Musterlösung Serie 2

Ordnung, Homo-, Iso-, Automorphismen

1. Bestimme die Ordnungen der folgenden Gruppenelemente:

   (a) Von i und $e^{i\sqrt{3}\,\pi}$ und $e^{\frac{2\pi i}{17}}$ in der Gruppe $\mathbb{C}^\times$.

   (b) Von $A = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$, $B = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 1 \end{smallmatrix}\right)$, AB und $C = \left(\begin{smallmatrix} 2 & 3 \\ 1 & 4 \end{smallmatrix}\right)$ in der Gruppe $\mathrm{GL}_2(\mathbb{C})$.

   (c) Von 1, 2, 3 in der Gruppe $\mathbb{F}_{17}^\times$.

   Lösung: Generell gilt für jedes Element g einer Gruppe G: Jede ganze Zahl $n > 0$ mit $g^n = 1$ ist ein Vielfaches der Ordnung von g.

   Denn in diesem Fall hat g bereits eine endliche Ordnung $m \geqslant 1$. Schreiben wir dann $n = ma + b$ mit $a, b \in \mathbb{Z}$ und $0 \leqslant b < m$, so erhalten wir wegen $g^m = 1$ auch $g^b = (g^m)^a g^b = g^{ma+b} = g^n = 1$. Da aber m die kleinste positive ganze Zahl mit $g^m = 1$ ist, muss dann $b = 0$ sein, also $n = ma$, wie behauptet.

   (a) Wegen $i^4 = 1$ ist die Ordnung von i ein Teiler von 4, und wegen $i^2 = -1 \neq 1$ ist sie kein Teiler von 2. Somit hat i die Ordnung 4.

   Sodann erfüllt eine reelle Zahl r die Gleichung $e^{ir} = 1$ genau dann, wenn $r = 2\pi k$ ist für ein $k \in \mathbb{Z}$, das heisst, wenn $r/2\pi \in \mathbb{Z}$ ist. Für $n \in \mathbb{Z}_{>0}$ ist daher $(e^{i\sqrt{3}\,\pi})^n = e^{i\sqrt{3}\,n\pi} = 1$ genau dann, wenn $\sqrt{3}\,n\pi/2\pi = \sqrt{3}\,n/2$ in $\mathbb{Z}$ liegt. Da $\sqrt{3}$ irrational ist, gilt dies für keine ganze Zahl $n > 0$; somit hat $e^{i\sqrt{3}\,\pi}$ die Ordnung ∞.

   Weiter ist $(e^{\frac{2\pi i}{17}})^n = e^{\frac{2\pi i n}{17}} = 1$ genau dann, wenn $\frac{2\pi n}{17}/2\pi = \frac{n}{17}$ in $\mathbb{Z}$ liegt, das heisst, wenn n durch 17 teilbar ist. Somit hat $e^{\frac{2\pi i}{17}}$ die Ordnung 17.

   (b) Direkte Rechnung zeigt $A^2 = -I_2$ und folglich $A^4 = I_2$. Somit ist die Ordnung von A ein Teiler von 4, aber kein Teiler von 2, also gleich 4.

   Analog berechnen wir $B^2 = \left(\begin{smallmatrix} -1 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ und $B^3 = -I_2$ und folglich $B^6 = I_2$. Somit ist die Ordnung von B ein Teiler von 6, aber kein Teiler von 2 oder 3, also gleich 6.

   Sodann berechnen wir $AB = \left(\begin{smallmatrix} 1 & -1 \\ 0 & 1 \end{smallmatrix}\right)$. Durch Induktion folgt daraus $(AB)^n = \left(\begin{smallmatrix} 1 & -n \\ 0 & 1 \end{smallmatrix}\right)$ für alle $n \geqslant 1$. Da dies $\neq I_2$ ist, hat AB unendliche Ordnung.

   Bemerkung: Dies gilt, obwohl sowohl A als auch B endliche Ordnung haben! Daraus folgt insbesondere, dass die beiden Elemente endlicher Ordnung eine unendliche Untergruppe $\langle A, B \rangle$ von $\mathrm{GL}_2(\mathbb{C})$ erzeugen.

   Schliesslich gilt $\det(C) = 5$. Für alle $n \geqslant 1$ folgt daraus $\det(C^n) = 5^n \neq 1$ und daher $C^n \neq I_2$. Somit hat auch C unendliche Ordnung.

(c) Die Ordnung jedes Elements von $\mathbb{F}_{17}^\times$ ist ein Teiler der Gruppenordnung $|\mathbb{F}_{17}^\times| = 17 - 1 = 16$. Somit sind nur die Ordnungen $1, 2, 4, 8, 16$ möglich. Da 1 das neutrale Element von $\mathbb{F}_{17}^\times$ ist, hat es die Ordnung 1. Für die anderen beiden Elemente berechnen wir modulo 17:

$$2^2 = 4, \quad 2^4 = 16 = -1, \quad 2^8 = (-1)^2 = 1; \quad \text{beziehungsweise}$$

$$3^2 = 9, \quad 3^4 = 81 = -4, \quad 3^8 = (-4)^2 = 16 = -1, \quad 3^{16} = 1.$$

Daher hat 2 die Ordnung 8 und 3 die Ordnung 16.

