Übung zu Algebraische und Geometrische Strukturen in der Mathematik, SoSe 2014

8. Übungsblatt – Lösungsskizze

Aufgabe P23

Man macht sich zunächst klar, dass $S_3 \times S_3$ als direktes Produkt zweier Gruppen wieder eine Gruppe ist. Sei $\bullet$ die komponentenweise definierte Multiplikation auf $S_3 \times S_3$. Für $(\pi, \pi'), (\chi, \chi') \in S_3 \times S_3$ mit $\pi = \chi' = \mathrm{id}$, $\pi' = (12)$ und $\chi = (123)$ rechnen wir einerseits

$$m((\pi, \pi')) \circ m((\chi, \chi')) = \pi \circ \pi' \circ \chi \circ \chi' = \pi' \circ \chi = (132)$$

und andererseits

$$m((\pi, \pi') \bullet (\chi, \chi')) = m((\pi \circ \chi, \pi' \circ \chi')) = \pi \circ \chi \circ \pi' \circ \chi' = \chi \circ \pi' = (23).$$

Es ist m also kein Homomorphismus.
Für eine allgemeine Gruppe $(G, \cdot)$ und das direkte Produkt $(G \times G, \bullet)$ mit $g, g', h, h' \in G$ beliebig rechnet man genauso nach, dass einerseits $m((g, g')) \cdot m((h, h')) = gg'hh'$ und andererseits $m((g, g') \bullet (h, h')) = m((gh, g'h')) = ghg'h'$ gilt. Es ist also m genau dann ein Homomorphismus, wenn G abelsch ist.

Aufgabe P24

1. $[\Rightarrow]$: Sei G_x normal. Dann wählen wir $h \in G$ und betrachten $y := h.x$. Wir müssen zeigen, dass $G_x = G_y$ gilt. Dafür zeigen wir zunächst, dass $G_x \subseteq G_y$ gilt. Sei $g \in G_x$, d.h. $g.x = x$. Wegen der Normalität von G_x gilt $(h \cdot g).x = (g \cdot h).x$ und somit können wir ausrechnen, dass

   $$y = h.x = h.(g.x) = (h \cdot g).x = (g \cdot h).x = g.(h.x) = g.y.$$

   Somit ist $g \in G_y$.

   Nun zeigen wir, dass $G_y \subseteq G_x$. Sei dafür $g \in G_y$, d.h. $g.y = y$. Dann gilt $g.(h.x) = y$ und somit $h^{-1}.(g.(h.x)) = h^{-1}.y = x$. Daraus folgt, dass $(h^{-1} \cdot g \cdot h).x = x$ und somit $(h^{-1} \cdot g \cdot h) \in G_x$. Erneut wegen der Normalität von G_x folgt hieraus, dass $g \in G_x$ gilt.

   $[\Leftarrow]$: Sei $G_x = G_y$ für alle $y \in G.x$. Wir zeigen, dass G_x normal ist, indem wir zeigen, dass für jedes $h \in G$ und jedes $g \in G_x$ gilt, dass $h \cdot g \cdot h^{-1} \in G_x$. Seien hierfür $h \in G$ und $g \in G_x$ beliebig und sei $y := h^{-1}.x$. Dann ist $y \in G.x$. Es gilt $(h \cdot g \cdot h^{-1}).x = x$ genau dann, wenn $(h \cdot g).y = x$ und dies wiederum genau dann, wenn $g.y = h^{-1}.x = y$, also wenn $g \in G_y$. Da aber $G_y = G_x$ gilt, folgt bereits, dass $g \in G_x$. Dies zeigt, dass G_x normal ist.

2. $[\Rightarrow]$: Angenommen $G \curvearrowright X$ ist derartig, dass $\bigcap_{x \in X} G_x \neq \{e\}$. Dann gibt es ein $g \in G$ mit $g \neq e$, sodass $g.x = x$ für alle $x \in X$ und somit $g.x = e.x$ für alle $x \in X$. Somit ist die Wirkung nicht treu.

