Übung zur Vorlesung Einführung in die Algebra

Prof. Dr. J. H. Bruinier
Stephan Ehlen

TECHNISCHE UNIVERSITÄT DARMSTADT

Sommersemester 2009
Lösungshinweise zu Übungsblatt 4

Aufgabe G4.1 Isomorphe Gruppen

(a) Da jeder Isomorphismus insbesondere eine Bijektion ist, ist die Behauptung offensichtlich.

(b) Ist G abelsch, so gilt für alle $x, y \in H$:

$$xy = \phi(\phi^{-1}(xy)) = \phi(\phi^{-1}(x)\phi^{-1}(y)) = \phi(\phi^{-1}(y)\phi^{-1}(x)) = \phi(\phi^{-1}(yx)) = yx\,.$$

Also ist auch H abelsch.

(c) Ist G zyklisch, so gibt es ein Element $g \in G$ mit $G = \langle g \rangle = \{g^n : n \in \mathbb{Z}\}$. Es gilt

$$H = \phi(G) = \{\phi(g^n) : n \in \mathbb{Z}\} = \{\phi(g)^n : n \in \mathbb{Z}\} = \langle \phi(g) \rangle\,,$$

(formal wäre das eine Induktion nach n, die keine Schwierigkeiten bereiten sollte) es ist also H zyklisch mit Erzeuger $\phi(g)$.

(d) Sind $x, y \in H$ beide vom neutralen Element $1 \in H$ verschieden, so sind $\phi^{-1}(x)$ und $\phi^{-1}(y)$ beide vom neutralen Element $1 \in G$ verschieden. Nach Voraussetzung existieren also Zahlen $n, m \in \mathbb{Z} \setminus \{0\}$ derart, dass $\phi^{-1}(x)^n = \phi^{-1}(y)^m$. Es ist dann

$$\phi(\phi^{-1}(x)^n) = \phi(\phi^{-1}(x))^n = x^n \tag{1}$$

und analog

$$\phi(\phi^{-1}(y)^m) = y^m\,. \tag{2}$$

Da die linken Seiten von (1) und (2) nach dem Vorigen übereinstimmen, stimmen auch die rechten Seiten überein, es ist also $x^n = y^m$.

Aufgabe G4.2 Was kann zwei Gruppen unterscheiden?

(a) $\mathbb{R}$ ist überabzählbar, $\mathbb{Q}$ hingegen abzählbar. Da jeder Isomorphismus insbesondere eine Bijektion ist, können $\mathbb{R}$ und $\mathbb{Q}$ also nicht ismorph sein.

(b) Jedes nicht-triviale Element $x \in \mathbb{R}$ hat unendliche Ordnung, in S^1 hingegen gibt es das Element -1 von der Ordnung 2. Also können $\mathbb{R}$ und S^1 nicht isomorph sein.

(c) In $\mathbb{Q}$ haben je zwei von 0 verschiedene Elemente m/n, k/ℓ ein gemeinsames Vielfaches wie in Aufgabe G4.1 (d), da $(kn)(m/n) = km = (m\ell)(k/\ell)$. In $\mathbb{Q}^2$ hingegen ist dies nicht der Fall.

(d) Jedes nicht-triviale Element der additiven Gruppe $\mathbb{R}$ hat unendliche Ordnung, während es in der multiplikativen Gruppe $\mathbb{R}^\times$ ein nicht-triviales Element endlicher Ordnung gibt (nämlich -1, ein Element der Ordnung 2). Gäbe es einen Isomorphismus $\phi : \mathbb{R} \to \mathbb{R}^\times$, wäre $0 = \phi^{-1}(1) = \phi^{-1}((-1)^2) = 2\phi^{-1}(-1)$ mit $\phi^{-1}(-1) \neq 0$, es wäre also $\phi^{-1}(-1)$ ein Element der Ordnung 2 in $\mathbb{R}$, was unmöglich ist.

