Aufgabe 1 (???)**.** Sei G die Isometriegruppe der Euklidische Ebene, unter der ein gleichseitiges Dreieck Δ invariant ist. Zeigen Sie, daß G zur symmetrischen Gruppe $\mathfrak{S}_3$ isomorph ist.

Lösung. Sei $T = \{A, B, C\}$ die Menge bestehend aus den drei Eckpunkten des Dreiecks. Es genügt einen Isomorphismus von G auf die symmetrische Gruppe $\mathfrak{S}_T$ anzugeben. Sei $\phi : G \to \mathfrak{S}_T, g \mapsto g|_T$ die Einschränkung von der Ebene auf die Punkte in T. Wir zeigen, daß ϕ ein Isomorphismus ist.
Zunächst stellen wir fest, daß ϕ wohldefiniert ist. In der Tat sendet jedes Element g der Gruppe G jeden Eckpunkt des Dreiecks Δ wieder auf einen Eckpunkt des Dreiecks Δ. Und da g bijektiv ist (als Isometrie), ist die Einschränkung auf die Eckpunkte auch wieder bijektiv. Also ist in der Tat $\phi(g) = g|_T \in \mathfrak{S}_T$ und es ist klar, daß ϕ ein Gruppenhomomorphismus ist.
Wir zeigen nun, daß er injektiv ist. Sei $\phi(g) = g|_T = \mathrm{id}_T$. Dann ist g eine Isometrie der Ebene mit mindestens drei Fixpunkten. Daher kann g nur die Identität sein.
Zeigen wir nun, daß ϕ surjektiv ist. Da $\mathfrak{S}_3$ von Transpositionen erzeugt wird, genügt es zu zeigen, daß die Transpositionen im Bild von ϕ sind. Betrachten wir zum Beispiel die Transposition $(A\ B) = \begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix}$. Ihr Urbild ist die Spiegelung an der Achse die orthogonal auf der Linie $[A, B]$ und durch C verläuft. Ähnlich für die übrigen Transpositionen.

Aufgabe 2 (Frühjahr 1973)**.** G sei eine Gruppe, $Q(G)$ das Erzeugnis der Quadrate:

$$Q(G) := \langle g^2\ ;\ g \in G \rangle.$$

(a) Man bestimme die Elemente von $Q(\mathfrak{S}_4)$, wobei $\mathfrak{S}_4$ die symmetrische Gruppe vierten Grades ist.

(b) Man beweise, daß $Q(G)$ bei jedem Automorphismus von G im ganzen festbleibt.

(c) Man bestätige, daß $Q(\mathfrak{A}_n) = \mathfrak{A}_n$ ist, wobei $\mathfrak{A}_n$ die alternierende Gruppe n-ten Grades ist.

(d) Man zeige: Hat G eine Untergruppe vom Index 2, so ist $Q(G) \neq G$.

Lösung. **(a)** Es ist

$$\begin{aligned}\mathfrak{S}_4 = \{&\mathrm{id}, (12), (13), (14), (23), (24), (34), (12)(34), (13)(24), (14)(23), (123), (132), (124), (142), (134),\\ &(143), (234), (243), (1234), (1243), (1324), (1342), (1423), (1432)\}\end{aligned}$$

Elemente der Ordnung 2 sind: $\{(12), (13), (14), (23), (24), (34), (12)(34), (13)(24), (14)(23)\}$, für dies gilt $x^2 = \mathrm{id}$.
Elemente der Ordnung drei sind: $\{(123), (132), (124), (142), (134), (143), (234), (243)\}$, für diese gilt

$$\begin{aligned}(123)^2 &= (132) \text{ und } (132)^2 = (123)\\ (124)^2 &= (142) \text{ und } (142)^2 = (124)\\ (134)^2 &= (143) \text{ und } (143)^2 = (134)\\ (234)^2 &= (243) \text{ und } (243)^2 = (234)\end{aligned}$$

Elemente der Ordnung 4 sind: $\{(1234), (1243), (1324), (1342), (1423), (1432)\}$, für diese gilt

$$\begin{aligned}(1234)^2 &= (13)(24) = (1432)^2\\ (1243)^2 &= (14)(23) = (1342)^2)\\ (1324)^2 &= (12)(34) = (1423)^2)\end{aligned}$$

Also ist

$$Q(\mathfrak{S}_4) = \langle \mathrm{id}, (13)(24), (14)(23), (12)(34), (123), (132), (124), (142), (134), (143), (234), (243) \rangle = \langle \mathfrak{A}_4 \rangle = \mathfrak{A}_4.$$

(b) Sei $\psi \in \mathrm{Aut}(G)$. Dann ist für $g \in G$ $\psi(g^2) = \psi(g)^2 \in Q(G)$. Also werden Erzeuger auf erzeuger abgebildet, und damit ist $\psi(Q(G)) \subset Q(G)$.

