Lineare Algebra

für Informatiker [MA 0901]

Übungsblatt 3

Tutorium

T3.1 *Sudoku für Mathematiker.* Es sei $G \doteq \{a, b, c, x, y, z\}$ eine sechselementige Menge mit einer inneren Verknüpfung $\cdot : G \times G \to G$. Vervollständigen Sie die untenstehende Multiplikationstafel unter der Annahme, dass $(G, \cdot)$ eine Gruppe ist.

$\cdot$	a	b	c	x	y	z
a	x	z	y	a	c	b
b	y	x	z	b	a	c
c	z	y	x	c	b	a
x	a	b	c	x	y	z
y	b	c	a	y	z	x
z	c	a	b	z	x	y

T3.2 Im Folgenden sind vier multiplikative Gruppen gegeben, die wir jeweils mit G bezeichnen. Stellen Sie jeweils die Verknüpfungstafel für die Gruppe G auf; dabei sei jeweils e das neutrale Element von G:

(a) $G = \{e, a\}$,

(b) $G = \{e, a, b\}$,

(c) $G = \{e, a, b, c\}$ mit $a^2 = b$,

(d) $G = \{e, a, b, c\}$ mit $a^2 = b^2 = c^2 = e$.

T3.3 Zeigen Sie für reelle $n \times n$-Matrizen, $n \in \mathbb{N}$: Die Menge $\mathrm{O}(n) = \{A \in \mathbb{R}^{n\times n} \mid A\,A^\top = E_n\}$ der sogenannten *orthogonalen* $n \times n$-Matrizen bildet eine Untergruppe von $\mathrm{GL}(n) := (\mathbb{R}^{n\times n})^\times$.

T3.4 Es sei G eine Gruppe, deren Elemente sämtlich eine Ordnung ≤ 2 haben. Man zeige, dass G abelsch ist.

T3.5 Es sei $\varepsilon = \cos(\frac{2\pi}{6}) + \mathrm{i}\,\sin(\frac{2\pi}{6}) \in \mathbb{C}$ eine 6-te Einheitswurzel (d. h. eine 6-te Wurzel aus 1).

(a) Zeigen Sie, dass $G = \{1, \varepsilon, \varepsilon^2, \ldots, \varepsilon^5\}$ mit der Multiplikation $\cdot$ komplexer Zahlen eine Gruppe ist.

(b) Geben Sie, soweit möglich, zu jedem $k \in \{1, \ldots, 6\}$ eine Untergruppe U_k von G an mit $|U_k| = k$.

T3.6 Es sei R ein Ring mit der Eigenschaft $a^2 = a$ für alle $a \in R$. Beweisen Sie:

(a) In R gilt $a + a = 0$ für alle $a \in R$.

(b) R ist kommutativ.

Zusätzliche Übungen

Z3.1 Beweisen Sie den Satz von Euler erneut für endliche abelsche Gruppen G. Berechnen Sie dazu für ein beliebiges $a \in G$ zum einen $\prod_{x \in G} x$ und zum anderen $\prod_{x \in G}(a\,x)$.

Z3.2 Welche Ordnungen haben die Elemente $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$ und $A\,B$ aus $\mathrm{GL}_2(\mathbb{R})$?

Z3.3 Man zeige: In $\mathbb{Z}/n$ ist jedes Element $\neq 0$ entweder ein Nullteiler oder invertierbar. Dabei heißt ein Element $a \neq 0$ **Nullteiler**, falls es ein $b \neq 0$ gibt, sodass $a\,b = 0$ gilt.

Lineare Algebra

für Informatiker [MA 0901]

Übungsblatt 3

Tutorium

T3.1 *Sudoku für Mathematiker.* Es sei $G = \{a, b, c, x, y, z\}$ eine sechselementige Menge mit einer inneren Verknüpfung $\cdot : G \times G \to G$. Vervollständigen Sie die untenstehende Multiplikationstafel unter der Annahme, dass $(G, \cdot)$ eine Gruppe ist.

