M. Truong, M. Künzer

Algebra für Lehramt, SoSe 22

Lösung 11

Aufgabe 41 Sei G eine Gruppe mit $|G| = 175$.

(1) Sei $U \leqslant G$ mit $|U| = 35$. Man zeige mittels Lemma 177: Es ist $U \trianglelefteq G$.

(2) Man zeige, daß G eine normale 5-Sylowgruppe und eine normale 7-Sylowgruppe hat.

(3) Man zeige: G ist abelsch. Man zeige damit erneut: Es ist $U \trianglelefteq G$.

(4) Man gebe bis auf Isomorphie alle abelschen Gruppen der Ordnung 175 an.

Lösung.
Zu (1). Der kleinste Primteiler von $|U| = 35$ ist $p = 5$.
Es ist $[G : U] = 175/35 = 5 \leqslant p$. Dank Lemma 177 ist also $U \trianglelefteq G$.

Zu (2).
Es ist $|\operatorname{Syl}_5(G)| \equiv_5 1$ und $|\operatorname{Syl}_5(G)|$ ein Teiler von $175/25 = 7$. Also ist $|\operatorname{Syl}_5(G)| = 1$. Somit gibt es eine normale 5-Sylowgruppe M. Es ist $|M| = 5^2$. Also ist M abelsch.
Es ist $|\operatorname{Syl}_7(G)| \equiv_5 1$ und $|\operatorname{Syl}_7(G)|$ ein Teiler von $175/7 = 25$. Also ist $|\operatorname{Syl}_7(G)| = 1$. Somit gibt es eine normale 7-Sylowgruppe N. Es ist $|N| = 7$. Also ist N zyklisch, insbesondere abelsch.

Zu (3).
Es ist $M \cap N \leqslant M$. Also ist $|M \cap N|$ ein Teiler von 25. Es ist $M \cap N \leqslant N$. Also ist $|M \cap N|$ ein Teiler von 7. Zusammen folgt $|M \cap N| = 1$, d.h. $M \cap N = 1$.
Ferner ist $|M| \cdot |N| = 25 \cdot 7 = 175 = |G|$.
Also ist $G \simeq M \times N$. Da $M \times N$ abelsch ist, ist auch G abelsch.
Die Untergruppe $U \leqslant G$ mit $|U| = 35$ aus (1) ist also, wie jede Untergruppe von G, ein Normalteiler, d.h. $U \trianglelefteq G$.

Zu (4). Es gibt die Faktorisierungen $175 = 175$ und $175 = 5 \cdot 35$ mit sich konsekutiv teilenden Faktoren.
Also erhalten wir bis auf Isomorphie die abelschen Gruppen C_{175} und $\mathrm{C}_5 \times \mathrm{C}_{35}$.
In anderen Worten, bis auf Isomorphie gibt es die abelschen Gruppen $\mathrm{C}_{25} \times \mathrm{C}_7$ und $\mathrm{C}_5 \times \mathrm{C}_5 \times \mathrm{C}_7$.

Aufgabe 42

(1) Man bestimme alle abelschen Gruppen von Ordnung 81 bis auf Isomorphie.

(2) Man bestimme alle abelschen Gruppen von Ordnung 72 bis auf Isomorphie.

Lösung.
Zu (1). Es gibt die Faktorisierungen $81 = 81$, $81 = 9 \cdot 9$, $81 = 3 \cdot 27$, $81 = 3 \cdot 3 \cdot 9$ und $81 = 3 \cdot 3 \cdot 3 \cdot 3$ mit sich konsekutiv teilenden Faktoren.
Also erhalten wir bis auf Isomorphie die abelschen Gruppen C_{81}, $\mathrm{C}_9 \times \mathrm{C}_9$, $\mathrm{C}_3 \times \mathrm{C}_{27}$, $\mathrm{C}_3 \times \mathrm{C}_3 \times \mathrm{C}_9$ und $\mathrm{C}_3 \times \mathrm{C}_3 \times \mathrm{C}_3 \times \mathrm{C}_3$.

Zu (2). Es gibt die Faktorisierungen $72 = 72$, $72 = 6 \cdot 12$, $72 = 3 \cdot 24$, $72 = 2 \cdot 36$, $72 = 2 \cdot 6 \cdot 6$, $72 = 2 \cdot 2 \cdot 18$ mit sich konsekutiv teilenden Faktoren.
Also erhalten wir bis auf Isomorphie die folgenden abelschen Gruppen.