Aufgabe G4.3 Untergruppen von $\mathbb{Z}$

(a) $\Leftarrow$ (b): Sei $\mathrm{ggT}(m,n)=1$. Klar ist $mn\mathbb{Z}\subset n\mathbb{Z}\cap m\mathbb{Z}$. Ist $a\in n\mathbb{Z}\cap m\mathbb{Z}$, so gilt $a=nb=mc$ mit $a,b\in\mathbb{Z}$ geeignet. Da $\mathrm{ggT}(m,n)=1$, existieren $x,y\in\mathbb{Z}$, so dass $mx+ny=1$ (nach Aufgabe H3.2 (a)). Also erhalten wir, dass

$$\begin{aligned} c &= c(mx+ny)\\ &= xmc+cny\\ &= xa+ync\\ &= xnb+ync\\ &= (xb+yc)n. \end{aligned}$$

Setzen wir $c' := xb+yc\in\mathbb{Z}$, erhalten wir $a=mnc'\in mn\mathbb{Z}$.

(a) $\Rightarrow$ (b): Sei $m\mathbb{Z}\cap n\mathbb{Z}=mn\mathbb{Z}$. Angenommen, es sei $\mathrm{ggT}(m,n)=k>1$. Dann existieren $r,s\in\mathbb{Z}$, so dass $m=rk$ und $n=sk$. Dann ist aber $rsk\in m\mathbb{Z}\cap n\mathbb{Z}$, denn $rsk=sm=rn$, aber $rsk\notin mn\mathbb{Z}$.

Aufgabe G4.4 Abelsche Gruppen und Normalteiler

(a) Da G abelsch ist, erhalten wir für alle Nebenklassen xN, yN von N in G:

$$xNyN = xyN = yxN = yNxN\,.$$

Somit is auch G/N abelsch.

(b) Ist G zyklisch, so gilt $G=\langle g\rangle=\{g^n : n\in\mathbb{Z}\}$ für ein Element $g\in G$. Da die Quotientenabbildung $\pi\colon G\to G/N$ ein Homomorphismus ist, erhalten wir

$$\pi(G)=\{\pi(g^n)\colon n\in\mathbb{Z}\}=\{\pi(g)^n : n\in\mathbb{Z}\}=\langle\pi(g)\rangle.$$

Es ist somit G/N zyklisch, mit Erzeuger $\pi(g)$.

Aufgabe G4.5 Die Quotientengruppe $\mathbb{Q}/\mathbb{Z}$

Für $m/n\in\mathbb{Q}$ mit $m,n\in\mathbb{Z}$ ist $n\cdot(m/n)=n\in\mathbb{Z}$, also ist $\mathrm{tor}(\mathbb{Q}/\mathbb{Z})=\mathbb{Q}/\mathbb{Z}$.

Aufgabe G4.6 Inversion

Ist die Inversion ein Gruppenhomomorphismus, so gilt $a^{-1}b^{-1}=(ab)^{-1}=b^{-1}a^{-1}$. Wendet man dies auf a^{-1} und b^{-1} an, so sieht man, dass G abelsch sein muss.

Aufgabe H4.1 Gruppen gerader Ordnung

Ist G eine endliche Gruppe *gerader Ordung*, so betrachte die Mengen

$$A := \{x\in G : x\neq x^{-1}\} \qquad \text{und} \qquad B := \{x\in G : x=x^{-1}\}\,.$$

Dann hat A eine gerade Zahl von Elementen. Schreiben wir nämlich $x\sim y$ für $x,y\in A$ genau dann, wenn $x=y$ oder $y=x^{-1}$, so ist $\sim$ eine Äquivalenzrelation auf A (Nachweis !), deren Äquivalenzklassen $\{x,x^{-1}\}$ je zwei Elemente besitzen. Da A eine disjunkte Vereinigung

$$A=\bigcup_{X\in A/\sim} X$$

zwei-elementiger Mengen ist, ist die Anzahl der Elemente von A gerade,

$$|A| = 2\cdot|A/\sim|\,.$$

Die Menge B ist nicht leer (denn $1\in B$). Da $|B|=|G|-|A|$ gerade ist, muss B also mindestens zwei Elemente besitzen. Es existiert also $x\in B$ mit $x\neq 1$, und dieses Element hat die verlangten Eigenschaften.

