G. Nebe, M. Künzer

Algebra I, WS 04/05

Lösung 7

Aufgabe 27.

(1) Es ist $|\operatorname{Syl}_p(G)| \in \{1, q\}$, und $|\operatorname{Syl}_q(G)| \in \{1, p\}$. Wäre $|\operatorname{Syl}_p(G)| = q$ und $|\operatorname{Syl}_q(G)| = p$, so wäre wegen $q \equiv_p 1$ und $p \equiv_q 1$ sowohl $q > p$ als auch $p > q$, was nicht der Fall sein kann. Also gibt es eine normale Sylowgruppe S. Da S und G/S zyklisch sind, ist G auflösbar.

(2) Es ist $|\operatorname{Syl}_p(G)| \in \{1, q\}$, und $|\operatorname{Syl}_q(G)| \in \{1, p, p^2\}$.

Ist $|\operatorname{Syl}_q(G)| = 1$, so ist die zyklische q-Sylowgruppe normal in G. Da auch der Quotient abelsch ist, ist G auflösbar.

Ist $|\operatorname{Syl}_q(G)| = p$, so erhalten wir im Fall $|\operatorname{Syl}_p(G)| = q$ den Widerspruch $p > q$ und $q > p$. Also ist $|\operatorname{Syl}_p(G)| = 1$, und wir haben eine normale p-Sylowgruppe, welche abelsch ist, und welche einen zyklischen Quotienten hat. Damit ist G auflösbar.

Ist $|\operatorname{Syl}_q(G)| = p^2$, so gibt es $p^2(q-1)$ Elemente der Ordnung q in G, und also höchstens p^2 Elemente, deren Ordnung eine p-Potenz ist. Also folgt diesenfalls, daß die p-Sylowgruppe normal ist. Da diese abelsch ist, und da der Quotient zyklisch ist, ist G auflösbar.

(3) Es ist $|\operatorname{Syl}_p(G)| \in \{1, q, q^2\}$, und $|\operatorname{Syl}_q(G)| \in \{1, p, p^2\}$. Wir können o.E. $p > q$ annehmen. Da dies $q \equiv_p 1$ ausschließt, ist $|\operatorname{Syl}_p(G)| \in \{1, q^2\}$.

Fall $|\operatorname{Syl}_p(G)| = 1$. Die p-Sylowgruppe ist normal in G. Da diese wie auch auch der Quotient abelsch ist, ist G auflösbar.

Fall $|\operatorname{Syl}_p(G)| = q^2$. Es ist $q^2 \equiv_p 1$, d.h. p ist ein Teiler von $(q-1)(q+1)$. Da $p > q$, folgt $p = q+1$, und somit $p = 3$, $q = 2$, $|G| = 2^2 3^2 = 36$ sowie $|\operatorname{Syl}_3(G)| = 4$. Damit haben wir einen Morphismus $G \xrightarrow{\varphi} \mathcal{S}_{\operatorname{Syl}_3(G)} \simeq \mathcal{S}_4$ mit $\varphi(G) \neq 1$, da $\operatorname{Syl}_3(G)$ als transitiv bekannt ist. Es ist $\mathcal{S}_4$ auflösbar, wie aus 20 (3) und 20 (1) folgt. Damit ist auch $\varphi(G)$ als Untergruppe einer auflösbaren Gruppe selbst auflösbar. Da $|\operatorname{Kern}\varphi| \in \{1, p, p^2, q, q^2, pq, p^2q, pq^2\}$, ist $\operatorname{Kern}\varphi$ abelsch ist oder nach (1) oder (2) auflösbar. Also ist auch G auflösbar.

Gruppen der Ordnung $p^a q^b$ sind auflösbar für $a, b \geq 0$ beliebig. Das ist der Inhalt eines Theorem von Burnside, welches mit Hilfe der gewöhnlichen Darstellungstheorie (i.e. der Theorie der Gruppenmorphismen $G \longrightarrow \mathrm{GL}_n(\mathbf{C})$) gezeigt werden kann. Genauer: welches historisch den Ausgangspunkt der Darstellungstheorie darstellt.

