C. Dietzel, M. Künzer

Algebra für Lehramt, SoSe 20

Lösung 4

Aufgabe 13

(1) Man zeige $\mathrm{S}_4 = \langle (1,2), (1,2,3,4) \rangle$.

(2) Man zeige $\mathrm{A}_4 = \langle (1,2,3), (1,2)(3,4) \rangle$.

Lösung zu Aufgabe 13:
Es gibt viele mögliche Lösungswege. Man kann z.B. so lange Produkte der Erzeuger auf der rechten Seite ausrechnen, bis sichergestellt ist, daß die rechte Seite keine echte Untergruppe der linken Seite mehr sein kann.
Wir werden versuchen, mit Argumenten wie z.B. Lagrange uns Rechnungen möglichst zu sparen.

(1) Schreibe $U = \langle (1,2), (1,2,3,4) \rangle$.

Wir zeigen zunächst, dass $H := U \cap \mathrm{A}_4 = \mathrm{A}_4$ ist:

Wir haben $(1,2) \circ (1,2,3,4) = (2,3,4) \in U$. Außerdem ist $(2,3,4) \in \mathrm{A}_4$. Also ist $(2,3,4) \in H$.

$(2,3,4)$ besitzt die Ordnung 3, folglich ist $|\langle (2,3,4) \rangle| = 3$. Wegen $\langle (2,3,4) \rangle \leqslant H$ gilt nach Lemma 87 auch $3 \,|\, |H|$.

Weiterhin ist $(1,2,3,4)^2 = (1,3)(2,4) \in U$, demnach ist auch ${}^{(1,2)}((1,3)(2,4)) = (1,4)(2,3) \in U$ (siehe Bemerkung 103 zur Berechnung der Konjugation in der S_n). Damit ist auch $(1,3)(2,4) \circ (1,4)(2,3) = (1,2)(3,4) \in U$. Damit ist $V = \{\mathrm{id}, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$ eine Untergruppe von U.

Weiterhin ist $V \leqslant \mathrm{A}_4$, also ist $V \leqslant H$. Es folgt $4 \,|\, |H|$.

Demzufolge gilt $12 \,|\, |H|$. Da H in A_4 liegt und $|\mathrm{A}_4| = 12$ ist, muss $H = \mathrm{A}_4$ sein.

Damit ist $\mathrm{A}_4 \leqslant U \leqslant \mathrm{S}_4$. Nach Lemma 87 gilt also $12 \,|\, |U|$ und $|U| \,|\, 24$, d.h. $|U| \in \{12, 24\}$.

Wäre $|U| = 12$, so wäre $U = \mathrm{A}_4$; dies ist aber nicht möglich, da $(1,2) \in U \setminus \mathrm{A}_4$. Somit kommt nur $|U| = 24$ und damit $U = \mathrm{S}_4$ in Frage.

> Man kann allgemeiner zeigen, dass für alle $n \geq 2$ gilt, dass $\mathrm{S}_n = \langle (1,2), (1,2,\ldots,n) \rangle$ ist.
> Hierfür zeigt man zunächst, dass $\mathrm{S}_n = \langle (1,2), (2,3), \ldots, (n-1,n) \rangle$ ist. Da die Untergruppe $U = \langle (1,2), (1,2,\ldots,n) \rangle$ die Elemente ${}^{(1,2,\ldots,n)^k}(1,2) = (k+1, k+2)$ $(0 \leq k \leq n-2)$ enthält, muss demnach $U = \mathrm{S}_n$ sein.

(2) Schreibe $U = \langle (1,2,3), (1,2)(3,4) \rangle$. Wir haben ${}^{(1,2,3)}((1,2)(3,4)) = (2,3)(1,4) \in U$ und damit auch ${}^{(1,2,3)}((2,3)(1,4)) = (3,1)(2,4) \in U$.

Damit enthält U die Untergruppe $V = \{\mathrm{id}, (1,2)(3,4), (2,3)(1,4), (1,3)(2,4)\}$ aus Beispiel 104(2). Damit folgt $4 \,|\, |U|$.

$(1,2,3)$ besitzt die Ordnung 3, folglich ist $|\langle (1,2,3) \rangle| = 3$. Wegen $\langle (1,2,3) \rangle \, U$ folgt $3 \,|\, |U|$.

Folglich gilt $12 \,|\, |U|$. Wegen $|\mathrm{A}_4| = 12$ ist $U = \mathrm{A}_4$.

Aufgabe 14

(1) Sei G eine Gruppe. Sei $U \leqslant G$. Zu zeigen ist folgendes.

