Fachbereich Mathematik
Prof. Dr. J.H. Bruinier
Martin Fuchssteiner
Kay Schwieger

TECHNISCHE UNIVERSITÄT DARMSTADT
WS 07/08 08./09.11.07

Lineare Algebra I

4. Übung mit Lösungshinweisen

Gruppenübungen

(G 1) Minitest

Wobei handelt es sich **nicht** um eine Gruppe?

☐ $(\mathbb{R}, +)$ ☐ $(\mathbb{R}^n, +)$ ☐ $(\mathbb{R}, \cdot)$ ☐ $(\mathbb{Q} \setminus \{0\}, \cdot)$
☐ $(\mathbb{Z} \setminus \{0\}, \cdot)$ ☐ $(\mathbb{Z} \setminus \{0\}, +)$ ☐ $(\mathbb{N}, +)$ ☐ $(\mathbb{Z}, -)$

LÖSUNG: Bei $(\mathbb{R}, +)$, $(\mathbb{R}^n, +)$ und $(\mathbb{Q} \setminus \{0\}, \cdot)$ handelt es sich um Gruppen. Alle anderen Beispiele sind keine Gruppen: Bei $(\mathbb{R}, \cdot)$ besitzt $0 \in \mathbb{R}$ kein Inverses. Bei $(\mathbb{Z} \setminus \{0\}, \cdot)$ besitzt z.B. $2 \in \mathbb{Z}$ kein Inverses, bei $(\mathbb{Z} \setminus \{0\}, +)$ gibt es kein neutrales Element, bei $(\mathbb{N}, +)$ besitzt z.B. $1 \in \mathbb{N}$ kein Inverses und $(\mathbb{Z}, -)$ ist nicht assoziativ.

Satz 1. *Sei A eine $m \times n$-Matrix und B eine $n \times k$-Matrix. Dann gilt*

$$\operatorname{Rang}(A \cdot B) \leq \operatorname{Rang}(A) \qquad \textit{und} \qquad \operatorname{Rang}(A \cdot B) \leq \operatorname{Rang} B\,.$$

(G 2)

Sei A eine $m \times n$-Matrix und $U \subseteq \mathbb{R}^n$ ein linearer Teilraum.

(a) Zeigen Sie, dass
$$V := \{Ax \mid x \in U\}$$
ein linearer Teilraum des $\mathbb{R}^m$ ist.

(b) Zeigen Sie, dass die Dimension von V kleiner gleich der Dimension von U ist.

(c) Beweisen Sie damit Satz 1.

LÖSUNG: (a) Seien $y_1, y_2 \in V$ und $\lambda \in \mathbb{R}$. Dann gibt es $x_1, x_2 \in U$ mit $y_1 = Ax_1$ und $y_2 = Ax_2$. Somit folgt

$$y_1 + y_2 = Ax_1 + Ax_2 = A(x_1 + x_2) \in V \qquad \lambda y_1 = \lambda A x_1 = A(\lambda x_1) \in V\,,$$

da U ein lineare Teilraum ist und $x_1 + x_2 \in U$ bzw. $\lambda x_1 \in U$ gilt.

(b) Seien $y_1, \ldots, y_k \in V$ linear unabhängig. Dann gibt es $x_1, \ldots, x_k \in U$ mit $y_i = Ax_i$ für alle Indizes i. Wir zeigen, dass dann auch $x_1, \ldots, x_k$ linear unabhängig sind. Seien hierzu $\lambda_1, \ldots, \lambda_k \in \mathbb{R}$ mit $0 = \sum_{i=1}^k \lambda_i x_i$. Dann gilt

$$\sum_{i=1}^k \lambda_i y_i = \sum_{i=1}^k \lambda_i A x_i = A\Big(\sum_{i=1}^k \lambda_i x_i\Big) = A(0) = 0\,.$$

Wegen der linearen Unabhängigkeit der y_i folgt daraus $\lambda_i = 0$ für alle Indizes i. Somit sind die x_i linear unabhängig.

Sei k die Dimension von V. Sei weiter $y_1, \ldots, y_k \in V$ eine Basis von V und $x_1, \ldots, x_n \in U$ mit $y_i = Ax_i$ für alle Indizes i. Dann sind $x_1, \ldots, x_k$ linear unabängig. Somit hat U mindestens Dimension k.

