Musterlösung 13

p-Gruppen, Sylowsätze, Kleine endliche Gruppen

Sei p eine Primzahl.

1. (a) Zeige, dass jede echte Untergruppe einer endlichen p-Gruppe echt in ihrem Normalisator enthalten ist.

   (b) Zeige, dass jede p-Gruppe nilpotent ist.

   Lösung: (a) Sei H eine echte Untergruppe einer endlichen p-Gruppe G. Wir beweisen die Behauptung mit Induktion über $|G|$, nehmen also an, dass die Behauptung für Gruppen von kleinerer Ordnung richtig ist.

   Weil H eine echte Untergruppe ist, ist G nicht trivial. Daher ist das Zentrum $Z(G)$ nicht trivial (siehe Vorlesung). Da die Elemente von $Z(G)$ mit allen Elementen in G kommutieren, ist $Z(G)$ im Normalisator $N_G(H)$ von H enthalten. Falls $Z(G) \not\subset H$ ist, gibt es somit ein Element in $N_G(H)$, das nicht in H liegt. Dann ist also H echt in $N_G(H)$ enthalten.

   Es bleibt der Fall $Z(G) \subset H$ zu betrachten. In diesem Fall ist $H/Z(G)$ eine echte Untergruppe von $G/Z(G)$, wobei $G/Z(G)$ von kleinerer Ordnung als G ist. Daher ist nach Induktionsvoraussetzung $H/Z(G)$ echt in seinem Normalisator enthalten. Diesen können wir als $N/Z(G)$ schreiben für eine Untergruppe N von G, die H echt enthält. Nach dem ersten Isomorphiesatz ist H normal in N, da $H/Z(G)$ normal in seinem Normalisator $N/Z(G)$ ist. Es folgt somit $H \subsetneq N \subset N_G(H)$.

   (b) Consider the ascending central series $1 = Z_0 \lhd Z_1 \lhd \ldots$, defined in Serie 12, Aufgabe 3 as follows: $Z_0 := 1$ and

   $$Z_{i+1} := \{z \in G \mid \forall g \in G\colon [g, z] \in Z_i\}.$$

   We claim that for all i such that $Z_i \neq G$, we have $|Z_i| < |Z_{i+1}|$. For such i it follows that G/Z_i is a non-trivial p-group and thus has non-trivial center. From the definition we see that Z_{i+1} consists exactly of the elements sent to $Z(G/Z_i)$ by the quotient homomorphism $G \to G/Z_i$. In other words, this restricts to a surjective homomorphism $Z_{i+1} \twoheadrightarrow Z(G/Z_i)$ with kernel Z_i. Thus $|Z_{i+1}| = |Z(G/Z_i)| \cdot |Z_i|$. Since $|Z(G/Z_i)| > 1$, the claim follows.

   As the Z_i form an increasing sequence of subgroups of G and $|G|$ is finite, there must exist an n such that $Z_n = G$. Then G is nilpotent by Serie 12, Aufgabe 3b.

2. (a) Sei G eine p-Gruppe, die auf einer endlichen Menge X operiert, mit der Fixpunktmenge $X^G := \{x \in X \mid \forall g \in G\colon gx = x\}$. Zeige $|X| \equiv |X^G| \mod (p)$.

(b) Sei K ein endlicher Körper der Ordnung p^m, und sei $G < \mathrm{GL}_n(K)$ eine p-Gruppe. Sei $U < \mathrm{GL}_n(K)$ die Gruppe aller oberen Dreiecksmatrizen mit Diagonaleinträgen 1. Zeige, dass ein $h \in \mathrm{GL}_n(K)$ existiert mit $hGh^{-1} < U$.

Lösung:

(a) Write $|G| = p^n$, and let $\mathcal{R}$ be a system of representatives for the orbits of the action of G on X. Each fixed point is the unique representative of its orbit, so $X^G \subset \mathcal{R}$. The length of any orbit is a divisor of $|G|$ and hence a power of p. Thus for any $x \in \mathcal{R} \smallsetminus X^G$ we have $|Gx| \equiv 0 \bmod p$. We thus have

$$\begin{aligned} |X| \;&=\; \sum_{x\in\mathcal{R}} |Gx| \;\equiv\; \sum_{x\in X^G} |Gx| \mod (p) \\ &=\; \sum_{x\in X^G} 1 \;=\; |X^G|. \end{aligned}$$

