Prof. Dr. Benjamin Klopsch
Wintersemester 2017–18

HEINRICH HEINE
UNIVERSITÄT DÜSSELDORF

Lineare Algebra I – Blatt 10

Abgabe der Lösungen bis zum 20.12.2017, 10:15 Uhr in den dafür vorgesehenen Kästen

Sei G eine Gruppe. Für $g \in G$ bezeichnet g^{-1} das zu g inverse Element; man erweitert diese Schreibweise für $k \in \mathbb{Z}$ durch die Abmachung

$$g^k = \begin{cases} g \cdot g \cdot \ldots \cdot g \quad (k \text{ Faktoren}) & \text{falls } k \geq 0, \\ (g^{-k})^{-1} & \text{falls } k < 0 \end{cases}$$

Aufgabe 10.1 (4 Punkte)

Sei G eine Gruppe und $g \in G$.

(1) Die Zahl $\mathrm{ord}(g) = \min(\{\infty\} \cup \{k \in \mathbb{N} \mid g^k = 1\})$ heißt die *Ordnung* von g. Zeigen Sie: $\langle g \rangle = \{g^k \mid k \in \mathbb{Z}\}$ ist eine Untergruppe von G und $|\langle g \rangle| = \mathrm{ord}(g)$.

(2) Zeigen Sie: Ist $\mathrm{ord}(g) < \infty$ und $m \in \mathbb{Z}$ mit $g^m = 1$, so gilt $\mathrm{ord}(g) \mid m$.

Aufgabe 10.2 (4 Punkte)

Sei $m \in \mathbb{N}$ und $\varphi(m) = |\{a \in \mathbb{N} \mid 1 \leq a \leq m \text{ und } \mathrm{ggT}(a, m) = 1\}|$.

(1) Zeigen Sie: Für jedes $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a, m) = 1$ gilt $a^{\varphi(m)} \equiv_m 1$.

(2) Leiten Sie den kleinen Satz von Fermat ab: Für $p \in \mathbb{P}$ und $a \in \mathbb{Z}$ gilt $a^p \equiv_p a$.

(3) Bestimmen Sie 2^{2014} modulo 2017 (als Element von $\{0, 1, \ldots, 2016\}$).

Hinweis. Betrachten Sie die Einheitengruppe von $\mathbb{Z}/m\mathbb{Z}$ und benutzen Sie, was Sie in den Aufgaben 9.1, 9.4 und 10.1 gelernt haben.

Aufgabe 10.3 (4 Punkte)

(1) Sei K ein Körper, und sei $f \in K[X]$ mit $\mathrm{grad}(f) = 2$ oder $\mathrm{grad}(f) = 3$. Beweisen Sie, dass f genau dann irreduzibel in $K[X]$ ist, wenn f keine Nullstelle in K besitzt.

(2) Geben Sie konkret ein Polynom $f \in \mathbb{R}[X]$ vom Grad 4 an, das zwar keine Nullstelle in $\mathbb{R}$ besitzt, aber dennoch nicht irreduzibel in $\mathbb{R}[X]$ ist.

Aufgabe 10.4 (4 Punkte)

Seien $\varphi: U \to V$ und $\psi: V \to W$ lineare Abbildungen zwischen Vektorräumen U, V, W über einem Körper K. Zeigen Sie:

(1) Die Hintereinanderausführung $\varphi\psi: U \to W$ ist eine lineare Abbildung.

(2) $\mathrm{Kern}(\psi) = \{v \in V \mid v\psi = 0\}$ ist ein Unterraum von V.

(3) $\mathrm{Bild}(\psi) = \{v\psi \mid v \in V\}$ ist ein Unterraum von W.

(4) Aus $V = \langle v_1, \ldots, v_r \rangle$ folgt $\mathrm{Bild}(\psi) = \langle v_1\psi, \ldots, v_r\psi \rangle$.

(5) $\dim \mathrm{Bild}(\psi) \leq \dim V$.