(c) Der Rang von AB ist die Dimension des linearen Teilraumes $\{ABx \mid x \in \mathbb{R}^k\}$, der Rang von A ist die Dimension von $\{Ay \mid y \in \mathbb{R}^n\}$ und der Rang von B ist die Dimension von $\{Bx \mid x \in \mathbb{R}^k\}$. Nun gilt

$$\{ABx \mid x \in \mathbb{R}^k\} \subseteq \{Ay \mid y \in \mathbb{R}^n\} .$$

Insbesondere ist auch die Dimension des linken Teilraumes kleiner gleich der Dimension des rechten Teilraumes, d.h. $\mathrm{Rang}(AB) \leq \mathrm{Rang}(A)$.

Setzen wir $U := \{Bx \mid x \in \mathbb{R}^k\}$ und $V := \{Ay \mid y \in U\} = \{ABx \mid x \in \mathbb{R}^k\}$, so haben wir im vorherigen Aufgabenteil gezeigt, dass die Dimension von V kleiner gleich der Dimension von U ist, d.h

$$\mathrm{Rang}(AB) = \dim(V) \leq \dim(U) = \mathrm{Rang}(B) .$$

Definition 1. *Sei $(G, \cdot)$ eine Gruppe mit neutralem Element $e \in G$. Eine Untergruppe von G ist eine Teilmenge $H \subseteq G$ mit den Eigenschaften:*

(i) $e \in H$,

(ii) für alle $a, b \in H$ gilt auch $ab \in H$,

(iii) für alle $a \in H$ gilt auch $a^{-1} \in H$.

(G 3)

Sei G ein Gruppe mit der Verknüpfung $\bullet : G \times G \to G$ und neutralem Element $e \in G$. Zeigen Sie, dass für eine nicht-leere Teilmenge $H \subseteq G$ die folgenden Bedinungen äquivalent sind:

(a) H ist eine Untergruppe von G.

(b) Die Verknüpfung lässt sich zu $\bullet : H \times H \to H$ einschränken und das Paar $(H, \bullet)$ bildet eine Gruppe mit neutralem Element e.

(c) Für alle $a, b \in H$ gilt auch $ab^{-1} \in H$.

LÖSUNG:

- Wir zeigen zuerst die Implikation (a) $\Rightarrow$ (b): Weil für alle Paar $(a, b) \in H \times H$ das Produkt $a \bullet b$ wieder in H liegt, lässt sich die Verknüpfung zu $\bullet : H \times H \to H$ einschränken.

  Wir müssen also nur zeigen, dass $(H, \bullet)$ eine Gruppe mit neutralem Elment e bildet. Weil G assoziativ ist, gilt das Assoziativgesetzt insbesondere für alle Elemente aus H, d.h. $(H, \bullet)$ erfüllt das Assoziativgesetz. Das neutrale Element e von G liegt wegen Punkt (i) der Definition in H. Weil e das neutrale Element in $G \supseteq H$ ist bildet es auch ein neutrales Element bezüglich der eingeschränkten Verknüpfung, d.h. e ist das neutrale Element von $(H, \bullet)$. Für ein Element $a \in H$ liegt nach Punkt (iii) der Definition auch das Inverse a^{-1} in H und, weil G eine Gruppe ist, gilt $aa^{-1} = e = a^{-1}a$.

- Wir zeigen nun die Implikation (b) $\Rightarrow$ (a):

  Weil sich die Verknüpfung auf $\bullet : H \times H \to H$ einschränken lässt, gilt für alle $a, b \in H$ auch $a \bullet b \in H$ (vgl. Punkt (ii) der Definition). Da e das neutrale Element von $(H, \bullet)$ bildet, gilt insbesondere $e \in H$ (vgl. Punkt (i) der Definition). Weil $(H, \bullet)$ eine Gruppe bildet, gibt es für jedes Element $a \in H$ ein Element $b \in H$ mit $ba = e = ab$. Damit ist b auch in der Gruppe $(G, \bullet)$ das inverse Element von a, d.h. $b = a^{-1} \in H$ (vgl. Punkt (iii) der Definition).

