M. Truong, M. Künzer

Algebra für Lehramt, SoSe 22

Lösung 6

Aufgabe 21

(1) Sei $m \geqslant 2$. Man zeige: $\mathrm{U}(\mathbb{Z}/(m)) = \{\, k + (m) \,:\, k \in \mathbb{Z},\ \mathrm{ggT}(k, m) = 1 \,\}$.

Wir machen auch wieder Gebrauch von der Kurzschreibweise $k \overset{\text{kurz}}{=} k + (m)$.

(2) Man bestimme $|\mathrm{U}(\mathbb{Z}/(8))|$. Ist $\mathrm{U}(\mathbb{Z}/(8))$ zyklisch?

(3) Man bestimme $|\mathrm{U}(\mathbb{Z}/(27))|$. Ist $\mathrm{U}(\mathbb{Z}/(27)) = \langle 2 \rangle$?

Lösung.
Zu (1).
Zu $\supseteq$. Ist $\mathrm{ggT}(k, m) = 1$, dann gibt es $s,\ t \in \mathbb{Z}$ mit $sk + tm = 1$; vgl. Bemerkung 66. Also ist $sk \equiv_m 1$. Also ist $k + (m) \in \mathrm{U}(\mathbb{Z}/(m))$.
Zu $\subseteq$. Sei $k + (m) \in \mathrm{U}(\mathbb{Z}/(m))$. Dann gibt es ein $s \in \mathbb{Z}$ mit $1 + (m) = (s + (m))(k + (m)) = sk + (m)$. Dann gibt es ein $t \in \mathbb{Z}$ mit $1 = sk + tm$. Also können k und m keinen gemeinsamen Primteiler haben. Somit ist $\mathrm{ggT}(k, m) = 1$.

Zu (2). Unter Verwendung der Kurzschreibweise wird

$$\mathrm{U}(\mathbb{Z}/(8)) \;=\; \{1, 3, 5, 7\}\,;$$

vgl. (1). Darin hat 1 die Ordnung 1 und 3, 5, 7 haben die Ordnung 2. Da es in dieser Gruppe also kein Element der Ordnung 4 gibt, ist $\mathrm{U}(\mathbb{Z}/(8))$ nicht zyklisch.

Zu (3). Unter Verwendung der Kurzschreibweise wird

$$\mathrm{U}(\mathbb{Z}/(27)) = \{1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 20, 22, 23, 25, 26\}\,;$$

vgl. (1).
Darin wird

$$\langle 2 \rangle \;=\; \{1, 2, 4, 8, 16, 5, 10, 20, 13, -1, -2, -4, -8, -16, -5, -10, -20, -13\} \;=\; \mathrm{U}(\mathbb{Z}/(27))\,.$$

Aufgabe 22 Man zeige oder widerlege.

Sei G eine Gruppe.

(1) Sei $N \trianglelefteq G$. Sei $x \in G$. Es ist $|\langle xN \rangle|$ ein Teiler von $|\langle x \rangle|$.

(2) Ist $n \in N \triangleleft G$ und $x \in G$, dann ist $xn = nx$.

(3) Seien $U,\ V \leqslant G$. Es ist $UV := \{\, uv \,:\, u \in U,\ v \in V \,\} \leqslant G$.

(4) Seien $U,\ V \leqslant G$. Es ist $U \cap V \leqslant G$.

Lösung.
Zu (1). Die Aussage ist richtig.
Schreiben wir $k := |\langle x \rangle|$ und $\ell := |\langle xN \rangle|$, dann ist $x^k = 1$ und also auch $(xN)^k = x^k N = 1$. Dank Bemerkung 94 ist

$$k \;\in\; \{\, m \in \mathbb{Z} \,:\, (xN)^m = 1 \,\} \;=\; \ell\mathbb{Z}\,,$$

und folglich ℓ ein Teiler von k.

Zu (2). Die Aussage ist falsch. Sei z.B. $G = \mathrm{S}_3 = (\mathrm{S}_3, \circ)$. Sei $N = \langle (1,2,3) \rangle = \mathrm{A}_3$. Dann ist $N \trianglelefteq G$.
Sei $n := (1,2,3) \in N$. Sei $x := (1,2) \in G$.
Dann ist

$$n \circ x \;=\; (1,2,3) \circ (1,2) \;=\; (1,3)$$

und

$$x \circ n \;=\; (1,2) \circ (1,2,3) \;=\; (2,3)\,.$$

Folglich ist hier $n \circ x \neq x \circ n$.

