6. Die Symmetrische Gruppe

Erinnerung: Ist $X \neq \varnothing$ eine Menge und $S_X = \{f : X \to X \mid f \text{ ist bijektiv}\}$, so ist $(S_X, \circ)$ eine Gruppe und wird als symmetrische Gruppe bezeichnet. Statt $S_{\{1,\dots,n\}}$ schreibt man kurz S_n. Die Gruppe S_n hat Ordnung $|S_n| = n!$.

Satz 38: Jede Gruppe G ist zu einer Untergruppe der symmetrischen Gruppe S_G isomorph.

Beweis: Es sei $\varphi : G \to S_G$ definiert als $\varphi(a) = \sigma_a$, wobei $\sigma_a(x) = ax \ \forall x \in G$. Dann ist $\sigma_a \in S_G$, denn $\sigma_a(x) = \sigma_a(y) \Rightarrow ax = ay \Rightarrow x = y$ und $\sigma_a(a^{-1}x) = a(a^{-1}x) = x \ \forall x \in G$. Weiters ist φ ein Homomorphismus, da

$$\varphi(ab)(x) = \sigma_{ab}(x) = (ab)x = a(bx) = \sigma_a\big(\sigma_b(x)\big) = (\sigma_a \circ \sigma_b)(x) = \big(\varphi(a) \circ \varphi(b)\big)(x)$$

für alle $x \in G$ und daher $\varphi(ab) = \varphi(a) \circ \varphi(b) \ \forall a, b \in G$. Nach Lemma 25 (i) ist $\varphi(G) \leq S_G$. Schließlich ist φ injektiv, denn $\varphi(a) = \mathrm{id}_G \Rightarrow \sigma_a = \mathrm{id}_G \Rightarrow ax = x \ \forall x \in G \Rightarrow a = ae = e$, d.h. $\ker \varphi = \{e\}$. Daher ist $\varphi(G) \cong G$.

Notation: Ein $\sigma \in S_n$ kann man als

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

notieren. Die Verknüpfung von $\sigma, \tau \in S_n$ ergibt sich als

$$\begin{aligned} \sigma \circ \tau &= \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & \cdots & n \\ \tau(1) & \tau(2) & \cdots & \tau(n) \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(\tau(1)) & \sigma(\tau(2)) & \cdots & \sigma(\tau(n)) \end{pmatrix}. \end{aligned}$$

Das Inverse zu

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

ist

$$\sigma^{-1} = \begin{pmatrix} \sigma(1) & \sigma(2) & \cdots & \sigma(n) \\ 1 & 2 & \cdots & n \end{pmatrix}.$$

(Um die übliche Darstellung zu erhalten, muss man die Spalten so umordnen, dass in der ersten Zeile $1\ 2\ \cdots\ n$ steht.) Für das neutrale Element der Gruppe S_n schreiben wir

$$\varepsilon = \begin{pmatrix} 1 & 2 & \cdots & n \\ 1 & 2 & \cdots & n \end{pmatrix}.$$

Beispiele: 1) In dieser Notation ist

$$S_3 = \left\{ \varepsilon, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}$$

2) In der Gruppe S_6 ist

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 3 & 4 & 2 & 1 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 2 & 5 & 6 & 1 \end{pmatrix}.$$

Bemerkung: Permutationen $\sigma \in S_n$ werden manchmal auch als $\sigma = \big(\sigma(1), \dots, \sigma(n)\big)$ notiert. Diese Notation wird in dieser Vorlesung *nicht* verwendet.

Definition: Ein $\sigma \in S_n$ wird k-Zyklus (oder kurz Zyklus) genannt, wenn $k \leq n$ und wenn es k paarweise verschiedene $i_1, \dots, i_k \in \{1, \dots, n\}$ gibt, derart dass

$\sigma(i_\alpha) = i_{\alpha+1}$ für $1 \leq \alpha \leq k-1$, $\sigma(i_k) = i_1$ und $\sigma(j) = j$ für $j \in \{1, \dots, n\} \setminus \{i_1, \dots, i_k\}$.

