Lineare Algebra Übungsstunde 4

Wiona Glänzer

12.10.2020

Definition: Gruppe

Eine Menge G zusammen mit einer Verknüpfung $*$ heisst eine **Gruppe** falls das folgende gilt:

1. $a * (b * c) = (a * b) * c$ für alle $a, b, c \in G$ (Assoziativgesetz),
2. Es gibt ein **neutrales Element** $e \in G$ so dass:
   2.1 $e * a = a$, für alle $a \in G$,
   2.2 zu jedem $a \in G$ gibt es ein **inverses Element** $a' \in G$, d.h. $a' * a = e$.

Untergruppen

Sei G eine Gruppe. Eine Teilmenge $H \subseteq G$ heisst **Untergruppe** falls:

1. H ist nicht die leere Menge.
2. Wenn $a, b \in H$, dann ist $ab \in H$,
3. Wenn $a \in H$, dann ist $a^{-1} \in H$.

Um 1. zu überprüfen kann auch $e \in H$ geprüft werden, denn:

Untergruppen

Sei G eine Gruppe. Eine Teilmenge $H \subseteq G$ heisst **Untergruppe** falls:

1. H ist nicht die leere Menge.
2. Wenn $a, b \in H$, dann ist $ab \in H$,
3. Wenn $a \in H$, dann ist $a^{-1} \in H$.

Um 1. zu überprüfen kann auch $e \in H$ geprüft werden, denn:
$\Leftarrow$ Gilt $e \in H$ so folgt direkt H $\neq \emptyset$.

Untergruppen

Sei G eine Gruppe. Eine Teilmenge $H \subseteq G$ heisst **Untergruppe** falls:

1. H ist nicht die leere Menge.
2. Wenn $a, b \in H$, dann ist $ab \in H$,
3. Wenn $a \in H$, dann ist $a^{-1} \in H$.

Um 1. zu überprüfen kann auch $e \in H$ geprüft werden, denn:
$\Leftarrow$ Gilt $e \in H$ so folgt direkt H $\neq \emptyset$.
$\Rightarrow$ Es gelten Bedingungen 1,2 und 3.
Dann existiert nach 1. ein $a \in H$.

Untergruppen

Sei G eine Gruppe. Eine Teilmenge $H \subseteq G$ heisst **Untergruppe** falls:

1. H ist nicht die leere Menge.
2. Wenn $a, b \in H$, dann ist $ab \in H$,
3. Wenn $a \in H$, dann ist $a^{-1} \in H$.

Um 1. zu überprüfen kann auch $e \in H$ geprüft werden, denn:
$\Leftarrow$ Gilt $e \in H$ so folgt direkt H $\neq \emptyset$.
$\Rightarrow$ Es gelten Bedingungen 1,2 und 3.
Dann existiert nach 1. ein $a \in H$.
Da $a \in H$ existiert nach 3. ein $a^{-1} \in H$ sodass $a * a^{-1} = e$.
Mit 2. folgt $e \in H$.

Gruppenhomomorphismen

Seien G, und H Gruppen mit Verknüpfungen $\cdot$, und $\odot$, so heisst eine Abbildung

$$\varphi\colon G \to H,$$

Homomorphismus von Gruppen, wenn

$$\varphi(a \cdot b) = \varphi(a) \odot \varphi(b), \quad \forall a, b \in G.$$

Ein Homomorphismus, der auch bijektiv ist, heisst **Isomorphismus**.

Definition: Ringe

Eine Menge R mit zwei Verknüpfungen

$$+\colon R \times R \to R, (a, b) \mapsto a + b,$$
$$\cdot\colon R \times R \to R, (a, b) \mapsto a \cdot b$$

heisst **Ring** falls folgendes gilt:

1. R zusammen mit $+$ ist eine abelsche Gruppe.
2. Die Multiplikation ist assoziativ.
3. Es gelten die Distributivgesetze, d.h. für alle $a, b, c \in R$ gilt

$$a + (b + c) = (a + b) + c, \quad \text{und} \quad a \cdot (b \cdot c) = a \cdot (b \cdot c).$$

Restklassenring $\mathbb{Z}/n\mathbb{Z}$

- Definiert über Äquivalenzrelation: $a \sim b \Leftrightarrow a = bn$ für alle $a, b \in \mathbb{Z}$
- $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, ..., \overline{n-1}\}$
- $\bar{0}$ bezeichnet die Äquivalenzklasse von n, also alle $a \in \mathbb{Z}$ für die ein $b \in \mathbb{Z}$ existiert, sodass $a = bn$.

Beispielrechnung

Betrachte den Körper $\mathbb{F}_5 = \mathbb{Z}/5\mathbb{Z}$.
$\overline{4}^{2018}$

Definition: Körper

Eine Menge K mit zwei Verknüpfungen

$$+\colon K \times K \to K, (a,b) \mapsto a+b,$$
$$\cdot\colon K \times K \to K, (a,b) \mapsto a \cdot b$$

heisst **Körper** falls folgendes gilt:

1. K zusammen mit $+$ ist eine abelsche Gruppe
2. Bezeichnet $K^* = K \setminus \{0\}$, so gilt für $a, b \in K^*$ auch $a \cdot b \in K^*$, und K^* mit der so erhaltene Multiplikation ist eine abelsche Gruppe.
3. Es gelten die Distributivgesetze, d.h. für alle $a, b, c \in K$ gilt

$$a \cdot (b+c) = a \cdot b + a \cdot c, \quad \text{und} \quad (a+b) \cdot c = a \cdot c + b \cdot c.$$

Sind Restklassenringe auch Körper?