   $[\Leftarrow]$: Angenommen $G \curvearrowright X$ sei nicht treu. Dann gibt es ein $g \neq e$, sodass $g.x = x$ für alle $x \in X$. Hieraus folgt, dass $g \in \bigcap_{x \in X} G_x$. Somit gilt $\bigcap_{x \in X} G_x \neq \{e\}$.

Aufgabe P26

1. Wir nehmen an, dass $A, B, A \cup B \leq G$ und dass $A \nsubseteq B$, d.h. es gibt ein $a \in A \setminus B$. Wir zeigen nun, dass dann $B \subseteq A$. Wir nehmen dazu $b \in B$. Da $A \cup B$ eine Gruppe ist, ist dann $a \cdot b \in A \cup B$, d.h. $a \cdot b \in A$ oder $a \cdot b \in B$. Angenommen $a \cdot b \in B$. Dann wäre auch $a \in B$, da $a = a \cdot b \cdot b^{-1}$, ein Widerspruch. Somit ist $a \cdot b \in A$. Da $b = a^{-1} \cdot a \cdot b$ folgt dann aber, dass $b \in A$. Dies zeigt, dass $B \subseteq A$ gilt.

2. Für $j \leq k$ schreiben wir $F_j := \bigcup_{i=0}^{j} H_i$. Wir zeigen durch Induktion über j, dass F_j für jedes $j \leq k$ eine Untergruppe von G ist und dass $[G : F_j] \leq \prod_{i=0}^{j} [G : H_i]$ gilt. Der Fall $j = k$ liefert dann die Behauptung. Als Induktionsanfang betrachten wir F_0. Dies ist nach Voraussetzung eine Untergruppe von G von endlichem Index, da $F_0 = H_0$ gilt. Nun nehmen wir an, die Behauptung sei für ein festes $j < k$ gezeigt und betrachten F_{j+1}. Zunächst sehen wir, dass $F_{j+1} \leq G$, da für $a, b \in F_{j+1}$ gilt, dass $a, b \in H_i$ für alle $i \leq j + 1$. Da die H_is Untergruppen von G sind, gilt dann, dass $a \cdot b^{-1} \in H_i$ für alle $i \leq j + 1$. Daraus folgt, dass $a \cdot b^{-1} \in F_{j+1}$. Somit ist F_{j+1} eine Untergruppe von G.

   Nun bemerken wir, dass $F_{j+1} = F_j \cap H_{j+1}$ gilt. Für jedes $g \in G$ gilt also

   $$gF_{j+1} = \{g \cdot h \mid h \in F_j \cap H_{j+1}\} = \{g \cdot h \mid h \in F_j\} \cap \{g \cdot h \mid h \in H_{j+1}\} = gF_j \cap gH_{j+1}.$$

   Somit sind die Linksnebenklassen von F_{j+1} Partitionen von Linksnebenklassen in F_j in jeweils maximal $[G : H_{j+1}]$ Teilklassen. Hieraus folgt, dass $[G : F_{j+1}] \leq [G : F_j] \cdot [G : H_{j+1}]$ gilt. Mit der Induktionsvoraussetzung erhalten wir schließlich

   $$[G : F_{j+1}] \leq \left(\prod_{i=0}^{j} [G : H_i] \right) \cdot [G : H_{j+1}] = \prod_{i=0}^{j+1} [G : H_i].$$

Aufgabe H20 (4P)

1. Da $\{x_i \mid i \in I\}$ ein Repräsentatensystem der Bahnen ist gilt

   $$X = \cup_{i \in I} G.x_i$$

   und da $G.x_i \cap G_{x_j} = \emptyset$ für $i \neq j$ gilt somit

   $$|X| = \sum_{i \in I} |G.x_i|.$$

   Nach der Bahnformel gilt $|G.x_i| = [G : G_{x_i}]$, also insbesondere $|G.x_i| = 1$ falls $x_i \in X^G$. Daraus folgt direkt

   $$|X| = \sum_{\in I} [G : G_{x_i}] = |X^G| + \sum_{i \in I, x_i \notin X^G} [G : G_{x_i}].$$

2. Es gilt wegen der Bahnformel, dass $19 = \sum_{i=1}^{n} |G_{x_i}|$, wobei $x_1, ..., x_n$ ein Repräsentantensystem der Bahnen ist. Da die Ordnung der Untergruppen G_{x_i} nach dem Satz von Lagrange entweder 7 oder 5 sein muss und sich 19 eindeutig als $2 \cdot 7 + 1 \cdot 5$ schreibt, muss es genau drei Bahnen geben.