Man schreibt dafür $\sigma = (i_1\ i_2\ \cdots\ i_k)$.

Lemma 39: Es seien $\sigma, \tau \in S_n$ zwei elementfremde Zyklen, d.h.

$$\sigma = (i_1\ \cdots\ i_k),\ \tau = (j_1\ \cdots\ j_\ell) \ \text{ und } \ \{i_1, \dots, i_k\} \cap \{j_1, \dots, j_\ell\} = \varnothing.$$

Dann gilt $\sigma \circ \tau = \tau \circ \sigma$.

Beweis: Es ist

$$(\sigma \circ \tau)(i_\alpha) = (\tau \circ \sigma)(i_\alpha) = \begin{cases} i_{\alpha+1} & \text{für } 1 \leq \alpha < k, \\ i_1 & \text{für } \alpha = k, \end{cases}$$

$$(\sigma \circ \tau)(j_\beta) = (\tau \circ \sigma)(j_\beta) = \begin{cases} j_{\beta+1} & \text{für } 1 \leq \beta < \ell, \\ j_1 & \text{für } \beta = \ell, \end{cases}$$

und $(\sigma \circ \tau)(m) = (\tau \circ \sigma)(m) = m$ für $m \in \{1, \dots, n\} \setminus \big(\{i_1, \dots, i_k\} \cup \{j_1, \dots, j_\ell\}\big)$.

Definition: Ein 2-Zyklus $\tau \in S_n$ wird Transposition genannt. (Ist τ eine Transposition, so gibt es also $i, j \in \{1, \dots, n\}$, $i \neq j$, derart dass $\tau(i) = j$, $\tau(j) = i$ und $\tau(m) = m$ für $m \in \{1, \dots, n\} \setminus \{i, j\}$ und man schreibt $\tau = (i\ j)$.)

Satz 40: Jede Permutation $\sigma \in S_n$ lässt sich als Produkt paarweise elementfremder Zyklen schreiben. Diese Darstellung ist bis auf die Reihenfolge der Zyklen eindeutig.

Beweis: Wir führen auf $\{1, \dots, n\}$ die Relation $\sim$ ein, die durch

$$i \sim j \quad :\Longleftrightarrow \quad \exists \alpha \in \mathbb{Z} : j = \sigma^\alpha(i)$$

gegeben ist. Die Relation $\sim$ ist eine Äquivalenzrelation (denn $i = \sigma^0(i)$ $\forall i \in \{1, \dots, n\}$, $j = \sigma^\alpha(i) \Rightarrow i = \sigma^{-\alpha}(j)$ und $j = \sigma^\alpha(i)$, $k = \sigma^\beta(j) \Rightarrow k = \sigma^\beta\big(\sigma^\alpha(i)\big) = \sigma^{\alpha+\beta}(i)$), deren Äquivalenzklassen Bahnen genannt werden.
Es seien $B_1, \dots, B_s$ diese Bahnen und $i_\alpha = \min B_\alpha$ für $1 \leq \alpha \leq s$. Betrachte nun die Folge

$$i_\alpha, \sigma(i_\alpha), \sigma^2(i_\alpha) = \sigma\big(\sigma(i_\alpha)\big), \sigma^3(i_\alpha), \dots.$$