Es ist $(\sim_U)$ eine Äquivalenzrelation. Für $x \in G$ ist xU die Äquivalenzklasse von $x \in G$.

Vgl. Definition 86.(2).

(2) Sei G eine Gruppe. Sei $U \trianglelefteq V \trianglelefteq G$. Ist dann $U \trianglelefteq G$?

(3) Seien R und S Ringe. Sei $\varphi : R \to S$ ein Ringmorphismus.

Ist $\varphi(\mathrm{U}(R)) \subseteq \mathrm{U}(S)$?

Ist die Einschränkung $\varphi|_{\mathrm{U}(R)}^{\mathrm{U}(S)} : \mathrm{U}(R) \to \mathrm{U}(S) : x \mapsto \varphi(x)$ ein Gruppenmorphismus?

Lösung zu Aufgabe 14:

(1) Wir prüfen für die Relation $x \sim_U y :\Leftrightarrow x^{-1}y \in U$ die Axiome einer Äquivalenzrelation nach:

Reflexivität: Für alle $x \in G$ gilt $x^{-1}x = 1 \in U$, also $x \sim_U x$.

Symmetrie: Gilt $x \sim_U y$ für $x, y \in G$, so ist $x^{-1}y \in U$, folglich ist auch $y^{-1}x = (x^{-1}y)^{-1} = 1 \cdot (x^{-1}y)^{-1} \in U$, also folgt $y \sim_U x$.

Transitivität: Gilt sowohl $x \sim_U y$ als auch $y \sim_U z$ für $x, y, z \in G$, so sind $x^{-1}y, y^{-1}z \in U$. Da U unter der Gruppenverknüpfung abgeschlossen ist, ist auch $x^{-1}z = (x^{-1}y)(y^{-1}z) \in U$.

Damit ist $(\sim_U)$ eine Äquivalenzrelation auf G.

Ist $x \in G$, so gilt für alle $y \in G$

$$x \sim_U y \Leftrightarrow x^{-1}y \in U \Leftrightarrow \exists u \in U : x^{-1}y = u \Leftrightarrow \exists u \in U : y = xu \Leftrightarrow y \in xU.$$

(2) Wir bedienen uns des Normalteilers $V = \{\mathrm{id}, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\} \trianglelefteq \mathrm{S}_4$ aus Beispiel 104(2). Für die Untergruppe $U = \{\mathrm{id}, (1,2)(3,4)\}$ gilt $U \trianglelefteq V$ (hier kann man damit argumentieren, dass V abelsch ist oder wegen $[V : U] = 2$ Bemerkung 94 verwenden). Wir haben also $U \trianglelefteq V \trianglelefteq \mathrm{S}_4$.

U ist aber nicht normal in S_4, denn es ist $(1,2)(3,4) \in U$, aber ${}^{(2,3)}((1,2)(3,4)) = (1,3)(2,4) \notin U$, damit ist U nicht abgeschlossen unter Konjugation, nach Bemerkung 102 also auch kein Normalteiler.

(3) In der Tat ist $\varphi(\mathrm{U}(R)) \subseteq \mathrm{U}(S)$. Ist nämlich $x \in \mathrm{U}(R)$, so gibt es nach Voraussetzung ein $y \in R$ mit $xy = yx = 1_R$. Damit ist

$$1_S = \varphi(1_R) = \varphi(xy) = \varphi(x)\varphi(y),$$

und

$$1_S = \varphi(1_R) = \varphi(yx) = \varphi(y)\varphi(x),$$

folglich ist $\varphi(x) \in \mathrm{U}(S)$.

Die Einschränkung $\varphi|_{\mathrm{U}(R)}^{\mathrm{U}(S)}$ ist ein Gruppenhomomorphismus, denn es gilt $\varphi(1_R) = 1_S$ und weiterhin auch $\varphi(xy) = \varphi(x)\varphi(y)$ für alle $x, y \in \mathrm{U}(R)$ – letzteres gilt nach Definition eines Ringmorphismus (Definition 12) nämlich für alle $x, y \in R$.

Aufgabe 15

(1) Ist $\mathrm{U}(\mathbb{Z}/(15))$ zyklisch?

(2) Ist $\mathrm{U}(\mathbb{Z}/(16))$ zyklisch?

(3) Sei $p \in \mathbb{Z}_{\geqslant 5}$ prim. Ist die Ordnung von 3 in $\mathbb{F}_p^\times = \mathrm{U}(\mathbb{F}_p)$ gleich $p-1$?

(4) Gibt es ein $p \in \mathbb{Z}_{\geqslant 7}$ derart, daß 3 in $\mathbb{F}_p^\times$ die Ordnung 4 hat?

