Musterlösung 12

Subnormalreihen, Kompositionsreihen, Auflösbare Gruppen, Semidirekte Produkte

1. (a) Gib eine Kompositionsreihe der Diedergruppe D_{12} an.

   (b) Sei p eine Primzahl. Gib eine Kompositionsreihe der Matrixgruppe

$$G = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \quad : \quad a, b, c \in \mathbb{Z}/p\mathbb{Z} \right\}$$

   an.

   (c) Finde alle Kompositionsreihen der Diedergruppe D_4.

Lösung:

(a) Sei D_{12} erzeugt von der Drehung T der Ordnung 12 und der Spiegelung S, d.h. $D_{12} = \{1, T, \ldots, T^{11}, S, ST, \ldots, ST^{11}\}$. Die Untergruppe $\langle T \rangle$ der Drehungen ist vom Index 2 in D_{12} und somit normal. Da $\langle T \rangle$ abelsch ist, sind sämtliche Untergruppen dieser Gruppe normal in $\langle T \rangle$. Deshalb ist zum Beispiel die Reihe

$$D_{12} \rhd \langle T \rangle \rhd \langle T^3 \rangle \rhd \langle T^6 \rangle \rhd \{1\}$$

eine Subnormalreihe. Da deren Faktoren als Gruppen von Primzahlordnung alle einfach sind, ist sie eine Kompositionsreihe von D_{12}.

Es kann gezeigt werden, dass D_{12} insgesamt 11 Kompositionsreihen hat. Weitere Kompositionsreihen sind beispielsweise

$$\begin{array}{ccccccccc} D_{12} & \rhd & \langle T \rangle & \rhd & \langle T^2 \rangle & \rhd & \langle T^6 \rangle & \rhd & \{1\}, \\ D_{12} & \rhd & \langle T \rangle & \rhd & \langle T^2 \rangle & \rhd & \langle T^4 \rangle & \rhd & \{1\}, \\ D_{12} & \rhd & \langle T^2, S \rangle & \rhd & \langle T^4, S \rangle & \rhd & \langle T^4 \rangle & \rhd & \{1\}. \end{array}$$

(b) Wir betrachten die Untergruppen

$$G_1 := \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} : a, b \in \mathbb{Z}/p\mathbb{Z} \right\}, \ G_2 := \left\{ \begin{pmatrix} 1 & 0 & b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} : b \in \mathbb{Z}/p\mathbb{Z} \right\}$$

von G. Es gilt $|G| = p^3$ und $|G_1| = p^2$ und $|G_2| = p$. Nach Lagrange folgt daher $[G : G_1] = [G_1 : G_2] = p$. Da die Ordnungen von G und G_1 Potenzen von p sind, folgt mit Aufgabe 8 der Serie 11, dass G_1 normal in G und G_2 normal in G_1

ist (alternativ sieht man das für $G_1 < G$ auch mit einer leichten Rechnung, für $G_2 < G_1$ mit der Tatsache, dass G_1 abelsch ist). Somit ist die Reihe

$$G \rhd G_1 \rhd G_2 \rhd \{1\}$$

eine Subnormalreihe von G. Da deren Subfaktoren als Gruppen von der Ordnung p einfach sind, ist sie eine Kompositionsreihe von G.

(c) Write $D_4 = \{1, T, T^2, T^3, S, ST, ST^2, ST^3\}$ as before with a rotation T and a reflection S. The first term from above of a composition series of D_4 must be a subgroup of index 2. Any such subgroup contains T^2. The factor group $D_4/\langle T\rangle \cong C_2^2$ possesses three subgroups of index 2. Lifting them to D_4 shows that D_4 has the following three subgroups of order 2:

$$\begin{array}{rcl} \langle T\rangle & \cong & C_4, \\ \langle T^2, S\rangle & \cong & C_2^2, \\ \langle T^2, ST\rangle & \cong & C_2^2. \end{array}$$