Da B_α endlich ist, muss es ein $r \geq 0$ mit der Eigenschaft

$$\sigma^{r+1}(i_\alpha) \in \big\{i_\alpha, \sigma(i_\alpha), \sigma^2(i_\alpha), \dots, \sigma^r(i_\alpha)\big\}$$

geben. Es sei r_α das Minimum aller $r \geq 0$ mit dieser Eigenschaft (für $1 \leq \alpha \leq s$). Dann muss $\sigma^{r_\alpha+1}(i_\alpha) = i_\alpha$ gelten. (Denn wäre $\sigma^{r_\alpha+1}(i_\alpha) = \sigma^\ell(i_\alpha)$ für ein $\ell \in \{1, \dots, r_\alpha\}$, so würde $\sigma^{r_\alpha+1-\ell}(i_\alpha) = i_\alpha$ folgen, was der Minimalität von r_α widersprechen würde.) Es folgt, dass σ die Darstellung

$$\sigma = \big(i_1\ \sigma(i_1)\ \sigma^2(i_1)\ \cdots\ \sigma^{r_1}(i_1)\big) \circ \big(i_2\ \sigma(i_2)\ \sigma^2(i_2)\ \cdots\ \sigma^{r_2}(i_2)\big) \circ \cdots \\ \cdots \circ \big(i_s\ \sigma(i_s)\ \sigma^2(i_s)\ \cdots\ \sigma^{r_s}(i_s)\big)$$

besitzt (womit die Existenz bewiesen ist). Die Eindeutigkeit folgt aus der Tatsache, dass es sich bei

$$\{1, \dots, n\} = \bigcup_{\alpha=1}^{s} \big\{i_\alpha, \sigma(i_\alpha), \sigma^2(i_\alpha), \dots, \sigma^{r_\alpha}(i_\alpha)\big\}$$

um die Vereinigung paarweise disjunkter Äquivalenzklassen bezüglich $\sim$ handelt.

Beispiel: Es ist

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 8 & 2 & 7 & 5 & 6 & 1 \end{pmatrix} = (1\ 3\ 8) \circ (2\ 4) \circ (5\ 7\ 6).$$

Bemerkung: Zyklen der Länge 1 (d.h. Fixpunkte) werden in dieser Schreibweise nicht notiert, d.h. für $\left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{smallmatrix}\right)$ schreibt man $(1\ 2)$ und

$$S_3 = \big\{\varepsilon, (1\ 2), (1\ 3), (2\ 3), (1\ 2\ 3), (1\ 3\ 2)\big\}.$$

Bei paarweise disjunkten Zyklen werden wir die Verknüpfung oft nicht notieren, d.h. im obigen Beispiel würde man $(1\ 3\ 8)(2\ 4)(5\ 7\ 6)$ schreiben.

Beispiele: 1) Auch in dieser Notation kann man die Verknüpfung von Permutationen gut berechnen. Das obige Beispiel aus der Gruppe S_6 würde als

$$(1\ 6\ 3\ 4\ 2\ 5) \circ (1\ 6\ 5)(2\ 3\ 4) = (1\ 3\ 2\ 4\ 5\ 6)$$

geschrieben werden.
2) In $(1\ 4\ 7\ 6\ 3) \circ (2\ 4\ 3) \circ (4\ 5\ 8\ 1) = (2\ 7\ 6\ 3)(4\ 5\ 8)$ sind mehrere 1-Zyklen nicht notiert worden, z.B. beim Ergebnis rechts (1).

Korollar 41: (i) Die Gruppe S_n wird von den Transpositionen erzeugt.
(ii) $S_n = \big\langle (1\ 2), (1\ 3), \dots, (1\ n) \big\rangle$.
(iii) $S_n = \big\langle (1\ 2), (2\ 3), \dots, (n-1\ n) \big\rangle$.

Beweis: (i) Ist $(i_1\ i_2\ \cdots\ i_r) \in S_n$ ein Zyklus, so gilt

$$(i_1\ i_2\ \cdots\ i_r) = (i_1\ i_2) \circ (i_2\ i_3) \circ \cdots \circ (i_{r-1}\ i_r).$$

Die Behauptung folgt aus Satz 40.
(ii) Für $1 < i < j \leq n$ ist $(i\ j) = (1\ i) \circ (1\ j) \circ (1\ i)$. Die Behauptung folgt aus (i).
(iii) Für $1 \leq i < j \leq n$ mit $j > i+1$ ist

$$\begin{aligned}(i\ j) = (i\ i+1) \circ (i+1\ i+2) \circ \cdots \\ \cdots \circ (j-2\ j-1) \circ (j-1\ j) \circ (j-2\ j-1) \circ \cdots \\ \cdots \circ (i+1\ i+2) \circ (i\ i+1).\end{aligned}$$

Die Behauptung folgt aus (i).

