Gruppentheorie

FSU Jena - SS 2009

Übungsserie 06 - Lösungen

Stilianos Louca

July 9, 2009

Aufgabe 22

Vorbetrachtung

Sei G eine endliche Gruppe. Ein echter Normalteiler $N \lhd G$ hat *minimalen Index* falls

$$|G:N| = |G:M| \quad \forall\, M \lhd G,\ |G:M| \leq |G:N|$$

Beachte: Jeder Normalteiler $N \lhd G$ mit minimalen Index ist auch ein maximaler Normalteiler, denn:

$$N \leq M \lhd G \quad \Rightarrow \quad |G| = |G:M| \cdot |M| = |G:M| \cdot |M:N| \cdot \underbrace{|N|}_{\frac{|G|}{|G:N|}}$$

$$\Rightarrow \quad |G:N| = |G:M| \cdot |M:N| \quad \Rightarrow \quad |G:M| = |G:N|$$

$$\Rightarrow \quad |M| = |G| \ \Rightarrow \ M = N$$

also insbesondere G/N ist einfach.
Für einen beliebigen Normalteiler $N \trianglelefteq G$ sei nun

$$\mathcal{J}_{G,N} := \bigcap_{\substack{H \trianglelefteq G \\ G/H \cong G/N}} H$$

Zeigen $\mathcal{J}_{G,N} \trianglelefteq G$ ist vollinvariant in G, falls $N \lhd G$ minimalen Index hat.
Beweis: Sei $f \in \mathrm{End}(G)$. Es genügt zu zeigen, dass

$$f(\mathcal{J}_{G,N}) \subset H \quad \forall\, H \trianglelefteq G,\ G/H \cong G/N$$

denn dann wären wir fertig. Sei also $H \trianglelefteq G$ mit $G/H \cong G/N$, dazu

$$K := f^{-1}(H) \trianglelefteq G$$

O.B.d.A sei $K < G$ (denn sonst wäre $f(\mathcal{J}_{G,N}) \subseteq f(G) = f(K) \subseteq H$). Betrachten die Abbildung

$$\Phi : G/K \to G/H\ ,\ kK \mapsto f(k)H$$

Dann:

- Φ ist tatsächlich wohldefiniert und sogar injektiv, denn

$$kK = k'K \ \Leftrightarrow\ k^{-1}k \in K \ \Leftrightarrow\ \underbrace{f(k^{-1}k')}_{f(k)^{-1}f(k')} \in H \ \Leftrightarrow\ \underbrace{f(k)H}_{\Phi(kK)} = \underbrace{f(k')H}_{\Phi(k'K)}$$

- Φ ist homomorph, denn
$$\Phi((kK)(k'K)) = \Phi(kk'K) \overset{\text{def.}}{=} f(kk')H = \underbrace{f(k)H}_{\Phi(kK)}\underbrace{f(k')H}_{\Phi(k'K)}$$

- Φ ist surjektiv.
Beweis: Da Φ injektiv ist, ist $|G:K| \leq \underbrace{|G:H|}_{|G:N|}$, nach Voraussetzung also $|G:K| = |G:N|$. Wegen Injektivität von Φ folgt somit auch dessen Surjektivität.

Φ ist also ein Isomorphismus, insbesondere $G/K \overset{\Phi}{\cong} G/H \cong G/N$, das heißt nach Definition $\mathcal{J}_{G,N} \subseteq K$. Daher
$$f(\mathcal{J}_{G,N}) \subseteq f(K) \subseteq H$$

Beweis der Aussage

Sei nun G eine endliche, einfache End(G)-Gruppe. Ist $G = \{1\}$ so ist G ohnehin charakteristisch einfach, daher sei o.B.d.A. $G \neq 1$. Dann besitzt G sicher einen Normalteiler $N \lhd G$ mit minimalen Index (wählen einfach einen mit $|G:N| = \min \underbrace{\{|G:N'| : N' \lhd G\}}_{\substack{\neq\emptyset \\ \text{da } \{1\}\lhd G}}$). Nach obigen Überlegungen, ist dann $\mathcal{J}_{G,N}$ vollinvariant. Wegen $\mathcal{J}_{G,N} \subseteq N < G$ ist nach Voraussetzung $\mathcal{J}_{G,N} = \{1\}$.

