Lineare Algebra und Analytische Geometrie 1 **Wintersemester 2016**
http://www.algebra.uni-linz.ac.at/teaching/ws2016/linalg/

Übungsblatt 4

Besprechung am **31.10.2016**

Aufgabe 3 (Kern und Bild) Zeigen Sie, dass $(\mathbb{Z}_{15}, +)$ eine Untergruppe hat, die zu $(\mathbb{Z}_5, +)$ isomorph ist, sowie eine Untergruppe, die zu $(\mathbb{Z}_3, +)$ isomorph ist. Geben Sie dazu einen Homomorphismus $h\colon \mathbb{Z}_{15} \to \mathbb{Z}_{15}$ an mit $\ker h \cong \mathbb{Z}_5$ und $\operatorname{im} h \cong \mathbb{Z}_3$.

Lösung. Betrachte die Funktion $h\colon \mathbb{Z}_{15} \to \mathbb{Z}_{15}$, $h([x]_{\equiv_{15}}) = [5x]_{\equiv_{15}}$. Die Funktion ist wohldefiniert, denn wenn $x \equiv_{15} y$ gilt, gilt $15 \mid x - y$, dann auch $15 \mid 5(x - y)$, also $5x \equiv_{15} 5y$.

Im übrigen handelt es sich bei h um einen Gruppenhomomorphismus, denn für beliebige $x, y \in \mathbb{Z}$ gilt

$$\begin{aligned} h([x]_{\equiv_{15}} + [y]_{\equiv_{15}}) &= h([x + y]_{\equiv_{15}}) = [5(x + y)]_{\equiv_{15}} = [5x + 5y]_{\equiv_{15}} = [5x]_{\equiv_{15}} + [5y]_{\equiv_{15}} \\ &= h([x]_{\equiv_{15}}) + h([y]_{\equiv_{15}}). \end{aligned}$$

Weiters lässt sich nachrechnen, dass $\ker h = \{[0]_{\equiv_{15}}, [3]_{\equiv_{15}}, [6]_{\equiv_{15}}, [9]_{\equiv_{15}}, [12]_{\equiv_{15}}\}$ und $\operatorname{im} h = \{[0]_{\equiv_{15}}, [5]_{\equiv_{15}}, [10]_{\equiv_{15}}\}$ gilt. Nach Satz der Vorlesung handelt es sich bei $\ker h$ und $\operatorname{im} h$ um Untergruppen von $\mathbb{Z}_{15}$.

Wir zeigen jetzt, dass $\ker h$ isomorph zu $\mathbb{Z}_5$ ist. Betrachte dazu die Funktion $f\colon \mathbb{Z}_5 \to \mathbb{Z}_{15}$ mit $f([x]_{\equiv_5}) := [3x]_{\equiv_{15}}$. Wie oben überzeugt man sich, dass f wohldefiniert ist. Ebenfalls zeigt man wie oben, dass f ein Homomorphismus ist. Nachrechnen bestätigt $\ker f = \{[0]_{\equiv_5}\}$ und $\operatorname{im} f = \ker h$. Damit ist f auch bijektiv und also ein Isomorphismus.

Der Beweis, dass $\operatorname{im} h$ isomorph zu $\mathbb{Z}_3$ ist, geht genauso. In diesem Fall kann man die Funktion $f\colon \mathbb{Z}_3 \to \mathbb{Z}_{15}$ mit $f([x]_{\equiv_3}) = [5x]_{\equiv_{15}}$ verwenden.

Aufgabe 5 (Körper) Zeigen Sie, dass die Menge

$$\mathbb{Q}(\sqrt[3]{2}) = \{\, a + b\sqrt[3]{2} + c\sqrt[3]{4} : a, b, c \in \mathbb{Q} \,\} \subseteq \mathbb{R}$$

zusammen mit der üblichen Addition und Multiplikation einen Körper bildet.

Lösung. 1. Addition:

- Assoziativität und Kommutativität übertragen sich unmittelbar von der Addition in $\mathbb{R}$.
- Das Neutralelement $0 = 0 + 0\sqrt[3]{2} + 0\sqrt[3]{4}$ liegt in $\mathbb{Q}(\sqrt[3]{2})$
- Für je zwei Elemente $x_1 = a_1 + b_1\sqrt[3]{2} + c_1\sqrt[3]{4}, x_2 = a_2 + b_2\sqrt[3]{2} + c_2\sqrt[3]{4} \in \mathbb{Q}(\sqrt[3]{2})$ liegt auch die Summe $x_1 + x_2 = (a_1 + a_2) + (b_1 + b_2)\sqrt[3]{2} + (c_1 + c_2)\sqrt[3]{4}$ wieder in $\mathbb{Q}(\sqrt[3]{2})$.
- Für jedes $x = a + b\sqrt[3]{2} + c\sqrt[3]{4} \in \mathbb{Q}(\sqrt[3]{2})$ liegt auch das additive Inverse $-x = (-a) + (-b)\sqrt[3]{2} + (-c)\sqrt[3]{4}$ wieder in $\mathbb{Q}(\sqrt[3]{2})$.

Damit ist gezeigt, dass $(\mathbb{Q}(\sqrt[3]{2}), +)$ eine Untergruppe von $(\mathbb{R}, +)$ ist.

