N. Krauß, M. Künzer

Algebra für Lehramt, SoSe 21

Lösung 5

Aufgabe 17

(1) Sei G eine Gruppe. Sei $U \leqslant G$. Zu zeigen ist folgendes. Zum einen ist $({}_U\!\sim)$ eine Äquivalenzrelation. Zum anderen ist Ux die Äquivalenzklasse von $x \in G$. Vgl. Definition 96.(1).

(2) Gilt für $x, y \in G$ mit $x \,{}_U\!\sim y$ auch $zx \,{}_U\!\sim zy$ für $z \in G$?

Lösung zu Aufgabe 17:

(1) Wir erinnern: Für $x, y \in G$ ist $x \,{}_U\!\sim y$ genau dann, wenn $xy^{-1} \in U$ ist.

Die Relation ist reflexiv, da für $x \in G$ gilt: $xx^{-1} = 1 \in U$, also $x \,{}_U\!\sim x$.

Sie ist symmetrisch, denn gilt $x \,{}_U\!\sim y$ für $x, y \in G$, so ist $xy^{-1} \in U$ und folglich ist auch, da U eine Untergruppe ist, $yx^{-1} = (xy^{-1})^{-1} \in U$, d.h. $y \,{}_U\!\sim x$.

Die Relation ist transitiv, denn gilt $x \,{}_U\!\sim y$ und $y \,{}_U\!\sim z$ für $x, y, z \in U$, so sind xy^{-1}, $yz^{-1} \in U$ und folglich, da $U \leqslant G$, auch $xy^{-1} \cdot yz^{-1} = xz^{-1} \in U$, d.h. $x \,{}_U\!\sim z$.

Damit ist $({}_U\!\sim)$ eine Äquivalenzrelation.

Sei $x \in G$. Dann ist $x \,{}_U\!\sim y \Leftrightarrow xy^{-1} \in U$ für $y \in G$. Das ist genau dann der Fall, wenn es $u \in U$ gibt mit $xy^{-1} = u$, d.h. $y = u^{-1}x$. Also genau dann, wenn $y \in Ux$ liegt. Somit ist Ux die Äquivalenzklasse von x in G.

(2) Nein. Sei $G := \mathrm{S}_3$ und $U := \langle(1,2)\rangle$. Dann ist für $x = (1,2)$, $y = \mathrm{id}$ und $z = (1,3)$ zwar $x \,{}_U\!\sim y$, da $x \circ y^{-1} = (1,2) \circ \mathrm{id}^{-1} = (1,2) \in U$, aber $zx \,{}_U\!\not\sim zy$, da

$$zx(zy)^{-1} = (1,3) \circ (1,2) \circ \mathrm{id}^{-1} \circ (1,3)^{-1} = (2,3) \notin U \ .$$

Aufgabe 18 Seien G und H Gruppen. Sei $\varphi : G \to H$ ein Gruppenmorphismus.
Man zeige oder widerlege.

(1) Das Urbild einer Untergruppe von H unter φ ist eine Untergruppe von G.

(2) Das Urbild eines Normalteilers von H unter φ ist ein Normalteiler von G.

(3) Das Bild einer Untergruppe von G unter φ ist eine Untergruppe von H.

(4) Das Bild eines Normalteilers von G unter φ ist ein Normalteiler von H.

Lösung zu Aufgabe 18:

(1) Die Aussage ist wahr. Sei $V \leqslant H$ eine Untergruppe. Sei

$$U := \varphi^{-1}(V) = \{g \in G : \varphi(g) \in V\} \subseteq G$$

ihr Urbild. Es ist $1_G \in U$, da $\varphi(1_G) = 1_H \in V$. Für $g, \tilde{g} \in U$ ist $\varphi(g \cdot \tilde{g}^{-1}) = \varphi(g) \cdot \varphi(\tilde{g}^{-1}) = \varphi(g) \cdot \varphi(\tilde{g})^{-1} \in V$ und also $g \cdot \tilde{g}^{-1} \in U$.

Somit ist $U \leqslant G$.

(2) Die Aussage ist wahr. Sei $V \trianglelefteq H$ ein Normalteiler. Sei

$$U := \varphi^{-1}(V) = \{g \in G : \varphi(g) \in V\} \subseteq G$$

sein Urbild. Nach (1) ist $U \leqslant G$ eine Untergruppe. Zu zeigen ist für $x \in G$ und $u \in U$, dass ${}^x u \in U$ liegt.

