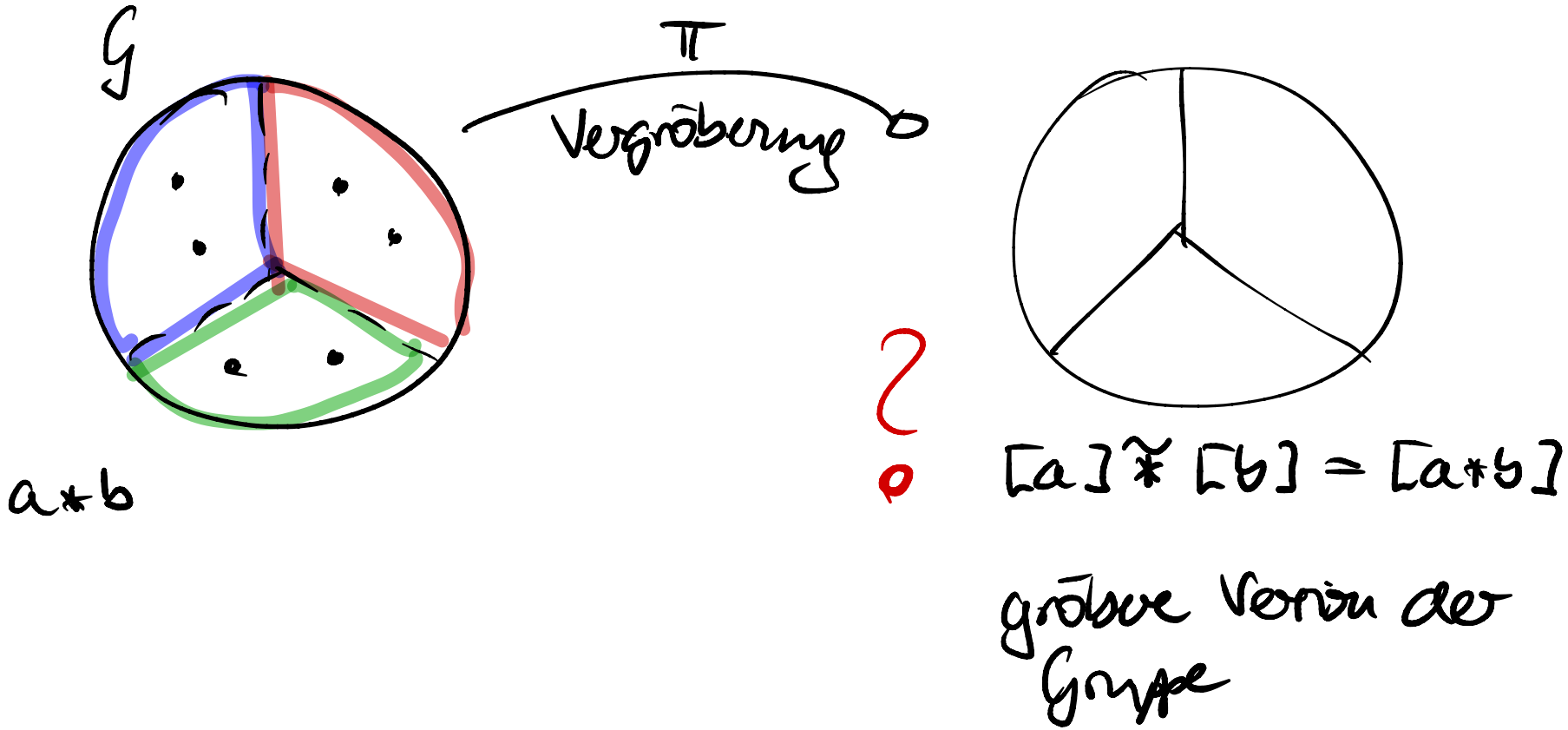
Es sei $b \in \mathrm{Kern}(f)$ beliebig. Zu zeigen ist $a * b \in f^{-1}(\{f(a)\})$.

$f(a * b) = f(a) \square f(b) = f(a) \square e_2 = f(a)$, d.h.

$a * b \in f^{-1}(\{f(a)\})$.

