Musterlösung 9

Exponent, Homomorphismen, Automorphismen, Normalteiler, Faktorgruppen

1. Zeige: Jede Gruppe vom Exponenten 2 ist abelsch.

   Lösung: Nach Voraussetzung gilt $g^2 = e$ für alle $g \in G$, wobei e das Einselement von G ist. Es ist zu zeigen, dass $gh = hg$ für alle $g, h \in G$ gilt.

   1. Weg: Seien $g, h \in G$ beliebig. Nach Voraussetzung gilt $ghgh = e$, sowie $gg = e$ und $hh = e$, und somit

$$gh = geh = g(ghgh)h = (gg)hg(hh) = ehge = hg.$$

   2. Weg: Zunächst stellen wir fest, dass für jedes $g \in G$ die Voraussetzung $gg = e$ gleichbedeutend zu $g = g^{-1}$ ist. Seien also $g, h \in G$ beliebig. Nach Voraussetzung ist $gh = (gh)^{-1}$. Es gilt aber auch $(gh)^{-1} = h^{-1}g^{-1}$ und somit (da $g^{-1} = g$ und $h^{-1} = h$ ist) gilt $(gh)^{-1} = hg$. Wir haben also gezeigt, dass $gh = (gh)^{-1} = h^{-1}g^{-1} = hg$ gilt.

*2. Zeige, dass für jede natürliche Zahl $m \geqslant 3$ eine endliche Gruppe vom Exponenten m existiert, die nicht abelsch ist.

   Hinweis: Untersuche Diedergruppen und Gruppen der Form

$$\begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix} < \mathrm{GL}_3(\mathbb{Z}/m\mathbb{Z}).$$

   Lösung: Zunächst betrachten wir die Diedergruppen D_m für $m \geqslant 3$, die alle nicht abelsch sind. Die darin enthaltenen Rotationen haben alle eine Ordnung, die m teilt, wobei eine Rotation der genauen Ordnung m auftritt. Da die übrigen Elemente von D_m alles Spiegelungen der Ordnung 2 sind, ist der Exponent von D_m somit gleich dem kleinsten gemeinsamen Vielfachen von m und 2. Für jedes gerade $m \geqslant 4$ ist daher D_m eine endliche Gruppe vom Exponenten m, die nicht abelsch ist.

   Weiter betrachten wir für jedes $m \geqslant 2$ die Untergruppen

$$U_m = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \in \mathrm{GL}_3(\mathbb{Z}/m\mathbb{Z}) \ : \ a, b, c \in \mathbb{Z}/m\mathbb{Z} \right\}$$

von $\mathrm{GL}_3(\mathbb{Z}/m\mathbb{Z})$. Diese sind nicht abelsch, da beispielsweise

$$B = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{und} \quad C = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

nicht kommutieren. Jedes Element A von U_m lässt sich schreiben als $A = E + N$, wobei E die Einheitsmatrix und N eine nilpotente Matrix mit $N^3 = 0$ ist. Da E und N kommutieren, kann für die Berechnung der i-ten Potenz eines solchen Elements der binomische Lehrsatz angewendet werden. Es ergibt sich somit

$$A^i = (E+N)^i = E + iN + \frac{i(i-1)}{2} N^2.$$

Für die obige Matrix B gilt demnach

$$B^i = \begin{pmatrix} 1 & i & \frac{i(i-1)}{2} \\ 0 & 1 & i \\ 0 & 0 & 1 \end{pmatrix},$$

insbesondere $B^i \neq E$, falls i nicht durch m teilbar ist. Die Ordnung von B ist also ein Vielfaches von m, und der Exponent von U_m folglich ebenso.

Falls m ungerade ist, gilt $(m-1)/2 \in \mathbb{Z}^{>0}$, daher ist $m(m-1)/2$ durch m teilbar und $m(m-1)/2 = 0$ in $\mathbb{Z}/m\mathbb{Z}$. Nach obiger Formel gilt deshalb $A^m = E$ für alle $A \in U_m$, also ist der Exponent von U_m ein Teiler von m.