Auch sind Gruppen ungerader Ordnung auflösbar. Das ist ein Satz von Feit und Thompson von 1963.

Aufgabe 28.

(1) Sei G eine einfache nichtabelsche Gruppe von Ordnung $|G| \leq 96$. Insbesondere ist G nicht auflösbar. Denn wäre G auflösbar, so gäbe es $N \lhd G$ mit G/N abelsch; da notwendig $N = 1$, folgte hieraus G abelsch.

Da p-Gruppen auflösbar sind, ist $|G|$ keine Potenz einer Primzahl. Mit Aufgabe 27 wissen wir damit, daß

$$|G| \in \{24, 30, 40, 42, 48, 54, 56, 60, 66, 70, 72, 78, 80\}\,.$$

Bemerken wir noch, daß eine transitive G-Menge M einen nichttrivialen Gruppenmorphismus $G \longrightarrow \mathcal{S}_M$ liefert, der *wegen G einfach* den Kern 1 haben und daher injektiv sein muß.

Ist $|G| = 60$, so ist G nach 18 (8) isomorph zu $\mathcal{A}_5$. In jedem der folgenden Fälle haben wir einen Widerspruch herzuleiten.

$|G| = 24$ Es ist $|\operatorname{Syl}_2(G)| = 3$, was einen injektiven Gruppenmorphismus $G \hookrightarrow \mathcal{S}_3$ liefert, was nicht geht.

$|G| = 30$ Es ist $|\operatorname{Syl}_5(G)| = 6$ und $|\operatorname{Syl}_3(G)| = 10$. Damit gibt es $6 \cdot 4$ Elemente der Ordnung 5 und $10 \cdot 2$ Elemente der Ordnung 3, was nicht geht.

$|G| = 40$ Da die 5-Sylowgruppe nicht normal ist, und keine weitere Möglichkeit besteht, ist ein Widerspruch erreicht.

$|G| = 42$ Da die 7-Sylowgruppe nicht normal ist, und keine weitere Möglichkeit besteht, ist ein Widerspruch erreicht.

$|G| = 48$ Es ist $|\operatorname{Syl}_2(G)| = 3$, was einen injektiven Gruppenmorphismus $G \hookrightarrow \mathcal{S}_3$ liefert, was nicht geht.

$|G| = 54$ Da die 3-Sylowgruppe nicht normal ist, und keine weitere Möglichkeit besteht, ist ein Widerspruch erreicht

$|G| = 56$ Wegen $|\operatorname{Syl}_7(G)| = 8$ gibt es $8 \cdot 6$ Elemente der Ordnung 7, woraus $|\operatorname{Syl}_2(G)| = 1$ folgt, was nicht geht.

$|G| = 66$ Da die 11-Sylowgruppe nicht normal ist, und keine weitere Möglichkeit besteht, ist ein Widerspruch erreicht.

$|G| = 70$ Da die 7-Sylowgruppe nicht normal ist, und keine weitere Möglichkeit besteht, ist ein Widerspruch erreicht.

$|G| = 72$ Es ist $|\operatorname{Syl}_3(G)| = 4$, was einen injektiven Gruppenmorphismus $G \hookrightarrow \mathcal{S}_4$ liefert, was nicht geht.

$|G| = 78$ Da die 13-Sylowgruppe nicht normal ist, und keine weitere Möglichkeit besteht, ist ein Widerspruch erreicht.

$|G| = 80$ Es ist $|\operatorname{Syl}_2(G)| = 5$, was einen injektiven Gruppenmorphismus $G \hookrightarrow \mathcal{S}_5$ liefert, was nicht geht, da $|G|$ kein Teiler von $|\mathcal{S}_5|$ ist.

Jede nichtabelsche Gruppe von Ordnung ≤ 167 ist nicht einfach oder isomorph zu $\mathcal{A}_5$.

(2) Angenommen, es sei

$$M := \{G \text{ Gruppe} : |G| \leq 80, G \text{ nicht auflösbar}, G \not\simeq \mathcal{A}_5\} \neq \emptyset .$$

Sei H ein Element minimaler Ordnung von M.