Ist nun andererseits G eine endliche Gruppe *ungerader Ordnung*, so gibt es kein Element $x\in G$ mit $x\neq 1$ und $x=x^{-1}$. Wäre nämlich x ein solches, so wäre $x^2=1$ und daher $\langle x\rangle=\{1,x\}$ eine Gruppe der Ordnung 2. Nach dem Satz von Lagrange müsste nun die Untergruppenordnung 2 die Ordnung von G teilen, diese wäre also eine gerade Zahl, im Widerspruch zur Annahme.

Aufgabe H4.2 Die Diedergruppe D_3

(a) Wir zeigen, dass $H := \left\{a^i b^j : i \in \{0,1,2\},\ j \in \{0,1\}\right\}$ eine Untergruppe von G ist. Dann ist offensichtlich $H = \langle a, b\rangle$, also $H = G$ (da G per Voraussetzung von a und b erzeugt ist).

Offensichtlich ist $1 = a^0 b^0 \in H$.

Die folgende Beobachtung ist nützlich: Da $ab = ba^2$, haben wir $a^2 b = aab = aba^2 = ba^2a^2 = ba^4$ und analog per Induktion

$$a^k b = ba^{2k} \qquad \text{für alle } k \in \mathbb{N}. \tag{3}$$

Abgeschlossenheit von H unter der Multiplikation von G: Es seien $a^i b^j$ und $a^k b^\ell \in H$, mit $i,k \in \{0,1,2\}$ und $j,\ell \in \{0,1\}$

Fall $j = 0$: Dann ist $a^i b^j a^k b^\ell = a^i a^k b^\ell = a^{i+k} b^\ell = a^m b^\ell \in H$, wobei $m \in \{0,1,2\}$ mit $m \equiv i + k \pmod 3$.

Fall $j = 1$: Dann ist

$$\begin{aligned} a^i b^j a^k b^\ell &= a^i b a^k b^\ell = a^i b a^k \underbrace{bb}_{=1} b^\ell \overset{(1)}{=} a^i b b a^{2k} b b^\ell \\ &= a^i a^{2k} b^{1+\ell} = a^{i+2k} b^{1+\ell} = a^r b^s \in H \end{aligned}$$

mit $r \in \{0,1,2\}$ und $s \in \{0,1\}$ derart, dass $r \equiv i + 2k \pmod 3$ und $s \equiv 1 + \ell \pmod 2$.

Abgeschlossenheit von H unter der Inversion: Gegeben $x = a^i b^j \in H$ gilt

$$x^{-1} = (a^i b^j)^{-1} = b^{-j} a^{-i} = (b^{-1})^j (a^{-1})^i = b^j (a^2)^i = b^j a^{2i}\,.$$

Falls $j = 0$, ist also $x^{-1} = a^{2i} \in H$. Andernfalls ist $x^{-1} = ba^{2i} = a^i b = x \in H$, wobei (3) benutzt wurde.

(b) Wir betrachten das gleichseitige Dreieck $\Delta \subseteq \mathbb{R}^2$ mit den Ecken $(1,0)$; $(\cos\frac{2\pi}{3}, \sin\frac{2\pi}{3}) = (-\frac{1}{2}, \frac{1}{2}\sqrt{3})$; $(-\frac{1}{2}, -\frac{1}{2}\sqrt{3})$.

Das Dreieck wird von Vielfachen einer 120^0-Drehung um den Ursprung und von einer Spiegelung an der x-Achse in sich selbst überführt. Wir wählen dadurch motiviert

$$A := \begin{pmatrix} -\frac{1}{2} & -\frac{1}{2}\sqrt{3} \\ \frac{1}{2}\sqrt{3} & -\frac{1}{2} \end{pmatrix}$$

und

$$B := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Dann gilt offensichtlich $A^3 = B^2 = E_2$. Weiter ist

$$A^2 = A^{-1} = \begin{pmatrix} -\frac{1}{2} & \frac{1}{2}\sqrt{3} \\ -\frac{1}{2}\sqrt{3} & -\frac{1}{2} \end{pmatrix}$$

