Übung zur Vorlesung Einführung in die Algebra

Prof. Dr. J. H. Bruinier
Stephan Ehlen

Sommersemester 2009
Lösungshinweise zu Übungsblatt 5

Aufgabe G5.1 Ordnungen berechnen

(a) (a) Gegeben $k \in \mathbb{N}$ gilt $k\overline{m} = \overline{km} = \overline{0}$ in $\mathbb{Z}/n\mathbb{Z}$ genau dann, wenn $km \in n\mathbb{Z}$. In diesem Falle ist $\ell := km \in m\mathbb{Z} \cap n\mathbb{Z}$ und $k = \frac{1}{m}\ell$. Ist umgekehrt $\ell \in m\mathbb{Z} \cap n\mathbb{Z}$, so erfüllt $k := \ell/m \in \mathbb{Z}$ die Bedingung $km = \ell \in n\mathbb{Z}$, es ist also $k\overline{m} = \overline{0}$. Somit

$$\{k \in \mathbb{Z} \colon k\overline{m} = \overline{0}\} = \{\ell/m \colon \ell \in m\mathbb{Z} \cap n\mathbb{Z}\} = \{\ell/m \colon \ell \in \mathrm{kgV}(m,n)\mathbb{Z}\} = \frac{\mathrm{kgV}(m,n)}{m}\mathbb{Z},$$

da $m\mathbb{Z} \cap n\mathbb{Z} = \mathrm{kgV}(m,n)\mathbb{Z}$ nach Vorlesung, §1. Der Homomorphismus

$$\phi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \quad k \mapsto k\overline{m}$$

hat also den Kern $N\mathbb{Z}$ mit $N := \frac{\mathrm{kgV}(m,n)}{m}$. Der Homomorphiesatz liefert nun $\langle \overline{m} \rangle = \mathrm{im}\,\phi \cong \mathbb{Z}/\ker\phi = \mathbb{Z}/N\mathbb{Z}$, es ist also $\langle \overline{m} \rangle$ eine N-elementige Gruppe, somit $\mathrm{ord}(\overline{m}) = N = \frac{\mathrm{kgV}(m,n)}{m}$.

(b) Gegeben $x \in H$, $y \in G$ betrachten wir die Potenzabbildung

$$\phi : \mathbb{Z} \to G \times H, \quad \phi(n) := (x,y)^n,$$

die ein Homomorphismus ist (alte Aufgabe finden, oder Nachrechnen!). Hierbei ist $(x,y)^n = (x^n, y^n)$ und somit $\phi(n) = (1,1)$ genau dann, wenn $x^n = 1$ und $y^n = 1$, wenn also $n \in \mathrm{ord}(x)\mathbb{Z} \cap \mathrm{ord}(y)\mathbb{Z} = \mathrm{kgV}(\mathrm{ord}(x), \mathrm{ord}(y))\mathbb{Z}$. Nach dem Homomorphiesatz folgt $\langle (x,y) \rangle = \mathrm{im}\,\phi \cong \mathbb{Z}/\mathrm{kgV}(\mathrm{ord}(x), \mathrm{ord}(y))\mathbb{Z}$. Diese Gruppe hat $\mathrm{kgV}(\mathrm{ord}(x), \mathrm{ord}(y))$ Elemente; die Ordnung von (x,y) ist somit $\mathrm{kgV}(\mathrm{ord}(x), \mathrm{ord}(y))$.