(b) We prove this by induction on n. For $n = 0$ the statement holds trivially. For $n > 0$ consider the action of G on K^n by multiplication. Since $|(K^n)| = p^{mn}$ with $mn \geqslant 1$, part (a) implies that the number of fixed points is congruent to 0 modulo p. Since $0 \in K^n$ is already a fixed point, it follows that there also exists a fixed point $v \in K^n \smallsetminus \{0\}$. Choose $A \in \mathrm{GL}_n(K)$ with $Av = e_1$. Then for any $g \in G$ we have

$$({}^A g)(e_1) = (AgA^{-1})(Av) = Agv = Av = e_1.$$

Thus e_1 is a fixed point of the subgroup ${}^A G < \mathrm{GL}_n(K)$. Equivalently ${}^A G$ consists of block triangular matrices of the form

$$\begin{pmatrix} 1 & * \\ 0 & g' \end{pmatrix}, \;\; g' \in \mathrm{GL}_n(K).$$

Let $G' < \mathrm{GL}_{n-1}(K)$ be the image of ${}^A G$ under the projection to the lower right block. By the induction hypothesis there exists $h' \in \mathrm{GL}_{n-1}(K)$ such that ${}^{h'}G'$ is contained in the subgroup $U' < \mathrm{GL}_{n-1}(K)$ of all upper triangular matrices with diagonal entries 1. With

$$h \;:=\; \begin{pmatrix} 1 & 0 \\ 0 & h' \end{pmatrix} \cdot A \;\in \mathrm{GL}_n(K)$$

a direct calculation shows that ${}^h G < U$.

*3. Sei G eine Gruppe und P eine p-Sylowuntergruppe von G. Zeige für beliebige Untergruppen H von G:

$$N_G(P) < H \implies H = N_G(H).$$

Lösung: Sei $H < G$ eine Untergruppe mit $N_G(P) < H$. Die Inklusion $H \subset N_G(H)$ gilt bereits nach Konstruktion. Für die Umkehrung betrachte ein beliebiges $x \in N_G(H)$. Wegen $P < N_G(P) < H$ gilt dann

$$xPx^{-1} < xHx^{-1} = H.$$

Nun ist $|P| = |xPx^{-1}|$ die maximale p-Potenz in $|G|$, also a fortiori auch in dessen Teiler $|H|$. Somit sind P und xPx^{-1} beides p-Sylowuntergruppen von H. Nach den Sylowsätzen existiert deshalb ein $h \in H$ mit

$$P = hxPx^{-1}h^{-1}.$$

Somit liegt hx in $N_G(P)$, also nach Voraussetzung in H, und es folgt $x = h^{-1}(hx) \in H$. Daher gilt die umgekehrte Inklusion $H \supset N_G(H)$.

4. Zeige, dass jede endliche Gruppe der Ordnung pqr für paarweise verschiedene Primzahlen p, q, r auflösbar ist.

   Lösung: Sei G eine Gruppe der Ordnung pqr. Wir nehmen o.B.d.A. $p < q < r$ an. Nach den Sylowsätzen ist die Anzahl der r-Sylowgruppen kongruent zu 1 modulo r und ein Teiler von pq. Wegen $p < q < r$ kommen dafür nur 1 und pq in Frage.

   Falls es nur eine r-Sylowuntergruppe H gibt, ist diese normal. Dann ist H als zyklische Gruppe von Primzahlordnung auflösbar und G/H als Gruppe der Ordnung pq ebenfalls auflösbar. Deshalb ist in diesem Fall G auflösbar.

   Im Folgenden nehmen wir an, dass die Anzahl der r-Sylowuntergruppen gleich pq ist. Der Schnitt von zwei verschiedenen r-Sylowuntergruppen von G ist trivial, da dessen Ordnung die Primzahl r echt teilen muss. Zudem hat jedes nicht-triviale Element einer r-Sylowuntergruppe die Ordnung r und jedes Element von G der Ordnung r liegt in einer r-Sylowuntergruppe. Daher hat G genau $pq(r-1)$ Elemente der Ordnung r.

   Die Anzahl q-Sylowuntergruppen von G ist kongruent zu 1 modulo q und ein Teiler von pr. Wegen $p < q < r$ gibt es dafür höchstens die Möglichkeiten 1, r und pr. Falls es nur eine q-Sylowuntergruppe gibt, ist diese normal und es folgt wie oben, dass G auflösbar ist. Andernfalls hat G nach obigem Argument genau $r(q-1)$ bzw. $pr(q-1)$ Elemente der Ordnung q. Das ist aber nicht möglich, da bereits $pq(r-1)$ Elemente die Ordnung r haben und

   $$pq(r-1) + r(q-1) \geqslant pq(r-1) + rp = pqr + p(r-q) > pqr = |G|$$

   gilt. Somit ist jede Gruppe der Ordnung pqr auflösbar.

5. (a) Zeige, dass jede endliche Gruppe G mit einer nicht-trivialen zyklischen 2-Sylowuntergruppe eine normale Untergruppe vom Index 2 hat.