*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: Für jedes $m \geqslant 3$ ist die Diedergruppe D_m nicht abelsch, weil eine Drehung um den Winkel $\frac{2\pi}{m}$ nicht mit einer Spiegelung kommutiert. Diese Drehung hat ausserdem die genaue Ordnung m. Andererseits hat jede Drehung $g \in D_m$ ein Vielfaches des Winkels $\frac{2\pi}{m}$ und erfüllt somit $g^m = 1$; und jede Spiegelung in D_m hat die genaue Ordnung 2. Der Exponent von G ist somit gleich $\mathrm{kgV}\{m, 2\}$. Für jedes gerade $m \geqslant 4$ ist D_m daher eine nicht abelsche endliche Gruppe vom Exponenten m. (Für ungerades m erhalten wir den geraden Exponenten $2m$; darum benötigen wir noch eine andere Konstruktion.)

Für jedes $m \geqslant 2$ betrachte die Untergruppe

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

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

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

nicht miteinander kommutieren. Jedes Element A von U_m hat die Form $A = E + N$ mit der Einheitsmatrix E und einer nilpotenten Matrix N mit $N^3 = 0$. 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

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

Für die obige Matrix B gilt zum Beispiel

$$B^i = \begin{pmatrix} 1 & i & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Insbesondere gilt $B^i = E$ genau dann, wenn i durch m teilbar ist, und B hat die Ordnung m. Folglich ist der Exponent von U_m ein Vielfaches von m.

Falls m ungerade ist, gilt $\frac{m-1}{2} \in \mathbb{Z}$ und somit $\frac{m(m-1)}{2} \equiv 0 \bmod (m)$. Die Gleichung (1) impliziert dann $A^m = E$ für alle $A \in U_m$. Also ist der Exponent von U_m ein Teiler von m, und somit gleich m. Für jedes ungerade $m \geqslant 3$ ist U_m daher eine endliche nicht-abelsche Gruppe vom Exponenten m.

(Für gerades $m \geqslant 2$ gilt $\frac{m(m-1)}{2} \equiv \frac{m}{2} \not\equiv 0 \bmod (m)$; die entsprechende Rechnung liefert daher nur $A^{2m} = E$. Tatsächlich hat die obige Matrix C die genaue Ordnung $2m$; somit hat U_m den Exponenten $2m$.)

3. (a) Seien G und H endliche Gruppen von teilerfremder Ordnung. 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, und seien H und H' endliche Untergruppen von teilerfremder Ordnung. Zeige, dass $H \cap H' = \{1_G\}$ gilt.

   Lösung: (a) Seien $m := |G|$ und $n := |H|$. Sei $\varphi : G \to H$ ein Homomorphismus und sei $x \in G$ beliebig. Nach dem Satz von Lagrange für G gilt dann $x^m = 1_G$ und somit auch $\varphi(x)^m = \varphi(x^m) = \varphi(1_G) = 1_H$; und nach dem Satz von Lagrange für H gilt $\varphi(x)^n = 1_H$. Also ist die Ordnung von $\varphi(x)$ ein Teiler von m und von n. Nach Voraussetzung muss diese Ordnung daher gleich 1 sein und somit $\varphi(x) = 1_H$.

   (b) Nach dem Satz von Lagrange ist $|H \cap H'|$ ein Teiler von $|H|$ und von $|H'|$. Da diese teilerfremd sind, kommt nur $|H \cap H'| = 1$ in Frage. Somit ist $H \cap H' = \{1_G\}$.

4. Seien G eine endliche Gruppe der Ordnung n und X eine beliebige Menge der Kardinalität n. Zeige:

   (a) Für jede Bijektion $\varphi\colon X \to G$ existiert genau eine Gruppenstruktur auf X, so dass φ ein Isomorphismus wird.

   (b) Zwei Bijektionen $\varphi, \psi\colon X \to G$ liefern dieselbe Gruppenstruktur auf X genau dann, wenn die Bijektion $\gamma := \psi \circ \varphi^{-1}\colon G \to G$ ein Automorphismus ist.

   (c) Die Anzahl der Gruppenstrukturen auf X, für die X isomorph zu G wird, ist $n!/|\operatorname{Aut}(G)|$.

