Einführung in die Algebra
1. Übung
Lösungsvorschlag

Gruppenübung

G 1 (Gruppen und Untergruppen)

Welche der folgenden Mengen sind Untergruppen der allgemeinen linearen Gruppe $GL_2(\mathbb{R})$?

$$H_1 = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in \mathbb{R} \right\}, \qquad H_2 = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \mid a \in \mathbb{R}^*, b \in \mathbb{R} \right\},$$
$$H_3 = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL_2(\mathbb{R}) \mid a, b, c, d \in \mathbb{Z} \right\},$$
$$H_4 = \{ A \in GL_2(\mathbb{R}) \mid det\, A > 0 \}, \qquad H_5 = \{ A \in GL_2(\mathbb{R}) \mid tr\, A = 0 \},$$

(1) $\begin{pmatrix} 1 & b_1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & b_2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & b_1 + b_2 \\ 0 & 1 \end{pmatrix}$, $\Rightarrow H_1 \cong (\mathbb{R}, +)$.

(2) $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}^{-1} = \frac{1}{a} \begin{pmatrix} 1 & -b \\ 0 & a \end{pmatrix} \in H_2$.

(3) $\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}^{-1} = \frac{1}{2} \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \notin H_3$.

(4) $det\left(A^{-1}\right) = (det\, A)^{-1} > 0$, $det\,(AB) = det\,(A)\, det\,(B) > 0$

(5) $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ *hat Spur* -2.

G 2 (Monoid, Modul, Algebra)

Wir betrachten die Menge M aller Abbildungen $\varphi : \mathbb{R} \to \mathbb{R}$ erst als Monoid, dann als $\mathbb{R}$-Modul und schließlich als $\mathbb{R}$-Algebra.

(a) Welche Verknüpfungen auf M müssen dazu betrachtet werden?

(b) Was ist jeweils das Erzeugnis der Abbildung $id : x \mapsto x$?

(a) Monoid: Addition $(M, +)$, *Komposition* $(M, \circ)$, *punktweise Multiplikation* $(M, \cdot)$; $\mathbb{R}$-*Modul: Addition* $(M, +, (\mathbb{R}, +, \cdot))$; $\mathbb{R}$-*Algebra:* $(M, +, \circ)$ *oder* $(M, +, \cdot)$

(b)

Struktur	$\langle id \rangle$
$(M, +)$	$\{id, 2id, 3id, \dots\}$
$(M, \circ)$	$\{id\}$
$(M, \cdot)$	$\{x, x^2, x^3, \dots\}$ *(enthält nicht die 1)*
$(M, +, (\mathbb{R}, +, \cdot))$	$\mathbb{R} \cdot id$
$(M, +, \circ)$	$\mathbb{R} \cdot id$
$(M, +, \cdot)$	$\mathbb{R}[x, x^2, x^3, \dots]$ *(als Polynomfunktionen)*

G 3 (Erzeugende und Relationen)

(a) Die Gruppe G werde von zwei Elementen $a, b \in G$ erzeugt, welche die folgenden Gleichungen erfüllen: $a^4 = b^2 = 1$ und $ab = ba^3$. Zeigen Sie, dass sich jedes Element von G schreiben lässt in der Form $a^i b^j$ mit $i \in \{0, 1, 2, 3\}$ und $j \in \{0, 1\}$. Wieviele Elemente hat G mindestens, wieviele höchstens?

(b) Es ist zu zeigen, dass die Matrizen

$$a = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \text{ und } b = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

die Relationen aus (a) erfüllen. Wieviele Elemente hat die von ihnen erzeugte Untergruppe $D_4 := \langle a, b \rangle \subseteq GL_2(\mathbb{R})$? Welche geometrische Bedeutung hat dieses Ergebnis?

(a) Wir zeigen zunächst, dass $ba = baa^4a^4 = ba^3a^2a^4 = aba^2a^4 = aba^3a^3 = aaba^3 = a^3b$. *Damit lässt sich jeder Ausdruck in die angegeben Reihenfolge umordnen. Die Bedingungen an* i *und* j *sind klar nach Vorr.; höchstens* 8, *mindestens* 1.

