Aufgabe 1

Offensichtlich gilt $e \in HK$. Um die Abgeschlossenheit bezüglich Multiplikation zu zeigen, wählen wir beliebige Elemente $h \cdot k, h' \cdot k' \in HK$ und betrachten das Produkt $h \cdot k \cdot h' \cdot k'$. Da die Gruppen HK und KH identisch sind und $k \cdot h' \in KH$, gibt es $h'' \cdot k'' \in HK$ mit $k \cdot h' = h'' \cdot k''$. Setzen wir dies ein, so erhalten wir

$$h \cdot k \cdot h' \cdot k' = \underbrace{h \cdot h''}_{\in H} \cdot \underbrace{k'' \cdot k'}_{\in K} \in HK.$$

Schließlich zeigen wir noch die Abgeschlossenheit bezüglich Inversenbildung. Sei also erneut $h \cdot k$ ein beliebiges Element in HK. Das Inverse $k^{-1}h^{-1}$ liegt in KH. Wegen $KH = HK$ existiert also ein Element $h' \cdot k' \in HK$ mit

$$(h \cdot k)^{-1} = k^{-1}h^{-1} = h'k' \in HK.$$

Aufgabe 2

(a) Es gilt $\forall g \in G : g^{-1} \in G$. Sofern also $g \neq g^{-1}$ ist, kürzen sich beim Produkt über alle Gruppenelemente $g \cdot g^{-1} = e$. Daher ist also

$$a = \prod_{g \in G} g = \prod_{\substack{g \in G \\ g = g^{-1}}} g = \prod_{\substack{g \in G \\ g^2 = e}} g.$$

Insbesondere erhalten wir also

$$a^2 = \Big(\prod_{\substack{g \in G \\ g^2 = e}} g \Big)^2 = \prod_{\substack{g \in G \\ g^2 = e}} g^2 = \prod_{\substack{g \in G \\ g^2 = e}} e = e.$$

(b) Zunächst bestimmen wir alle natürlichen Zahlen $0 < z < p$, für die $\exists k \in \mathbb{N}_0$ mit

$$\begin{aligned} z^2 &= k \cdot p + 1 \\ z^2 - 1 &= k \cdot p \\ (z+1) \cdot (z-1) &= k \cdot p. \end{aligned}$$

Da p eine Primzahl ist und $z < p$ gilt, muss entweder $k = 0 \Leftrightarrow z = 1$ oder $p = z + 1 \Leftrightarrow z = p - 1$ gelten. Nach Teilaufgabe (a) erhalten wir also

$$(p-1)! = 1 \cdot (p-1) = p - 1 \equiv -1 \mod p$$

Aufgabe 3

(a) Offensichtlich ist $e \in Z(G)$. Ist $Z(G) = \{e\}$, so handelt es sich um einen Normalteiler. Seien ansonsten $g, g' \in Z(G)$. Dann ist $h \cdot g \cdot g' = g \cdot h \cdot g' = g \cdot g' \cdot h$ und damit $gg' \in Z(G)$. Ist $g \in Z(G)$, so gilt wegen

$$g^{-1} \cdot h = g^{-1} \cdot h \cdot g \cdot g^{-1} \overset{g \in Z(G)}{=} g^{-1} \cdot g \cdot h \cdot g^{-1} = h \cdot g^{-1}$$

auch $g^{-1} \in Z(G)$. $Z(G)$ ist also eine Untergruppe von G. Sei nun $g \in Z(G)$ und $a \in G$. Dann gilt

$$a \cdot g \cdot a^{-1} = a \cdot a^{-1} \cdot g = g \in Z(G)$$

und damit also $aZ(G)a \subset Z(G) \quad \forall a \in G$. Nach Lemma 1.24 ist daher $Z(G)$ ein Normalteiler.

(b) Sei $G/Z(G)$ zyklisch. Dann $\exists g \in G$ mit $G/Z(G) = \langle gZ(G) \rangle$. Nun gilt

$$G = \bigcup_{n \in \mathbb{N}} (gZ(G))^n = \bigcup_{n \in \mathbb{N}} g^n Z(G).$$

Jedes Element von G lässt sich also in der Form $g^n \cdot h$ mit $n \in \mathbb{N}$ und $h \in Z(G)$ schreiben. Betrachten wir ein Produkt zweier solcher Elemente, so erhalten wir, da g mit sich selbst kommutiert,

$$g^n h \cdot g^k h' \overset{h \in Z(G)}{=} g^n g^k h \cdot h' = g^k g^n h' \cdot h \overset{h' \in Z(G)}{=} g^k h' \cdot g^n h.$$

Die Gruppe ist also abelsch.

Aufgabe 4

(a) Offensichtlich ist $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in D_4$. Wendet man zwei lineare Abbildungen nacheinander an, die beide das Quadrat invariant lassen, so bleibt das Quadrat auch unter der Hintereinanderausführung invariant. Da die Hintereinanderausführung zweier linearen Abbildungen äquivalent zur Ausführung des Produkts der beiden zugehörigen Matrizen ist, liegt also das Produkt zweier Matrizen aus der D_4 wieder in der D_4. Genauso lässt auch die Umkehrabbildung einer Matrix bzw. der zugehörigen Abbildung aus der D_4 das Quadrat invariant und liegt damit selbst wieder in der D_4.

(b) Sei $R \in \overline{PQ}$, R ist also ein Punkt auf der Strecke von P nach Q. Dann lässt sich R als Konvexkombination von P und Q schreiben, $R = \lambda P + (1-\lambda)Q$. Unter einer linearen Abbildung A wird R auf den Punkt $A(R) = A(\lambda P + (1-\lambda)Q) = \lambda A(P) + (1-\lambda)A(Q)$ abgebildet, der nun auf der Strecke $\overline{A(P)A(Q)}$ liegt. Ist nun R ein Endpunkt von $\overline{PQ}$, so ist $\lambda \in \{0, 1\}$. Dann ist $A(R)$ auch ein Endpunkt der Strecke $\overline{A(P)A(Q)}$. Da $E_1 = (1, 1)^T$ und $E_2 = (-1, 1)^T$ eine Basis des $\mathbb{R}^2$ bilden, sind lineare Abbildungen bereits durch ihre Werte auf E_1 und E_2 eindeutig bestimmt. Da E_1 und E_2 aber beides Endpunkte von Strecken sind, müssen sie unter einer linearen Abbildung, die das Quadrat erhält, wieder auf einen Endpunkt von Strecken abgebildet werden, also auf einen der 4 Eckpunkte. Für E_1 gibt es vier Eckpunkte zur Auswahl, für E_2 dann nur noch drei. Insgesamt erhalten wir also 12 Möglichkeiten.

(c) Da jede der Möglichkeiten bereits durch die Werte für E_1 und E_2 bestimmt ist und die Werte nur in $\{E_1, E_2, E_3 := (-1, -1)^T, E_4 := (1, -1)^T\}$ liegen dürfen, genügt es, Tupel (i, j) anzugeben, wobei dann E_1 auf E_i und E_2 auf E_j abgebildet werde. Damit erhalten wir die Möglichkeiten

$$(1,2), (1,3), (1,4), (2,1), (2,3), (2,4), (3,1), (3,2), (3,4).$$