Übung zur Vorlesung Einführung in die Algebra

Prof. Dr. J. H. Bruinier
Stephan Ehlen

TECHNISCHE UNIVERSITÄT DARMSTADT

Sommersemester 2009
Lösungshinweise zu Übungsblatt 3

Aufgabe G3.1 Automorphismen von $\mathbb{Z}$

Das ist im Prinzip lineare Algebra: Sei $f \in \mathrm{Aut}(\mathbb{Z}^2)$. Für die Bilder der Einheitsvektoren schreiben wir

$$f((1,0)^T) = (a,c)^T, \text{ und } f((0,1)^T) = (b,d)^T.$$

Dann ist für $(m,n)^T \in \mathbb{Z}^2$, da f ein Homomorphismus ist

$$f((m,n)^T) = mf((1,0)^T) + nf((0,1)^T) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} m \\ n \end{pmatrix}.$$

Insbesondere ist f durch eine 2×2-Matrix A mit Einträgen in $\mathbb{Z}$ darstellbar. Das Gleiche gilt natürlich für f^{-1} und für die darstellende Matrix A' von f^{-1} (bzgl. der Standardbasis) folgt

$$AA' = A'A = E_2.$$

Somit ist $\mathrm{Aut}(\mathbb{Z}^2) = \mathrm{GL}_2(\mathbb{Z}) = \{A \in M_n(\mathbb{Z}) : \det(A) \neq 0\} = \{A \in M_n(\mathbb{Z}) : \det(A) = \pm 1\}$.

Allgemein lässt sich festhalten, dass $\mathrm{Hom}(\mathbb{Z}^n, \mathbb{Z}^n)$ durch den multiplikativen Monoid $(M_n(\mathbb{Z}), \cdot, E_n)$ der $n \times n$ Matrizen mit ganzzahligen Einträgen gegeben ist. Dessen Einheitengruppe $\mathrm{GL}_n(\mathbb{Z}) := M_n(\mathbb{Z})^\times$ ist dann die Automorphismengruppe von $(\mathbb{Z}^n, +)$.

Aufgabe G3.2 Eine von zwei Elementen erzeugte Gruppe

(a) Wenn wir zeigen können, dass

$$H := \{a^i b^j : i, j \in \mathbb{Z}\}$$

eine Untergruppe von G ist, so ist dies offensichtlich die von a und b erzeugte Untergruppe (und somit gleich G), denn letztere enthält all die Elemente $a^i b^j$ (vgl. Lemma I.1.9 (3) im Skript) - was Teil (a) beweist. Dass H eine Untergruppe ist, folgt daraus, dass

$$a^i b^j = b^j a^i \qquad \text{für alle } i, j \in \mathbb{Z} \tag{1}$$

(wie wir gleich beweisen werden). Es ist dann nämlich $1 = a^0 b^0 \in H$ und stets $(a^i b^j)(a^k b^\ell) = a^i a^k b^j b^\ell = a^{i+j} b^{k+\ell} \in H$ sowie $(a^i b^j)^{-1} = (b^j)^{-1}(a^i)^{-1} = b^{-j} a^{-i} = a^{-i} b^{-j} \in H$, wie für eine Untergruppe verlangt.

Es bleibt nur, (1) zu beweisen.

Erste Beweisstrategie für (1): Schritt 1. Zeige zunächst durch Induktion nach $i \in \mathbb{N}_0$, dass $a^i b = b a^i$ und $a^{-i} b = b a^{-i}$.

Schritt 2. Zeige durch Induktion nach $j \in \mathbb{N}_0$, dass

$$(\forall i \in \mathbb{Z}) \qquad a^i b^j = b^j a^i \quad \text{und} \quad a^i b^{-j} = b^{-j} a^i$$

(die Ausführung der Induktionen ist dem Leser überlassen).

