Musterlösung Serie 18

Semidirekte Produkte, p-Gruppen

1. Sei σ ein n-Zykel in S_n.

   (a) Bestimme den Zentralisator $\mathrm{Cent}_{S_n}(\langle\sigma\rangle)$.

   (b) Bestimme den Normalisator $\mathrm{Norm}_{S_n}(\langle\sigma\rangle)$ als semidirektes Produkt, mit Gruppenordnung und Struktur.

   Lösung: (a) We claim that $\mathrm{Cent}_{S_n}(\langle\sigma\rangle) = \langle\sigma\rangle$. The inclusion "$\supset$" follows from the fact that $\langle\sigma\rangle$ is abelian. Conversely consider any $\tau \in \mathrm{Cent}_{S_n}(\langle\sigma\rangle)$. Writing $\sigma = (i_1, \ldots, i_n)$, we then have $\sigma = {}^{\tau}\sigma = (\tau(i_1), \ldots, \tau(i_n))$. Thus there exists an integer $1 \leqslant m \leqslant n$ such that $(\tau(i_1), \ldots, \tau(i_n)) = (i_{m+1}, \ldots, i_n, i_1, \ldots, i_m)$. It follows that $\tau = \sigma^m$. This yields the reverse inclusion.

   (b) Set $N := \langle\sigma\rangle$ and $G := \mathrm{Norm}_{S_n}(N)$ and $H := \mathrm{Stab}_G(1)$. We have $H \cap N = 1$, since the only element of N fixing 1 is the identity. On the other hand consider any $\tau \in G$. Since N acts transitively on $\{1, \ldots, n\}$, there exists an integer i such that $\tau 1 = \sigma^i 1$. Thus $\sigma^{-i}\tau 1 = 1$ and hence $\sigma^{-i}\tau \in H$, or again $\tau \in \sigma^i H$. Varying τ this shows that $G = NH = HN$. All together, this shows that $G = N \rtimes H$.

   Consider the homomorphism $\psi : H \to \mathrm{Aut}(N)$ corresponding to the action of H on N by conjugation. An element $\nu \in H$ is in $\ker(\psi)$ if and only if it acts trivially on every element of N. This is equivalent to $\nu \in \mathrm{Cent}_{S_n}(N)$. We know by part (a) that $\mathrm{Cent}_{S_n}(N) = N$. Since $H \cap N = 1$, it follows that $\ker(\psi)$ is trivial and that ψ is thus injective.

   Since $N \cong \mathbb{Z}/n\mathbb{Z}$, we have $\mathrm{Aut}(N) \cong \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$, with an element $i + n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^\times$ acting by $\sigma \mapsto \sigma^i$. For any i this image σ^i is another generator of N. Thus it also acts transitively on $\{1, \ldots, n\}$ and is therefore again an n-cycle. As all n-cycles in S_n are conjugate, there exists a permutation $\tau \in S_n$ such that ${}^{\tau}\sigma = \sigma^i$. It follows that ${}^{\tau}N = \langle\sigma^i\rangle = N$, and so $\tau \in G$. Since $G = HN$, we may write $\tau = \tau'\sigma^m$ with $\tau' \in H$ and $1 \leqslant m \leqslant n$. Since N is abelian, we have

   $$ {}^{\tau}\sigma = {}^{\tau'\sigma^m}\sigma = {}^{\tau'}({}^{\sigma^m}\sigma) = {}^{\tau'}\sigma. $$

   It follows that $\psi(\tau')$ is the automorphism corresponding to $i + n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^\times$. As $i + n\mathbb{Z}$ was arbitrary, this shows that ψ is surjective.

   Therefore ψ is bijective and hence an isomorphism. It also follows that

   $$ G \;=\; N \rtimes H \;\cong\; \mathbb{Z}/n\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^\times, $$

   where $(\mathbb{Z}/n\mathbb{Z})^\times$ acts on $\mathbb{Z}/n\mathbb{Z}$ by multiplication. Its order is $n \cdot \varphi(n)$ with Euler's function $\varphi(n) := |(\mathbb{Z}/n\mathbb{Z})^\times|$.

2. (a) Bestimme die Gruppenstruktur von $(\mathbb{Z}/8\mathbb{Z})^\times$.

