Karlsruher Institut für Technologie
Institut für Algebra und Geometrie
PD Dr. Stefan Kühnlein Dipl.-Math. Jochen Schröder

Einführung in Algebra und Zahlentheorie – Übungsblatt 4 – Musterlösung

Aufgabe 1 (4 Punkte)
Seien G und H endliche Gruppen und $\varphi\colon G \to H$ ein Gruppenhomomorphismus. Zeige die folgenden Aussagen:

a) Für $g \in G$ ist die Ordnung $\mathrm{ord}(\varphi(g))$ ein Teiler der Ordnung $\mathrm{ord}(g)$.

b) Seien nun $n \in \mathbb{N}$, $G = S_n$ und H eine Gruppe ungerader Ordnung. Dann ist φ trivial.

Lösung:
Erinnerung: Die Ordnung eines Elements g in einer Gruppe G ist die kleinste natürliche Zahl n mit $g^n = e_G$.
Minimale Vorüberlegung: Ist G endlich, so besitzt jedes Element $g \in G$ endliche Ordnung, denn nach dem Schubfachprinzip finden wir in $g^0, g^1, g^2, \ldots$ zwei Elemente $g^i = g^j$ mit $i > j$. Dann ist $g^{i-j} = e_G$.
Weiterhin gilt für ein Element g mit Ordnung 2: $\{e_g, g\}$ ist eine Untergruppe von G nach dem Untergruppenkriterium. Der Satz von Lagrange besagt dann, dass es ein solches Element nicht geben kann, wenn $\#G$ ungerade ist.

Mehr nachgedacht finden wir, dass für ein Element g endlicher Ordnung n gilt, dass $\langle g\rangle \overset{(!)}{=} \{g^0, \ldots, g^{n-1}\}$, wobei die n Potenzen paarweise verschieden sind (wie oben!). Es gilt also – bei einer endlichen Gruppe G – $\mathrm{ord}(g)|\mathrm{ord}(G)$ für alle $g \in G$. Das ist eine schöne Übungsaufgabe zum Selbermachen.[1]

a) Sei $n := \mathrm{ord}(g) \in \mathbb{N}$. Dann gilt $\varphi(g)^n = \varphi(g^n) = \varphi(e_G) = e_H$, also ist $m := \mathrm{ord}(\varphi(g)) \leq n$.
Wir stellen n dar als $n = k \cdot m + r$ für ein $r \in \{0, \ldots, m-1\}$:
Dann ist $e_H = \varphi(g)^n = \varphi(g)^{km+r} = (\varphi(g)^m)^k \cdot \varphi(g)^r = \varphi(g)^r$ und wegen $r < \mathrm{ord}(\varphi(g))$ folgt $r = 0$, also $n = k \cdot m$, also $m|n$.

b) Für eine beliebige Transposition τ gilt: $\mathrm{ord}(\tau) = 2 \overset{a)}{\Rightarrow} \mathrm{ord}(\varphi(\tau))|2$. Da H ungerade Ordnung besitzt, gibt es nach Lagrange (siehe Vorüberlegung) kein Element der Ordnung 2: Also gilt $\mathrm{ord}(\varphi(\tau)) = 1 \Rightarrow \varphi(\tau) = e_H$.
Sei nun $\sigma \in S_n$ beliebig. σ lässt sich als Produkt von Transpositionen schreiben, also gilt $\sigma = \prod_{i=1}^{r} \tau_i$ mit einem $r \in \mathbb{N}_0$ und Transpositionen τ_i.
Wir berechnen $\varphi(\sigma) = \varphi(\prod_{i=1}^{r} \tau_i) = \prod_{i=1}^{r} \varphi(\tau_i) = \prod_{i=1}^{r} e_H = e_H$, was zu zeigen war.

Aufgabe 2 (4 Punkte)
Sei G eine Gruppe und $g \in G$. Die *Konjugation* mit g ist die Abbildung $k_g\colon G \to G$, gegeben durch $k_g(h) = ghg^{-1}$. Zeige die folgenden Aussagen:

a) Die Konjugation mit g ist ein Gruppenautomorphismus von G.

b) Die Zuordnung $g \mapsto k_g$ definiert einen Gruppenhomomorphismus $G \to \mathrm{Aut}(G)$.

c) $\mathrm{Aut}(S_3) \cong S_3$.
(*Hinweis:* Zeige, dass der Homomorphismus aus b) injektiv ist. Wieso ist er auch surjektiv? Hier könnte ein Mächtigkeitsargument helfen.)