Mit (1) ist H als nicht einfach bekannt. Sei $1 < N \lhd H$. Da H nicht auflösbar ist, ist N oder H/N nicht auflösbar.

Ferner sind $|N|$ und $|H/N|$ echte Teiler von $|H|$. Insbesondere sind $|N| \leq 40$ und $|H/N| \leq 40$. Damit sind aus Ordnungsgründen weder N noch H/N isomorph zu $\mathcal{A}_5$.

Also ist N oder H/N in M enthalten. Dies widerspricht der minimalen Wahl von H.

Jede Gruppe von Ordnung ≤ 119 ist auflösbar oder isomorph zu $\mathcal{A}_5$.

Aufgabe 29.

(1) Da G nicht abelsch ist, ist $|\mathrm{Z}(G)| \neq p^3$. Da G eine p-Gruppe ist, ist $|\mathrm{Z}(G)| \neq 1$. Wäre $|\mathrm{Z}(G)| = p^2$, so wäre $G/\mathrm{Z}(G)$ von Ordnung p, also zyklisch, und G mithin abelsch, was nicht der Fall ist (und unter der Voraussetzung $|\mathrm{Z}(G)| = p^2$ sowieso nicht sein darf). Also bleibt nur $|\mathrm{Z}(G)| = p$ möglich, und das bedeutet $\mathrm{Z}(G) \simeq C_p$.

Berechnen wir die Kommutatorreihe. Es ist $|G/\mathrm{Z}(G)| = p^2$, also $G/\mathrm{Z}(G)$ abelsch (22 (1)), und mithin $G' \leq \mathrm{Z}(G)$. Da G nicht abelsch ist, ist $G' \neq 1$. Also ist $G' = \mathrm{Z}(G)$, und $G'' = 1$. Die Kommutatorreihe hat die Gestalt

$$G \geq G' = \mathrm{Z}(G) \geq G'' = 1 .$$

(2) Sei $\mathrm{Z}(G) = \langle z \rangle$, und sei $x \in G \setminus \mathrm{Z}(G)$. Da z mit x vertauscht, und x von Ordnung p ist, hat $N := \langle z, x \rangle = \langle z \rangle \langle x \rangle$ höchstens p^2 Elemente, und da $x \notin \langle z \rangle$ liegt, sogar genau p^2 Elemente. Es ist N mithin abelsch nach 22 (1). Da $\langle z \rangle \cap \langle x \rangle = 1$, folgt $N \simeq C_p \times C_p$. Mit 18 (2) ist N in der Tat ein Normalteiler in G.

Sei $y \in G \setminus N$. Wegen $y^p = 1$ ist $N \cap \langle y \rangle = 1$. Da aus Ordnungsgründen auch $N \cdot \langle y \rangle = G$ gilt, ist $\langle y \rangle$ ein Komplement zu N in G.

(3) Sei b ein Element von G von Ordnung p^2. Dann ist $N := \langle b \rangle$ ein Normalteiler in G wegen 18 (2).

Sei nun angenommen, es habe N kein Komplement in G. Sei $c \in G \setminus N$. Wäre c von Ordnung p, so wäre $\langle c \rangle$ ein Komplement von N in G. Also ist c von Ordnung p^2. Da die Ordnung von G kleiner p^4 ist, ist $\langle b \rangle \cap \langle c \rangle \neq 1$. Dies ist wegen $\langle b \rangle \neq \langle c \rangle$ nur möglich, falls $c^{tp} = b^p$ für ein $t \geq 1$ teilerfremd zu p. Ersetzen wir c durch c^t, so ist $c^p = b^p$.

Da $G = \langle b, c \rangle$, da $b^p = c^p$ mit b und c vertauscht, und da b^p die Ordnung p hat, ist $\mathrm{Z}(G) \simeq \langle b^p \rangle$ mit (1).

Da $N \trianglelefteq G$, ist $c^{-1}bc \in \langle b \rangle$. Schreiben wir $c^{-1}bc = b^k$ für ein $k \in \mathbf{Z}$.

