

Lösung 26

Aufgabe 68.

Es ist $168 = 2^3 \cdot 3 \cdot 7$. Sei H eine 7-Sylowgruppe, und sei $N = N_G(H)$. Es ist die Anzahl $[G : N]$ der 7-Sylowgruppen kongruent zu 1 modulo 7, ein Teiler von 21 und ungleich 1. Also ist $[G : N] = 8$, i.e. $|N| = 21$. Das Theorem von Schur-Zassenhaus aus §3.2.2 ⁽¹⁾ impliziert nun, daß $G \simeq C_7 \rtimes C_3$. Da mit dem Satz aus §2.5.5.3, Teil (1), der Schnitt $Z(N) \cap H$ verschwindet, kann N nicht abelsch, und also dieses semidirekte Produkt nicht trivial sein. Schreibe $C_7 = \langle c \rangle$ und $C_3 = \langle a \rangle$. Es hat C_7 wegen $\text{Aut } C_7 \simeq (\mathbf{Z}/7\mathbf{Z})^* \simeq C_6$ zwei Automorphismen von Ordnung 3, namentlich $c \mapsto c^2$ und $c \mapsto c^4$. Durch eventuelle Ersetzung von a durch a^2 dürfen wir annehmen, daß ${}^a c = c^2$.

Sei X die Menge der 7-Sylowgruppen von G . Es operiert $\langle a \rangle$ via Konjugation auf X . Da $A := \langle a \rangle$ das Element $H \in X$ festläßt, und da $X \setminus \{H\}$ aus 7 Elementen besteht, hat A einen weiteren Fixpunkt $K \neq H$ in X .

Es operiert H via Konjugation auf X . Dabei ist H ein Fixpunkt. Schreibe $K = {}^g H$ mit einem geeigneten $g \in G$. Es ist $N_G(K) = N_G({}^g H) = {}^g N_G(H)$ von Ordnung 21 (man hätte hierfür auch das Argument für $|N_G(H)| = 21$ mit K statt H zitieren können). Wäre $H \leq N_G(K)$, so wäre auch die Menge $K \cdot H$ in $N_G(K)$ enthalten. Wegen $H \cap K = 1$ enthält $K \cdot H$ aber 7^2 Elemente, was dann nicht sein kann. Also ist $H \not\leq N_G(K)$, i.e. $K \in X$ ist kein Fixpunkt von H . Insgesamt ist $H \in X$ also der einzige Fixpunkt von H , und X zerfällt in die beiden Bahnen

$$X = \{H\} \sqcup \{c^0 K, c^1 K, \dots, c^6 K\}$$

unter der Operation von H .

Wir erinnern an die Definition der projektiven Geraden $P^1(\mathbf{F}_7)$ als der Menge der eindimensionalen Teilräume des \mathbf{F}_7 -Vektorraums \mathbf{F}_7^2 . Hierbei schreibt man $(u : v) := \langle \begin{pmatrix} u \\ v \end{pmatrix} \rangle$ für $\begin{pmatrix} u \\ v \end{pmatrix} \in \mathbf{F}_7^2 \setminus \{0\}$. Es operiert $\text{GL}_2(\mathbf{F}_7)$ geradenbewahrend auf \mathbf{F}_7^2 , und folglich auf $P^1(\mathbf{F}_7)$. Ausgeschrieben wird

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \cdot (u : v) = (\alpha u + \beta v : \gamma u + \delta v).$$

Die Elemente aus $Z(\text{GL}_2(\mathbf{F}_7)) = \{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} : a \in \mathbf{F}_7 \setminus \{0\} \}$ operieren hierbei trivial, so daß wir auch eine Operation von $\text{PGL}_2(\mathbf{F}_7) = \text{GL}_2(\mathbf{F}_7)/Z(\text{GL}_2(\mathbf{F}_7))$ auf $P^1(\mathbf{F}_7)$ erhalten. Diese Operation ist treu, d.h. gegeben durch einen injektiven Gruppenmorphismus von $\text{PGL}_2(\mathbf{F}_7)$ in die entgegengesetzte Gruppe symmetrischen Gruppe auf der Menge $P^1(\mathbf{F}_7)$.

Wir identifizieren nun $P^1(\mathbf{F}_7)$ mit X , indem wir $(1 : 0)$ mit H und $(u : 1)$ mit $c^u K$ identifizieren, wobei $u \in [1, 6]$. Insbesondere operiert nun G auf $P^1(\mathbf{F}_7)$.