$\cdot$	a	b	c	x	y	z
a					c	b
b			z			
c		y				
x						
y						
z		a				

Lösung T3.1: Um die unvollständige Gruppentafel zu vervollständigen, können folgende Argumente genutzt werden:

(1) In der vierten Spalte und vierten Zeile steht der Eintrag $x^2 = x$. Daraus folgt, dass x das neutrale Element der Gruppe sein muss. Damit sind bereits alle Eintragungen der vierten Spalte und der vierten Zeile eindeutig festgelegt.

(2) Die in der Gruppentafel angegebenen Gleichungen $ay = c$, $az = b$, $b^2 = x$, usw. sowie die jeweils beim Ausfüllen neu dazukommenden Gleichungen, können (und müssen) verwendet werden.

(3) In jeder Zeile und in jeder Spalte kann jedes Element der Gruppe nur genau einmal vorkommen. Sind also in einer Zeile oder Spalte 5 der 6 Eintragungen bekannt, ist der sechste Eintrag bereits eindeutig bestimmt.

Wir starten mit der gegebenen Gruppentafel und nutzen aus, dass aus $x^2 = x$ folgt, dass x das neutrale Element ist:

	a	b	c	x	y	z
a					c	b
b		x	z			
c		y				
x				x		
y						
z		a			x	

$\longrightarrow$

	a	b	c	x	y	z
a				a	c	b
b		x	z	b		
c		y		c		
x	a	b	c	x	y	z
y				y		
z		a		z	x	

Nun stehen in der zweiten Spalte vier von sechs Einträgen. Es fehlen die Einträge c und z. In der ersten Zeile der zweiten Spalte kann aber das c *nicht* stehen, weil das c in dieser Zeile schon aufgeführt ist. Also muss dort ein z stehen. Wir benutzen dann die beiden Gleichungen $b^2 = x$ und $bc = z$, um den Eintrag

von bz zu bestimmen: $bz = bbc = xc = c$.

	a	b	c	x	y	z
a		z		a	c	b
b		x	z	b		
c		y		c		
x	a	b	c	x	y	z
y		c		y		
z		a		z	x	

$\longrightarrow$

	a	b	c	x	y	z
a		z		a	c	b
b		x	z	b		c
c		y		c		
x	a	b	c	x	y	z
y		c		y		
z		a		z	x	

So wie wir eben die vierte Zeile vervollständigt haben, können wir nun auch die zweite, damit dann die erste Zeile und hiermit schließlich die letzte Zeile vervollständigen (siehe nächste Gruppentafeln). Schließlich erhalten wir aus dieser Tafel dann wiederum

$$c\,a = (b\,z)\,a = b\,(z\,a) = b\,c = z \quad \text{und dann} \quad c\,z = c\,(a\,b) = (c\,a)\,b = z\,b = a\,.$$

Durch weiteres Anwenden der oben aufgeführten Regeln bekommen wir die komplette Gruppentafel:

	a	b	c	x	y	z
a	x	z	y	a	c	b
b	y	x	z	b	a	c
c		y		c		
x	a	b	c	x	y	z
y		c		y		
z	c	a	b	z	x	y

$\longrightarrow$

	a	b	c	x	y	z
a	x	z	y	a	c	b
b	y	x	z	b	a	c
c	z	y	x	c	b	a
x	a	b	c	x	y	z
y	b	c	a	y	z	x
z	c	a	b	z	x	y