Mit (1) ist $[b, c] \in G' = \mathrm{Z}(G) = \langle b^p \rangle$. Ausgeschrieben heißt dies,

$$[b, c] = b^{-1}c^{-1}bc = b^{k-1} = b^{pt}$$

für ein $t \in \mathbf{Z}$. Folglich ist $k - 1 \equiv_{p^2} pt$, und also $k \equiv_p 1$.

Berechnen wir nun

$$(bc^{-1})^p = bc^{-1}bc^{-1} \cdots bc^{-1} = b^{1+k+\cdots+k^{p-1}} c^{-p} = b^{1+k+\cdots+k^{p-1}-p} = b^{\frac{k^p-1}{k-1}-p} .$$

Da $k \equiv_p 1$, können wir $k = 1 + pk'$ mit einem $k' \in \mathbf{Z}$ schreiben. Wäre $k' \equiv_p 0$, so wäre $[b, c] = 1$, und G mithin abelsch, was nicht der Fall ist. Also ist $k' \not\equiv_p 0$.

Wegen $p \geq 3$ ist nun

$$(1+pk')^p - 1 \equiv_{p^3} (1 + \tbinom{p}{1} pk') - 1 = p^2 k'$$

und somit der fragliche Exponent

$$\frac{k^p - 1}{k-1} - p = \frac{(1+pk')^p - 1}{k'p} - p \equiv_{p^2} 0 .$$

Es folgt $(bc^{-1})^p = 1$. Da $b \neq c$, ist bc^{-1} somit von Ordnung p. Also ist $\langle bc^{-1} \rangle$ ein Komplement von N in G, und wir haben einen Widerspruch.

> Die Quaternionengruppe Q_8 zeigt, daß nicht nur das Argument, sondern auch die Schlußfolgerung im Falle $p = 2$ versagt. Denn darin gibt es ein Element von Ordnung 4, dessen Erzeugnis zwar ein Normalteiler ist, aber kein Komplement hat. Vgl. 20 (2).

(4) Betrachten wir den **Fall,** in welchem G nur Elemente von Ordnung p hat. Nach (2) ist G isomorph zu $(\langle z \rangle \times \langle x \rangle) \rtimes \langle y_0 \rangle$, wobei z zentral ist. Hierbei schreiben wir y_0 statt y wie in (2), aus einem Grund, der weiter unten ersichtlich wird.

Identifizieren wir $\mathrm{Aut}(\langle z \rangle \times \langle x \rangle)$ mit $\mathrm{GL}_2(\mathbf{F}_p)$, indem wir eine Matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ mit der Operation $z \longmapsto z^a x^c$, $x \longmapsto z^b x^d$ identifizieren, so sehen wir, daß unter dem Morphismus $\langle y_0 \rangle \longrightarrow \mathrm{Aut}(\langle z \rangle \times \langle x \rangle)$ wegen $z \in \mathrm{Z}(G)$ das Element y_0 auf eine Matrix der Form $\left(\begin{smallmatrix} 1 & b \\ 0 & c \end{smallmatrix}\right)$ abgebildet wird.

Da $y_0^p = 1$, muß auch $c^p = 1$ in $\mathbf{F}_p$ gelten, und folglich $c = 1$ sein. Somit kommt y_0 auf eine Matrix der Form $\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right)$, mit $b \in \mathbf{F}_p \smallsetminus \{0\}$, da G nicht abelsch ist.

Sei $b' \in \mathbf{F}_p$ so, daß darin $bb' = 1$ (i.e. $bb' \equiv_p 1$, wenn man mit Repräsentanten rechnet), und sei $y := y_0^{b'}$. Es ist $\langle y \rangle = \langle y_0 \rangle$. Ferner wird y auf $\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right)^{b'} = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ abgebildet.

Damit erhalten wir einen surjektiven Morphismus

$$\begin{array}{rcl} \langle \hat{z}, \hat{x}, \hat{y} \mid \hat{z}^p, \hat{x}^p, \hat{y}^p, [\hat{z}, \hat{x}], {}^{\hat{y}}\hat{z} \cdot \hat{z}^{-1}, {}^{\hat{y}}\hat{x} \cdot (\hat{x}\hat{z})^{-1} \rangle & \longrightarrow & G \\ \hat{z} & \longmapsto & z \\ \hat{x} & \longmapsto & x \\ \hat{y} & \longmapsto & y . \end{array}$$

In der Gruppe auf der linken Seite kann jedes Element in der Form $\hat{z}^a \hat{x}^b \hat{y}^c$ mit $a, b, c \in [0, p-1]$ geschrieben werden. Somit enthält die linke Seite $\leq p^3$ Elemente.