Zweite, elegantere Beweisstrategie für (1): Wir betrachten die Menge

$$X := \{x \in G : xb = bx\}$$

der mit b vertauschenden Elemente von G. Dann ist X eine Untergruppe von G, denn es gilt: $1 \in X$ wegen $1b = b = b1$. Gegeben $x \in X$ gilt $xb = bx$ und somit, durch Multiplikation letzterer Gleichung mit x^{-1} von links und rechts, $bx^{-1} = x^{-1}b$; also $x^{-1} \in X$. Schließlich gilt für alle $x, y \in X$:

$$(xy)b = x(yb) = x(by) = (xb)y = (bx)y = b(xy),$$

also $xy \in X$. Es ist also X eine Untergruppe von G, und da diese per Aufgabenstellung das Element a enthält, gilt $\{a^i : i \in \mathbb{Z}\} = \langle a \rangle \subseteq X$ und somit

$$a^i b = b a^i, \qquad \text{für alle } i \in \mathbb{Z}. \tag{2}$$

Analog sehen wir, dass

$$Y := \{x \in G : (\forall i \in \mathbb{Z})\ xa^i = a^i x\}$$

eine Untergruppe von G ist, die wegen (2) das Element b enthält. Es gilt daher $\langle b \rangle \subseteq Y$ und somit $a^i b^j = b^j a^i$ für alle $i, j \in \mathbb{Z}$.

(b) Unter Benutzung von (1) haben wir für alle $x = a^i b^j$, $y = a^k b^\ell \in G$:

$$xy = a^i b^j a^k b^\ell = a^i a^k b^j b^\ell = a^{i+k} b^{j+\ell}$$

und

$$yx = a^k b^\ell a^i b^j = a^{k+i} b^{\ell+j},$$

also $xy = yx$. Somit ist G abelsch.

Aufgabe G3.3 Normalteiler

Zu zeigen ist nach ganz kurzer Überlegung nur $(c) \Rightarrow (b)$.
Dazu: Es ist zu zeigen, dass für jedes $g \in G$ gilt: $N \subset gNg^{-1}$.
Sei $n \in N$, dann wissen wir, dass $g^{-1}ng = n' \in N$ gilt, indem man (c) auf g^{-1} anwendet. Somit ist $n = gn'g^{-1} \in gNg^{-1}$ und das war zu zeigen.

Aufgabe G3.4 Die Quaternionengruppe

(a) Es ist z.B. $IJ = K$, aber $JI = -K$.

(b) Man stellt fest, dass die Ordnung der Elemente $\pm I, \pm J$ und $\pm K$ gleich 4 ist und damit $-E$ das einzige selbstinverse Element (d.h. $\mathrm{ord}(-E) = 2$) ist. Nach dem Satz von Lagrange kann es überhaupt nur nichttriviale Untergruppen der Ordnung 2 und 4 geben. Ist H eine Untergruppe mit $|H| = 4$, so ist der Index also 2 und nach Aufgabe H3.4 (b) ist H dann normal. Ist $|H| = 2$, so ist offensichtlich $H = \{\pm E\}$. Diese Gruppe ist normal, da sie mit allen Elementen von Q vertauscht.

Aufgabe G3.5 Permutationsdarstellung

Sei $G = \{g_1, \ldots, g_n\}$ eine endliche Gruppe und S_n bezeichne die symmetrische Gruppe einer n-elementigen Menge.

(a) Zunächst mal muss man sich die Definition vielleicht an einem Beispiel klar machen - dies sei dem Leser überlassen. Seien nun $g, h \in G$ und $i \in \{1, \ldots, n\}$. Es gelte $hg_i = g_j$ und $gg_j = g_k$. Dann gilt

$$\begin{aligned}(gh)g_i &= g(hg_i)\\ &= gg_j\\ &= g_k.\end{aligned}$$

Somit ist einerseits $\rho(gh)(i) = \sigma_{gh}(i) = k$ und andererseits

$$\begin{aligned}(\rho(h) \circ \rho(g))(i) &= \rho(h)(\rho(g)(i))\\ &= \sigma_h(\sigma_g(i))\\ &= \sigma_h(j)\\ &= k.\end{aligned}$$

Dies zeigt, dass ρ ein Homomorphismus ist.

