7. Übungsblatt zu Mathematik für Informatiker II, SS 2004

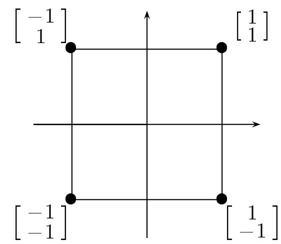
JOACHIM VON ZUR GATHEN & MICHAEL NÜSKEN

Abgabe bis Montag, 21. Juni 2004, 12^{23} Uhr
in den jeweils richtigen Kasten auf dem D1-Flur.

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.

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

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

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

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

(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.]

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

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

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

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

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?

(xii) Welche Nebenklassen hat H in G?

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

Aufgabe 7.2 (Verkleidungen). (8 Punkte)

Wir betrachten die folgenden Gruppen:

- $G_0 = (\mathbb{Z}_4, +)$.
- $G_1 = (\mathbb{Z}_6, +)$.
- $G_2 = (\mathbb{Z}_2 \times \mathbb{Z}_2, +)$.
- $G_3 = (\mathbb{Z}_2 \times \mathbb{Z}_3, +)$.
- $G_4 = (\mathbb{Z}_3 \times \mathbb{Z}_2, +)$.
- $G_5 = (\mathbb{Z}_5^\times, \cdot)$.
- $G_6 = (\mathbb{Z}_7^\times, \cdot)$.
- $G_7 = (\mathbb{Z}_8^\times, \cdot)$.
- $G_8 = (S_3, \circ)$.
- $G_9 = (\mathrm{GL}_2(\mathbb{F}_2), \cdot)$.

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.

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.

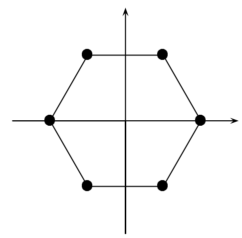
7. Übungsblatt zu Mathematik für Informatiker II, SS 2004, Mündlicher Teil

JOACHIM VON ZUR GATHEN & MICHAEL NÜSKEN

Mündliche Aufgabe 7.4 (Symmetrien).

Sei $S = \left\{ \left[\begin{smallmatrix}1\\0\end{smallmatrix}\right], \begin{bmatrix}\frac{1}{2}\\ \frac{1}{2}\sqrt{3}\end{bmatrix}, \begin{bmatrix}-\frac{1}{2}\\ \frac{1}{2}\sqrt{3}\end{bmatrix}, \left[\begin{smallmatrix}-1\\0\end{smallmatrix}\right], \begin{bmatrix}-\frac{1}{2}\\ -\frac{1}{2}\sqrt{3}\end{bmatrix}, \begin{bmatrix}\frac{1}{2}\\ -\frac{1}{2}\sqrt{3}\end{bmatrix} \right\} \subset \mathbb{R}^2$ die Menge der Ecken eines regelmäßigen Sechsecks. Wir betrachten die Menge

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



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

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

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

(iii) Erstelle eine Liste aller Elemente von G.

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

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

(vi) Betrachte die Abbildungen

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

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

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

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

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

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

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

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?

(xii) Welche Nebenklassen hat H in G?

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

Mündliche Aufgabe 7.5 (Verkleidungen).

Wir betrachten die folgenden Gruppen:

- $G_0 = (\mathbb{Z}_8, +)$.
- $G_1 = (\mathbb{Z}_{10}, +)$.
- $G_2 = (\mathbb{Z}_2 \times \mathbb{Z}_4, +)$.
- $G_3 = (\mathbb{Z}_2 \times \mathbb{Z}_5, +)$.
- $G_4 = (\mathbb{Z}_5 \times \mathbb{Z}_2, +)$.
- $G_5 = (\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, +)$.
- $G_6 = (\mathbb{Z}_{11}^\times, \cdot)$.
- $G_7 = (\mathbb{Z}_{15}^\times, \cdot)$.
- $G_8 = (\mathbb{Z}_{16}^\times, \cdot)$.
- $G_9 = (\mathrm{Sym(Quadrat)}, \circ)$ wie G in Aufgabe 7.1.
- $G_{10} = (\mathrm{Sym(Fünfeck)}, \circ)$ analog Aufgabe 7.1.
- $G_{11} = \left\{ \begin{matrix} (), (1234), (13)(24), (1432), \\ (12)(34), (14)(23), (13), (24) \end{matrix} \right\}$.
- $G_{12} = \left\{ \begin{matrix} (), (12345), (13524), (14253), \\ (15432), (25)(34), (13)(45), \\ (15)(24), (12)(35), (14)(23) \end{matrix} \right\}$.
- $G_{13} = (A_4, \circ)$, die Untergruppe der geraden Permutationen aus S_4 (siehe Übungsblatt 6).
- $G_{14} = (\mathrm{Sym(Sechseck)}, \circ)$ wie G in Mündliche Aufgabe 7.4.

Entscheide, welche Gruppen isomorph sind, und gib jeweils einen Isomorphismus an oder einen Gegenbeweis. **Lexikon.** Siehe Aufgabe 7.2.

Mündliche Aufgabe 7.6 (Ordnung).

Die Ordnung x eines Elementes einer Gruppe G ist ja bekanntlich der kleinste positive Exponent $e \in \mathbb{N}_{>0}$ mit $x^e = 1_G$. Andererseits erzeugt ein Element x nun aber auch die Untergruppe $\langle x \rangle = \left\{ \dots, x^{-2}, x^{-1}, x^0, x^1, x^2, \dots \right\}$ von G. Nach dem Satz von Lagrange ist deren Ordnung ein Teiler der Gruppengröße $\#G$.

(i) Zeige, dass $x^{\operatorname{ord} x} = 1_G$ gilt.

(ii) Zeige, dass $\# \langle x \rangle = \operatorname{ord} x$.

(iii) Zeige, dass die Ordnung $\operatorname{ord} x$ ein Teiler der Gruppengröße $\#G$ ist.