Lineare Algebra I

Woche 06

21.11.2023 und 23.11.2023

Normalteiler

Die Untergruppe $(U, \star)$ einer Gruppe $(G, \star)$ induziert die 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

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

$$a \star N = N \star a \quad \text{für alle } a \in G.$$

Beispiel

Kerne von Gruppenhomomorphismen sind Normalteiler

Lemma

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

Dann gilt
$$f^{-1}(\{f(a)\}) = a \star \operatorname{Kern}(f) = \operatorname{Kern}(f) \star a,$$
also ist $\operatorname{Kern}(f)$ ein Normalteiler von G_1.

Beweis.

Faktormenge der durch Normalteiler induzierten Relation

Faktormenge $\quad G \,/\, N = \left\{ [a] = a \star N \,\middle|\, a \in G \right\}$

Faktorgruppe der durch Normalteiler induzierten Relation

Satz

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

1. Die Faktormenge $G \,/\, N = \big\{ [a] = a \star N \;\big|\; a \in G \big\}$ mit

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

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

2. Die **kanonische Surjektion** von G auf $G \,/\, N$

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

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

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

Faktorgruppe

Beispiel

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

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

Faktorgruppe

Beispiel

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 $[a] \mathbin{\widetilde{+}} [b] = [a + b]$.

Homomorphiesatz für Gruppen

Satz

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

Dann ist

$$\begin{aligned} I\colon\; G_1 \,/\, \operatorname{Kern}(f) \quad &\longrightarrow \quad \operatorname{Bild}(f) \\ [a] \quad &\longmapsto \quad f(a) \end{aligned}$$

ein Gruppenisomorphismus.

Homomorphiesatz für Gruppen

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

Beweis.

Homomorphiesatz für Gruppen

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

Beweis.

Homomorphiesatz für Gruppen

Beispiel

1.

Homomorphiesatz für Gruppen

Beispiel

2.

Homomorphiesatz für Gruppen

Beispiel

3.

Ring

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.
2. $(R, \cdot)$ ist eine Halbgruppe.
3. Es gelten die **Distributivgesetze**

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

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.

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

Ring

Beispiel

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

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**.

Beispiel

5. 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

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

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

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

Rechenregeln in Ringen

Lemma

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

Beweis.

Lemma

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

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

Beweis.

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
2. Der Nullring hat Charakteristik
3. $(\mathbb{Z}_m, +_m, \cdot_m)$ hat Charakteristik

Restklassenring modulo m

Definition

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

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

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

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

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

Restklassenring modulo 4

Beispiel

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

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

Nullteiler, Integritätsring

Definition

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

1. $a \in R$ heißt **Linksnullteiler**, wenn es $b \neq 0_R$ gibt mit $a \cdot b = 0_R$.
2. $b \in R$ heißt **Rechtsnullteiler**, wenn es $a \neq 0_R$ gibt mit $a \cdot b = 0_R$.
3. $(R, +, \cdot)$ heißt **nullteilerfrei**, wenn es außer 0_R keine weiteren Links- oder Rechtsnullteiler gibt, wenn also gilt:
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

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 $R^X = \{f \mid f\colon X \to R\}$ 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!

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.

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.

Definition

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

1. Eine bzgl. $+$ und $\cdot$ abgeschlossene Teilmenge $U \subseteq R$ heißt ein **Unterring** von $(R, +, \cdot)$, wenn $(U, +, \cdot)$ selbst wieder ein Ring ist.
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.
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 $f \colon R_1 \to R_2$ heißt **strukturverträglich** oder ein **Homomorphismus** von $(R_1, +_1, \cdot_1)$ in $(R_2, +_2, \cdot_2)$, wenn gilt:

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

   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 $f \colon H_1 \to H_2$ bijektiv, so heißt f auch **strukturerhaltend** oder ein **Isomorphismus**.

Bild und Kern eines Ringhomomorphismus

Definition

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

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

$$\begin{aligned} \operatorname{Bild}(f) &:= \{f(x) \in R_2 \mid x \in R_1\} = f(R_1), \\ \operatorname{Kern}(f) &:= \{x \in R_1 \mid f(x) = 0_{R_2}\} = f^{-1}(\{0_{R_2}\}). \end{aligned}$$

Lemma

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

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.

Homomorphismus von Ringen

Beispiel

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

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

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