Lösung:

a) Für $x, y \in G$ ist $k_g(xy) = gxyg^{-1} = gxg^{-1}gyg^{-1} = k_g(x)k_g(y)$, also ist k_g ein Homomorphismus.
k_g ist injektiv, denn $k_g(x) = k_g(y) \Rightarrow gxg^{-1} = gyg^{-1} \overset{\cdot g}{\Rightarrow} gx = gy \overset{g^{-1}\cdot}{\Rightarrow} x = y$.
k_g ist surjektiv, denn für $x \in G$ ist $x = g(g^{-1}xg)g^{-1} = k_g(g^{-1}xg)$.
Natürlich ist k_g eine Abbildung von G nach G, also ein Automorphismus.
(**Alternative für die Bijektivität:** $(k_g)^{-1} = k_{(g^{-1})}$ nachrechnen....)

[1] In der Übung kannten viele diesen Sachverhalt nicht mehr, der in der Vorlesung dran war. Hier finden wir noch einmal eine Methode, wie wir die Aussage begründen können. Merke dir diesen Sachverhalt in jedem Fall als direkte Folgerung des Satzes von Lagrange.

b) Nach a) ist die Abbildung wohldefiniert. Zu zeigen ist die Homomorphie, also $k_{gh} \overset{(!)}{=} k_g \circ k_h$ für alle $g, h \in G$. Für $x \in G$ beliebig ist $k_{gh}(x) = (gh)x(gh)^{-1} = ghxh^{-1}g^{-1} = gk_h(x)g^{-1} = k_g(k_h(x)) = (k_g \circ k_h)(x)$.

c) Da id die Identität aus S_n ist, schreiben wir $\mathbb{1}$ für die Identität aus $\mathrm{Aut}(S_n)$.

b) liefert einen Gruppenhomomorphismus von $k\colon S_3 \to \mathrm{Aut}(S_3), \sigma \mapsto k_\sigma$.

Was ist der Kern von k?
Fall 1: Sei σ ein Element der Ordnung 2. Ohne Einschränkung $\sigma = (1\ 2)$, die anderen beiden Fälle gehen analog:
Es ist $(1\ 2)^{-1} = (1\ 2)$, also $k_\sigma(1\ 3) = (1\ 2) \circ (1\ 3) \circ (1\ 2) = (2\ 3) \neq (1\ 3)$, also $k_\sigma \neq \mathbb{1}$, $\sigma \notin \mathrm{Kern}(k)$.
Fall 2: Sei σ ein Element der Ordnung 3. Ohne Einschränkung ist $\sigma = (1\ 2\ 3)$, der andere Fall geht analog.
Es ist $(1\ 2\ 3)^{-1} = (1\ 3\ 2)$, also $k_\sigma(1\ 2) = (1\ 2\ 3) \circ (1\ 2) \circ (1\ 3\ 2) = (2\ 3) \neq (1\ 2)$, also $k_\sigma \neq \mathbb{1}$, $\sigma \notin \mathrm{Kern}(k)$.
Da alle Elemente in S_3 Ordnung $1, 2$ oder 3 haben, folgt $\mathrm{Kern}(k) = \{\mathrm{id}\}$, k ist injektiv.

Wegen der Injektivität gilt $\#(\mathrm{Aut}(S_3)) \geq \#S_3 = 6$. Wir zeigen $\#(\mathrm{Aut}(S_3)) \overset{(!)}{\leq} 6$, dann folgt $\#(\mathrm{Aut}(S_3)) = 6$ und damit wegen $\#S_3 = \#(\mathrm{Aut}(S_3))$ aus der Injektivität die Surjektivität.

S_3 wird erzeugt von $T = \{(1\ 2), (1\ 3), (2\ 3)\}$. Jeder Automorphismus φ ist eindeutig gegeben durch die Bilder der Erzeuger, aber für alle $\tau \in T$ gilt:
$\varphi(\tau) \neq \mathrm{id}$, denn φ ist injektiv, und damit $\mathrm{ord}(\varphi(\tau)) = 2$ nach 1a), also $\varphi(\tau) \in T$.
Weiterhin werden verschiedene Transpositionen auf verschiedene Transpositionen abgebildet, denn φ ist injektiv.
φ ist also gegeben durch eine Permutation der Transpositionen ($\mathrm{Sym}(T)$) – und davon gibt es aber nur 6 Stück, was zu zeigen war.