$$\begin{aligned}
\mathrm{C}_{72} &\simeq \mathrm{C}_8 \times \mathrm{C}_9 \\
\mathrm{C}_6 \times \mathrm{C}_{12} &\simeq \mathrm{C}_2 \times \mathrm{C}_4 \times \mathrm{C}_3 \times \mathrm{C}_3 \\
\mathrm{C}_3 \times \mathrm{C}_{24} &\simeq \mathrm{C}_8 \times \mathrm{C}_3 \times \mathrm{C}_3 \\
\mathrm{C}_2 \times \mathrm{C}_{36} &\simeq \mathrm{C}_2 \times \mathrm{C}_4 \times \mathrm{C}_9 \\
\mathrm{C}_2 \times \mathrm{C}_6 \times \mathrm{C}_6 &\simeq \mathrm{C}_2 \times \mathrm{C}_2 \times \mathrm{C}_2 \times \mathrm{C}_3 \times \mathrm{C}_3 \\
\mathrm{C}_2 \times \mathrm{C}_2 \times \mathrm{C}_{18} &\simeq \mathrm{C}_2 \times \mathrm{C}_2 \times \mathrm{C}_2 \times \mathrm{C}_9
\end{aligned}$$

Aufgabe 43

(1) Sei G eine zyklische Gruppe. Sei H eine Gruppe. Sei $G \simeq H$. Man zeige: Es ist H zyklisch.

(2) Seien G und H endliche Gruppen. Sei $G \simeq H$. Sei p prim.
Sei $P \in \mathrm{Syl}_p(G)$. Sei $Q \in \mathrm{Syl}_p(H)$. Man zeige: $P \simeq Q$.

(3) Man bestimme eine abelsche Gruppe G mit $|G| = 12$, die ein Element von Ordnung 4 enthält.

Man bestimme eine abelsche Gruppe H mit $|H| = 12$, die kein Element von Ordnung 4 enthält.

Man zeige: $G \not\simeq H$.

Lösung.
Zu (1). Wir wählen einen Isomorphismus $\varphi : G \xrightarrow{\sim} H$. Wir wählen ein $g \in G$ mit $G = \langle g \rangle$.
Wir behaupten, daß $H \overset{!}{=} \langle \varphi(g) \rangle$ ist. Zu zeigen ist $H \overset{!}{\subseteq} \langle \varphi(g) \rangle$.
Sei $h \in H$. Es ist $\varphi^{-1}(h) \in G$. Also können wir ein $k \in \mathbb{Z}$ wählen mit $\varphi^{-1}(h) = g^k$. Also ist

$$h \;=\; \varphi(\varphi^{-1}(h)) \;=\; \varphi(g^k) = \varphi(g)^k \;.$$

Zu (2). Wir schreiben $|G| = p^a \cdot m$ mit $a \geqslant 0$ und $m \geqslant 1$ mit $m \not\equiv_p 0$. Es ist dann auch $|H| = |G| = p^a \cdot m$.
Es ist $\varphi|_P^{\varphi(P)} : P \xrightarrow{\sim} \varphi(P) =: \tilde{P}$ ein Gruppenoisomorphismus von $P \leqslant G$ zur Untergruppe $\tilde{P} \leqslant H$. Insbesondere ist $P \simeq \tilde{P}$.
Es bleibt zu zeigen: $\tilde{P} \overset{!}{\simeq} Q$.
Es ist $|\tilde{P}| = |P| = p^a$, da $P \in \mathrm{Syl}_p(G)$. Also ist $\tilde{P} \in \mathrm{Syl}_p(H)$. N
Da auch $Q \in \mathrm{Syl}_p(G)$ ist, können wir ein $h \in H$ wählen mit $\tilde{P} = {}^hQ$.
Wir betrachten den Gruppenautomorphismus $\psi : H \xrightarrow{\sim} H : x \mapsto {}^hx$.
Es ist $\psi(Q) = {}^hQ = \tilde{P}$. Also haben wir den Gruppenisomorphismus $\psi|_Q^{\tilde{P}} : Q \xrightarrow{\sim} \tilde{P}$. Insbesondere ist $\tilde{P} \simeq Q$.

Zu (3). Schreiben wir $b := (1,2) \in \mathrm{S}_2$, $c := (1,2,3) \in \mathrm{S}_3$ und $d := (1,2,3,4) \in \mathrm{S}_4$.
Es ist $\mathrm{C}_2 = \langle b \rangle$, $\mathrm{C}_3 = \langle c \rangle$ und $\mathrm{C}_4 = \langle d \rangle$.
Es ist $|\mathrm{C}_3 \times \mathrm{C}_4| = 3 \cdot 4 = 12$. Es ist $(1, d) \in \mathrm{C}_3 \times \mathrm{C}_4$ ein Element von Ordnung 4.
Wir können also $G := \mathrm{C}_3 \times \mathrm{C}_4$ wählen.

Man kann auch $\mathrm{C}_3 \times \mathrm{C}_4 \simeq \mathrm{C}_{12}$ verwenden und stattdessen C_{12} anführen.

