

Anmerkungen und Lösungen zu
Einführung in die Algebra
Blatt 3

Jendrik Stelzner

Letzte Änderung: 17. November 2017

Aufgabe 2

(d)

Für jedes $S \in \mathrm{GL}_n(\mathbb{R})$ ist die Abbildung $\mathbb{R}^n \rightarrow \mathbb{R}^n$, $x \mapsto Sx$ bijektiv. Ist $A \subseteq \mathbb{R}^n$ eine k -elementige Teilmenge, so ist deshalb die Teilmenge $S.A = \{Sx \mid x \in A\}$ ebenfalls k -elementig. Für jedes $A \in X$ gilt

$$I.A = \{Ix \mid x \in A\} = \{x \mid x \in A\} = A,$$

und für alle $S, T \in \mathrm{GL}_n(\mathbb{R})$ und $A \in X$ gelten

$$S.(T.A) = S.\{Tx \mid x \in A\} = \{STx \mid x \in A\} = (ST).A.$$

Ingesamt zeigt dies, dass es sich um eine wohldefinierte Gruppenwirkung handelt.

Zur Bestimmung der Bahnen nutzen wir Lineare Algebra:

Lemma 1. *Es seien $x_1, \dots, x_k \in \mathbb{R}^n$ mit $k \leq n$. Dann gibt es $S \in \mathrm{GL}_n(\mathbb{R})$ mit $Se_i = x_i$ für alle $i = 1, \dots, k$ (wobei $e_1, \dots, e_n \in \mathbb{R}^n$ die Standardbasis bezeichnet).*

Beweis. Durch Basisergänzung ergibt sich eine Basis (x_1, \dots, x_n) von \mathbb{R}^n . Die Matrix $S := (x_1 x_2 \cdots x_n) \in \mathrm{GL}_n(\mathbb{R})$ leistet das Gewünschte. \square

Um die Bahn und den Stabilisator von $A \in X$ zu bestimmen, unterscheiden wir zwischen zwei Fällen:

- Ist $A = \{x_1, x_2\}$ linear unabhängig, so gilt $n \geq 2$. Dann gibt es nach Lemma 1 ein Gruppenelement $S \in G$ mit $S.\{e_1, e_2\} = \{x_1, x_2\} = A$. Das zeigt, dass alle linear unabhängigen Teilmengen eine Bahn bilden. Der Stabilisator von $B := \{e_1, e_2\}$

besteht aus all jenen $S \in \text{GL}_n(\mathbb{R})$, so dass $Se_1 = e_1$ und $Se_2 = e_2$, oder $Se_1 = e_2$ und $Se_2 = e_1$. Also gilt

$$G_B = \left\{ \begin{pmatrix} S_1 & * \\ 0 & S_2 \end{pmatrix} \middle| S_1 \in \left\{ \begin{pmatrix} 1 & \\ & 1 \end{pmatrix}, \begin{pmatrix} & 1 \\ 1 & \end{pmatrix} \right\}, S_2 \in \text{GL}_{n-2}(\mathbb{R}) \right\}$$

Der Stabilisator einer linear unabhängige Teilmenge $A \in X$ ist entsprechend konjugiert zu G_B .

- Ist $A = \{x_1, x_2\}$ linear abhängig, so gilt immer noch $x_1 \neq 0$ oder $x_2 \neq 0$ (da $|A| = 2$); wir können o.B.d.A. davon ausgehen, dass $x := x_1 \neq 0$ gilt. Da A linear unabhängig ist, gibt es dann ein $\lambda \in \mathbb{R}$ mit $x_2 = \lambda x$, und somit $A = \{x, \lambda x\}$; dabei gilt $\lambda \neq 1$ da $|A| = 2$. Da $x \neq 0$ gilt, gibt es nach Lemma 1 eine Matrix $S \in \text{GL}_n(\mathbb{R})$ mit $Se_1 = x$. Dann gilt

$$A = \{x, \lambda x\} = \{Se_1, \lambda Se_1\} = S \cdot \{e_1, \lambda e_1\}.$$

Zur Bestimmung der restlichen Bahnen genügt es also, die Mengen $B_\lambda := \{e_1, \lambda e_1\}$ mit $\lambda \in \mathbb{R}$, $\lambda \neq 1$ zu betrachten.

