6. Übungsblatt zu Lineare Algebra und analytische Geometrie 1

Prof. M. Geck, Dr. L. Iancu

WiSe 2022/23

Aufgabe 1. (**S**, 6=2+2+2 Punkte) Sei X eine nicht-leere Menge, $A = \mathrm{Abb}(X, X)$ die Menge aller Abbildungen $f : X \to X$ und $S := \mathrm{Bij}(X, X)$ die Menge aller bijektiven Abbildungen $f : X \to X$.

(a) Wir definieren eine Verknüpfung $A \times A \to A$ durch $(f, g) \mapsto f \circ g$ für $f, g \in A$ (wobei $\circ$ = Hinteranderausführung wie in Definition 5.4 der Vorlesung). Zeigen Sie, dass diese Verknüpfung assoziativ ist. Offenbar ist id_X das neutrale Element bezüglich dieser Verknüpfung.

(b) Zeigen Sie: Sind $f, g \in S$, so gilt auch $f \circ g \in S$. Also kann man genauso wie in (a) auch $S \times S \to S$, $(f, g) \mapsto f \circ g$, definieren. Zeigen Sie, dass $(S, \circ)$ eine Gruppe ist.

(c) Zeigen Sie: Wenn X mindestens 3 Elemente enthält, so ist die Gruppe $(S, \circ)$ nicht kommutativ. Was passiert, wenn X genau 1 oder genau 2 Elemente hat?

Aufgabe 2. (V)
(a) Sei G eine Gruppe mit Verknüpfung $\star : G \times G \to G$. Zeigen Sie die folgende Kürzungsregel: Sind $a, b, c \in G$ gegeben mit $a \star c = b \star c$ oder $c \star a = c \star b$, so folgt $a = b$.

(b) Sei $(R, +, \cdot)$ ein Ring. Zeigen Sie: Es gilt $-(a \cdot b) = (-a) \cdot b = a \cdot (-b)$ für alle $a, b \in R$.

Aufgabe 3. (V) Sei R ein Ring mit 1. Seien $a, b \in R$ mit $a \cdot b = b \cdot a$. Durch einfaches Nachrechnen erhält man $a^2 - b^2 = (a - b) \cdot (a + b)$ und $a^3 - b^3 = (a - b) \cdot (a^2 + a \cdot b + b^2)$. Zeigen Sie allgemein: Für alle $n \in \mathbb{N}$ gibt es ein $c_n \in R$ mit $a^n - b^n = (a - b) \cdot c_n = c_n \cdot (a - b)$. Finden Sie eine Formel für c_n.

Aufgabe 4. (V) Seien $p, q \in \mathbb{N}$ zwei verschiedene Primzahlen und sei $n \in \mathbb{Z}$ teilerfremd zu p und zu q. Zeigen Sie:

$$n^{(p-1)(q-1)} \equiv 1 \bmod (pq).$$

Hinweis: Benutzen Sie den Kleinen Satz von Fermat.

Aufgabe 5. (**S**, 12=4+4+4 Punkte)

(a) Bestimmen Sie die Multiplikationstabelle des Körpers $\mathbb{F}_7 = \mathbb{Z}/7\mathbb{Z}$.

(b) Sei $m \in \mathbb{N}$ fest und betrachte den Ring $\mathbb{Z}/m\mathbb{Z}$ (siehe Satz 8.1 der Vorlesung); für $a \in \mathbb{Z}$ bezeichne wie üblich $\bar{a} \in \mathbb{Z}/m\mathbb{Z}$ die Restklasse von a. Zeigen Sie:

$$\bar{a} \in R \text{ bezitzt ein Inverses bezüglich der Multiplikation in } \mathbb{Z}/m\mathbb{Z} \quad \Leftrightarrow \quad \operatorname{ggT}(a,m) = 1.$$

Hinweis zu (b): Lemma von Bézout.

(c) Welche Elemente des Rings $\mathbb{Z}/22\mathbb{Z}$ besitzen ein Inverses bezüglich der Multiplikation? Geben Sie die Inversen jeweils an.

Aufgabe 6. (V) Sei $K = \mathbb{Z}/7\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$. Gegeben sei die Polynomfunktion $f \in P(K)$ mit $f(x) = x^5 + \bar{3}x^4 + x^3 + \bar{1}$ für alle $x \in K$, sowie das Element $c := \bar{2} \in K$. Bestimmen Sie gemäß Satz 9.1 (Horner-Schema) die Polynomfunktion $g \in P(K)$ sowie die Konstante $r \in K$ mit

$$f(\bar{2}) = r \qquad \text{und} \qquad f(x) = (x - \bar{2}) \cdot g(x) + r \quad \text{für alle } x \in K.$$

Aufgabe 7. (Z) Sei $m \in \{18, 20, 21, 22, 25, 26, 45\}$. Finden Sie alle invertierbaren Elemente (bezüglich der Multiplikation) in dem Ring $\mathbb{Z}/m\mathbb{Z}$ und geben Sie jeweils die Inversen an.

Aufgabe 8. (Z) Sei $\mathcal{F} = \operatorname{Abb}(\mathbb{N}_0, \mathbb{Q})$ die Menge aller Folgen $(a_n)_{n \geq 0}$ mit $a_n \in \mathbb{Q}$ für alle $n \geq 0$ (wie in der Vorlesung S. 38). Seien $A = \operatorname{Abb}(\mathcal{F}, \mathcal{F})$ und eine Verknüpfung $A \times A \to A$ wie in Aufgabe 1 definiert. Diese ist dann also assoziativ, und $\mathrm{id}_{\mathcal{F}} \in A$ ist das neutrale Element; wir können nun auch nach inversen Elementen in A schauen. Seien $f, g \in A$ gegeben durch

$$f\big(a_0, a_1, a_2, \ldots\big) := (0, a_0, a_1, a_2, \ldots) \qquad \text{und} \qquad g\big(a_0, a_1, a_2 \ldots\big) := (a_1, a_2, a_3, \ldots).$$

Untersuchen Sie, ob $g \circ f = \mathrm{id}_{\mathcal{F}}$ bzw. $f \circ g = \mathrm{id}_{\mathcal{F}}$ gilt. Ist f injektiv oder surjektiv ? Ist g injektiv oder surjektiv ? Besitzt f oder g ein Inverses bezüglich $\circ$?

Schriftliche Aufgaben sind mit (**S**) markiert. Die mit (V) markierten Aufgaben sind zum *Votieren* bzw. zum *Vorrechnen* in den Gruppenübungen. Die mit (Z) markierten Aufgaben sind *zusätzliche Aufgaben.*

Abgabe der schriftlichen Aufgaben: *In den Übungsgruppen Dienstag/Mittwoch 29./30. November, oder online.*