Somit ist für jedes ungerade $m \geqslant 3$ die Gruppe U_m endlich nicht-abelsch mit Exponenten m.

Bemerkung: Falls m oben gerade ist, gilt $m/2 \in \mathbb{Z}^{>0}$ und somit $m(m-1)/2 = m \cdot (m/2 - 1) + m/2 = m/2 \neq 0$ in $\mathbb{Z}/m\mathbb{Z}$. Daher ist in diesem Fall $B^m \neq E$ und wegen $2m(2m-1)/2 = m(2m-1) = 0$ in $\mathbb{Z}/m\mathbb{Z}$ hat B die Ordnung $2m$ und es gilt $A^{2m} = E$ für alle $A \in U_m$, d. h. U_m ist vom Exponenten $2m$.

3. (a) Seien G, H endliche Gruppen und seien $|G|$ und $|H|$ teilerfremd. Zeige, dass jeder Homomorphismus $\varphi : G \to H$ trivial ist, also $\varphi(x) = 1_H$ für alle $x \in G$.

   (b) Sei G eine Gruppe, seien H und H' endliche Untergruppen und seien $|H|$ und $|H'|$ teilerfremd. Zeige, dass $H \cap H' = \{1_G\}$ gilt.

Lösung: (a) Seien $n := |G|$ und $m := |H|$. Sei $\varphi : G \to H$ ein Homomorphismus und sei $x \in G$ beliebig. Sei k die Ordnung von $\varphi(x)$. Nach dem Satz von Lagrange gilt $k|m$. Zudem gilt ebenfalls nach dem Satz von Lagrange, dass die Ordnung von x ein Teiler von n ist, also $x^n = 1_G$ und somit $\varphi(x)^n = \varphi(x^n) = 1_H$. Also gilt $k|n$. Da n und m teilerfremd sind, folgt daraus $k = 1$, also $\varphi(x) = 1_H$.

(b) Seien $n := |H|$, $m := |H'|$ und $k := |H \cap H'|$. Nach dem Satz von Lagrange gilt $k|n$ und $k|m$, also $k = 1$, da n und m teilerfremd sind. Somit besteht $H \cap H'$ nur aus dem Einselement.

Variante, analog zu (a): Seien $n := |H|$ und $m := |H'|$. Sei $x \in H \cap H'$ beliebig und sei k die Ordnung von x. Nach dem Satz von Lagrange gilt $k|n$ und $k|m$ und somit $k = 1$, da n und m teilerfremd sind.

4. Finde alle Isomorphieklassen von Gruppen der Ordnung höchstens 7.

   Lösung: Wir wissen bereits, dass jede Gruppe mit genau einem Element oder genau p Elementen, für eine Primzahl p, zyklisch ist. Für $n \in \{1, 2, 3, 5, 7\}$ gibt es also je genau eine Isomorphieklasse von Gruppen der Ordnung n. Es bleiben noch die Gruppen der Ordnung 4 und 6.

   Sei G eine Gruppe mit 4 Elementen. Da die Ordnung jedes Elements die Gruppenordnung teilt, hat jedes Element Ordnung 1 (das Neutralelement e), 2 oder 4. Wenn es ein Element der Ordnung 4 gibt, ist G von diesem Element erzeugt, also zyklisch. Sonst ist die Ordung jedes von e verschiedenen Elements gleich 2. Deshalb ist der Exponent von G gleich 2. Wegen Aufgabe 1 ist dann G abelsch. Nach dem Klassifikationssatz für endliche abelsche Gruppen gibt es nur eine Möglichkeit, nämlich $G \cong (\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$. Wir haben somit gezeigt, dass es genau zwei Isomorphieklassen von Gruppen der Ordnung 4 gibt, nämlich die zyklischen Gruppen und Gruppen, die zu $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z})$ isomorph sind.