Faktormenge der durch Normalteiler induzierten Relation

Faktormenge $G / N = \{[a] = a \star N \mid a \in G\}$



Faktorgruppe der durch Normalteiler induzierten Relation

Satz

Es sei $(G, \star)$ eine Gruppe und $(N, \star)$ ein Normalteiler. Dann gilt:

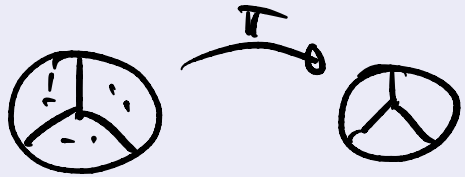
1. Die Faktormenge $G / N = \{[a] = a \star N \mid a \in G\}$ mit

$$[a] \mathbin{\tilde{\star}} [b] := [a \star b]$$

ist eine Gruppe. Neutrales Element ist $[e] = N$. Für die Inversen gilt $[a]' = [a']$.

2. Die **kanonische Surjektion** von G auf G / N

Vergrößerungsabb.



$$\pi \colon G \ni a \mapsto [a] \in G / N$$

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

erst verknüpfen, dann vergrößern = erst vergrößern, dann verknüpfen

3. Wenn $(G, \star)$ abelsch ist, dann auch $(G / N, \tilde{\star})$.

Faktorgruppe

Beispiel

1. Ausfaktorisieren des trivialen Normalteilers $\{e\}$ einer Gruppe $(G, \star)$:

$G/\{e\} \cong G$

Jede Nebenklasse hat genau ein Element.

2. Ausfaktorisieren des trivialen Normalteilers G einer Gruppe $(G, \star)$:

$G/G \cong \{e\}$

Alle Elemente in einer Nebenklasse.

Faktorgruppe

Beispiel

$m=2$: $2\mathbb{Z}$ = gerade Zahlen

3. In $(\mathbb{Z}, +)$ ist $m\mathbb{Z}$ für beliebiges $m \in \mathbb{N}$ ein Normalteiler.

   Die Elemente der Faktorgruppe $\mathbb{Z} / m\mathbb{Z}$ sind $[a] = a + m\mathbb{Z}$.

   In der Faktorgruppe rechnen wir $[a] \mathbin{\tilde{+}} [b] = [a + b]$.

$(\mathbb{Z}/5\mathbb{Z}, \tilde{+})$: $\quad [-21] \mathbin{\tilde{+}} [9] = [-12]$

Isomorphismus „natürliche Repr. mod 5"

$(\mathbb{Z}_5, +_5)$: $\quad 4 +_5 4 = 3$

$= \{0, 1, 2, 3, 4\}$

Homomorphiesatz für Gruppen

Wie arbeitet ein Gruppenhomomorphismus?