Bemerkung: Die Darstellung einer Permutation als Produkt von Transpositionen ist nicht eindeutig, da (für $n \geq 3$) z.B. $(2\ 3) = (1\ 2) \circ (1\ 3) \circ (1\ 2)$ gilt.

Definition: Für $\sigma \in S_n$ sei $\operatorname{sgn}\sigma$ (das Signum von σ) als $(-1)^w$ definiert, wobei w die Anzahl der Paare (i,j) mit $1 \leq i < j \leq n$ und $\sigma(i) > \sigma(j)$ bezeichnet.

Lemma 42: Für $\sigma \in S_n$ gilt

$$\operatorname{sgn}\sigma = \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i}.$$

Beweis: Im Zähler und Nenner treten (bis auf das Vorzeichen) die selben Differenzen auf. Für jedes Paar (i,j) mit $1 \leq i < j \leq n$ und $\sigma(i) > \sigma(j)$ wechselt das Vorzeichen einmal.

Satz 43: Die Abbildung $\operatorname{sgn} : S_n \to \{+1, -1\}$ ist ein Homomorphismus, d.h.

$$\operatorname{sgn}(\sigma \circ \tau) = \operatorname{sgn}\sigma \cdot \operatorname{sgn}\tau \ \forall \sigma, \tau \in S_n.$$

Für $n \geq 2$ ist sgn ein Epimorphismus.

Beweis: Für $\sigma, \tau \in S_n$ ist

$$\begin{aligned}\operatorname{sgn}(\sigma \circ \tau) &= \prod_{1 \leq i < j \leq n} \frac{(\sigma \circ \tau)(j) - (\sigma \circ \tau)(i)}{j - i} \\ &= \prod_{1 \leq i < j \leq n} \frac{(\sigma \circ \tau)(j) - (\sigma \circ \tau)(i)}{\tau(j) - \tau(i)} \prod_{1 \leq i < j \leq n} \frac{\tau(j) - \tau(i)}{j - i} \\ &= \prod_{1 \leq i < j \leq n} \frac{\sigma(j) - \sigma(i)}{j - i} \prod_{1 \leq i < j \leq n} \frac{\tau(j) - \tau(i)}{j - i} = (\operatorname{sgn}\sigma) \cdot (\operatorname{sgn}\tau).\end{aligned}$$

Ist $n \geq 2$, so ist $\operatorname{sgn}\varepsilon = +1$ und $\operatorname{sgn}(1\ 2) = -1$, d.h. sgn ist surjektiv.

Lemma 44: (i) Ist $\tau \in S_n$ eine Transposition, so ist $\operatorname{sgn}\tau = -1$.
(ii) Ist $\sigma \in S_n$ ein r-Zyklus, so ist $\operatorname{sgn}\sigma = (-1)^{r+1}$.

Beweis: (i) Ist $\tau = (i\ j)$ (mit $1 \leq i < j \leq n$), so haben die Paare

$$(i, i+1), (i+1, j), (i, i+2), (i+2, j), \dots, (i, j-1), (j-1, j) \text{ und } (i, j)$$

die Eigenschaft aus der Definition des Signum, d.h. $2 \nmid w$ und $\operatorname{sgn}\tau = -1$.
(ii) Nach (i) ist die Behauptung für $r = 2$ korrekt. Nach dem Beweis von Korollar 41 (i) gibt es Transpositionen $\tau_1, \dots, \tau_{r-1} \in S_n$, derart dass $\sigma = \tau_1 \circ \cdots \circ \tau_{r-1}$. Aus Satz 43 folgt

$$\operatorname{sgn}\sigma = \prod_{i=1}^{r-1} \operatorname{sgn}\tau_i \overset{\text{(i)}}{=} (-1)^{r-1} = (-1)^{r+1}.$$

Definition: Ein $\sigma \in S_n$ heißt gerade wenn $\operatorname{sgn}\sigma = +1$ und ungerade wenn $\operatorname{sgn}\sigma = -1$.

