Aufgabe 7.1

(i) Eine invertierbare Abbildung $x \to M_x$, die Q in sich abbildet, muss natürlich injektiv sein. Da Q aber endlich ist, muss sie dann auch surjektiv sein, also permutiert sie Q.

(ii) Wir wählen zwei benachbarte Punkte und halten diese Fest.
Punkt 1 fest:

$$M \cdot \begin{pmatrix} -1 \\ 1 \end{pmatrix} = \begin{pmatrix} -1 \\ 1 \end{pmatrix}$$

$$\Leftrightarrow \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} -1 \\ 1 \end{pmatrix} = \begin{pmatrix} -1 \\ 1 \end{pmatrix}$$

Daraus ergeben sich die Gleichungen:

$$a \cdot (-1) + b = -1$$

$$c \cdot (-1) + d = 1$$

Punkt 2 fest:

$$M \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

$$\Leftrightarrow \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

Daraus ergeben sich die Gleichungen:

$$a + b = 1$$

$$c + d = 1$$

Aus den 4 Gleichungen erhält man $M = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = E$.

Eine lineare Abbildung, die die erste und zweite Ecke unverändert lässt, ist also die identische Abbildung. Also kann keine Symmetrie, die erste und zweite Ecke festhalten und gleichzeitig die dritte und vierte Ecke vertauschen.
Somit ist beispielsweise (P_1, P_2, P_4, P_3) eine Permutation der Eckenmenge Q, die nicht durch G abgebildet werden kann.

(iii) $G = \{id, R_{90}, R_{180}, R_{270}, S_1, S_2, S_3, S_4\}$ mit R : Rotationen und S : Spiegelungen

(iv) G ist eine Gruppe, da folgende Eigenschaften erfüllt sind:

- Abgeschlossenheit:
  Hintereinanderausführung ist linear und bildet Q in sich ab.
- Assoziativität:
- Neutrales Element:
  Die Identität $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ ist das neutrale Element.
- Inverse:
  Die Inverse zu M ist auch linear und bildet wegen (i) auch Q in sich ab.

G ist nicht kommutativ., da Matrixoperationen nicht kommutativ sind.

(v) Die Identität hat die Ordnung 1, die Rotationen die Ordnung 4 und die Spiegelungen die Ordnung 2.
G ist nicht zyklisch, da kein Element die Ordnung 8 hat.

(vi) d_1 ist kein Homomorphismus (Gruppenoperation Addition), da die Bedingung $f(x \circ y) = f(x) \circ f(y)$ nicht erfüllt ist.

Bewies:
$$
\begin{aligned}
\det(M_1 \cdot M_2) &= \det\left(\begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix} \cdot \begin{pmatrix} n_{11} & n_{12} \\ n_{21} & n_{22} \end{pmatrix}\right) \\
&= \det\begin{pmatrix} m_{11}n_{11} + m_{12}n_{21} & m_{11}n_{12} + m_{12}n_{22} \\ m_{21}n_{11} + m_{22}n_{21} & m_{21}n_{12} + m_{22}n_{22} \end{pmatrix} \\
&= \ldots \\
&= \det(M_1) \cdot \det(M_2) + m_{11}n_{22} + n_{11}m_{22} - m_{21}n_{12} - n_{21}m_{12} \\
&\neq \det(M_1) \cdot \det(M_2)
\end{aligned}
$$

d_2 ist ein Homomorphismus (Gruppenoperation Multiplikation), da die Abbildung wohldefiniert ist und $f(x \circ y) = f(x) \circ f(y)$ gilt.

Beweis:
$$
\begin{aligned}
\det(M_1 \cdot M_2) &= \det\left(\begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix} \cdot \begin{pmatrix} n_{11} & n_{12} \\ n_{21} & n_{22} \end{pmatrix}\right) \\
&= \det\begin{pmatrix} m_{11}n_{11} + m_{12}n_{21} & m_{11}n_{12} + m_{12}n_{22} \\ m_{21}n_{11} + m_{22}n_{21} & m_{21}n_{12} + m_{22}n_{22} \end{pmatrix} \\
&= \ldots \\
&= (m_{11}m_{22} - m_{12}m_{22}) \cdot (n_{11}n_{22} - n_{12}n_{21}) \\
&= \det(M_1) \cdot \det(M_2)
\end{aligned}
$$

d_3 ist ein Homomorphismus (Gruppenoperation Multiplikation) , da die Abbildung wohldefiniert ist und $f(x \circ y) = f(x) \circ f(y)$ gilt.

