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

Einführung in Algebra und Zahlentheorie – Übungsblatt 6 – Musterlösung

Aufgabe 1 (4 Punkte + 2 Sonderpunkte für b))
In dieser Aufgabe lernen wir eine Methode kennen, die Freiheit einer Gruppe zu zeigen.

a) Seien G eine Gruppe und $a, b \in G$ Elemente unendlicher Ordnung, die G erzeugen. Weiterhin sei $\bullet$ eine Gruppenoperation von G auf einer Menge M, so dass es nichtleere disjunkte Teilmengen $A, B \subset M$ gibt mit $a^z \bullet A \subseteq B$ und $b^z \bullet B \subseteq A$ für alle $z \in \mathbb{Z} \setminus \{0\}$.
Zeige, dass G frei in den Erzeugern a, b ist.

b) Sei nun $G = \langle \{ \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \} \rangle$ eine Untergruppe von $\mathrm{SL}_2(\mathbb{Z})$.
Zeige, dass G frei in zwei Erzeugern ist.
(*Hinweis:* G operiert auf $\mathbb{R}^2$ durch Matrizenmultiplikation. Finde $A, B \subset \mathbb{R}^2$, so dass die Bedingung aus a) erfüllt ist.)

Lösung: Das ist das *Ping-Pong-Lemma* oder *Tischtennis-Lemma*: A und B kann man sich als Seiten einer Tischtennisplatte vorstellen, der Ball – ein geeignet zu wählendes Element – wird durch a- und b-Potenzen hin- und hergespielt.

a) Zunächst sei nur $G = \langle a, b \rangle$ gegeben. Dann kann jedes Element aus G als Produkt von a- und b-Potenzen geschrieben werden. Insbesondere können wir nebeneinanderstehende Faktoren aa^{-1} (usf.) kürzen und erhalten eine Darstellung wie folgt:
Jedes Element $w \in G$ ist von der Form $a^{z_1} b^{z_2} \cdots a^{z_k}$ (**Fall 1**) oder $a^{z_1} b^{z_2} \cdots b^{z_k}$ (**Fall 2**) oder $b^{z_1} a^{z_2} \cdots a^{z_k}$ (**Fall 3**) oder $b^{z_1} a^{z_2} \cdots b^{z_k}$ (**Fall 4**) mit $k \in \mathbb{N}_0$ und Koeffizienten $z_1, ..., z - k \in \mathbb{Z} \setminus \{0\}$. Das leere Wort (für $k = 0$) ist das Neutralelement der Gruppe. Die Darstellung ist im Allgemeinen nicht eindeutig.[1]
G ist frei in a und b, wenn es keine Relationen zwischen a, b gibt (außer den trivialen $aa^{-1} = e$ usf.). Das ist äquivalent dazu, dass das leere Wort e nur als leeres Produkt geschrieben werden kann.

(**Bemerkung:** Das geht ganz ähnlich wie in der linearen Algebra und der linearen Unabhängigkeit. Kann e auf eine weitere Art geschrieben werden, so gibt dies eine Relation in a und b, andersherum kann aber jede Relation zwischen a und b umgeformt werden und es bleibt $e = ...$ als nichttriviale Kombination über.
Insbesondere kann man auch – wie in der LA – zeigen, dass die Freiheit bedeutet, dass jedes Element eindeutig als Produkt über a- und b-Potenzen geschrieben werden kann.
Der geneigte Student wird Unterschiede zur Linearen Algebra und der Vektorraumtheorie feststellen, aber die Beweise sind eigentlich sehr gut vergleichbar.)