   Lösung:

(a) Sei $\circ$ eine Gruppenstruktur mit Einselement 1_X auf X, so dass φ ein Isomorphismus wird. Für alle $x, y \in X$ gilt dann $\varphi(x \circ y) = \varphi(x)\varphi(y)$ und folglich $x \circ y = \varphi^{-1}(\varphi(x)\varphi(y))$; und weiter folgt aus $\varphi(1_X) = 1_G$ auch $1_X = \varphi^{-1}(1_G)$. Somit bestimmt φ die Gruppenstruktur auf X. Umgekehrt definieren diese Formeln eine binäre Operation $\circ\colon X \times X \to X$ und ein Element $1_X \in X$. Dass diese eine Gruppenstruktur auf X induzieren, folgt mit $1_X := \varphi^{-1}(1_G)$ aus den Rechnungen

$$\begin{aligned}
\forall\, x, y, z \in X\colon \quad x \circ (y \circ z) &= \varphi^{-1}\big(\varphi(x)\varphi(\varphi^{-1}(\varphi(y)\varphi(z)))\big) \\
&= \varphi^{-1}\big(\varphi(x)\varphi(y)\varphi(z)\big) \\
&= \varphi^{-1}\big(\varphi(\varphi^{-1}(\varphi(x)\varphi(y)))\varphi(z)\big) \\
&= (x \circ y) \circ z; \\
\forall\, x \in X\colon \quad 1_X \circ x &= \varphi^{-1}\big(\varphi(1_G)\varphi(x)\big) \\
&= \varphi^{-1}\big(\varphi(1_G x)\big) \\
&= \varphi^{-1}(\varphi(x)) \;=\; x; \\
\forall\, x \in X\colon \quad \varphi^{-1}(\varphi(x)^{-1}) \circ x &= \varphi^{-1}\big(\varphi(x)^{-1}\varphi(x)\big) \\
&= \varphi^{-1}(1_G) \;=\; 1_X.
\end{aligned}$$

(b) Für jede Gruppenstruktur ist das Einselement eindeutig bestimmt; daher sind die induzierten Gruppenstrukturen genau dann gleich, wenn die binären Operationen gleich sind. Nach der Rechnung in (a) ist dies äquivalent zu

$$\forall\, x, y \in X\colon\; \varphi^{-1}(\varphi(x)\varphi(y)) \;=\; \psi^{-1}(\psi(x)\psi(y)).$$

Aufgrund der Bijektivität von ψ ist dies äquivalent zu

$$\forall\, x, y \in X\colon\; \psi(\varphi^{-1}(\varphi(x)\varphi(y))) \;=\; \psi(x)\psi(y).$$

Da auch φ eine Bijektion ist, ist dies weiter äquivalent zu

$$\forall\, g, h \in G\colon\; \psi(\varphi^{-1}(gh)) \;=\; \psi(\varphi^{-1}(g))\psi(\varphi^{-1}(h)),$$

das heisst zu

$$\forall\, g, h \in G\colon\; \gamma(gh) \;=\; \gamma(g)\gamma(h).$$

Da γ bereits bijektiv ist, bedeutet dies genau, dass γ ein Automorphismus von G ist.

(c) Sei S_G die symmetrische Gruppe aller Bijektionen $G \to G$ mit der Komposition und dem neutralen Element id_G. Fixiere irgendeine Bijektion $\varphi\colon X \to G$. Dann haben alle Bijektionen $X \to G$ die Form $\sigma \circ \varphi$ für ein $\sigma \in S_G$.

Betrachte eine Gruppenstruktur auf X, für die X isomorph zu G wird. Dann existiert ein Gruppenisomorphismus $X \to G$. Dieser ist insbesondere eine Bijektion, hat also die Form $\sigma \circ \varphi$ für ein $\sigma \in S_G$. Nach (a) bestimmt er ausserdem die Gruppenstruktur auf X.

Betrachte nun zwei Elemente $\sigma, \tau \in S_G$. Nach (b) induzieren $\sigma \circ \varphi$ und $\tau \circ \varphi$ genau dann dieselbe Gruppenstruktur auf X, wenn

$$(\tau \circ \varphi) \circ (\sigma \circ \varphi)^{-1} \; = \; \tau \circ \varphi \circ \varphi^{-1} \circ \sigma^{-1} \; = \; \tau \circ \sigma^{-1}$$

ein Automorphismus von G ist. Nun ist aber

$$\tau \circ \sigma^{-1} \in \operatorname{Aut}(G) \iff \tau \in \operatorname{Aut}(G) \circ \sigma \iff \operatorname{Aut}(G) \circ \tau = \operatorname{Aut}(G) \circ \sigma.$$

Zusammen zeigt dies, dass die Gruppenstrukturen auf X, für die X isomorph zu G wird, in Bijektion stehen zu den Rechtsnebenklassen in $\operatorname{Aut}(G)\backslash S_G$. Ihre Anzahl ist daher, unter Benutzung des Satzes von Lagrange, gleich

$$|\operatorname{Aut}(G)\backslash S_G| \; = \; |S_G/\operatorname{Aut}(G)| \; = \; |S_G|/|\operatorname{Aut}(G)| \; = \; n!/|\operatorname{Aut}(G)|.$$

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

   (a) Bestimme alle Untergruppen von Q.

