Musterlösung Serie 19

Sylowsätze und Gruppen kleiner endlicher Ordnung

1. 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.

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

   Lösung: Sei G eine Gruppe der Ordnung $561 = 3 \cdot 11 \cdot 17$.

   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.

Sei nun R eine 3-Sylowuntergruppe von G, die als Gruppe der Ordnung 3 isomorph zur zyklischen Gruppe Z_3 ist. Weil P und Q normale Untergruppen sind, operiert R durch Konjugation auf ihnen. Diese Operation entspricht einem Homomorphismus $R \to \mathrm{Aut}(P)$ bzw. $R \to \mathrm{Aut}(Q)$. Weil $|\mathrm{Aut}(P)| = 10$ und $|\mathrm{Aut}(Q)| = 16$ teilerfremd zu $|R| = 3$ ist, ist jeder solche Homomorphismus trivial. Daher operiert R trivial auf P und Q, also kommutieren alle Elemente von R mit allen Elementen aus P und Q. Analog ist die Konjugation von P auf Q trivial, weil $|P| = 11$ teilerfremd zu $|\mathrm{Aut}(Q)| = 16$ ist. Also kommutieren auch alle Elemente von P mit allen Elementen aus Q. Es folgt, dass die Produktabbildung

$$\begin{aligned} P \times Q \times R &\to G \\ (p, q, r) &\mapsto pqr \end{aligned}$$

ein Homomorphismus ist. Dessen Bild enthält Elemente der Ordnungen 3 und 11 und 17; die Ordnung dieses Bilds ist daher ein Vielfaches von $3 \cdot 11 \cdot 17 = |G|$; somit ist der Homomorphismus surjektiv. Wegen $|P \times Q \times R| = |G|$ ist er dann schon bijektiv und folglich ein Isomorphismus. Schliesslich folgt aus dem chinesischen Restsatz:

$$G \;\cong\; P \times Q \times R \;\cong\; Z_{11} \times Z_{17} \times Z_3 \;\cong\; Z_{561}.$$

3. (a) Sei G eine endliche Gruppe der Ordnung $p^k m$ für eine Primzahl p und natürliche Zahlen k und m mit $p \nmid m$ und $m > 1$. Zeige: Falls ein Normalteiler $N \lhd G$ der Ordnung m existiert, so ist G ein semidirektes Produkt von nicht-trivialen Untergruppen.

   (b) Zeige, dass eine endliche abelsche Gruppe genau dann ein direktes Produkt von nicht-trivialen Untergruppen ist, wenn sie nicht zyklisch von Primpotenzordnung ist.

   (c) Bestimme alle Gruppen ungerader Ordnung < 60, die kein semidirektes Produkt von nicht-trivialen Untergruppen sind.

   Lösung:

   (a) Sei P eine p-Sylowuntergruppe. Weil die Ordnungen von P und N teilerfremd sind, gilt $P \cap N = \{1\}$ und der natürliche Homomorphismus $P \to G/N$ ist injektiv. Wegen $|P| = p^k = |G/N|$ ist er dann schon bijektiv; also gilt $G = PN$. Somit ist G ein semidirektes Produkt der Form $N \rtimes H$.

   (b) Nach dem Struktursatz ist jede endliche abelsche Gruppe G isomorph zu $\boxplus_{i=1}^{m} \mathbb{Z}/p_i^{\mu_i}\mathbb{Z}$ mit Primpotenzen $p_i^{\mu_i}$, die eindeutig bis auf Vertauschung sind. Ist $m \geqslant 2$, so ist G also ein nicht-triviales Produkt. Andernfalls ist $G = 1$ oder $G \cong \mathbb{Z}/p^{\mu}\mathbb{Z}$ für eine Primzahl p. Wäre dann $G \cong G_1 \times G_2$ mit zwei nicht-trivialen Gruppen G_1 und G_2, so wäre $G_1 \cong \boxplus_{i=1}^n \mathbb{Z}/q_i^{\mu_i}\mathbb{Z}$ und $G_2 \cong \boxplus_{j=1}^k \mathbb{Z}/r_j^{\nu_j}\mathbb{Z}$ mit $n, k \geqslant 1$ und Primpotenzen $q_i^{\mu_i}, r_j^{\nu_j} > 1$, und folglich

$$G \;\cong\; \mathop{\boxplus}_{i=1}^{n} \mathbb{Z}/q_i^{\mu_i}\mathbb{Z} \boxplus \mathop{\boxplus}_{j=1}^{k} \mathbb{Z}/r_j^{\nu_j}\mathbb{Z}$$

mit mindestens 2 nicht-trivialen Summanden. Dies widerspricht der Eindeutigkeit der Primpotenzen im Struktursatz über endlich erzeugte abelsche Gruppen.