Es ist $|\mathrm{C}_3 \times \mathrm{C}_2 \times \mathrm{C}_2| = 12$.
Für i, j k $\in \mathbb{Z}$ ist

$$(c^i, b^j, b^k)^6 \;=\; ((c^3)^{2i}, (b^2)^{3j}, (b^2)^{3k}) \;=\; (1,1,1) \;.$$

Also macht der Exponent 6 jedes Element von $\mathrm{C}_3 \times \mathrm{C}_2 \times \mathrm{C}_2$ zu $(1,1,1) = 1$.
Annahme, es gibt in $\mathrm{C}_3 \times \mathrm{C}_2 \times \mathrm{C}_2$ ein Element von Ordnung 4. Dann ist 4 ein Teiler von 6. *Widerspruch.*
Also gibt es in $\mathrm{C}_3 \times \mathrm{C}_2 \times \mathrm{C}_2$ kein Element von Ordnung 4.
Wir können also $H := \mathrm{C}_3 \times \mathrm{C}_2 \times \mathrm{C}_2$ wählen.
Annahme, es ist $G \simeq H$. Es ist $P := \langle (1,d) \rangle \leqslant G$ eine 2-Sylowgruppe. Sie ist zyklisch. Sei $Q \in \mathrm{Syl}_2(H)$. Gemäß (2) ist $P \simeq Q$. Gemäß (1) ist Q zyklisch. Dann enthält Q ein Element der Ordnung 4. Dann enthält H ein Element der Ordnung 4. Wir haben einen *Widerspruch.*
Also ist $G \not\simeq H$.

Aufgabe 44 Wir erinnern an $\zeta := \zeta_3 = \exp(\frac{2\pi \mathrm{i}}{3}) \in \mathbb{C}$ mit $\zeta^3 = 1$.

(1) Man zeige: ζ ist algebraisch über $\mathbb{Q}$.

(2) Man zeige: $(X - \zeta)(X - \overline{\zeta}) \in \mathbb{Q}[X]$.

(3) Man bestimme das Minimalpolynom $\mu_{\zeta,\mathbb{Q}}(X)$.
Teilt es jedes $f(X) \in \mathbb{Q}[X]$ mit $f(\zeta) = 0$?
Teilt es jedes $f(X) \in \mathbb{C}[X]$ mit $f(\zeta) = 0$?

(4) Man bestimme eine $\mathbb{Q}$-lineare Basis von $\mathbb{Q}(\zeta)$. Man bestimme $[\mathbb{Q}(\zeta) : \mathbb{Q}]$.

Lösung.
Zu (1). Für $u(X) = X^3 - 1 \in \mathbb{Q}[X]$ ist $u(\zeta) = 0$. Also ist ζ algebraisch über $\mathbb{Q}$.

Zu (2). Es ist $X^3 - 1 = (X - \zeta^0)(X - \zeta^1)(X - \zeta^2)$.
Polynomdivision in $\mathbb{Q}[X]$ gibt $(X^3 - 1) = (X - 1) \cdot (X^2 + X + 1)$.
Da $\mathbb{Q}[X]$ ein Integritätsbereich ist, folgt $(X - \zeta)(X - \zeta^2) = X^2 + X + 1 \in \mathbb{Q}[X]$.
Uns bleibt, $\zeta^2 = \overline{\zeta}$ nachzuweisen. Aus $|\zeta|^3 = |\zeta^3| = 1$ folgt, daß $|\zeta| = 1$ und also $\zeta \cdot \overline{\zeta} = |\zeta|^2 = 1$ ist. Folglich ist $\overline{\zeta} = \zeta^{-1} = \zeta^{-1} \cdot \zeta^3 = \zeta^2$.

> Alternativ kann man auch $\zeta = -\frac{1}{2} + \frac{\mathrm{i}}{2}\sqrt{3}$ verwenden, um auf $(X - \zeta)(X - \overline{\zeta}) = X^2 - (\zeta + \overline{\zeta})X + \zeta \cdot \overline{\zeta} = X^2 + X + 1$ zu kommen.

Zu (3). Es ist $X^2 + X + 1 \in \mathbb{Q}[X]$ irreduzibel, da $X^2 + X + 1$ von Grad 2 ist keine Nullstelle in $\mathbb{Q}$ hat, denn die Kandidaten dafür nach Descartes sind 1 und -1, und beide sind keine Nullstelle.
Es hat das normierte irreduzible Polynom $X^2 + X + 1 \in \mathbb{Q}[X]$ die Nullstelle ζ. Folglich ist $\mu_{\zeta,\mathbb{Q}}(X) = X^2 + X + 1$.
Es ist $\mu_{\zeta,\mathbb{Q}}(X)$ ein Teiler jedes Polynoms $f(X) \in \mathbb{Q}[X]$ mit $f(\zeta) = 0$, denn dies ist eine Eigenschaft des Minimalpolynoms.
Es ist aber $\mu_{\zeta,\mathbb{Q}}(X)$ z.B. kein Teiler von $X - \zeta \in \mathbb{C}[X]$, obwohl dieses Polynom Nullstelle ζ hat.

Zu (4). Eine $\mathbb{Q}$-lineare Basis von $\mathbb{Q}(\zeta)$ ist gegeben durch $(\zeta^0, \zeta^1) = (1, \zeta)$.
Es ist $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \dim_{\mathbb{Q}} \mathbb{Q}(\zeta) = 2$.