   (b) Zeige: Alle Untergruppen sind normal, aber Q ist nicht abelsch.

   Lösung:

   (a) Since $|Q| = 8$, each subgroup and each element has order 1, 2, 4, or 8. The only subgroup of order 1 is $\{1\}$, and the only subgroup of order 8 is Q. Also $(\pm i)^2 = (\pm j)^2 = (\pm k)^2 = -1 \neq 1$ and $(-1)^2 = 1$ show that $\pm i$, $\pm j$, $\pm k$ have order 4 and -1 has order 2. 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. Furthermore $i^3 = -i$ generates the same cyclic subgroup as i, and likewise for j and k. A complete list of subgroups is therefore
   $$\{1\},\ \langle -1 \rangle,\ \langle i \rangle,\ \langle j \rangle,\ \langle k \rangle,\ G.$$

   (b) The subgroups $\{1\}$ and Q are always normal in Q. By construction -1 commutes with every element of Q; hence the subgroup $\langle -1 \rangle$ 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 ${}^j i = -i$ and therefore ${}^j\langle i \rangle = \langle {}^j i \rangle = \langle -i \rangle = \langle i \rangle$ and so on.)

Die restlichen Aufgaben befassen sich mit unendlichen abelschen Gruppen, welche eine interessante innere Struktur besitzen können.

6. Elemente $g_1, \ldots, g_r$ einer additiv geschriebenen abelschen Gruppe G heissen $\mathbb{Z}$-*linear unabhängig*, wenn für alle $n_1, \ldots, n_r \in \mathbb{Z}$ gilt:

$$n_1 g_1 + \ldots + n_r g_r = 0 \implies n_1 = \ldots = n_r = 0.$$

   Der *Rang von G* ist das Supremum der Menge aller natürlichen Zahlen r, für die $\mathbb{Z}$-linear unabhängige Elemente $g_1, \ldots, g_r \in G$ existieren.

   (a) Zeige, dass der Rang invariant unter Isomorphie ist.

   (b) Betrachte eine natürliche Zahl n und eine Untergruppe G der additiven Gruppe $\mathbb{Q}^{\oplus n}$ mit $\mathbb{Z}^{\oplus n} \subset G$. Bestimme den Rang von G.

   Lösung:

   (a) Betrachte einen Isomorphismus von additiv geschriebenen abelschen Gruppen $\varphi \colon G \xrightarrow{\sim} H$ und Elemente $g_1, \ldots, g_r \in G$. Wegen der Bijektivität von φ und der Eigenschaft $\varphi(0) = 0$ gilt dann für alle $n_1, \ldots, n_r \in \mathbb{Z}$:

$$n_1 g_1 + \ldots + n_r g_r = 0 \iff n_1 \varphi(g_1) + \ldots + n_r \varphi(g_r) \;=\; \varphi(n_1 g_1 + \ldots + n_r g_r) = 0.$$

   Somit sind $g_1, \ldots, g_r$ genau dann $\mathbb{Z}$-linear unabhängig, wenn $\varphi(g_1), \ldots, \varphi(g_r)$ $\mathbb{Z}$-linear unabhängig sind. Daraus folgt, dass G und H denselben Rang haben.

   (b) Die Standardbasis $e_1, \ldots, e_n \in G$ ist $\mathbb{Q}$-linear unabhängig und daher auch $\mathbb{Z}$-linear unabhängig. Also hat G einen Rang $\geqslant n$.

   Betrachte andererseits beliebige Elemente $g_1, \ldots, g_r \in G$ mit $r > n$. Diese sind dann $\mathbb{Q}$-linear abhängig in $\mathbb{Q}^{\oplus n}$; es existieren also $a_1, \ldots, a_r \in \mathbb{Q}$, nicht alle gleich Null, mit $a_1 g_1 + \ldots a_r g_r = 0$. Sei k ein gemeinsamer Nenner von $a_1, \ldots, a_r$ und setze $n_i := k a_i$ für alle $1 \leqslant i \leqslant r$. Dann sind $n_1, \ldots, n_r \in \mathbb{Z}$ nicht alle gleich Null mit $n_1 g_1 + \ldots n_r g_r = 0$. Somit sind $g_1, \ldots, g_r$ nicht $\mathbb{Z}$-linear unabhängig. Zusammen zeigt dies, dass G den Rang n hat.

7. Betrachte eine Primzahl p und die folgenden additiven Untergruppen von $\mathbb{Q}$:

$$\begin{aligned} \mathbb{Z}[\tfrac{1}{p}] &:= \left\{ \tfrac{m}{p^i} \;\middle|\; m \in \mathbb{Z},\ i \in \mathbb{Z}^{\geqslant 0} \right\}, \\ \mathbb{Z}_{(p)} &:= \left\{ \tfrac{m}{n} \;\middle|\; m, n \in \mathbb{Z},\ p \nmid n \right\}. \end{aligned}$$

   Sei G eine der Gruppen $\mathbb{Z}$, $\mathbb{Z}[\frac{1}{p}]$, $\mathbb{Z}_{(p)}$, $\mathbb{Q}$ oder die direkte Summe von zweien davon.