(c) Nach (b) hat eine abelsche Gruppe genau dann die gesuchte Eigenschaft, wenn sie zyklisch von Primpotenzordnung ist. Wir schauen, ob es noch weitere gibt.

Die ungeraden Zahlen < 60 sind Produkte von Primzahlen $\geqslant 3$. Wegen $3^4 = 81 \geqslant 60$ können sie daher nur aus höchstens 3 Faktoren bestehen. Ausserdem ist $3 \cdot 5 \cdot 7 = 105 \geqslant 60$. Somit kommen nur Gruppen der Ordnungen p, p^2, p^3, pq, p^2q für ungerade Primzahlen $p \neq q$ in Frage.

Da jede Gruppe der Ordnung p oder p^2 abelsch ist, sind diese bereits erledigt.

In der Vorlesung wurde gezeigt, dass es genau zwei Isomorphieklassen von nicht-abelschen Gruppen der Ordnung p^3 gibt, und für p ungerade wurden beide als semidirekte Produkte von abelschen Gruppen konstruiert. Diese haben daher nicht die gesuchte Eigenschaft.

Sei nun G eine Gruppe der Ordnung pq und sei ohne Beschränkung der Allgemeinheit $p > q$. Dann gibt es wegen der Sylowsätze nur eine p-Sylowgruppe, also ist diese normal. Aus (a) folgt dann, dass G auf nicht-triviale Weise ein semidirektes Produkt ist.

Schliesslich bleiben nur Gruppen der Ordnung p^2q mit $p \neq q$, und wegen $|G| < 60$ kommt dabei nur noch $3^2 \cdot 5$ in Frage. Aus den Sylowsätzen folgt hier ebenfalls, dass es nur eine 5-Sylowgruppe und nur eine 3-Sylowgruppe gibt, diese also normal ist. Daher folgt wiederum aus (a), dass G auf nicht-triviale Weise ein semidirektes Produkt ist.

Zusammenfassend sind also die Gruppen ungerader Ordnung < 60, die auf keine nicht-triviale Weise ein semidirektes Produkt sind, genau die zyklischen Gruppen von Primpotenzordnung.

4. Sei p eine Primzahl.

(a) Bestimme die Anzahl der p-Sylowgruppen der symmetrischen Gruppe S_p.

(b) Folgere daraus den *Satz von Wilson*:

$$(p-1)! \equiv -1 \bmod (p).$$

Lösung:

(a) Weil p die Gruppenordnung $|S_p| = p!$ teilt, aber p^2 nicht, ist jede p-Sylowuntergruppe zyklisch der Ordnung p, also erzeugt durch ein Element der Ordnung p. Die Elemente der Ordnung p in S_p sind genau die p-Zykel. Jeder solche hat eine eindeutige Darstellung der Form $(1\ i_2\ \ldots\ i_n)$ mit $\{i_2, \ldots, i_n\} = \{2, \ldots, n\}$; also gibt es genau $(p-1)!$ verschiedene. Jede p-Sylowgruppe enthält genau $p-1$ verschiedene p-Zykel, und umgekehrt liegt jeder p-Zykel in genau einer p-Sylowgruppe; also ist die Anzahl der p-Sylowgruppen in S_p gleich $(p-1)!/(p-1) = (p-2)!$.

(b) Aus den Sylowsätzen folgt dann $(p-2)! \equiv 1 \bmod p$, und daraus $(p-1)! \equiv p-1 \equiv -1 \bmod p$.

*5. Betrachte einen endlichen Körper K mit $q := p^m$ Elementen für eine Primzahl p und eine natürliche Zahl $m \geqslant 1$.

(a) Finde eine p-Sylowuntergruppe P in $\mathrm{GL}_n(K)$ und bestimme ihre Ordnung.

(b) Bestimme den Normalisator von P und seine Ordnung.

(c) Folgere daraus und mit Aufgabe 5 der Serie 18 die Sylowsätze für $\mathrm{GL}_n(K)$ und die Primzahl p.