   Hinweis: Betrachte G als Untergruppe von $S(G)$ nach dem Satz von Cayley und achte auf das Vorzeichen.

   (b) Folgere daraus, dass eine nicht abelsche endliche Gruppe der Ordnung $\equiv 2 \bmod 4$ nicht einfach sein kann.

Lösung:

(a) Wie im Beweis des Satzes von Cayley betrachten wir die Operation von G auf G durch Linkstranslation, welche einem injektiven Homomorphismus

$$\begin{aligned} \ell\colon G &\longrightarrow S(G) \\ x &\longmapsto \ell_x\colon g \mapsto xg \end{aligned}$$

entspricht. Nach Voraussetzung hat G eine nicht-triviale zyklische 2-Sylowuntergruppe $P = \langle x \rangle$. Es ist also $|P| = 2^m$ für ein $m > 0$ und $|G| = 2^m q$ mit q ungerade. Jede Bahn von $\langle x \rangle$ hat dann die Form Pg für ein $g \in G$ und folglich die Kardinalität $|Pg| = |P| = 2^m$. Das Element $\ell_x \in S(G)$ ist daher ein Produkt von q disjunkten 2^m-Zykeln. Als Zykeln gerader Länge sind diese 2^m-Zykel ungerade, und da auch q ungerade ist, folgt

$$\operatorname{sgn}(\ell_x) = (-1)^q = -1.$$

Darum ist der zusammengesetzte Homomorphismus $\operatorname{sgn} \circ \ell : G \to \{\pm 1\}$ surjektiv und sein Kern nach dem Homomorphiesatz eine normale Untergruppe vom Index 2 in G.

(b) Sei G eine nicht abelsche Gruppe der Ordnung $n \equiv 2 \bmod 4$. Jede 2-Sylowgruppe einer solchen Gruppe hat die Ordnung 2 und ist daher zyklisch. Somit hat G nach a) eine normale Untergruppe vom Index 2. Diese ist nicht trivial, da G als nicht abelsche Gruppe nicht die Ordnung 2 haben kann. Daher ist G nicht einfach.

6. Zeige, dass jede Gruppe der Ordnung 561 zyklisch ist.

   Hinweis: Zeige zunächst, dass es einen zyklischen Normalteiler N der Ordnung $11 \cdot 17$ gibt. Beweise und benutze dann, dass die Ordnung von $\operatorname{Aut}(N)$ nicht durch 3 teilbar ist.

   Lösung: Sei G eine Gruppe der Ordnung $561 = 3 \cdot 11 \cdot 17$. Wir zeigen zuerst, dass G eine zyklische normale Untergruppe der Ordnung $11 \cdot 17$ enthält.

   Die Anzahl von 11-Sylowuntergruppen von G ist ein Teiler von $3 \cdot 17$ und kongruent zu 1 modulo 11. Dafür kommt nur 1 in Frage. Analog gibt es nur eine 17-Sylowuntergruppe von G, da die Anzahl von 17-Sylowuntergruppen von G ein Teiler von $3 \cdot 11$ und kongruent zu 1 modulo 17 ist. Somit hat G genau eine 11-Sylowuntergruppe P und genau eine 17-Sylowuntergruppe Q, die beide normal sind. Zudem sind P und Q als Gruppen von Primzahlordnung zyklisch.

   Da P und Q normal in G sind, ist auch $N := PQ$ eine normale Untergruppe von G, denn es gilt für alle $g \in G$

   $$gPQg^{-1} = (gPg^{-1})(gQg^{-1}) = PQ.$$

   Ausserdem ist der Schnitt von P und Q trivial, da 11 und 17 teilerfremd sind. Da P und Q beide normal in G sind, ist daher N isomorph zum direkten Produkt

$P \times Q$ der zyklischen Gruppen $P \cong Z_{11}$ und $Q \cong Z_{17}$. Dieses ist zyklisch, da für Erzeuger x von P und y von Q die Ordnung des Elements $(x, y) \in P \times Q$ gleich $\mathrm{kgV}(11, 17) = 11 \cdot 17 = |P \times Q|$ ist.

Sei nun R eine 3-Sylowuntergruppe von G, die als Gruppe der Ordnung 3 isomorph zur zyklischen Gruppe Z_3 ist. Der Schnitt von R und N ist trivial, da 3 und $11 \cdot 17$ teilerfremd sind. Da N ein Normalteiler ist und $|N| \cdot |R| = |G|$ gilt, ist deshalb G isomorph zum semidirekten Produkt $N \rtimes_\varphi R$ bezüglich dem Homorphismus $\varphi : R \to \mathrm{Aut}(N)$, der zur Operation von R auf N durch Konjugation gehört.