(b) Seien $g, h \in G$ mit $\rho(g) = \rho(g)$. Dann ist insbesondere $\sigma_g(1) = \sigma_h(1)$ und nach Definition

$$g g_1 = h g_1.$$

Mit Übung H2.2 (a) folgert man, dass dann $g = h$ gelten muss.
Nun ist das Bild einer Gruppe unter einem Homomorphismus wieder eine Gruppe und da ρ injektiv ist, erhalten wir $G \cong \rho(G) \subset S_n$.

Aufgabe H3.1 Rechnen mit Kongruenzen

(a) Wir schreiben nun abkürzend $\bar{x} = x + m\mathbb{Z}$. Wähle z.B. $\{\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{m-1}\}$ als Repräsentantensystem.

(b) Unabhängigkeit von der Wahl der Vertreter: Falls $x' \in \bar{x}$ und $y' \in \bar{y}$ sind, so existieren $a, b \in \mathbb{Z}$, so dass

$$x' = x + am \quad \text{und} \quad y' = y + bm$$

gilt. Somit ist

$$\overline{x'y'} = \overline{xy + aym + bxm + abm^2} = \overline{xy}$$

und demnach ist die Definition unabhängig von der Wahl der Vertreter.

Dass $(\mathbb{Z}/m\mathbb{Z}, \cdot, \bar{1})$ ein Monoid ist, ist klar, denn dies folgt direkt daraus, dass $(\mathbb{Z}, \cdot, 1)$ ein Monoid ist (Nachrechnen kann natürlich nicht schaden).

(c) $\mathbb{Z}/m\mathbb{Z}$ hat genau dann nichttriviale Nullteiler, wenn m keine Primzahl ist.

Es sei $\bar{x} \in \mathbb{Z}/m\mathbb{Z}$ ein Nullteiler mit $\bar{x} \neq \bar{0}$. Dann existiert ein $\bar{y} \in \mathbb{Z}/m\mathbb{Z}, \bar{y} \neq \bar{0}$, so dass $\bar{x}\bar{y} = \bar{0}$ ist. Daraus folgt $xy \in m\mathbb{Z}$, also existiert ein $a \in \mathbb{Z}$, so dass $xy = am$. Da $\bar{x}, \bar{y} \neq \bar{0}$, teilt m weder x noch y. Somit ist m keine Primzahl.

Ist umgekehrt $m > 1$ keine Primzahl, so gibt es $m_1, m_2 \in \mathbb{Z}$ mit $m = m_1 m_2$ und $|m_1|, |m_2| > 1$. Es ist also $\overline{m_1}, \overline{m_2} \neq \bar{0}$ und $\bar{m_1}\bar{m_2} = \bar{m_1}\bar{m_2} = \bar{m} = \bar{0}$. Somit sind m_1 und m_2 nichttriviale Nullteiler.

(d) **Behauptung:** $((\mathbb{Z}/m\mathbb{Z}) \setminus \{0\}, \cdot, \bar{1})$ ist eine Gruppe, genau dann, wenn m eine Primzahl ist.

Beweis: Wir wissen schon aus (c), dass $(\mathbb{Z}/m\mathbb{Z}, \cdot, \bar{1})$ ein Monoid ist, genau dann, wenn m eine Primzahl ist. Dies gilt dann auch für $((\mathbb{Z}/m\mathbb{Z}) \setminus \{0\}, \cdot, \bar{1})$. Daraus folgt bereits, dass $((\mathbb{Z}/m\mathbb{Z}) \setminus \{0\}, \cdot, \bar{1})$ keine Gruppe ist, wenn m keine Primzahl ist. Um zu zeigen, dass es eine Gruppe ist, wenn m eine Primzahl ist müssen wir nur noch zeigen, dass jedes Element in $(\mathbb{Z}/m\mathbb{Z}) \setminus \{0\}$ ein Inverses besitzt. Wir zeigen hierzu, dass die Multiplikationsabbildung

$$\begin{aligned} \alpha_{\bar{x}} : \mathbb{Z}/m\mathbb{Z} &\to \mathbb{Z}/m\mathbb{Z} \\ \bar{y} &\mapsto \overline{xy} \end{aligned}$$