   (a) Bestimme für jede Primzahl q die Untergruppe $\mathrm{Div}_q(G) := \bigcap_{r \geqslant 0} q^r G$.

   (b) Entscheide, welche der fraglichen Gruppen G zueinander isomorph sind.

Lösung:

(a) Eine von Null verschiedene ganze Zahl ist nur durch eine grösste endliche Potenz von q teilbar; daher ist $\mathrm{Div}_q(\mathbb{Z}) = 0$. Sodann gilt $q^r\mathbb{Q} = \mathbb{Q}$ für alle $r \geqslant 0$ und daher $\mathrm{Div}_q(\mathbb{Q}) = \mathbb{Q}$. Für jedes $r \geqslant 0$ gilt weiter $p^r\mathbb{Z}[\frac{1}{p}] = \mathbb{Z}[\frac{1}{p}]$ und daher $\mathrm{Div}_p(\mathbb{Z}[\frac{1}{p}]) = \mathbb{Z}[\frac{1}{p}]$. Andererseits besteht $p^r\mathbb{Z}_{(p)}$ aus allen rationalen Zahlen der Form $\frac{m}{n}$ mit $m, n \in \mathbb{Z}$ und $p^r|m$ und $p \nmid n$. Da ein festes $m \neq 0$ nur durch eine grösste endliche Potenz von q teilbar ist, folgt daraus $\mathrm{Div}_p(\mathbb{Z}_{(p)}) = 0$.

Betrachte nun eine Primzahl $q \neq p$. Aus $\mathbb{Z}[\frac{1}{p}] \subset \mathbb{Z}_{(q)}$ und $\mathrm{Div}_q(\mathbb{Z}_{(q)}) = 0$ folgt dann auch $\mathrm{Div}_q(\mathbb{Z}[\frac{1}{p}]) = 0$. Schliesslich gilt $q^r\mathbb{Z}_{(p)} = \mathbb{Z}_{(p)}$ für alle $r \geqslant 0$ und daher $\mathrm{Div}_q(\mathbb{Z}_{(p)}) = \mathbb{Z}_{(p)}$. Zusammen erhalten wir also die folgende Tabelle:

G	$\mathbb{Z}$	$\mathbb{Z}[\frac{1}{p}]$	$\mathbb{Z}_{(p)}$	$\mathbb{Q}$
$\mathrm{Div}_p(G)$	0	$\mathbb{Z}[\frac{1}{p}]$	0	$\mathbb{Q}$
$\mathrm{Div}_q(G)$	0	0	$\mathbb{Z}_{(p)}$	$\mathbb{Q}$

Ist schliesslich $G = A \oplus B$, so folgt direkt $q^rG = q^rA \oplus q^rB$ für alle $r \geqslant 0$ und daher $\mathrm{Div}_q(G) = \mathrm{Div}_q(A) \oplus \mathrm{Div}_q(B)$.

(b) Nach Aufgabe 6 (b) hat jede der Gruppen $\mathbb{Z}$, $\mathbb{Z}[\frac{1}{p}]$, $\mathbb{Z}_{(p)}$, $\mathbb{Q}$ den Rang 1, und jede direkte Summe von zweien davon den Rang 2. Aus Aufgabe 6 (a) folgt daraus, dass keine der Gruppen $\mathbb{Z}$, $\mathbb{Z}[\frac{1}{p}]$, $\mathbb{Z}_{(p)}$, $\mathbb{Q}$ isomorph zu einer direkten Summe von zweien davon ist. Die Tabelle in (a) zeigt zudem, dass keine der vier ersteren zueinander isomorph sind.

Betrachte nun eine Gruppe der Form $G = A \oplus B$ für $A, B \in \{\mathbb{Z}, \mathbb{Z}[\frac{1}{p}], \mathbb{Z}_{(p)}, \mathbb{Q}\}$. Zusammen mit der Gleichung $\mathrm{Div}_q(G) = \mathrm{Div}_q(A) \oplus \mathrm{Div}_q(B)$ und der Tabelle in (a) erhalten wir die folgende Tabelle für $(\mathrm{Div}_p(G), \mathrm{Div}_q(G))$ mit $q \neq p$:

