Blatt #2, 24. Okt. 2002

**Aufgabe 5.**

(1) $\sigma = (1,4)(2,3,5), \rho = (2,5,3,4), \sigma^{-1} = (1,4)(2,5,3), \rho^{-1} = (2,4,3,5)$.

(2) Es ist
$\sigma \circ \rho = (1,4,3)$,
$\rho^{-1} \circ \sigma^2 = (3,4)$,
$\sigma^2 \circ \rho^{-1} = (2,4)$.

(3) Berechnung entweder direkt mit (2) oder durch Verwendung der Faktorisierung des Signums:

| $x$ | $\sigma$ | $\rho$ | $\sigma \circ \rho$ | $\rho^{-1} \circ \sigma^2$ | $\sigma^2 \circ \rho^{-1}$ |
|---|---|---|---|---|---|
| $\varepsilon_x$ | $-1$ | $-1$ | $1$ | $-1$ | $-1$ |

(4) Es ist $\sigma^2 = (2,5,3)$, $\sigma^3 = (1,4)$, $\sigma^4 = (2,3,5)$, $\sigma^5 = (1,4)(2,5,3)$, $\sigma^6 = 1$, also Ordnung $= 6$. Es ist $\rho^2 = (2,3)(5,4)$, $\rho^3 = (2,4,3,5)$, $\rho^4 = 1$, also Ordnung $= 4$.

**Aufgabe 6.** (1)

| $\circ$ | $1$ | $(1,2,3)$ | $(1,3,2)$ | $(1,2)$ | $(1,3)$ | $(2,3)$ |
|---|---|---|---|---|---|---|
| $1$ | $1$ | $(1,2,3)$ | $(1,3,2)$ | $(1,2)$ | $(1,3)$ | $(2,3)$ |
| $(1,2,3)$ | $(1,2,3)$ | $(1,3,2)$ | $1$ | $(1,3)$ | $(2,3)$ | $(1,2)$ |
| $(1,3,2)$ | $(1,3,2)$ | $1$ | $(1,2,3)$ | $(2,3)$ | $(1,2)$ | $(1,3)$ |
| $(1,2)$ | $(1,2)$ | $(2,3)$ | $(1,3)$ | $1$ | $(1,3,2)$ | $(1,2,3)$ |
| $(1,3)$ | $(1,3)$ | $(1,2)$ | $(2,3)$ | $(1,2,3)$ | $1$ | $(1,3,2)$ |
| $(2,3)$ | $(2,3)$ | $(1,3)$ | $(1,2)$ | $(1,3,2)$ | $(1,2,3)$ | $1$ |

(2)

| $\sigma$ | $1$ | $(1,2)$ | $(1,3)$ | $(2,3)$ | $(1,2,3)$ | $(1,3,2)$ |
|---|---|---|---|---|---|---|
| $\varepsilon_\sigma$ | $1$ | $-1$ | $-1$ | $-1$ | $1$ | $1$ |
| Ordnung | $1$ | $2$ | $2$ | $2$ | $3$ | $3$ |

(3) Nach Aufgabe 4.(1) muß die Anzahl der Elemente einer Untergruppe $\#\mathcal{S}_3 = 6$ teilen. Wir erhalten $G_1 = \{1\}$, $G_2 = \mathcal{S}_3$, $G_3 = \{1,(1,2)\}$, $G_4 = \{1,(1,3)\}$, $G_5 = \{1,(2,3)\}$, $G_6 = \{1,(1,2,3),(1,3,2)\}$.

