Lineare Algebra 1 Hausaufgabenblatt Nr. 4

Jun Wei Tan*

Julius-Maximilians-Universität Würzburg

(Dated: November 10, 2023)

Problem 1. Direktes Produkt

(a) Zeigen Sie: Sind $(G, *, e_G)$ und $(H, \star, e_H)$ Gruppen, dann ist auch $G \times H$ mit der Verknüpfung

$$\odot\, (G \times H) \times (G \times H) \to G \times H, \qquad (g_1, h_1) \odot (g_2, h_2) := (g_1 * g_2, h_1 \star h_2)$$

und dem neutralen Element (e_G, e_H) eine Gruppe. Diese Gruppe nennt man auch das *direktes Produkt* von G und H.

(b) Zeigen Sie: Sind $(R, +, \cdot)$ und $(S, \star, *)$ Ringe, dann ist auch $R \times S$ mit den Verknüpfung $\oplus$ und $\odot$, definiert durch $(r_1, s_1) \oplus (r_2, s_2) := (r_1 + r_2, s_1 \star s_2)$ bzw. $(r_1, s_1) \odot (r_2, s_2) := (r_1 \cdot r_2, s_1 * s_2)$ ein Ring.

(c) Beweisen oder widerlegen Sie: Ist $(K, +, \cdot)$ ein Körper, dann ist auch $K \times K$ mit den Verknüpfungen wie in (b) ein Körper.

Proof. (a) (i) (Assoziativität)

$$\begin{aligned}
(g_1, h_1) \odot ((g_2, h_2) \odot (g_3, h_3)) =& (g_1, h_1) \odot (g_2 * g_3, h_2 \star h_3) \\
=& (g_1 * (g_2 * g_3), h_1 \star (h_2 \star h_3)) \\
=& ((g_1 * g_2) * g_3, (h_1 \star h_2) \star h_3) \\
=& (g_1 * g_2, h_1 \star h_2) \odot (g_3, h_3) \\
=& ((g_1, h_1) \odot (h_1, h_2)) \odot (g_3, h_3)
\end{aligned}$$

(ii) (Neutrales Element)

$$(g_1, h_1) \odot (e_G, e_H) = (g_1, h_1) = (e_G, e_H) \odot (g_1, h_1).$$

* jun-wei.tan@stud-mail.uni-wuerzburg.de

(iii) (Existenz des Inverses) Sei $(g_1, h_1) \in G \times H$. Weil G und H gruppe sind, gibt es elemente $g_1^{-1} \in G, h_1^{-1} \in H$, sodass $g_1 * g_1^{-1} = e_G = g_1^{-1} * g_1$ und $h_1 \star h_1^{-1} = e_H = h_1^{-1} \star h_1$. Es gilt

$$(g_1, h_1) \odot (g_1^{-1}, h_1^{-1}) = (g_1 * g_1^{-1}, h_1 \star h_1^{-1}) = (e_G, e_H),$$

und ähnlich auch $(g_1^{-1}, h_1^{-1}) \odot (g_1, h_1) = (e_G, e_H)$

Schluss: $(G \times H, \odot, (e_G, e_H))$ ist eine Gruppe.

(b) (i) $(R \times S, \oplus, (0_R, 0_S))$ ist eine abelsche Gruppe.

Folgt aus (a).

(ii) $\oplus$ ist assoziativ:

Beweis läuft ähnlich zu (a), die Behauptung folgt aus die Assoziativität von $\cdot$ und $*$.

(iii) Distributivgesetz:

$$\begin{aligned}
(r_1, s_1) \odot ((r_2, s_2) \oplus (r_3, s_3)) =& (r_1, s_1) \odot (r_2 + r_3, s_2 \star s_3) \\
=& (r_1 \cdot (r_2 + r_3), s_1 * (s_2 \star s_3)) \\
=& (r_1 \cdot r_2 + r_1 \cdot r_3, s_1 * s_2 \star s_1 * s_3) \\
=& (r_1 \cdot r_2, s_1 * s_2) \oplus (r_1 \cdot r_3, s_1 * s_3) \\
=& [(r_1, s_1) \odot (r_2, s_2)] \oplus [(r_1, s_1) \odot (r_3, s_3)]
\end{aligned}$$