Existiert überhaupt eine nichtabelsche Gruppe von Ordnung p^3, in welcher alle Elemente in $G \smallsetminus \{1\}$ die Ordnung p haben, so folgt mit der angegebenen Surjektion, daß auch die linke Seite Ordnung p^3 hat, und daß mithin ein Isomorphismus vorliegt.

Dies dürfen wir als gegeben annehmen, da ansonsten der vorliegende Fall nicht eintritt. Er tritt aber ein, wie wir kurz begründen wollen.

Hierzu können wir aber drei Kopien von C_p heranziehen, sagen wir, unter Mißbrauch der Elementbezeichnungen, $\langle z \rangle$, $\langle x \rangle$ und $\langle y \rangle$, und das semidirekte Produkt $(\langle z \rangle \times \langle x \rangle) \rtimes \langle y \rangle$ mittels $y \longmapsto \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ konstruieren. Es ist darin

$$\Big((z^a, x^b), y^c\Big)^p = \Big({}^{y^{0\cdot c}}(z^a, x^b) \cdot {}^{y^{1\cdot c}}(z^a, x^b) \cdots {}^{y^{(p-1)\cdot c}}(z^a, x^b), \underbrace{y^{pc}}_{=1}\Big)$$

für $a, b, c \in \mathbf{Z}/p\mathbf{Z}$ beliebig. Werten wir dies weiter aus. Da wegen $p \geq 3$

$$\left(\begin{smallmatrix} 1 & 0\cdot c \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} a \\ b \end{smallmatrix}\right) + \left(\begin{smallmatrix} 1 & 1\cdot c \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} a \\ b \end{smallmatrix}\right) + \cdots + \left(\begin{smallmatrix} 1 & (p-1)\cdot c \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} a \\ b \end{smallmatrix}\right) = \left(\begin{smallmatrix} p & cp(p-1)/2 \\ 0 & p \end{smallmatrix}\right)\left(\begin{smallmatrix} a \\ b \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} a \\ b \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 \\ 0 \end{smallmatrix}\right) ,$$

folgt in der Tat $\Big((z^a, x^b), y^c\Big)^p = \Big((z^0, x^0), 1\Big) = 1$.

Die Gruppe ist nichtabelsch, da der definierende Morphismus in die Automorphismengruppe nicht jedes Element auf die Identität schickt.

Ende der Begründung.

Alternative Begründung (kurz). Man verwende die p-Sylowgruppe $G = \{\left(\begin{smallmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{smallmatrix}\right)\} \leq \mathrm{GL}_3(\mathbf{F}_p)$.

Um schließlich in Übereinstimmung zur Aufgabenstellung zu kommen, wechseln wir die Notation für die Erzeuger und schreiben z für $\hat{z}$ etc.

Betrachten wir nun noch den **Fall,** in welchem es ein Element der Ordnung p^2 in G gibt. Mit (3) ist $G \simeq \langle b\rangle \rtimes \langle x_0\rangle$ mit einem Element x_0 von Ordnung p. Es wird x_0 unter dem Morphismus $\langle x_0\rangle \longrightarrow \mathrm{Aut}(\langle b\rangle)$ auf den Automorphismus $b \longmapsto b^s$ geschickt, für ein $s \in \mathbf{Z}$ mit $s^p \equiv_{p^2} 1$, da $x_0^p = 1$. Da a fortiori $s^p \equiv_p 1$, ist $s \equiv_p 1$, d.h. $s = 1 + pt$ für ein $t \in [0, p-1]$. Wir können noch $t = 0$ ausschließen, da G nichtabelsch ist. Sei $t' \in \mathbf{Z}$ mit $t't \equiv_p 1$. Dann wird $x := x^{t'}$ auf den Automorphismus $b \longmapsto b^{(1+pt)^{t'}} = b^{1+ptt'} = b^{1+p}$ geschickt.