Aufgabe 3 (4 Punkte + 1 Zusatzpunkt)
Die Menge $\mathrm{SL}_2(\mathbb{Z}) = \{A \in \mathbb{Z}^{2\times 2} : \det(A) = 1\}$ ist mit der Multiplikation von Matrizen eine Gruppe.[1]
In $\mathrm{SL}_2(\mathbb{Z})$ seien die Matrizen $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ und $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ gegeben.
Berechne für $k \in \mathbb{Z}$ die Potenzen S^k und T^k und gib die Ordnung von S und T an. Zeige anschließend, dass S und T die Gruppe $\mathrm{SL}_2(\mathbb{Z})$ erzeugen.

Einen Zusatzpunkt erhältst du, wenn du zwei Matrizen endlicher Ordnung findest, die $\mathrm{SL}_2(\mathbb{Z})$ erzeugen.

Lösung:
Es ist $S^2 = -I$, $S^3 = -S$, $S^4 = I$, also ist $\mathrm{ord}(S) = 4$ und $S^k = S^{4m+r} = S^r$ mit dem eindeutigen $r \in \{0, 1, 2, 3\}$ mit $k \equiv r\ (4)$.
Die Ordnung von T ist unendlich: Allgemein ist $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & y \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & x+y \\ 0 & 1 \end{pmatrix}$ und es folgt:
$T^k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$ für $k \in \mathbb{N}$ (induktiv), außerdem für $k = 0$.
Für $k \in \mathbb{Z}, k < 0$ gilt $T^k = (T^{-k})^{-1} = (\begin{pmatrix} 1 & -k \\ 0 & 1 \end{pmatrix})^{-1} = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$.
Also gilt $T^k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$ für alle $k \in \mathbb{Z}$.

$\det(S) = 1, \det(T) = 1$, also $S, T \in \mathrm{SL}_2(\mathbb{C})$. Es reicht zu zeigen, dass jedes $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{C})$ Produkt von S- und T-Potenzen ist. Das ist äquivalent dazu, dass A durch Multiplikation von links und rechts mit S- und T-Potenzen in die Einheitsmatrix (oder eine andere Matrix aus dem Erzeugnis von S und T) überführt werden kann.
Fall 1: $a \neq 0$. Wir zeigen die Behauptung per Induktion nach $|a| + |c|$:
Induktionsanfang $|a| + |c| = 1$, dann ist $|a| = 1$ und $c = 0$ und damit $A = \begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix}$ (**Fall 1.1**) oder $A = \begin{pmatrix} -1 & b \\ 0 & d \end{pmatrix}$ (**Fall 1.2**).

[1] Das muss nicht gezeigt werden, sondern ist eine schöne Aufgabe für das Tutorium.

Im Fall 1.1 ist $d = 1$ wegen $1 = \det(A) = ad$ und damit $A = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = T^b$.

Im Fall 1.2 ist $d = -1$ und $S^2A = -A = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = T^b$.
In beiden Fällen sind wir fertig.

Induktionsschritt: Sei $|a| + |c| > 1$ und die Aussage richtig für **alle** Matrizen $A' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in \mathrm{SL}_2(\mathbb{C})$, bei denen die Summe $|a'| + |c'| < |a| + |c|$ ist.
Wäre $c = 0$, so wäre a ein Teiler von $\det(A)$ und damit $a = \pm 1$, was ausgeschlossen war. Also ist $a \neq 0, c \neq 0$.
Fall 1.3: Sei $|a| \geq |c|$:
Für $a > 0, c > 0$ oder $a < 0, c < 0$ erfüllt $T^{-1}A = \begin{pmatrix} a - c & b - d \\ c & d \end{pmatrix}$ nach Induktionsvoraussetzung die Bedingung, also auch A.
Für $a < 0, c > 0$ oder $a > 0, c < 0$ betrachten wir analog $TA = \begin{pmatrix} a + c & b + d \\ c & d \end{pmatrix}$...
Fall 1.4: $|a| < |c|$. Dann ist SA eine Matrix aus dem Fall 1.3.

Fall 2 $a = 0$. Dann ist $c \neq 0$, sonst wäre $\det(A) = 0$. Dann aber ist TA eine Matrix aus dem Fall 1.

Zusatz: Offensichtlich gilt $\langle S, T \rangle = \langle S, ST \rangle$.
Es ist $ST = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$ und nachrechnen zeigt $(ST)^3 = -I$, also $(ST)^6 = I$ und somit hat auch ST endliche Ordnung.