Sei nun $\{1\} < L \unlhd G$ ein minimaler Normalteiler (existiert immer da G endlich). Für jeden Normalteiler $M \unlhd G$ gilt dann $\underbrace{M \cap L}_{\unlhd L} \in \{1, L\}$. Wegen

$$\{1\} = L \cap \overbrace{\mathcal{J}_{G,N}}^{\{1\}} = \bigcap_{\substack{H \unlhd G \\ G/H \cong G/N}} \underbrace{L \cap H}_{\in\{\{1\},L\}}$$

muss es ein $H \unlhd G$ geben mit $G/H \cong G/N$ und $H \cap L = \{1\}$. Da H ein maximaler Normalteiler ist (da H mit minimalen Index), folgt $G = HL$ (da sonst $H \lhd HL \lhd G$), bzw. $G = H \oplus L$. Daher $L \cong G/H \cong G/N$.

Haben also gezeigt: Jeder minimale Normalteiler $\{1\} < L \unlhd G$ ist ein direkter Faktor von G und isomorph zur einfachen (da N maximaler Normalteiler) Gruppe G/N. Somit kann G (iterativ) zerlegt werden in eine direkte Summe einfacher, isomorpher Untergruppen:

- Wählen minimalen Normalteiler $\{1\} < L_1 \unlhd G$, dann ist $G = L_1 \oplus H_1$.
- Ist $G = L_1 \oplus \cdots \oplus L_n \oplus H_n$ mit $H_n > \{1\}$, so wähle minimalen Normalteiler $1 < L_{n+1} \unlhd H_n$, dazu $K \unlhd G$ mit $G = K \oplus L_{n+1}$. Dann ist
$$H_n = H_n \cap G = H_n \cap (KL_{n+1}) \underset{\text{Dedekind}}{\overset{L_{n+1}\subseteq H_n}{=}} (H_n \cap K)L_{n+1} \overset{L_{n+1}\cap K=\{1\}}{=} \underbrace{(H_n \cap K)}_{H_{n+1}} \oplus L_{n+1}$$
das heißt
$$G = L_1 \oplus \cdots \oplus L_{n+1} \oplus H_{n+1}$$
- Dieser Prozess kann nur endlich oft wiederholt werden, da G endlich ist. Dabei sind stets alle L_i einfach und $L_i \cong G/N$.

Bekanntlich ist dann G charakteristisch einfach. $\square$

Motivation

In Analogie zur obigen Aussage, stellt sich die ähnliche Frage: Ist jede endliche, charakteristisch einfache Gruppe G auch einfach?
Hier ist die Antwort negativ. Zum Beispiel hat die charakteristisch einfache Gruppe
$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$
einen echten, nicht-trivialen Normalteiler, z.B. $\mathbb{Z}/2\mathbb{Z} \times \{1\}$.

Aufgabe 23

Zu Gruppe G ohne explizite Ω-Angabe, sei $\Omega = \{1\}$ gesetzt mit ${}^1 g = g \quad \forall\, g \in G$.

(i) Jeder endlich dimensionale $\mathbb{K}$-Vektorraum ($\mathbb{K}$-Gruppe) erfüllt die Minimal- bzw. Maximalbedingung, da aus einer Menge von $\mathbb{K}$-Untergruppen (also Unterräume) einfach einer mit minimaler bzw. maximaler Dimension gewählt werden kann.
Alternativ: Jede endliche Gruppe, da sie ohnehin nur endlich viele Untergruppen besitzt.