Having index 2, each of these is abelian and normal in D_4. The next term in the composition series must and can be any subgroup of order 2 of this one. For $\langle T\rangle$ there exists only one choice $\langle T^2\rangle$, for the others three. Altogether this yields the following 7 composition series

$$\begin{array}{ccccccc} D_4 & \rhd & \langle T\rangle & \rhd & \langle T^2\rangle & \rhd & \{1\}, \\ D_4 & \rhd & \langle T^2, S\rangle & \rhd & \langle T^2\rangle & \rhd & \{1\}, \\ D_4 & \rhd & \langle T^2, S\rangle & \rhd & \langle S\rangle & \rhd & \{1\}, \\ D_4 & \rhd & \langle T^2, S\rangle & \rhd & \langle ST^2\rangle & \rhd & \{1\}, \\ D_4 & \rhd & \langle T^2, ST\rangle & \rhd & \langle T^2\rangle & \rhd & \{1\}, \\ D_4 & \rhd & \langle T^2, ST\rangle & \rhd & \langle ST\rangle & \rhd & \{1\}, \\ D_4 & \rhd & \langle T^2, ST\rangle & \rhd & \langle ST^3\rangle & \rhd & \{1\}. \end{array}$$

2. Die *absteigende Zentralreihe* einer Gruppe G ist induktiv definiert durch $G^{[0]} := G$ und
$$G^{[m+1]} := [G, G^{[m]}] := \big\langle \{[g, g'] : g \in G,\ g' \in G^{[m]}\} \big\rangle.$$
Existiert ein m mit $G^{[m]} = 1$, so heisst G *nilpotent*.

(a) Zeige, dass jedes $G^{[m]}$ die entsprechende höhere Kommutatoruntergruppe $G^{(m)}$ enthält.

(b) Folgere, dass jede nilpotente Gruppe auflösbar ist.

(c) Zeige, dass die Untergruppe der oberen Dreiecksmatrizen in $\mathrm{GL}_n(K)$ mit allen Diagonaleinträgen 1 nilpotent ist.

(d) Zeige, dass die Untergruppe aller oberen Dreiecksmatrizen in $\mathrm{GL}_2(K)$ auflösbar, aber nicht nilpotent ist, wenn $|K| > 2$ ist.

(e) Zeige, dass jede Untergruppe und Faktorgruppe einer nilpotenten Gruppe auch nilpotent ist.

Lösung: (a) For $m = 0$, we have $G^{[0]} = G = G^{(0)}$. Now take $m \geqslant 1$ and suppose $G^{(m-1)} < G^{[m-1]}$. It is enough to show that each generator of $G^{(m)}$ is contained in $G^{[m]}$. By definition, such generators are of the form $[g, g']$ with $g, g' \in G^{(m-1)}$. Since $g \in G$ and $g' \in G^{[m-1]}$ by assumption, we have $[g, g'] \in G^{[m]}$. The result follows by induction.

(b) We have seen that a group G is solvable if and only if one of its higher commutator groups is trivial. If G is nilpotent, there exists an $m \geqslant 0$ such that $G^{[m]} = 1$. By part (a), this implies that $G^{(m)} = 1$, so G is solvable.

(c) Define for each $1 \leqslant k \leqslant n$ the group

$$U_k \ := \ \big\{(a_{ij})_{i,j} \in \mathrm{GL}_n(R) \bigm| a_{ij} = \delta_{ij} \text{ für alle } i > j - k\big\}.$$

Then $U := U_1$ is the group of upper triangular matrices with ones on the diagonal. We claim that $U^{[m]} < U_{m+1}$. For $m = 0$ this is clear. Suppose that $m > 1$ and that $U^{[m-1]} < U_m$. Then $U^{[m]} = [U_1, U^{[m-1]}] < [U_1, U_m]$, so it suffices to show that $[U_1, U_m] < U_{m+1}$.