3. Nein, da die Gruppe nur echte Untergruppen der Ordnung 5 haben kann und sich 19 nicht als eine Summe von 5 schreiben lässt.

Aufgabe H21 (4P)

1. Es ist $\pi = (m\ m')$ für $m, m' \in \{1, ..., p\}$. Wir setzen $m_1 := m$ und definieren induktiv $m_i := \pi(m_{i-1})$ für $1 < i \leq p$. Da σ ein Zyklus der Länge p ist gilt damit $\sigma = (m_1\ m_2\ ...\ m_p)$. Da $m_i \neq m_j$ für $i \neq j$ gilt muss dann auch schon $m' = m_i$ für ein $i \in \{1, ..., p\}$ sein.

2. Als Motivaion beobachten wir zunächst, dass die Anforderungen für den Zykel σ^{i-1} erfüllt sind, also dass also $\sigma^{i-1}(m_1) = m_i$ gilt. Es reicht also zu zeigen, dass $\langle \sigma, \pi \rangle = \langle \sigma^{i-1}, \pi \rangle$ gilt. Da $\sigma^{i-1}, \pi \in \langle \sigma, \pi \rangle$ gilt auch $\langle \sigma^{i-1}, \pi \rangle \subseteq \langle \sigma, \pi \rangle$. Weil $p = \text{ord}(\sigma)$ eine Primzahl ist, gilt $\text{ord}(\sigma^{i-1}) = p$ für jedes $2 \leq i < p$ (da nach dem Satz von Lagrange die Ordnung von σ^{i-1} ein Teiler der Ordnung von $\langle \sigma \rangle$ ist). Also gilt $|\langle \sigma^{i-1} \rangle| = p$ und es muss ein $k \in \mathbb{N}$ geben, so dass $(\sigma^{i-1})^k = \sigma$ gilt. Das impliziert $\langle \sigma \rangle \subseteq \langle \sigma^{i-1} \rangle$ und das wiederum $\langle \sigma, \pi \rangle \subseteq \langle \sigma^{i-1}, \pi \rangle$.

3. Nach Satz II.1.26 b) gilt

$$\begin{aligned}
(m_2\ m_3) &= (m_1\ m_2\ ...\ m_p)(m_1\ m_2)(m_1\ m_2\ ...\ m_p)^{-1} \\
(m_3\ m_4) &= (m_1\ m_2\ ...\ m_p)(m_2\ m_3)(m_1\ m_2\ ...\ m_p)^{-1} \\
&\vdots \\
(m_{p-1}\ m_p) &= (m_1\ m_2\ ...\ m_p)(m_{p-2}\ m_{p-1})(m_1\ m_2\ ...\ m_p)^{-1}.
\end{aligned}$$

   Dieses sind alles Elemente von H, da $(m_1\ m_2\ ...\ m_p)$ und $(m_1 m_2)$ Elemente von H sind. Damit sind auch

$$\begin{aligned}
(m_1\ m_3) &= (m_1\ m_2)(m_2\ m_3)(m_1\ m_2) \\
(m_1\ m_4) &= (m_1\ m_3)(m_3\ m_4)(m_1\ m_3) \\
&\vdots \\
(m_1\ m_p) &= (m_1\ m_{p-1})(m_{p-1}\ m_p)(m_1\ m_{p-1})
\end{aligned}$$

   Elemente von H, da sie sich wiederrum als Produkt von Permutationen schreiben lassen, die wir bereits als Elemente von H identifiziert haben. Somit gilt

$$(m_i\ m_j) = (m_1\ m_i)(m_1\ m_j)(m_1; m_i) \in H$$

   für $i < j$.

