Anmerkungen und Lösungen zu

Einführung in die Algebra

Blatt 3

Jendrik Stelzner

Letzte Änderung: 20. November 2017

Aufgabe 1

(a)

Es gilt

$$n! = 1 \cdot 2 \cdot 3 \cdots n.$$

Wir zählen, wie häufig der Primfaktor p in $n!$ vorkommt:

Jeder p-te Faktor ist durch p teilbar, d.h. in $\lfloor n/p \rfloor$ vielen der Faktoren kommt der Primfaktor p vor. In jedem p^2-ten Faktor kommt er sogar zweimal vor, und im jedem p^3-ten dreimal, usw. Somit kommt der Primfaktore p in dem Produkt $1 \cdot 2 \cdots n$ ingesamt $\sum_{i=1}^{\infty} \lfloor n/p^i \rfloor$ mal vor. Inbesondere ist die Summe endlich.

(b)

Wegen der Additivität von ν_p (es gilt $\nu_p(ab) = \nu_p(a) + \nu_p(b)$ für alle $a, b \in \mathbb{N}$) gilt

$$\nu_p\left(\binom{p^r m}{p^k}\right) = \nu_p\left(\frac{(p^r m)!}{(p^k)!(p^r m - p^k)!}\right) = \nu_p((p^r m)!) - \nu_p((p^k)!) - \nu_p((p^r m - p^k)!)\,.$$

Dabei gelten

$$\begin{aligned}\nu_p((p^r m!)) = \sum_{i=1}^{\infty} \left\lfloor \frac{p^r m}{p^i} \right\rfloor &= \sum_{i=1}^{k} p^{r-i} m + \sum_{i=k+1}^{\infty} \left\lfloor \frac{p^r m}{p^i} \right\rfloor \\ &= \sum_{i=1}^{k} p^{r-i} m + \sum_{j=1}^{\infty} \left\lfloor \frac{p^{r-k} m}{p^j} \right\rfloor = \sum_{i=1}^{k} p^{r-i} m + \nu_p((p^{r-k} m)!)\,,\end{aligned}$$

sowie

$$\nu_p((p^k)!) = \sum_{i=1}^{\infty} \left\lfloor \frac{p^k}{p^i} \right\rfloor = \sum_{i=1}^{k} p^{k-i}$$

und

$$\begin{aligned}
\nu_p((p^r m - p^k)!) &= \sum_{i=1}^{\infty} \left\lfloor \frac{p^r m - p^k}{p^i} \right\rfloor = \sum_{i=1}^{k} (p^{r-i} m - p^{k-i}) + \sum_{i=k+1}^{\infty} \left\lfloor \frac{p^r m - p^k}{p^i} \right\rfloor \\
&= \sum_{i=1}^{k} (p^{r-i} m - p^{k-i}) + \sum_{j=1}^{\infty} \left\lfloor \frac{p^{r-k} m - 1}{p^j} \right\rfloor \\
&= \sum_{i=1}^{k} (p^{r-i} m - p^{k-i}) + \nu_p((p^{r-k} m - 1)!).
\end{aligned}$$

Damit folgt, dass

$$\begin{aligned}
\nu_p\left(\binom{p^r m}{p^k}\right) &= \nu_p((p^{r-k} m)!) - \nu_p((p^{r-k} m - 1)!) \\
&= \nu_p\left(\frac{(p^{r-k} m)!}{(p^{r-k} m - 1)!}\right) = \nu_p(p^{r-k} m) = r - k,
\end{aligned}$$

wobei wir für die letzte Gleichheit nutzen, dass $p \nmid m$.

(c)

Es gilt $S \trianglelefteq N_G(S)$ nach Definition von $N_G(S)$, und nach Annahme gilt $H \leq N_G(S)$. Nach einem der Isomorphiesätze ist deshalb HS eine Untergruppe von $N_G(S)$, sowie $H \cap S$ eine normale Untergruppe von H mit $HS/S \cong H/(H \cap S)$. Inbesondere ist HS/S mit der Multiplikation $\overline{g_1 g_2} = \overline{g_1 g_2}$ eine wohldefinierte Gruppe. Es handelt sich um eine p-Gruppe da

$$|HS/S| = |H/(H \cap S)| = \frac{|H|}{|H \cap S|} \,\Big|\, |H|$$

und $|H|$ eine p-Gruppe ist.