in diesem Fall für jedes $\bar{x} \in (\mathbb{Z}/m\mathbb{Z}) \setminus \{0\}$ bijektiv ist. Da $(\mathbb{Z}/m\mathbb{Z})$ endlich ist, reicht es zu zeigen dass $\alpha_{\bar{x}}$ injektiv ist. Dies haben wir jedoch schon in (c) gesehen, denn $\bar{y} \in \ker(\alpha_{\bar{x}})$ ist äquivalent zu $\bar{x}\bar{y} = 0$ und dies bedeutet für $\bar{x} \neq \bar{0}$, dass $\bar{y}$ ein Nullteiler ist. Falls m eine Primzahl ist, folgt jedoch, dass $\bar{y} = \bar{0}$ ist und somit $\ker(\alpha_{\bar{x}}) = \{\bar{0}\}$.

Aufgabe H3.2 Additive Darstellung des ggT; Erzeuger zyklischer Gruppen

(a) Gegeben zwei Zahlen $k_1, k_2 \in \mathbb{Z}$, die nicht beide 0 sind, ist $\mathrm{ggT}(k_1, k_2)$ die eindeutig festgelegte natürliche Zahl mit

$$\langle k_1, k_2 \rangle = \mathrm{ggT}(k_1, k_2)\mathbb{Z},$$

wobei $\langle k_1, k_2 \rangle$ die von k_1, k_2 erzeugte Untergruppe von $(\mathbb{Z}, +, 0)$ ist. (Dies war eine Bemerkung zu Lemma 3 in §1 in der Vorlesung, auch zu finden als Bemerkung I.1.12 im Skript von Herrn Prof. Neeb).

Da $(\mathbb{Z}, +, 0)$ und somit auch $(\langle k_1, k_2 \rangle, +, 0)$ abelsch sind, haben wir nach Aufgabe G3.2 :

$$\langle k_1, k_2 \rangle = \{ik_1 + jk_2 : i, j \in \mathbb{Z}\}.$$

Gilt also $\mathrm{ggT}(k_1, k_2) = 1$, so ist

$$1 \in \mathbb{Z} = \mathrm{ggT}(k_1, k_2)\mathbb{Z} = \{ik_1 + jk_2 : i, j \in \mathbb{Z}\},$$

weswegen wir $a, b \in \mathbb{Z}$ finden mit $ak_1 + bk_2 = 1$.

Gibt es umgekehrt $a, b \in \mathbb{Z}$ mit $ak_1 + bk_2 = 1$, so gilt

$$1 \in \{ik_1 + jk_2 : i, j \in \mathbb{Z}\} = \mathrm{ggT}(k_1, k_2)\mathbb{Z}.$$

Es existiert also ein $n \in \mathbb{Z}$ mit $1 = \mathrm{ggT}(k_1, k_2)n$. Daraus folgt $\mathrm{ggT}(k_1, k_2) = 1$.

(b) Sei $k \in \{0, 1, \ldots, n-1\}$. Falls das Element $\zeta := e^{\frac{2\pi i k}{n}}$ die Gruppe C_n erzeugt, so gilt $C_n = \{\zeta^m : m \in \mathbb{Z}\}$, es gibt also ein $m \in \mathbb{Z}$ derart, dass

$$\zeta^m = e^{\frac{2\pi i}{n}}.$$

Somit $e^{\frac{2\pi i k m}{n}} = e^{\frac{2\pi i}{n}}$. Es existiert also ein $\ell \in \mathbb{Z}$ mit $\frac{2\pi k m}{n} = \frac{2\pi}{n} + 2\pi\ell$. Dann ist

$$km - \ell n = 1$$

und somit $\mathrm{ggT}(k, n) = 1$, nach Teil (a).

