AGLA – Woche 3

Max Offermann, Tom Witjes und Jonas Hahn

2025-04-09

A1	A2	A3	A4		$\sum$

Contents

Problem 1: Ringe mit Addition und Multiplikation

a) Zeigen Sie, dass

$$(\mathbb{Z}/5\mathbb{Z})^* := \{1+5\mathbb{Z}, 2+5\mathbb{Z}, 3+5\mathbb{Z}, 4+5\mathbb{Z}\} \subset \mathbb{Z}/5\mathbb{Z} \tag{1}$$

$$(\mathbb{Z}/9\mathbb{Z})^* := \{1+9\mathbb{Z}, 2+9\mathbb{Z}, 4+9\mathbb{Z}, 5+9\mathbb{Z}, 7+9\mathbb{Z}, 8+9\mathbb{Z}\} \subset \mathbb{Z}/9\mathbb{Z} \tag{2}$$

jeweils eine Gruppe bezueglich Multiplikation sind.

Geforderte Eigenschaften an eine Gruppe:

- Abgeschlossenheit: Das Produkt zweier Elemente muss wieder in der Gruppe sein.
- Inverses Element: Jedes Element muss ein multiplikatives Inverses in der Gruppe haben.
- Assoziativität: Diese Eigenschaft wird von den ganzen Zahlen vererbt. ✓
- Neutrales Element: Es muss ein neutrales Element in der Gruppe geben. Dieses ist hier die 1. ✓

Für $(\mathbb{Z}/5\mathbb{Z})^*$ gibt es durch Modulo-Rechnen folgende Elemente in der Gruppe $E = \{1, 2, 3, 4\}$.

Das Produkt zweier Elemente aus E ergibt wieder ein Element in dieser Menge:

$$1 \cdot 1 = 1, 1 \cdot 2 = 2, 1 \cdot 3 = 3, 1 \cdot 4 = 4 \tag{3}$$

$$2 \cdot 2 = 4, 2 \cdot 3 = 1, 2 \cdot 4 = 3 \tag{4}$$

$$3 \cdot 3 = 4, 3 \cdot 4 = 2 \tag{5}$$

$$4 \cdot 4 = 1 \tag{6}$$

Jedes Element hat ein Inverses:

$$1^{-1} = 1, 2^{-1} = 3, 3^{-1} = 2, 4^{-1} = 4 \tag{7}$$

Für $(\mathbb{Z}/9\mathbb{Z})^*$ gibt es durch Modulo-Rechnen folgende Elemente in der Gruppe $E = \{1, 2, 4, 5, 7, 8\}$.

Das Produkt zweier Elemente aus E ergibt wieder ein Element in dieser Menge:

$$1 \cdot 1 = 1, 1 \cdot 2 = 2, 1 \cdot 4 = 4, 1 \cdot 5 = 5, 1 \cdot 7 = 7, 1 \cdot 8 = 8 \tag{8}$$

$$2 \cdot 2 = 4, 2 \cdot 4 = 8, 2 \cdot 5 = 1, 2 \cdot 7 = 5, 2 \cdot 8 = 7 \tag{9}$$

$$4 \cdot 4 = 7, 4 \cdot 5 = 2, 4 \cdot 7 = 1, 4 \cdot 8 = 5 \tag{10}$$

$$5 \cdot 5 = 7, 5 \cdot 7 = 8, 5 \cdot 8 = 4 \tag{11}$$

$$7 \cdot 7 = 4, 7 \cdot 8 = 2 \tag{12}$$

$$8 \cdot 8 = 1 \tag{13}$$

Jedes Element hat ein Inverses:

$$1^{-1} = 1, 2^{-1} = 5, 4^{-1} = 7, 5^{-1} = 2, 7^{-1} = 4, 8^{-1} = 8 \tag{14}$$

Damit ist alles gezeigt. ■

b) Finden Sie ein Element $x \in (\mathbb{Z}/9\mathbb{Z})^*$, sodass $\langle\{x\}\rangle = (\mathbb{Z}/9\mathbb{Z})^*$ gilt.

Nach Aufgabe 1a ist hat die Gruppe $(\mathbb{Z}/9\mathbb{Z})^*$ folgende Elemente $1, 2, 4, 5, 7, 8$. Es gilt $|(\mathbb{Z}/9\mathbb{Z})^*| = 6$.

Durch Testen jedes Elements finden wir, dass $x = 2$ die gesamte Gruppe erzeugt, da:

$$2^1 = 2, \quad 2^2 = 4, \quad 2^3 = 8, \quad 2^4 = 7, \quad 2^5 = 5, \quad 2^6 = 1. \tag{15}$$

Somit ist $x = 2$ ein Generator von $(\mathbb{Z}/9\mathbb{Z})^*$, und wir haben $\langle 2\rangle = (\mathbb{Z}/9\mathbb{Z})^*$.

c) Geben Sie einen Isomorphismus zwischen $(\mathbb{Z}/9\mathbb{Z}, \cdot)$ und $(\mathbb{Z}/6\mathbb{Z}, +)$ an.