In der Tat ist

$$\varphi({}^x u) = \varphi(xux^{-1}) = \varphi(x)\varphi(u)\varphi(x^{-1}) = \varphi(x)\varphi(u)\varphi(x)^{-1} \ .$$

Da $\varphi(u) \in V$ ist, und da V ein Normalteiler von H ist, ist $\varphi(x)\varphi(u)\varphi(x)^{-1} \in V$. Also ist ${}^x u \in U$. Nach Bemerkung 107 ist U ein Normalteiler von G.

(3) Die Aussage ist wahr. Sei $U \leqslant G$ eine Untergruppe und $\varphi(U) \subseteq H$ ihr Bild. Es ist $1_H \in \varphi(U)$, da $\varphi(1_G) = 1_H$. Für $h, \tilde{h} \in \varphi(U)$ gibt es $u, \tilde{u} \in U$ mit $h = \varphi(u)$ und $\tilde{h} = \varphi(\tilde{u})$. Dann ist auch $h\tilde{h}^{-1} = \varphi(u)\varphi(\tilde{u})^{-1} = \varphi(u\tilde{u}^{-1}) \in \varphi(U)$.

Somit ist $\varphi(U) \leqslant H$.

(4) Die Aussage ist falsch. Sei $G = \langle(1,2)\rangle \leqslant \mathrm{S}_3$ und $H := \mathrm{S}_3$. Sei $\varphi : G \to H : g \mapsto g$ die Einbettung. Es ist $G \trianglelefteq G$, aber $\varphi(G) = \langle(1,2)\rangle \ntrianglelefteq H$, denn für $(1,3) \in H$ ist

$$(1,3) \circ (1,2) \circ (1,3) = (2,3) \notin \varphi(G) \ .$$

Aufgabe 19 Sei die abelsche Untergruppe

$$V := \langle(1,2)(3,4), (1,3)(2,4)\rangle = \{\mathrm{id}, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\} \leqslant \mathrm{A}_4$$

gegeben.

(1) Man bestimme die Linksnebenklassen modulo V in A_4 und die Rechtsnebenklassen modulo V in A_4. Vgl. Definition 96.(1),(2).

(2) Sei $U := \langle(1,2)(3,4)\rangle \leqslant V$. Gilt $U \trianglelefteq V \trianglelefteq \mathrm{A}_4$? Ist $U \trianglelefteq \mathrm{A}_4$?

(3) Bestimmen Sie die Ordnung der Faktorgruppe A_4/V. Ist diese Faktorgruppe zyklisch?

Lösung zu Aufgabe 19:

(1) Es sind

$$\begin{aligned} \mathrm{id}\, V &= \{\mathrm{id}, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\} \ , \\ (1,2,3)V &= \{(1,2,3), (1,3,4), (2,4,3), (1,4,2)\} \text{ und} \\ (1,2,4)V &= \{(1,2,4), (1,4,3), (1,3,2), (2,3,4)\} \end{aligned}$$

die Linksnebenklassen modulo V in A_4.

Es sind

$$\begin{aligned} V\,\mathrm{id} &= \{\mathrm{id}, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\} \ , \\ V(1,2,3) &= \{(1,2,3), (2,4,3), (1,4,2), (1,3,4)\} \text{ und} \\ V(1,2,4) &= \{(1,2,4), (2,3,4), (1,4,3), (1,3,2)\} \end{aligned}$$

die Rechtsnebenklassen modulo V in A_4.

(2) Da für $x \in \mathrm{A}_4$ dank (1) gilt, dass $xV = Vx$ ist, ist V ein Normalteiler von A_4.

Die Gruppe V ist abelsch. Also ist jede Untergruppe von V ein Normalteiler. Somit ist $U \trianglelefteqslant V$.

Aber $U \ntrianglelefteq \mathrm{A}_4$, da z.B. für $(1,3,2) \in \mathrm{A}_4$ gilt, dass

$$(1,3,2) \circ (1,2)(3,4) \circ (1,2,3) = (1,3)(2,4) \notin U \ .$$

(3) Es ist nach dem Satz von Lagrange (Satz 97)

$$|\mathrm{A}_4/V| = \frac{|\mathrm{A}_4|}{|V|} = \frac{12}{4} = 3 \ .$$

Es ist $\mathrm{A}_4/V = \langle (1,2,3)V \rangle$, da $(1,2,3)V \cdot (1,2,3)V = (1,3,2)V = (1,2,4)V$. Insbesondere ist A_4/V zyklisch.

Aufgabe 20

(1) Man bestimme gewisse Elemente $x, y \in \mathrm{U}(\mathbb{Z}/(12))$ so, dass $\mathrm{U}(\mathbb{Z}/(12)) = \langle x, y \rangle$ ist.

(2) Man bestimme alle Elemente $x \in \mathrm{U}(\mathbb{F}_{11})$, für welche $\mathrm{U}(\mathbb{F}_{11}) = \langle x \rangle$ ist.