(c) Für jede Gruppe gilt $Q(G) \lhd G$: Für $g \in G$ ist die Konjugation mit g, ein Automorphismus von Gm nämlich $\kappa(g)(x) = gxg^{-1}$. Also folgt nach (b) $gQ(G)g^{-1} = \kappa(g)(Q(G)) \subset Q(G)$.

Da für $n \geqslant 5$ die alternierende Gruppe $\mathfrak{A}_n$ einfach ist, folgt $Q(\mathfrak{A}_n) = \mathfrak{A}_n$ oder $Q(\mathfrak{A}_n) = \{e\}$. Den letzten Fall können wir ausschließen, da $Q(\mathfrak{A}_n)$ alle Zakel ungerader Ordnung enthält, denn für einen solchen Zykel σ der ungeraden Ordnung n ist $\sigma = (\sigma^{\frac{n+1}{2}})^2$. Also $Q(\mathfrak{A}_n) = \mathfrak{A}_n$.
Für $\mathfrak{A}_i$, $i = 1, 2, 3, 4$, kann man das von Hand zeigen.

(d) Sei $H \subset G$ eine Untergruppe vom Index 2. Für jedes $x \in G \setminus H$ ist $G = H \cup xH = H \cup Hx$ disjunkte Vereinigung. Insbesondere $G \setminus H = xH = Hx$. Angenommen $x^2 \in G \setminus H$. Dann gibt $h \in H$ mit $x^2 = xh$, unmöglich, da dann $x = h \in H \cap xH$. Also ist $x^2 \in H$ und damit

$$Q(G) \subset H \subsetneq G.$$

Aufgabe 3 (Herbst 2013)**.** Zeigen Sie, daß die alternierende Gruppe A_4 keine Untergruppe der Ordnung 6 beztzt.

Lösung. Annahme A_4 enhält Untergruppe H der Ordnung 6. Dann ist $H \triangleleft A_4$. Da für die Klein'sche Vierergruppe V gilt $V \not\subseteq H$, ist $A_4 = VH = HV$, $V \cap H \triangleleft H$, $A_4/V \cong HV/V \cong H/H \cap V$ ist zyklische Gruppe der Ordnung 3, $|H \cap V| = 2$. Sei $h \in H \backslash (H \cap V)$. Wegen $3 = \operatorname{ord}(hH \cap V) \big| \operatorname{ord}(h)$ ist $\operatorname{ord}(h) \in \{3, 6\}$. In beiden Fällen ist H zyklisch: Das ist klar, wenn $\operatorname{ord}(h) = 6$. Falls $\operatorname{ord}(h) = 3$, dann gilt $[H : \langle h \rangle] = 2$, also $\langle h \rangle \triangleleft H$. Es folgt $H = \langle h \rangle \times (H \cap V)$, also $H \cong \mathbb{Z}/\mathbb{Z}3 \times \mathbb{Z}/\mathbb{Z}2 \cong \mathbb{Z}/\mathbb{Z}6$. Da $\mathfrak{S}_4$ kein Element der Ordnung 6 enthält, hat man einen Widerspruch. (Die Gruppe $\mathfrak{S}_4$ enthält Diedergruppen der Ordnung 6 aber keine zyklischen Gruppen der Ordnung 6.)

Aufgabe 4 (Herbst 2013)**.** (a) Eine Permutation sei das Produkt zweier disjunkter Zykel der teilerfremden Längen k und l. Welche Ordnung hat σ?

(b) Sei $\alpha(n)$ die größte Elementordnung in der symmetrischen Gruppe S_n. Man zeige $\lim_{n\to\infty} \frac{\alpha(n)}{n} = \infty$.