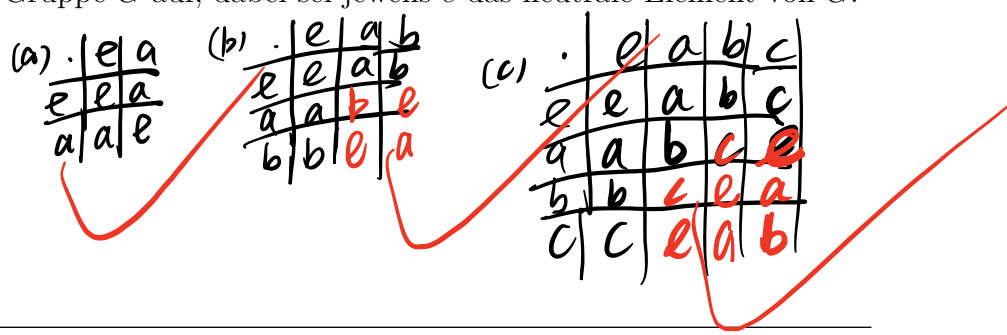
T3.2 Im Folgenden sind vier multiplikative Gruppen gegeben, die wir jeweils mit G bezeichnen. Stellen Sie jeweils die Verknüpfungstafel für die Gruppe G auf; dabei sei jeweils e das neutrale Element von G:

(a) $G = \{e, a\}$,

(b) $G = \{e, a, b\}$,

(c) $G = \{e, a, b, c\}$ mit $a^2 = b$,

(d) $G = \{e, a, b, c\}$ mit $a^2 = b^2 = c^2 = e$.



Lösung T3.2: Wir begründen vorab, dass in jeder Zeile der Verknüpfungstafel einer Gruppe jedes Element der Gruppe genau einmal auftaucht. Dazu betrachten wir die Zeile zu einem Element x:

- Jedes Element kommt höchstens einmal vor: Aus $xa_1 = xa_2$ folgt nämlich $a_1 = a_2$.
- Jedes Element kommt mindestens einmal vor: Man findet y als $x\,(x^{-1}y)$.

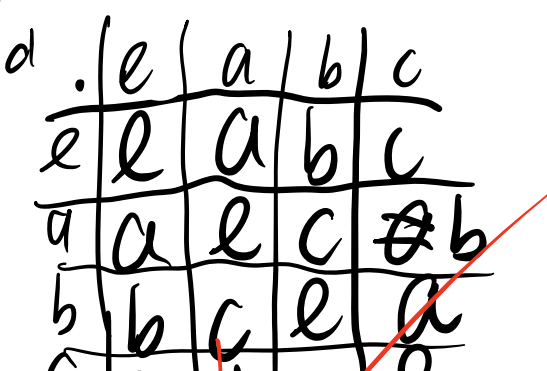
Man begründet analog, dass in jeder Spalte der Verknüpfungstafel einer Gruppe jedes Element der Gruppe genau einmal auftaucht.

(a) Besteht G aus zwei Elementen, so ist die Verknüpfungstafel festgelegt, sie lautet:

$\cdot$	e	a
e	e	a
a	a	

$\longrightarrow$

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



(b) Besteht G aus drei Elementen, so ist erneut die Verknüpfungstafel festgelegt: Es muss $b\,a = e$ gelten, die restlichen Einträge sind dann leicht zu vervollständigen:

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

$\longrightarrow$

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

(c) Besteht G aus vier Elementen, so ist die Verknüpfungstafel hierdurch noch nicht festgelegt. Erst die zusätzliche Bedingung $a^2 = b$ legt diese fest. Man beachte, dass $a\,b = c$ gelten muss, $a\,b = e$ würde zu zwei c in der letzten Spalte führen. Damit liegt die zweite Zeile fest. Nun muss $b\,a = c$ gelten, da aus $b\,a = e$ folgen würde, dass auch $a\,b = e$ gilt. So fortfahrend erhält man:

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

$\longrightarrow$

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

(d) Das ist die sogenannte Kleinsche Vierergruppe:

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

$\longrightarrow$

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

Bemerkung. Man beachte, dass durch eine solche Konstruktion einer Gruppentafel nicht gewährleistet ist, dass die zugrundeliegende Menge mit dieser Verknüpfung $\cdot$ auch eine Gruppe ist, sprich, dass alle Axiome einer Gruppe erfüllt sind. Insbesondere der Nachweis des Assoziativitätsgesetzes ist meist problematisch.

