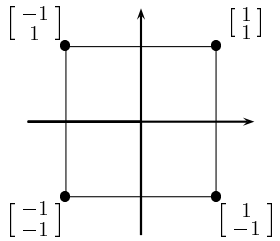
7. Musterlösung zu Mathematik für Informatiker II, SS 2004

MARTIN LOTZ & MICHAEL NÜSKEN

Aufgabe 7.1 (Symmetrien). (15 Punkte)

Sei $Q = \left\{ \left[\begin{smallmatrix}1\\1\end{smallmatrix}\right], \left[\begin{smallmatrix}1\\-1\end{smallmatrix}\right], \left[\begin{smallmatrix}-1\\1\end{smallmatrix}\right], \left[\begin{smallmatrix}-1\\-1\end{smallmatrix}\right] \right\} \subset \mathbb{R}^2$ die Menge der Ecken eines Quadrates. Wir betrachten die Menge

$$G := \left\{ M \in \mathbb{R}^{2\times 2} \;\middle|\; \begin{array}{l} M \text{ invertierbar,} \\ \forall x \in Q \colon M \cdot x \in Q \end{array} \right\}$$



der Symmetrien des Quadrates mit der Multiplikation von Matrizen als Operation.

(i) Zeige, dass jedes Element M von G die Eckenmenge Q permutiert, also bijektiv auf sich selbst abbildet.

Lösung. Die Matrix M ist invertierbar, also ist die dadurch gegebene Abbildung insbesondere injektiv. Ferner lässt sich M auf Q einschränken und alle Bilder liegen wieder in Q, sodass wir eine Abbildung $Q \to Q$ erhalten. Diese ist offenbar immer noch injektiv. Da nun Q endlich ist, muss sie auch surjektiv und damit bijektiv sein. Also ist M eingeschränkt auf Q ein Permutation. ◯

(ii) Gib eine Permutation der Eckenmenge Q an, die hierbei nicht vorkommt.

Lösung. Eine Abbildung, die zwei benachbarte Eckpunkte vertauscht und die anderen zwei Punkte festhält, ist nicht in G. Wir beweisen dies indem wir zeigen, dass jede Abbildung in G, die zwei benachbarte Punkte festhält, bereits die Identität ist.

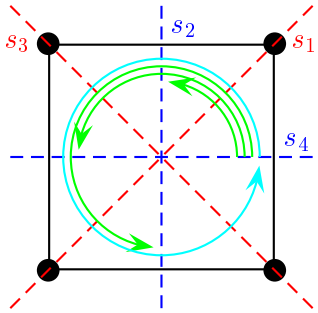
Sei M die Matrix einer Abbildung, die die Ecken $\left[\begin{smallmatrix}-1\\1\end{smallmatrix}\right]$ und $\left[\begin{smallmatrix}-1\\-1\end{smallmatrix}\right]$ von M festhält. Schreiben wir die Matrix M als $M = \left[\begin{smallmatrix}m_{11} & m_{12}\\ m_{21} & m_{22}\end{smallmatrix}\right] \in G$, so bedeutet dies $M \left[\begin{smallmatrix}-1\\1\end{smallmatrix}\right] = \left[\begin{smallmatrix}-1\\1\end{smallmatrix}\right]$ und $M \left[\begin{smallmatrix}-1\\-1\end{smallmatrix}\right] = \left[\begin{smallmatrix}-1\\-1\end{smallmatrix}\right]$. Als Gleichungssystem sehen diese Bedinungen wie folgt aus:

$$(*) \qquad -m_{11} + m_{12} = -1,$$
$$(**) \qquad -m_{21} + m_{22} = +1,$$
$$(\#) \qquad -m_{11} - m_{12} = -1,$$
$$(\#\#) \qquad -m_{21} - m_{22} = -1..$$

Durch Vergleich von $(*)$ und $(\#)$ folgt $m_{11} = 1$ und $m_{12} = 0$. Durch Vergleich von $(**)$ und $(\#\#)$ folgt $m_{21} = 0$ und $m_{22} = 1$. Also muss M die Identitätsmatrix sein. ◯

(iii) Erstelle eine Liste aller acht Elemente von G.