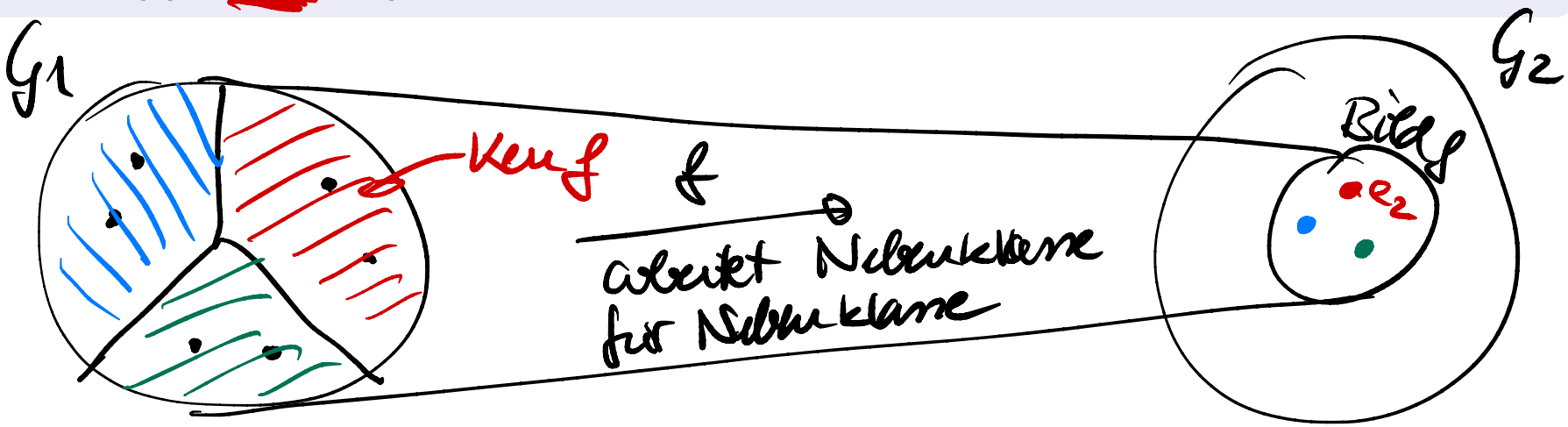
Satz

Es sei $f : (G_1, \star) \to (G_2, \square)$ ein Gruppenhomomorphismus.

Dann ist

$$\begin{array}{rccc} I : & G_1 \,/\, \mathrm{Kern}(f) & \longrightarrow & \mathrm{Bild}(f) \\ & [a] & \longmapsto & f(a) \end{array}$$

ein Gruppenisomorphismus.



Homomorphiesatz für Gruppen

Gruppe Gruppe

$$I : G_1 / \mathrm{Kern}(f) \longrightarrow \mathrm{Bild}(f)$$
$$[a] \longmapsto f(a) \qquad \text{ist Gruppenisomorphismus}$$

Beweis. • I ist wohldefiniert: $a \sim b \in G_1$, also
$a * \mathrm{Kern}(f) = b * \mathrm{Kern}(f)$.
$f(a * \mathrm{Kern}(f)) = f(a) \square f(\mathrm{Kern}(f)) = f(a) \square \{e_2\} =$
$\{f(a)\}$. Analog: $f(b * \mathrm{Kern}(f)) = \{f(b)\}$.
$a \sim b \Rightarrow f(a) = f(b)$

• I ist Homomorphismus zw. Gruppe:
$I([a] * [b]) = I([a * b]) = f(a * b)$
$= f(a) \square f(b) = I([a]) \square I([b])$

Homomorphiesatz für Gruppen

$$\begin{array}{rcll} I\colon G_1/\mathrm{Kern}(f) & \longrightarrow & \mathrm{Bild}(f) & \\ [a] & \longmapsto & f(a) & \text{ist Gruppenisomorphismus} \end{array}$$

Beweis. • I ist surjektiv: Ist $y \in \mathrm{Bild}(f)$, also $y = f(a)$ für ein $a \in G_1$, dann ist $y = f(a) = I([a])$, also ist I surjektiv.

• I ist injektiv: Wir zeigen: $\mathrm{Kern}(I) = \{[e]\}$.

$= \{\mathrm{Kern}(f)\}$: $\mathrm{Kern}(I) = \{[a] \mid a \in \mathrm{Kern}(f)\}$

$= \{a * \mathrm{Kern}\, f \mid a \in \mathrm{Kern}\, f\} = \{\mathrm{Kern}\, f\}$, also

ist I injektiv, ($\mathrm{Kern}\, f$ ist UG)

Homomorphiesatz für Gruppen

Beispiel

1. $f : (\mathbb{R}_{\neq 0}, \cdot) \ni x \mapsto x^2 \in (\mathbb{R}_{\neq 0}, \cdot)$

Gruppenendomorphismus

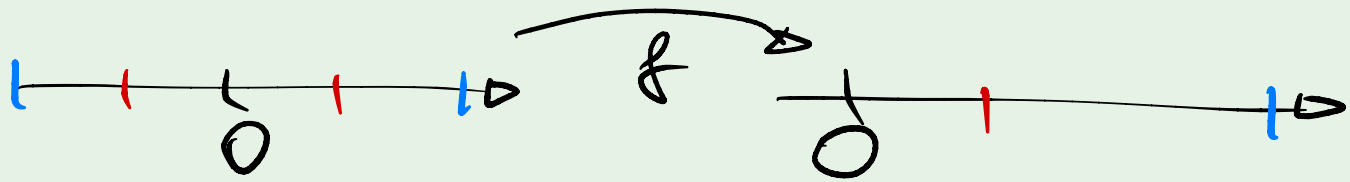
$\operatorname{Ker}(f) = \{\pm 1\}$.

$\bar{f} : \mathbb{R}_{\neq 0} / \{\pm 1\} \longrightarrow \operatorname{Bild}(f) = \mathbb{R}_{>0}$

$[x] \longmapsto x^2$

$= \{x, -x\}$

Das Vorzeichen wird ausfaktorisiert.