4. Nach dem letzten Teil enthält H alle Transpositionen und ist nach Satz II.26 c) gleich S_p.

Aufgabe H22 (4P)

1. Wir zeigen zunächst, dass $(\mathbb{S}^1, \cdot)$ eine Untergruppe der Gruppe $(\mathbb{C}, \cdot)$ ist. Dazu bemerken wir einerseits, dass für $z, w \in \mathbb{S}^1$ gilt, dass $zw\overline{zw} = z\overline{z} \cdot w\overline{w} = 1$ und somit $zw \in \mathbb{S}^1$. Andererseits gilt für $z \in \mathbb{S}^1$, dass $z^{-1}\overline{(z^{-1})} = (z\overline{z})^{-1} = 1$ und somit $z^{-1} \in \mathbb{S}^1$. Also ist $\mathbb{S}^1$ abgeschlossen unter Multiplikation und multiplikativ Inversen, somit eine Untergruppe von $\mathbb{C}$ und also eine Gruppe.

   Sei n irgendeine natürliche Zahl. Um zu sehen, dass E_n eine Untergruppe von $\mathbb{S}^1$ ist, zeigen wir zunächst, dass $E_n \subseteq \mathbb{S}^1$. Sei dazu $z \in E_n$ und somit $z^n = 1$. Dann ist auch $\overline{z^n} = 1$. Da $(z\overline{z})^n = z^n \cdot \overline{z^n}$ gilt[1], ist somit $(z\overline{z})^n = 1$. Da $z\overline{z}$ aber eine positive reelle Zahl ist, folgt hieraus bereits, dass $z\overline{z} = 1$, d.h., dass $z \in E_n$. Somit ist $E_n \subseteq \mathbb{S}^1$. Nun beobachten wir ferner, dass für $z, w \in E_n$ gilt, dass $(z^{-1})^n = z^{-n} = 1$ und $(zw)^n = z^n w^n = 1$. Also ist E_n abgeschlossen unter Multiplikation und Inversen und somit eine Untergruppe von $\mathbb{S}^1$.

2. Um zu sehen, dass $(\mathbb{R}_{>0}, \cdot)$ eine Gruppe ist, zeigen wir, dass $(\mathbb{R}_{>0}, \cdot)$ eine Untergruppe der Gruppe $(\mathbb{R}, \cdot)$ ist. Hierfür bemerken wir einfach, dass das Produkt zweier positiver reeller Zahlen immer positiv ist und auch das multiplikativ Inverse einer positiven reellen Zahl wieder positiv ist.

   Somit ist auch das direkte Produkt $\mathbb{R}_{>0} \times \mathbb{S}^1$ eine Gruppe. Um zu zeigen, dass $\mathbb{R}_{>0} \times \mathbb{S}^1 \cong \mathbb{C} \setminus \{0\}$, betrachten wir die Abbildung

   $$m : \mathbb{R}_{>0} \times \mathbb{S}^1 \to \mathbb{C} \setminus \{0\},\ (r, \zeta) \mapsto r \cdot \zeta.$$

   Diese Abbildung ist ein Homomorphismus, da für $r, r' \in \mathbb{R}_{>0}$ und $\zeta, \zeta' \in \mathbb{C} \setminus \{0\}$ gilt, dass

   $$m((r, \zeta) \bullet (r', \zeta')) = m(rr', \zeta\zeta') = rr'\zeta\zeta' = r\zeta \cdot r'\zeta' = m(r, \zeta) \cdot m(r', \zeta'),$$

   wobei wir benutzt haben, dass $(\mathbb{C} \setminus \{0\}, \cdot)$ eine abelsche Gruppe ist. Um zu sehen, dass m in der Tat ein Isomorphismus ist, geben wir ein beidseitiges Inverses an. Zunächst bemerken wir, dass sich jedes $z \in \mathbb{C} \setminus \{0\}$ eindeutig als $z = |z| \cdot n_z$ mit $n_z := \frac{z}{|z|}$ zerlegen lässt, wobei $|z| \in \mathbb{R}_{>0}$ und $n_z \in \mathbb{S}^1$, da $|n_z| = \left|\frac{z}{|z|}\right| = \frac{1}{|z|} \cdot |z| = 1$ gilt. Dann definieren wir

   $$m' : \mathbb{C} \setminus \{0\} \to \mathbb{R}_{>0} \times \mathbb{S}^1,\ |z| \cdot n_z \mapsto (|z|, n_z).$$

   Es lässt sich leicht nachrechnen, dass $m \circ m' = \mathrm{id}_{\mathbb{C} \setminus \{0\}}$ und $m' \circ m = \mathrm{id}_{\mathbb{R}_{>0} \times \mathbb{S}^1}$. Somit ist m ein Isomorphismus.