Ein Isomorphismus zwischen den Gruppen $(\mathbb{Z}/9\mathbb{Z}, \cdot)$ und $(\mathbb{Z}/6\mathbb{Z}, +)$ kann durch die Funktion

$$\varphi : (\mathbb{Z}/9\mathbb{Z})^* \to \mathbb{Z}/6\mathbb{Z} \tag{16}$$

gegeben werden, wobei $\varphi(x)$ die Ordnung von x in $(\mathbb{Z}/9\mathbb{Z})^*$ modulo 6 ist.

Wählen wir nach Aufgabe 1b $x = 2$ als Generator von $(\mathbb{Z}/9\mathbb{Z})^*$, so laesst sich φ definieren durch

$$\varphi\left(2^k\right) = k \bmod 6. \tag{17}$$

Diese Zuordnung ist ein Isomorphismus, da sie bijektiv ist und die Gruppenoperationen respektiert:

$$\varphi\left(2^k \cdot 2^m\right) = \varphi\left(2^{k+m}\right) = (k+m) \bmod 6 = \varphi\left(2^k\right) + \varphi(2^m). \tag{18}$$

Ist $(\mathbb{Z}/5\mathbb{Z})^*$ auch zu einer Gruppe der Form $\mathbb{Z}/n\mathbb{Z}$ für ein $n \in N$ isomorph? Falls ja, geben Sie einen Isomorphismus an.

Die Gruppe $(\mathbb{Z}/5\mathbb{Z})^*$ ist also isomorph zu $\mathbb{Z}/4\mathbb{Z}$, da beide Gruppen die gleiche Ordnung haben und zyklisch sind.

Ein Isomorphismus zwischen $(\mathbb{Z}/5\mathbb{Z})^*$ und $\mathbb{Z}/4\mathbb{Z}$ ist durch die Abbildung

$$\varphi : (\mathbb{Z}/5\mathbb{Z})^* \to \mathbb{Z}/4\mathbb{Z}, \quad \varphi(1) = 0, \quad \varphi(2) = 1, \quad \varphi(3) = 3, \quad \varphi(4) = 2 \tag{19}$$

gegeben.

Problem 2: Homomorphismen

Seien G und H Gruppen. Angenommen G ist endlich und ihre Ordnung eine Primzahl p. Zeigen Sie:

a) Jeder Homomorphismus $\varphi : G \to H$ ist entweder trivial oder injektiv.

Sei $\phi : G \to H$ ein Homomorphismus. Da G endlich und $|G| = p$ eine Primzahl ist, gilt nach Lagrange für jede Untergruppe von G entweder $|H| = 1$ oder $|H| = p$.

Fuer den Kern gilt:

$$\varphi(e_G) = e_H \Longrightarrow \ker(\varphi) \neq \emptyset \tag{20}$$

Sei $a, b \in \ker(\varphi)$. Dann:

$$\varphi(a) = e_H \text{ und } \varphi(b) = e_H \tag{21}$$

Da φ ein Homomorphismus ist, folgt:

$$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b) = e_H \cdot e_H = e_H \tag{22}$$

Also ist $a \cdot b \in \ker(\varphi)$

Sei $a \in \ker(\varphi)$. Dann:

$$\varphi(a) = e_H \tag{23}$$

Da $e_H = e_H^{-1}$ folgt:

$$\varphi(a^{-1}) = \varphi(a)^{-1}) = e_H^{-1} = e_H \tag{24}$$

Da alle Eigenschaften fuer eine Untergruppe, namentlich nicht Leerheit, Abgeschlossenheit und die Existenz eines Inversen gegeben sind, ist das Kernbild des Homomorphismus, $\ker(\varphi)$, eine Untergruppe von G.

Falls $|\ker(\varphi)| = G$, ist φ trivial. Andernfalls ist $|\ker(\varphi)| = 1$, was bedeutet, dass $\ker(\varphi) = \{e\}$, das neutrale Element.

Angenommen $\varphi(a) = \varphi(b)$ fuer beliebige $a, b \in G$, dann:

Wir betrachten das Element $a \cdot b^{-1} \in G$ fuer beliebige $a, b \in G$.

$$\varphi(a \cdot b^{-1}) = \varphi(a) \cdot \varphi(b^{-1}) \tag{25}$$

Da $\varphi(a) = \varphi(b)$ und $\varphi(b^{-1}) = \varphi(b)^{-1}$, folgt:

$$\varphi(a \cdot b^{-1}) = \varphi(a) \cdot \varphi(a)^{-1} = e_H \tag{26}$$

Da $a \cdot b^{-1}$ nun im Kern ist, aber $\ker(\varphi) = \{e\}$, folgt:

$$a \cdot b^{-1} = e \Longrightarrow a = b \tag{27}$$

Da $\varphi(a) = \varphi(b) \Longrightarrow a = b$ ist φ injektiv.

b) Jeder Homomorphismus $\varphi : H \to G$ ist entweder trivial oder surjektiv.

