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 $\mathrm{ord}(g) = p$. □

(a)

Für $\mathrm{ord}(G) = p^n$ zeigen wir die Aussage per Induktion über n:

Für $n = 1$ ist $G \cong \mathbb{Z}/p$ und $1 \trianglelefteq G$ bereits eine entsprechende Normalenreihe.

Für $n \geq 2$ gibt es nach Korollar 2 ein Element $x \in G$. Die Untergruppe $\langle x \rangle \leq G$ ist normal, da x zentral in G ist. (Für alle $g \in G$ gilt $gx^k g^{-1} = gg^{-1}x^k = x^k \in \langle x \rangle$ für alle k.) Für $G' \coloneqq G/\langle x \rangle$ gilt

$$|G'| = |G/\langle x \rangle| = \frac{|G|}{|\langle x \rangle|} = \frac{p^n}{p} = p^{n-1}.$$

Nach Induktionsvoraussetzung gibt es eine Normalenreihe

$$1 = G'_0 \trianglelefteq G'_1 \trianglelefteq \cdots \trianglelefteq G'_{n-1} = G'$$

mit $G'_i/G'_{i-1} \cong \mathbb{Z}/p$ für alle i. Bezeichnet $p\colon G \to G/\langle x\rangle = G'$, $g \mapsto \overline{g}$ die kanonische Projektion, so ergibt sich mit den Untergruppen $G_{i+1} \coloneqq p^{-1}(G_i)$ eine Normalenreihe

$$\langle x\rangle = G_1 \trianglelefteq G_2 \trianglelefteq \cdots \trianglelefteq G_n = G$$

mit $G_i/G_{i-1} \cong G'_{i-1}/G'_{i-2} \cong \mathbb{Z}/p$ für alle $i = 2, \ldots, n$ (siehe Übungsblatt 2, Aufgabe 4). Mit $G_1 \coloneqq \langle x\rangle$ erhalten wir die Normalenreihe

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \cdots\cdots \trianglelefteq G_n = G.$$

mit $G_i/G_{i-1} \cong \mathbb{Z}/p$ für alle i.

Bemerkung 3. Eine Normalenreihe

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$$

einer Gruppe G ist eine *Kompositionsreihe* falls die Quotienten G_i/G_{i-1} alle einfach sind. Ähnlich zum obigen Vorgehen lässt sich per Induktion über die Gruppenordnung $|G|$ zeigen, dass jede endliche Gruppe eine Kompositionsreihe besitzt, und dass sich jede Normalenreihe durch Hinzufügen von Termen zu einer Kompositionsreihe verfeinern lässt. Die Wichtigkeit von Kompositionsreihen für das Verständnis endlicher Gruppen ergibt sich aus dem Satz von Jordan–Hölder:

Satz 4 (Jordan–Hölder)**.** *Es sei G eine endliche Gruppe und es seien*

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G,$$
$$1 = G'_0 \trianglelefteq G'_1 \trianglelefteq \cdots \trianglelefteq G'_m = G$$

zwei Kompositionreihen von G. Dann gilt $n = m$, und die Quotienten $(G_i/G_{i-1})_{i=1}^n$ und $(G'_j/G'_{j-1})_{j=1}^m$ stimmen bis auf Permutation überein.

Ist G eine endliche Gruppe, so sind nach dem Satz von Jordan–Hölder in einer Kompositionsreihe

$$1 = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G$$

die Quotienten $F_i \coloneqq G_i/G_{i-1}$ eindeutig bis auf Permutations; die F_i sind die *Kompositionsfaktoren* von G.

In dieser Aufgabe haben wir gezeigt, dass eine endliche Gruppe G genau dann eine p-Gruppe ist, wenn $F_i \cong \mathbb{Z}/p$ für alle i gilt. Allgemeiner ist eine endliche Gruppe G genau dann auflösbar, wenn alle auftretenden Kompositionsfaktoren abelsch sind, d.h. von der Form $F_i \cong \mathbb{Z}/p_i\mathbb{Z}$ für passende Primzahlen p_i sind. Endliche auflösbare Gruppen sowie p-Gruppen lassen sich also durch die auftretenden Kompositionsfaktoren beschreiben.

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

Nach Proposition 1 gibt es $x \in \mathrm{Z}(G)$ mit $x \neq 1$, und nach Annahme gilt $\operatorname{ord}(x) = p$. (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 $\operatorname{ord}(x) = \operatorname{ord}(x) = p$ 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 5. 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 6. *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 7. 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 8. 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.

(c)

Es sei G eine Gruppe der Ordnung 4. Nach Korollar 2 gibt es ein Element $x \in G$ von Ordnung 2, und

$$1 \trianglelefteq \langle x \rangle \trianglelefteq G$$

ist eine Normalenreihe für G mit der gewünschten Eigenschaft. In Abhängigkeit von der Isomorphieklasse lassen sich Normalenreihen auch konkreter angeben:

- Es kann $G \cong \mathbb{Z}/4$ gelten. Eine entsprechende Normalenreihe für $\mathbb{Z}/4$ ist durch

  $$0 = \{\overline{0}\} \trianglelefteq \{\overline{0}, \overline{2}\} \trianglelefteq \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\} = \mathbb{Z}/4$$

  gegeben. (Dies ist auch schon die einzige Möglichkeit, da $\langle \overline{2} \rangle = \{\overline{0}, \overline{2}\}$ die einzige echte, nicht-triviale Untergruppe von $\mathbb{Z}/4$ ist.)

- Ansonsten gilt $G \cong (\mathbb{Z}/2) \times (\mathbb{Z}/2)$. Für $(\mathbb{Z}/2) \times (\mathbb{Z}/2)$ gibt es drei entsprechende Normalenreihen, nämlich

  $$0 = \{(\overline{0}, \overline{0})\} \trianglelefteq \{(\overline{0}, \overline{0}), (\overline{0}, \overline{1})\} \trianglelefteq \{(\overline{0}, \overline{0}), (\overline{0}, \overline{1}), (\overline{1}, \overline{0}), (\overline{1}, \overline{1})\} = (\mathbb{Z}/2) \times (\mathbb{Z}/2),$$
  $$0 = \{(\overline{0}, \overline{0})\} \trianglelefteq \{(\overline{0}, \overline{0}), (\overline{1}, \overline{0})\} \trianglelefteq \{(\overline{0}, \overline{0}), (\overline{0}, \overline{1}), (\overline{1}, \overline{0}), (\overline{1}, \overline{1})\} = (\mathbb{Z}/2) \times (\mathbb{Z}/2),$$
  $$0 = \{(\overline{0}, \overline{0})\} \trianglelefteq \{(\overline{0}, \overline{0}), (\overline{1}, \overline{1})\} \trianglelefteq \{(\overline{0}, \overline{0}), (\overline{0}, \overline{1}), (\overline{1}, \overline{0}), (\overline{1}, \overline{1})\} = (\mathbb{Z}/2) \times (\mathbb{Z}/2).$$