Beispiel:
$$
\begin{aligned}
&\det\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}\right) = \det\left(\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\right) \cdot \det\left(\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}\right) \\
&\Leftrightarrow \det\left(\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}\right) = 1 \cdot 1 \\
&\Leftrightarrow 1 = 1
\end{aligned}
$$

d_4 ist kein Homomorphismus, da die Abbildung nicht wohldefiniert ist. Ist $\det(M) = -1$, so befindet sich dieser Wert nicht im Wertebereich der Abbildung.

(vii) $\ker(d_2)$ sind alle Elemente, die auf das neutrale Element abgebildet werden. Da ein Homomorphismus nur mit der Gruppenoperation Multiplikation vorliegt, ist also

$\ker(d_2) = \{x \in G \mid \det(x) = 1\}$

$$\ker(d_2) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\}$$

$im(d_2)$ sind alle Elemente, die durch die Abbildung getroffen werden. In diesem Fall ist also $im(d_2) = \{1, -1\}$.

(viii) $\ker(d_2)$ ist eine Gruppe, da sie

- ein neutrales Element besitzt: $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$
- abgeschlossen ist (z.B. $\begin{pmatrix} -1 & 0 \\ 0 & .1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$)
- assoziativ ist.

$\ker(d_2)$ ist zudem zyklisch, da ein erzeugendes Element ($\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$) mit der Ordnung 4 vorhanden ist.

Außerdem ist $\ker(d_2)$ kommutativ.

(ix) Die erste Nebenklasse ist $\ker(d_2)$ selbst:

$$NK_1 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\}$$

In G gibt es 2 Nebenklassen, wegen $\frac{\text{Gruppenordnung}}{\text{Ordnung der NK}} = \frac{8}{4} = 2$

Die zweite Nebenklasse ist:

$$NK_2 = \left\{ \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} \right\}$$

(x) In (vii) wurde bereits gezeigt, dass $\ker(d_2)$ eine Gruppe ist, somit ist auch NK_1 eine Gruppe.

NK_2 ist keine Gruppe, da sie kein neutrales Element besitzt.

NK_1 ist ein Normalteiler, da nur zwei Nebenklassen existieren und eine Nebenklasse der Kern selbst ist. Da NK_1 kommutativ ist (vgl. (vii)), gilt $gU = Ug$.

(xi) H ist eine Gruppe, da sie

- Abgeschlossen ist:

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in H$$

$$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in H$$

- Assoziativ ist (Matrixoperationen sind assoziativ)
- Ein neutrales Element besitzt ($\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$)

H ist zyklisch, das Erzeugende Element ist $\left\langle \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle$.

H ist außerdem kommutativ:

$$\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

(xii) G hat genau $\frac{8}{2} = 4$ Nebenklassen.

Für jedes Element $g \in G$ gibt es eine Nebenklasse gH , die g enthält. Somit gibt es folgende Nebenklassen:

$$NK_1 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$$

$$NK_2 = \left\{ \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$$

$$NK_3 = \left\{ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \right\}$$

$$NK_4 = \left\{ \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\}$$

(xiii) Da nur NK_1 das neutrale Element enthält, können die anderen Nebenklassen keine Gruppe bilden.

Aufgabe 7.2

$G_0 = (\mathbb{Z}_4, +) = (\{0,1,2,3\}, +)$

Gruppenordnung: 4
Zyklisch: Ja
Erzeugende Elemente: $\langle 1\rangle, \langle 3\rangle$

Element	0	1	2	3
Ordnung	1	4	2	4

$G_1 = (\mathbb{Z}_6, +) = (\{0,1,2,3,4,5\}, +)$

Gruppenordnung: 6
Zyklisch: Ja
Erzeugende Elemente: $\langle 1\rangle, \langle 5\rangle$