und somit

$$AB = \begin{pmatrix} -\frac{1}{2} & \frac{1}{2}\sqrt{3} \\ \frac{1}{2}\sqrt{3} & \frac{1}{2} \end{pmatrix} = BA^2,$$

wie verlangt. Vergleich der für die Matrizen E_2, A, A^2, B, AB und A^2B berechneten Ausdrücke zeigt, dass diese paarweise verschieden sind. Da $D_3 := \langle A, B\rangle$ nach (a) genau die vorigen Elemente enthält, hat diese Gruppe also 6 Elemente, wie verlangt. Die den Elementen von D_3 entsprechenden linearen Abbildungen sind: E_2 - identische Abbildung; A - 120^0-Drehung; A^2 - 240^0-Drehung; B - Spiegelung an der x-Achse; AB - Spiegelung an der Ursprungsgeraden $\mathbb{R}(-\frac{1}{2}, -\frac{1}{2}\sqrt{3})$ durch die linke untere Ecke von Δ; A^2B - Spiegelung an der Ursprungsgeraden $\mathbb{R}(-\frac{1}{2}, \frac{1}{2}\sqrt{3})$ durch die linke obere Ecke von Δ. Jede dieser Abbildungen bildet Δ bijektiv auf sich ab.

(c) Offensichtlich sind $\{E_2\}$ und D_3 Untergruppen (und Normalteiler) von D_3. Ist nun $\{E_2\} \neq H \neq D_3$ eine Untergruppe von D_3, so existiert ein Element $X \neq E_2$ in H. Ist $X = A$ oder $X = A^2$, so gilt $\langle X \rangle = \{E_2, A, A^2\} \subseteq H$ und somit

$$H = \{E_2, A, A^2\} = \langle A \rangle;$$

weil die Ordnung von H die Gruppenordnung $6 = 2 \cdot 3$ teilt und $\{E_2, A, A^2\}$ bereits 3 Elemente hat, kann nämlich H als echte Untergruppe von G nicht mehr als drei Elemente besitzen. Nach dem Satz von Lagrange hat $\langle A \rangle$ als 3-elementige Untergruppe der 6-elementigen Gruppe D_3 den Index $[G : \langle A \rangle] = |G| : |\langle A \rangle| = 2$. Nach Aufgabe H3.4 (b) ist somit $\langle A \rangle$ ein Normalteiler von D_3.

Analog sehen wir, dass

$$H = \{E_2, B\}, \qquad H = \{E_2, AB\} \qquad \text{bzw.} \qquad H = \{E_2, A^2B\},$$

falls $X = B$, $X = AB$ bzw. $X = A^2B$. Genauere Begründung: Falls z.B. $B \in H$, so ist $\langle B \rangle = \{E_2, B\}$ eine Untergruppe der Ordnung 2 von H. Nach dem Satz von Lagrange ist also die Ordnung $|H|$ durch 2 teilbar. Da $|H|$ zudem $|G| = 2 \cdot 3$ teilt, ist nur $|H| = 2$ (also $H = \{E_2, B\}$) oder $|H| = 6$ möglich, wobei wir zweiteren Fall durch die Voraussetzung $H \neq D_3$ jedoch ausgeschlossen haben. Also $H = \{E_2, B\}$.

Keine der letzteren drei Untergruppen ist ein Normalteiler, denn es gilt $A\{E_2, B\}A^{-1} \ni ABA^{-1} = A^2B \notin \{E_2, B\}$, $A\{E_2, AB\}A^{-1} \ni AABA^{-1} = A^3B = B \notin \{E_2, AB\}$ und $A\{E_2, A^2B\}A^{-1} \ni A^3BA^{-1} = BA^{-1} = AB \notin \{E_2, A^2B\}$ (was nach Aufgabe G3.3 im Falle eines Normalteilers nicht sein könnte).

(d) Beachte zunächst, dass ϕ wohldefiniert ist, denn nach Teil (b) sind die Elemente A^iB^j mit $i \in \{0, 1, 2\}$, $j \in \{0, 1\}$ paarweise verschieden.

Nach Teil (a) lässt sich jedes Element $x \in G$ in der Form a^ib^j schreiben mit $i \in \{0, 1, 2\}$ und $j \in \{0, 1\}$. Dann ist $\phi(A^iB^j) = a^ib^j = x$. Somit ist ϕ surjektiv.