Lemma. *Let $a = (a_{ij})_{ij} \in U_1$ and $b = (b_{ij})_{ij} \in U_m$, and write $ab = (c_{ij})_{ij}$ and $ba = (d_{ij})_{ij}$. Then $c_{ij} = d_{ij}$ for all $n \geqslant i > j - (m + 1)$.*

Beweis. Let i be as in the statement of the lemma. We have $c_{ij} = \sum_{k=1}^{n} a_{ik}b_{kj}$ and $d_{ij} = \sum_{k=1}^{n} b_{ik}a_{kj}$. Since $b_{kj} = \delta_{kj}$ for $k > j - m$, it follows that

$$c_{ij} = \textstyle\sum_{k=1}^{n} a_{ik}b_{kj} = \sum_{k=1}^{j-m} a_{ik}b_{kj} + b_{jj}a_{ij} = \sum_{k=1}^{j-m} a_{ik}b_{kj} + a_{ij}.$$

Now $a_{ik} = 0$ whenever $i > k$. Since $i > j - (m + 1)$, the terms in the sum are zero except in the case $i = j - m$, where the sum reduces to $a_{(j-m)(j-m)}b_{(j-m)j} = b_{(j-m)j}$. Thus

$$c_{ij} = \begin{cases} a_{ij} & \text{if } i > j - m, \\ b_{(j-m)j} + a_{ij} & \text{if } i = j - m. \end{cases}$$

Since $b_{ik} = \delta_{ik}$ if $i > k - m$, we have

$$d_{ij} = \textstyle\sum_{k=1}^{n} b_{ik}a_{kj} = \sum_{k=i+m}^{n} b_{ik}a_{kj} + a_{ij}.$$

Now $i > j - (m + 1) \leftrightarrow i + m \geqslant j$. Since $a_{kj} = 0$ for $k > j$ it follows similarly as above that the terms in the sum are zero except in the case $i = j - m$, yielding

$$d_{ij} = \begin{cases} a_{ij} & \text{if } i > j - m, \\ b_{(j-m)j} + a_{ij} & \text{if } i = j - m. \end{cases}$$

□

Now for a and b as in the lemma, we have $[a,b] \in U_{m+1}$ if and only if $ab = ba$ modulo U_{m+1}. This is equivalent to the statement proved in the lemma. Since a and b are arbitrary, it follows that $U^{[m]} < [U_1, U_m] < U_{m+1}$ and the claim holds by induction. In particular, for $m = n-1$ we have $U^{[n-1]} < U_n = \{1\}$, so $U^{[n-1]}$ is trivial; hence U is nilpotent.

(d) Let $G < \mathrm{GL}_2(K)$ be the group of upper triangular matrices. We have seen in the course that G is solvable. Let $U_1 \lhd G$ be as defined in the solution to (c) above. Then G/U_1 is isomorphic the the group $T < \mathrm{GL}_2$ of diagonal matrices. In particular G/U_1 is abelian, and so $G^{[1]} \stackrel{\text{def}}{=} [G,G] \lhd U_1$ by Serie 10, Aufgabe 1b. Since $|K| > 2$, we can choose an element $a \in K \smallsetminus \{\pm 1\}$. Consider $t := \left(\begin{smallmatrix} a & 0 \\ 0 & 1 \end{smallmatrix}\right) \in T$. For any element $u = \left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) \in U_1$ a direct calculation yields $[t,u] = \left(\begin{smallmatrix} 1 & (a^2-1)b \\ 0 & 1 \end{smallmatrix}\right)$. Since $a^2 - 1 \neq 0$, any element of U_1 arises in this way for some choice of b. Thus $U_1 \subset [T, U_1]$. In particular $U_1 \subset [G,G] = G^{[1]}$ and therefore $G^{[1]} = U_1$. It also follows that $U_1 \subset [G, U_1] \subset U_1$ and hence $G^{[2]} \stackrel{\text{def}}{=} [G, U_1] = U_1$. By induction it follows that $G^{[m]} = U_1$ for all $m \geqslant 1$, and G is not nilpotent.