   (b) Bestimme die Isomorphieklassen aller Gruppen der Ordnung 16, welche ein semidirektes Produkt einer zyklischen Gruppe der Ordnung 8 mit einer Gruppe der Ordnung 2 sind.

Lösung: (a) Die Gruppe $(\mathbb{Z}/8\mathbb{Z})^\times$ besteht aus den paarweise verschiedenen Restklassen $[a] := a + 8\mathbb{Z}$ für $a = 1, 3, 5, 7$. Wegen $3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \mod (8)$ hat jedes nichttriviale Element die Ordnung 2. Also ist $(\mathbb{Z}/8\mathbb{Z})^\times$ isomorph zu $C_2 \times C_2$.

(b) Die fraglichen Gruppen sind isomorph zu $(\mathbb{Z}/8\mathbb{Z}) \rtimes (\mathbb{Z}/2\mathbb{Z})$ für Homomorphismen $\mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/8\mathbb{Z}) \cong (\mathbb{Z}/8\mathbb{Z})^\times$. Jeder solche Homomorphismus hat die Form $i + 2\mathbb{Z} \mapsto [a^i]$ für ein $[a] \in (\mathbb{Z}/8\mathbb{Z})^\times$. Da $(\mathbb{Z}/8\mathbb{Z})^\times$ selbst Exponent 2 hat, liefert umgekehrt jedes Element $[a] \in (\mathbb{Z}/8\mathbb{Z})^\times$ einen solchen Homomorphismus. Wir haben also die Möglichkeiten

$$\begin{aligned} G_1 &:= (\mathbb{Z}/8\mathbb{Z}) \rtimes (\mathbb{Z}/2\mathbb{Z}) \quad \text{mit } i + 2\mathbb{Z} \mapsto [1], \\ G_3 &:= (\mathbb{Z}/8\mathbb{Z}) \rtimes (\mathbb{Z}/2\mathbb{Z}) \quad \text{mit } i + 2\mathbb{Z} \mapsto [3^i], \\ G_5 &:= (\mathbb{Z}/8\mathbb{Z}) \rtimes (\mathbb{Z}/2\mathbb{Z}) \quad \text{mit } i + 2\mathbb{Z} \mapsto [5^i], \\ G_7 &:= (\mathbb{Z}/8\mathbb{Z}) \rtimes (\mathbb{Z}/2\mathbb{Z}) \quad \text{mit } i + 2\mathbb{Z} \mapsto [7^i]. \end{aligned}$$

Wir müssen noch überprüfen, ob welche dieser vier Gruppen isomorph sind. Dafür untersuchen wir zunächst, ob es ausser den Elementen von $(\mathbb{Z}/8\mathbb{Z})^\times \subset \mathbb{Z}/8\mathbb{Z}$ noch weitere Elemente der Ordnung 8 gibt. Betrachte ein Element der Form $([b], [1]) \in G_a$. Sein Quadrat ist

$$([b], [1]) \cdot ([b], [1]) = ([b] + {}^{[1]}[b], [1] + [1]) = ([b] + [ab], [2]) = ([b(1 + a)], [0]).$$

Dieses hat Ordnung 4 genau dann, wenn $b(1 + a) \equiv 2$ modulo 4 ist. Für $a \in \{3, 7\}$ ist das nie der Fall, also hat G_a genau 4 Elemente der Ordnung 8. Für $a \in \{1, 5\}$ ist das der Fall zum Beispiel mit $b = 1$, und dann hat G_a mehr als 4 Elemente der Ordnung 8. Somit gibt es, wenn überhaupt, nur Isomorphismen $G_3 \cong G_7$ und/oder $G_1 \cong G_5$.

Die Gruppe G_1 ist das übliche direkte Produkt $(\mathbb{Z}/8\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ und folglich abelsch. Die übrigen Gruppen sind nichtabelsch, weil der jeweilige Homomorphismus nichttrivial ist. Insbesondere ist $G_1 \ncong G_5$.