Korollar 45: Es sei $\sigma \in S_n$ und $\sigma = \tau_1 \circ \cdots \circ \tau_r$ mit Transpositionen $\tau_1, \dots, \tau_r \in S_n$. Dann gelten:
(i) σ ist gerade $\Leftrightarrow$ r ist gerade.
(ii) σ ist ungerade $\Leftrightarrow$ r ist ungerade.

Beweis: Nach Satz 43 und Lemma 44 (i) ist $\operatorname{sgn}\sigma = (-1)^r$ und daher

$$\operatorname{sgn}\sigma = +1 \Leftrightarrow r \text{ ist gerade und } \operatorname{sgn}\sigma = -1 \Leftrightarrow r \text{ ist ungerade.}$$

Definition: Für $n \geq 1$ wird $(A_n, \circ)$ mit

$$A_n = \{\sigma \in S_n \mid \sigma \text{ ist gerade}\} = \{\sigma \in S_n \mid \operatorname{sgn}\sigma = +1\}$$

als alternierende Gruppe bezeichnet.

Satz 46: (i) Für $n \geq 1$ ist $A_n \trianglelefteq S_n$.
(ii) Für $n \geq 2$ ist $|A_n| = \frac{n!}{2}$.
(iii) Für $n \geq 3$ wird A_n von den 3-Zyklen erzeugt.
(iv) Für $n \geq 3$ ist $A_n = \big\langle (1\ 2\ 3), (1\ 2\ 4), (1\ 2\ 5), \dots, (1\ 2\ n) \big\rangle$.
(v) $A_1 = \{\varepsilon\}$, $A_2 = \{\varepsilon\}$ und $A_3 \cong \mathbb{Z}_3$.
(vi) A_n ist abelsch für $n \in \{1, 2, 3\}$ und nicht abelsch für $n \geq 4$.

Beweis: (i) Folgt aus $A_n = \ker \operatorname{sgn}$ und Lemma 26 (i).
(ii) Für $n \geq 2$ gilt nach Satz 43 und Korollar 28 $S_n/A_n \cong \{+1, -1\}$ und daher nach Korollar 19 (i)

$$n! = |S_n| = \big|S_n/A_n\big| \cdot |A_n| = 2|A_n|.$$

(iii) Wir zeigen zunächst: Sind $\tau_1, \tau_2 \in S_n$ zwei Transpositionen, so kann man $\tau_1 \circ \tau_2$ als Verknüpfung von 3-Zyklen schreiben. Sind $i, j, k, \ell \in \{1, \dots, n\}$ paarweise verschieden, so

ist $(i\ j) \circ (k\ \ell) = (i\ k\ j) \circ (i\ k\ \ell)$. Sind $i, j, k \in \{1, \dots, n\}$ paarweise verschieden, so ist $(i\ j) \circ (i\ k) = (i\ k\ j)$. Ist $\tau_1 = \tau_2$, so ist $\tau_1 \circ \tau_2 = \varepsilon$. Wegen Korollar 41 (i) und Korollar 45 (i) kann jedes $\sigma \in A_n$ als Produkt einer geraden Zahl von Transpositionen dargestellt werden und daher (nach dem schon Gezeigten) als Produkt von 3-Zyklen.
(iv) Jeder 3-Zyklus in A_n hat eine der Gestalten

$$(1\ 2\ a), (1\ a\ 2), (1\ a\ b), (2\ a\ b) \text{ oder } (a\ b\ c),$$

wobei $a, b, c \geq 3$ paarweise verschieden sein sollen. Die Behauptung folgt aus (iii) und den Identitäten