   Sei jetzt G eine Gruppe mit 6 Elementen. Die Ordnung jedes Elements muss entweder 1 (das Neutralelement e), 2, 3 oder 6 sein. Wir unterscheiden folgende Fälle:

   - G enthält ein Element der Ordnung 6. Dann ist G von diesem Element erzeugt, also zyklisch.

   Nun nehmen wir an, G sei nicht zyklisch.

   Lemma: Es existieren ein Element x der Ordnung 2 und ein Element y der Ordnung 3.

   Beweis: Wir nehmen zuerst (ad absurdum) an, jedes von e verschiedene Element von G habe Ordnung 2. Dann wäre G abelsch nach Aufgabe 1. Je zwei von einander und von e verschiedene Elemente von G erzeugen dann eine Untergruppe mit 4 Elementen, im Widerspruch zum Satz von Lagrange. Es existiert also ein Element der Ordnung 3.

   Nun nehmen wir (ad absurdum) an, jedes von e verschiedene Element habe Ordnung 3. Sei y_1 ein solches Element, und sei $y_2 \in S_3 \setminus \langle y_1 \rangle$. Dann sind (unter Verwendung der Kürzungsregeln und der Eindeutigkeit des Inversen) die Elemente $e, y_1, y_1^2, y_2, y_2^2, y_1 y_2, y_1 y_2^2$ paarweise verschieden, also $|G| \geqslant 7$, Widerspruch. $\square$

   Es verbleiben noch die folgenden beiden Fälle:

   - $xy = yx$. Dann ist $(xy)^2 = x^2 y^2 = y^{-1} \neq e$ und $(xy)^3 = x^3 y^3 = x \neq e$ und ausserdem $xy \neq e$; also hat xy die Ordnung 6 und wir sind im ersten Fall.

- $xy \neq yx$. Die Ordnungen von x und y implizieren $xy, yx, xy^2 \neq e, x, y, y^2$. Somit besteht G aus den 6 verschiedenen Elementen e, x, y, y^2, xy, yx, und es gilt $yx = xy^2$. Wir erhalten einen Isomorphismus $G \to D_3$ durch $x \mapsto S$ und $y \mapsto T$, wobei S eine Spiegelung und T eine Rotation der Ordnung 3 ist.

Wir haben also gezeigt, dass es genau zwei Isomorphieklassen von Gruppen der Ordnung 6 gibt, nämlich zyklische Gruppen und solche, die zu D_3 isomorph sind.

Insgesamt gibt es also 9 Isomorphieklassen von Gruppen der Ordnung höchstens 7.

5. Die *Quaternionengruppe* ist die Untergruppe $Q := \{\pm 1, \pm i, \pm j, \pm k\}$ der multiplikativen Gruppe der Hamiltonschen Quaternionen $\mathbb{H} = \mathbb{R} \oplus i\mathbb{R} \oplus j\mathbb{R} \oplus k\mathbb{R}$.

   Zeige: In Q sind alle Untergruppen normal, aber Q ist nicht abelsch.

   Lösung: We begin by identifying the subgroups of Q. Since $|Q| = 8$, all subgroups have order 1, 2, 4, or 8. The only subgroup of order 1 is $\{1\}$, and the only subgroup of order 8 is Q. Since $(\pm i)^2 = (\pm j)^2 = (\pm k)^2 = -1 \neq 1$, the only element of order 2 of Q is -1. Therefore the only subgroup of order 2 is $\langle -1 \rangle$. Any subgroup of order 4 must therefore contain one of the elements $\pm i$, $\pm j$, $\pm k$. Since each of these has order 4, the subgroups of order 4 are the cyclic subgroups generated by them. These are precisely $\langle i \rangle = \{\pm 1, \pm i\}$ and $\langle j \rangle$ and $\langle k \rangle$.