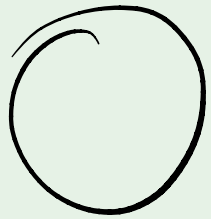
Homomorphiesatz für Gruppen

Beispiel

2. $f : (\mathbb{C}_{\neq 0}, \cdot) \ni z \mapsto |z| \in (\mathbb{R}_{\neq 0}, \cdot)$

ist Gruppenhomomorphismus.

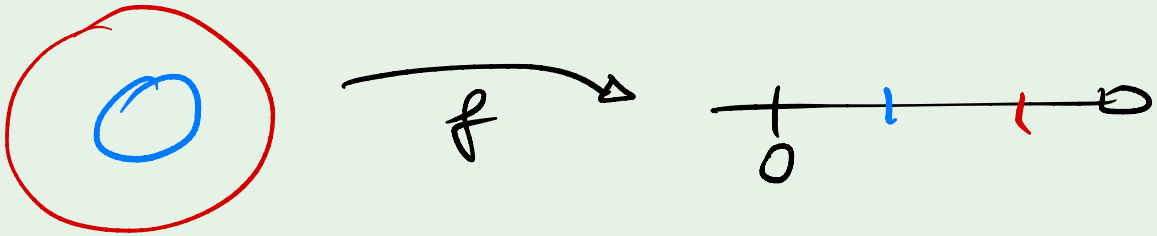
$\ker(f) = f^{-1}(\{1\}) = \{z \in \mathbb{C} : |z| = 1\}$



$\bar{f} : \mathbb{C}_{\neq 0} / \ker(f) \longrightarrow \mathrm{Bild}(f) = \mathbb{R}_{>0}$

$[z] \longmapsto |z|$

$[z]$: Kreislinie in $\mathbb{C}$



Homomorphiesatz für Gruppen

Beispiel

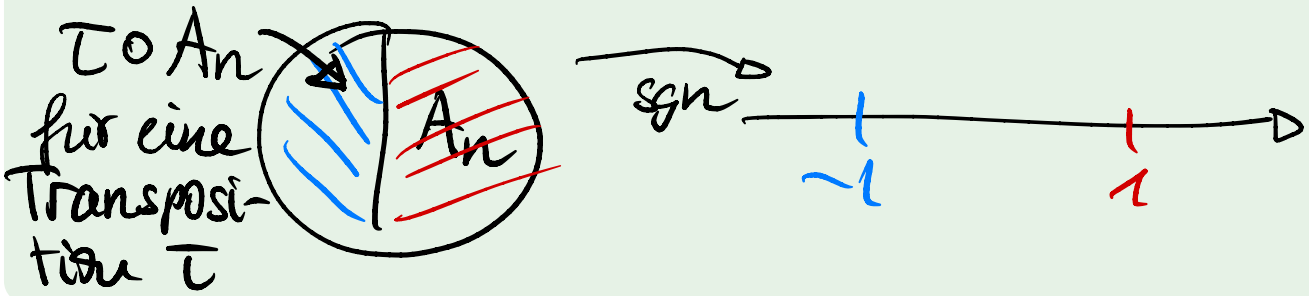
3. $\operatorname{sgn}: S_n \to (\{\pm 1\}, \cdot)$ $(n \geq 2)$

$\operatorname{Kern}(\operatorname{sgn}) = A_n$ (alle geraden Permutationen)

$\bar{I}: S_n / \operatorname{Kern}(\operatorname{sgn}) = S_n / A_n \longrightarrow \operatorname{Bild}(\operatorname{sgn}) = \{\pm 1\}$

$[\sigma] \longmapsto \operatorname{sgn}(\sigma)$

sgn bildet
alle geraden Permutationen auf 1
alle ungeraden —"— auf -1 ab,



Ring

typische Notation

Definition

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

1. $(R, +)$ ist eine abelsche Gruppe.
   ↕ kommutativ
2. $(R, \cdot)$ ist eine Halbgruppe.
3. Es gelten die **Distributivgesetze**

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

fallen zusammen für kommutative 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.