Lösung zu Aufgabe 15:

(1) Es ist $\mathrm{U}(\mathbb{Z}/(15)) = \{1, 2, 4, 7, 8, 11, 13, 14\}$. Wenn $\mathrm{U}(\mathbb{Z}/(15))$ zyklisch ist, muss es ein Element der Ordnung 8 geben. Man prüft allerdings leicht nach, dass jedes Element Ordnung $1, 2$ oder 4 besitzt:

Ordnung 1: 1.

Ordnung 2: $4^2 = 1$, $11^2 = (-4)^2 = 1$, $14^2 = (-1)^2 = 1$.

Ordnung 4: $2^4 = 1$, $7^4 = (7^2)^2 = 4^2 = 1$, $8^4 = (8^2)^2 = 4^2 = 1$, $13^4 = (-2)^4 = 1$.

Damit enthält $\mathrm{U}(\mathbb{Z}/(15))$ kein Element der Ordnung 8 und ist somit nicht zyklisch.

> Alternativ kann man folgendermaßen vorgehen: In $\mathbb{Z}$ gilt $(3) \cap (5) = (15)$ und $(3, 5) = (1)$. Nach Blatt 3, Aufgabe 10(2) sind die Ringe $\mathbb{Z}/(15)$ und $\mathbb{Z}/(3) \times \mathbb{Z}/(5)$ isomorph. Folglich sind auch die Gruppen $\mathrm{U}(\mathbb{Z}/(15))$ und $\mathrm{U}(\mathbb{Z}/(3) \times \mathbb{Z}/(5))$ isomorph, und letzere ist isomorph zu $\mathrm{U}(\mathbb{Z}/(3)) \times \mathrm{U}(\mathbb{Z}/(5))$.
>
> Wir haben $|\mathrm{U}(\mathbb{Z}/(3))| = 2$ und $|\mathrm{U}(\mathbb{Z}/(5)| = 4$. Nach Korollar 88 gilt also $x^2 = 1$ für alle $x \in \mathrm{U}(\mathbb{Z}/(3))$ bzw. $y^4 = 1$ für alle $y \in \mathrm{U}(\mathbb{Z}/(5))$.
>
> Folglich gilt für alle $(x, y) \in \mathrm{U}(\mathbb{Z}/(3)) \times \mathrm{U}(\mathbb{Z}/(5))$, dass $(x, y)^4 = ((x^2)^2, y^4) = (1, 1)$ ist. Demnach hat jedes Element in $\mathrm{U}(\mathbb{Z}/(3)) \times \mathrm{U}(\mathbb{Z}/(5))$ – und somit auch jedes Element in $\mathrm{U}(\mathbb{Z}/(15))$ – maximal die Ordnung 4.

(2) Es ist $\mathrm{U}(\mathbb{Z}/(16)) = \{1, 3, 5, 7, 9, 11, 13, 15\}$. Wenn $\mathrm{U}(\mathbb{Z}/(16))$ zyklisch ist, muss es ein Element der Ordnung 8 geben. Man prüft allerdings leicht nach, dass jedes Element Ordnung $1, 2$ oder 4 besitzt:

Ordnung 1: 1.

Ordnung 2: $7^2 = 1$, $9^2 = (-7)^2 = 1$, $15^2 = (-1)^2 = 1$.

Ordnung 4: $3^4 = 9^2 = 1$, $5^4 = (5^2)^2 = 9^2 = 1$, $11^4 = (-5)^4 = 1$, $13^4 = (-3)^4 = 1$.

Damit enthält $\mathrm{U}(\mathbb{Z}/(16))$ kein Element der Ordnung 8 und ist somit nicht zyklisch.

> Man kann auch folgendermaßen vorgehen: Wir haben $x + 16\mathbb{Z} \in \mathrm{U}(\mathbb{Z}/(16))$ genau dann, wenn x ungerade ist. Schreiben wir $x = 1 + 2k$, so gibt eine Anwendung des binomischen Lehrsatzes
>
> $$(1+2k)^4 = 1 + 8k + 24k^2 + 32k^3 + 16k^4 = 1 + 8 \cdot \underbrace{k(3k+1)}_{\equiv_2 0} + 32k^3 + 16k^4 \equiv_{16} 1 + 0 + 0 + 0 = 1,$$
>
> folglich hat jedes Element in $\mathrm{U}(\mathbb{Z}/(16))$ maximal die Ordnung 4.

(3) Nein. So z.B. ist in $\mathbb{F}_{13}$ bereits $3^3 = 27 = 1$, folglich hat 3 in $\mathbb{F}_{13}^\times$ höchstens die Ordnung 3.