(4) Für $\sigma, \rho, \tau \in \mathcal{S}_3$ gilt $g_\sigma(\tau \circ \rho) = \sigma \circ \tau \circ \rho \circ \sigma^{-1} = (\sigma \circ \tau \circ \sigma^{-1}) \circ (\sigma \circ \rho \circ \sigma^{-1}) = g_\sigma(\tau) \circ g_\sigma(\rho)$, also ist $g_\sigma$ ein Gruppenmorphismus von $\mathcal{S}_3$ nach $\mathcal{S}_3$. Aus $g_\sigma \circ g_{\sigma^{-1}} = g_{\sigma^{-1}} \circ g_\sigma = 1_{\mathcal{S}_3}$ folgt, daß $g_\sigma$ bijektiv ist. Damit ist $g$ wohldefiniert.

- Für $\rho, \sigma \in \mathcal{S}_3$ gilt für alle $\tau \in \mathcal{S}_3$

$$g_{\sigma\circ\rho}(\tau) = (\sigma \circ \rho) \circ \tau \circ (\sigma \circ \rho)^{-1} = \sigma \circ \rho \circ \tau \circ \rho^{-1} \circ \sigma^{-1} = g_\sigma(\rho \circ \tau \circ \rho^{-1}) = g_\sigma(g_\rho(\tau)) = (g_\sigma \circ g_\rho)(\tau),$$

  also ist $g$ ein Gruppenhomomorphismus.
- Es ist $\operatorname{Kern} g = \{\sigma \in \mathcal{S}_3 \mid g_\sigma = 1_{\mathcal{S}_3}\} = \{\sigma \in \mathcal{S}_3 \mid g_\sigma(\tau) = \tau \text{ für alle } \tau \in \mathcal{S}_3\}$. Nun gilt $g_\sigma(\tau) = \tau$ für alle $\tau \in \mathcal{S}_3 \Leftrightarrow \sigma \circ \tau = \tau \circ \sigma$ für alle $\tau \in \mathcal{S}_3$. Aus der Verknüpfungstafel liest man $\sigma = 1$ ab. Damit ist $g$ injektiv.
- Jedes $\tau \in \mathcal{S}_3$ kann eindeutig als $\tau = (1,2)^k \circ (1,2,3)^l$ mit $k \in [0,1], l \in [0,2]$ geschrieben werden. Damit ist für $a \in \operatorname{Aut}(\mathcal{S}_3)$ dann $a(\tau) = a((1,2)^k \circ (1,2,3)^l) = a((1,2))^k \circ a((1,2,3))^l$, Folglich ist $a$ mit Angabe von $a((1,2))$ und $a((1,2,3))$ eindeutig bestimmt. Da die Ordnung unter $a$ erhalten bleibt, gilt: $a((1,2)) \in \{(1,2),(1,3),(2,3)\}$, $a((1,2,3)) \in \{(1,2,3),(1,3,2)\}$. Man hat also ingesamt $3 \cdot 2 = 6$ Möglichkeiten. Damit ist $\#\operatorname{Aut}(\mathcal{S}_3) \leq \#\mathcal{S}_3$. Da $g$ injektiv ist folgt die Surjektivität.

**Aufgabe 7.** Sei $M$ Menge.

(1)

| $\cdot$ | $\emptyset$ | $\{1\}$ | $\{2\}$ | $\{1,2\}$ |
|---|---|---|---|---|
| $\emptyset$ | $\emptyset$ | $\{1\}$ | $\{2\}$ | $\{1,2\}$ |
| $\{1\}$ | $\{1\}$ | $\emptyset$ | $\{1,2\}$ | $\{2\}$ |
| $\{2\}$ | $\{2\}$ | $\{1,2\}$ | $\emptyset$ | $\{1\}$ |
| $\{1,2\}$ | $\{1,2\}$ | $\{2\}$ | $\{1\}$ | $\emptyset$ |

(2) Sei $A \in \mathfrak{P}(M)$. Es ist $A \cdot \emptyset = \emptyset \cdot A = A$, also $\emptyset =: 1$. Weiter ist $A^2 = (A \setminus A) \cup (A \setminus A) = \emptyset = 1$.