(c) Falsch. Sei $x, y \in K$ beliebige Elemente von K. Es ist klar, dass $(0, 0)$ das Nullelement ist, weil

$$(x, y) \oplus (0, 0) = (x + 0, y + 0) = (x, y).$$

Sei jetzt $x \neq 0 \neq y$. Es gilt

$$(x, 0) \odot (0, y) = (x \cdot 0, 0 \cdot y) = (0, 0),$$

also es gibt Nullteiler. □

Problem 2. Zeigen Sie: In einem Ring $(R, +, \cdot)$ gilt genau dann die Kürzungsregel

Falls $a \in R \backslash \{0\}$ und $x, y \in R$ beliebig sind, dann gilt $a \cdot x = a \cdot y \implies x = y$

wenn R nullteilerfrei ist.

Proof. 1. R hat Nullteiler $\implies$ die Kürzungsregel gilt nicht.

Per Ausnahme gibt es $x \in R\setminus\{0\}$ mit Nullteiler $a \in R\setminus\{0\}$, also $a \cdot x = 0$. Es gilt auch, dass $a \cdot 0 = 0$, daher

$$a \cdot x = a \cdot 0 = 0.$$

Aber $x \neq 0$, und die Kürzungsregel gilt nicht.

2. R nullteilerfrei $\implies$ Kürzungsregel gilt.

Seien $a \in R\setminus\{0\}$ und $x, y \in R$ beliebig und

$$\begin{aligned} a \cdot x &= a \cdot y \\ a \cdot x + [-(a \cdot y)] &= a \cdot y + [-(a \cdot y)] \\ 0 &= a \cdot x - a \cdot y \\ &= a \cdot (x - y) \end{aligned}$$

Daraus folgt, dass entweder $a = 0$ oder $x - y = 0$. Weil wir schon ausgenommen haben, dass $a \neq 0$, gilt $x - y = 0$, oder $x = y$. □

Problem 3. (Verknüpfungsverträglich) Es seien $(G, \cdot, e_G), (H, *, e_H)$ Gruppen und $\alpha : G \to H$ ein Gruppenhomomorphismus. Zeigen Sie

(a) $U = \{u \in G | \alpha(u) = e_H\}$ ist eine Untergruppe von G.

(b) $\alpha(G)$ ist eine Untergruppe von H.

(c) Durch $a \sim b \iff ab^{-1}$ wird eine eine verknüpfungsverträgliche Äquivalenzrelation auf G definiert.

Proof. (a) (i) Neutrales Element.

$\alpha(e_G) = e_H$, weil, für alle $x \in G$ gilt

$$\alpha(x) = \alpha(x \cdot e_G) = \alpha(x) * \alpha(e_G).$$

(ii) U ist abgeschlossen.

Sei $x, y \in U$, also $\alpha(x) = e_H = \alpha(y)$. Es gilt

$$\alpha(x \cdot y) = \alpha(x) * \alpha(y) = e_H * e_H = e_H$$

also $x \cdot y \in U$.

(iii) Existenz des Inverses

Sei $x \in U$, und $x \cdot x^{-1} = e_G$. Es gilt

$$e_H = \alpha(e_G) = \alpha(x \cdot x^{-1}) = \alpha(x) * \alpha\left(x^{-1}\right) = e_H * \alpha\left(x^{-1}\right) = \alpha\left(x^{-1}\right),$$

also $x^{-1} \in U$.

(b) (a) Neutrales Element

$\alpha(e_G) = e_H$, der Beweis ist schon in (a) geschrieben.

(b) $\alpha(G)$ ist abgeschlossen.

Sei $\alpha(G) \ni y_1 = \alpha(x_1)$ bzw. $\alpha(G) \ni y_2 = \alpha(x_2)$, für $x_1, x_2 \in G$. Es gilt

$$y_1 * y_2 = \alpha(x_1) * \alpha(x_2) = \alpha(x_1 \cdot x_2) \in \alpha(G).$$

(c) Existenz des Inverses

Sei $\alpha(G) \ni y = \alpha(x)$. Sei auch $x^{-1} \in G$, sodass $x \cdot x^{-1} = e_G = x^{-1} \cdot x$. Es gilt

$$y * \alpha(x^{-1}) = \alpha(x) * \alpha(x^{-1}) = \alpha(x \cdot x^{-1}) = \alpha(e_G) = e_H,$$

also $\exists \alpha(x^{-1}) \in \alpha(G)$, für die gilt $y * \alpha(x^{-1}) = e_H = \alpha(x^{-1}) * y$.