Lösung: Wir bestimmen zuerst die Ordnung von $\mathrm{GL}_n(K)$. Die Elemente von $\mathrm{GL}_n(K)$ korrespondieren zur Wahl eines Tupels aus n linear unabhängigen Vektoren in K^n. Der erste Vektor unterliegt nur der Bedingung, dass er nicht Null sein darf, dafür gibt es also $q^n - 1$ Auswahlmöglichkeiten. Der zweite Vektor muss dann ausserhalb des 1-dimensionalen Vektorraumes liegen, der vom ersten Vektor erzeugt wird, dafür gibt es $q^n - q$ Auswahlmöglichkeiten. Der dritte Vektor muss ausserhalb des 2-dimensionalen Vektorraumes liegen, der von den ersten beiden Vektoren erzeugt wird, also haben wir noch $q^n - q^2$ Auswahlmöglichkeiten. So geht es weiter; insgesamt ist die Ordnung von $\mathrm{GL}_n(K)$ also gleich

$$\prod_{i=0}^{n-1}(q^n - q^i) \;=\; \prod_{i=0}^{n-1} q^i(q^{n-i} - 1) \;=\; q^{\frac{n(n-1)}{2}} \cdot r$$

ist, wobei p die Zahl r nicht teilt.

(a) Aus der obigen Formel folgt schon, dass jede p-Sylowuntergruppe von $\mathrm{GL}_n(K)$ die Ordnung $q^{\frac{n(n-1)}{2}}$ hat. Sei nun P die Untergruppe aller oberen Dreiecksmatrizen mit 1 auf der Diagonalen. Eine solche Matrix hat $\frac{n^2-n}{2}$ Einträge oberhalb der Diagonalen, die wir frei aus K wählen können. Also hat P die Ordnung $q^{\frac{n(n-1)}{2}}$ und ist damit eine p-Sylowuntergruppe von $\mathrm{GL}_n(K)$.

(b) Betrachte zuerst eine obere Dreiecksmatrix $A \in \mathrm{GL}_n(K)$. Für jedes $B \in P$ ist dann ABA^{-1} eine obere Dreiecksmatrix mit denselben Diagonaleinträgen wie B, also ein Element von P. Somit gilt $APA^{-1} \subset P$. Dieselbe Überlegung zeigt auch $A^{-1}PA \subset P$ und folglich $P \subset APA^{-1}$ und daher $APA^{-1} = P$. Also liegt A im Normalisator von P.

Betrachte umgekehrt eine Matrix $A \in \mathrm{GL}_n(K)$ mit $A^{-1}PA \subset P$, also mit $PA \subset AP$. Betrachte die Standardbasis $e_1, \ldots, e_n \in K^n$ und für jedes $1 \leqslant i \leqslant n$ den Untervektorraum $V_i := \langle e_1, \ldots, e_i \rangle$. Mittels Elementarmatrizen zeigt man schnell, dass dies der eindeutige i-dimensionale Untervektorraum von K^n mit der Eigenschaft $PV_i \subset V_i$ ist. Wegen $PA \subset AP$ ist dann auch $PAV_i \subset APV_i \subset AV_i$, und aus der Eindeutigkeit von V_i folgt $AV_i = V_i$. Insgesamt zeigt dies, dass A eine obere Dreiecksmatrix ist. Daher ist der Normalisator von P genau die Gruppe der oberen Dreiecksmatrizen.

Für ein Element davon haben wir ausser der $\frac{n^2-n}{2}$ Einträge oberhalb der Diagonalen, die wir frei aus K wählen können, noch die n Einträge auf der Diagonalen, die wir frei aus $K \setminus \{0\}$ wählen können. Daher hat der Normalisator die Ordnung $|P| \cdot |K^\times|^n = q^{\frac{n(n-1)}{2}} \cdot (q-1)^n$.

(c) Die Existenz einer p-Sylowuntergruppe ist (a). Sodann besagt Aufgabe 5 (b) der Serie 18, dass für jede p-Untergruppe G ein $h \in \mathrm{GL}_n(K)$ existiert mit $hGh^{-1} \subset P$. Also ist G in der p-Sylowgruppe $h^{-1}Ph$ enthalten, und falls G schon selbst eine p-Sylowgruppe ist, ist sie gleich $h^{-1}Ph$. Schliesslich gilt wegen der Bahnengleichung

$$|\,\mathrm{GL}_n(K)| \;=\; |\,\mathrm{Norm}_{\mathrm{GL}_n(K)}(P)| \cdot |\,\mathrm{Syl}_p(\mathrm{GL}_n(K))|.$$

Also teilt $|\,\mathrm{Syl}_p(\mathrm{GL}_n(K))|$ den Faktor r der Gruppenordnung. Aus der Teilaufgabe (b) folgt weiter

$$|\,\mathrm{Syl}_p(\mathrm{GL}_n(K))| \;=\; \frac{r}{(q-1)^n} \;=\; \prod_{i=0}^{n-1} \frac{q^{n-i}-1}{q-1} \;\equiv\; 1 \bmod (p).$$

6. Bestimme für jeden Primteiler von $|\,\mathrm{SL}_2(\mathbb{F}_7)|$ eine Sylowuntergruppe von $\mathrm{SL}_2(\mathbb{F}_7)$.