Zu (3). Die Aussage ist falsch. Sei z.B. $G = \mathrm{S}_3$. Sei $U = \langle (1,2) \rangle$. Sei $V = \langle (2,3) \rangle$. Dann wird

$$UV \;=\; \{\, u \circ v \,:\, u \in U,\, v \in V \,\} \;=\; \{\, \mathrm{id} \circ \mathrm{id},\, \mathrm{id} \circ (2,3),\, (1,2) \circ \mathrm{id},\, (1,2) \circ (2,3) \,\} \;=\; \{\, \mathrm{id},\, (2,3),\, (1,2),\, (1,2,3) \,\}\,.$$

Also ist $|UV| = 4$. Nach dem Satz von Lagrange kann UV keine Untergruppe von G sein, da $|UV| = 4$ kein Teiler von $|G| = 6$ ist.

Zu (4). Die Aussage ist richtig. Wir wollen $U \cap V \leqslant G$ zeigen.
Es ist $1 \in U$ und $1 \in V$, also $1 \in U \cap V$.
Seien $x,\, y \in U \cap V$. Da $x,\, y \in U \leqslant G$, ist $xy^{-1} \in U$. Da $x,\, y \in V \leqslant G$, ist $xy^{-1} \in V$. Also ist $xy^{-1} \in U \cap V$.
Somit ist $U \cap V$ eine Untergruppe von G, wie behauptet.

Aufgabe 23 Sei $Z := \langle \left(\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}\right) \rangle \leqslant \mathrm{GL}_2(\mathbb{F}_5) =: G$.

(1) Man zeige: $Z \trianglelefteq G$.

(2) Sei $P := \mathrm{PGL}_2(\mathbb{F}_5) := G/Z$. Für $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in G$ schreiben wir auch $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] := \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) Z \in P$.
Man zeige: $|\langle \left(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right) \rangle| > |\langle \left[\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right] \rangle| > 1$.

(3) Man bestimme $|P|$.

(4) Sei $U := \langle \left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right] \rangle \leqslant P$. Ist $U \trianglelefteq P$? Ist P abelsch?

Lösung.
Zu (1). Es ist

$$Z \;=\; \langle \left(\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}\right) \rangle \;=\; \{ \left(\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}\right)^0, \left(\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}\right)^1, \left(\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}\right)^2, \left(\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}\right)^3 \} \;=\; \{ \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}\right), \left(\begin{smallmatrix} 4 & 0 \\ 0 & 4 \end{smallmatrix}\right), \left(\begin{smallmatrix} 3 & 0 \\ 0 & 3 \end{smallmatrix}\right) \} \;=\; \{ \left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right) : a \in \mathbb{F}_5^\times \}\,.$$

Folglich ist $gz = zg$ für $z \in Z$ und $g \in G$. Folglich ist $gZ = Zg$ für $g \in G$. Also ist $Z \trianglelefteq G$.

Zu (2). Wir beachen allgemein, daß für $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right), \left(\begin{smallmatrix} \tilde{a} & \tilde{b} \\ \tilde{c} & \tilde{d} \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{F}_5)$ genau dann $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] = \left[\begin{smallmatrix} \tilde{a} & \tilde{b} \\ \tilde{c} & \tilde{d} \end{smallmatrix}\right]$ ist, wenn es ein $x \in \mathbb{F}_5^\times$ gibt mit $\left(\begin{smallmatrix} xa & xb \\ xc & xd \end{smallmatrix}\right) = \left(\begin{smallmatrix} \tilde{a} & \tilde{b} \\ \tilde{c} & \tilde{d} \end{smallmatrix}\right)$.
Es ist $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right)^2 = \left(\begin{smallmatrix} -1 & -1 \\ 1 & 0 \end{smallmatrix}\right)$. Es ist $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right)^3 = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$. Es ist $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right)^6 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Also ist die Ordnung von $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right)$ ein Teiler von 6. Nach den vorangegangenen Rechnungen folgt

$$|\langle \left(\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right) \rangle| \;=\; 6\,.$$

Es ist $\left[\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right]^2 = \left[\begin{smallmatrix} -1 & -1 \\ 1 & 0 \end{smallmatrix}\right]$. Es ist $\left[\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right]^3 = \left[\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right]$. Also ist

$$|\langle \left[\begin{smallmatrix} 0 & -1 \\ 1 & 1 \end{smallmatrix}\right] \rangle| \;=\; 3\,.$$

In der Tat ist $6 > 3 > 1$.