Lösung. Die Elemente von G bestehen aus der Identität, Drehungen um 90, 180 und 270 Grad und Spiegelungen an den vier Symmetrieachsen:



In Matrixform sind dies:

$$G = \left\{ \begin{array}{llll} \mathrm{id} = \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right], & t_{90} = \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right], & t_{180} = \left[\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right], & t_{270} = \left[\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right], \\ s_1 = \left[\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right], & s_2 = \left[\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right], & s_3 = \left[\begin{smallmatrix} 0 & -1 \\ -1 & 0 \end{smallmatrix}\right], & s_4 = \left[\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right] \end{array} \right\}.$$

Beachte, dass die Drehungen genau die Elemente aus G mit Determinante 1, und die Spiegelungen die mit Determinante -1 sind. ◯

(iv) Ist G eine Gruppe? Ist G kommutativ?

Lösung. G ist eine Gruppe:

- Die Eins ist die Identitätsmatrix $I = \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right]$.
- Multipliziert man je zwei Matrizen aus G, ist das Ergebnis wieder in G. Das erkennt man am Einfachsten direkt an der Definition: Die Zusammensetzung zweier linearer, invertierbarer Abbildungen ist wieder linear und invertierbar. Bilden diese Abbildungen dazu noch Q auf sich selber ab, so tut dies auch die Zusammensetzung. Also ist G abgeschlossen unter Matrixmultiplikation. Beispiel:

$$\left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right] \left[\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right] = \left[\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right] \in G,$$

$$\left[\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right] \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right] \in G.$$

Dieses Beispiel zeigt auch gleich, dass G nicht kommutativ ist. ◯

(v) Bestimme für jedes Element seine Ordnung. Ist G zyklisch?

Lösung. Die Identität hat natürlich Ordnung eins. Die Spiegelungen $s_1, \ldots, s_4$ und die Drehung t_{180} um 180 Grad haben Ordnung zwei (Beispiel: $\left[\begin{smallmatrix} 0 & -1 \\ -1 & 0 \end{smallmatrix}\right] \left[\begin{smallmatrix} 0 & -1 \\ -1 & 0 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right]$). Die Drehung t_{90} um 90 Grad und die Drehung t_{270} um 270 Grad haben Ordnung vier. Insbesondere ist G nicht zyklisch, da kein Element Ordnung acht hat. ◯

(vi) Betrachte die Abbildungen

$$d_1\colon \begin{array}{ccc} G & \longrightarrow & \mathbb{R}, \\ M & \longmapsto & \det M, \end{array} \qquad d_2\colon \begin{array}{ccc} G & \longrightarrow & \mathbb{R}^\times, \\ M & \longmapsto & \det M, \end{array}$$

$$d_3\colon \begin{array}{ccc} G & \longrightarrow & \{1,-1\}, \\ M & \longmapsto & \det M, \end{array} \qquad d_4\colon \begin{array}{ccc} G & \longrightarrow & \mathbb{R}_{>0}, \\ M & \longmapsto & \det M. \end{array}$$

Wodurch wird ein Homorphismus von (welchen) Gruppen definiert und wodurch nicht? [Jeweils mit Begründung.]

Lösung.
- d_1 ist kein Homomorphismus. $\mathbb{R}$ ist eine Gruppe bezüglich Addition, aber beispielsweise ist $\det(\mathrm{id}\cdot\mathrm{id}) = 1 \neq 1+1 = \det\mathrm{id} + \det\mathrm{id}$. Bezüglich der Multiplikation ist $\mathbb{R}$ *keine* Gruppe, die Null stört.
- d_2 ist ein Homomorphismus. $\mathbb{R}^\times$ ist eine multiplikative Gruppe, und es gilt $\det MN = \det M \det N$ für $M, N \in G$.
- d_3 ist ein Homomorphismus. $\{1,-1\}$ ist bezüglich der Multiplikation eine Gruppe mit Einselement 1. Alle Matrizen in G haben Determinante 1 oder -1.
- d_4 ist nicht einmal wohldefiniert. Zwar ist $\mathbb{R}_{>0}$ eine multiplikative Gruppe, allerdings ist $-1 = \det s_1$ negativ und gar nicht in $\mathbb{R}_{>0}$. ◯

(vii) Bestimme den Kern $\ker d_2$ und das Bild $\operatorname{im} d_2$ von d_2.