- Als nächstes zeigen wir die Implikation (a) $\Rightarrow$ (c): Sei $H \subseteq G$ eine Untergruppe, und seien $a, b \in G$. Dann gilt nach (iii) in der Definition auch $b^{-1} \in H$. Nach Punkt (ii) der Definition gilt dann auch $ab^{-1} \in H$.

- Zuletzt zeigen wir die Implikation (c) $\Rightarrow$ (a). Sei hierzu $H \subseteq G$ eine nicht-leere Teilmenge mit Eigenschaft (c). Weil H nicht leer ist, gibt es ein Element $h \in H$. Nach Voraussetzung gilt dann auch $e = hh^{-1} \in H$ (vgl. Punkt (i) der Definition). Für jedes Element $a \in H$ folgt dann auch $a^{-1} = ea^{-1} \in H$ (vgl. Punkt (iii) der Definition). Für zwei Elemente $a, b \in H$ gilt also auch $b^{-1} \in H$ und damit nach Voraussetzung $ab = a(b^{-1})^{-1} \in H$ (vgl. Punkt (ii) der Definition).

(G 4)

Wir betrachten die Gruppe $(\mathbb{Z}, +)$.

(a) Zeigen Sie, dass für jedes $k \in \mathbb{Z}$ die Menge $k\mathbb{Z} := \{kn \mid n \in \mathbb{Z}\}$ eine Untergruppe ist.

(b) Zeigen Sie, dass jede Untergruppe von $(\mathbb{Z}, +)$ von dieser Form ist.

LÖSUNG: (a) Das neutrale Element $0 = k \cdot 0$ liegt in $k\mathbb{Z}$.

Seien $a, b \in k\mathbb{Z}$. Dann gibt es $n_a, n_b \in \mathbb{Z}$ mit $a = kn_a$ und $b = kn_b$. Somit liegen auch $a + b = kn_a + kn_b = k(n_a + n_b)$ und $-a = -(kn_a) = k(-n_a)$ in $k\mathbb{Z}$.

(b) Sei $H \subseteq \mathbb{Z}$ eine Untergruppe. Ist $H = \{0\}$, so brauchen wir nichts zu zeigen, denn $\{0\} = 0\,\mathbb{Z}$. Wir nehmen deshalb im Folgenden o.B.d.A. $H \neq \{0\}$ an. Wir setzen

$$k := \min\{n \in H \mid n > 0\}$$

und wollen zeigen, dass $H = k\mathbb{Z}$ gilt.

Zuerst zeigen wir $k\mathbb{Z} \subseteq H$. Sei hierzu $a \in k\mathbb{Z}$. Dann gibt es ein $n \in \mathbb{Z}$ mit $a = kn$. Weil nach Konstruktion $k \in H$ gilt, folgt daraus

$$a = kn = \underbrace{k + k + \cdots + k}_{n \text{ viele Summanden}} \in H\ .$$

Nun zeigen wir $H \subseteq k\mathbb{Z}$. Wir zeigen dies durch einen Widerspruchsbeweis und nehmen an, dass es ein $a \in H \setminus (k\mathbb{Z})$ gibt. Durch Division durch k mit Rest erhalten wir ein $q \in \mathbb{Z}$ und ein $r \in \{0, \ldots, n-1\}$ mit

$$a = k \cdot q + r\ .$$

Das Element kq liegt in $k\mathbb{Z} \subseteq H$. Somit liegt wegen $a, kq \in H$ auch $r = a - k \cdot q$ in H. Aufgrund der Konstruktion von k muss dann $r = 0$ gelten, denn andernfalls wäre k nicht minimal. Es folgt $a = kq \in k\mathbb{Z}$ und dies steht im Widerspruch zur Annahme $a \notin k\mathbb{Z}$.

Hausübungen

(A 11) (10 Punkte)

Sei G eine Gruppe mit neutralem Element $e \in G$. Zeigen Sie:

(a) (Kürzungsregel)
Seien $a, b \in G$. Gibt es ein Element $c \in G$ mit $ac = bc$ oder mit $ca = cb$, so gilt $a = b$.

(b) Gilt $a^2 = e$ für jedes Element $a \in G$, so ist G abelsch.