(c) In (i) - (iii) beweisen wir, dass es eine Äquivalenzrelation ist. Dann beweisen wir, dass sie verknüpfungsverträglich ist. Sei im Beweis $x, y, z, w \in G$ beliebige Elemente.

(i) (Reflexivität) $x \sim x$, weil $x \cdot x^{-1} = e_G \in U$.

(ii) (Symmetrie) Sei $x \sim y$, also $xy^{-1} \in U$. Es gilt dann, $(xy^{-1})^{-1} = yx^{-1}$. Weil U eine Gruppe ist, gilt $(xy^{-1})^{-1} \in U$, also $yx^{-1} \in U$. Daraus folgt $y \sim x$.

(iii) (Transitivität) Sei $x \sim y$ und $y \sim z$, also $x \cdot y^{-1} \in U$ und $y \cdot z^{-1} \in U$. Es folgt

$$x \cdot z^{-1} = \underbrace{x \cdot y^{-1}}_{\in U} \cdot \underbrace{y \cdot z^{-1}}_{\in U} \in U,$$

also $x \sim z$.

(iv) Sei $x \sim y$ und $z \sim w$, also $x \cdot y^{-1} \in U$ und $z \cdot w^{-1} \in U$. Wir möchten zeigen, dass $x \cdot z \sim y \cdot w$, also

$$x \cdot z \cdot (y \cdot w)^{-1} = x \cdot z \cdot w^{-1} \cdot y^{-1} \in U.$$

Es gilt

$$\begin{aligned}\alpha(x \cdot z \cdot w^{-1} \cdot y^{-1}) =& \alpha(x) * \alpha(z \cdot w^{-1}) * \alpha(y^{-1}) \\ =& \alpha(x) * e_H * \alpha(y^{-1}) \\ =& \alpha(x \cdot y^{-1}) \\ =& e_H\end{aligned}$$

also $x \cdot z \sim y \cdot w$. □

Problem 4. (Rechnen in verschiedenen Ringen)

(a) Bestimmen Sie das inverse Element von $\overline{6}$ in $\mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/5\mathbb{Z}, \mathbb{Z}/7\mathbb{Z}$ bzw. $\mathbb{Z}/35\mathbb{Z}$ oder weisen Sie nach, dass es nicht existiert.

(b) Bestimmen Sie die Charakteristik von $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ bzw. $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, wobei die beiden Teile des Produktes als Ringe interpretiert werden und die Verknüpfung wie in 1(b) definiert wird.

(c) Bestimmen Sie alle $z \in \mathbb{C}$, die die Gleichung $z^2 + 2$ erfüllen.

(d) Berechnen Sie $(7 + i)(6 - i)^{-1}$ und geben Sie das Ergebnis ale komplexe Zahl gemäß Definition 2.4.14 an.

(e) Bestimmen Sie die Einerstelle von 27^{101}.

Proof. (a) (i) ($\mathbb{Z}/4\mathbb{Z}$) $\overline{6} = \overline{2}$, und es gibt kein inverse Element.

$$\begin{aligned}\overline{2} \cdot \overline{0} &= \overline{0} \\ \overline{2} \cdot \overline{1} &= \overline{2} \\ \overline{2} \cdot \overline{2} = \overline{4} &= \overline{0} \\ \overline{2} \cdot \overline{3} = \overline{6} &= \overline{2}\end{aligned}$$

(ii) ($\mathbb{Z}/5\mathbb{Z}$) $\overline{6} = \overline{1}$. Daher ist $\overline{6} = \overline{6}^{-1}$.

(iii) ($\mathbb{Z}/7\mathbb{Z}$) $\overline{6} \cdot \overline{6} = \overline{36} = \overline{1}$.

(iv) ($\mathbb{Z}/35\mathbb{Z}$) $\overline{6} \cdot \overline{6} = \overline{36} = \overline{1}$.