Sei nun also w ein nichtleeres Produkt von a- und b-Potenzen. Wir sind fertig, wenn wir $w \overset{(!)}{\neq} e$ zeigen können. Dazu betrachten wir die vier Fälle von oben.
Im **Fall 1** wählen wir $x \in A$ beliebig. Was ist $w \bullet x$?
Es ist $a^{z_k} \bullet x \in B$ (Ping!) und dann $b^{z_{k-1}} \bullet (a^{z_k} \bullet x) \in A$ (Pong!) und damit ... Schlussendlich sehen wir $w \bullet x \in B$, also insbesondere $B \ni w \bullet x \neq x \in A$, denn A, B waren disjunkt.
Wegen $ex = x$ folgt $w \neq e$.
Im **Fall 2** konjugieren wir w mit a^s für ein $s \in \mathbb{Z}$ mit $s \notin \{0, -z_1\}$. Dann ist $a^s w a^{-s} \neq e$, denn wir sind im Fall 1. Wäre $w = e$, dann gilt $a^s w a^{-s} = a^s e a^{-s} = e$, was wir eben ausgeschlossen haben. Also gilt $w \neq e$.
Die **Fälle 3 und 4** verlaufen analog zu den ersten beiden Fällen.

b) Die Potenzen der Matrizen $a := \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$, $b := \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$ sehen wie folgt aus:
$\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}^z = \begin{pmatrix} 1 & 2z \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}^z = \begin{pmatrix} 1 & 0 \\ 2z & 1 \end{pmatrix}$ für alle $z \in \mathbb{Z}$ – dies ist eine leichte Induktionsaufgabe für positive z und einfache Matrizeninversion für negative z. Wir haben das ganz ähnlich in Aufgabe 4 vom dritten Übungsblatt gesehen.

Sei nun $A = \{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{R}^2 : |x| < |y| \}$ und $B = \{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{R}^2 : |x| > |y| \}$.
Achtung, ab hier war ein Fehler in der Musterlösung! Das habe ich am 28.08.2013 verbessert. Danke für die Rückmeldung!

Seien nun $\begin{pmatrix} x \\ y \end{pmatrix} \in A$ (das heißt $|x| < |y|$) und $a^z = \begin{pmatrix} 1 & 2z \\ 0 & 1 \end{pmatrix}, z \neq 0$.

[1] Man denke z.B. an $G = \mathbb{Z}/2\mathbb{Z}$, $\overline{1}^2 = \overline{1} + \overline{1} = \overline{0}$.

Zu zeigen ist, dass $a^z \bullet \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x + 2zy \\ y \end{pmatrix} \overset{(!)}{\in} B$ ist.

Es ist $|x + 2zy| \geq |2zy| - |x| = 2|z||y| - |x| \overset{z \in \mathbb{Z} - \{0\}}{\geq} 2|y| - |x| \overset{|x|<|y|}{>} |y|$, was die Behauptung zeigt.

Analog rechnet man nach, dass $b^z \bullet \begin{pmatrix} x \\ y \end{pmatrix} \in A$ für ein $\begin{pmatrix} x \\ y \end{pmatrix} \in B$, $z \neq 0$.

Mehr war nicht zu tun, die Erzeuger a, b sind nach a) relationenfrei.

Aufgabe 2 (4 Punkte)
Sei $\mathbb{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$ und $\mathrm{SL}_2(\mathbb{R}) = \{A \in \mathbb{R}^{2\times 2} : \det(A) = 1\}$.
Im Tutorium haben wir gesehen, dass durch

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \bullet z = \frac{az + b}{cz + d}$$

eine Gruppenoperation von $\mathrm{SL}_2(\mathbb{R})$ auf $\mathbb{H}$ gegeben ist.

a) Zeige, dass die Operation transitiv ist.

b) Berechne den Stabilisator $\mathrm{Stab}_{\mathrm{SL}_2(\mathbb{R})}(\mathrm{i})$.

c) Berechne $\{A \in \mathrm{SL}_2(\mathbb{R}) : A \bullet z = z \text{ für alle } z \in \mathbb{H}\}$.

d) Finde eine Gruppe, die transitiv und treu[1] auf $\mathbb{H}$ operiert.

Lösung: Sei stets $z = x + iy$ mit $x, y \in \mathbb{R}, y > 0$ ($y > 0 \Leftrightarrow z \in \mathbb{H}$).