Für G_3 und G_7 ist $\mathbb{Z}/8\mathbb{Z}$ die einzige zyklische Untergruppe der Ordnung 8. Jeder Isomorphismus $\varphi\colon G_3 \xrightarrow{\sim} G_7$ muss also $\mathbb{Z}/8\mathbb{Z}$ isomorph auf sich abbilden. Sei also

$$\begin{aligned} &\varphi\colon ([b], [0]) \mapsto ([bc], [0]) \quad \text{für ein } [c] \in (\mathbb{Z}/8\mathbb{Z})^\times \text{ und} \\ &\varphi\colon ([0], [1]) \mapsto ([d], [1]) \quad \text{für ein } [d] \in (\mathbb{Z}/8\mathbb{Z}). \end{aligned}$$

In G_3 induziert die Konjugation mit $([0], [1])$ den Automorphismus $[b] \mapsto [3b]$ auf $\mathbb{Z}/8\mathbb{Z}$. Da $\mathbb{Z}/8\mathbb{Z}$ abelsch ist, induziert in G_7 die Konjugation mit $([d], [1])$

ebenso wie mit $([0],[1])$ den Automorphismus $[b] \mapsto [7b]$ auf $\mathbb{Z}/8\mathbb{Z}$. Da φ ein Homomorphismus ist, muss folglich gelten:

$$\begin{array}{lccc} G_3\colon & {\scriptstyle([0],[1])}([b],[0]) & ========== & ([3b],[0]) \\ & \varphi\downarrow & & \varphi\downarrow \\ G_7\colon & {\scriptstyle([d],[1])}([bc],[0]) & = ([7bc],[0]) \overset{?}{=} & ([3bc],[0]) \end{array}$$

Wegen $[c] \in (\mathbb{Z}/8\mathbb{Z})^\times$ ist aber $[7bc] \neq [3bc]$ für $b = 1$. Somit haben wir einen Widerspruch, und es folgt $G_3 \ncong G_7$.

Insgesamt sind die Gruppen G_1, G_3, G_5, G_7 also paarweise nicht isomorph.

3. Für welche Primzahlen p, q ist jedes semidirekte Produkt $\mathbb{Z}/p\mathbb{Z} \rtimes \mathbb{Z}/q\mathbb{Z}$ ein direktes Produkt?

   Erklärung: Die gesuchte Eigenschaft ist äquivalent dazu, dass jeder Homomorphismus $\mathbb{Z}/q\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/p\mathbb{Z}) \cong (\mathbb{Z}/q\mathbb{Z})^\times$ trivial ist. Da $(\mathbb{Z}/q\mathbb{Z})^\times = \mathbb{F}_p^\times$ zyklisch der Ordnung $p-1$ ist, ist dies äquivalent dazu, dass jeder Homomorphismus $\mathbb{Z}/q\mathbb{Z} \to \mathbb{Z}/(p-1)\mathbb{Z}$ trivial ist. Im Fall $q \nmid (p-1)$ gilt diese Bedingung, weil dann q und $p-1$ teilerfremd sind. Im Fall $q|(p-1)$ schreibe $p-1 = qa$; dann induziert die Multiplikation mit a einen injektiven Homomorphismus

   $$\mathbb{Z}/q\mathbb{Z} \to \mathbb{Z}/(p-1)\mathbb{Z},\ x + q\mathbb{Z} \mapsto ax + (p-1)\mathbb{Z},$$

   der folglich nicht-trivial ist. Somit gilt die gesuchte Eigenschaft genau dann, wenn q kein Teiler von $p-1$ ist.

4. Zeige, dass jede p-Gruppe nilpotent ist.

   Lösung: By Serie 17, Aufgabe 6, it suffices to show that the ascending central series $1 = Z_0 \lhd Z_1 \lhd \ldots$ of G eventually becomes constant with $Z_n = G$. This series was defined by setting $Z_0 := 1$ and

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

   and we already know that each Z_i is a normal subgroup of G and that Z_{i+1}/Z_i is the center of G/Z_i. Since G is a p-group, so is each G/Z_i. If $Z_i \neq G$, by a theorem of the lecture the non-trivial p-group G/Z_i possesses a non-trivial center. Thus $Z_{i+1}/Z_i \neq 1$ and hence $Z_i \neq Z_{i+1}$. A G is finite, the ascending chain $1 = Z_0 \lhd Z_1 \lhd \ldots$ must therefore become constant with $Z_n = G$, as desired.