Lösung. **(a)** Sei $\sigma = \rho\tau$ Produkt eines k- und eines l-Zykels, die disjunkt sind. Dann vertauschen ρ und τ: $\rho\tau = \tau\rho$, und $\operatorname{ord}(\rho) = k$, $\operatorname{ord}(\tau) = l$. Es gilt

$$\sigma^{kl} = (\rho\tau)^{kl} = \rho\tau\rho\tau \cdots \rho\tau = \rho^{kl}\sigma^{kl} = (\rho^k)^l(\sigma^l)^k = \mathrm{id}\,.$$

Also $\operatorname{ord}(\sigma)|kl$. Sei $m \in \mathbb{Z}$ mit $\sigma^m = \mathrm{id}$. Dann $\mathrm{id} = \sigma^m = (\rho\tau)^m = \rho^m\tau^m$, also $\rho^m = (\tau^{-1})^m \in \langle\rho\rangle \cap \langle\tau\rangle = \{\mathrm{id}\}$. (Es ist $\langle\rho\rangle \cap \langle\tau\rangle = \{\mathrm{id}\}$ da $(k, l) = 1$.) Da $\operatorname{ord}(\rho) = k$ und $\operatorname{ord}(\tau) = \operatorname{ord}(\tau^{-1}) = l$ also $k|m$ und $l|m$, also $kl|m$, da $(k, l) = 1$. Damit $kl|\operatorname{ord}(\sigma)$. Zusammen folgt $\operatorname{ord}(\sigma) = kl$.

(b) Sei $m = \lfloor \frac{n-1}{2} \rfloor$. Da $m + (m + 1) \leqslant \frac{n-1}{2} + \frac{m+1}{2} = n$ kann dann in S_n ein Produkt σ aus disjunkten Zykeln der Länge m und $m+1$ gebildet werden. Die Zahlen m und $m+1$ sind teilerfremd. Mit **(a)** erhalten wir

$$\operatorname{ord}(\sigma) = m(m+1) > \frac{n-3}{2}\frac{n-1}{2} = \frac{1}{4}(n-3)(n-1) = \frac{1}{4}(n^2 - 4n + 3),$$

abgeschätzt mit $m > \frac{n-1}{2} - 1 = \frac{n-3}{2}$. Also

$$\frac{\alpha(n)}{n} > \frac{1}{4}(n - 4 + \frac{3}{n}, \forall n \in \mathbb{N}\,.$$

Wegen $\lim_{n\to\infty} \frac{1}{4}(n - 4 + \frac{3}{n} = \infty$ also $\lim_{n\to\infty} \frac{\alpha(n)}{n} = \infty$.

Aufgabe 5 (??)**.** Geben Sie eine Untergruppe von $\mathfrak{S}_7$ der Ordnung 21 an.

Lösung. Wir brauchen $a, b \in \mathfrak{S}_7$ mit $\operatorname{ord}(a) = 7$, $\operatorname{ord}(b) = 3$, und einen nichttrivialen Homomorphismus $\tau : \langle b\rangle \to \operatorname{Aut}(\langle a\rangle)$, oder $\langle a\rangle \to \operatorname{Aut}(\langle b\rangle)$.
Da $\operatorname{Aut}(\langle a\rangle) \cong (\mathbb{Z}/\mathbb{Z}7)^\times$ hat $\operatorname{Aut}(\langle a\rangle)$ ein Element der Ordnung 3, also gibt es so ein τ. Es gibt aber keinen nicht-trivialen Homomorphismus $\langle a\rangle \to \operatorname{Aut}(\langle b\rangle)$.
Sei $a = (1234567)$, $a^2 = (1357246)$, $b = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 3 & 5 & 7 & 2 & 4 & 6 \end{pmatrix} = (235)(476)$, dann gilt $bab^{-1} = a^2$, dh. $ba = a^2b$. Sei

$$\tau : \langle b\rangle \to \operatorname{Aut}(\langle a\rangle), \tau(b^z) = (\kappa_b)^z = \kappa_{b^z}\,.$$

Resultat: $G = \langle a, b\rangle = \{\mathrm{id}, a, \ldots, a^6, b, ab, \ldots, a^6b, b^2, \ldots, a^6b^2\}$ ist semidirektes Produkt von $\langle a\rangle \triangleleft G$ und $\langle b\rangle \subset G$.