Fall	$B = \mathbb{Z}$	$B = \mathbb{Z}[\frac{1}{p}]$	$B = \mathbb{Z}_{(p)}$	$B = \mathbb{Q}$
$A = \mathbb{Z}$	$(0, 0)$	$(\mathbb{Z}[\frac{1}{p}], 0)$	$(0, \mathbb{Z}_{(p)})$	$(\mathbb{Q}, \mathbb{Q})$
$A = \mathbb{Z}[\frac{1}{p}]$	$(\mathbb{Z}[\frac{1}{p}], 0)$	$(\mathbb{Z}[\frac{1}{p}] \oplus \mathbb{Z}[\frac{1}{p}], 0)$	$(\mathbb{Z}[\frac{1}{p}], \mathbb{Z}_{(p)})$	$(\mathbb{Z}[\frac{1}{p}] \oplus \mathbb{Q}, \mathbb{Q})$
$A = \mathbb{Z}_{(p)}$	$(0, \mathbb{Z}_{(p)})$	$(\mathbb{Z}[\frac{1}{p}], \mathbb{Z}_{(p)})$	$(0, \mathbb{Z}_{(p)}) \oplus \mathbb{Z}_{(p)})$	$(\mathbb{Q}, \mathbb{Z}_{(p)} \oplus \mathbb{Q})$
$A = \mathbb{Q}$	$(\mathbb{Q}, \mathbb{Q})$	$(\mathbb{Q} \oplus \mathbb{Z}[\frac{1}{p}], \mathbb{Q})$	$(\mathbb{Q}, \mathbb{Q} \oplus \mathbb{Z}_{(p)}))$	$(\mathbb{Q} \oplus \mathbb{Q}, \mathbb{Q} \oplus \mathbb{Q})$

Sei jetzt G isomorph zu $G' = A' \oplus B'$ für $A', B' \in \{\mathbb{Z}, \mathbb{Z}[\frac{1}{p}], \mathbb{Z}_{(p)}, \mathbb{Q}\}$. Dann gilt auch $\mathrm{Div}_p(G) \cong \mathrm{Div}_p(G')$ und $\mathrm{Div}_q(G) \cong \mathrm{Div}_q(G')$, also stimmen die Einträge der obigen Tabelle für die Paare (A, B) und (A', B') bis auf Isomorphie überein. Da wir bereits wissen, dass die Gruppen $\mathbb{Z}$, $\mathbb{Z}[\frac{1}{p}]$, $\mathbb{Z}_{(p)}$, $\mathbb{Q}$ weder zueinander isomorph, noch isomorph zu einer direkten Summe von zweier dieser Gruppen sind, können wir aus der Tabelle ablesen, dass (A', B') gleich

(A, B) oder (B, A) sein muss. Im letzteren Fall ist aber die Abbildung

$$G = A \oplus B \longrightarrow B \oplus A = G', \ (a, b) \mapsto (b, a)$$

ein bijektiver Homomorphismus, also ein Isomorphismus. Somit haben wir gezeigt, dass $A \oplus B \cong A' \cong B'$ genau dann gilt, wenn (A', B') gleich (A, B) oder (B, A) ist.

**8. Sei p eine Primzahl. Für jedes $n \geqslant 0$ setze $\omega_n := \sum_{m=0}^{n} p^{m!}$. Betrachte die Menge

$$G \ := \ \big\{(a, b) \in \mathbb{Q}^{\oplus 2} \ \big| \ \exists\, n_0 \geqslant 0 \ \forall\, n \geqslant n_0 \colon \ a - b \cdot \omega_n \in \mathbb{Z}_{(p)}\big\}.$$

(a) Zeige, dass G eine Untergruppe der additiven Gruppe $\mathbb{Q}^{\oplus 2}$ ist.

(b) Zeige: Es existiert kein $x \in \mathbb{Q}$ mit der Eigenschaft

$$\forall\, r \geqslant 0 \ \exists\, n_0 \geqslant 0 \ \forall\, n \geqslant n_0 \colon \ x - \omega_n \in p^r \mathbb{Z}_{(p)}.$$

(c) Zeige $\mathrm{Div}_p(G) = 0$ und $\mathrm{Div}_q(G) = G$ für jede Primzahl $q \neq p$.

(d) Zeige $[\mathbb{Z}_{(p)} : p\mathbb{Z}_{(p)}] = p$ und $[G : pG] = p$.

(e) Folgere: Die Gruppe G ist isomorph zu keiner der Gruppen in Aufgabe 7.

Lösung:

(a) Für jedes $n \geqslant 0$ gilt $0 - 0 \cdot \omega_n = 0 \in \mathbb{Z}_{(p)}$ und daher $(0, 0) \in G$. Sodann betrachte (a, b), $(a', b') \in G$. Für alle $n \gg 0$ gilt dann $a - b \cdot \omega_n \in \mathbb{Z}_{(p)}$ und $a' - b' \cdot \omega_n \in \mathbb{Z}_{(p)}$ und folglich auch $(a + a') - (b + b') \cdot \omega_n = (a - b \cdot \omega_n) + (a' - b' \cdot \omega_n) \in \mathbb{Z}_{(p)}$. Somit ist $(a + a', b + b') \in G$. Ausserdem ist dann $(-a) - (-b) \cdot \omega_n = -(a - b \cdot \omega_n) \in \mathbb{Z}_{(p)}$ und daher auch $(-a, -b) \in G$. Deshalb ist G eine Untergruppe von $\mathbb{Q}^{\oplus 2}$.