(3) Zur Assoziativität: Für $A, B, C \in \mathfrak{P}(M)$ gilt

$$\begin{aligned} A \cdot (B \cdot C) &= \Big(A \setminus \big((B \setminus C) \cup (C \setminus B)\big)\Big) \cup \Big(\big((B \setminus C) \cup (C \setminus B)\big) \setminus A\Big) \\ &= \dots \\ &= (A \setminus (B \cup C)) \cup (B \setminus (A \cup C)) \cup (C \setminus (A \cup B)) \cup (A \cap B \cap C) \\ &= \dots \\ &= (A \cdot B) \cdot C \end{aligned}$$

Nach (1) ist $\emptyset$ ein neutrales Element und $A^{-1} = A$. Also ist $(\mathfrak{P}(M), \cdot)$ eine Gruppe und – da $A^2 = 1$ nach (1) – nach Aufgabe 4.(2) auch abelsch (, was man auch direkt sieht).

(4) Es ist $\emptyset \neq \mathfrak{P}(N) \subseteq \mathfrak{P}(M)$, und für $A, B \in \mathfrak{P}(N)$, d.h. $A, B \subseteq N$ gilt

$$A \cdot B^{-1} = A \cdot B = \underbrace{(A \setminus B)}_{\subseteq N} \cup \underbrace{(B \setminus A)}_{\subseteq N} \in \mathfrak{P}(N),$$

also ist $\mathfrak{P}(N)$ Untergruppe von $\mathfrak{P}(M)$.

**Aufgabe 8.** Sei $s_0 = 1$, $s_1 = (1,2)(3,4)$, $s_2 = (1,3)(2,4)$, $s_3 = (1,4)(2,3)$.

(1) Es ist $V \subseteq \mathcal{S}_4$. Man bemerke, daß $s_i^2 = 1$, d.h. $s_i^{-1} = s_i$ für $i \in [0,3]$. $V$ ist also Untergruppe wenn stets $s_i \circ s_j \in V$ gilt. Dies rechnet man nach und erhält die Verknüpfungstafel:

| $\circ$ | $s_0$ | $s_1$ | $s_2$ | $s_3$ |
|---|---|---|---|---|
| $s_0$ | $s_0$ | $s_1$ | $s_2$ | $s_3$ |
| $s_1$ | $s_1$ | $s_0$ | $s_3$ | $s_2$ |
| $s_2$ | $s_2$ | $s_3$ | $s_0$ | $s_1$ |
| $s_3$ | $s_3$ | $s_2$ | $s_1$ | $s_0$ |

(2) Es ist

$$U = \{(1,2,3), (1,3,2), (1,2,4), (1,4,2), (1,3,4), (1,4,3), (2,3,4), (2,4,3)\} \cup V.$$

Seien $\rho, \sigma \in U$. Dann ist $\varepsilon_{\rho \circ \sigma^{-1}} = \varepsilon_\rho \varepsilon_{\sigma^{-1}} = \varepsilon_\rho \varepsilon_\sigma = 1$, also ist $\rho \circ \sigma^{-1} \in U$.

(3) Es gibt kein Element der Ordnung 5 in $\mathcal{S}_4$. Es kommen nur folgende Typen von Elementen vor:

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

Diese haben Ordnung $1, 2, 3, 2, 4$, respektive.

Alternativ: Betrachte für $x \in \mathcal{S}_4$ die Menge $G_x := \{x^m \mid m \in \mathbf{Z}\}$. Da für $n, m \in \mathbf{Z}$ gilt, daß $x^m x^{-n} = x^{m-n} \in G_x$, ist $G_x \leqslant \mathcal{S}_4$ Untergruppe. Die Ordnung von $x$ ist gleich der Anzahl der Elemente in $G_x$. Nach Aufgabe 4.(1) gilt: $\#G_x$ teilt $\#\mathcal{S}_4 = 24$. Also kommen für die Ordnung von $x$ nur $1, 2, 3, 4, 6, 8, 12$ oder $24$ in Frage, und 5 nicht.