Anmerkungen und Lösungen zu

Einführung in die Algebra

Blatt 3

Jendrik Stelzner

Letzte Änderung: 11. November 2017

Aufgabe 3

Im Folgenden nutzen wir wiederholt die folgende Aussage, der in der Vorlesung formuliert und bewiesen wurde:

Proposition 1. *Es sei G ein endliche p-Gruppe mit $G \neq 1$. Dann ist auch $\mathrm{Z}(G) \neq 1$.*

Wichtig ist für uns die folgende Konsequenz:

Korollar 2. *Es sei G eine endliche p-Gruppe mit $G \neq 1$. Dann gibt es ein Element $g \in \mathrm{Z}(G)$ von Ordnung p.*

Beweis. Nach Propositon 1 ist $\mathrm{Z}(G) \neq 1$, weshalb es $\tilde{g} \in \mathrm{Z}(G)$ mit $\tilde{g} \neq 1$ gibt. Es gilt $\mathrm{ord}(\tilde{g}) \mid |G|$, weshalb $\mathrm{ord}(\tilde{g})$ eine nicht-triviale p-Potenz ist. Für $r > 1$ mit $\mathrm{ord}(\tilde{g}) = p^r$ gilt dann für das Element $g \coloneqq \tilde{g}^{(p^{r-1})} \in \mathrm{Z}(G)$, dass $\mathrm{ord}(g) = p$. □

(b)

Wir merken zunächst an, dass $(\mathbb{Z}/p) \times (\mathbb{Z}/p)$ nicht zyklisch ist, da jedes nicht-triviale Element $x \in (\mathbb{Z}/p) \times (\mathbb{Z}/p)$ Ordnung p hat. Es gilt also $\mathbb{Z}/p^2 \ncong (\mathbb{Z}/p) \times (\mathbb{Z}/p)$, weshalb jede Gruppe der Ordnung p^2 tatsächlich nur zu genau einer der beiden Gruppen isomorph seien kann.

Für jedes $g \in G$ gilt $\mathrm{ord}(g) \mid |G| = p^2$, und somit $\mathrm{ord}(g) \in \{1, p, p^2\}$. Gibt es ein $g \in G$ mit $\mathrm{ord}(g) = p^2 = |G|$, so ist G zyklisch, und somit $G \cong \mathbb{Z}/p^2$. Wir betrachten daher im Folgenden nur den Fall, dass $\mathrm{ord}(g) = p$ für alle $g \in G$ mit $g \neq 1$ gilt (der Fall $\mathrm{ord}(g) = 1$ tritt nur für $g = 1$ ein).

Nach Proposition 1 gibt es $x \in \mathrm{Z}(G)$ mit $x \neq 1$, und nach Annahme gilt $\mathrm{ord}(x) = p$. (Man könnte hier auch Korollar 2 anwenden.) Da $|G| = p^2 > p = \langle x \rangle$ gilt, gibt es auch $y \in G$ mit $y \notin \langle x \rangle$. Da $\mathrm{ord}(x) = \mathrm{ord}(x) = p$ gilt, ist die Abbildung

$$\varphi \colon (\mathbb{Z}/p) \times (\mathbb{Z}/p) \to G, \quad (\overline{n_1}, \overline{n_2}) \mapsto x^{n_1} y^{n_2}$$

wohldefiniert. Es handelt sich um einen Gruppenhomomorphismus, da x zentral in G ist: Für alle $(\overline{n_1}, \overline{n_2}), (\overline{m_1}, \overline{m_2}) \in (\mathbb{Z}/p) \times (\mathbb{Z}/p)$ gilt

$$\begin{aligned}\varphi(\overline{n_1}, \overline{n_2})\varphi(\overline{m_1}, \overline{m_2}) &= x^{n_1} y^{n_2} x^{m_1} y^{m_2} = x^{n_1} x^{m_1} y^{n_2} y^{m_2} = x^{n_1+n_2} y^{m_1+m_2} \\ &= \varphi(\overline{n_1 + n_2}, \overline{m_1 + m_2}) = \varphi((\overline{n_1}, \overline{n_2}) + (\overline{m_1}, \overline{m_2})).\end{aligned}$$

Es gilt $x \in \operatorname{im}\varphi$ und somit $|\operatorname{im}\varphi| \geq \langle x \rangle = p$. Es gilt zudem $y \in \operatorname{im}\varphi$ mit $y \notin \langle x \rangle$, und somit sogar $|\operatorname{im}\varphi| > p$. Da $\operatorname{im}\varphi$ die Gruppenordnung $|G| = p^2$ teilt, muss bereits $|\operatorname{im}\varphi| = p^2$ gelten, und φ somit surjektiv sein. Da außerdem $|(\mathbb{Z}/p) \times (\mathbb{Z}/p)| = p^2 = |G|$ gilt, ist φ bereits ein Isomorphismus.