Wir behaupten, daß das Bild des Operationsmorphismus von G auf $P^1(\mathbf{F}_7)$ mit dem Bild des Operationsmorphismus von $\text{PSL}_2(\mathbf{F}_7) (\leq \text{PGL}_2(\mathbf{F}_7))$ übereinstimmt. Wegen der Einfachheit von G operiert auch G treu auf $P^1(\mathbf{F}_7)$, sofern nur nicht jedes Element von G identisch operiert. Dies ist aber nicht der Fall, wie bereits gesehen (und wie aus der Transitivität von X auch a priori bekannt ist). Für die behauptete Übereinstimmung der Bilder muß wegen

$$|G| = 168 = (7^2 - 1)(7^2 - 7) \cdot \underbrace{(7 - 1)^{-1}}_{\text{Kern det}} \cdot \underbrace{2^{-1}}_{Z(\text{SL})} = |\text{PSL}_2(\mathbf{F}_7)|$$

nur noch gezeigt werden, daß jede Operation eines Elementes von G durch die Operation eines Elementes von $\text{PSL}_2(\mathbf{F}_7)$ geschrieben werden kann. Ferner kann man sich auf die Betrachtung einer Erzeugermenge von G beschränken.

¹Es genügt auch das Korollar aus §3.2.1. Ebenso kann man zitieren, daß ein Element der Ordnung 3 in einer Gruppe von durch 3 teilbarer Gruppenordnung existiert (Satz von Cauchy).

Die Operation von c schickt $(1 : 0)$ nach $(1 : 0)$ und $(u : 1)$ nach $(u + 1 : 1)$, stimmt also mit der Operation von $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ überein.

Die Operation von a schickt H nach H und $c^u K$ nach $ac^u K = c^{2u} a K = c^{2u} K$, i.e. es kommt $(1 : 0)$ nach $(1 : 0)$ und $(u : 1)$ nach $(2u : 1)$. In anderen Worten, die Operation von a stimmt mit der Operation von $\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$ überein, und also auch mit der Operation von $\begin{pmatrix} 4 & 0 \\ 0 & 2 \end{pmatrix}$. Unter der Operation von A haben wir die Bahnenzerlegung

$$P^1(\mathbf{F}_7) = \{(1 : 0)\} \sqcup \{(0 : 1)\} \sqcup \{(1 : 1), (2 : 1), (4 : 1)\} \sqcup \{(3 : 1), (5 : 1), (6 : 1)\}$$

Sei $M := N_G(A)$. Die Anzahl $[G : M]$ der 3-Sylowgruppen in G ist kongruent zu 1 modulo 3, ein Teiler von 56 und ungleich 1. Also $[G : M] \in \{4, 7, 28\}$, d.h. $[M : A] \in \{14, 8, 2\}$.

(Nach dem ersten Beispiel in §2.5.5.3, Teil (4), ist $[M : A] \equiv_2 0$. Das liefert aber keine neuen Erkenntnisse.)

Da mit dem Satz aus §2.5.5.3, Teil (1), der Schnitt $Z(M) \cap A$ verschwindet, gibt es ein $m \in M$, welches auf A nichttriviale operiert, i.e., für welches ${}^m a = a^{-1}$ ist. Da das Bild von m in $\text{Aut } A$ von Ordnung 2 ist, teilt 2 die Ordnung von m . Durch Übergang zu einer ungeraden Potenz können wir annehmen, daß die Ordnung von m eine Potenz von 2 ist.

Da für $(u : v) \in P^1(\mathbf{F}_7)$ und $i \in \mathbf{Z}/3\mathbf{Z}$ es sich ergibt, daß ${}^m(u : v)$ und ${}^{m^{a^i}}(u : v) = a^{-i}({}^m(u : v))$ in der selben Bahn unter A liegen, operiert m auf der Menge der A -Bahnen von $P^1(\mathbf{F}_7)$.

Auf der anderen Seite hat m keinen Fixpunkt in $P^1(\mathbf{F}_7)$, i.e. keinen Fixpunkt in X . Denn sonst wäre m in einem Normalisator einer 7-Sylowgruppe enthalten. Diese haben aber alle die ungerade Ordnung 21, so daß das nicht möglich ist. Also muß ${}^m(1 : 0) = (0 : 1)$ sein, und ${}^m(0 : 1) = (1 : 0)$. Insbesondere folgt ${}^{m^2}(1 : 0) = (1 : 0)$, und somit auch $m^2 \in N$. Da aber auch die Ordnung von m^2 eine Potenz von 2 ist, folgt mit $|N| = 21 \equiv_2 1$, daß $m^2 = 1$. Es hat m also die Ordnung 2.

Nun kann m die A -Bahn $\{(1 : 1), (2 : 1), (4 : 1)\}$ nicht in sich selbst überführen, da diese sonst wegen der Fixpunktfreiheit von m in $\langle m \rangle$ -Bahnen der Länge 2 zu zerfallen hätte. Also schickt m die A -Bahn $\{(1 : 1), (2 : 1), (4 : 1)\}$ auf die A -Bahn $\{(3 : 1), (5 : 1), (6 : 1)\}$, und umgekehrt. Schreibe ${}^m(1 : 1) =: (w : 1)$ mit $w \in \{3, 5, 6\}$.