(c) Sei $g \in G$. Wir definieren induktiv für $n \geq 0$

$$g^0 := e \qquad\qquad g^{n+1} := gg^n$$

und setzen $g^{-n} := (g^n)^{-1}$. Zeigen Sie, dass für alle $n, m \in \mathbb{Z}$ gilt

$$g^n g^m = g^{n+m} .$$

LÖSUNG: (a) Gilt $ac = bc$, so folgt

$$a \overset{\text{Neutral.}}{=} ae \overset{\text{Inverse}}{=} a(cc^{-1}) \overset{\text{Assoz.}}{=} (ac)c^{-1} = (bc)c^{-1} \overset{\text{Assoz.}}{=} b(cc^{-1}) \overset{\text{Inverse}}{=} be \overset{\text{Neutral.}}{=} b .$$

Den Fall $ca = cb$ zeigt man analog.

(b) Seien $a, b \in G$. Dann gilt

$$\begin{aligned} ab &\overset{\text{Neutral.}}{=} (ab)e \overset{\text{Vor.}}{=} (ab)(aa) \overset{\text{Neutral.}}{=} (ab)\big((ae)a\big) \overset{\text{Vor.}}{=} (ab)\big((a(bb))a\big) \\ &\overset{\text{Assoz.}}{=} (ab)\big(((ab)b)a\big) \overset{\text{Assoz.}}{=} (ab)\big((ab)(ba)\big) \overset{\text{Assoz.}}{=} \big((ab)(ab)\big)(ba) \overset{\text{Vor.}}{=} e(ba) \\ &\overset{\text{Neutral.}}{=} ba \end{aligned}$$

(c) Wir zeigen zuerst mit vollständiger Induktion über n, dass für alle $n, m \geq 0$ die Gleichung $g^n g^m = g^{n+m}$ gilt:

- Für den Induktionsanfang $n = 0$ rechnet man direkt nach:

$$g^0 g^m \overset{\text{Def.}}{=} eg^m \overset{\text{Neutral.}}{=} g^m = g^{0+m} .$$

- Wir nehmen an, dass für alle $m \in \mathbb{N}$ die Gleichung $g^n g^m = g^{n+m}$ gilt (Induktionsannahme). Dann gilt auch

$$g^{n+1} g^m \overset{\text{Def}}{=} (gg^n)g^m \overset{\text{Assoz.}}{=} g(g^n g^m) \overset{\text{Ind.Ann.}}{=} gg^{n+m} \overset{\text{Def}}{=} g^{n+m+1} = g^{(n+1)+m} .$$

Wir haben nun die Behauptung für $n, m \geq 0$ gezeigt. Als nächste sei $n < 0$ und $m \in \mathbb{Z}$. Gilt nun $n + m \geq 0$, so ergibt sich nach dem bereits Gezeigtem mit $k := -n$

$$g^k(g^n g^m) = (g^k g^n)g^m = \big(g^k (g^k)^{-1}\big)g^m = eg^m = g^m = g^{k+m+n} = g^k g^{m+n} .$$

Aus der Kürzungsregel folgt dann $g^n g^m = g^{n+m}$. Gilt hingegen $n + m < 0$, so gilt und $-m - n > 0$ und es ergibt sich aus dem Gezeigtem

$$\begin{aligned} g^n g^m &= ((g^n g^m)^{-1})^{-1} = \big((g^m)^{-1}(g^n)^{-1}\big)^{-1} = \big(g^{-m} g^{-n}\big)^{-1} = (g^{-m-n})^{-1} \\ &= (g^{-(n+m)})^{-1} = g^{n+m} \end{aligned}$$

Satz 2 (Satz von Lagrange). *Sei G eine endliche Gruppe und $H \subseteq G$ eine Untergruppe. Dann teilt die Kardinalität der Untergruppe $|H|$ die Kardinalität der Gruppe $|G|$.*

(A 12) (10 Punkte)

Wir wollen den Satz von Lagrange in mehreren Schritten beweisen. Sei hierzu G eine Gruppe mit endlich vielen Elementen und $H \subseteq G$ eine Untergruppe.