(d)

Es gilt

$$|HS| = \frac{|HS|}{|S|} |S| = |HS/S| \, |S|.$$

Da HS/S und S beides p-Gruppen sind, ist deshalb auch HS eine p-Gruppe. Als p-Sylowuntergruppe ist S kardinalitäts- und damit auch inklusionsmaximal unter allen p-Untergruppen von G; zusammen mit $S \leq HS$ folgt damit, dass bereits $S = HS$ gilt. Somit gelten $HS/S = S/S = 1$ und $H \leq HS = S$.

(e)

Für jede p-Sylowuntergruppe $S' \in \mathrm{Syl}_p(G)$ gilt

$$\begin{aligned} S' \in \mathrm{Syl}_p(G)^S &\iff \forall s \in S : s.S' = S' \iff \forall s \in S : sS's^{-1} = S' \\ &\iff \forall s \in S : s \in N_G(S') \iff S \leq N_G(S') \\ &\iff S \leq S' \iff S = S'. \end{aligned}$$

Dabei nutzen wir für die vorletzte Äquivalenz Aufgabenteil (d). Für die letzte Äquivalenz nutzen wir, dass $|S| = |S'|$ da S und S' zwei p-Sylowuntergruppen sind. Ingesamt zeigt dies, dass S der eindeutige Fixpunkt der gegebenen Wirkung ist.

(f)

Nach der Bahnengleichung gilt

$$|\mathrm{Syl}_p(G)| = \sum_{\mathcal{O} \in \mathrm{Syl}_p(G)/S} |\mathcal{O}| = \left|\mathrm{Syl}_p(G)^S\right| + \sum_{\substack{\mathcal{O} \in \mathrm{Syl}_p(G)/S \\ |\mathcal{O}|>1}} |\mathcal{O}|$$

Dabei gilt für $\mathcal{O} \in \mathrm{Syl}_p(G)/S$ und $S' \in \mathcal{O}$ mit $(S : S_{S'}) = |\mathcal{O}| > 1$ wegen $(S : S_{S'}) \mid |S|$, dass $|\mathcal{O}| = (S : S_{S'})$ eine nicht-trivale p-Potenz ist; inbesondere ist $|\mathcal{O}|$ ein Vielfaches von p. Zudem gilt nach Aufgabenteil (e), dass $|\mathrm{Syl}_p(G)| = 1$. Ingesamt gilt somit

$$|\mathrm{Syl}_p(G)| = \underbrace{\left|\mathrm{Syl}_p(G)^S\right|}_{=1} + \underbrace{\sum_{\substack{\mathcal{O} \in \mathrm{Syl}_p(G)/S \\ |\mathcal{O}|>1}} |\mathcal{O}|}_{\text{Vielfaches von } p} \equiv 1 \mod p.$$

(g)

Die Gruppe G wirkt auf $\mathrm{Syl}_p(G)$ durch Konjugation, d.h. durch

$$g.S' = gS'g^{-1} \qquad \text{für alle } g \in G,\ S' \in \mathrm{Syl}_p(G).$$

Nach dem zweiten Sylowsatz ist diese Wirkung transitiv, d.h. für jedes $S' \in \mathrm{Syl}_p(G)$ gibt es ein $g \in G$ mit $g.S = S'$. Dabei gilt

$$G_S = \{g \in G \mid g.S = S\} = \{g \in G \mid gSg^{-1} = S\} = N_G(S).$$

Somit gilt

$$|\mathrm{Syl}_p(G)| = |G.S| = (G : G_S) = (G : N_G(S)).$$

Dabei gilt

$$m = \frac{|G|}{|S|} = (G : S) = (G : N_G(S))(N_G(S) : S)$$

und somit

$$|\mathrm{Syl}_p(G)| = (G : N_G(S)) \mid m.$$

Aufgabe 2

(d)