(e) Let H be a subgroup of a nilpotent group G. We claim that $H^{[m]} < G^{[m]}$ for each $m \geqslant 0$. This is clear for $m = 0$. Suppose $m > 0$ and that $H^{[m-1]} < G^{[m-1]}$. By definition $H^{[m]}$ is generated by commutators $[h, h']$ with $h \in H$ and $h' \in H^{[m-1]}$. But then $h' \in G^{[m-1]}$ by assumption. Since $h \in G$, it follows that $[h, h'] \in G^{[m]}$; hence $H^{[m]} < G^{[m]}$. The claim follows by induction. Since G is nilpotent, there exists an m such that $G^{[m]} = \{1\}$. But then $H^{[m]} = \{1\}$ as well, so H is nilpotent.

Now let $N \lhd G$, and consider the quotient group G/N. From the definitions it follows that $(G/N)^{[m]} = G^{[m]}N/N$. Since the $G^{[m]}$ are eventually trivial, it follows immediately that the $(G/N)^{[m]}$ are as well. Hence G/N is nilpotent.

*3. Die *aufsteigende Zentralreihe* einer Gruppe G ist induktiv definiert durch $Z_0 := 1$ und

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

(a) Zeige, dass für alle $i \geqslant 0$ gilt $Z_i \lhd G$.

(b) Zeige, dass G genau dann nilpotent ist, wenn ein n existiert mit $Z_n = G$.

Lösung: (a) We have $Z_0 = \{1\} \lhd G$. Suppose $i > 0$ and Z_{i-1} is normal in G. From the definition, it follows that $z \in Z_i$ if and only if its image in G/Z_{i-1} is in $Z(G/Z_{i-1})$. Since $Z(G/Z_{i-1})$ is normal in G/Z_{i-1}, the subset Z_i is therefore the kernel of the quotient map $G \mapsto \big(G/Z_{i-1}\big)/\big(Z(G/Z_{i-1})\big)$. It is therefore a normal subgroup of G. The result follows by induction.

(b) If G is nilpotent, there exists an integer n such that $G^{[n]} = \{1\}$. We claim that $G^{[n-i]} < Z_i$ for all $0 \leqslant i \leqslant n$. For $i = 0$ we have $G^{[n]} = \{1\} = Z_0$. Suppose the claim holds for some given $i \geqslant 0$. By the definition of $G^{[n-i]}$ for all $z \in G^{[n-i-1]}$ and all $g \in G$ we then have $[g,z] \in G^{[n-i]} < Z_i$. By the definition of Z_{i+1} this means that $z \in Z_{i+1}$. Thus $G^{[n-i-1]} < Z_{i+1}$, and so the claim follows for all i by induction. In particular, for $i = n$ we find that $G^{[0]} = G < Z_n$, so $Z_n = G$.

Conversely, suppose there exists an n such that $Z_n = G$. Again we claim that $G^{[n-i]} < Z_i$ for all $0 \leqslant i \leqslant n$, but this time we proceed by reverse induction on i. For $i = n$, we have $G^{[0]} = G = Z_n$. Let $i < n$ and suppose that $G^{[n-(i+1)]} < Z_{i+1}$. Then $G^{[n-i]} = [G, G^{[n-(i+1)]}] < [G, Z_{i+1}]$. The definition of Z_{i+1} means that $[g, z] \in Z_i$ for all $g \in G$ and $z \in Z_{i+1}$. Thus $G^{[n-i]} < [G, Z_{i+1}] < Z_i$ and the claim follows. In particular, for $i = 0$ we find that $G^{[n]} < Z_0 = \{1\}$, so $G^{[n]} = \{1\}$ and G is nilpotent.

4. Zeige, dass für jedes $n \geqslant 1$ die Gruppe der orthogonalen Matrizen $\mathrm{O}_n(\mathbb{R})$ das semidirekte Produkt $\mathrm{SO}_n(\mathbb{R}) \rtimes C_2$ ist.