(a) Für $a \in G$ heißt die Menge $aH := \{ah \mid h \in H\}$ Nebenklasse von H. Zeigen Sie, dass für zwei Elemente $a, b \in G$ entweder $aH = bH$ oder $aH \cap bH = \emptyset$ gilt.

(b) Zeigen Sie, dass H eine Nebenklasse von sich selbst ist.

(c) Zeigen Sie, dass alle Nebenklassen die gleiche Anzahl von Elementen haben, d.h. für alle $a, b \in G$ gilt $|aH| = |bH|$.

Hinweis: Sie können benutzen, dass zwei endliche Mengen die gleich Anzahl an Elementen haben, falls es eine Bijektion zwischen ihnen gibt.

(d) Zeigen Sie: $|H|$ teilt $|G|$.

LÖSUNG: (a) Seien $a, b \in G$. Gilt $aH \cap bH = \emptyset$, so brauchen wir nichts zu zeigen. Wir betrachten deshalb den Fall $aH \cap bH \neq \emptyset$. In diesem Fall gibt es ein Element $c \in aH \cap bH$. Wegen $c \in aH$ gibt es ein $h_c \in H$ mit $c = ah_a$, und wegen $c \in bH$ gibt es ein $h_b \in H$ mit $c = bh_b$. Daraus ergibt sich dann durch Multiplikation mit h_a^{-1} bzw. h_b^{-1}

$$a = ch_a^{-1} = bh_b h_a^{-1} \qquad \text{und} \qquad b = ch_b^{-1} = ah_a h_b^{-1} .$$

Sei nun d ein Element in aH. Dann gibt es ein $h \in H$ mit $d = ah = bh_b h_a^{-1} h$. Weil das Element $h' := h_b h_a^{-1} h$ in H liegt, gilt also $d = bh' \in bH$. Damit ist gezeigt, dass alle Elemente aus aH auch in bH liegen, d.h. $aH \subseteq bH$. Analog zeigt man auch $bH \subseteq aH$. Zusammen ergibt sich daraus $aH = bH$.

(b) $H = eH$.

(c) Wir zeigen, dass alle Nebenklassen $|H|$-viele Elemente haben. Weil H selbst eine Nebenklasse ist, ergibt sich daraus die Behauptung. Sei also aH eine Nebenklasse mit $a \in G$. Wir zeigen $|aH| = |H|$, indem wir die Abbildung $\phi : H \to aH,\ h \mapsto ah$ betrachten und zeigen, dass sie bijektiv ist:

(i) Um zu zeigen, dass ϕ injektiv ist, seien $h_1, h_2 \in aH$ mit $\phi(h_1) = \phi(h_2)$. Dann gilt

$$h_1 = a^{-1}ah_1 = a^{-1}\,\phi(h_1) = a^{-1}\,\phi(h_2) = a^{-1}ah_2 = h_2 .$$

(ii) Um zu zeigen, dass ϕ surjektiv ist, sei $g \in aH$. Nach Definition der Nebenklasse gibt es dann ein Element $h \in H$ mit $g = ah = \phi(h)$.

Zusammenfassend ist $\phi : aH \to bH$ eine injektive und surjektive, also bijektive Abbildung. Die Menge H und aH müssen deshalb die gleiche Anzahl an Elementen haben.

(d) Für jedes Element $a \in G$ gilt $a \in aH$. Somit ist G die Vereinigung seiner Nebenklassen, d.h.

$$G = \bigcup_{a \in G} aH .$$

Weil zwei Nebenklassen entweder gleich oder disjunkt sind, können wir Elemente $a_1, \ldots, a_n \in G$ auswählen, so dass die zugehörigen Nebenklassen $a_i H$ paarweise disjunkt sind und dass

$$G = \bigcup_{i=1}^{n} a_i H$$

gilt. Weil all diese Nebenklassen disjunkt sind und genau $|H|$ Elemente haben, folgt daraus $|G| = |a_i H| + \cdots + |a_n H| = n \cdot |H|$.

Satz 3 (Kleiner Satz von Fermat). *Sei G eine endliche Gruppe mit $n = |G|$ Elementen und neutralem Element $e \in G$. Dann gilt für alle $g \in G$*

$$g^n = e .$$

(A 13) (10 Punkte)

Wir wollen in dieser Aufgabe in mehreren Schritten den kleine Satz von Fermat zeigen.