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

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

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

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

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

Zur Bestimmung der Bahnen nutzen wir Lineare Algebra:

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

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

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

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

  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 $x \coloneqq x_1 \neq 0$ 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 $S \in \mathrm{GL}_n(\mathbb{R})$ mit $Se_1 = x$. Dann gilt

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

  Zur Bestimmung der restlichen Bahnen genügt es also, die Mengen $B_\lambda \coloneqq \{e_1, \lambda e_1\}$ 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 $\mu \neq 0$ nicht 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 $Se_1 = e_1$, oder $Se_1 = \lambda e_1$ und $S(\lambda e_1) = e_1$ Dabei folgt aus $Se_1 = \lambda e_1$, dass $S(\lambda e_1) = \lambda S e_1 = \lambda^2 e_1 = 1$, 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

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

- 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

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

(g)

Für jedes $f \in X$ gilt

$$\mathrm{id}\,.f = f \circ \mathrm{id}^{-1} = f \circ \mathrm{id} = f\,,$$

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

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

weshalb es sich tatsächlich um eine Gruppenwirkung handelt.

Wir können eine Funktion $f\colon \{1, \ldots, n\} \to \{1, \ldots, n\}$ als ein Tupel $(f(1), \ldots, f(n))$ schreiben:

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

Die Wirkung von S_n auf X ist dann durch

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

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 $m_1, \dots, m_n \geq 0$, $m_1 + \cdots + m_n = n$ 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

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

gegeben.

Aufgabe 3

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

Proposition 2. *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 3. *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 2 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 $\operatorname{ord}(G) = p^n$ zeigen wir die Aussage per Induktion über n:

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

Für $n \geq 2$ gibt es nach Korollar 3 ein Element $x \in \mathrm{Z}(G)$ mit $\operatorname{ord}(x) = p$. Die Untergruppe $\langle x \rangle \leq G$ ist normal, da x zentral in G ist. 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 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*

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

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 $F_i := G_i/G_{i-1}$ eindeutig bis auf Permutations; die Gruppen 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 2 gibt es $x \in \mathrm{Z}(G)$ mit $x \neq 1$, und nach Annahme gilt $\operatorname{ord}(x) = p$. (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 $\operatorname{ord}(x) = \operatorname{ord}(x) = p$ 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

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

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 6. Ein alternativer Lösungsweg verläuft wie folgt:

Nach Proposition 2 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 7. *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 gibt es $x', y' \in \mathrm{Z}(G)$ 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 zykylisch 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 8. 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 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 $r \geq 0$, $p_1, \ldots, p_t$ 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 abelsche 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 3 gibt es ein zentrales 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 von G 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

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

(d)

Es sei R ein beliebiger kommutativer Ring. Dann ist

$$\mathrm{GL}_n(R) \coloneqq \mathrm{M}_n(R)^\times = \{A \in \mathrm{M}_n(R) \mid \text{es gibt } B \in \mathrm{M}_n(R) \text{ mit } AB = I = BA\}$$

eine Gruppe bezüglich der üblichen Matrixmultiplikation. Ferner ist dann

$$\mathrm{B}_n(R) \coloneqq \{S \in \mathrm{GL}_n(R) \mid S \text{ ist eine obere Dreiecksmatrix}\}$$

eine Untergruppe von $\mathrm{GL}_n(R)$. Wir zeigen, dass $G \coloneqq \mathrm{B}_n(R)$ auflösbar ist. Hierfür sei $C_0 \coloneqq [G,G]$ und $C_{k+1} \coloneqq [C_k, C_k]$ für alle $k \geq 1$. Wir zeigen, dass es ein $k \geq 1$ gibt, so dass $C_k = 1$ gilt.