(ii) Betrachten die Gruppe[1]

$$G := \left\langle \frac{1}{p^n} + \mathbb{Z} : n \in \mathbb{N} \right\rangle \leq \mathbb{Q}/\mathbb{Z}$$

für irgendeine Primzahl $p \in \mathbb{P}$. Die streng monoton wachsende Folge

$$\mathfrak{M} := \left(\left\langle \frac{1}{p^n} + \mathbb{Z} \right\rangle \right)_{n \in \mathbb{N}}$$

von Untergruppen zeigt, dass G <u>nicht</u> die Maximalbedingung erfüllt.

Wir zeigen nun, dass jede echte Untergruppe von G endlich ist. Dies würde insbesondere die Minimalbedingung für G implizieren, da man von allen echten Untergruppen stets eine mit minimaler Ordnung als minimales Element wählen kann. Sei $U \lneq G$, dazu ein $k \in \mathbb{N}_0$ mit $p^{-k} + \mathbb{Z} \in U$ aber $p^{-(k+1)} + \mathbb{Z} \notin U$. Solch ein k existiert immer, da $\underbrace{p^{-0} + \mathbb{Z}}_{1_G} \in U$ und $U \subsetneq G$ ist. Offensichtlich ist jedes Element $g \in \langle p^{-l} + \mathbb{Z} \rangle$ darstellbar als

$$g = \frac{m}{p^l} + \mathbb{Z}$$

für ein $0 \leq m \leq l$. Zusätzlich, ist auch jedes Element $g \in G$ in irgendeinem $\langle p^{-l} + \mathbb{Z} \rangle$ enthalten (da Kombination endlich vieler $(p^{-l_i})^{\varepsilon_i} + \mathbb{Z},\ \varepsilon_i \in \{\pm 1\},\ l_i \in \mathbb{N}$ und $\langle p^{-l_i} + \mathbb{Z} \rangle \leq \langle p^{\max_j \{l_j\}} + \mathbb{Z} \rangle$), so dass g schreibbar ist als

$$g = \frac{m}{l} + \mathbb{Z}$$

für irgendwelche $l \in \mathbb{N},\ 0 \leq m \leq 1$. O.B.d.A. können wir annehmen $\mathrm{ggT}(m, p^l) = 1$ (sonst $\mathrm{ggT}(m, p^l) = p^s$ für ein $s \in \mathbb{N} \to$ wählen $m' := \frac{m}{p^s},\ l' := l - s$). Nach Aufgabe 18 (ii) ist dann

$$\left| \langle mp^{-l} + \mathbb{Z} \rangle \right| = \frac{p^l}{\mathrm{ggT}(m, p^l)} = p^l = \langle p^{-l} + \mathbb{Z} \rangle \;\Rightarrow\; \langle mp^{-l} + \mathbb{Z} \rangle = \langle p^{-l} + \mathbb{Z} \rangle$$

das heißt

$$mp^{-l} + \mathbb{Z} \in U \quad \Leftrightarrow p^{-l} + \mathbb{Z} \in U \quad , \quad l \in \mathbb{N},\ \mathrm{ggT}(m, p^l) = 1$$

Ist nun $g \in U$ (mit $g = mp^{-l} + \mathbb{Z},\ \mathrm{ggT}(m, p^l) = 1$), so ist sogar $p^{-l} + \mathbb{Z} \in U$, also muss $l \leq k$ sein (da für $l > k$ stets $p^{-l} + \mathbb{Z} \notin U$), somit

$$U \subseteq \langle p^{-k} + \mathbb{Z} \rangle$$

Insbesondere $|U| \leq \left| \langle p^{-k} + \mathbb{Z} \rangle \right| = p^k$.

(iii) Die Gruppe $(\mathbb{Z}, +)$ erfüllt zwar Maximal- jedoch nicht Minimalbedingung.
Beweis: Die Menge von Untergruppen

$$\{\langle n \rangle\}_{n \in \mathbb{N}}$$

besitzt kein minimales Element, da jede $\langle n \rangle$ die Untergruppe $\langle 2n \rangle$ echt enthält.