Element	0	1	2	3	4	5
Ordnung	1	6	3	2	3	6

$G_2 = (\mathbb{Z}_2 \times \mathbb{Z}_2, +) = (\{(0,0),(0,1),(1,0),(1,1)\}, +)$

Gruppenordnung: 4
Zyklisch: Nein
Erzeugende Elemente: keine

Element	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
Ordnung	1	2	2	2

$G_3 = (\mathbb{Z}_2 \times \mathbb{Z}_3, +) = (\{(0,0),(0,1),(0,2),(1,0),(1,1),(1,2)\}, +)$

Gruppenordnung: 6
Zyklisch: Ja
Erzeugende Elemente: $(\langle 1,1\rangle), (\langle 1,2\rangle)$

Element	$(0,0)$	$(0,1)$	$(0,2)$	$(1,0)$	$(1,1)$	$(1,2)$
Ordnung	1	3	3	2	6	6

$G_4 = (\mathbb{Z}_3 \times \mathbb{Z}_2, +) = (\{(0,0),(0,1),(1,0),(1,1),(2,0),(2,1)\}, +)$

Gruppenordnung: 6
Zyklisch: Ja
Erzeugende Elemente: $(\langle 1,1\rangle), (\langle 2,1\rangle)$

Element	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$	$(2,0)$	$(2,1)$
Ordnung	1	2	3	6	3	6

$G_5 = \left(\mathbb{Z}_5^\times, \cdot\right) = \left(\{1,2,3,4\}, \cdot\right)$

Gruppenordnung: 4
Zyklisch: Ja
Erzeugende Elemente: $\langle 2\rangle, \langle 3\rangle$

Element	1	2	3	4
Ordnung	1	4	4	2

$G_6 = \left(\mathbb{Z}_7^\times, \cdot\right) = \left(\{1,2,3,4,5,6\}, \cdot\right)$

Gruppenordnung: 6
Zyklisch: Ja
Erzeugende Elemente: $\langle 3\rangle, \langle 5\rangle$

Element	1	2	3	4	5	6
Ordnung	1	3	6	3	6	2

$G_7 = \left(\mathbb{Z}_8^\times, \cdot\right) = \left(\{1,3,5,7\}, \cdot\right)$

Gruppenordnung: 4
Zyklisch: Nein
Erzeugende Elemente: keine

Element	1	3	5	7
Ordnung	1	2	2	2

$G_8 = \left(S_3, \circ\right) = \left(\{(123),(132),(12),(13),(23)\}, \circ\right)$

Gruppenordnung: 6
Zyklisch: Nein
Erzeugende Elemente: keine

Element	id	(123)	(132)	(12)	(13)	(23)
Ordnung	1	3	3	2	2	2

$$G_9 = \left(GL_2(\mathbb{F}_2), \cdot\right) = \left(\left\{\begin{pmatrix}1&0\\0&1\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}, \begin{pmatrix}1&0\\1&1\end{pmatrix}, \begin{pmatrix}0&1\\1&1\end{pmatrix}, \begin{pmatrix}0&1\\1&0\end{pmatrix}, \begin{pmatrix}1&1\\1&0\end{pmatrix}\right\}, \cdot\right)$$

Gruppenordnung: 6
Zyklisch: Nein
Erzeugende Elemente: keine

Element	$\begin{pmatrix}0&1\\1&0\end{pmatrix}$	$\begin{pmatrix}0&1\\1&1\end{pmatrix}$	$\begin{pmatrix}1&0\\0&1\end{pmatrix}$	$\begin{pmatrix}1&0\\1&1\end{pmatrix}$	$\begin{pmatrix}1&1\\0&1\end{pmatrix}$	$\begin{pmatrix}1&1\\1&0\end{pmatrix}$
Ordnung	2	3	1	2	2	3

Nach Überprüfung der oben angegebenen Eigenschaften, können nur noch folgende Isomorphismen vorliegen:

	G_0	G_1	G_2	G_3	G_4	G_5	G_6	G_7	G_8	G_9
G_0	$=$	$\ncong$	$\ncong$	$\ncong$	$\ncong$	$\cong$	$\ncong$	$\ncong$	$\ncong$	$\ncong$
G_1	$\ncong$	$=$	$\ncong$	$\cong$	$\cong$	$\ncong$	$\cong$	$\ncong$	$\ncong$	$\ncong$
G_2	$\ncong$	$\ncong$	$=$	$\ncong$	$\ncong$	$\ncong$	$\ncong$	$\cong$	$\ncong$	$\ncong$
G_3	$\ncong$	$\cong$	$\ncong$	$=$	$\cong$	$\ncong$	$\cong$	$\ncong$	$\ncong$	$\ncong$
G_4	$\ncong$	$\cong$	$\ncong$	$\cong$	$=$	$\ncong$	$\cong$	$\ncong$	$\ncong$	$\ncong$
G_5	$\cong$	$\ncong$	$\ncong$	$\ncong$	$\ncong$	$=$	$\ncong$	$\ncong$	$\ncong$	$\ncong$
G_6	$\ncong$	$\cong$	$\ncong$	$\cong$	$\cong$	$\ncong$	$=$	$\ncong$	$\ncong$	$\ncong$
G_7	$\ncong$	$\ncong$	$\cong$	$\ncong$	$\ncong$	$\ncong$	$\ncong$	$=$	$\ncong$	$\ncong$
G_8	$\ncong$	$\ncong$	$\ncong$	$\ncong$	$\ncong$	$\ncong$	$\ncong$	$\ncong$	$=$	$\cong$
G_9	$\ncong$	$\ncong$	$\ncong$	$\ncong$	$\ncong$	$\ncong$	$\ncong$	$\ncong$	$\cong$	$=$

- Zyklische Gruppen mit 4 Elementen
  $$g1: \begin{array}{c} G_0 \to G_5 \\ x \mapsto 2^x \bmod 5 \end{array}$$
- Nicht-zyklische Gruppen mit 4 Elementen
  $$g_2: \begin{array}{c} G_2 \to G_7 \\ (x,y) \mapsto \left(5^x \cdot 3^y\right) \bmod 8 \end{array}$$
- Zyklische Gruppen mit 6 Elementen (Jeweils eine isomorphe Abbildung, aufgrund der Bijektivität lassen sich alle anderen Abbildungen durch Komposition der angegebenen finden)
  $$g_3: \begin{array}{c} G_1 \to G_3 \\ x \mapsto (x \bmod 2, x \bmod 3) \end{array}$$
  $$g_4: \begin{array}{c} G_3 \to G_4 \\ (x,y) \mapsto (y,x) \end{array}$$
  $$g_5: \begin{array}{c} G_1 \to G_6 \\ x \mapsto 3^x \bmod 7 \end{array}$$

- Nicht-zyklische Gruppen mit 6 Elementen

$$G_9 \to G_8$$

$$g_6 : x \mapsto \begin{cases} (\ ) \text{ falls } x = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \\ (23) \text{ falls } x = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \\ (13) \text{ falls } x = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \\ (12) \text{ falls } x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \\ (123) \text{ falls } x = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \\ (132) \text{ falls } x = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \end{cases}$$

Aufgabe 7.3

Zu zeigen: $ord\left(x^e\right) = \frac{a}{ggT(a,e)}$, für $e \in \mathbb{N}$

$$x^{ord(x)} = 1 = \left(x^e\right)^{ord\left(x^e\right)}$$

$$\Rightarrow x^{f \cdot ord(x)} = x^{e \cdot ord\left(x^e\right)}$$

Da die Basen gleich sind, betrachten wir die Exponenten:

$$f \cdot ord(x) = e \cdot ord\left(x^e\right)$$

$$\Rightarrow ord\left(x^e\right) = \frac{f}{e} \cdot ord(x)$$

Gemäß Definition der Ordnung (minimal und ganzzahlig) gilt:

$$ord\left(x^e\right) = \frac{ord(x)}{ggT(e, ord(x))}$$

$$\Rightarrow ord\left(x^e\right) = \frac{a}{ggT(e,a)}$$

Die beiden Fälle $e \mid a$ und $ggT(e,a) = 1$ liefern:

- $e \mid a$

  $$ord\left(x^e\right) = \frac{a}{ggT(e,a)} = \frac{a}{e}$$

- $ggT(e,a) = 1$

  $$ord\left(x^e\right) = \frac{a}{ggT(e,a)} = \frac{a}{1} = a$$