Berechnung des Kommutators $C_0 = [G,G]$

Für $S, T \in G$ mit

$$S = \begin{pmatrix} a_1 & \cdots & * \\ & \ddots & \vdots \\ & & a_n \end{pmatrix} \quad \text{und} \quad T = \begin{pmatrix} b_1 & \cdots & * \\ & \ddots & \vdots \\ & & b_n \end{pmatrix}$$

gelten

$$S^{-1} = \begin{pmatrix} a_1^{-1} & \cdots & * \\ & \ddots & \vdots \\ & & a_n^{-1} \end{pmatrix} \quad \text{und} \quad T^{-1} = \begin{pmatrix} b_1^{-1} & \cdots & * \\ & \ddots & \vdots \\ & & b_n^{-1} \end{pmatrix},$$

und somit

$$\begin{aligned}
[S,T] &= STS^{-1}T^{-1}\\
&= \begin{pmatrix} a_1 & \cdots & * \\ & \ddots & \vdots \\ & & a_n \end{pmatrix} \begin{pmatrix} b_1 & \cdots & * \\ & \ddots & \vdots \\ & & b_n \end{pmatrix} \begin{pmatrix} a_1^{-1} & \cdots & * \\ & \ddots & \vdots \\ & & a_n^{-1} \end{pmatrix} \begin{pmatrix} b_1^{-1} & \cdots & * \\ & \ddots & \vdots \\ & & b_n^{-1} \end{pmatrix}\\
&= \begin{pmatrix} a_1 b_1 a_1^{-1} b_1^{-1} & \cdots & * \\ & \ddots & \vdots \\ & & a_n b_n a_n^{-1} b_n^{-1} \end{pmatrix} = \begin{pmatrix} 1 & * & \cdots & * \\ & \ddots & \ddots & \vdots \\ & & \ddots & * \\ & & & 1 \end{pmatrix}.
\end{aligned}$$

Es gilt also

$$C_0 = [G, G] \subseteq \{\text{Einheitsmatrix} + \text{echte obere Dreiecksmatrizen}\}\,. \tag{1}$$

Berechnung der iterierten Kommutatoren $C_{k+1} = [C_k, C_k]$

Wir verallgemeinern (1) auf die iterierten Kommutatoren $C_{k+1} = [C_k, C_k]$:

Für alle $k \geq 1$ sei $N_k \subseteq \mathrm{M}_n(R)$ die Menge der oberen Dreiecksmatrizen, deren Diagonale sowie $(k-1)$ oberen Nebendiagonalen alle verschwinden. Es ist also N_1 die Menge der echten oberen Dreiecksmatrizen, und im Schritt $N_k \to N_{k+1}$ verschwindet jeweils eine zusätzliche obere Nebendiagonale. Für alle $k \geq 1$ sei

$$Z_k \coloneqq I + N_k = \{I + N \mid N \in N_k\}\,.$$

Wir haben bereits gezeigt, dass $C_0 \leq Z_1$ gilt. Wir zeigen im Folgenden induktiv, dass $C_k \leq Z_{2^k}$ für alle $k \geq 1$ gilt. Da $Z_k = 1$ für alle $k \geq n$ gilt, folgt dann, dass auch $C_k = 1$ für alle $k \geq n$ gilt.

Ums uns die Rechnungen zu vereinfachen, nutzen wir, dass die Matrizen aus Z_k alle von der Form

$$\text{Einheitsmatrix} + \text{nilpotente Matrix}$$

sind.

Lemma 10. *Es seien $k, k_1, k_2 \geq 1$.*

1. *Alle Matrizen $N \in N_k$ sind nilpotent.*
2. *Es gilt $N_{k_1} N_{k_2} \subseteq N_{k_1+k_2}$.*

Beweis.