Bemerkung 3. Ein alternativer Lösungsweg verläuft wie folgt:

Nach Proposition 1 ist $\mathrm{Z}(G) \neq 1$, und somit $|G/\mathrm{Z}(G)| \in \{1, p\}$. Inbesondere ist $G/\mathrm{Z}(G)$ zyklisch. Es gilt nun die folgende Standardaussage (die in der Vorlesung anscheinend nicht gezeigt wurde):

Lemma 4. *Ist G eine Gruppe, so dass $G/\mathrm{Z}(G)$ zyklisch ist, so ist G bereits abelsch (und somit bereits $\mathrm{Z}(G) = G$ und $G/\mathrm{Z}(G) = 1$.)*

Beweis. Es sei $g \in G$ mit $G/\mathrm{Z}(G) = \langle \overline{g} \rangle$. Für $x, y \in G$ gibt es dann $n, m \geq 0$ mit $\overline{x} = \overline{g}^n = \overline{g^n}$ und $\overline{y} = \overline{g}^m = \overline{g^m}$, und somit $x', y' \in \mathrm{Z}(G)$ mit $x = g^n x'$ und $y = g^m y'$. Die Elemente x', y', g^n, g^m kommutieren alle miteinander, weshalb auch x und y kommutieren. □

Somit folgt, dass G bereits abelsch ist; wir schreiben daher G im Folgenden additiv. Falls es ein Element $g \in G$ der Ordnung $\operatorname{ord}(g) = p^2$ gibt, so ist G zkylisch und $G \cong \mathbb{Z}/p^2$. Ansonsten gilt $\operatorname{ord}(g) = p$ für alle $g \in G$, $g \neq 1$; dann trägt die abelsche Gruppe G die Struktur eines $\mathbb{F}_p$-Vektorraums durch

$$\overline{n}.g = n \cdot g \qquad \text{für alle } \overline{n} \in \mathbb{F}_p,\ g \in G.$$

Aus $|G| = p^2$ erhalten wir, dass $G \cong \mathbb{F}_p^2$ als $\mathbb{F}_p$-Vektorräume, also $G \cong (\mathbb{Z}/p) \times (\mathbb{Z}/p)$ als (abelsche) Gruppen.

Bemerkung 5. Gruppen der Ordnung p^n mit $n \geq 3$ sind nicht notwendigerweise abelsch: Für $n = 3$ dient die Heisenberg-Gruppe

$$\mathrm{B}_3(\mathbb{F}_p) = \left\{ \begin{pmatrix} 1 & a & b \\ & 1 & c \\ & & 1 \end{pmatrix} \,\middle|\, a, b, c \in \mathbb{F}_p \right\}$$

als ein Gegenbeispiel (es handelt sich um eine Untergruppe von $\mathrm{GL}_3(\mathbb{F}_p)$). Für $n \geq 3$ lässt sich somit allgemeiner das Gegenbeispiel $\mathrm{B}_3(\mathbb{F}_p) \times (\mathbb{Z}/p)^{n-3}$ wählen.

Bemerkung 6. Für endlich erzeugte abelsche Gruppen verallgemeinert sich die hier gezeigte Aussagen zum *Fundamentalsatz über endlich erzeugte abelsche Gruppen*: Jede endlich erzeugte abelsche Gruppe G ist von der Form

$$G \cong \mathbb{Z}^r \times (\mathbb{Z}/p_1^{n_1}) \times \cdots \times (\mathbb{Z}/p_t^{n_t})$$

mit $r \geq 0$, $p_1, \ldots, p_t$ prim und $n_1, \ldots, n_t \geq 1$. Die Zahl $r \geq 0$ ist dabei eindeutig, und wird der *Rang* von G genannt; die Paare $(p_1, n_1), \ldots, (p_t, n_t)$ sind eindeutig bis auf Permutation.

Insbesondere ist jede endliche Gruppe von der Form $(\mathbb{Z}/p_1^{n_1}) \times \cdots \times (\mathbb{Z}/p_t^{n_t})$. Wir haben in dieser Aufgabe also den Fundentalsatz für den Fall $|G| = p^2$ gezeugt.