T3.3 Zeigen Sie für reelle $n \times n$-Matrizen, $n \in \mathbb{N}$: Die Menge $\mathrm{O}(n) = \{A \in \mathbb{R}^{n\times n} \mid A\,A^\top = E_n\}$ der sogenannten *orthogonalen* $n \times n$-Matrizen bildet eine Untergruppe von $\mathrm{GL}(n) := (\mathbb{R}^{n\times n})^\times$.

Lösung T3.3: Da $E_n \in \mathrm{O}(n)$, ist $\mathrm{O}(n)$ nicht leer. Jedes $A \in \mathrm{O}(n)$ ist invertierbar, es gilt $A^\top = A^{-1}$, sodass $A \in \mathrm{GL}(n)$. Damit gilt $\mathrm{O}(n) \subseteq \mathrm{GL}(n)$. Sind A, $B \in \mathrm{O}(n)$, so gilt

$$A\,B\,(A\,B)^\top = A\,B\,B^\top A^\top = E_n\,,$$

sodass $A\,B \in \mathrm{O}(n)$. Schließlich gilt für $A \in \mathrm{O}(n)$ wegen $A^\top = A^{-1}$ auch $A^{-1}(A^{-1})^\top = A^\top (A^\top)^\top = A^\top A = E_n$, sodass $A^{-1} \in \mathrm{O}(n)$.

T3.4 Es sei G eine Gruppe, deren Elemente sämtlich eine Ordnung ≤ 2 haben. Man zeige, dass G abelsch ist.

Lösung T3.4: Es seien a, $b \in G$. Aus $a^2 = e_G = b^2$ und $(a\,b)^2 = e_G$ folgt

$$a\,a\,b\,b = a^2 b^2 = (a\,b)^2 = a\,b\,a\,b\,,$$

nach Kürzen von a und b also $a\,b = b\,a$.

T3.5 Es sei $\varepsilon = \cos(\frac{2\pi}{6}) + \mathrm{i}\,\sin(\frac{2\pi}{6}) \in \mathbb{C}$ eine 6-te Einheitswurzel (d. h. eine 6-te Wurzel aus 1).

(a) Zeigen Sie, dass $G = \{1, \varepsilon, \varepsilon^2, \ldots, \varepsilon^5\}$ mit der Multiplikation $\cdot$ komplexer Zahlen eine Gruppe ist.

(b) Geben Sie, soweit möglich, zu jedem $k \in \{1, \ldots, 6\}$ eine Untergruppe U_k von G an mit $|U_k| = k$.

Lösung T3.5: (a) Wegen $o(\varepsilon) = 6$ gilt $G = \langle\varepsilon\rangle$; und da die von Elementen einer Gruppe (nämlich von $(\mathbb{C}, \cdot)$) erzeugten Untergruppen insbesondere Untergruppen und als solche Gruppen sind, ist $(G, \cdot)$ eine Gruppe.

(b) Nach dem Satz von Lagrange kommen nur Untergruppen der Ordnungen 1, 2, 3, 6 infrage, da dies die einzigen Teilen von $6 = |G|$ sind.

Die Untergruppen von der Ordnung 1 und 6 sind klar, es sind dies $U_1 = \{1\}$ und $U_6 = G$.

Eine Untergruppe von der Ordnung 2 kann man erraten: $U_2 = \{1, \varepsilon^3\}$, da $\varepsilon^3 \cdot \varepsilon^3 = 1$; übrigens ist $U_2 = \langle\varepsilon^3\rangle$.

Eine Untergruppe von der Ordnung 3 findet man ähnlich: $U_3 = \{1, \varepsilon^2, \varepsilon^4\}$; hier ist $U_3 = \langle\varepsilon^2\rangle$.

Mit etwas Mühe kann man zeigen, dass es neben U_2 bzw. U_3 keine weiteren Untergruppen in G von der Ordnung 2 bzw. 3 gibt – aber das wurde nicht verlangt.

T3.6 Es sei R ein Ring mit der Eigenschaft $a^2 = a$ für alle $a \in R$. Beweisen Sie:

(a) In R gilt $a + a = 0$ für alle $a \in R$.