Aufgabe 4 (4 Punkte)
In dieser Aufgabe wollen wir ein wenig Topologie betreiben. Sei $X \subseteq \mathbb{R}$ eine Teilmenge von $\mathbb{R}$.
X heißt *dicht* in $\mathbb{R}$, wenn für alle $x \in \mathbb{R}$ und alle $\varepsilon > 0$ ein $g \in G$ existiert mit $|x - g| < \varepsilon$.
X heißt *diskret* in $\mathbb{R}$, wenn für alle $x \in \mathbb{R}$ ein $t > 0$ existiert, so dass $\{g \in G : |g - x| < t\}$ endlich ist.
Aus der Analysis wissen wir zum Beispiel, dass $\mathbb{Q}$ dicht in $\mathbb{R}$ ist.

a) Zeige, dass für eine Untergruppe G von $(\mathbb{R}, +)$ die folgenden Eigenschaften äquivalent sind:
   (i) G ist zyklisch.
   (ii) Für alle $r > 0$ ist $G \cap [-r, r]$ endlich.
   (iii) Es gibt ein $r > 0$, so dass $G \cap [-r, r]$ endlich ist.
   (iv) G ist nicht dicht in $\mathbb{R}$.
   (v) G ist diskret in $\mathbb{R}$.

b) Zeige, dass die Menge $\{\pm 2^a 3^b : a, b \in \mathbb{Z}\}$ dicht in $\mathbb{R}$ liegt.
   (*Hinweis:* Der Logarithmus log ist ein stetiger Gruppenisomorphismus von $(\mathbb{R}_{>0}, \cdot)$ nach $(\mathbb{R}, +)$.)

Lösung:

a) Ist $G = \{0\}$ trivial, so sind alle Aussagen (i) bis (v) gleichzeitig erfüllt. Es reicht also zu zeigen, dass die Aussagen für $G \neq \{0\}$ äquivalent sind.
   Wir erfinden neu die Aussage (i'): G besitzt ein kleinstes positives Element m.
   Es gilt „$(i') \Rightarrow (i)$“, denn m ist ein Erzeuger. Wir können jedes $x \in \mathbb{R}$ darstellen als $kx + r$ mit $k \in \mathbb{Z}$ und einem Rest $r \in [0, m)$. Für jedes $y = km + r \in G$, ist $r = y - km \in G$, also $r = 0$ wegen der Minimalität von m. Also ist jedes $y \in G$ ein m-Vielfaches, also m ein Erzeuger.
   (**Bemerkung:** (i) und (i') sind äquivalent. Ist nämlich z ein Erzeuger von der zyklischen Untergruppe G, so ist auch $-z$ einer. Es ist $z > 0$ oder $-z > 0$ und das ist dann das gesuchte Minimum m.
   Das Ganze funktioniert genauso wie bei den nichttrivialen Untergruppen von $\mathbb{Z}$.)

   Gelte zunächst (i), dann ist $G = \langle z \rangle$ für ein $z \in \mathbb{R}$, $z > 0$:
   - Dann gilt (ii), denn für alle $R > 0$ ist $|mz| > R$ für hinreichend großes $|m|$ und damit gibt es nur endlich viele $m \in \mathbb{Z}$ mit $-R \leq mz \leq R$, also $G \cap [-R, R]$ endlich.
   - Außerdem gilt (v), denn für alle $x \in \mathbb{R}$ wählen wir $\varepsilon = \frac{z}{2}$. Dann ist $G \cap (x - \varepsilon, x + \varepsilon)$ endlich.

Offensichtlich gilt „$(ii) \Rightarrow (iii)$“.
Auch „$(v) \Rightarrow (iv)$“ sollte klar sein: Diskret und dicht schließen sich in $\mathbb{R}$ aus. Ausführlich liest sich das so: Ist G diskret, so wählen wir zu $x = 0$ ein $t > 0$, so dass $\{g \in G : |g| < t\}$ endlich ist – dann gibt aber insbesondere ein Element g_0 kleinsten Betrages. Zu $\varepsilon = \frac{|g_0|}{3}$ und $y = \frac{|g_0|}{3}$ gibt es kein $g \in G$ mit $|y - g| < \varepsilon$.

Es verbleibt zu zeigen, dass $(iv) \overset{(!)}{\Rightarrow} (iii)$ und dass $(iii) \overset{(!)}{\Rightarrow} (i')$, dann sind wir fertig.