(4) Nein. Dann wäre $3^4 \equiv_p 1 \Leftrightarrow 3^4 - 1 \equiv_p 0$. Das wäre aber gleichbedeutend damit, dass p ein Teiler von $3^4 - 1 = 80$ ist, was nur für $p \in \{2, 5\}$ der Fall ist.

Aufgabe 16

(1) Gibt es ein $p \in \mathbb{Z}_{\geqslant 2}$ prim mit $\mathrm{SL}_2(\mathbb{F}_p)$ abelsch?
Gibt es einen Normalteiler $N \trianglelefteq \mathrm{SL}_2(\mathbb{F}_5)$ mit $1 < |N| < |\mathrm{SL}_2(\mathbb{F}_5)|$?

(2) Wir betrachten den Ringmorphismus $f : \mathbb{Z}/(4) \to \mathbb{Z}/(2) : x + (4) \mapsto x + (2)$.
Zur Erinnerung: $\mathbb{Z}/(4) = \mathbb{Z}/4\mathbb{Z}$ und $\mathbb{Z}/(2) = \mathbb{Z}/2\mathbb{Z} = \mathbb{F}_2$.
Wir betrachten den Gruppenmorphismus

$$\varphi \ : \ \mathrm{GL}_2(\mathbb{Z}/(4)) \ \to \ \mathrm{GL}_2(\mathbb{Z}/(2)) \ : \ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \ \mapsto \ \left(\begin{smallmatrix} f(a) & f(b) \\ f(c) & f(d) \end{smallmatrix}\right) .$$

Welche Ordnung hat $\mathrm{Kern}(\varphi)$? Ist $\mathrm{Kern}(\varphi)$ abelsch?

Lösung zu Aufgabe 16:

(1) Es ist $\mathrm{SL}_2(\mathbb{F}_p)$ für keine Primzahl p abelsch: es sind $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{F}_p)$, diese Matrizen kommutieren aber nicht miteinander:

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix},$$
$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}.$$

Es enthält $\mathrm{SL}_2(\mathbb{F}_5)$ die Untergruppe $N = \{E_2, -E_2\}$. Für diese gilt $|N| = 2$. Wir zeigen, dass sie außerdem ein Normalteiler ist:
Für alle $A \in \mathrm{SL}_2(\mathbb{F}_5)$ gilt $\pm E_2 \cdot A = A \cdot (\pm E_2)$. Umstellen ergibt ${}^A(\pm E_2) = A(\pm E_2)A^{-1} = \pm E_2$.
Es folgt, dass ${}^A N = N$ für alle $A \in \mathrm{SL}_2(\mathbb{F}_p)$ gilt. Nach Bemerkung 102 ist N also ein Normalteiler.

(2) Wir beantworten zunächst für eine allgemeine Matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in (\mathbb{Z}/(4))^{2\times 2}$ die Frage, wann $\begin{pmatrix} f(a) & f(b) \\ f(c) & f(d) \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ ist. Dies ist offensichtlich genau dann der Fall, wenn $a, d \in 1 + (2)$ und $b, d \in (2)$ ist, d.h. wenn $A = E_2 + 2B$ mit $B \in (\mathbb{Z}/(4))^{2\times 2}$ gilt. Da es für die Belegung der Einträge a, b, c, d je 2 Optionen gibt, gibt es 16 solche Matrizen.
Wir zeigen, dass jede dieser Matrizen in $\mathrm{GL}_2(\mathbb{Z}/(4))$ liegt – für alle $B \in (\mathbb{Z}/(4))^{2\times 2}$ gilt nämlich $(E_2 + 2B)^2 = E_2 + 4B + 4B^2 = E_2$.
Wir haben also gezeigt, dass $\mathrm{Kern}(\varphi) = \{E_2 + 2B \ : \ B \in (\mathbb{Z}/4\mathbb{Z})^{2\times 2}\}$ ist und dass $|\mathrm{Kern}(\varphi)| = 16$ ist.
Wir zeigen, dass dieser abelsch ist: Sind $E_2 + 2B_1, E_2 + 2B_2 \in \mathrm{Kern}(\varphi)$, so ist

$$(E_2 + 2B_1)(E_2 + 2B_2) = E_2 + 2B_1 + 2B_2 + 4B_1B_2 = E_2 + 2(B_1 + B_2).$$

Vertauschen von B_1, B_2 in dieser Rechnung liefert

$$(E_2 + 2B_2)(E_2 + 2B_1) = E_2 + 2(B_2 + B_1) = E_2 + 2(B_1 + B_2) = (E_2 + 2B_1)(E_2 + 2B_2).$$