Eine Menge $A \in X$ ist genau dann in der Bahn von B_λ , wenn eines der Elemente von A das λ -fache des anderen Elements ist. Es folgt, dass

- B_0 und B_μ für $\mu \neq 0$ nie in derselben Bahn liegen,
- B_λ und B_μ für $\lambda \neq 0$ genau dann in der gleichen Bahn liegen, wenn $\mu = \lambda$ oder $\mu = 1/\lambda$ gilt.

Man bemerke, dass dabei für $\lambda = -1$ gilt, dass $1/\lambda = -1 = \lambda$. Mit Ausnahme von B_0 und B_{-1} liegen also je genau zwei B_λ in der gleichen Bahn. Ist $\Lambda \subseteq \mathbb{R}$ eine Teilmenge mit

- $1 \notin \Lambda$,
- $0, -1 \in \Lambda$,

und

- für alle $\lambda \neq 1, 0, -1$ entweder $\lambda \in \Lambda$ oder $1/\lambda \in \Lambda$,

so sind die Mengen $B_\lambda \in X$ mit $\lambda \in \Lambda$ also ein Repräsentantensystem für die Bahnen der linear abhängigen Mengen. (Man kann etwa $\Lambda = [-1, 1]$ wählen.)

Für $S \in G_{B_\lambda}$ müssen die Vektoren e_1 und λe_1 entweder fixiert werden oder vertauscht werden; es gilt also $Se_1 = \lambda e_1$, oder $Se_1 = e_1$ und $S(\lambda e_1) = e_1$. Dabei folgt aus $Se_1 = \lambda e_1$, dass $S(\lambda e_1) = \lambda Se_1 = \lambda^2 e_1 = 1$, und wegen $S(\lambda e_1) = e_1$ somit $\lambda^2 = 1$. Der zweite Fall kann also nur für $\lambda = -1$ eintreten. Damit können wir G_{B_λ} in Abhängigkeit von λ bestimmen:

- Im Fall $\lambda \neq -1$ gilt für $S \in G$ genau dann $S \in G_{B_\lambda}$, wenn $Se_1 = e_1$ gilt. In diesem Fall gilt also

$$G_{B_\lambda} = \left\{ \begin{pmatrix} 1 & * \\ 0 & T \end{pmatrix} \middle| T \in \text{GL}_{n-1}(\mathbb{R}) \right\}.$$

- Im Fall $\lambda = 1$ gilt für $S \in G$ genau dann $S \in G_{B_{-1}}$, wenn $Se_1 = \pm e_1$ gilt. In diesem Fall gilt also

$$G_{B_\lambda} = \left\{ \begin{pmatrix} \pm 1 & * \\ 0 & T \end{pmatrix} \middle| T \in \text{GL}_{n-1}(\mathbb{R}) \right\}.$$

(g)

Für jedes $f \in X$ gilt

$$\text{id} \cdot f = f \circ \text{id}^{-1} = f \circ \text{id} = f,$$

und für alle $\pi_1, \pi_2 \in S_n$ und jedes $f \in X$ gilt

$$\pi_1 \cdot (\pi_2 \cdot f) = \pi_1 (f \circ \pi_2^{-1}) = f \circ \pi_2^{-1} \circ \pi_1^{-1} = f \circ (\pi_1 \circ \pi_2)^{-1} = (\pi_1 \pi_2) \cdot f,$$

weshalb es sich tatsächlich um eine Gruppenwirkung handelt.