2. Multiplikation:

- Assoziativität und Kommutativität übertragen sich unmittelbar von der Multiplikation in $\mathbb{R}$.
- Das Neutralelement $1 = 1 + 0\sqrt[3]{2} + 0\sqrt[3]{4}$ liegt in $\mathbb{Q}(\sqrt[3]{2}) \setminus \{0\}$
- Für je zwei Elemente $x_1 = a_1 + b_1\sqrt[3]{2} + c_1\sqrt[3]{4}, x_2 = a_2 + b_2\sqrt[3]{2} + c_2\sqrt[3]{4} \in \mathbb{Q}(\sqrt[3]{2}) \setminus \{0\}$ liegt auch das Produkt

$$\begin{aligned} x_1 + x_2 &= (a_1 + b_1\sqrt[3]{2} + c_1\sqrt[3]{4})(a_2 + b_2\sqrt[3]{2} + c_2\sqrt[3]{4}) \\ &= (a_1a_2 + 2b_1c_2 + 2c_1b_2) + (b_1b_2 + a_1c_2 + a_2c_1)\sqrt[3]{2} + (2c_1c_2 + a_1b_2 + a_1b_2)\sqrt[3]{4} \end{aligned}$$

  zumindest wieder in $\mathbb{Q}(\sqrt[3]{2})$. Es kann nicht Null sein, weil $\mathbb{R}$ ein Körper ist, also liegt es sogar in $\mathbb{Q}(\sqrt[3]{2}) \setminus \{0\}$.

- Für jedes Element $x = a + b\sqrt[3]{2} + c\sqrt[3]{4} \in \mathbb{Q}(\sqrt[3]{2}) \setminus \{0\}$ gehört auch das multiplikative Inverse $1/x$ wieder zu $\mathbb{Q}(\sqrt[3]{2})$. Um dies zu sehen, berechnet man zunächst

$$\begin{aligned} \frac{1}{x} &= \frac{1}{a + b\sqrt[3]{2} + c\sqrt[3]{4}} \\ &= \frac{(-a^2 + 2bc) + (ab - 2c^2)\sqrt[3]{2} + (-b^2 + ac)\sqrt[3]{4}}{(a + b\sqrt[3]{2} + c\sqrt[3]{4})((-a^2 + 2bc) + (ab - 2c^2)\sqrt[3]{2} + (-b^2 + ac)\sqrt[3]{4})} \\ &= \frac{(-a^2 + 2bc) + (ab - 2c^2)\sqrt[3]{2} + (-b^2 + ac)\sqrt[3]{4}}{-a^3 - 2b^3 - 4c^3 + 6abc}. \end{aligned}$$

  Jetzt muss man noch überprüfen, dass der Nenner nicht Null sein kann, wenn $x \neq 0$ ist. Dazu kann man (wie vom Kollegen Hopfenwieser vorgeschlagen) noch einmal mit $a^3 - 4c^3$ erweitern. Danach lautet der Nenner

$$\begin{aligned} (-a^3 - 2b^3 - 4c^3 + 6abc)(a^3 - 4c^3) &= -a^6 + 6a^4bc - 2a^3b^3 - 24abc^4 + 8b^3c^3 + 16c^6 \\ &= 2(2c^2 - ab)^3 - (a^2 - 2bc)^3. \end{aligned}$$

  Wann kann das Null sein? Wir unterscheiden zwei Fälle.

  1\. Fall: $2c^2 - ab \neq 0$. Dann würde aus $2(2c^2 - ab)^3 - (a^2 - 2bc)^3 = 0$ folgen $2 = \big((a^2 - 2bc)/(2c^2 - ab)\big)^3$, also $\sqrt[3]{2} = \frac{a^2-2bc}{2c^2-ab} \in \mathbb{Q}$, was nicht der Fall ist.

  2\. Fall: $2c^2 - ab = 0$. Dann würde mit $2(2c^2 - ab)^3 - (a^2 - 2bc)^3 = 0$ folgen $a^2 - 2bc = 0$, also $a^2 = 2bc$, also $a^3 = 2abc$, also $a^3 = 2c^3$, also $c = 0$ (weil sonst $\sqrt[3]{2} = a/c \in \mathbb{Q}$), also $a = 0$. Dann ist also $x = b\sqrt[3]{2}$ mit $b \neq 0$. In diesem Fall ist der Nenner in der obigen Darstellung tatsächlich Null, aber diesen Fall kann man leicht gesondert behandeln: Es gilt $(b\sqrt[3]{2})(\frac{1}{2b}\sqrt[3]{4}) = \frac{b}{2b}2 = 1$, also $(b\sqrt[3]{2})^{-1} = \frac{1}{2b}\sqrt[3]{4} \in \mathbb{Q}(\sqrt[3]{2})$.

  Insgesamt ist also gezeigt, dass für jedes $x \in \mathbb{Q}(\sqrt[3]{2}) \setminus \{0\}$ auch $1/x \in \mathbb{Q}(\sqrt[3]{2}) \setminus \{0\}$ ist.

Damit ist gezeigt, dass $(\mathbb{Q}(\sqrt[3]{2}) \setminus \{0\}, \cdot)$ eine Untergruppe von $(\mathbb{R} \setminus \{0\}, \cdot)$ ist.

Die Distributivgesetze übertragen sich wieder unmittelbar aus $\mathbb{R}$. Es folgt also, dass $\mathbb{Q}(\sqrt[3]{2})$ tatsächlich ein Körper ist.