Da ich die Rechnung eh noch getext rumliegen habe, hänge ich die Rechnung, dass eine Gruppenoperation vorliegt, an die Musterlösung an. So ähnlich habt ihr das im Tutorium gesehen.
Seien $z \in H$, $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R})$ und $B = \begin{pmatrix} e & f \\ g & h \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R})$ beliebig.
Wäre $cz + d = 0$ für ein $z \in \mathbb{H}$, so wäre wegen des Imaginärteils zunächst $c = 0$ und dann $d = 0$, was wegen $\det(A) = 1$ nicht sein kann – also ist $A \bullet z$ ein wohldefinierter Ausdruck in $\mathbb{C}$.
Es ist $A \bullet z = \frac{az+b}{cz+d} = \frac{ax+b+iay}{cx+d+icy} = \frac{(ax+b+iay)(cx+d-icy)}{(cx+d)^2+(cy)^2}$. Wegen $(cx + d)^2 + (cy)^2 \in \mathbb{R}_{>0}$ gilt
$\mathrm{Im}(\frac{(ax+b+iay)(cx+d-icy)}{(cx+d)^2+(cy)^2}) > 0 \Leftrightarrow \mathrm{Im}((ax + b + iay)(cx + d - icy)) > 0$.
Es ist $\mathrm{Im}((ax + b + iay)(cx + d - icy)) = -axcy - bcy + aycx + ayd = y(ad - bc) = y \cdot \det(A) = y > 0$. Also ist $A \bullet z \in \mathbb{H}$.

Desweiteren gilt $I_2 \bullet z = \frac{z}{1} = z$ und
$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \bullet (\begin{pmatrix} e & f \\ g & h \end{pmatrix} \bullet z) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \bullet \frac{ez+f}{gz+h} = \frac{a\frac{ez+f}{gz+h}+b}{c\frac{ez+f}{gz+h}+d} = \frac{aez+af+bgz+bh}{cez+cf+dgz+dh} = \begin{pmatrix} ae + bg & af + bh \\ ce + dg & cf + dh \end{pmatrix} \bullet z = (\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} e & f \\ g & h \end{pmatrix}) \bullet z$.

a) Wir zeigen, dass wir jedes $z \in \mathbb{H}$ auf i abbilden können.
Es ist $\begin{pmatrix} 1 & -x \\ 0 & 1 \end{pmatrix} \bullet (x + iy) = iy$. Weiterhin ist $\begin{pmatrix} \frac{1}{\sqrt{y}} & 0 \\ 0 & \sqrt{y} \end{pmatrix} iy = i$.
Hintereinanderausführung zeigt, dass i in der Bahn $\mathrm{SL}_2(\mathbb{R}) \bullet z$ für beliebiges $z \in \mathbb{H}$ liegt, also gibt es genau eine Bahn.

b) Wir suchen alle $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R})$, $i \overset{!}{=} A \bullet i = \frac{ai+b}{ci+d}$. Umstellen ergibt die Bedingung $ai + b = -c + di$, Koeffizientenvergleich: $a = d, b = -c$.
Wegen $\det(A) \overset{!}{=} 1$ erhalten wir $\mathrm{Stab}_{\mathrm{SL}_2(\mathbb{R})}(i) = \{\begin{pmatrix} a & b \\ -b & a \end{pmatrix} : a, b \in \mathbb{R}, a^2 + b^2 = 1\}$.

c) Analog zu b) berechnen wir $\mathrm{Stab}_{\mathrm{SL}_2(\mathbb{R})}(2i) = \{\begin{pmatrix} a & b \\ -\frac{b}{2} & a \end{pmatrix} : a, b \in \mathbb{R}, a^2 + \frac{b^2}{2} = 1\}$.
Es gilt $\{A \in \mathrm{SL}_2(\mathbb{R}) : A \bullet z = z \text{ für alle } z \in \mathbb{H}\} \subseteq \mathrm{Stab}_{\mathrm{SL}_2(\mathbb{R})}(i) \cap \mathrm{Stab}_{\mathrm{SL}_2(\mathbb{R})}(2i) = \{\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} : a \in \mathbb{R}, a^2 = 1\} = \{\pm I_2\}$.
Wegen $I_2 \bullet z = -I_2 \bullet z = z$ für alle $z \in \mathbb{H}$ gilt Gleichheit der Mengen. $I_2, -I_2$ sind die *Nichtsnutze* der Operation.