Zu (3). Es ist $|G| = |\,\mathrm{GL}_2(\mathbb{F}_5)| = (5^2 - 1)(5^2 - 5) = 24 \cdot 20 = 480$. Es ist $|Z| = 4$. Also ist

$$|P| \;=\; \frac{|G|}{|Z|} = \frac{480}{4} \;=\; 120\,.$$

Zu (4). Es ist $\left[\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right]^m = \left[\begin{smallmatrix}1&m\\0&1\end{smallmatrix}\right]$ für $m \in \mathbb{Z}$, wobei der Matrixeintrag als $m + (5)$ zu lesen ist.
Also ist $U = \langle \left[\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right] \rangle = \{ \left[\begin{smallmatrix}1&x\\0&1\end{smallmatrix}\right] : x \in \mathbb{F}_5 \}$.
Wir wollen zeigen, daß $U \not\trianglelefteq P$ ist. Z.B. wird

$$\left[\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right] \left[\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right] \left[\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right]^{-1} = \left[\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right] \left[\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right] \left[\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right] = \left[\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right] \left[\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right] = \left[\begin{smallmatrix}1&0\\1&1\end{smallmatrix}\right] \notin U .$$

Also ist i.a. nicht ${}^gU = U$ für $g \in P$. Somit ist $U \not\trianglelefteq P$.

Als zyklische Gruppe ist U abelsch.

Aufgabe 24

(1) Sei $\mathbb{Q}(X^2) := \{ \frac{u(X^2)}{v(X^2)} : u(X) \in \mathbb{Q}[X],\ v(X) \in \mathbb{Q}[X]^\times \}$.

Man zeige: Es ist $\mathbb{Q}(X^2)$ ein Teilring von $\mathbb{Q}(X)$. Jedes Element in $\mathbb{Q}(X^2)^\times$ hat ein multiplikativ Inverses in $\mathbb{Q}(X^2)$.

(2) Man finde a, b, $c \in \mathbb{F}_5$ mit

$$\frac{1}{X^3 + 2X^2} = \frac{a}{X} + \frac{b}{X^2} + \frac{c}{X+2} \in \mathbb{F}_5(X) .$$

Sind die Elemente a, b und c in $\mathbb{F}_5$ dadurch eindeutig bestimmt?

Lösung.
Zu (1). Wir zeigen: Es ist $\mathbb{Q}(X^2)$ ein Teilring von $\mathbb{Q}(X)$.
Es ist $1 = \frac{1}{1} \in \mathbb{Q}(X^2)$.
Seien $u(X)$, $\tilde{u}(X) \in \mathbb{Q}[X]$ und $v(X), \tilde{v}(X) \in \mathbb{Q}[X]^\times$ gegeben.
Dann ist

$$\frac{u(X^2)}{v(X^2)} - \frac{\tilde{u}(X^2)}{\tilde{v}(X^2)} = \frac{u(X^2)\cdot\tilde{v}(X^2) - \tilde{u}(X^2)\cdot v(X^2)}{v(X^2)\cdot\tilde{v}(X^2)}$$

unter Verwendung des Polynoms $u(X)\cdot\tilde{v}(X) - \tilde{u}(X)\cdot v(X) \in \mathbb{Q}[X]$ für den Zähler und $v(X)\cdot\tilde{v}(X) \in \mathbb{Q}[X]^\times$ für den Nenner in $\mathbb{Q}(X^2)$ enthalten.
Ferner ist

$$\frac{u(X^2)}{v(X^2)} \cdot \frac{\tilde{u}(X^2)}{\tilde{v}(X^2)} = \frac{u(X^2)\cdot v(X^2)}{v(X^2)\cdot\tilde{v}(X^2)}$$

unter Verwendung des Polynoms $u(X)\cdot v(X) \in \mathbb{Q}[X]$ für den Zähler und $v(X)\cdot\tilde{v}(X) \in \mathbb{Q}[X]^\times$ für den Nenner in $\mathbb{Q}(X^2)$ enthalten.

Seien schließlich $u(X)$, $v(X) \in \mathbb{Q}[X]^\times$ gegeben. Wir haben zu zeigen, daß $(\frac{u(X^2)}{v(X^2)})^{-1}$ in $\mathbb{Q}(X^2)$ liegt. In der Tat ist

$$\Big(\frac{u(X^2)}{v(X^2)}\Big)^{-1} = \frac{v(X^2)}{u(X^2)}$$

unter Verwendung des Polynoms $v(X) \in \mathbb{Q}[X]$ für den Zähler und $u(X) \in \mathbb{Q}[X]^\times$ für den Nenner in $\mathbb{Q}(X^2)$ enthalten.

Zu (2). Siehe Lösung zu Aufgabe 12.(2).