Wir können eine Funktion $f: \{1, \dots, n\} \rightarrow \{1, \dots, n\}$ als ein Tupel $(f(1), \dots, f(n))$ schreiben:

$$f \equiv (f(1), \dots, f(n)).$$

Die Wirkung von S_n auf X ist dann durch

$$\pi \cdot (a_1, \dots, a_n) = (a_{\pi^{-1}(1)}, \dots, a_{\pi^{-1}(n)})$$

gegeben. (Man bemerke, dass sich diese Wirkung analog zu der Wirkung aus Aufgabenteil (a) verhält.) Zwei Tupel $(a_1, \dots, a_n), (b_1, \dots, b_n) \in X$ sind genau dann in der gleichen Bahn, wenn sie die gleichen Einträge mit jeweils gleicher Vielfachheit erhalten. Ein Repräsentantensystem der Bahnen ist deshalb durch die Tupel

$$(\underbrace{1, \dots, 1}_{m_1}, \underbrace{2, \dots, 2}_{m_2}, \dots, \underbrace{n, \dots, n}_{m_n})$$

mit $m_1, \dots, m_n \geq 0$, $m_1 + \dots + m_n = n$ gegeben. Der Stabilisator eines solchen Repräsentanten

$$f = (\underbrace{1, \dots, 1}_{m_1}, \underbrace{2, \dots, 2}_{m_2}, \dots, \underbrace{n, \dots, n}_{m_n})$$

ist durch

$$\begin{aligned} & G_f \\ &= \left\{ \pi \in S_n \middle| \begin{array}{l} \pi \text{ permutiert das diskrete Intervall} \\ \{m_1 + \dots + m_k + 1, \dots, m_1 + \dots + m_{k+1}\} \\ \text{für jedes } k = 0, \dots, n-1 \end{array} \right\} \\ &\cong S_{m_1} \times \dots \times S_{m_n} \end{aligned}$$

gegeben.

Aufgabe 3

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

Proposition 2. *Es sei G eine endliche p -Gruppe mit $G \neq 1$. Dann ist auch $Z(G) \neq 1$.*

Wichtig ist für uns die folgende Konsequenz:

Korollar 3. *Es sei G eine endliche p -Gruppe mit $G \neq 1$. Dann gibt es ein Element $g \in Z(G)$ von Ordnung p .*

Beweis. Nach Proposition 2 ist $Z(G) \neq 1$, weshalb es $\tilde{g} \in Z(G)$ mit $\tilde{g} \neq 1$ gibt. Es gilt $\text{ord}(\tilde{g}) \mid |G|$, weshalb $\text{ord}(\tilde{g})$ eine nicht-triviale p -Potenz ist. Für $r > 1$ mit $\text{ord}(\tilde{g}) = p^r$ gilt dann für das Element $g := \tilde{g}^{(p^{r-1})} \in Z(G)$, dass $\text{ord}(g) = p$. \square

(a)

Für $\text{ord}(G) = p^n$ 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 3 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 $G' := G/\langle x \rangle$ 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 $p: G \rightarrow G/\langle x \rangle = G'$, $g \mapsto \bar{g}$ die kanonische Projektion, so ergibt sich mit den Untergruppen $G_{i+1} := p^{-1}(G'_i)$ 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 $i = 2, \dots, n$ (siehe Übungsblatt 2, Aufgabe 4). Mit $G_1 := \langle x \rangle$ erhalten wir die Normalenreihe

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

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

Bemerkung 4. 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 5 (Jordan–Hölder). *Es sei G eine endliche Gruppe und es seien*

$$\begin{aligned} 1 &= G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_n = G, \\ 1 &= G'_0 \trianglelefteq G'_1 \trianglelefteq \cdots \trianglelefteq G'_m = G \end{aligned}$$

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 $F_i := G_i/G_{i-1}$ eindeutig bis auf Permutations; die F_i sind die *Kompositions faktoren* 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 Kompositions faktoren 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 Kompositions faktoren 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 $\mathbb{Z}/p^2 \not\cong (\mathbb{Z}/p) \times (\mathbb{Z}/p)$, weshalb jede Gruppe der Ordnung p^2 tatsächlich nur zu genau einer der beiden Gruppen isomorph sein kann.