(a) Sei G eine Gruppe und $g \in G$. Zeigen Sie, dass die Menge

$$\langle g \rangle := \{g^n \mid n \in \mathbb{Z}\}$$

eine abelsche Untergruppe von G ist.

(b) Sei G eine endliche Gruppe und $g \in G$. Zeigen Sie, dass es ein $n \in \mathbb{N}$ gibt mit

$$\langle g \rangle = \{e, g^1, \ldots, g^{n-1}\} .$$

(c) Beweisen Sie den kleinen Satz von Fermat.

Hinweis: Beweisen Sie den Satz erst für die Gruppe $\langle g \rangle$ und nutzen Sie dann den Satz von Lagrange.

LÖSUNG: Wir bezeichnen mit $e \in G$ das neutrale Element von G.

(a) $e = g^0 \in \langle g \rangle$.

Seien $a, b \in \langle g \rangle$. Dann gibt es $n, m \in \mathbb{Z}$ mit $a = g^n$ und $b = g^m$. Somit gilt

$$ab = g^n g^m = g^{n+m} \in \langle g \rangle \qquad \text{und} \qquad a^{-1} = (g^n)^{-1} = g^{-n} \in \langle g \rangle$$

Somit ist $\langle g \rangle$ eine Untergruppe. Weil außerdem $ab = g^{n+m} = ba$ gilt, ist diese Untergruppe abelsch.

(b) Wären alle Elemente g^n mit $n \in \mathbb{Z}$ verschieden, so hätte H (und damit auch G) unendlich viele Elemente. Es müssen deshalb mindestens zwei dieser Elemente gleich sein, d.h. es gibt $n, m \in \mathbb{Z}$ mit $n \neq m$ und $g^n = g^m$. Wir können o.B.d.A. $n > m$ annehmen. Daraus ergibt sich nach den Potenzgesezten $g^{n-m} = e$. Indem wir die Exponenten jeweils ganzzahlig (mit Rest) durch $(n - m)$ dividieren, folgt für die Gruppe H

$$\begin{aligned} H &= \{g^k \mid k \in \mathbb{Z}\} = \{g^{q(n-m)+r} \mid q \in \mathbb{Z}, r \in \{0, \ldots, n-m-1\}\} \\ &= \{(g^{n-m})^q g^r \mid q \in \mathbb{Z}, r \in \{0, \ldots, n-m-1\}\} = \{g^r \mid r \in \{0, \ldots, n-m-1\}\} . \end{aligned}$$

(Allerdings können wir hier noch nicht $|H| = n - m$ folgern, weil u.U. nicht alle Elemente g^r mit $r \in \{0, \ldots, n-m-1\}$ verschieden sind.)

(c) Wir zeigen den kleinen Satz von Fermat zuerst für die Untergruppe $H := \langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$. Wählen setzen

$$k_0 := \min\{n - m \mid n > m,\ g^n = g^m\} .$$

Wie im vorherigen Aufgabenpunkt ergibt sich dann $g^{k_0} = e$ und

$$H = \{e, g^1, \ldots, g^{k_0-1}\} .$$

Würde nun $g^i = g^j$ für zwei Zahlen $0 \leq i < j \leq k_0 - 1$ gelten, so würde daraus $e = g^j (g^i)^{-1} = g^{j-i}$ folgern. Dies stünde dann wegen $j - i < k_0$ jedoch im Widerspruch zur Minimalität von k_0. Folglich sind alle Elemente $e, g^1, \ldots, g^{k_0-1}$ verschieden. Es gilt somit

$$|H| = k_0 \qquad \text{und} \qquad g^{|H|} = g^{k_0} = e .$$

Wir haben damit den kleinen Satz von Fermat für die Untergruppe $H = \langle g \rangle \subseteq G$ gezeigt. Nach dem Satz von Lagrange ist $|H|$ ein Teiler von $|G|$. Es gibt also ein $k \in \mathbb{N}$ mit $|G| = k \cdot |H|$. Für das Element g gilt somit

$$g^{|G|} = g^{k \cdot |H|} = (g^{|H|})^k = e^k = e .$$