Lösung. Der Kern $\ker d_2$ besteht aus allen Matrizen in G mit Determinante 1, also aus der Menge

$$\left\{\mathrm{id} = \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right], t_{90} = \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right], t_{180} = \left[\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right], t_{270} = \left[\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right]\right\}.$$

Dies sind die Identität und die Drehungen, also die orientierungserhaltenden Transformationen. Das Bild ist die Menge $\{1,-1\}$. ◯

(viii) Ist $\ker d_2$ eine Gruppe? Ist $\ker d_2$ kommutativ?

Lösung. Der Kern $\ker d_2$ ist eine zyklische Gruppe, erzeugt von $t_{90} = \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]$. Das ist einfach zu veranschaulichen: dreht man das Objekt vier mal um 90 Grad, erwischt man wieder die Ausgangsposition. Insbesondere ist $\ker d_2$ kommutativ. ◯

(ix) Welche Nebenklassen hat $\ker d_2$ in G?

Lösung. $\ker d_2$ hat Ordnung 4. Nach dem Satz von Lagrange hat $\ker d_2$ in G den Index 2, besitzt also 2 Nebenklassen. Eine dieser Nebenklassen ist $\ker d_2$ selber, die andere ist die Menge $\{s_1, s_2, s_3, s_4\}$ der Spiegelungen. ◯

(x) Bilden diese Nebenklassen eine Gruppe? Wenn ja, welche?

Lösung. Da der Kern ein Normalteiler ist, ist die Menge der Nebenklassen $G/\ker d_2$ eine Gruppe. Diese hat Ordnung 2 und ist nach dem Homomorphiesatz isomorph zu $\operatorname{im} d_2 = \{1, -1\}$ mit der multiplikativen Gruppenstruktur. Genauer: Die eine Nebenklasse ist der Kern selber, also die Menge der Drehungen. Die andere Nebenklasse ist die Menge der Spiegelungen (äquivalent dazu: die Menge der $M \in G$ mit Determinante -1). Die Bedeutung der Gruppenstruktur von $G/\ker d_2$ ist folgende: Schaltet man zwei Drehungen oder zwei Spiegelungen hintereinender, entsteht eine Drehung. Schaltet man dagen eine Drehung und eine Spiegelung hintereinander, entsteht eine Spiegelung. ◯

Sei $H := \left\{ \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right], \left[\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right] \right\}$

(xi) Ist H eine Gruppe? Ist H kommutativ?

Lösung. Die Menge H ist eine kommutative Gruppe der Ordnung 2. Diese Gruppe besteht aus der Identität und der Spiegelung s_2 um die y-Achse. Alle Gruppen der Ordnung zwei sind kommutativ. ◯

(xii) Welche Nebenklassen hat H in G?

Lösung. Die Gruppe G hat Ordnung 8, die Untergruppe H Ordnung 2. Also folgt aus dem Satz von Lagrange, dass H vier Linksnebenklassen in G hat. Wir berechnen:

$$H = s_2 H = \{\mathrm{id}, s_2\}, t_{90}H = s_3 H = \{t_{90}, s_3\},$$
$$t_{180}H = s_4 H = \{t_{180}, s_4\}\ t_{270}H = s_1 H = \{t_{270}, s_1\}$$

Die erste Identität folgt zum Beispiel aus der Rechnung:

$$t_{90} \circ s_2 = \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right] \left[\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 0 & -1 \\ -1 & 0 \end{smallmatrix}\right] = s_3.$$

Geometrisch bedeutet dies, dass die Spiegelung s_3 dasselbe ist wie eine Spiegelung an der y-Achse (s_2), gefolgt von einer Drehung um 90 Grad gegen den Uhrzeigersinn (t_{90}). Die Rechtsnebenklassen sind:

$$H = Hs_2 = \{\mathrm{id}, s_2\}, Ht_{90} = Hs_1 = \{t_{90}, s_1\},$$
$$Ht_{180} = Hs_4 = \{t_{180}, s_4\}\ Ht_{270} = Hs_3 = \{t_{270}, s_3\}.$$