Sei anderseits $\mathfrak{M} := \{U_i\}_{i \in I}$ eine Menge von Untergruppen von $\mathbb{Z}$, also $U_i = n_i \mathbb{Z}$ für irgendwelche $\{n_i\}_{i \in I} \subset \mathbb{N}_0$. Wählen das kleinste $n := \min \{n_i\}_{i \in I}$, dann ist $n\mathbb{Z} \in \mathfrak{M}$ maximal, da für $m \geq n$ gilt $m\mathbb{Z} \not< n\mathbb{Z}$.

[1] Man nennt G *quasizyklische* p-Gruppe oder *Prüfer* p-Gruppe. Beachte dass stets

$$\left\langle \frac{1}{p^n} + \mathbb{Z} \right\rangle \lneq \left\langle \frac{1}{p^{n+1}} + \mathbb{Z} \right\rangle$$

gilt, formal

$$G = \left\langle \frac{1}{p^\infty} + \mathbb{Z} \right\rangle$$

was den ersten Namen rechtfertigt.

(iv) Weder Maximal- noch Minimalbedingung sind für $(\mathbb{Q},+)$ erfüllt, da z.B. die Menge von Untergruppen

$$\{\langle 2^n\rangle\}_{n\in\mathbb{Z}}$$

kein maximales Element besitzt, da jede $\langle 2^n\rangle$ in $\left\langle 2^{n-1}\right\rangle$ echt enthalten ist. Auch enthält sie kein minimales Element, da jede $\langle 2^n\rangle$ die Untergruppe $\left\langle 2^{n+1}\right\rangle$ echt enthält.

Aufgabe 24

(i) Da $f : x \mapsto x^{-1}$ bijektiv ist, genügt es die Homomorphie von f zu untersuchen:

$$(f : x \mapsto x^{-1}) \in \mathrm{End}(G) \;\Leftrightarrow\; \forall\, x^{-1}, y^{-1} \in G : \underbrace{f(x^{-1}y^{-1})}_{yx} = \underbrace{f(x^{-1})f(y^{-1})}_{xy} \;\Leftrightarrow\; G \text{ abelsch}$$

(ii) Analog:

$$(f : x \mapsto x^{2}) \in \mathrm{End}(G) \;\Leftrightarrow\; \forall\, x, y \in G : \underbrace{f(xy)}_{xyxy} = \underbrace{f(x)f(y)}_{x^2y^2} \;\Leftrightarrow\; yx = xy \;\Leftrightarrow\; G \text{ abelsch}$$

(iii) **Richtung "$\Leftarrow$":** Sei G abelsch von ungerader Ordnung, dann ist $f : x \mapsto x^2$ nach (ii) ein Endomorphismus. f ist dabei injektiv, da sonst für ein $1 \neq x \in G$ gelten würde $x^2 = 1 \;\Rightarrow\; |\langle x\rangle| = 2$ und somit nach Lagrange $2 \,\big|\, |G|$, ein Widerspruch! Surjektivität folgt dann aus Endlichkeit von G.

Richtung "$\Rightarrow$": Sei $f : x \mapsto x^2$ Automorph. Dann ist nach (ii) G abelsch. Jedes Element $1 \neq g \in G$ ist außerdem von ungerader Ordnung, da sonst $g^{2n} = 1$ (und $g^n \neq 1$) für irgendein $n \in \mathbb{N}$ sein würde, das heißt $f(g^n) = 1 = f(1)$, ein Widerspruch zur Injektivität von f.

Nun Beweis durch vollständige Induktion (über $|G|$). Für $|G| \leq 2$ und $(x \mapsto x^2) \in \mathrm{Aut}(G)$ ist Behauptung klar, denn $G = \langle x\rangle$ für ein $x \in G$, das natürlich ungerade Ordnung hat.