1. Dies ergibt sich direkt daraus, dass N_k aus echten oberen Dreiecksmatrizen besteht.
2. Dies ergibt sich direkt daraus, dass genau dann $N \in N_k$ gilt, wenn

$$N \cdot \langle e_1, \ldots, e_l \rangle \subseteq \langle e_1, \ldots, e_{l-k} \rangle \qquad \text{für alle } l = 1, \ldots, n.$$

□

Lemma 11. *Ist $N \in \mathrm{M}_n(R)$ nilpotent, so ist $I + N$ invertierbar, und es gilt*

$$(I + N)^{-1} = \sum_{k=0}^{\infty} (-1)^k N^k\,.$$

Beweis. Die Summe $\sum_{k=0}^{\infty} (-1)^k N^k$ ist wohldefiniert, da N nilpotent ist. Es gilt

$$\begin{aligned}(I + N)\left(\sum_{k=0}^{\infty} (-1)^k N^k\right) &= \sum_{k=0}^{\infty} (-1)^k N^k + \sum_{k=0}^{\infty} (-1)^k N^{k+1} \\ &= \sum_{k=0}^{\infty} (-1)^k N^k - \sum_{k=1}^{\infty} (-1)^k N^k = I\,,\end{aligned}$$

sowie analog auch $(\sum_{k=0}^{\infty} (-1)^k N^k)(I + N) = I$. □

Korollar 12. *Es sei $k \geq 1$.*

1. *Es gilt $Z_k Z_k \subseteq Z_k$.*
2. *Für $S \in Z_k$ mit*

$$S = \begin{pmatrix} 1 & 0 & \cdots & 0 & a_1 & * & \cdots & * \\ & \ddots & \ddots & & \ddots & \ddots & \ddots & \vdots \\ & & \ddots & \ddots & & \ddots & \ddots & * \\ & & & \ddots & \ddots & & \ddots & a_m \\ & & & & \ddots & \ddots & & 0 \\ & & & & & \ddots & \ddots & \vdots \\ & & & & & & \ddots & 0 \\ & & & & & & & 1 \end{pmatrix}$$

gilt $S \in \mathrm{GL}_n(R)$, und es gilt

$$S^{-1} = \begin{pmatrix} 1 & 0 & \cdots & 0 & -a_1 & * & \cdots & * \\ & \ddots & \ddots & & \ddots & \ddots & \ddots & \vdots \\ & & \ddots & \ddots & & \ddots & \ddots & * \\ & & & \ddots & \ddots & & \ddots & -a_m \\ & & & & \ddots & \ddots & & 0 \\ & & & & & \ddots & \ddots & \vdots \\ & & & & & & \ddots & 0 \\ & & & & & & & 1 \end{pmatrix}.$$

3. *Es ist Z_k eine Untergruppe von G.*

Beweis.

1. Für $S, T \in Z_k$ gibt es $N, M \in N_k$ mit $S = I + N$ und $T = I + M$. Dann gilt

$$ST = (I + N)(I + M) = I + N + M + NM$$

   mit $NM \in N_{2k} \subseteq N_k$, und somit $N + M + NM \in N_k$.

2. Dies folgt direkt aus Lemma 11.

3. Es gilt $I \in Z_k$, und nach den beiden vorherigen Aussagenteilen ist abgeschlossen unter Produkten und Inversen. □

Korollar 13. *Für alle $k_1, k_2 \geq 1$ gilt $[Z_{k_1}, Z_{k_2}] \subseteq Z_{k_1+k_2}$.*

Beweis. Für $S \in Z_{k_1}$ und $T \in Z_{k_2}$ gibt es $N \in N_{k_1}$ und $M \in N_{k_2}$ mit $S = I + N$ und $T = I + M$. Nach der Inversionsformel aus Korollar 12 gibt es $N' \in N_{k_1+1}$ und $M' \in N_{k_2+1}$, so dass

$$S^{-1} = I - N + N' \quad \text{und} \quad T^{-1} = I - M + M'.$$

Deshalb gilt

$$\begin{aligned}[S,T] = STS^{-1}T^{-1} &= (I+N)(I+M)(I-N+N')(I-M+M') \\ &= I + N + M - N - M + \text{Terme aus } N_{k_1+k_2},\end{aligned}$$

und somit $[S,T] \in I + N_{k_1+k_2} = Z_{k_1+k_2}$. □

Aus Korollar 13 ergibt sich mit $C_0 \leq Z_1$ induktiv, dass $C_k \leq Z_{2^k}$ für alle $k \geq 0$.