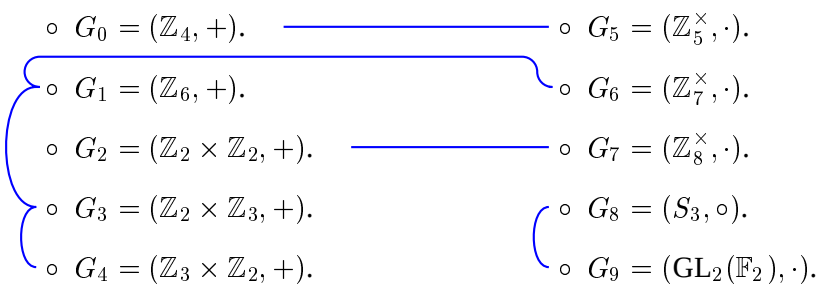
Daraus folgt, dass H kein Normalteiler in G ist. ◯

(xiii) Bilden diese Nebenklassen eine Gruppe? Wenn ja, welche?

Lösung. Die Nebenklassen bilden keine Gruppe, da H kein Normalteiler ist. Die Verknüpfung $[t_{90}H][t_{90}H]$ ist zum Beispiel nicht wohldefiniert. Nimmt man als Represäntanten dieser Nebenklasse das Element t_{90}, so müsste das Produkt $[t_{180}H]$ sein. Wird dagegen s_3 genommen, so ist das Ergebnis $[H]$. ◯

Aufgabe 7.2 (Verkleidungen). (8 Punkte)

Wir betrachten die folgenden Gruppen:



Entscheide, welche Gruppen isomorph sind, und gib jeweils einen Isomorphismus an oder einen Gegenbeweis. [Es sind deutlich weniger als 45 Fälle zu betrachten, wenn man eine geeignete Einteilung vornimmt! Beispielsweise muss man nicht jeden Isomorphismus explizit angeben, man kann ihn beispielsweise als Komposition von anderen angeben.]

Lexikon. Ein *Isomorphismus von Gruppen G und G'* ist ein bijektiver Homomorphismus von G nach G'. Zwei Gruppen G, G' heißen *isomorph* (griech. gleichförmig), in Zeichen $G \cong G'$, wenn es einen solchen Isomorphismus gibt. Zwei isomorphe Gruppen haben in jeder relevanten Hinsicht dieselben Eigenschaften. Beispielsweise sind zwei isomorphe Gruppen immer gleich groß und beide sind kommutativ oder keine. Ob allerdings die Elemente Äpfel oder Birnen, schwarz oder blau oder grün sind, ist nicht relevant.

Lexikon. Die *allgemeine lineare Gruppe* $\mathrm{GL}_n(F)$ *über dem Körper* F besteht aus den invertierbaren $n \times n$-Matrizen, deren Einträge Elemente aus F sind. Die zugehörige Operation ist die Multiplikation von Matrizen.

Lösung. Es handelt sich tatsächlich um nur vier unterschiedliche Gruppen: Da sind einmal die vierelementigen Gruppen: $G_0 \cong G_5$ und $G_2 \cong G_7$. Die letzteren haben kein Element der Ordnung 4. Die übrigen Gruppen haben alle sechs Elemente: $G_1 \cong G_3 \cong G_4 \cong G_6$ und $G_8 \cong G_9$, aber letztere sind nicht kommutativ. Die Argumente belegen schon alle Nichtisomorphien. Wir fassen

die Antwort nochmal in folgender Tabelle zusammen:

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

Wir müssen nun noch ein paar Isomorphismen angeben:

$G_0 \cong G_5$**.** Beide Gruppen sind zyklisch und haben vier Elemente. Die Gruppe $G_5 = \{1, 2, 3, 4\}$ besitzt als einen Erzeuger die 2, da dieses Element die Ordnung vier hat. Ein Isomorphismus ist wie folgt gegeben:

$$f\colon \begin{array}{ccc} \mathbb{Z}_4 & \longrightarrow & \mathbb{Z}_5^\times, \\ i & \longmapsto & 2^i \end{array} .$$