3. Aus der Analysis ist bekannt, dass die Abbildung $\varphi' : \mathbb{R} \to \mathbb{S}^1, x \mapsto e^{i2\pi x}$ surjektiv ist. Ferner haben wir für je zwei $x, y \in \mathbb{R}$ die Exponentialgleichung $e^{i2\pi x} \cdot e^{i2\pi y} = e^{i2\pi(x+y)}$. Somit ist φ' ein surjektiver Homomorphismus von $(\mathbb{R}, +)$ auf $(\mathbb{S}^1, \cdot)$. Es ist ferner $x \in \ker(\varphi')$ genau dann, wenn $e^{i2\pi x} = 1$. Dies ist genau der Fall für alle $x \in \mathbb{Z}$ und somit ist $\ker \varphi' = \mathbb{Z}$.

   Nun definieren wir $\varphi : \mathbb{R}/\mathbb{Z} \to \mathbb{S}^1$ indem wir $\varphi([x]) := \varphi'(x) = e^{i2\pi x}$ für $x \in \mathbb{R}$ setzen. Die Abbildung φ ist wohldefiniert und injektiv, da $\ker(\varphi') = \mathbb{Z}$ gilt. Sie ist ein surjektiver Homomorphismus, da φ' ein surjektiver Homomorphismus ist. Insgesamt ist φ also ein Isomorphismus.

[1] Dies zeigt man mittels Induktion.

4. Sei $x \in \mathbb{R}$. Dann ist $[x] \in \mathbb{R}/\mathbb{Z}$ genau dann von endlicher Ordnung, wenn es ein $n \in \mathbb{N} \setminus \{0\}$ gibt, sodass $n[x] = [0]$, also $n \cdot x \in \mathbb{Z}$. Dies ist offenbar der Fall genau dann, wenn es ein $n \in \mathbb{N} \setminus \{0\}$ und ein $k \in \mathbb{Z}$ gibt, sodass $x = \frac{k}{m}$. Dies wiederum ist genau dann der Fall, wenn $x \in \mathbb{Q}$. Somit ist $[x]$ genau dann von endlicher Ordnung, wenn $x \in \mathbb{Q}$ ist, d.h. die Menge der Elemente von endlicher Ordnung in $\mathbb{R}/\mathbb{Z}$ ist gerade $\mathbb{Q}/\mathbb{Z}$. Da $(\mathbb{Q}, +)$ eine abelsche Gruppe und $(\mathbb{Z}, +)$ eine Untergruppe von $(\mathbb{Q}, +)$ ist, ist $(\mathbb{Z}, +)$ eine normale Untergruppe von $(\mathbb{Q}, +)$ und somit ist $\mathbb{Q}/\mathbb{Z}$ wieder eine Gruppe.

   Da φ aus Aufgabenteil (3) ein Isomorphismus ist, ist $z \in \mathbb{S}^1$ von endlicher Ordnung genau dann, wenn es ein $[x] \in \mathbb{R}/\mathbb{Z}$ von endlicher Ordnung gibt, sodass $\varphi([x]) = z$. Dies folgt aus der Surjektivität von φ und der Tatsache dass $n \cdot [x] = \varphi([x])^n$ für alle $n \in \mathbb{N}$. Somit erhalten wir, dass die Menge der Elemente endlicher Ordnung in $\mathbb{S}^1$ gerade

$$E_{\mathbb{N}} := \{z \in \mathbb{S}^1 \mid \exists q \in \mathbb{Q} : e^{i2\pi q}\}$$

   ist. Dies ist eine Gruppe, da $\varphi|_{\mathbb{Q}/\mathbb{Z}} : \mathbb{Q}/\mathbb{Z} \to E_{\mathbb{N}}$ ein Gruppenisomorphismus ist.