- für p Primzahl ist $\mathbb{Z}$ /p $\mathbb{Z}$ ein Körper
- Dies wir gezeigt über die Nullteilerfreiheit.
- Für n keine Primzahl ist $\mathbb{Z}$ /n $\mathbb{Z}$ **kein** Körper.
- Denn es existieren $a, b \neq 0 \in \mathbb{Z}$, sodass $ab = n = 0$

Beispielrechnung

Betrachte den Körper $\mathbb{F}_5 = \mathbb{Z}/5\mathbb{Z}$.
$\overline{4}^{2018}$:

$$\overline{4}^{2018} = \overline{4^2}^{1009} = \overline{16}^{1009} = \overline{1}^{1009} = \overline{1}.$$

Beispielrechnung

Betrachte den Körper $\mathbb{F}_5 = \mathbb{Z}/5\mathbb{Z}$.
$\frac{\overline{3}}{\overline{4}} + \frac{\overline{1}}{\overline{3}} =?$
Wir bearbeiten den ersten Term zuerst, und benutzen, dass $\overline{3} \cdot \overline{2} = \overline{6} = \overline{1}$, also $\frac{\overline{1}}{\overline{3}} = \overline{3}^{-1} = \overline{2}$

$$\frac{\overline{2}}{\overline{3}} = \overline{2} \cdot \overline{2} = \overline{4}.$$

Beispielrechnung

Betrachte den Körper $\mathbb{F}_5 = \mathbb{Z}/5\mathbb{Z}$.
$\frac{\overline{3}}{\overline{4}} + \frac{\overline{1}}{\overline{3}} =?$
Wir bearbeiten den ersten Term zuerst, und benutzen, dass $\overline{3} \cdot \overline{2} = \overline{6} = \overline{1}$, also $\frac{\overline{1}}{\overline{3}} = \overline{3}^{-1} = \overline{2}$

$$\frac{\overline{2}}{\overline{3}} = \overline{2} \cdot \overline{2} = \overline{4}.$$

Weiter ist $\overline{4} \cdot \overline{4} = \overline{1}$, also $\frac{\overline{1}}{\overline{4}} = \overline{4}^{-1} = \overline{4}$ und

$$\frac{\overline{1}}{\overline{4}} = \overline{1} \cdot \overline{4} = \overline{4}.$$

Beispielrechnung

Betrachte den Körper $\mathbb{F}_5 = \mathbb{Z}/5\mathbb{Z}$.

$\frac{\overline{3}}{\overline{4}} + \frac{\overline{1}}{\overline{3}} =?$

Wir bearbeiten den ersten Term zuerst, und benutzen, dass $\overline{3} \cdot \overline{2} = \overline{6} = \overline{1}$, also $\frac{\overline{1}}{\overline{3}} = \overline{3}^{-1} = \overline{2}$

$$\frac{\overline{2}}{\overline{3}} = \overline{2} \cdot \overline{2} = \overline{4}.$$

Weiter ist $\overline{4} \cdot \overline{4} = \overline{1}$, also $\frac{\overline{1}}{\overline{4}} = \overline{4}^{-1} = \overline{4}$ und

$$\frac{\overline{1}}{\overline{4}} = \overline{1} \cdot \overline{4} = \overline{4}.$$

Also

$$\frac{\overline{2}}{\overline{3}} + \frac{\overline{1}}{\overline{4}} = \overline{4} + \overline{4} = \overline{3}.$$

Übungsaufgabe 1

Sei $\mathbb{F}$ ein Körper. Zeigen oder widerlegen Sie die folgenden Aussagen.
Tipp: Für das Widerlegen genügt es, ein Gegenbeispiel zu finden.

- Für alle $a, b \in \mathbb{F}$ gilt $-(a - b) = b - a$.
- Für $a, b \in \mathbb{F}$ folgt aus $a + a + a = b + b + b$, dass $a = b$
- Für $a, b \in \mathbb{F}$ folgt aus $a + a + a + a = b + b + b + b$, dass $a = b$

Übungsaufgabe 2

Gibt es ein surjektiven Gruppenhomomorphismus von $\mathbb{Z}/6\mathbb{Z}$ nach $\mathbb{Z}/2\mathbb{Z}$?

Übungsaufgabe 3

Gibt es ein surjektiven Gruppenhomomorphismus von $\mathbb{Z}/5\mathbb{Z}$ nach $\mathbb{Z}/2\mathbb{Z}$?

Übungsaufgabe 4

Seien $G_1, G_2, ..., G_n$ Gruppen, mit neutralen Elementen $e_i \in G_i$ für $i \in \{1, \ldots, n\}$, und betrachte das kartesische Produkt
$G = G_1 \times G_2 \times \cdots \times G_n$.
Definiere die Verknüpfung in G als
$(g_1, g_2, \ldots, g_n) * (h_1, h_2, \ldots, h_n) = (g_1 h_1, g_2 h_2, \ldots, g_n h_n)$.
Zeige: Die Menge G mit Verknüpfung $*$ ist eine Gruppe.