(c) Es ist $\overline{2} \neq \overline{0}$ in $\mathbb{Z}/4\mathbb{Z}$, jedoch $2\,\overline{2} = \overline{4} = \overline{0}$; somit $\mathrm{ord}(\overline{2}) = 2$. Da 3 und 7 teilerfremd sind, ist $\mathrm{kgV}(3,7) = 21$, nach Teil (a) somit $\mathrm{ord}(\overline{3}) = 21/3 = 7$ (alternatives Argument: Da $\mathbb{Z}/7\mathbb{Z}$ Primzahlordnung 7 hat, ist jedes von $\overline{0}$ verschiedene Element ein Erzeuger dieser Gruppe, also auch $\overline{3}$; somit $\langle \overline{3} \rangle = \mathbb{Z}/7\mathbb{Z}$ und somit $\mathrm{ord}(\overline{3}) = 7$ in $\mathbb{Z}/7\mathbb{Z}$). Nach Teil (b) ist die Ordnung von $(\overline{2}, \overline{3})$ das kleinste gemeinsame Vielfache der Ordnungen 2 und 7 der beteiligten Elemente, also 14.

Aufgabe G5.2 Exakte Sequenzen

(a) Diese Abbildungen sind eindeutig bestimmt: Inklusion und die triviale Abbildung, die alle Elemente aus H auf die 1 abbildet.

(b) Es ist $\mathrm{im}\,\iota = N = \ker\pi$ sowie $\pi(G) = G/N$ und natürlich ist ι injektiv.

(c) Man nimmt zum Beispiel

$$1 \longrightarrow N \xrightarrow{\varphi} G \xrightarrow{\pi} H \longrightarrow 1,$$

wobei $\varphi(n) = (n,1)$ und $\pi((n,h)) = h$ ist. Siehe den Abschnitt zu direkten Produkten in §2 der Vorlesung.

(d) Es gelte 1. Dann existiert also ein Gruppenisomorphismus $\Psi : N \rtimes_\alpha H \to G$. Es ist $N \cong N \times \{1\} \subset N \rtimes_\alpha H$ und somit definiert man durch $\varphi(n) := \Psi((n,1))$ einen injektiven Gruppenhomomorphismus. Weiterhin ist nach Vorlesung die Abbildung $\tilde{\pi} : N \rtimes_\alpha H \to H$, $(n,h) \mapsto h$ surjektiv mit $\ker\tilde{\pi} = N \times \{1\}$. Deshalb definiert auch $\pi(g) := \tilde{\pi}(\Psi^{-1}(g))$ einen surjektiven Homomorphismus.

Nach Vorlesung existiert ein Homomorphismus $\tilde{\sigma} : H \to N \rtimes_\alpha H$ mit der Eigenschaft $\tilde{\pi} \circ \tilde{\sigma} = \mathrm{id}_H$. Deshalb erhält man durch $\sigma(h) := \Psi(\tilde{\sigma}(h))$ einen Homomorphismus mit $\pi \circ \sigma = \mathrm{id}_H$. Somit gilt 2.

Gilt umgekehrt 2., so definiert man, wie in der Vorlesung gezeigt

$$\alpha(h)(n) := \varphi^{-1}(\sigma(h))\, n\, \varphi^{-1}(\sigma(h)^{-1}).$$

In der Vorlesung wurde vorgerechnet, dass dies einen Gruppenhomomorphismus $\alpha : H \to \mathrm{Aut}(N)$ liefert (ohne das φ, aber das sollte hier keine Schwierigkeit mehr bereiten) und dass durch

$$\Phi : N \rtimes_\alpha H \to G,\ (n,h) \mapsto \varphi(n)\sigma(h)$$

ein Gruppenisomorphismus definiert wird. Man sollte das an dieser Stelle nochmals sorgfältig nachrechnen und immer genau nachprüfen, welche Voraussetzung man wann benutzt hat.

Aufgabe G5.3 Alle abelschen Gruppen der Ordnung 6

(a) Angenommen, es existiert kein Element der Ordnung 3 in G. Dann hat nach dem Satz von Lagrange jedes von 1 verschiedene Lement die Ordnung 2, denn es kommen nur $1,2,3,6$ als Ordnungen in Frage und für eine Element x der Ordnung 6 hätte x^2 die Ordnung 3. Aus Aufgabe H2.1 wissen wir nun bereits, dass G abelsch ist. Es existieren also 2 verschiedene Elemente $g,h \in G$ der Ordnung 2, so dass $gh \neq 1$ ebenso ein Element der Ordnung 2 ist. Dies sieht man durch Abzählen. Gibt man sich $g \in G$ vor und schließt das Inverse g^{-1} von g aus, so ist das Produkt gh eines von zwei weiteren Elementen der Ordnung 2.