   Lösung: Since $\mathrm{SO}_n(\mathbb{R})$ is the kernel of the surjective homomorphism $\det : \mathrm{O}_n(\mathbb{R}) \to \{\pm 1\}$, it follows that $\mathrm{SO}_n(\mathbb{R})$ is normal of index 2 in $\mathrm{O}_n(\mathbb{R})$. Let $R \in O_n(\mathbb{R})$ be of order 2 with determinant -1, for example, a diagonal matrix with entries in $\{1, -1\}$, such that -1 appears with odd multiplicity. Consider the subgroup $\langle R \rangle = \{I_n, R\} < O_n(\mathbb{R})$. Since $[\mathrm{O}_n(\mathbb{R}) : \mathrm{SO}_n(\mathbb{R})] = 2$ and $R \notin \mathrm{SO}_n(\mathbb{R})$, it follows that $\mathrm{SO}_n(\mathbb{R}) \cdot \langle R \rangle = \mathrm{O}_n(\mathbb{R})$. Now $R \notin \mathrm{SO}_n(\mathbb{R})$ also implies that $\mathrm{SO}_n(\mathbb{R}) \cap \langle R \rangle = I_n$. It follows that $\mathrm{O}_n(\mathbb{R})$ is the inner semidirect product of $\mathrm{SO}_n(\mathbb{R})$ by $\langle R \rangle$. Identifying $\langle R \rangle$ with C_2 yields the desired result.

   Remark: Observe that when n is odd, we may choose $R = -I_n$, in which case $\langle R \rangle$ is normal in $O_n(\mathbb{R})$, the action is trivial, and $O_n(\mathbb{R})$ is the inner direct product $SO_n(\mathbb{R}) \times \{\pm I_n\}$.

5. 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 $N := \mathrm{Norm}_{S_n}(\langle \sigma \rangle)$ and $N' := \mathrm{Stab}_N(1)$. We have $N' \cap \langle \sigma \rangle = 1$, since the only element of $\langle \sigma \rangle$ stabilizing 1 is the identity. On the other hand consider any $\tau \in N$. Since $\langle \sigma \rangle$ 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 $\sigma^{-i}\tau \in N'$, or again $\tau \in \sigma^i N'$. Varying τ this shows that $N = \langle \sigma \rangle N' = N' \langle \sigma \rangle$. All together, we have shown that $N = N' \ltimes \langle \sigma \rangle$.

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

Since $\langle\sigma\rangle \cong \mathbb{Z}/n\mathbb{Z}$, we have $\mathrm{Aut}(\langle\sigma\rangle) \cong \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$, with an element $i + n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^\times$ acting by $\sigma \mapsto \sigma^i$. This image σ^i is another generator of $\langle\sigma\rangle$. 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 ${}^\tau\langle\sigma\rangle = \langle\sigma^i\rangle = \langle\sigma\rangle$, and so $\tau \in N$. Since $N = N'\langle\sigma\rangle$, we may write $\tau = \tau'\sigma^m$ with $\tau' \in N'$ and $1 \leqslant m \leqslant n$. Since $\langle\sigma\rangle$ is abelian, we have

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

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

$$ N \;=\; N' \rtimes \langle\sigma\rangle \;\cong\; \mathbb{Z}/n\mathbb{Z} \rtimes (\mathbb{Z}/n\mathbb{Z})^\times, $$

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 $\varphi(n) := |(\mathbb{Z}/n\mathbb{Z})^\times|$.

6. (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 $b(1+a) \equiv 2 \mod 4$ 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:

$$\begin{tikzcd} G_3\colon & {}^{([0],[1])}([b],[0]) \arrow[d, mapsto, "\varphi"'] \arrow[rr, equal] & & ([3b],[0]) \arrow[d, mapsto, "\varphi"'] \\ G_7\colon & {}^{([d],[1])}([bc],[0]) = ([7bc],[0]) & \overset{?}{=} & ([3bc],[0]) \end{tikzcd}$$

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.