(b) Betrachte ein solches $x \in \mathbb{Q}$ und schreibe $x = \frac{a}{b}$ mit teilerfremden $a, b \in \mathbb{Z}$ und $b > 0$. Dann gilt

$$\forall\, r \geqslant 0 \ \exists\, n_0 \geqslant 0 \ \forall\, n \geqslant n_0 \colon \ a - b \cdot \omega_n \in p^r b \cdot \mathbb{Z}_{(p)}.$$

Hier liegt die linke Seite in $\mathbb{Z}$, und alle rationalen Zahlen auf der rechten Seite haben p^r im Zähler. Somit folgt

$$\forall\, r \geqslant 0 \ \exists\, n_0 \geqslant 0 \ \forall\, n \geqslant n_0 \colon \ a - b \cdot \omega_n \in p^r \cdot \mathbb{Z}.$$

Wäre b durch p teilbar, so würde für $r = 1$ daraus folgen, dass auch a durch p teilbar ist. Somit ist b nicht durch p teilbar. Wähle nun irgendein $m \geqslant 2$ mit $|a|, |b| < p^{m!}$. Da die ω_m paarweise verschieden sind, können wir zusätzlich annehmen, dass $a - b \cdot \omega_m \neq 0$ ist. Dann gilt

$$0 \ < \ |a - b \cdot \omega_m| \ < \ p^{m!} + 2(p^{m!})^2 \ < \ 3p^{2 \cdot m!} \ < \ p^{(m+1)!}.$$

Nimm jetzt $r > (m+1)!$ und darauf $n > m$ mit $a - b \cdot \omega_n \in p^r \cdot \mathbb{Z}$. Dann ist

$$a - b \cdot \omega_m \;=\; (a - b \cdot \omega_n) + b \cdot (\omega_n - \omega_m) \;\in\; p^r \cdot \mathbb{Z} + b \cdot (\omega_n - \omega_m).$$

Hierbei ist

$$\omega_n - \omega_m \;=\; p^{(m+1)!} + \ldots + p^{r!} \;=\; p^{(m+1)!} \cdot \big(1 + \ldots + p^{r! - (m+1)!}\big)$$

genau durch $p^{(m+1)!}$ teilbar, aber nicht durch p^r. Wegen $p \nmid b$ gilt dasselbe für $b \cdot (\omega_n - \omega_m)$. Wegen $r > (m+1)!$ folgt nun auch dasselbe für $a - b \cdot \omega_m$. Aber dies widerspricht den obigen Abschätzungen für $|a - b \cdot \omega_m|$. Somit haben wir einen Widerspruch, und das fragliche x kann nicht existieren.

(c) Ein Paar $(a, b) \in \mathbb{Q}^{\oplus 2}$ liegt in $p^r G$ genau dann, wenn $p^{-r}(a, b)$ in G liegt. Nach der Definition von G ist dies äquivalent zu

$$\exists\, n_0 \geqslant 0 \;\forall\, n \geqslant n_0\colon\;\; a - b \cdot \omega_n \in p^r \mathbb{Z}_{(p)}.$$

Daher ist $(a, b) \in \mathrm{Div}_p(G)$ genau dann, wenn gilt

$$\forall\, r \geqslant 0 \;\exists\, n_0 \geqslant 0 \;\forall\, n \geqslant n_0\colon\;\; a - b \cdot \omega_n \in p^r \mathbb{Z}_{(p)}.$$

Im Fall $b = 0$ bedeutet dies $a \in \mathrm{Div}_p(\mathbb{Z}_{(p)})$ und nach Aufgabe 7 (a) also $a = 0$. Im Fall $b \neq 0$ ist die Bedingung äquivalent zu

$$\forall\, r \geqslant 0 \;\exists\, n_0 \geqslant 0 \;\forall\, n \geqslant n_0\colon\;\; x - \omega_n \in \frac{p^r}{b} \cdot \mathbb{Z}_{(p)}$$

für $x := \frac{a}{b}$. Schreibe $b = p^i c$ mit $i \in \mathbb{Z}$ und $c \in \mathbb{Q}^\times$ ohne p im Zähler oder Nenner. Dann ist $\frac{1}{b} \cdot \mathbb{Z}_{(p)} = \mathbb{Z}_{(p)}$ und folglich

$$\forall\, r \geqslant 0 \;\exists\, n_0 \geqslant 0 \;\forall\, n \geqslant n_0\colon\;\; x - \omega_n \in p^{r-i} \cdot \mathbb{Z}_{(p)}.$$

Dies ist äquivalent zu der Bedingung in (b). Nach (b) haben wir somit einen Widerspruch, und damit ist $\mathrm{Div}_p(G) = 0$ bewiesen.