(b) Im Allgemein ist die Charakteristik von $\mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ das kleinste gemeinsame Vielfaches von a und b. Es gilt $n \cdot 1_{\mathbb{Z}/a\mathbb{Z}} = 1_{\mathbb{Z}/a\mathbb{Z}}$, und auch $n \cdot 1_{\mathbb{Z}/b\mathbb{Z}} = 1_{\mathbb{Z}/b\mathbb{Z}}$. Für $\mathbb{N} \ni n < kgV(a,b)$ kann die beides gleichzeitig per Definition nicht gelten. Die Antworten folgen:

   (i) $(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}))$ 15

   (ii) $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z})$ 6

(c) $z^2 + 2 = 0, z^2 = -2$. Wir haben $|z|^2 = |2|$, und $|z| = \sqrt{2}$. Daraus folgt:

$$z = \pm\sqrt{2}i.$$

(d)

$$\begin{aligned}\frac{7+i}{6-i} =& \frac{(7+i)(6+i)}{(6-i)(6+i)} \\ =& \frac{42+13i-1}{36+1} \\ =& \frac{41+13i}{37} \\ =& \left(\frac{41}{37}, \frac{13}{37}\right)\end{aligned}$$

(e) $27^{101} = (3^3)^{101} = 3^{303}$. Sei a die Einerstells von 3^{303}. Es gilt

$$3^{303} \equiv a \pmod{10}.$$

Wir berechnen

$$\begin{aligned}3^1 = 3 \equiv& 3 \pmod{10} \\ 3^2 = 9 \equiv& 9 \pmod{10} \\ 3^3 = 27 \equiv& 7 \pmod{10} \\ 3^4 \equiv& 1 \pmod{10} \\ 3^5 \equiv& 3 \pmod{10}\end{aligned}$$

Daraus folgt

$$3^{303} = 3^{4\times 75+3}$$

$$\begin{aligned} &\equiv 3^3 \pmod{10} \\ &\equiv 7 \pmod{10} \end{aligned}$$

also die Einerstelle von 27^{101} ist 7. $\square$

Problem 5. Wir können analog zur Konstruktion komplexer Zahlen vorgehen, um aus $\mathbb{Z}/n\mathbb{Z}$ größere Ringe zu konstruieren, d.h. für festes $n \in N$ definieren wir auf $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ die Addition $\oplus$ bzw. Multiplikation $\odot$ durch

$$(a_1, b_2) \oplus (a_2, b_2) := (a_1 + a_2, b_1 + b_2)$$

bzw.

$$(a_1, b_1) \odot (a_2, b_2) := (a_1 a_2 - b_1 b_2, a_1 b_2 + a_2 b_1)$$

für alle $(a_1, b_2), (a_2, b_2) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

Entscheiden Sie, für welche $n \in \{2, 3, 4\}$ mit dieser Konstruktion ein Körper entsteht.

Proof. **($n = 2$)** Es ist kein Körper, weil es nicht nullteilerfrei ist.

$$(\overline{1}, \overline{1}) \odot (\overline{1}, \overline{1}) = (\overline{0}, \overline{2}) = (\overline{0}, \overline{0}).$$

($n = 3$) Es ist ein Körper. Wir wissen, weil 3 ein Primzahl ist, dass $\mathbb{Z}/3\mathbb{Z}$ ein Körper ist. Wir vermuten, dass das inverse Element

$$(a, b)^{-1} = \left(a \left(a^2 + b^2 \right)^{-1}, -b \left(a^2 + b^2 \right)^{-1} \right),$$

was wohldefiniert ist, weil $\mathbb{Z}/3\mathbb{Z}$ ein Körper ist. Wir wissen (und werde benutzen), dass multiplikation in der ganzen Zahlen kommutativ ist. Es folgt

$$\begin{aligned} (a, b) \odot (a, b)^{-1} &= \left(a^2 \left(a^2 + b^2 \right)^{-1} - b^2 \left(a^2 + b^2 \right)^{-1}, 0 \right) \\ &= \left(\left(a^2 + b^2 \right) \left(a^2 + b^2 \right)^{-1}, 1 \right) \\ &= (1, 0), \end{aligned}$$

was das neutrale Element ist (beweis gleich wie der Beweis bzgl. $\mathbb{C}$).

($n = 4$) Es ist noch einmal kein Körper, weil es nicht nullteilerfrei ist.

$$(\overline{2}, \overline{2}) \odot (\overline{2}, \overline{2}) = (\overline{0}, \overline{4} + \overline{4}) = (\overline{0}, \overline{0}).$$ $\square$