Allgemein wird für $u \in \mathbf{F}_7 \setminus \{0\}$

$${}^m(2u : 1) = {}^{ma}(u : 1) = a^{-1}({}^m(u : 1)).$$

Zusammengefaßt wird somit

$$\begin{aligned} {}^m(0 : 1) &= (1 : 0) \\ {}^m(1 : 1) &= (w : 1) \\ {}^m(2 : 1) &= (w/2 : 1) \\ {}^m(4 : 1) &= (w/4 : 1), \end{aligned}$$

und die Operation von m ist von Ordnung 2.

Sei nun $w' \in \mathbf{F}_7$ mit $w'^2 = -w$ gewählt. Dann ist die Operation von m gegeben durch $\begin{pmatrix} 0 & -w' \\ w' & 0 \end{pmatrix}$. Denn letztere ist von Ordnung 2 und schickt für $u \in \mathbf{F}_7$ das Element $(u : 1)$ auf $(-w' : uw'^{-1}) = (w : u)$, was für $u \neq 0$ gleich $(w/u : 1)$ ist.

Da nun die Operationen von c , a und m auf $P^1(\mathbf{F}_7)$ alle als Operationen von Elementen in $\text{PSL}_2(\mathbf{F}_7)$ geschrieben werden konnten, bleibt zu zeigen, daß $G = \langle c, a, m \rangle$. Da bereits $\langle c, a \rangle = N$ die Ordnung 21 hat und da $m \notin N$ aus Ordnungsgründen, ist der Index von $\langle c, a, m \rangle$ in G in $\{1, 2, 4\}$. Nun hat G aber keine Untergruppe U von Index $1 < [G : U] \leq 5$, da die transitive Operation von G auf G/U einen nichtverschwindenden und also injektiven Morphismus von G nach $\mathcal{S}_{[G:U]}$ lieferte, was wegen $|G| > |\mathcal{S}_5| \geq |\mathcal{S}_{[G:U]}|$ ausgeschlossen ist. Insbesondere ist der Index von $\langle c, n, m \rangle$ in G gleich 1.

Aufgabe 69.

Sei K ein Komplement von N in G , i.e. es sei $N \cap K = 1$ und $NK = G$. Dann ist $N \cap (H \cap K) = 1$ und

$N(H \cap K) = H \cap NK = H$ mit der ersten Bemerkung in §3.2.2, und also $H \cap K$ ein Komplement von N in H .

Bleibt zu zeigen, daß die Erweiterung

$$N \longrightarrow G \longrightarrow G/N$$

semidirekt ist, falls nur die Erweiterung

$$N \longrightarrow H \longrightarrow H/N$$

semidirekt ist.

Schreibe $\bar{G} := G/N$ und $\bar{H} := H/N$. Mit dem Satz aus §3.2.1 genügt es zu zeigen, daß

$$\mathrm{H}^2(\bar{G}, N) \xrightarrow{\mathrm{Res}_{\bar{H}}^{\bar{G}}} \mathrm{H}^2(\bar{H}, N)$$

injektiv ist; cf. das Lemma am Ende von §2.5.4 für die Tatsache, daß hier tatsächlich $\mathrm{Res}_{\bar{H}}^{\bar{G}}$ anzuwenden ist. Mit dem Satz aus §2.5.4 ist aber die Komposition

$$\mathrm{H}^2(\bar{G}, N) \xrightarrow{\mathrm{Res}_{\bar{H}}^{\bar{G}}} \mathrm{H}^2(\bar{H}, N) \xrightarrow{\mathrm{Tr}_{\bar{H}}^{\bar{G}}} \mathrm{H}^2(\bar{G}, N)$$

durch Multiplikation mit $[\bar{G} : \bar{H}] = [G : H]$ auf $\mathrm{H}^2(\bar{G}, N)$ gegeben. Diese Multiplikation gibt aber wegen $[G : H]$ teilerfremd zu $|N|$ einen Automorphismus von $\mathrm{H}^2(\bar{G}, N)$; cf. die Lösung zu Aufgabe 39 (3). Damit folgt die Injektivität des ersten Teilnehmers an dieser Komposition.

Die Voraussetzung N abelsch ist nicht entbehrlich; vgl. [?, I.18.7].

Die Aussage ist eine Verallgemeinerung des Korollars in §3.2.1, in welchem der Spezialfall $N = H$ behandelt wird. Ein ähnlicher Übergang zum nichtabelschen Fall, wie er von diesem Korollar in §3.2.1 zum Theorem von Schur-Zassenhaus in §3.2.2 durchgeführt wird, ist also in dieser Allgemeinheit nicht möglich. (Es bleibt natürlich dennoch die Frage, ob mit Schur-Zassenhaus bereits die maximale vom abelschen zum nichtabelschen Fall hebbare Aussage erreicht ist.)