Ring

Beispiel

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

$(\mathbb{Z}, +)$ ist abelsche Gruppe

$(\mathbb{Z}, \cdot)$ ist komm. Halbgruppe mit Einselement 1

Distributivgesetze ✓

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

$0_R + 0_R = 0_R$ komm. Gruppe

$0_R \cdot 0_R = 0_R$ " "

Das Einselement ist 0_R! Distributivgesetze ✓

Ring

Beispiel

$m=2$: gerade Zahlen

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

   $(m\mathbb{Z}, +)$ ist abelsche Gruppe

   $(m\mathbb{Z}, \cdot)$ ist komm. Halbgruppe, ohne neutrales Element, wenn $m \geq 2$

   Distr.gesetz (e) vererbt sich von $(\mathbb{Z}, +, \cdot)$

4. Für $m \in \mathbb{N}$ ist $(\mathbb{Z}_m, +_m, \cdot_m)$ ein kommutativer Ring mit Einselement 1, der **Ring von $\mathbb{Z}$ modulo m**. $\{0, 1, \ldots, m-1\}$

   $m=1$: Nullring

   $(\mathbb{Z}_m, +_m)$ ist abelsche Gruppe

   $(\mathbb{Z}_m, \cdot_m)$ ist komm. Monoid mit 1

   Distributivgesetz (e)

Ring

Beispiel

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

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

mit den Verknüpfungen

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

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

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

Rechenregeln in Ringen

Lemma $a, b \in R$ beliebig

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

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

$= 0_R \cdot a + 0_R \cdot a$ | kürzen: $0_R = 0_R \cdot a$.

Dist. Rest analog

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

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

Rest analog

Rechenregeln in Ringen

Lemma

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

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

mind. 2 Elemente

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

$= a\cdot b$ (Invertierung ist involutorisch)

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

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

Charakteristik eines Ringes

Definition

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

1. $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$ und $(\mathbb{R}, +, \cdot)$ haben Charakteristik 0.
2. Der Nullring hat Charakteristik 1.
3. $(\mathbb{Z}_m, +_m, \cdot_m)$ hat Charakteristik $m \in \mathbb{N}$

Restklassenring modulo m (wichtiges Beispiel)

Definition

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

abelsche Gruppe $[a] \mathbin{\tilde{+}} [b] = [a+b]$ ← Beispiel S. 15

kommutativ Monoid $[a] \mathbin{\tilde{\cdot}} [b] = [a \cdot b]$ ← Hausaufgabe 6.1

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

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

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

Restklassenring modulo 4

Beispiel

$\tilde{+}$	[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 ist 0_R, aber beide Faktoren sind nicht 0_R!

Nullteiler, Integritätsring

Definition

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. $(R, +, \cdot)$ heißt **Integritätsring** oder **Integritätsbereich** im Fall
   - $(R, +, \cdot)$ ist kommutativer Ring mit Eins
   - $(R, +, \cdot)$ ist nullteilerfrei
   - $(R, +, \cdot)$ ist ungleich dem Nullring (hat mind. 2 Elemente)

Integritätsringe

Beispiel

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, und X habe mindestens zwei Elemente. Dann ist $(R^X, +, \cdot)$ nicht nullteilerfrei!

nicht Nullring

Funktionenring

$x_1 \neq x_2$

Wähle $f(x) = \begin{cases} 0_R & x = x_1 \\ 1_R & \text{sonst} \end{cases}$ $\quad g(x) = \begin{cases} 1_R & x = x_1 \\ 0_R & \text{sonst} \end{cases}$

$f \cdot g = 0_{R^X}$ Nullfunktion

Restklassenring modulo m

Satz

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

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

Beweis. $m=1 \Rightarrow (\mathbb{Z}/m\mathbb{Z}, \tilde{+}, \tilde{\cdot})$ ist der Nullring, kein Integritätsring.

Ab jetzt $m \geq 2$, $(\mathbb{Z}/m\mathbb{Z}, \tilde{+}, \tilde{\cdot})$ ist nicht der Nullring, kommut. Ring mit Eins $[1]$. Es kommt also nur auf die Nullteilerfreiheit an.

$\neg$ (2) $\Rightarrow \neg$ (1) d.h. (1) $\Rightarrow$ (2) Es sei $m \geq 4$ keine Primzahl. $m = a \cdot b$ für $a, b \in [2, m-1]$.