„$(iii) \Rightarrow (i')$“ sehen wir wie folgt ein: Wir finden ein $R > 0$, so dass $[0, R] \cap G$ endlich ist. Enthält der Schnitt neben 0 mindestens ein weiteres Element, so enthält er auch ein minimales solches wie in (i') gefordert.
Ist nun $G \cap [0, R] = \{0\}$, so betrachten wir die Intervalle $I_1 = [R, 2R], I_2 = [2R, 3R]$, ... und sicher gibt es ein minimales $j \in \mathbb{N}$, so dass $I_j \cap G \neq \emptyset$. Dieser Schnitt enthält keine zwei Elemente, sonst gäbe es $g_1, g_2 \in G$ mit $jR \leq g_1 < g_2 \leq (j + 1)R$ und es wäre $g_2 - g_1 \in G$, $g_1 - g_1 \in (0, R]$. WIDERSPRUCH
Also ist $I_j \cap G$ einelementig und dieses Element ist ein minimales positives Element wie gefordert.

„$(iv) \Rightarrow (iii)$“: Da G nicht dicht in $\mathbb{R}$ liegt finden wir $x \in \mathbb{R}$, $t > 0$, so dass $(x - t, x + t) \cap G = \emptyset$. Wäre nun $G \cap [-t, t] \neq \{0\}$, so gäbe es ein $g \in G, 0 < g \leq t$ und damit liegen alle g-Vielfachen in G, also insbesondere ein Element aus $(x - t, x + t)$. WIDERSPRUCH.
Also ist $R = t$ geeignet.

b) Sei $H := \{2^a 3^b : a, b \in \mathbb{Z}\}$. Wir zeigen, dass H dicht in $\mathbb{R}_{>0}$ liegt (**Behauptung**).
Dann liegt $\{\pm 2^a 3^b : a, b \in \mathbb{Z}\}$ dicht in $\mathbb{R} \setminus \{0\}$, aber da wir mit $\frac{1}{2^n}$, $n \to \infty$ beliebig nahe an 0 herankommen, liegt es sogar dicht in $\mathbb{R}$.
Beweis der Behauptung: Es ist $H = \langle 2, 3 \rangle$ als Untergruppe von $(\mathbb{R}_{>0}, \cdot)$.

Schritt 1: H ist nicht zyklisch, sonst wäre $H = \langle \frac{z}{n} \rangle = \{\frac{z^r}{n^r}, r \in \mathbb{Z}\}$ mit teilerfremden ganzen Zahlen z, n. Es ist $2 \in H$, also $2 = \frac{z^r}{n^r}$ für ein $r \in \mathbb{Z}$:
Fall 1: Ist $r \geq 0$, dann gilt $2n^r = z^r$, also $2|z$, also $2 \nmid n$. Die Anzahl von 2 in der Primfaktorzerlegung impliziert $r = 1$ und dann folgt $n = 1$, $z = 2$.
Fall 2: Ist $r < 0$, dann gilt $2z^{-r} = n^{-r}$ und analog $z = 1$, $n = 2$.
In beiden Fällen ist $\{z, n\} = \{1, 2\}$.
Analog ist aber auch $3 \in H$ und wir sehen $\{z, n\} = \{1, 3\}$. Das geht nicht!

Schritt 2: log: $\mathbb{R}_{>0} \to \mathbb{R}$ und exp: $\mathbb{R} \to \mathbb{R}_{>0}$ sind zueinander inverse Homomorphismen, also Isomorphismen. Beide Abbildungen sind stetig (also *Homöomorphismen*). Damit gilt:

$$H \leq (\mathbb{R}_{>0}, \cdot) \text{ nicht zyklisch} \overset{\log \text{Iso}}{\Rightarrow} \log(H) \leq (\mathbb{R}, +) \text{ nicht zyklisch} \overset{a)}{\Rightarrow} \log(H) \text{ dicht in } \mathbb{R} \overset{(!)}{\Rightarrow} H \text{ dicht in } \mathbb{R}_{>0}.$$

Topologen kennen die letzte Implikation, das folgt wegen der *Homöomorphie*. Nicht-Topologen greifen auf die Grunddefinition der Dichtheit und die Epsilon-Delta-Definition der Stetigkeit von exp[1] zurück:
Sei $x \in \mathbb{R}_{>0}, \varepsilon > 0$ gegeben. Wir müssen ein $h \in H$ finden mit $|x - h| \overset{(!)}{<} \varepsilon$.
Da exp stetig ist, existiert ein $\delta > 0$, so dass für $|\log(x) - z| < \delta \Rightarrow |x - e^z| < \varepsilon$ ist. Ein solches z existiert in $\log(H)$, also ist $h = e^z$ eine gute Wahl.

[1] Auf dem Übungsblatt wurde ungeschickterweise die Stetigkeit von log als Tipp vorgegeben... Wir brauchen die Stetigkeit der Exponentialfunktion, aber die ist aus der Analysis bekannt.