Wegen der Beobachtung $f(i+j) = 2^{i+j} \bmod 5 = (2^i \bmod 5)(2^j \bmod 5) = f(i)f(j)$ ist f ein Homomorphismus. Man rechnet nun leicht nach, dass dies ein Isomorphismus ist: Dies ergibt sich zu Fuß durch eine kleine Wertetabelle:

$\mathbb{Z}_4 \ni i$	0	1	2	3
$\mathbb{Z}_5^\times \ni 2^i$	1	2	4	3

oder beflügelt so: Die Funktion f ist injektiv, da für $i \neq j$ folgt $2^i \bmod 5 \neq 2^j \bmod 5$ (sonst: $2^{i-j} \bmod 5 = 1 \bmod 5$ und die Ordnung von $2 \bmod 5$ wäre kleiner als 4). Auch ist f surjektiv: da $2 \bmod 5$ die Gruppe G_5 erzeugt, wird durch $2^j \bmod 5$ jedes Element getroffen.

Allgemeiner sind je zwei zyklische Gruppen gleicher endlicher Ordnung isomorph. Jeder Homomorphismus von solchen Gruppen gleicher Ordnung, der zwei Erzeuger aufeinander abbildet, ist bereits ein Isomorphismus.

$G_2 \cong G_7$**.** Beide Gruppen haben folgende Struktur: Die Ordnung ist vier, jedes Element ausser der Eins hat Ordnung 2, und die Verknüpfung je zwei solcher Elemente liefert das dritte. Folgende Abbildung ist also ein Isomorphismus von $G_2 = \{(0,0), (0,1), (1,0), (1,1)\}$ auf $G_7 = \{1, 3, 5, 7\}$:

$$(0,0) \mapsto 1,\ (0,1) \mapsto 3,\ (1,0) \mapsto 5,\ (1,1) \mapsto 7.$$

Es gibt insgesamt $6 = 3!$ verschiedene Isomorphismen von G_2 nach G_7.

$G_1 \cong G_6$. Die Gruppe $G_6 = (\mathbb{Z}_7^\times, \cdot)$ ist zyklisch der Ordnung 6, etwa erzeugt durch 3, womit $G_6 = \langle 3 \rangle$. Hier funktioniert wieder, wie in Teil (a), die Abbildung $i \mapsto x^i \bmod 7$, wobei x ein Erzeuger von $\mathbb{Z}_7^\times$ sei.

$G_1 \cong G_3$. Die Abbildung

$$f\colon \begin{array}{rcl} \mathbb{Z}_6 & \longrightarrow & \mathbb{Z}_2 \times \mathbb{Z}_3, \\ x \bmod 6 & \longmapsto & (x \bmod 2, x \bmod 3) \end{array}$$

ist ein Isomorphismus. Nach Aufgabe 6.2 sind $x \bmod 6 \mapsto x \bmod 2$ und $x \bmod 6 \mapsto x \bmod 3$ Homomorphismen und damit auch f. Nach dem Chinesischen Restsatz gibt es zu jedem $a, b \in \mathbb{Z}$ ein $x \in \mathbb{Z}$ mit $x \equiv a \bmod 2$ und $x \equiv b \bmod 3$, womit f surjektiv ist. Und für $a = b = 0$ folgt $6 \mid x$, sodass $x \bmod 6 = 0$ ist, womit f injektiv ist.

$G_3 \cong G_4$. Ein Isomorphismus ist durch die Vertauschung $(x, y) \mapsto (y, x)$ gegeben.

Aus den bisher gezeigten Isomorphismen folgen gleich eine Reihe weiter Isomorphismen. So folgt zum Beispiel aus $G_1 \cong G_3$ und und $G_1 \cong G_6$ auch $G_3 \cong G_6$. Insgesamt erhalten wir die Isomorphismen $G_1 \cong G_3 \cong G_4 \cong G_6$.