Lösung: Wir bestimmen zuerst die Gruppenordnung von $\mathrm{SL}_2(\mathbb{F}_7)$. Wie in Aufgabe 5 erklärt, gilt für jede Primzahl p

$$|\,\mathrm{GL}_2(\mathbb{F}_p)| \;=\; (p^2-1)(p^2-p) \;=\; (p^2-1)(p-1)p.$$

Sodann ist der Determinantenhomomorphismus $\mathrm{GL}_2(\mathbb{F}_p) \to \mathbb{F}_p^\times$ surjektiv, weil $\det\left(\begin{smallmatrix}\alpha & 0\\ 0 & 1\end{smallmatrix}\right) = \alpha$ ist für jedes $\alpha \in \mathbb{F}_p^\times$. Daher hat $\mathrm{GL}_2(\mathbb{F}_p)/\mathrm{SL}_2(\mathbb{F}_p) \cong \mathbb{F}_p^\times$ die Ordnung $p-1$, also $\mathrm{SL}_2(\mathbb{F}_p)$ den Index $p-1$ und somit die Ordnung $(p^2-1)p$. Für $p=7$ ergibt sich damit die Ordnung $7 \cdot 6 \cdot 8 = 2^4 \cdot 3 \cdot 7$. Wir müssen also eine p-Sylowuntergruppe finden für die Primzahlen 2, 3 und 7.

Wie in Aufgabe 5 ist die Gruppe der oberen Dreiecksmatrizen mit 1 auf der Diagonalen eine 7-Sylowuntergruppe.

Da $2 \in \mathbb{F}_7^\times$ die Ordnung 3 hat mit $2^{-1} = 4$, ist $\langle\left(\begin{smallmatrix}2 & 0\\ 0 & 4\end{smallmatrix}\right)\rangle$ eine 3-Sylowuntergruppe.

Eine 2-Sylowgruppe ist eine Untergruppe der Ordnung 16. Um eine solche zu finden, suchen wir zuerst eine Matrix $A \in \mathrm{SL}_2(\mathbb{F}_7)$, deren Ordnung ein grösstmöglicher Teiler m von 16 ist. Für diesen muss das Minimalpolynom ein Teiler von $X^m - 1$ im Polynomring $\mathbb{F}_7[X]$ sein. Ein bisschen Experimentieren zeigt $X^8 - 1 = (X^4 - 1)(X^4 + 1)$ und liefert die Zerlegung in irreduzible Faktoren über $\mathbb{F}_7$

$$X^4 + 1 \;=\; (X^2 + 3X + 1)(X^2 + 4X + 1).$$

Die Begleitmatrix $A := \left(\begin{smallmatrix}0 & -1\\ 1 & -3\end{smallmatrix}\right)$ des Polynoms X^2+3X+1 hat also das Minimalpolynom X^2+3X+1; somit gilt $\det(A) = 1$ und $A^8 = 1$. Wegen $(X^2+3X+1)|(X^4+1)$ und $\mathrm{ggT}(X^4+1, X^4-1) \sim 1$ gilt weiter $A^4 \neq 1$; also hat A tatsächlich die Ordnung 8. Nach den Sylowsätzen liegt A in einer 2-Sylowgruppe P von $\mathrm{SL}_2(\mathbb{F}_7)$. Die von A erzeugte Untergruppe $\langle A\rangle$ hat dann Ordnung 8 und somit Index 2 in P, ist also normal in P. Umgekehrt ist daher P im Normalisator von $\langle A\rangle$ enthalten. Für jedes Element $B \in P \smallsetminus \langle A\rangle$ ist dann BAB^{-1} ein weiteres Erzeugendes von $\langle A\rangle$, also gleich A^i für $i \in \{1,3,5,7\}$. Ein solches B erfüllt daher das lineare Gleichungssystem $BA = A^iB$ sowie die Gleichung $\det(B) = 1$. Probieren liefert die Lösung $B = \left(\begin{smallmatrix}2 & 2\\ 1 & 5\end{smallmatrix}\right)$ mit $i = -1$. Wegen $BAB^{-1} = A^{-1} \neq A$ ist dann sicher $B \notin \langle A\rangle$.

Ausserdem gilt $B^2 = -I_2 = A^4 \in \langle A\rangle$. Somit hat das Bild von B in der Faktorgruppe $\mathrm{Norm}_{\mathrm{SL}_2(\mathbb{F}_7)}(\langle A\rangle)/\langle A\rangle$ die Ordnung 2; und daher erzeugen A und B zusammen eine Gruppe der Ordnung 16, das heisst, eine 2-Sylowgruppe von $\mathrm{SL}_2(\mathbb{F}_7)$.

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