Da G abelsch ist und $g^2 = h^2 = 1$, gilt nach Aufgabe G3.2, dass $H := \langle g,h \rangle = \{1,g,h,gh\}$. Das ist aber nicht möglich, denn H wäre dann ein Normalteiler in G (G ist abelsch) und nach dem Satz von Lagrange wäre $|G| = |G/H||H| \Leftrightarrow 6 = |G/H| \cdot 4$. Also existiert ein Element $a \in G$ der Ordnung 3.

(b) Wir haben in Aufgabe H4.1 gesehen, dass Gruppen gerader Ordnung immer ein selbstinverses Element besitzen.

(c) Wir definieren $U := \langle a \rangle$ und $V := \langle b \rangle$. Dann ist nach Aufgabe H4.3 (a) die Abbildung

$$\varphi : U \times V \to G,\ (u,v) \mapsto uv$$

ein Gruppenhomomorphismus mit $\ker\varphi = \{(u,u^{-1}) : u \in U \cap V\}$. Da jedoch $U \cap V = \{1\}$ gilt, ist φ injektiv und es folgt (aufgrund von $|U \times V| = 6$), dass φ ein Gruppenisomorphismus ist. Somit ist $G \cong U \times V \cong \mathbb{Z}/3/\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z}$. Letzteres ist der Fall, da $\mathrm{ggT}(2,3) = 1$, siehe Vorlesung.

Aufgabe G5.4 Beispiel zu Gruppenoperationen und Bahnen

(a) Wir prüfen die Bedingungen aus der Definition nach:

Bedingung O1: Für alle $z \in \mathbb{C}$ ist $\sigma(0,z) = e^{0\lambda}z = 1z = z$, wie gefordert.

Bedingung O2: Für alle $s,t \in \mathbb{R}$ und $z \in \mathbb{C}$ gilt

$$\sigma(s,\sigma(t,z)) = \sigma(s,e^{t\lambda}z) = e^{s\lambda}e^{t\lambda}z = e^{(s+t)\lambda}z = \sigma(s+t,z),$$

unter Benutzung der Funktionalgleichung der Exponentialfunktion.

Also ist σ eine Operation der additiven Gruppe $(\mathbb{R},+,0)$ auf $\mathbb{C}$.

(b) Die Bahn eines Elements $z \in \mathbb{C}$ ist

$$\mathcal{O}_z := \{e^{t\lambda}z : t \in \mathbb{R}\} = \{e^{t\lambda} : t \in \mathbb{R}\} \cdot z = Ez$$

mit $E := \{e^{t\lambda} : t \in \mathbb{R}\}$. Die Bahn von $0 \in \mathbb{C}$ ist also immer die einpunktige Menge $E0 = \{0\}$. Interessant sind die Bahnen der Elemente $0 \neq z \in \mathbb{C}$.