(b) $\#D_4 = 8$*; Die Diedergruppe ist die Isometriegruppe des Quadrats.* a *entspricht einer Drehung um* $90°$ *nach rechts* $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} cos\frac{\pi}{2} & -sin\frac{\pi}{2} \\ sin\frac{\pi}{2} & cos\frac{\pi}{2} \end{pmatrix}$ *und* b *einer Spiegelung.*

G 4 (Relativistische Addition von Geschwindigkeiten)

Sei $(-1, 1)$ das offene Intervall zwischen -1 und 1. Wir definieren eine Abbildung $* : (-1, 1) \times (-1, 1) \to (-1, 1)$ durch $r * s = \frac{r+s}{1+rs}$ für $r, s \in (-1, 1)$ unter Benutzung der Addition und Multiplikation in $\mathbb{R}$. Ist $((-1, 1), *, 0)$ eine Gruppe?

Ja. Das neutrale Element ist die 0, Inverses zu s *ist* $-s$*. Assoziativität ist auch schnell gezeigt. Wir müssen nun noch zeigen, dass der Quotient betragsmäßig immer* < 1 *ist:* $-1 < \frac{r+s}{1+rs} < 1$ *g.d.w.*

$$-(1 + rs) < r + s < 1 + rs \Leftrightarrow -(r + 1)(s + 1) < 0 < (r - 1)(s - 1),$$

was offensichtlich ist.

Hausübung

H 1 (Erzeuger der speziellen linearen Gruppe)

Sei $\mathbb{k}$ ein Körper. Zeige, dass die Gruppe $SL_n(\mathbb{k})$ der $n \times n$-Matrizen mit Determinante 1 von den elementaren Scherungsmatrizen $E + rE_{ij}$ $(i \neq j)$ erzeugt wird. Dabei ist E_{ij} die Matrix mit 1 an der Position (i, j) und 0 sonst.
Hinweis: Stellen Sie zuerst folgende Matrizen als Produkte von Scherungsmatrizen dar:

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \qquad \begin{pmatrix} r & 0 \\ 0 & r^{-1} \end{pmatrix}$$

und benutzen Sie den Gauß-Algorithmus.

(1) $\begin{pmatrix} 0 & -r^{-1} \\ r & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ r & 1 \end{pmatrix} \begin{pmatrix} 1 & -r^{-1} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ r & 1 \end{pmatrix}$*; damit haben wir für* $r = 1$ *auch* $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ *und* $\begin{pmatrix} r & 0 \\ 0 & r^{-1} \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & r^{-1} \\ -r & 0 \end{pmatrix}$.

(2) Die Multipliktionen einer Matrix in $GL_n(\mathbb{k})$ *mit den Matrizen* $E + rE_{ij}$ *(von links),*

$$E + E_{ij} + E_{ji} - E_{ii} - E_{jj} = \begin{pmatrix} 1 & & & & & & 0 \\ & \ddots & & & & & \\ & & 0 & & 1 & & \\ & & & \ddots & & & \\ & & 1 & & 0 & & \\ & & & & & \ddots & \\ 0 & & & & & & 1 \end{pmatrix}$$

und

$$E + (r-1)\,E_{ii} = \begin{pmatrix} 1 & & & & & & 0 \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & r & & & \\ & & & & 1 & & \\ & & & & & \ddots & \\ 0 & & & & & & 1 \end{pmatrix}$$

entsprechen den elementaren Zeilenumformungen "Addition des Vielfachen der j-ten Zeile zur i-ten", "Vertauschen der j-ten Zeile mit der i-ten" und "Multiplikation der i-ten Zeile mit einem Skalar". Durch suksessive Anwendung dieser Operationen lässt sich gemäß dem Gauß-Algorithmus jede Matrix in Eins-Dreiecks-Gestalt bringen und weiter in E überführen. Analog zu (1) zeigt man, dass sich die Matrizen $E+E_{ij}-E_{ji}-E_{ii}-E_{jj}$ *und* $E + (r-1)\,E_{ii} + \left(r^{-1} - 1\right) E_{jj}$ *aus den elementaren Scherungsmatrizen erzeugen lassen. Jede Matrix in* $SL_n(\mathbb{k})$ *lässt sich durch suksessive Multiplikation mit Matrizen vom Typ* $E + E_{ij} - E_{ji} - E_{ii} - E_{jj}$ *und* $E + rE_{ij}$ *in Diagonalgestalt bringen und dann durch Multiplikation mit Matrizen* $E + (r-1)\,E_{ii} + \left(r^{-1} - 1\right) E_{jj}$ *in die Einheitsmatrix E überführen, wobei die Determinante offensichtlich erhalten bleibt. q.e.d.*

H 2 (Kleine Gruppen und Körper)

- Bestimmen Sie bis auf Isomorphie alle Gruppen mit genau drei bzw. vier Elementen.