Nun nehmen wir umgekehrt an, dass $\mathrm{ggT}(k, n) = 1$ (d.h. k und n sind teilerfremd); wir wollen zeigen, dass dann ζ die Gruppe C_n erzeugt. Nach Teil (a) existieren $a, b \in \mathbb{Z}$ derart, dass

$$ak + bn = 1.$$

Für $\zeta := e^{\frac{2\pi i k}{n}}$ gilt also

$$\zeta^a = e^{\frac{2\pi i a k}{n}} = e^{\frac{2\pi i (1-bn)}{n}} = e^{\frac{2\pi i}{n} - 2\pi i b} = e^{\frac{2\pi i}{n}},$$

somit $e^{\frac{2\pi i}{n}} \in \langle\zeta\rangle$, und somit $e^{\frac{2\pi i \ell}{n}} = (e^{\frac{2\pi i}{n}})^\ell \in \langle\zeta\rangle$ für alle $\ell \in \mathbb{Z}$. Da jede n-te Einheitswurzel vorige Gestalt hat, gilt $C_n \subseteq \langle\zeta\rangle$ und somit $C_n = \langle\zeta\rangle$, d.h. ζ ist ein Erzeuger für C_n.

Aufgabe H3.3 Gruppenhomomorphismus

Wir schreiben die Verknüpfung in G hier multiplikativ. Die Elemente g und h müssen vertauschen, denn es ist

$$gh = \phi(1,0)\phi(0,1) = \phi((1,0)+(0,1)) = \phi(1,1) = \phi((0,1)+(1,0)) = \phi(0,1)\phi(1,0) = hg. \tag{3}$$

Dass g und h vertauschen ist also eine notwendige Bedingung für die Existenz eines solchen Gruppenhomomorphismus. Allgemein ist außerdem

$$\phi(m,n) = \phi(m(1,0)+n(0,1)) = \phi(1,0)^m \cdot \phi(0,1)^n = g^m h^n. \tag{4}$$

Wir zeigen, dass die Bedingung (3) auch hinreichend ist. Seien $g, h \in G$ mit $gh = hg$. Dann definieren wir durch (4) motiviert

$$\phi(m,n) := g^m h^n.$$

Zu zeigen ist, dass dies tatsächlich ein Gruppenhomomorphismus ist. Wir benutzen, dass die von g und h erzeugte Untergruppe abelsch ist (nach Aufgabe G3.2):

$$\begin{aligned}\phi((a,b)+(c,d)) &= g^{a+c}h^{b+d}\\ &= g^a g^c h^b h^d\\ &= (g^a h^b)(g^c h^d)\\ &= \phi(a,b)\phi(c,d).\end{aligned}$$

Also existiert ein solcher Gruppenhomomorphismus genau dann, wenn g und h miteinander vertauschen.

Aufgabe H3.4 Nebenklassen und Normalteiler

(a) Sei $1 \neq h \in G$ ein beliebiges Element. Wir betrachten die von h erzeugte Untergruppe $H := \langle h\rangle$. Nach dem Satz von Lagrange gilt

$$p = |G| = |H|[G:H].$$

Hierbei ist $[G:H]$ eine natürliche Zahl. Also gilt $|H| \mid p$. Da p eine Primzahl ist, folgt $|H| = 1$ oder $|H| = p$. Falls H nur ein Element enthält, ist $h = 1$, was ausgeschlossen war. Es muss also $H = G$ gelten und G ist zyklisch. Wir haben insbesondere gesehen, dass G von jedem Element außer der 1 erzeugt wird.

(b) Da $[G:H] = 2$ gilt, sind die Linksnebenklassen gegeben durch $G/H = \{H, M\}$, wobei $M := G \setminus H$ das Komplement von H in G ist. Ist also $g \in M = G \setminus H$, so ist $gH = M$. Analog sieht man, dass für $g \in M = G \setminus H$ auch $Hg = M$ sein muss. Damit ist also $gH = Hg$ für alle $g \in G$ und H ist Normalteiler.

(c)* Wir konstruieren eine Gegenbeispiel für den Fall $[G:H] = 3$. Es sei $\sigma = (12) \in S_3$ die Transposition der Zahlen 1 und 2. Dann ist $H := \langle\sigma\rangle = \{\mathrm{id}, \sigma\}$ und nach dem Satz von Lagrange gilt $[G:H] = 3$. Man sieht aber leicht, dass σ nicht mit $\tau = (23)$ vertauscht, also $\tau H \neq H\tau$.