$$(1\ a\ 2) = (1\ 2\ a)^2,\ (1\ a\ b) = (1\ 2\ b) \circ (1\ 2\ a)^2,\ (2\ a\ b) = (1\ 2\ b)^2 \circ (1\ 2\ a)$$

und

$$(a\ b\ c) = (1\ 2\ a)^2 \circ (1\ 2\ c) \circ (1\ 2\ b)^2 \circ (1\ 2\ a).$$

(v) Für $n = 1$ enthält S_n nur die (gerade) Permutation ε.
Für $n = 2$ ist $S_n = \{\varepsilon, (1\ 2)\}$, wobei $\operatorname{sgn} \varepsilon = +1$ und $\operatorname{sgn}(1\ 2) = -1$.
Für $n = 3$ ist

$$A_3 = \{\varepsilon, (1\ 2\ 3), (1\ 3\ 2)\} = \{\varepsilon, (1\ 2\ 3), (1\ 2\ 3)^2\} \cong \mathbb{Z}_3.$$

(vi) Dass A_n für $n \in \{1, 2, 3\}$ abelsch ist, folgt sofort aus (v). Für $n \geq 4$ ist

$$(1\ 2\ 3) \circ (1\ 2\ 4) = (1\ 3)(2\ 4) \neq (1\ 4)(2\ 3) = (1\ 2\ 4) \circ (1\ 2\ 3).$$

Bemerkung: Man kann zeigen, dass A_n genau dann einfach ist, wenn $n \neq 4$. Für $n \geq 5$ ist A_n daher eine nichtabelsche einfach Gruppe.

Definition: Für $n \geq 3$ sei die Diedergruppe $(D_n, \circ)$ definiert als $D_n = \langle \alpha, \beta \rangle$, d.h. D_n ist jene Untergruppe von S_n, die von $\alpha = (1\ 2\ 3\ \cdots\ n)$ und

$$\beta = \begin{pmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ 1 & n & n-1 & \cdots & 3 & 2 \end{pmatrix} = \begin{cases} (2\ n)(3\ n-1) \cdots \left(\frac{n}{2}\ \frac{n}{2}+2\right) & \text{für } 2 \mid n, \\ (2\ n)(3\ n-1) \cdots \left(\frac{n+1}{2}\ \frac{n+3}{2}\right) & \text{für } 2 \nmid n, \end{cases}$$

erzeugt wird.

Bemerkung: Statt D_n wird oft die Bezeichnung D_{2n} verwendet, da $|D_n| = 2n$.

Satz 47: Es sei $n \geq 3$ und $\alpha, \beta \in S_n$ wie eben definiert. Dann gelten
(i) $\alpha^k \neq \varepsilon$ für $1 \leq k < n$, $\alpha^n = \varepsilon$ und $\beta^2 = \varepsilon$,
(ii) $\beta \circ \alpha = \alpha^{-1} \circ \beta = \alpha^{n-1} \circ \beta$,
(iii) $D_n = \{\alpha^i \circ \beta^j \mid 0 \leq i < n, j \in \{0, 1\}\}$,
(iv) $|D_n| = 2n$,
(v) D_n ist nicht abelsch.

Beweis: (i) Das gilt, da α ein n-Zyklus und β ein Produkt elementfremder Transpositionen ist.
(ii) Ergibt sich aus

$$\begin{aligned}\beta \circ \alpha &= \begin{pmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ 1 & n & n-1 & \cdots & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ 2 & 3 & 4 & \cdots & n & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & \cdots & n-2 & n-1 & n \\ n & n-1 & n-2 & \cdots & 3 & 2 & 1 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ n & 1 & 2 & \cdots & n-2 & n-1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ 1 & n & n-1 & \cdots & 3 & 2 \end{pmatrix} \\ &= \alpha^{-1} \circ \beta.\end{aligned}$$