   The subgroups $\{1\}$ and Q are always normal in Q. By construction -1 commutes with every element of Q; hence $\langle -1 \rangle$ is normal. (In fact we have $Z(G) = \langle -1 \rangle$.) The subgroups of order 4 have index 2 and are therefore normal. (In fact we have ${}^{j}\langle i \rangle = \langle {}^{j}i \rangle = \langle -i \rangle = \langle i \rangle$ and so on.)

6. Eine Untergruppe $H < G$, welche unter allen Automorphismen von G in sich übergeht, heisst eine *charakteristische Untergruppe von G*.

   (a) Bestimme alle charakteristischen Untergruppen von $(\mathbb{Z}/4\mathbb{Z})^2$.

   (b) Bestimme alle charakteristischen Untergruppen von D_4.

   (c) Bestimme alle charakteristischen Untergruppen von Q.

   Lösung: First observe that $\{e\}$ and G are always characteristic subgroups of G. Let φ be an automorphism of G. In the following we make repeated use of the fact that if $g \in G$ has order n, then so does $\varphi(g) \in G$.

   (a) Let $G := (\mathbb{Z}/4\mathbb{Z})^2$. For any element $\binom{a}{b} \in G$ we have $2\binom{a}{b} = \binom{2a}{2b}$ and $4\binom{a}{b} = \binom{4a}{4b} = \binom{0}{0}$. Thus

$$\begin{pmatrix} a \\ b \end{pmatrix} \text{ has order } \begin{cases} 1 & \text{if } \binom{a}{b} = \binom{0}{0}, \\ 2 & \text{if } \binom{a}{b} \in (2\mathbb{Z}/4\mathbb{Z})^2 \smallsetminus \left\{\binom{0}{0}\right\}, \\ 4 & \text{otherwise.} \end{cases}$$

Claim: Any characteristic subgroup containing an element of order 2 contains all elements of order 2, and any characteristic subgroup containing an element of order 4 contains all elements of order 4.

To prove this observe first that $\mathrm{Aut}(G) = \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$. The elements of order 2 are $\binom{2}{0}$, $\binom{2}{2}$, $\binom{0}{2}$ and permuted transitively by multiplication with $\left(\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$. Thus if a characteristic subgroup contains one of them, it contains all of them.

Next consider any element $\binom{a}{b}$ of order 4. Then at least one of a, b is equal to ± 1. Set $g := \left(\begin{smallmatrix}a&0\\b&1\end{smallmatrix}\right)$ if $a = \pm 1$ and $g := \left(\begin{smallmatrix}a&1\\b&0\end{smallmatrix}\right)$ otherwise. In both cases we have $g \in \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$ and $g\binom{1}{0} = \binom{a}{b}$. Thus if a characteristic subgroup contains $\binom{a}{b}$, it also contains $g^{-1}\binom{a}{b} = \binom{1}{0}$. For any other element $\binom{a'}{b'}$ of order 4 there likewise exists an element $g' \in \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z})$ with $g'\binom{1}{0} = \binom{a'}{b'}$, which is therefore also contained in the characteristic subgroup. This finishes the proof of the claim.

Since the elements of order 4 generate G, the claim implies that the only characteristic subgroup containing an element of order 4 is G itself. Any other non-trivial characteristic subgroup must contain an element of order 2 and hence all elements of order 2, and must therefore be $(2\mathbb{Z}/4\mathbb{Z})^2$. Conversely, being the subset of all elements of order 1 or 2, this is already invariant under any automorphism of G; hence it is a characteristic subgroup. All in all the characteristic subgroups of $(\mathbb{Z}/4\mathbb{Z})^2$ are therefore $(\mathbb{Z}/4\mathbb{Z})^2$ and $(2\mathbb{Z}/4\mathbb{Z})^2$ and $\{0\}$.

(b) Recall that $D_4 = \{1, T, T^2, T^3, S, ST, ST^2, ST^3\}$, where T is a fundamental rotation and S is a reflection through an axis of symmetry of the square.