Sei $\varphi : H \to G$ ein Homomorphismus. Da G die Ordnung p hat, ist jede echte Untergruppe von G trivial. Das Bild $\mathrm{im}(\varphi)$ ist nach dem selben Argument wie in 2a eine Untergruppe von G, daher gilt $|\mathrm{im}(\varphi)| = 1$ oder $|\mathrm{im}(\varphi)| = p$.

Falls $|\mathrm{im}(\varphi)| = 1$, ist φ trivial. Sonst ist $|\mathrm{im}(\varphi)| = p$, was bedeutet, dass $\mathrm{im}(\varphi) = G$.

Fuer surjektivitaet gilt es jetzt zu zeigen, dass

$$\forall y \in G : \exists x \in G : \phi(x) = y. \tag{28}$$

Dabei gilt:

$$\mathrm{im}(\varphi) = G \Longrightarrow \forall y \in G : y \in \mathrm{im}(\varphi) \tag{29}$$

$$y \in \operatorname{im}(\varphi) \Longrightarrow \exists x \in G : \varphi(x) = y \tag{30}$$

also ist φ surjektiv.

Problem 3: Vektorraeume I

Wir betrachten den Vekorraum $V = \mathbb{R}^4$ mit den folgenden Unterraeumen:

$$U_1 = \langle\{(0,1,0,2),(1,0,1,0),(-1,0,1,0)\}\rangle, U_2 = \langle\{(1,0,3,0),(0,1,0,0),(1,3,3,3)\}\rangle \tag{31}$$

a) Bestimmen Sie $U_1 \cap U_2$.

   Loesung in Papierform.

b) Ist $U_1 \cup U_2 = V$?

   Loesung in Papierform.

Problem 4: Vektorraeume II

a) Zeigen Sie, dass die Menge

$$V = \{(x_1, x_2, x_3) \in \mathbb{Q}^3 : 7x_1 + 2x_2 - 3x_3 = 0\} \tag{32}$$

   ein Untervektorraum von $\mathbb{Q}^3$ ist.

   Sei $V = \{(x_1, x_2, x_3) \in \mathbb{Q}^3 : 7x_1 + 2x_2 - 3x_3 = 0\}$. Um zu zeigen, dass V ein Untervektorraum ist, prüfen wir die drei Bedingungen:

   V ist nicht leer: Es gilt $\begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \in V \Longrightarrow V \neq \emptyset$.

   Abgeschlossenheit unter Addition: Fuer $\vec{v} = (x_1, x_2, x_3) \in V$ und $\vec{w} = (y_1, y_2, y_3) \in V$ gilt:

$$7(x_1 + y_1) + 2(x_2 + y_2) - 3(x_3 + y_3) = (7x_1 + 2x_2 - 3x_3) + (7y_1 + 2y_2 - 3y_3) = 0, \tag{33}$$

   also ist $\vec{v} + \vec{w} \in V$.

   Abgeschlossenheit unter skalarer Multiplikation: Fuer $\vec{v} = (x_1, x_2, x_3) \in V$ und $\lambda \in \mathbb{Q}$ gilt:

$$7(\lambda x_1) + 2(\lambda x_2) - 3(\lambda x_3) = \lambda(7x_1 + 2x_2 - 3x_3) = 0, \tag{34}$$

   also ist $\lambda \vec{v} \in V$.

   Restliche Eigenschaften, wie die Assoziativitaet oder Kommutativitaet werden vom Koerper der rationalen Zahlen $\mathbb{Q}$ vererbt.

   Da sonst alle drei Bedingungen erfüllt sind, ist V ein Untervektorraum von $\mathbb{Q}^3$.

b) Zeigen Sie, dass $V = \langle\{(2,-7,0),(0,3,2),(1,1,3)\}\rangle$ ist.

   Loesung in Papierform.

c) Ist die Menge

$$W = \{(x_1, x_2, x_3) \in \mathbb{Q}^3 : 7x_1 + 2x_2 - 3x_3 = 1\} \tag{35}$$

   ein Untervektorraum von $\mathbb{Q}^3$?

   Zuerst pruefe ich ob das neutrale Element in W enthalten ist durch einsetzen von $\begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$ in das Aussonderungsaxiom der Menge:

$$7 \cdot 0 + 2 \cdot 0 - 3 \cdot 0 = 0 \neq 1 \tag{36}$$

So kann W kein Untervektorraum von $\mathbb{Q}^3$ sein, da diese Menge kein neutrales Element enthaelt.