Aufgabe H3.5 Freiwillige Zusatzaufgabe: Elemente der Ordnung p

Wir betrachten die im Hinweis angegebene Menge $S = \{(a_0, \dots, a_{p-1}) \in G^p : a_0 \cdots a_{p-1} = 1\}$. Falls $(a_0, \dots, a_{p-1}) \in S$, so ist auch $(a_1, \dots, a_{p-1}, a_0) \in S$, denn $a_1 \cdots a_{p-1} a_0 = a_0^{-1}(a_0 \cdots a_{p-1})a_0 = 1$. Wir bezeichnen diese zyklische Permutation mit $\pi \in S_S$, d.h.

$$\pi((a_0, \dots, a_{p-1})) = (a_1, \dots, a_{p-1}, a_0)$$

für $(a_0, \dots, a_{p-1}) \in S$. Die p-fache Hintereinanderausführung π^p liefert die Identität auf S. Die einzigen Punkte, die von π festgehalten werden, sind die Elemente der Form $(a, \dots, a) \in S$, das heißt solche, die von Elementen $a \in G$ kommen mit $a^p = 1$. Für diese Elemente schreiben wir nun $H := \{a \in G \mid a^p = 1\}$. Es ist $|H| = n + 1$, da $1 \in H$.

Wir bezeichnen im Folgenden abkürzend $Z := \mathbb{Z}/p\mathbb{Z}$ und mit $Z_s := \{\bar{n} \in \mathbb{Z}/p\mathbb{Z}, \pi^n(s) = s\}$ den Stabilisator von s unter den zyklischen Permutationen. Außerdem bezeichnen wir mit $B_s := \{\pi^n(s) : n \in \mathbb{N}\}$ die *Bahn* unter den zyklischen Permutationen von $s \in S$. Man mache sich klar, dass diese Definitionen Sinn machen! Der Trick ist nun der Folgende: Z_s ist eine Untergruppe von $\mathbb{Z}/p\mathbb{Z}$, denn für $\bar{k}, \bar{l} \in Z_s$ ist $\pi^{k+l}(s) = \pi^k(\pi^l(s)) = \pi^k(s) = s$ und wenn $\pi^k(s) = s$, so ist $s = \pi^{-k}(s)$. Außerdem ist natürlich $\pi^0(s) = \mathrm{id}(s) = s$. Nun sind aber die einzigen Untergruppen von Z gleich $\{\bar{0}\}$ und Z selbst. Der Fall $Z_s = \{\bar{0}\}$ tritt nur ein, wenn $s = (a, \dots, a)$ ist mit $a \in G$.

So erkennen wir, dass für alle anderen Elemente $s \in S \setminus H$ gilt $|B_s| = p$, wobei wir H hier als Teilmenge von S ansehen (über die offensichtliche Inklusion).

Zwei Bahnen B_s, B_r für $r, s \in S$ sind entweder disjunkt oder identisch. Deshalb gibt es Elemente $s_1, \dots, s_m \in S$, so dass die Menge S folgendermaßen zerfällt:

$$S = B_{s_1} \cup \dots \cup B_{s_m} \cup \{(a, \dots, a) : a \in H\}.$$

Es gilt somit

$$|S| = mp + n + 1.$$

Andererseits ist $|S| = |G|^{p-1}$ und nach dem Satz von Lagrange ist dies durch p teilbar, falls ein Element der Ordnung p existiert. Also ist entweder $n = 0$ oder p teilt $n + 1$, da $p \mid |G|^{p-1} = mp + (n + 1)$ gilt.

In der Lösung dieser Aufgabe haben wir ein Beispiel für eine Gruppenoperation gesehen. Gruppenoperationen (manchmal auch Gruppenwirkungen genannt) werden später ausführlich in der Vorlesung behandelt. Im vorliegenden Fall ist die zyklische Permutation eine Gruppenoperation der additiven Gruppe $\mathbb{Z}/p\mathbb{Z}$.