5. (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 $|Gx| \equiv 0 \mod p$. 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

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

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

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

   Let $G' < \mathrm{GL}_{n-1}(K)$ be the image of ${}^AG$ 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 ${}^hG < U$.

6. Zeige, dass jede nichtabelsche Gruppe der Ordnung 8 zur D_4 oder zur Quaternionengruppe isomorph ist.

   Lösung: Sei G eine solche Gruppe. Dann hat jedes Element die Ordnung 1, 2, 4 oder 8. Gäbe es ein Element der Ordnung 8, so wäre $G \cong Z_8$ und daher abelsch. Hätten alle nichttrivialen Elemente die Ordnung 2, so hätte G den Exponenten

2 und wäre wieder abelsch nach Proposition 1.4.11 der Vorlesung. Somit besitzt G kein Element der Ordnung 8, aber ein Element n der Ordnung 4. Die von n erzeugte Untergruppe N ist dann isomorph zu Z_4 und als Untergruppe vom Index 2 normal.

Wir nehmen zuerst an, dass $G \setminus N$ ein Element h der Ordnung 2 enthält. Die von h erzeugte Untergruppe H ist dann isomorph zu Z_2 und es gilt $G = NH$ und $N \cap H = 1$. Also ist G ein semidirektes Produkt $N \rtimes H \cong Z_4 \rtimes Z_2$. Da G nicht abelsch ist, muss dabei die Operation von H auf N nichttrivial sein. Es gibt aber nur einen nichttrivialen Homomorphismus $H \cong Z_2 \to (\mathbb{Z}/4\mathbb{Z})^\times = \mathrm{Aut}(Z_4) \cong \mathrm{Aut}(N)$, und für diesen ist $Z_4 \rtimes Z_2 \cong D_4$. In diesem Fall ist daher $G \cong D_4$.

Andernfalls haben alle Elemente von $G \setminus N$ die Ordnung 4, und n^2 ist das einzige Element der Ordnung 2 von G. Für jedes $h \in G \setminus N$ ist dann h^2 ein Element der Ordnung 2 und somit gleich n^2. Mit $k := nh$ ist dann auch $k \in G \setminus N$ und folglich $k^2 = n^2$. Anders ausgedrückt gilt $nhnh = n^2$, woraus $h^{-1}n = nh = k$ folgt. Aus den letzten Gleichungen folgt sofort $hk = n$. Durch zyklische Vertauschung von n, h, k folgt analog $k^{-1}h = hk = n$ und $n^{-1}k = kn = h$. Da diese Relationen genau die Quaternionengruppe Q beschreiben, ist daher $G \cong Q$ und wir sind fertig.

7. Betrachte eine Primzahl p und eine natürliche Zahl n.

   (a) Zeige, dass jede Gruppe der Ordnung p^n von n Elementen erzeugt ist.

   (b) Gibt es eine Gruppe der Ordnung p^n, die nicht von $n-1$ Elementen erzeugt ist?

   Lösung:

   (a) Setze $G_0 := \{1\}$. Solange $G_i \neq G$ ist, wähle induktiv ein Element $g_{i+1} \in G \setminus G_i$ und setze $G_{i+1} := \langle G_i \cup \{g_{i+1}\}\rangle$. Jedes G_i ist dann von i Elementen erzeugt und es ist $|G_i| > |G_{i-1}|$. Da alle G_i Untergruppen der p-Gruppe sind, folgt daraus $|G_i| \geqslant p^i$. Somit bricht die Folge für ein $i_0 \leqslant n$ ab. Dann gilt $G_{i_0} = G$ und G ist somit von $i_0 \leqslant n$ Elementen erzeugt.

   (b) Die Gruppe Z_p^n ist nicht von $n-1$ Elementen erzeugt. Denn als $\mathbb{Z}$-Modul ist diese ein $\mathbb{F}_p$-Vektorraum, und jede von $n-1$ Elementen erzeugte Untergruppe ist ein von $n-1$ Elementen erzeugter $\mathbb{F}_p$-Unterraum, hat also Dimension $\leqslant n-1$, und ist daher echt in Z_p^n enthalten.