Universität Augsburg
Institut für Mathematik

Prof. Dr. Katrin Wendland
Dr. Katrin Leschke
WS 2006/2007

Lineare Algebra I, Lösungshinweise zur 1. und 4. Aufgabe

Aufgabe 1 (4 Punkte). Sei $(R, +)$ eine abelsche Gruppe mit neutralem Element 0. Sei $\cdot$ eine weitere Verknüpfung auf R, so dass:

- das Assoziativgesetz für die Verknüpfung $\cdot$ gilt.
- $1 \in R - \{0\}$ existiert mit $1 \cdot x = x \cdot 1 = x$ für alle $x \in R$.
- $x \cdot y = y \cdot x$ für alle $x, y \in R$.
- $x \cdot y = 0$ für $x, y \in R$ impliziert, dass $x = 0$ oder $y = 0$ ("Nullteilerfreiheit").
- $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$ für alle $x, y, z \in R$.

Sei außerdem $|R| = n < \infty$.
Zeigen Sie: R ist ein Körper.
(Hinweis: Zeigen Sie zunächst, dass für jedes $x \in R - \{0\}$ gilt: Falls $y_1, y_2 \in R$ und $x \cdot y_1 = x \cdot y_2$ gilt, dann folgt $y_1 = y_2$.)

Nach Voraussetzung sind A1-A4, sowie M1, M2, M4 und D1 erfüllt. D1 und M4 geben D2:

$$(x+y)z \stackrel{M4}{=} z(x+y) \stackrel{D1}{=} zx + zy \stackrel{M4}{=} xz + yz\,.$$

Es bleibt also die Existenz des Inversen zu zeigen.
Sei also $x \in R \setminus \{0\}$ und $\varphi_x : R \to R, y \mapsto x \cdot y$. Dann ist φ_x eine injektive Abbildung, da

$$\begin{aligned} \varphi_x(y_1) = \varphi_x(y_2) \quad &\Longrightarrow \quad xy_1 = xy_2 \implies xy_1 - xy_2 = 0 \stackrel{D1}{\Longrightarrow} x(y_1 - y_2) = 0 \\ &\stackrel{\text{nullteilerfrei}}{\Longrightarrow} \quad x = 0 \text{ oder } y_1 - y_2 = 0 \stackrel{x \in R\setminus\{0\}}{\Longrightarrow} y_1 - y_2 = 0 \implies y_1 = y_2\,. \end{aligned}$$

Eine injektive Abbildung einer endlichen Menge auf sich selbst ist auch surjektiv. Da $|R| = n < \infty$ und $\varphi_x : R \to R$ injektiv, ist also φ_x surjektiv. Das heißt, für alle $z \in R$ existiert ein $y \in R$ mit $\varphi_x(y) = z$. Dies gilt insbesondere für $z = 1 \in R$, also existiert $y \in R$ mit

$$1 = \varphi_x(y) = xy\,.$$

Damit ist $y \in R \setminus \{0\}$ das Inverse von $x \in R \setminus \{0\}$ ($y \neq 0$, da sonst $y \cdot x = 0 \cdot x = 0 \neq 1$).
Also gilt auch M3, und $(R, +, \cdot)$ ist ein Körper.

Aufgabe 4 (4 Punkte). Es sei K ein Körper, G die von 1 erzeugte Untergruppe der additiven Gruppe $(K, +)$ und $Q = \{ab^{-1} \mid a, b \in G, b \neq 0\}$.
Zeigen Sie:

- Q ist ein Unterkörper von K.
- Q ist der kleinste Unterkörper von K,

Vorbemerkungen:

- Falls $K = \mathbb{Z}/p\mathbb{Z}$, p prim, dann ist $\mathbb{Z} \neq G \subset K$.

- Und: K ist noch nicht einmal isomorph zu $\mathbb{Z}$ oder einer Teilmenge von $\mathbb{Z}$.
- Aber: für jeden Körper K ist G isomorph zu $\mathbb{Z}$ oder $\mathbb{Z}/m\mathbb{Z}$ (siehe Blatt 3, Aufg. 4).

Zunächst einmal zeigen wir für $x, y \in G$, dass

$$x \cdot y \in G\,. \tag{1}$$

Ohne Einschränkung können wir $x \neq 0$ annehmen, da sonst $x \cdot y = 0 \in G$.
Da $x \in G$ gilt $x = \underbrace{1 + 1 + \ldots + 1}_{m-\text{mal}}$ oder $x = \underbrace{(-1) + (-1) + \ldots + (-1)}_{m-\text{mal}}$ mit $m \in \mathbb{N}$. Wir schreiben kurz:

$$x = m \cdot 1 = m \quad \text{ oder } x = (-m) \cdot 1 = -m\,.$$

(Vorsicht! Das heißt nicht $x \in \mathbb{Z}$, sondern ist nur eine abkürzende Schreibweise!!! - siehe Vorbemerkungen.)
Da G eine Gruppe ist, gilt für alle $g, h \in G$, dass $g + h \in G$ und $(-g) + (-h) \in G$, also auch

$$x \cdot y = \begin{cases} \underbrace{(1 + 1 + \ldots + 1)}_{m-\text{mal}} \cdot y \overset{D2}{=} \underbrace{1 \cdot y + \ldots + 1 \cdot y}_{m-\text{mal}} = \underbrace{y + \ldots + y}_{m-\text{mal}} \in G \\ \underbrace{((-1) + (-1) + \ldots + (-1))}_{m-\text{mal}} \cdot y \overset{D2}{=} \underbrace{(-1) \cdot y + \ldots + (-1) \cdot y}_{m-\text{mal}} = \underbrace{(-y) + \ldots + (-y)}_{m-\text{mal}} \in G \end{cases}$$

Nun zeigen wir, dass Q Unterkörper von K ist.