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

Nach Proposition 2 gibt es $x \in Z(G)$ mit $x \neq 1$, und nach Annahme gilt $\text{ord}(x) = p$. (Man könnte hier auch Korollar 3 anwenden.) Da $|G| = p^2 > p = \langle x \rangle$ gilt, gibt es auch $y \in G$ mit $y \notin \langle x \rangle$. Da $\text{ord}(x) = \text{ord}(y) = p$ gilt, ist die Abbildung

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

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 $x \in \text{im } \varphi$ und somit $|\text{im } \varphi| \geq \langle x \rangle = p$. Es gilt zudem $y \in \text{im } \varphi$ mit $y \notin \langle x \rangle$, und somit sogar $|\text{im } \varphi| > p$. Da $\text{im } \varphi$ die Gruppenordnung $|G| = p^2$ teilt, muss bereits $|\text{im } \varphi| = p^2$ 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 6. Ein alternativer Lösungsweg verläuft wie folgt:

Nach Proposition 2 ist $Z(G) \neq 1$, und somit $|G/Z(G)| \in \{1, p\}$. Insbesondere ist $G/Z(G)$ zyklisch. Es gilt nun die folgende Standardaussage (die in der Vorlesung anscheinend nicht gezeigt wurde):

Lemma 7. *Ist G eine Gruppe, so dass $G/Z(G)$ zyklisch ist, so ist G bereits abelsch (und somit bereits $Z(G) = G$ und $G/Z(G) = 1$.)*

Beweis. Es sei $g \in G$ mit $G/Z(G) = \langle \bar{g} \rangle$. Für $x, y \in G$ gibt es dann $n, m \geq 0$ mit $\bar{x} = \bar{g}^n = \overline{g^n}$ und $\bar{y} = \bar{g}^m = \overline{g^m}$, und somit $x', y' \in Z(G)$ 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. \square

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

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

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

$$B_3(\mathbb{F}_p) = \left\{ \begin{pmatrix} 1 & a & b \\ & 1 & c \\ & & 1 \end{pmatrix} \mid a, b, c \in \mathbb{F}_p \right\}$$

als ein Gegenbeispiel (es handelt sich um eine Untergruppe von $\text{GL}_3(\mathbb{F}_p)$). Für $n \geq 3$ lässt sich somit allgemeiner das Gegenbeispiel $B_3(\mathbb{F}_p) \times (\mathbb{Z}/p)^{n-3}$ wählen.

Bemerkung 9. 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 $r \geq 0, p_1, \dots, p_t$ prim und $n_1, \dots, n_t \geq 1$. Die Zahl $r \geq 0$ ist dabei eindeutig, und wird der *Rang* von G genannt; die Paare $(p_1, n_1), \dots, (p_t, n_t)$ 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 Fundamentalsatz für den Fall $|G| = p^2$ gezeugt.

(c)

Es sei G eine Gruppe der Ordnung 4. Nach Korollar 3 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

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

gegeben. (Dies ist auch schon die einzige Möglichkeit, da $\langle \bar{2} \rangle = \{\bar{0}, \bar{2}\}$ 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

$$\begin{aligned} 0 &= \{(\bar{0}, \bar{0})\} \trianglelefteq \{(\bar{0}, \bar{0}), (\bar{0}, \bar{1})\} \trianglelefteq \{(\bar{0}, \bar{0}), (\bar{0}, \bar{1}), (\bar{1}, \bar{0}), (\bar{1}, \bar{1})\} = (\mathbb{Z}/2) \times (\mathbb{Z}/2), \\ 0 &= \{(\bar{0}, \bar{0})\} \trianglelefteq \{(\bar{0}, \bar{0}), (\bar{1}, \bar{0})\} \trianglelefteq \{(\bar{0}, \bar{0}), (\bar{0}, \bar{1}), (\bar{1}, \bar{0}), (\bar{1}, \bar{1})\} = (\mathbb{Z}/2) \times (\mathbb{Z}/2), \\ 0 &= \{(\bar{0}, \bar{0})\} \trianglelefteq \{(\bar{0}, \bar{0}), (\bar{1}, \bar{1})\} \trianglelefteq \{(\bar{0}, \bar{0}), (\bar{0}, \bar{1}), (\bar{1}, \bar{0}), (\bar{1}, \bar{1})\} = (\mathbb{Z}/2) \times (\mathbb{Z}/2). \end{aligned}$$