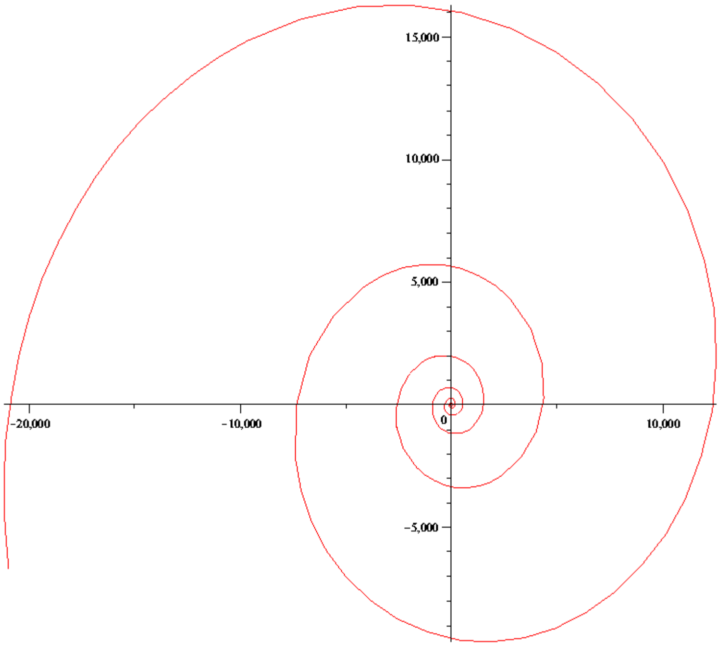
Ist $\lambda = 0$, so ist $E = \{1\}$, somit jede Bahn $\mathcal{O}_z = \{1\}z = \{z\}$ eine einpunktige Menge.

Ist $0 \neq \lambda$ und $\lambda \in \mathbb{R}$, so ist $E =]0,\infty[$ die positive reelle Achse und somit $\mathcal{O}_z =]0,\infty[\ z$ der vom Nullpunkt aus durch z laufende Halbstrahl (ohne die 0).

Ist $0 \neq \lambda$ und $\lambda \in i\mathbb{R}$, so ist $E = \mathrm{S}^1 = \{w \in \mathbb{C} : |w| = 1\}$ der Einheitskreis. Nach Aufgabe G1 (b) ist die Bahn von $0 \neq z$ somit der Kreis um 0 vom Radius $|z|$:

$$\mathcal{O}_z = \mathrm{S}^1 z = |z|\mathrm{S}^1\,.$$

Ist schließlich $\lambda = x + iy$ mit $x, y \in \mathbb{R} \setminus \{0\}$, so ist E eine durch 1 laufende logarithmische Spirale und somit auch Ez eine (um einen Faktor gestreckte) logarithmische Spirale:



Rechnung: Für $z = |z|e^{i\phi}$ erhält man $Ez = \{|z|e^{x(t+\phi/y)+iy(t+\phi/y)-\phi x/y} : t \in \mathbb{R}\} = |z|e^{-\phi x/y}\{e^{t(x+iy)} : t \in \mathbb{R}\} = |z|e^{-\phi x/y}E$.

Aufgabe H5.1 Semidirekte Produkte abelscher Gruppen und $\mathbb{Z}/p^2\mathbb{Z}$

(a) Falls α trivial ist, ist das semidirekte Produkt gleich dem direkten Produkt $H \times G$ und klarerweise abelsch für G, H abelsch. Ist umgekehrt $H \rtimes_\alpha G$ abelsch, so gilt

$$(n, g)(n', g') = (n\alpha(g)(n'), gg') = (n', g')(n, g) = (n'\alpha(g')(n), g'g).$$

Somit ist insbesondere für alle $g, g' \in G, n, n' \in N$: $n\alpha(g)(n') = n'\alpha(g')(n)$. Wählt man $n = n'$, so erhält man $\alpha(g)(n) = \alpha(g')(n)$ für alle $g, g' \in G$. Also ist

$$\alpha(g)(n) = \alpha(1)(n) = 1$$

für alle $g \in G$.

(b) Man überlegt sich leicht mit dem zweiten Homomorphiesatz, dass $H \cong \mathbb{Z}/p\mathbb{Z}$ ist. Angenommen G wäre nun isomorph zu $N \rtimes_\alpha H$ für einen Gruppenhomomorphismus $\alpha : H \to \mathrm{Aut}(N)$. Da G abelsch ist, sind auch N und $H = G/N$ abelsch. Damit muss nach Teil (a) α trivial sein und G wäre isomorph zum direkten Produkt $N \times H \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Dies ist aber nicht möglich, da $G = \mathbb{Z}/p^2\mathbb{Z}$ zyklisch ist (es existiert ein Element der Ordnung p^2, $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ jedoch nicht.