d) Als Kern eines Gruppenhomomorphismus ($\mathrm{SL}_2(\mathbb{R}) \to \mathrm{Sym}(\mathbb{H})$) ist $\{\pm I_2\}$ ein Normalteiler in $\mathrm{SL}_2(\mathbb{R})$. Wir definieren $\mathrm{PSL}_2(\mathbb{R}) := \mathrm{SL}_2(\mathbb{R})/\{\pm I_2\}$.
Die Operation von $\mathrm{PSL}_2(\mathbb{R})$ auf $\mathbb{H}$ gegeben durch $\overline{A} \bullet z = A \bullet z$ ist nach Konstruktion wohldefiniert, transitiv und treu.

(Diese Konstruktion funktioniert stets, um eine treue Operation zu erhalten. Das ist ganz direkt einzusehen, wenn wir die äquivalente „andere Welt" der Gruppenoperation als Gruppenhomomorphismus einer Gruppe in die Symmetriegruppe einer Menge betrachten. In dieser Anschauung ist eine Operation treu, wenn der Kern des zugehörigen Gruppenhomomorphismus trivial ist. Das schaffen wir doch mit Hilfe des Homomorphiesatzes immer, indem wir den Kern rausfaktorisieren und den induzierten Homomorphismus betrachten.)

[1] Eine Operation einer Gruppe G auf einer Menge M heißt *treu*, wenn kein Element außer e_G trivial operiert, das heißt, gilt $gm = m$ für alle m, so ist $g = e_G$.

Aufgabe 3 (4 Punkte)
Seien p eine Primzahl, $r \in \mathbb{N}$ und G eine Gruppe mit p^r Elementen. Zeige:

a) Das Zentrum $Z(G)$ besteht nicht nur aus dem neutralen Element.

b) Ist $r = 2$, so ist G abelsch.

Lösung:

a) G operiert auf sich selbst durch Konjugation: $g \bullet h = ghg^{-1}$.
Die endliche Menge G zerfällt in disjunkte Bahnen, wegen $\#Gh = [G : \mathrm{Stab}_G(h)]$ ist dabei nach Satz von Lagrange jede Bahnenlänge einer Bahn Gh ein Teiler von p^r, also insbesondere auch eine p-Potenz.
Die Fixpunkte der Operation sind gerade die Elemente aus dem Zentrum. Also gilt $\#Gh = 1$ für alle $h \in Z(G)$ (und jedes Element vertritt seine eigene Klasse) und $p|\#Gh$ für jedes $h \notin Z(G)$. $(*)$
Sei R ein Vertretersystem der Bahnen, dann ist insbesondere $Z(G) \subseteq R$. Sei $R' := R \setminus Z(G)$. Es gilt
$p^r = \#G = \sum\limits_{r \in R} \#Gr = \sum\limits_{r \in Z(G)} 1 + \sum\limits_{r \in R'} \#Gr = \#Z(G) + p \cdot c$ für eine Konstante c, die wegen $(*)$ existiert.
Umstellen zeigt $p|\#Z(G)$, was zu zeigen war.

b) Nach dem Satz von Lagrange ist $\#Z(G) \in \{1, p, p^2\}$, aber nach a) nicht 1. Ist $\#Z(G) = p^2$, so ist $G = Z(G)$ und damit G abelsch. Es reicht also zu zeigen, dass $\#Z(G) \overset{(!)}{\neq} p$ gilt. **Nehmen wir an**, das wäre der Fall:
Dann ist $Z(G)$ zyklisch, etwa $Z(G) = \langle a \rangle$. Weiterhin ist auch die Faktorgruppe $G/Z(G)$ zyklisch (denn es ist $\#Z(G)/G = \frac{\#G}{\#Z(G)} = p$), etwa $Z(G) = \langle bZ(G) \rangle$.
Für jedes $g \in G$ gilt dann $gZ(G) = b^m Z(G)$ für ein $m \in \mathbb{N}$ (sogar $m \in \{0, ..., p-1\}$), also $g \cdot b^{-m} \in Z(G)$, also $g \cdot b^{-m} = a^n$ für ein $n \in \mathbb{N}$ (sogar $n \in \{0, ..., p-1\}$), also $g = a^n b^m$ für passende m, n.
Wegen $a \in Z(G)$ können wir die a-Faktoren beliebig sortieren und somit gilt für beliebige $g = a^n b^m, g' = a^{n'} b^{m'}$, dass $gg' = a^n b^m a^{n'} b^{m'} = a^{n+n'} b^{m+m'} = a^{n'} b^{m'} a^n b^m = g'g$ ist und G ist doch abelsch. WIDERSPRUCH