$G_8 \cong G_9$. Die Gruppe $G_9 = (\mathrm{GL}_2(\mathbb{F}_2), \cdot)$ besteht aus allen invertierbaren 2×2-Matrizen mit Einträgen in $\mathbb{F}_2$. Diese sind:

$$\mathrm{GL}_2(\mathbb{F}_2) = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \right\}$$

Wir stellen fest, dass es sechs Elemente gibt. Wir haben hier mal mit Maple die ganze Verknüpfungstafel ausgerechnet:

	$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$
$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$
$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$
$\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$
$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$
$\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$
$\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$	$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$	$\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$

Wir lesen ab, dass $\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \neq \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$, also ist $\mathrm{GL}_2(\mathbb{F}_2)$ nicht kommutativ. Ferner sind die Ordnungen 1 für die Identität, 2 für die drei folgenden und 3 für die letzten beiden Elemente. Das legt die Idee nahe, sich entsprechende Elemente der S_3 zu suchen und das zu einem Isomorphismus auszubauen. Beispielsweise können wir versuchen $s := \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ und (12) einander zuzuordnen und $t := \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}$ und (123). Da stimmen schon einmal die Ordnungen. Natürlich muss dann automatisch $\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} = t^2$ auf $(123)^2 = (132)$ abgebildet werden, damit es ein Homomorphismus werden kann. Wenn wir so fortfahren, erhalten wir die Abbildung

$$\varphi\colon \begin{array}{rcl} \mathrm{GL}_2(\mathbb{F}_2) & \longrightarrow & S_3, \\ s^i t^j & \longmapsto & (12)^i (123)^j \end{array}$$

mit der Wertetabelle

x	id	st	st^2	s	t	t^2
x	$\left[\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right]$	$\left[\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right]$	$\left[\begin{smallmatrix}1&0\\1&1\end{smallmatrix}\right]$	$\left[\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right]$	$\left[\begin{smallmatrix}0&1\\1&1\end{smallmatrix}\right]$	$\left[\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right]$
$\varphi(x)$	$()$	(23)	(13)	(12)	(123)	(132).

Wir müssen nun nachprüfen, dass es sich um einen Homomorphismus handelt, dass also für alle Paare $a, b \in \mathrm{GL}_2(\mathbb{F}_2)$ die Gleichung $\varphi(a \cdot b) = \varphi(a) \circ \varphi(b)$ erfüllt ist. Zum Teil ist das schon nach Konstruktion so.

Wir können jedes Element in $\mathrm{GL}_2(\mathbb{F}_2)$ als $s^i t^j$ schreiben. (Das prüft man einfach nach.) Wichtig ist nun, dass

- die Elemente s und (12) beide Ordnung zwei haben.
- die Elemente t und (123) beide Ordnung drei haben.
- die Gleichung $ts = st^2$ und entsprechend $(123)(12) = (12)(123)^2$ gilt. (Das zeigen die Gleichungen $tsts = \mathrm{id}$ und $(123)(12)(123)(12) = ()$.)

Daraus ergibt sich tatsächlich schon alles: Ist $a = s^i t^j$ und $b = s^k t^\ell$, dann ist $a \cdot b = s^i t^j s^k t^\ell$. Einerseits ist $\varphi(a) \circ \varphi(b) = \varphi(s^i t^j)\varphi(s^k t^\ell) = (12)^i (123)^j (12)^k (123)^\ell$. Andererseits ist im Fall $k = 0$ nun $a \cdot b = s^i t^{j+\ell}$ und $\varphi(a \cdot b) = \varphi(s^i t^{j+\ell}) = (12)^i (123)^{j+\ell} = (12)^i (123)^j (12)^0 (123)^\ell$ und im Fall $k = 1$ folgt $a \cdot b = s^{i+1} t^{2j+\ell}$ und $\varphi(a \cdot b) = \varphi(s^{i+1} t^{2j+\ell}) = (12)^{i+1} (123)^{2j+\ell} = (12)^i (123)^j (12)^1 (123)^\ell$. Damit ist φ ein Homorphismus. Und weil er offensichtlich bijektiv ist, sogar ein Isomorphismus.