Aufgabe H5.2 Alle nicht-abelschen Gruppen der Ordnung 6

Es sei G eine nicht abelsche Gruppe der Ordnung 6; dann existieren Elemente $a, b \in G$ der Ordnungen 3 und 2 (siehe Aufgabe G5.3).

(a) (a) Die Untergruppe $\langle a \rangle$ hat Ordnung 3 und nach dem Satz von Lagrange somit den Index $[G :< a >] = |G|/|\langle a \rangle| = 6/3 = 2$ und daher ein Normalteiler von G.

(b) Nach Teil (a) gilt $b^{-1}ab \in \langle a \rangle$ und somit $b^{-1}ab = a^i$ für ein $i \in \{0, 1, 2\}$. Wäre $i = 0$, so wäre $b^{-1}ab = 1$ und somit $a = bb^{-1} = 1$; dies ist ein Widerspruch, da a als Element der Ordnung 3 nicht das Neutralelement ist. Wäre $i = 1$, so hätten wir $b^{-1}ab = a$ und somit

$$ab = ba;$$

wäre also die von a und b erzeugte Untergruppe $\langle a, b \rangle \subseteq G$ abelsch. Da $\langle a \rangle$ und $\langle b \rangle$ Untergruppen der Ordnung 2 bzw. 3 von $\langle a, b \rangle$ sind, sind nach dem Satz von Lagrange sowohl 2 als auch 3 Teiler der Gruppenordnung $|\langle a, b \rangle|$, welche wiederum $|G| = 6$ teilt; daher $|\langle a, b \rangle| = 6$ und somit $\langle a, b \rangle = G$; die Gruppe G wäre also abelsch, im Widerspruch zur Aufgabenstellung. Es gilt also $b^{-1}ab = a^2$ und somit $ab = ba^2$.

(c) Die Elemente $a, b \in G$ erzeugen G (nach dem in der Lösung von (b) gegebenen Argument), und es gilt $a^3 = b^2 = 1$ sowie, wie eben gezeigt, $ab = ba^2$. Mit Aufgabe H4.2 folgt, dass $G \cong D_3$.

Aufgabe H5.3 Gruppe der oberen Dreiecksmatrizen

Wir erhalten eine kurze exakte Sequenz

$$1 \longrightarrow N \xrightarrow{\iota} \Delta \xrightarrow{\pi} H \longrightarrow 1,$$

wobei $\iota : N \to \Delta$ die Inklusionsabbildung und $\pi\left(\begin{pmatrix} a & b \\ 0 & c \end{pmatrix}\right) = \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix}$ sind. Die Abbildungen sind Homomorphismen und $\ker \pi = N$. Außerdem ist $\sigma : H \to \Delta$, definiert durch $\sigma(h) = h$ natürlich ein Homomorphismus und es gilt $\pi \circ \sigma = \mathrm{id}_H$ (prüfen!). Die Sequenz spaltet also.

Nach Aufgabe G2.5 (d) gilt dann $\Delta \cong N \rtimes_\alpha H$, wobei

$$\alpha : H \to \mathrm{Aut}(N), \ \alpha(h)(n) = \sigma(h) n \sigma(h)^{-1}.$$

Expliziter ist für $h = \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix}$ das Inverse $\sigma(h)^{-1} = \begin{pmatrix} a^{-1} & 0 \\ 0 & c^{-1} \end{pmatrix}$ und somit für $n = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$:

$$\alpha(h)(n) = \begin{pmatrix} 1 & abc^{-1} \\ 0 & 1 \end{pmatrix}.$$

Aufgabe H5.4 Möbiustransformationen

(a) Zunächst einmal gilt es zu überprüfen, dass $A.z \in \mathbb{H}$ ist:

$$A.z = \frac{az+b}{cz+d} = \frac{(az+b)(c\bar{z}+d)}{|cz+d|^2} = \frac{1}{|cz+d|^2}(acz\bar{z} + bd + (adz + bc\bar{z})).$$