$[a] \neq [0] \neq [b]$. Es gilt $[0] = [m] = [a \cdot b]$

$= [a] \tilde{\cdot} [b]$, also ist $\mathbb{Z}/m\mathbb{Z}$ nicht nullteilerfrei.

Restklassenring modulo m

Satz

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

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

Beweis. (2) $\Rightarrow$ (1) Es sei $m \geq 2$ eine Primzahl. Es seien $[a], [b] \in \mathbb{Z}/m\mathbb{Z}$ mit $[0] = [a] \tilde{\cdot} [b] = [a \cdot b]$. 0 und $a \cdot b$ liegen also in derselben Restklasse, d.h. $a \cdot b - 0 = a \cdot b = mz$ für ein $z \in \mathbb{Z}$. m ist Primzahl, also enthält der Primfaktorzerlegung von a oder von b das m, also gilt $m \mid a$ oder $m \mid b$, d.h. $[a] = [0]$ oder $[b] = [0]$. Das heißt, $\mathbb{Z}/m\mathbb{Z}$ ist nullteilerfrei.

Unterring

vgl. Untergruppe

Definition

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

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

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

Das bedeutet: $(U, +)$ ist (kommut.) UG von $(R, +)$.
$(U, \cdot)$ ist abgeschlossen.

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

Es reicht nicht, zu fordern, dass $(U, \cdot)$ irgendein neutrales Element hat, es muss 1_R sein.

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

Homomorphismus von Ringen

Definition

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

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

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

   Besitzen beide Ringe ein Einselement 1_{R_1} bzw. 1_{R_2}, so wird zusätzlich $f(1_{R_1}) = 1_{R_2}$ gefordert.

2. Ist zudem $f : H_1 \to H_2$ bijektiv, so heißt f auch **strukturerhaltend** oder ein **Isomorphismus**.

Bild und Kern eines Ringhomomorphismus

Definition

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

$$\text{Bild}(f) := \{f(x) \in R_2 \,|\, x \in R_1\} = f(R_1),$$
$$\text{Kern}(f) := \{x \in R_1 \,|\, f(x) = 0_{R_2}\} = f^{-1}(\{0_{R_2}\}).$$

Lemma

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

Beweis. Übung

Homomorphismus von Ringen

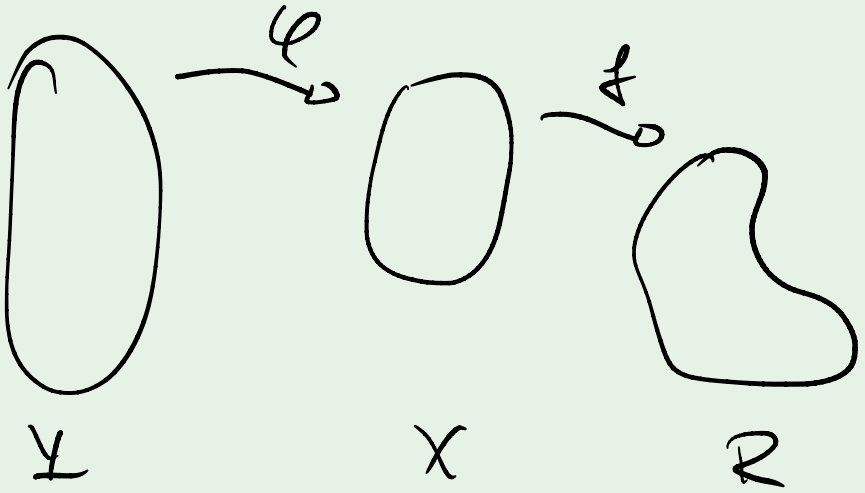
Beispiel

1. Es sei $(R, +, \cdot)$ 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 den **Pullback** φ^* von φ.



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

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

Homomorphismus von Ringen

Beispiel f^{-1} ist auch ein Isomorphismus: „Rest mod m"

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

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

$\{0, 1, \ldots, m-1\}$ $[a]$

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

$\mathbb{Z}/5\mathbb{Z}$ $\quad [21] \tilde{+} [9] = [-12] \quad | \quad [21] \tilde{\cdot} [9] = [-189]$

f^{-1} $\quad 4 +_5 4 = 3 \quad | \quad 4 \cdot_5 4 = 1$

vgl. Folie 7