(b) R ist kommutativ.

(a) $a+a = (a+a)^2 = a^2+a^2+a^2+a^2 = a+a+a+a$

$\Rightarrow a+a = 0.$

(b) $\forall a,b: (a+b)^2 = a+b$

$\Rightarrow a^2 + a\cdot b + b\cdot a + b^2 = a+b$

$a + a\cdot b + b\cdot a + b = a+b$

$\Rightarrow a\cdot b = -a\cdot b = b\cdot a$ (a)

Zusätzliche Übungen

Z3.1 Beweisen Sie den Satz von Euler erneut für endliche abelsche Gruppen G. Berechnen Sie dazu für ein beliebiges $a \in G$ zum einen $\prod_{x\in G} x$ und zum anderen $\prod_{x\in G}(a\,x)$.

Lösung Z3.1: Für jedes Element $a \in G$ gilt $G = \{a\,x \mid x \in G\}$, da $\lambda_a : G \to G$, $x \mapsto a\,x$ eine Bijektion ist. Da G abelsch ist, gilt mit $n = |G|$:

$$a^n \prod_{x\in G} x = \prod_{x\in G} (a\,x) = \prod_{x\in G} x\,,$$

nach Kürzen von $\prod_{x\in G} x$ also $a^n = e_G$. Damit ist der Satz von Euler für abelsche Gruppen bereits bewiesen.

Z3.2 Welche Ordnungen haben die Elemente $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$ und $A\,B$ aus $\mathrm{GL}_2(\mathbb{R})$?

Lösung Z3.2: Wegen $A^2 = \left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, $A^3 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ und $A^4 = E_2$ hat A die Ordnung 4.

Wegen $B^2 = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$ und $B^3 = E_2$ hat B die Ordnung 3.

Wegen $A\,B = \begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix}$, $(A\,B)^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$, $\ldots$, $(A\,B)^{2n} = \begin{pmatrix} 1 & 2n \\ 0 & 1 \end{pmatrix}$ gilt $o\,(A\,B) = \infty$.

Z3.3 Man zeige: In $\mathbb{Z}/n$ ist jedes Element $\neq 0$ entweder ein Nullteiler oder invertierbar. Dabei heißt ein Element $a \neq 0$ **Nullteiler**, falls es ein $b \neq 0$ gibt, sodass $a\,b = 0$ gilt.

Lösung Z3.3: Wir wissen, dass die invertierbaren Elemente in $\mathbb{Z}/n$ genau jene $\overline{k}$ sind mit $\mathrm{ggT}(k, n) = 1$. Ist nun $\overline{k} \neq \overline{0}$ nicht invertierbar, so ist $d = \mathrm{ggT}(k, n) \neq 1$. Zu zeigen ist nun, dass ein Element $\overline{0} \neq \overline{l} \in \mathbb{Z}/n$ existiert mit $\overline{k}\,\overline{l} = \overline{0}$; anders ausgedrückt: Gesucht ist ein $l \in \{1, \ldots, n-1\}$ mit $k\,l \in n\,\mathbb{Z}$. Hierfür bietet sich $l := \frac{n}{d}$ an. Es gilt nämlich:

$$\overline{k}\,\overline{\left(\frac{n}{d}\right)} = \overline{\left(\frac{k}{d}\right)}\,\overline{n} = \overline{0}\,,$$

also ist $\overline{k}$ ein Nullteiler. In $\mathbb{Z}/12$ gilt beispielhaft

$$\overline{2}\cdot\overline{6} = \overline{0}\,,\ \overline{3}\cdot\overline{4} = \overline{0}\,,\ \overline{8}\cdot\overline{3} = \overline{0}\,,\ \overline{9}\cdot\overline{4} = \overline{0} \ \text{ bzw. } \ \overline{5}\cdot\overline{5} = \overline{1}\,,\ \overline{7}\cdot\overline{7} = \overline{7} \quad \text{und} \quad \overline{11}\cdot\overline{11} = \overline{1}\,.$$