Wir schreiben nun $z = x + iy$ mit $x, y \in \mathbb{R}$ und erhalten

$$A.z = \frac{1}{|cz+d|^2}(ac|z|^2 + bd + (ad+bc)x + iy(ad-bc)).$$

Somit ist

$$\mathrm{Im}(A.z) = \det(A)\frac{\mathfrak{I}(z)}{|cz+d|^2} > 0$$

und $A.z \in \mathbb{H}$. Dann überprüfen wir die Eigenschaften O1) und O2).

O1) $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.z = \frac{1z+0}{0+1} = z$ – das neutrale Element operiert also trivial, wie gefordert.

O2) Wir errechnen

$$\begin{aligned}
\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} e & f \\ g & h \end{pmatrix}\right).z = \begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix}.z &= \frac{(ae+bg)z+af+bh}{(ce+dg)z+cf+dh} \\
&= \frac{a(ez+f)+b(gz+h)}{c(ez+f)+d(gz+h)} \\
&= \frac{a\frac{ez+f}{gz+h}+b}{c\frac{ez+f}{gz+h}+d} \\
&= A.(B.z)
\end{aligned}$$

und somit ist auch diese Eigenschaft erfüllt.

(b) Wenn $z = x + iy \in \mathbb{H}$, so kann einfach die Matrix

$$A_z = \begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix}$$

nehmen, denn es ist $\det(A) = y > 0$ und $A_z.i = yi + x = z$. Es gibt also nur eine einzige Bahn, d.h. die Gruppe G operiert transitiv auf $\mathbb{H}$.

(c) Schreiben wir für $M \in G$

$$M = \begin{pmatrix} \sqrt{\det(M)} & 0 \\ 0 & \sqrt{\det(M)} \end{pmatrix} A,$$

mit $A \in \mathrm{SL}_2(\mathbb{R})$, so ist $M.z = A.z$. Es ist also $G_i = Z \cdot \mathrm{SL}_2(\mathbb{R})_i$, wobei $Z \lhd G$ die Untergruppe der Diagonalmatrizen mit gleichen Diagonaleinträgen ist, also

$$Z = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} : a \in \mathbb{R}^+ \right\}.$$

Dies ist im Übrigen das Zentrum von G (warum?). Sei nun $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R})_i$, dann muss gelten

$$A.i = \frac{ai+b}{ci+d} = \frac{ac+bd+i}{c^2+d^2} = i.$$

Daraus erhält man, dass $c^2+d^2=1$ ist. Es existiert also ein $\theta \in \mathbb{R}$, so dass $\sin(\theta) = c$ und somit auch $\cos(\theta) = d$ ist. Es muss nun noch gelten $a\sin(\theta) + b\cos(\theta) = 0$ und $a\cos(\theta) - b\sin(\theta) = 1$. Also ist $b = -a\tan(\theta)$ und daher $\frac{a}{\cos(\theta)} = 1$, d.h. $a = \cos(\theta)$ und $b = -\sin(\theta)$. Es ist also $A \in \mathrm{SO}_2(\mathbb{R})$ eine Drehmatrix und wir erhalten insgesamt $G_i = Z \cdot \mathrm{SO}_2(\mathbb{R})$.

(d) Wohldefiniertheit: Wenn $[A] = [B]$ gilt, dann existiert ein $C \in G_i$, so dass $A = BC$. Es ist somit $A.i = (BC).i = B.(C.i) = B.i$, da $C \in G_i$.

Die Abbildung ist surjektiv, da G transitiv operiert und sie ist injektiv, denn

$$A.i = B.i \iff (A^{-1}B).i = i \iff A^{-1}B \in G_i \iff B \in AG_i \iff [A] = [B].$$