Um zu sehen, dass ϕ ein Gruppenhomomorphismus ist, seien $X, Y \in D_3$. Dann ist $X = A^iB^j$ und $Y = A^kB^\ell$ für gewisse (eindeutig festgelegte) $i, k \in \{0, 1, 2\}$ und $j, \ell \in \{0, 1\}$.

Fall $j = 0$: Dann ist $XY = A^mB^\ell$ und $\phi(X)\phi(Y) = a^ib^ja^kb^\ell = a^mb^\ell = \phi(XY)$ mit m wie im Beweis des Falles $j = 0$ von Teil (a) (angewandt zweimal, einmal auf die Gruppe D_3, einmal auf G).

Fall $j = 1$: Dann ist $XY = A^rB^s$ und $\phi(X)\phi(Y) = a^ib^ja^kb^\ell = a^rb^s = \phi(XY)$ mit r, s wie im Beweis des Falles $j = 1$ von Teil (a). Da in beiden möglichen Fällen $\phi(XY) = \phi(X)\phi(Y)$, ist ϕ ein Gruppenhomomorphismus.

Nach dem Homomorphiesatz ist $G \cong D_3/\ker\phi$, wobei $\ker\phi$ ein Normalteiler von D_3 ist und somit nach dem Vorigen

$$\ker\phi \in \big\{\{E_2\},\ \langle A \rangle,\ D_3\big\}.$$

Es ist also $G \cong D_3/\{E_2\} \cong D_3$ oder $G \cong D_3/\langle A \rangle \cong \mathbb{Z}/2\mathbb{Z}$ (nach Aufgabe H3.4 (a), da dies eine Gruppe der Primzahlordnung 2 ist), oder $G \cong D_3/D_3 \cong \{E_2\}$ eine triviale Gruppe. Jeder der Fälle kann auftreten, denn für jeden Normalteiler N von D_3 gilt $D_3/N = \langle AN, BN \rangle$, wobei $a := AN$ und $b := BN$ die in (a) formulierten Relationen erfüllen.

Aufgabe H4.3 Alle Gruppen der Ordnung 4

(a) Gegeben $u_1, u_2 \in U$, $v_1, v_2 \in V$ gilt

$$\alpha((u_1, v_1)(u_2, v_2)) = \alpha(u_1u_2, v_1v_2) = u_1u_2v_1v_2 = u_1v_1u_2v_2 = \alpha(u_1, v_1)\alpha(u_2, v_2),$$

wobei das dritte Gleichheitszeichen gilt, weil G abelsch ist. Somit ist α ein Homomorphismus. Gegeben $u \in U$, $v \in V$ gilt $\alpha(u, v) = 1$ genau dann, wenn $uv = 1$, also $u = v^{-1}$. In diesem Falle ist $u = v^{-1} \in U \cap V$ und somit auch $v = u^{-1} \in U \cap V$. Umgekehrt haben wir $u^{-1} \in V$ für jedes $u \in U \cap V$, und $\alpha(u, u^{-1}) = uu^{-1} = 1$. Es ist also $\ker\alpha = \{(u, u^{-1}) : v \in U \cap V\}$.

(b) Es sei G eine Gruppe der Ordnung 4. Nach dem Satz von Lagrange kann die Ordnung eines Elements $x \in G$ nur 1, 2 oder 4 sein, denn sie teilt die Gruppenordnung.

Gibt es eine Element $x \in G$ der Ordnung 4, so hat $\langle x \rangle$ vier Elemente, weswegen $G = \langle x \rangle$ eine zyklische Gruppe der Ordnung 4 ist, somit isomorph zu $\mathbb{Z}/4\mathbb{Z}$ nach Vorlesung und klarerweise abelsch.

Andernfalls hat jedes Element $x \in G$ die Ordnung 1 oder 2, es gilt also stets $x^2 = 1$. Daher ist G abelsch nach Aufgabe H2.1 (a).

(c) Wir wissen schon: Falls G zyklisch ist, so ist G isomorph zu $\mathbb{Z}/4\mathbb{Z}$.