- Bestimmen Sie einen Körper mit vier Elementen. (*Hinweis:* Es gibt kein Element der Ordnung vier.)
- *Zusatz:* Zeigen Sie, dass es keinen weiteren Körper mit genau vier Elementen gibt.

- *Die zyklische Gruppe der Ordnung 3, C_3:*

$\cdot$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

.

Die zyklische Gruppe der Ordnung 4, C_4:

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	b	c	e
b	b	c	e	a
c	c	e	a	b

und die kleinsche Vierergruppe $D_2 \cong C_2 \times C_2$:

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

- *Wir müssen nur auf C_3 eine Addition definieren und ein additives Neutralelement ergänzen. Die Addition ist gegeben durch*

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

- *Nehmen wir an, $C_3 \cup \{0\}$ wäre bzgl. der Addition isomorph zu C_4:*

$+$	0	1	a	b
0	0	1	a	b
1	1	a	b	0
a	a	b	0	1
b	b	0	1	a

Dann würde gelten: $b + 1 = 0$ und somit $0 = b(b + 1) = a + b$, Widerspruch.

H 3 (Einheiten in Monoiden)

Sei M ein endlicher Monoid.

(a) Besitzt jedes Element $a \in M$, das ein Linksinverses hat (für das also ein $b \in M$ existiert mit $ba = 1$) auch ein Rechtsinverses?

(b) Sei $a \in M$ ein Element, das ein Links- und ein Rechtsinverses besitzt. Zeigen Sie, dass es genau ein $b \in M$ mit $ab = 1 = ba$ gibt.

(c) Zeigen Sie, dass die Menge aller $a \in M$, die Links- und Rechtsinverses besitzen, ein Untermonoid und eine Gruppe ist.

(d) *Zusatz:* Geben Sie ein Beispiel eines Monoids M, in dem für $a \in M$ ein Linksinverses jedoch kein Rechtsinverses existiert.

(a) Sei $\#M = n$. Der Fall $n = 1$ ist trivial. Sei also $n > 1$. Dann können wir $a, b \in M$, jeweils nichttrivial, so wählen, dass $ba = 1$. Nehmen wir an, a habe kein Rechtsinverses, also $ac \neq 1$ für alle $c \in M$. Das sind n Ausdrücke der Form ac_i, die jeweils einen der $n-1$ Werte aus $M \setminus \{1\}$ annehmen. Also kommt ein Wert mindestens zweimal vor (Dirichlet's Schubfachprinzip). Damit existieren $c_1 \neq c_2$ mit $ac_1 = ac_2 \Rightarrow c_1 = bac_1 = bac_2 = c_2$, Widerspruch.

(b) Seien $a \in M$ und $b, c \in M$ (Existenz nach Vorraussetzung), sodass $ab = 1 = ca$. Dann ist $c = c \cdot 1 = c\,(ab) = (ca)\,b = 1 \cdot b = b$.

(c) Es genügt zu zeigen, dass die Verknüpfung wohldefiniert ist: Seien $a, b \in M$ und $a^{-1}, b^{-1} \in M$ die (nach (b) eindeutigen) Inversen. Dann ist $1 = b^{-1}a^{-1}ab = g\,(ab)$ und damit das Inverse zu ab (eindeutig wg. (b)) durch $g = b^{-1}a^{-1}$ gegeben.

(d) Sei $a = S_R$ der Rechts-Shift-Operator auf einem Folgenraum. $S_R\,(a_1, a_2, \dots) = (0, a_1, a_2, \dots)$ und $b = S_L$ der entsprechende Links-Shift-Operator. Dann gilt $ba = id \neq ab$. Allgemein gilt: Ein Operator auf einem linearen hat genau dann keine rechtsinverse Abbildung, wenn er nicht surjektiv ist (siehe z.B. Heuser, Funktionalanalysis).

H 4 (Endlich erzeugte Moduln)

Sei $\Bbbk$ ein Körper, $A \in \Bbbk^{n\times n}$. Mit $\Bbbk\,[A]$ bezeichnen wir die von A erzeugte $\Bbbk$-Unteralgebra von $\Bbbk^{n\times n}$. Sei m minimal, sodass es $r_i \in \Bbbk$ gibt mit $A^m = r_0E + r_1A + \cdots + r_{m-1}A^{m-1}$. Zeigen Sie:

(a) $E, A, \dots, A^{m-1}$ ist eine Basis des $\Bbbk$-Vektorraums $\Bbbk\,[A]$.