Aufgabe 4 (4 Punkte) – eine alte Klausuraufgabe
Es seien G eine endliche Gruppe, n eine natürliche Zahl und $M := \mathrm{Abb}(G, \{1, \ldots, n\})$. Auf M haben wir die Gruppenoperation $\bullet\colon G \times M \to M$, gegeben durch

$$(g \bullet f)(x) := f(xg) \text{ für alle } g, x \in G, f \in M.$$

a) Was sind die Fixpunkte dieser Operation? Wie viele davon gibt es?

b) Es seien $H \leq G$ eine Untergruppe und $n > 1$. Gib eine Abbildung $f \in M$ an, die H als Stabilisator hat.

c) Nun sei G zyklisch von Ordnung p, wobei p eine Primzahl ist.
Benutze die Bahnbilanzformel und a), um zu zeigen, dass $c^p - c$ für alle $c \in \mathbb{N}$ ein Vielfaches von p ist.
(Dies ist ein Beweis des kleinen Satzes von Fermat.)

Lösung:

a) Die Fixpunkte sind die konstanten Funktionen, denn:
Sei f konstant, etwa $f(x) = m_0$ für ein $m_0 \in \{1, ..., n\}$ und für alle $x \in G$.
Für alle $g \in G$ berechnen wir $(g \bullet f)(x) = f(xg) = m_0 = f(x)$, also $g \bullet f = f$, f ist ein Fixpunkt.
Sei f nicht konstant, so finden wir $x_1 \neq x_2$ mit $f(x_1) \neq f(x_2)$. Dann ist
$((x_1^{-1} \cdot x_2) \bullet f)(x_1) = f(x_1 \cdot x_1^{-1} \cdot x_2) = f(x_2) \neq f(x_1)$, also $(x_1^{-1} \cdot x_2) \bullet f \neq f$, f ist kein Fixpunkt.

Es gibt also n Fixpunkte.

b) Wegen $n \geq 2$ können wir f wie folgt definieren: $f(x) = 1$, falls $x \in H$, $f(x) = 2$, falls $x \notin H$.
Für dieses f ist $\mathrm{Stab}_G(f) \overset{(!)}{=} H$, wie wir wie folgt einsehen:
Ist $x \notin H$, so ist $(x \bullet f)(e_G) = f(x) = 2 \neq 1 = f(e_G)$, also $x \notin \mathrm{Stab}_G(f)$.
Ist $x \in H$, so gilt $gx \in H \Leftrightarrow g \in H$ für alle $g \in G$ $((*))$, also $(x \bullet f)(g) = f(gx) \overset{(*)}{=} f(g)$ für alle $g \in G$, also $x \in \mathrm{Stab}_G(f)$.

c) Dies ist ein Spezialfall für $n = c$. G operiert auf $M = \mathrm{Abb}(G, \{1, ..., c\})$ mit $\#M = c^p$. Sei F die Menge der Fixpunkte, nach a) gilt $\#F = c$.
Für $f \in F$ gilt $\#Gf = 1$, für $r \in G \setminus F$ gilt $\#Gr | \#G, \#Gr \neq 1$, also $\#Gr = p$.
Sei R ein Vertretersystem der Bahnen, dann ist $R = F \cup R'$, wobei R' ein Vertretersystem der Bahnen der Länge > 1 darstellt. Dann gilt:
$\#M = c^p = \sum\limits_{r \in F} 1 + \sum\limits_{r \in R'} p = c + p \cdot \#R'$ und Umstellen zeigt die Behauptung.