Für die letzte Isomorphie ist der folgende Beweis viel eleganter, aber auch schwieriger zu finden.

$G_8 \cong G_9$. Die Gruppe $G_9 = (\mathrm{GL}_2(\mathbb{F}_2), \cdot)$ besteht aus allen invertierbaren 2×2-Matrizen mit Einträgen in $\mathbb{F}_2$. Diese sind:

$$\mathrm{GL}_2(\mathbb{F}_2) = \left\{ \begin{matrix} \left[\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right], \left[\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right], \left[\begin{smallmatrix}1&0\\1&1\end{smallmatrix}\right] \\ \left[\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right], \left[\begin{smallmatrix}0&1\\1&1\end{smallmatrix}\right], \left[\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right] \end{matrix} \right\}$$

Jede dieser Matrizen repräsentiert einen Isomorphismus des $\mathbb{F}_2$-Vektorraumes ${\mathbb{F}_2}^2$ auf sich selber. Die Elemente des Vektorraumes ${\mathbb{F}_2}^2$ sind:

$$v_0 = \left[\begin{smallmatrix}0\\0\end{smallmatrix}\right],\ v_1 = \left[\begin{smallmatrix}1\\0\end{smallmatrix}\right],\ v_2 = \left[\begin{smallmatrix}0\\1\end{smallmatrix}\right],\ v_3 = \left[\begin{smallmatrix}1\\1\end{smallmatrix}\right].$$

Insbesondere ist jede Matrix aus $\mathrm{GL}_2(\mathbb{F}_2)$ eine Bijektion auf ${\mathbb{F}_2}^2$. Da eine solche Matrix v_0 auf sich selber abbildet, induziert diese eine Bijektion der Menge $\{v_1, v_2, v_3\}$ auf sich selber. Somit entspricht jeder Matrix aus $\mathrm{GL}_2(\mathbb{F}_2)$ eine Permutation einer Menge $\{v_1, v_2, v_3\}$ mit drei Elementen, und so eine Permutation entspricht gerade einem Element aus S_3. Explizit kann der Isomorphismus wie folgt angegeben werden:

$$\left[\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right] \mapsto (), \left[\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right] \mapsto (23), \left[\begin{smallmatrix}1&0\\1&1\end{smallmatrix}\right] \mapsto (13)$$
$$\left[\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right] \mapsto (12), \left[\begin{smallmatrix}0&1\\1&1\end{smallmatrix}\right] \mapsto (123), \left[\begin{smallmatrix}1&1\\1&0\end{smallmatrix}\right] \mapsto (132).$$

Man kann nun direkt nachrechnen, dass die Verknüpfung der Permutationen der Multiplikation der zugehörigen Matrizen entspricht. ◯

Aufgabe 7.3 (Ordnung). (4 Punkte)

In einer Gruppe G sei ein Element x der Ordnung $a = \operatorname{ord} x$ gegeben. Zeige, dass für $e \in \mathbb{N}$ gilt

$$\operatorname{ord}(x^e) = \frac{a}{\operatorname{ggT}(e, a)}.$$

Tipp: Die Fälle $e \mid a$ und $\operatorname{ggT}(e, a) = 1$ aus der Vorlesung könnten hier helfen.

Lösung. Sei $g := \operatorname{ggT}(e, a)$ und $y := x^g$.

Da a von g geteilt wird, folgt: $\operatorname{ord} y = \operatorname{ord} x^g = (\operatorname{ord} x)/g = a/g$ (siehe Fall 1 der oben genannten Spezialfälle aus der Vorlesung.)

Weiter haben wir $x^e = y^{e/g}$. Wegen $\operatorname{ggT}(e, a) = g$ folgt jetzt aber $\operatorname{ggT}(a/g, e/g) = \operatorname{ggT}(\operatorname{ord} y, e/g) = 1$. Also folgt (siehe Fall 2 der oben genannten Spezialfälle aus der Vorlesung),

$$\operatorname{ord}(x^e) = \operatorname{ord}(y^{g/e}) = \operatorname{ord} y = a/g = \frac{a}{\operatorname{ggT}(a, e)},$$

und die Aussage ist bewiesen. ○