For any $i \in \{0, 1, 2, 3\}$ consider the map

$$D_4 \to D_4, \quad T^j \mapsto T^j, \quad ST^j \mapsto ST^{j+i}.$$

By explicit calculation using the relation $STS^{-1} = T^{-1}$ we show that this is a homomorphism. Being bijective, it is therefore an automorphism of D_4. For any two reflections ST^j and $ST^{j'}$ we can find an automorphism φ of this form with $\varphi(ST^j) = ST^{j'}$. Thus any characteristic subgroup of D_4 which contains one reflection contains all reflections. In particular it contains S and ST, which generate D_4. Thus the only characteristic subgroup containing a reflection is D_4 itself.

It remains to consider the subgroups of $\langle T \rangle$. Since $T^{\pm 1}$ are the only elements of D_4 of order 4, any automorphism of D_4 must send T to one of $T^{\pm 1}$. Thus it sends $\langle T \rangle$ to $\langle T^{\pm 1} \rangle = \langle T \rangle$; hence $\langle T \rangle$ is a characteristic subgroup of D_4. Likewise it follows that any automorphism of D_4 sends T^2 to $(T^{\pm 1})^2 = T^2$; hence $\langle T^2 \rangle$ is a characteristic subgroup of D_4. The only other subgroup of $\langle T \rangle$ is $\{1\}$, which is already characteristic.

In summary, the characteristic subgroups of D_4 are $\{1\}$, $\langle T \rangle$, $\langle T^2 \rangle$ and D_4.

(c) By the solution to exercise 5 the subgroups of Q are 1, $\langle -1\rangle$, $\langle i\rangle$, $\langle j\rangle$, $\langle k\rangle$, and Q. The homomorphism of Q defined by

$$\begin{aligned} \pm 1 &\to \pm 1 \\ \pm i &\to \pm j \\ \pm j &\to \pm k \\ \pm k &\to \pm i \end{aligned}$$

is an automorphism. By construction it sends $\langle i\rangle$ to $\langle j\rangle$ to $\langle k\rangle$ to $\langle i\rangle$. Thus none of these subgroups is characteristic. Since $\langle -1\rangle$ is the only subgroup of order 2, it is invariant under every automorphism of Q and hence characteristic. In summary, the characteristic subgroups of Q are therefore $\{1\}$, $\langle -1\rangle$, and Q.

Remark: In fact $Z(D_4) = \langle T^2\rangle$ and $Z(Q) = \langle -1\rangle$, and the center of a group is always a characteristic subgroup.

7. Zeige: Ist ein Normalteiler N einer Gruppe G im Zentrum von G enthalten und G/N zyklisch, so ist G abelsch.

   Lösung: Sei G/N erzeugt von xN für ein $x \in G$. Für jedes Element g von G gibt es dann eine ganze Zahl n mit $gN = x^n N$, also insbesondere mit $g \in x^n N$. Daher erzeugen N und x die ganze Gruppe G. Da sowohl N (als Teilmenge des Zentrums von G) als auch x im Zentralisator G_x von x liegen und $Z_G(x)$ eine Untergruppe ist, folgt deshalb $G_x = G$. Dies ist äquivalent dazu, dass x im Zentrum von G liegt. Das Zentrum enthält aber auch N, also ausserdem die von N und x erzeugte Untergruppe. Somit ist es ebenfalls gleich ganz G. Daher ist G abelsch.

   Variante: Für beliebige Elemente g, h gibt es ganze Zahlen m und n mit $gN = x^m N$ und $hN = x^n N$. Daher existieren $a, b \in N \subset Z(G)$ mit $g = x^m a$ und $h = x^n b$. Da a und b im Zentrum liegen, folgt

   $$gh = x^m a x^n b = x^m x^n ab = x^n x^m ba = x^n b x^m a = hg.$$

   Somit ist G abelsch.