Aus $\alpha^n = \varepsilon$ folgt sofort $\alpha^{-1} = \alpha^{n-1}$.
(iii) Folgt aus Satz 12, (i) und (ii).
(iv) Die Elemente der Menge $\left\{\alpha^i \circ \beta^j \,\middle|\, 0 \leq i < n, j \in \{0,1\}\right\}$ sind paarweise verschieden, denn

$$(\alpha^i \circ \beta^j)(1) = \alpha^i(1) = i + 1 \ \forall i \in \{0, 1, \ldots, n-1\} \ \forall j \in \{0,1\},$$

$$(\alpha^i \circ \beta^0)(2) = \alpha^i(2) = \begin{cases} i+2 & \text{für } 0 \leq i \leq n-2, \\ 1 & \text{für } i = n-1, \end{cases}$$

und

$$(\alpha^i \circ \beta^1)(2) = \alpha^i\big(\beta(2)\big) = \alpha^i(n) = \begin{cases} n & \text{für } i = 0, \\ i & \text{für } 1 \leq i \leq n-1. \end{cases}$$

(v) Da $(\alpha \circ \beta)(1) = 2$ und $(\beta \circ \alpha)(1) = n$ ist $\alpha \circ \beta \neq \beta \circ \alpha$.

Bemerkung: Die Diedergruppe D_n wird üblicherweise mit der Symmetriegruppe des regelmäßigen n-Ecks identifiziert, d.h. mit der Gruppe der Isometrien, die ein n-Eck deckungsgleich auf sich selbst abbilden.

Um diese Gruppe besser zu verstehen, wählen wir eine Ecke des n-Ecks aus und bezeichnen sie mit 1. Davon ausgehend nummerieren wir die anderen Ecken im Uhrzeigersinn mit $2, 3, \ldots, n$. Da die Elemente der Symmetriegruppe Isometrien sind, bilden sie Ecken auf Ecken ab und benachbarte Ecken bleiben benachbart. Es gibt nun n Möglichkeiten, auf welche Ecke die Ecke 1 abgebildet wird und die Reihenfolge der Ecken kann gleich bleiben oder umgekehrt werden. Da eine Isometrie dadurch bereits eindeutig festgelegt ist, gibt es insgesamt genau $2n$ Isometrien, die das n-Eck deckungsgleich auf sich selbst abbilden. Tatsächlich kann man diese $2n$ Abbildungen leicht angeben: Außer der Identität gibt es die $n-1$ Drehungen um die Winkel $\frac{2\pi}{n}, 2 \cdot \frac{2\pi}{n}, 3 \cdot \frac{2\pi}{n}, \ldots, (n-1)\frac{2\pi}{n}$ um den Mittelpunkt

des n-Ecks, sowie n Spiegelungen an Symmetrieachsen. Ist n ungerade, so gehen alle n Symmetrieachsen durch eine Ecke und die Mitte der gegebenüberliegenden Seite. Ist n gerade, so gehen $\frac{n}{2}$ der Symmetrieachsen durch eine Ecke und die gegenüberliegenden Ecke und $\frac{n}{2}$ der Symmetrieachsen durch die Mittelpunkte zweier gegenüberliegender Seiten.

Da jede dieser $2n$ Isometrien Ecken auf Ecken abbildet, bewirkt sie eine Permutation der Ecken des n-Ecks. Umgekehrt ist die Isometrie durch diese Permutation bereits eindeutig festgelegt. In der Diedergruppe D_n wird nun nur noch die Permutation der Ecken angegeben. Dabei entspricht α der Drehung um den Winkel $\frac{2\pi}{n}$ um den Mittelpunkt und β der Spiegelung an der Geraden, die durch die Ecke 1 und den Mittelpunkt geht. Weiters beschreiben $\alpha, \alpha^2, \alpha^3, \dots, \alpha^{n-1}$ die Drehungen und $\beta, \beta \circ \alpha, \beta \circ \alpha^2, \dots, \beta \circ \alpha^{n-1}$ die Spiegelungen an den n Symmetrieachsen.