Sei nun $|G| \in \mathbb{N}$, dazu ein Element $1 \neq g \in G$. Dann ist $\langle g\rangle \trianglelefteq G$ (da G abelsch) und $G/\langle g\rangle$ abelsch, das heißt die Abbildung

$$f' : G/\langle g\rangle \to G/\langle g\rangle \quad , \quad f' : h\langle g\rangle \mapsto \underbrace{(h\langle g\rangle)^2}_{h^2\langle g\rangle}$$

ist Homomorph. Sie ist sogar injektiv, denn für $h^2\langle g\rangle = q^2\langle g\rangle$, das heißt $(hq^{-1})^2 = h^2(q^2)^{-1} \in \langle g\rangle$, folgt aus der Tatsache $f\big|_{\langle g\rangle} \in \mathrm{Aut}(\langle g\rangle)$ (denn $f(\langle g\rangle) \subset \langle g\rangle$ auf injektiver also auch surjektiver Weise) dass auch $hq^{-1} \in \langle g\rangle$ ist, also $h\langle g\rangle = q\langle g\rangle$. Surjektivität folgt aus Endlichkeit von $G/\langle g\rangle$, also

$$f' \in \mathrm{Aut}(G/\langle g\rangle)$$

Wegen $g \neq 1$ ist $|G/\langle g\rangle| < |G|$, so dass nach Induktionsvoraussetzung $|G/\langle g\rangle|$ ungerade ist! Nach Lagrange folgt dann

$$|G| = \underbrace{\underbrace{|\langle g\rangle|}_{\text{ungerade}} \cdot \underbrace{|G/\langle g\rangle|}_{\text{ungerade}}}_{\text{ungerade}}$$

Alternativ, Richtung "$\Rightarrow$": Wegen

$$\{1\} = \ker\left(x \mapsto x^2\right) = \left\{x \in G : x^2 = 1\right\}$$

besitzt G kein Element der Ordnung 2. Also ist $G \setminus \{1\}$ disjunkte Vereinigung von Paaren der Form $\left\{x, x^{-1}\right\}$, $x \neq x^{-1}$. Das zeigt, dass G ungerade Ordnung hat.

□

Aufgabe 25

(i) Wegen

$$ab = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} = ba$$

ist $G := \langle a, b \rangle$ nicht-abelsch. Wegen

$$\langle a \rangle = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \underbrace{\begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}}_{a}, \underbrace{\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}}_{a^2}, \underbrace{\begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}}_{a^3} \right\}$$

muss nach Lagrange $\underbrace{|\langle a \rangle|}_{4} \mid |G|$. Wegen $b \notin \langle a \rangle$ ist jedoch $|G| > |\langle a \rangle|$, das heißt $G \geq 8$.

Ferner bilden reguläre diagonal- und schiefdiagonal-Matrizen eine Untergruppe. Dies kann leicht nachgerechnet werden:

$$\begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} \begin{pmatrix} \gamma & 0 \\ 0 & \delta \end{pmatrix} = \begin{pmatrix} \alpha\gamma & 0 \\ 0 & \beta\delta \end{pmatrix} \quad , \quad \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix} \begin{pmatrix} 0 & \gamma \\ \delta & 0 \end{pmatrix} = \begin{pmatrix} 0 & \alpha\gamma \\ \beta\delta & 0 \end{pmatrix}$$

$$\begin{pmatrix} 0 & \alpha \\ \beta & 0 \end{pmatrix} \begin{pmatrix} \gamma & 0 \\ 0 & \delta \end{pmatrix} = \begin{pmatrix} 0 & \alpha\delta \\ \beta\gamma & 0 \end{pmatrix} \quad , \quad \begin{pmatrix} 0 & a \\ \beta & 0 \end{pmatrix} \begin{pmatrix} 0 & \gamma \\ \delta & 0 \end{pmatrix} = \begin{pmatrix} \alpha\delta & 0 \\ 0 & \beta\gamma \end{pmatrix}$$

$$\begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}^{-1} = \begin{pmatrix} \alpha^{-1} & 0 \\ 0 & \beta^{-1} \end{pmatrix} \quad , \quad \begin{pmatrix} 0 & \gamma \\ \delta & 0 \end{pmatrix}^{-1} = \begin{pmatrix} 0 & \delta^{-1} \\ \gamma^{-1} & 0 \end{pmatrix}$$