- $(Q, +)$ **ist abelsche Gruppe. Dafür reicht es zu zeigen, dass Q eine Untergruppe von $(K, +)$ ist:**
  1. $Q \neq \emptyset$, da $1 \in G$ und $1 = 1 \cdot 1 = 1 \cdot 1^{-1} \in Q$.
  2. Q ist abgeschlossen bezüglich der Addition:
     Seien $x, y \in Q$, d.h. es existieren $a, \tilde{a} \in G, b, \tilde{b} \in G^*$ mit $x = ab^{-1}, y = \tilde{a}\tilde{b}^{-1}$. Dann gilt:
     $$x + y = ab^{-1} + \tilde{a}\tilde{b}^{-1} = (ab^{-1})(\tilde{b}\tilde{b}^{-1}) + (\tilde{a}\tilde{b}^{-1})(bb^{-1}) \overset{M1,M4,D2}{=} (a\tilde{b} + \tilde{a}b)(b\tilde{b})^{-1} \in Q,$$
     da $a\tilde{b}, \tilde{a}b, b\tilde{b} \in G$ mit (1), und $b\tilde{b} \neq 0$ (Nullteilerfreiheit in Körpern).
  3. Ist $x \in Q$ so ist auch $-x \in Q$:
     Sei $x = ab^{-1} \in Q$ mit $a, b \in G, b \neq 0$. Dann ist das Inverse von x bezüglich der Addition gegeben durch$(-x) = (-a)b^{-1}$, da
     $$(-x) + x = (-a)b^{-1} + ab^{-1} \overset{D2}{=} (-a + a)b^{-1} = 0b^{-1} = 0\,.$$
     Da G eine Gruppe ist, ist $-a \in G$ und daher $(-x) \in Q$.
- $(Q \setminus \{0\}, \cdot)$ **ist abelsche Gruppe. Dafür reicht es zu zeigen, dass Q eine Untergruppe von $(K \setminus \{0\}, \cdot)$ ist:**
  1. $Q \setminus \{0\} \neq \emptyset$, da $1 \in Q$ (s.o.).
  2. $Q \setminus \{0\}$ ist abgeschlossen bezüglich der Multiplikation:
     Seien $x, y \in Q \setminus \{0\}, x = ab^{-1}, y = \tilde{a}\tilde{b}^{-1}$. Wieder mit (1) erhalten wir:
     $$x \cdot y = (ab^{-1}) \cdot (\tilde{a}\tilde{b}^{-1}) \overset{M1,M4}{=} (a\tilde{a})(b\tilde{b})^{-1} \in Q\,.$$

3. Für $x \in Q \setminus \{0\}$ ist auch $x^{-1} \in Q$:
   Sei $x \in Q \setminus \{0\}$, d.h., $x = ab^{-1}$ mit $a, b \in G, a, b \neq 0$. Dann ist
   $$x^{-1} = (ab^{-1})^{-1} = ba^{-1} \in Q\,.$$

- Distributivgesetze gelten wegen der Distributivgesetze in K. (Nachrechnen!)

Z.z: Q ist kleinster Unterkörper von K.

Sei $\tilde{K}$ ein Unterkörper von K. Zu zeigen: $Q \subset \tilde{K}$.

Da $\tilde{K}$ Unterkörper von K ist, gilt $1 \in \tilde{K}$. Da $(\tilde{K}, +)$ abelsche Gruppe ist, gilt:

$$x \in \tilde{K} \implies (-x) \in \tilde{K} \text{ und } x, y \in \tilde{K} \implies x + y \in \tilde{K}\,.$$

Also ist auch $-1 \in \tilde{K}$ und $m \cdot 1 \in \tilde{K}$ für $m \in \mathbb{Z}$. Insbesondere ist auch $0 \in \tilde{K}$. Also insgesamt:

$$G \subset \tilde{K}\,.$$

Da $(\tilde{K} \setminus \{0\}, \cdot)$ eine abelsche Gruppe ist, gilt:

$$x \in \tilde{K} \implies x^{-1} \in \tilde{K} \text{ und } x, y \in \tilde{K} \implies x \cdot y \in \tilde{K}\,.$$

Somit gilt für $b \in \tilde{K} \setminus \{0\}$ auch $b^{-1} \in \tilde{K} \setminus \{0\}$ und $a, b \in \tilde{K} \setminus \{0\} \implies a \cdot b^{-1} \in \tilde{K} \setminus \{0\}$. Da für $a = 0$ auch $a \cdot b^{-1} = 0 \in \tilde{K}$, gilt damit:

$$a, b \in G \subset \tilde{K}, b \neq 0, \implies ab^{-1} \in \tilde{K}.$$

Da $x \in Q$ sich schreiben läßt als $x = ab^{-1}$ mit $a, b \in G, b \neq 0$, folgt also $x \in \tilde{K}$. Damit ist $Q \subset \tilde{K}$.