Damit erhalten wir einen surjektiven Morphismus

$$\begin{array}{rcl} \langle \hat{b},\, \hat{x} \,|\, \hat{b}^{b^2},\, \hat{x}^p,\ {}^{\hat{x}}\hat{b} \cdot \hat{b}^{-(1+p)} \rangle & \longrightarrow & G \\ \hat{b} & \longmapsto & b \\ \hat{x} & \longmapsto & x\,. \end{array}$$

In der Gruppe auf der linken Seite kann jedes Element in der Form $\hat{b}^s\hat{x}^t$ mit $s \in [0, p^2-1]$ und $t \in [0, p-1]$ geschrieben werden. Somit enthält die linke Seite $\leq p^3$ Elemente.

Existiert überhaupt eine nichtabelsche Gruppe von Ordnung p^3, in welcher es ein Element von Ordnung p^2 gibt, so folgt mit der angegebenen Surjektion, daß auch die linke Seite Ordnung p^3 hat, und daß mithin ein Isomorphismus vorliegt.

Dies dürfen wir als gegeben annehmen, da ansonsten der vorliegende Fall nicht eintritt. Er tritt aber ein, wie wir kurz begründen wollen.

Seien hierzu C_{p^2} erzeugt von einem Element b und C_p erzeugt von einem Element x herangezogen, wieder unter Mißbrauch der Elementbezeichnungen, und das semidirekte Produkt $\langle b\rangle \rtimes \langle x\rangle$ mittels $x \longmapsto (b \longmapsto b^{1+p})$ gebildet. Darin hat etwa $(b, 1)$ die Ordnung p^2. Die Gruppe ist nichtabelsch, da der definierende Morphismus in die Automorphismengruppe nicht jedes Element auf die Identität schickt. Ende der Begründung.

Um schließlich in Übereinstimmung zur Aufgabenstellung zu kommen, wechseln wir die Notation für die Erzeuger und schreiben b für $\hat{b}$ etc.

Die beiden Isomorphietypen der nichtabelschen Gruppen von Ordnung p^3 heißen *extraspeziell.* Übliche Bezeichnungen sind $p_+^{1+2} := (C_p \times C_p) \rtimes C_p$ und $p_-^{1+2} := (C_{p^2}) \rtimes C_p$.

Aufgabe 30.

(1) Aussage ist falsch. Sei $p \geq 3$ prim beliebig, sei $G := \langle z,\, x,\, y \,|\, z^p,\, x^p,\, [z,x],\ {}^{y}z \cdot z^{-1},\ {}^{y}x \cdot (xz)^{-1}\rangle$ wie in 29 (4) und sei $H = C_p \times C_p \times C_p$. Nach Lösung von 29 (4) ist $|G| = |H| = p^3$. Sei φ eine Bijektion von G nach H, welche 1_G nach 1_H schickt, und welche ansonsten beliebig gewählt sei.

Da sowohl jedes Element von $G \smallsetminus \{1\}$ als auch jedes Element von $H \smallsetminus \{1\}$ Ordnung p hat, ist dann $|\langle\varphi(g)\rangle| = |\langle g\rangle|$ für alle $g \in G$.

Dahingegen ist $G \not\simeq H$, da G nichtabelsch, H aber abelsch ist.

(2) Aussage ist richtig. Es genügt zu zeigen, daß G/G' unendlich ist. Bilden wir hierzu die ganzzahlige Matrix, deren Zeilen mit den Erzeugern indiziert sind, und in deren Spalten die Exponententupel der Relatoren stehen. Diese Matrix ist nun in $\mathbf{Z}^{s\times t}$, wobei $s > t \geq 0$. Die Elementarteilerform dieser Matrix enthält also wenigstens eine Nullzeile. Somit gibt es wenigstens einen direkten $\mathbf{Z}$-linearen Summanden von G/G' isomorph zu $\mathbf{Z}$. Damit kann G/G' nicht endlich sein.