(b) $V = \Bbbk^n$ ist auf genau eine Art ein $\Bbbk\,[A]$-Modul, sodass Av für $v \in V$ wie üblich definiert ist.

(c) Ist $A = \begin{pmatrix} 0 & & & & -a_0 \\ 1 & 0 & & & -a_1 \\ & \ddots & \ddots & & \vdots \\ & & & 0 & -a_{n-2} \\ & & & 1 & -a_{n-1} \end{pmatrix}$, so wird V als $\Bbbk\,[A]$-Modul von $e_1 = (1, 0, \dots, 0)^t$ erzeugt und es gilt $m = n$.

(a) Wir wissen

$$\Bbbk[A] = \{\sum_{i=0}^{k} s_i A^i \mid k \in \mathbb{N},\ s_i \in \Bbbk\}$$

Es gilt das bekannte Lemma: Sind die Vektoren $v_1, \dots, v_m$ unabhänging, so $v_{m+1} \in \mathsf{Spann}\{v_1, \dots, v_m\}$ genau dann, wenn $v_1, \dots, v_{m+1}$ linear abhängig sind. Es folgt nach Wahl von m mit Induktion, dass $E, A, \dots, A^k$ für $k < m$ linear unabhängig sind. Andererseits ist $A^k \in \mathsf{Spann}\{A^0, \dots, A^{m-1}\}$ für $k \geq m$, was durch Induktion über k gezeigt wird:

$$A^{k+1} = AA^k = A\sum_{i=0}^{m-1} s_i A^i = \sum_{i=0}^{m-1} s_i A^{i+1} = \sum_{i=1}^{m-1} s_{i-1} A^i + \sum_{i=0}^{m-1} s_{m-1} r_i A^i$$

(b) *Sind rv und Av wie üblich definiert, so muss, um einen $\Bbbk[A]$-Modul zu definieren, gelten:*

$$(\sum_{i=0}^{m} s_i A^i)v = (\sum_{i=0}^{m} s_i A^i v).$$

Damit ist $s_i A^i v$ eindeutig bestimmt. Dass V somit auch ein $\Bbbk[A]$-Modul ist, liegt daran, dass $\Bbbk[A]$ eine Unteralgebra von $\Bbbk^{n\times n}$ ist und $\Bbbk^n$ ein $\Bbbk^{n\times n}$-Modul auf bekannte Weise.

(c) *es ist a_{n-2} statt a_{n-1} und a_{n-1} statt a_n zu lesen. Für die kanonische Basis haben wir $Ae_i = e_{i+1} = A^i e_1$ für $i < n$ also wird V von e_1 erzeugt. Wir haben*

$$A^n e_1 = Ae_n = -\sum_{i=1}^{n} a_{i-1} e_i = \sum_{i=0}^{n-1} -a_i A^i e_1$$

und es folgt für $k = 1, \ldots, n$

$$A^n e_k = A^n A^{k-1} e_1 = A^{k-1} A^n e_1 = A^{k-1} \sum_{i=0}^{n-1} -a_i A^i e_1 = \sum_{i=0}^{n-1} -a_i A^i A^{k-1} e_1 = \sum_{i=0}^{n-1} -a_i A^i e_k$$

also

$$A^n = \sum_{i=0}^{n-1} -a_i A^i$$

Hätte man $A^m = \sum_{i=0}^{m-1} r_i A^i$ mit $m < n$, so

$$e_{m+1} = A^m e_1 = \sum_{i=0}^{m-1} r_i A^i e_1 = \sum_{i=1}^{m} r_{i-1} e_i$$

ein Widerspruch. Also $m = n$.

(d) *Aus $A^m = \sum_{i=0}^{m-1} r_i A^i$ folgt*

$$-r_0 E = (\sum_{i=1}^{m-1} r_i A^i) - A^m = A((\sum_{i=1}^{m-1} r_i A^{i-1}) - A^{m-1})$$

Ds die $A_1, \ldots, A^m$ als Bild der Basis von $\Bbbk[A]$ unter der invertierbaren linearen Abbildung $X \mapsto AX$ unabhängig sind, gilt $r_0 \neq 0$ und

$$A^{-1} = -\frac{1}{r_0}((\sum_{i=1}^{m-1} r_i A^{i-1}) - A^{m-1}) \in \Bbbk[A]$$

Abgabe der Hausübungen: Am 27./28. April und 4./5. Mai 2010 zu Beginn der Übung.