Wir betrachten nun $\mathrm{Aut}(N)$ für die zyklische Gruppe $N = \langle z \rangle \cong Z_{187}$. Ein Homomorphismus von N nach N ist durch das Bild vom Erzeuger z eindeutig bestimmt und ist genau dann ein Automorphismus, wenn z auf einen Erzeuger von N abgebildet wird. Ein Element $z^i \in N$ mit $1 \leqslant i < 187$ ist genau dann ein Erzeuger, wenn i teilerfremd zu 187 ist. Ein i mit $1 \leqslant i < 187$ ist ganau dann teilerfremd zu 187, wenn es weder von der Form $17j$ mit $1 \leqslant j < 11$ noch von der Form $11k$ mit $1 \leqslant k < 17$ ist. Daher ist

$$|\mathrm{Aut}(N)| = 186 - 10 - 16 = 160.$$

Da 160 nicht durch 3 teilbar ist, kann somit $\mathrm{Aut}(N)$ keine Untergruppe der Ordnung 3 haben. Das Bild $\varphi(R)$ von φ kann also nicht die Ordnung 3 haben und muss daher als Faktorgruppe von $R \cong Z_3$ trivial sein. Somit ist φ trivial und G isomorph zum direkten Produkt $N \times R \cong Z_{187} \times Z_3$. Da 187 und 3 teilerfremd sind, folgt mit dem gleichen Argument wie für $P \times Q$, dass $N \times R \cong G$ zyklisch ist.

*7. Zeige, dass jede Gruppe der Ordnung $2^2 \cdot 3 \cdot 7 \cdot 13 \cdot 17$ eine normale Untergruppe der Ordnung 17 hat.

Hinweis: Finde eine 13-Sylowgruppe P und eine 17-Sylowgruppe Q von G mit $Q \subset N_G(P)$ und betrachte dann $N_G(Q)$.

Lösung: Sei G eine Gruppe der Ordnung $2^2 \cdot 3 \cdot 7 \cdot 13 \cdot 17$. Nach den Sylowsätzen ist die Anzahl von 13-Sylowgruppen von G ein Teiler von $2^2 \cdot 3 \cdot 7 \cdot 17$ und kongruent zu 1 modulo 13. Nachrechnen ergibt dafür nur die Möglichkeiten 1 und 14. Analog liefert Nachrechnen die Möglichkeiten 1, $4 \cdot 13$ und $3 \cdot 7 \cdot 13$ für die Anzahl von 17-Sylowgruppen von G.

Sei nun P eine beliebige 13-Sylowgruppe von G. Der Normalisator $N_G(P)$ von P ist gleich dem Stabilisator von P bezüglich der Aktion von G durch Konjugation auf der Menge der 13-Sylowgruppen von G. Da diese Operation nach den Sylowsätzen transitiv ist, ist der Index $[G : N_G(P)]$ gleich der Anzahl von 13-Sylowgruppen. Nach obiger Rechnung ist also $[G : N_G(P)]$ nicht durch 17 teilbar. Da aber 17 ein Teiler von der Ordnung von G ist, muss darum $|N_G(P)|$ durch 17 teilbar sein. Eine 17-Sylowgruppe Q von $N_G(P)$ hat also Ordnung 17 und ist deshalb auch eine 17-Sylowgruppe von G. Wir haben also Untergruppen P und Q mit $P \cap Q = \{1\}$ und

$P \lhd N_G(P) > Q$. Nach dem zweiten Isomorphiesatz ist darum PQ eine Untergruppe von G der Ordnung $13 \cdot 17$.

Anwenden der Sylowsätze auf die Gruppe PQ ergibt nun wegen $13 \not\equiv 1 \bmod 17$, dass PQ nur eine 17-Sylowgruppe hat. Daher muss Q normal in PQ sein. Es gilt also $PQ \subset N_G(Q)$. Insbesondere ist darum die Ordnung von $N_G(Q)$ durch 13 teilbar und der Index $[G : N_G(Q)]$ nicht durch 13 teilbar. Letzterer Index ist aber nach obigem Argument genau gleich der Anzahl von 17-Sylowgruppen, für die nur 1, $4 \cdot 13$ oder $3 \cdot 7 \cdot 13$ in Frage kommen. Es folgt, dass $[G : N_G(Q)] = 1$ ist. Somit ist $N_G(Q) = G$ und Q normal in G. Die Gruppe G hat also eine normale Untergruppe der Ordnung 17.

**8. Zeige, dass die Ikosaedergruppe, das heisst die Gruppe aller Drehsymmetrien eines regelmässigen Ikosaeders, isomorph zu A_5 ist.