Lösung 2

Aufgabe 1.

(a) Sei G eine Gruppe. Wir zeigen, dass G auch ein Gruppi ist. Zunächst halten wir fest, dass die Abgeschlossenheit sowie (Gi 1) und (Gi 2) aus den üblichen Gruppenaxiomen folgen (vgl. Def. 1.2.1). Es bleibt zu zeigen, dass in G jedes Linksinverse auch Rechtsinverses ist. Es gilt:

$$\begin{aligned} e &= (a^{-1})^{-1}a^{-1} = (a^{-1})^{-1}(ea^{-1}) = (a^{-1})^{-1}(a^{-1}aa^{-1}) \\ &= ((a^{-1})^{-1}a^{-1})(aa^{-1}) = eaa^{-1} = aa^{-1} \end{aligned}$$

(b) Nicht jedes Gruppi ist eine Gruppe. Betrachte z.B. die Menge

$$G = \{\, f \,:\, \mathbb{N} \to \mathbb{N} \,;\; f surjektiv \,\}$$

mit der Verknüpfung $'\circ'$.
Zur Erinnerung: Eine Abbildung $f : M \to N$ ist injektiv (surjektiv), wenn eine Abbildung $g : N \to M$ existiert mit $g \circ f = \mathrm{id}_M$ ($f \circ g = \mathrm{id}_N$).
Also existiert zu jedem $f \in G$ ein $f^* \in G$ mit $ff^* = e$ und G ist somit ein Gruppi.
Hingegen ist

$$f \,:\, \mathbb{N} \to \mathbb{N}, n \mapsto \begin{cases} 0 & , n = 0 \\ n-1 & , n > 0 \end{cases}$$

surjektiv, aber nicht injektiv, also existiert kein $f^* \in G$ mit $f^*f = e$, also ist G keine Gruppe.

Aufgabe 2.

(a) (i) i=-1. Es gilt $(ab)^{-1} = a^{-1}b^{-1} = (ba)^{-1}$ nach Voraussetzung bzw. nach Notiz 1.2.2. Darauf folgt bereits $ab = ba$ für alle $a, b \in G$.
(ii) i=2. Hier gilt $(ab)^2 = abab = a^2b^2$. Multipliziert man diese Gleichung vor links mit a^{-1} und von rechts mit b^{-1} , so erhält man $ab = ba$ für alle $a, b \in G$.

(b) Gilt $a^2 = e$ für alle $a \in G$, so auch $e = (ab)^2 = abab$. Multiplikation von links (rechts) mit a (b) liefert $ab = ba$ für alle $a, b \in G$.

(c) Betrachte zunächst $(ab)^{k+2} = a^{k+2}b^{k+2} = a(ba)^{k+1}b$. Daraus folgt $a^{k+1}b^{k+1} = (ba)^{k+1} = (ab)^{k+1}$. Analog erhält man aus $(ab)^{k+1} = a^{k+1}b^{k+1} = a(ba)^kb$ die Gleichheit $a^kb^k = (ba)^k = b^ka^k$.
Es gilt also $(ab)^{k+1} = (ba)^{k+1}$, oder anders $(ab)(ab)^k = (ba)(ba)^k = (ba)(ab)^k$ und somit folgt $ab = ba$ für alle $a, b \in G$.

Aufgabe 3.

(a) Wir benutzen Notiz 1.4.2 und zeigen, dass für $M_1, M_2 \in M$ auch $M_1M_2^{-1} \in M$ gilt. Es ist

$$\begin{pmatrix} 1 & a_2 & b2 \\ 0 & 1 & c_2 \\ 0 & 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -a_2 & a_2c_2 - b2 \\ 0 & 1 & -c_2 \\ 0 & 0 & 1 \end{pmatrix}$$

und somit

$$\begin{pmatrix} 1 & a_1 & b1 \\ 0 & 1 & c_1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & a_2 & b2 \\ 0 & 1 & c_2 \\ 0 & 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & a_1 - a_2 & a_2c_2 - b_2 + b_1 - a_1c_2 \\ 0 & 1 & c_1 - c_2 \\ 0 & 0 & 1 \end{pmatrix} \in M$$

(b) Sei

$$A = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}.$$

Dann gilt

$$A^3 = \begin{pmatrix} 1 & 3a & b + 2ac + 2b + ac \\ 0 & 1 & 3c \\ 0 & 0 & 1 \end{pmatrix} = E_3$$

im Fall $K = \mathbb{F}_3$, denn $3 \equiv 0 \mod 3$.
Betrachtet man die Matrizen

$$M_1 = \begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{und} \quad M_1 = \begin{pmatrix} 1 & -1 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

so gilt $M_1 M_2 \neq M_2 M_1$. Also ist M nicht kommutativ.

Aufgabe 4.
Sei $g \in G$. Dann gilt entweder $\langle g \rangle = \{e\}$ oder $\langle g \rangle = G$. Insbesondere gibt es wegen $G \neq \{e\}$ mindestens ein $g \in G$ mit $\langle g \rangle = G$, also ist G zyklisch.
Angenommen $p := \#G$ besitzt einen Teiler d mit $1 < d < p$, so gibt es nach Korollar 1.7.7 eine Untergruppe $H < G$ mit $\#H = d$. Dies ist nach Voraussetzung unmöglich, also ist p eine Primzahl. Folglich ist $G \cong \mathbb{Z}/p\mathbb{Z}$ nach Korollar 1.7.6.