Für jede Primzahl $q \neq p$ und jedes $r \geqslant 0$ gilt hingegen $q^r \mathbb{Z}_{(p)} = \mathbb{Z}_{(p)}$. Daraus folgt direkt $q^r G = G$ und somit $\mathrm{Div}_q(G) = G$.

(d) Wir zeigen, dass $S := \{0, 1, \ldots, p-1\}$ ein Repräsentantensystem von $\mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)}$ ist. Zunächst betrachte zwei verschiedene $s, s' \in S$. Dann ist $s - s'$ nicht durch p teilbar, also nicht in $p\mathbb{Z}_{(p)}$, und somit folgt $s + p\mathbb{Z}_{(p)} \neq s' + p\mathbb{Z}_{(p)}$.

Sodann betrachte ein beliebiges Element $\frac{m}{n} \in \mathbb{Z}_{(p)}$ mit $m, n \in \mathbb{Z}$ und $p \nmid n$. In dem endlichen Körper $\mathbb{F}_p$ gilt dann $[n] \neq [0]$, also existiert ein $[s] \in \mathbb{F}_p$ mit $[m] = [s] \cdot [n]$. Daher existiert ein $s \in S$ mit $m \equiv sn$ modulo (p). Schreibe $m = sn + pk$ mit $k \in \mathbb{Z}$. Dann folgt

$$\frac{m}{n} \;=\; \frac{sn + pk}{n} \;=\; s + p \cdot \frac{k}{n} \;\in\; s + p\mathbb{Z}_{(p)}.$$

Zusammen zeigt dies, dass S ein Repräsentantesystem von $\mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)}$ ist. Daher ist $[\mathbb{Z}_{(p)} : p\mathbb{Z}_{(p)}] = |S| = p$.

Nun zeigen wir, dass $T := \{(s,0) \mid s \in S\}$ ein Repräsentantensystem von G/pG ist. Nach Definition von G ist dies eine Teilmenge von G. Wie in (c) berechnen wir sodann

$$pG \;=\; \bigl\{(a,b) \in \mathbb{Q}^{\oplus 2} \bigm| \exists\, n_0 \geqslant 0\ \forall\, n \geqslant n_0\colon\ a - b\cdot\omega_n \in p\mathbb{Z}_{(p)}\bigr\}$$

und stellen fest, dass ein Element der Form $(a,0)$ genau dann in pG liegt, wenn $a \in p\mathbb{Z}_{(p)}$ ist. Für zwei verschiedene $s, s' \in S$ folgt daraus $(s-s',0) \notin pG$ und somit $(s,0) + pG \neq (s',0) + pG$.

Jetzt betrachte ein beliebiges Element $(a,b) \in G$. Nach Definition von G existiert dann ein $n_0 \geqslant 0$, so dass für alle $n \geqslant n_0$ gilt $a - b\cdot\omega_n \in \mathbb{Z}_{(p)}$. Wir wählen ein solches n_0, für das zusätzlich $p^{n_0!}b \in \mathbb{Z}_{(p)}$ ist. Nach dem oben beschriebenen Repräsentantensystem für $\mathbb{Z}_{(p)}/p\mathbb{Z}_{(p)}$ existiert dann ein $s \in S$ mit $a - b\cdot\omega_{n_0} \in s + p\mathbb{Z}_{(p)}$. Für jedes $n \geqslant 0$ ist dann $\omega_n - \omega_{n_0}$ durch $p^{(n_0+1)!}$ teilbar ist und somit $b\cdot(\omega_n - \omega_{n_0}) \in p\mathbb{Z}_{(p)}$. Zusammen folgt daraus

$$(a-s) - b\cdot\omega_n \;=\; (a - b\cdot\omega_{n_0}) - s + b\cdot(\omega_n - \omega_{n_0}) \;\in\; p\mathbb{Z}_{(p)}.$$

Daher ist $(a-s,b) \in pG$ und somit $(a,b) \in (s,0) + pG$. Zusammen zeigt dies, dass T ein Repräsentantensystem von G/pG ist. Daher ist $[G : pG] = |T| = p$.

(e) Wegen $\mathbb{Z}^{\oplus 2} \subset G \subset \mathbb{Q}^{\oplus 2}$ und Aufgabe 6 (b) hat G den Rang 2. Somit kann G höchstens isomorph zu einer der Gruppen der Form $A \oplus B$ aus Aufgabe 7 (b) sein. Wegen Teil (c) und der Tabelle in Aufgabe 7 (a) gibt es dann nur die Möglichkeit $A = B = \mathbb{Z}_{(p)}$. Dann wäre also $G \cong \mathbb{Z}_{(p)}^{\oplus 2}$. Wegen (d) ist nun aber $[\mathbb{Z}_{(p)}^{\oplus 2} : p\mathbb{Z}_{(p)}^{\oplus 2}] = p^2 \neq p = [G : pG]$. Somit ist $G \ncong \mathbb{Z}_{(p)}^{\oplus 2}$.