(3) Man finde einen surjektiven Gruppenmorphismus $\varphi : \mathrm{U}(\mathbb{Z}/(21)) \to \mathrm{U}(\mathbb{Z}/(7))$ und bestimme seinen Kern.

Lösung zu Aufgabe 20:

Vorbemerkung

Sei $n \in \mathbb{Z}_{\geqslant 2}$. Für $k \in [1, n]$ ist $k + (n) \in \mathbb{Z}/(n)$ genau dann invertierbar, wenn $\mathrm{ggT}(k, n) = 1$ ist.

Sei zum einen $k+(n) \in \mathbb{Z}/(n)$ invertierbar. Dann gibt es $\tilde{k}+(n) \in \mathbb{Z}/(n)$ mit $k \cdot \tilde{k}+(n) = 1+(n)$. Also teilt n die Zahl $k \cdot \tilde{k} - 1$. Nun gibt es $t \in \mathbb{Z}$ mit $n \cdot t = k \cdot \tilde{k} - 1$ und also ist $k \cdot \tilde{k} - n \cdot t = 1$. Somit ist $(n, k) = (1)$ als Ideale von $\mathbb{Z}$, was $\mathrm{ggT}(k, n) = 1$ bedeutet.

Sei zum anderen $\mathrm{ggT}(k, n) = 1$. Dann ist $(k, n) = (1)$ als Ideale von $\mathbb{Z}$. Also gibt es $\tilde{k}, t \in \mathbb{Z}$ mit $1 = k \cdot \tilde{k} - n \cdot t$. Also ist $k \cdot \tilde{k} - 1$ durch n teilbar und also $k \cdot \tilde{k} - 1 + (n) = 0 + (n)$ dh. $k \cdot \tilde{k} + (n) = 1 + (n)$. Also ist $k + (n) \in \mathbb{Z}/(n)$ invertierbar mit Inversem $\tilde{k} + (n) \in \mathbb{Z}/(n)$. Das zeigt die *Vorbemerkung*.

(1) Es ist $\mathbb{Z}/(12) = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$ und unter Verwendung der Vorbemerkung, $\mathrm{U}(\mathbb{Z}/(12)) = \{1, 5, 7, 11\}$.

Wegen $5 \cdot 7 = 11$ ist $\mathrm{U}(\mathbb{Z}/(12)) = \langle 5, 7 \rangle$.

Es ist auch $\mathrm{U}(\mathbb{Z}/(12) = \langle 5, 11 \rangle = \langle 7, 11 \rangle$.

(2) Es ist $\mathbb{F}_{11} = \mathbb{Z}/(11) = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ und $\mathrm{U}(\mathbb{F}_{11}) = \mathbb{F}_{11}^{\times}$. Damit für $x \in \mathrm{U}(\mathbb{F}_{11})$ gilt, dass $\langle x \rangle = \mathrm{U}(\mathbb{F}_{11})$ ist, muss x Ordnung 10 haben. Man prüft:

Ordnung 1:	1
Ordnung 2:	10
Ordnung 5:	9, 3, 4, 5
Ordnung 10:	2, 6, 7, 8

(3) Wir haben den Restklassen-Ringmorphismus: $\rho : \mathbb{Z} \to \mathbb{Z}/(7) :\ x \mapsto x+(7)$. Da $\rho((21)) = 0$ ist, gibt es den Ringmorphismus $\psi : \mathbb{Z}/(21) \to \mathbb{Z}/(7) :\ x+(21) \mapsto x+(7)$, vgl. Lemma 30.

Nach Beispiel 110 ist die Einschränkung

$$\varphi := \psi^{\mathrm{U}} : \mathrm{U}(\mathbb{Z}/(21)) \to \mathrm{U}(\mathbb{Z}/(7)) :\ x + (21) \mapsto x + (7)$$

ein Gruppenmorphismus.

Es ist, in Kurzschreibweise,

$$\mathrm{U}(\mathbb{Z}/(21)) = \{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\} \subseteq \mathbb{Z}/(21)$$

und

$$\mathrm{U}(\mathbb{Z}/(7)) = \{1, 2, 3, 4, 5, 6\} \subseteq \mathbb{Z}/(7).$$

Da $\varphi(10) = 3$ ist und $\mathrm{U}(\mathbb{Z}/(7)) = \langle 3 \rangle$ ist, ist φ surjektiv.

Es ist $\mathrm{Kern}(\varphi) = \{x \in \mathrm{U}(\mathbb{Z}/(21)) : \varphi(x) = 1\} = \{1, 8\} \trianglelefteq \mathrm{U}(\mathbb{Z}/(21)) \subseteq \mathbb{Z}/(21)$.