Da a und b von obiger Form sind mit Elementen aus $\underbrace{\{\pm 1, \pm i\}}_{\substack{\text{geschlossen bzgl.} \\ \text{Multiplikation}}}$, sind auch alle Kombinationen in $\langle a, b \rangle$ der obigen Form mit Elementen aus $\{\pm 1, \pm i\}$. Wegen $\det(a) = \det(b) = 1$ gilt $\det(g) = 1 \ \forall \ g \in \langle a, b \rangle$, das heißt die einzigen Formen sind

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix}$$

und analog für die schiefdiagonalen. Demnach $|\langle a, b \rangle| = 8$.

(ii) Seien $A := \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}, B := \begin{pmatrix} 0 & \gamma \\ \delta & 0 \end{pmatrix} \in G$ beliebig. Sei $U \leq G$ eine Untergruppe und $C := \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix} \in U$ beliebig. Dann ist

$$ACA^{-1} = \begin{pmatrix} \alpha\lambda\alpha^{-1} & 0 \\ 0 & \beta\lambda^{-1}\beta^{-1} \end{pmatrix} = C \in U \quad , \quad BCB^{-1} = \begin{pmatrix} \lambda^{-1} & 0 \\ 0 & \lambda \end{pmatrix} = \left\{ \begin{array}{ll} C & : \lambda = \pm 1 \\ C^3 & : \lambda = \pm i \end{array} \right\} \in U$$

Analog für $D := \begin{pmatrix} 0 & \lambda \\ -\lambda^{-1} & 0 \end{pmatrix} \in U$, sind auch

$$\underbrace{\begin{pmatrix} 0 & -\lambda \\ \lambda^{-1} & 0 \end{pmatrix}}_{D^3} \in U \ , \ \begin{pmatrix} 0 & \lambda^{-1} \\ -\lambda & 0 \end{pmatrix} = \left\{ \begin{array}{ll} D & : \lambda = \pm 1 \\ -D & : \lambda = \pm i \end{array} \right\} \in U \ , \ \begin{pmatrix} 0 & -\lambda^{-1} \\ \lambda & 0 \end{pmatrix} = \left\{ \begin{array}{ll} -D & : \lambda = \pm 1 \\ D & : \lambda = \pm i \end{array} \right\} \in U$$

und somit

$$ADA^{-1} = \begin{pmatrix} 0 & \alpha\lambda\beta^{-1} \\ -\beta\lambda^{-1}\alpha^{-1} & 0 \end{pmatrix} \overset{\beta = \alpha^{-1}}{=} \begin{pmatrix} 0 & \alpha^2\lambda \\ (\alpha^{-1})^2(-\lambda^{-1}) & 0 \end{pmatrix} = \left\{ \begin{array}{ll} D & : \alpha = \pm 1 \\ -D & : \alpha = \pm i \end{array} \right\} \in U$$

$$BDB^{-1} = \begin{pmatrix} 0 & -\gamma\lambda^{-1}\delta^{-1} \\ \gamma^{-1}\lambda\delta & 0 \end{pmatrix} \overset{\delta = -\gamma^{-1}}{=} \begin{pmatrix} 0 & \gamma^2\lambda^{-1} \\ -(\gamma^{-1})^2\lambda & 0 \end{pmatrix} = \left\{ \begin{array}{ll} \begin{pmatrix} 0 & \lambda^{-1} \\ -\lambda & 0 \end{pmatrix} & : \gamma = \pm 1 \\ \begin{pmatrix} 0 & -\lambda^{-1} \\ \lambda & 0 \end{pmatrix} & : \gamma = \pm i \end{array} \right\} \in U$$

Demnach ist allgemein $AUA^{-1} \subseteq U$, $BUB^{-1} \subseteq U$, also U normal.

(iii) Die beiden Gruppen sind **nicht** isomorph, da die Gruppe G_9 aus Aufgabe (9), im Gegensatz zu G, nicht-normale Untergruppen besaß, z.B.

$$\left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\rangle$$