Wählen wir nun zwei vom Neutralelement verschiedene Elemente $x \neq y$ in G, so gilt $U := \langle x \rangle = \{1, x\}$, $V := \langle y \rangle = \{1, y\}$, also $U \cap V = \{1\}$. Der Homomorphismus $\alpha\colon U \times V \to G$ aus (a) hat Kern $\ker \alpha = \{(u, u^{-1})\colon u \in U \cap V\} = \{1\}$, er ist also injektiv. Da sowohl $U \times V$ als auch G jeweils 4 Elemente haben, muss die injektive Abbildung α surjektiv sein. Als bijektiver Gruppenhomomorphismus ist α ein Isomorphismus, also $G \cong U \times V = \langle x \rangle \times \langle y \rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Aufgabe H4.4 Die Gruppe $\mathrm{GL}_n(\mathbb{F})$

Es sei $n \in \mathbb{N}$ und $\mathbb{F}$ ein endlicher Körper mit q Elementen.

(a) Wir verfahren gemäß der gegebenen Anleitung: Jede Spalte s einer Matrix $A \in M_n(\mathbb{F})$ ist ein Vektor in $\mathbb{F}^n$, es gibt also $|\mathbb{F}|^n = q^n$ Möglichkeiten für s. Sind $s_1, \dots, s_n$ die Spalten von A und soll $A \in \mathrm{GL}_n(\mathbb{F})$ sein, so muss $s_1 \neq 0$ sein, es bleiben also $q^n - 1$ Möglichkeiten für s_1. Für gewähltes s_1 sollen s_1, s_2 linear unabhängig sein, also $s_2 \notin \mathbb{F}s_1$, was q Möglichkeiten für s_2 ausschließt; es verbleiben $q^n - q$. Weiter darf s_3 nicht im Spann $\mathbb{F}s_1 + \mathbb{F}s_2$ von s_1 und s_2 sein, welcher q^2 Elemente hat; es verbleiben $q^n - q^2$ Möglichkeiten für s_3. Analog haben wir zu bereits gewählten linear unabhängigen Spalten $s_1, \dots, s_{k-1}$ genau $q^n - q^{k-1}$ Möglichkeiten, die nächste Spalte s_k zu wählen (wobei $k \leq n$). Insgesamt gibt es für $A \in \mathrm{GL}_n(\mathbb{F})$ also

$$|\mathrm{GL}_n(\mathbb{F})| = (q^n - 1)(q^n - q) \cdots (q^n - q^{n-1}) = \prod_{i=0}^{n-1} \left(q^n - q^i\right)$$

Möglichkeiten.

(b) Gegeben $t \in \mathbb{F}^\times$ haben wir $\det A = t$ für die Diagonalmatrix $A \in \mathrm{GL}_n(\mathbb{F})$ mit Diagonaleinträgen $t, 1, \dots, 1$.

Also ist det ein surjektiver Homomorphismus und es gilt mit 1. Homomorphiesatz

$$\mathbb{F}^\times = \operatorname{im} \det \cong \mathrm{GL}_n(\mathbb{F}) / \ker \det = \mathrm{GL}_n(\mathbb{F}) / \mathrm{SL}_n(\mathbb{F}).$$

(c) Nach dem Satz von Lagrange gilt

$$\begin{aligned}(q^n - 1) \cdots (q^n - q^{n-1}) &= |\mathrm{GL}_n(\mathbb{F})| = [\mathrm{GL}_n(\mathbb{F}) : \mathrm{SL}_n(\mathbb{F})] \cdot |\mathrm{SL}_n(\mathbb{F})| = |\mathbb{F}^\times| \cdot |\mathrm{SL}_n(\mathbb{F})| \\ &= (q - 1) |\mathrm{SL}_n(\mathbb{F})|,\end{aligned}$$

somit

$$|\mathrm{SL}_n(\mathbb{F})| = (q-1)^{-1} (q^n - 1) \cdots \overbrace{(q^n - q^{n-1})}^{= q^{n-1}(q-1)} = q^{n-1} \prod_{i=0}^{n-2} \left(q^n - q^i\right).$$