2. Symmetrische Gruppen

Im letzten Kapitel haben wir Gruppen eingeführt und ihre elementaren Eigenschaften untersucht. Wir wollen nun eine neue wichtige Klasse von Beispielen von Gruppen — und insbesondere auch unsere ersten nicht-abelschen Gruppen — kennenlernen. Es handelt sich hierbei um die Gruppen aller bijektiven Abbildungen auf gegebenen Mengen.

Konstruktion 2.1 (Symmetrische Gruppen)**.** Zu einer gegebenen Menge M sei

$$S(M) := \{f\colon M \to M \text{ bijektiv}\}$$

die Menge aller bijektiven Abbildungen von M nach M. Wir behaupten, dass $S(M)$ mit der üblichen Verkettung von Abbildungen (die wir mit dem Symbol „$\circ$“ schreiben) eine Gruppe ist. Beachte dazu zunächst, dass die Verkettung zweier bijektiver Abbildungen wieder bijektiv ist und die Verkettung zweier Elemente aus $S(M)$ (also zweier bijektiver Abbildungen von M nach M) damit auch wirklich wieder in $S(M)$ (also wieder bijektiv) ist. Weiterhin gilt:

(G1) Wie wir aus den Grundlagen der Mathematik wissen, ist die Verkettung beliebiger (also insbesondere auch bijektiver) Abbildungen assoziativ [G, Lemma 2.19].

(G2) Die *Identität* $\mathrm{id}_M\colon M \to M$ ist bijektiv und somit ein Element von $S(M)$. Sie ist natürlich ein neutrales Element bezüglich der Verkettung, denn $\mathrm{id}_M \circ f = f$ für alle $f \in S(M)$ (also für alle bijektiven Abbildungen $f\colon M \to M$).

(G3) Zu jeder bijektiven Abbildung $f \in S(M)$ ist die Umkehrabbildung f^{-1} ein inverses Element bezüglich der Verkettung, denn es ist $f^{-1} \circ f = \mathrm{id}_M$. Sie ist bekanntlich auch bijektiv, also ein Element von $S(M)$.

Also ist $(S(M), \circ)$ eine Gruppe. Man nennt sie die **symmetrische Gruppe** auf M. Sie ist im Allgemeinen *nicht* kommutativ: Ist z. B. $M = \mathbb{R}$, so sind

$$f\colon \mathbb{R} \to \mathbb{R},\ x \mapsto x+1 \quad \text{und} \quad g\colon \mathbb{R} \to \mathbb{R},\ x \mapsto 2x$$

zwei bijektive Abbildungen (mit Umkehrabbildungen $f^{-1}(x) = x-1$ und $g^{-1}(x) = \frac{x}{2}$), also gilt $f, g \in S(\mathbb{R})$. Aber die Abbildungen $f \circ g$ und $g \circ f$ sind nicht gleich, denn für alle $x \in \mathbb{R}$ ist

$$(f \circ g)(x) = f(g(x)) = f(2x) = 2x+1,$$

aber

$$(g \circ f)(x) = g(f(x)) = g(x+1) = 2(x+1) = 2x+2.$$

Aufgabe 2.2. Stellt euch vor, ihr seid Übungsleiter für die Algebraischen Strukturen und bekommt von einem Studenten die folgende Abgabe. Was sagt ihr dazu? Stimmt der Beweis so? Stimmt der Satz überhaupt?

> *Satz:* Es sei M eine Menge und $G = \{f\colon M \to M \text{ injektiv}\}$ die Menge aller injektiven Abbildungen von M nach M. Dann ist G zusammen mit der üblichen Verkettung von Abbildungen eine Gruppe.
>
> *Beweis:* Wir prüfen die Gruppenaxiome nach:
>
> (G1) Die Verknüpfung ist assoziativ, weil die Verkettung beliebiger (und damit auch injektiver) Abbildungen immer assoziativ ist.
>
> (G2) Die Identität id_M ist ein (links-)neutrales Element bezüglich der Verkettung von Abbildungen. Sie ist außerdem injektiv, liegt also in G.
>
> (G3) Ist $f\colon M \to M$ injektiv, so existiert eine Abbildung $g\colon M \to M$ mit $g \circ f = \mathrm{id}_M$, also ein linksinverses Element zu f.

Also ist $(G,\circ)$ eine Gruppe.

Aufgabe 2.3. Es sei M eine Menge. Zeige, dass die symmetrische Gruppe $S(M)$ genau dann abelsch ist, wenn M höchstens zwei Elemente besitzt.

Notation 2.4 (Endliche symmetrische Gruppen)**.** Der mit Abstand wichtigste Fall von symmetrischen Gruppen $S(M)$ ist der, wenn M eine *endliche* Menge, also z. B. die Menge $\{1,\dots,n\}$ der natürlichen Zahlen von 1 bis n ist. In diesem Fall setzen wir

$$S_n := S(\{1,\dots,n\}) = \big\{\sigma\colon \{1,\dots,n\} \to \{1,\dots,n\} \text{ bijektiv}\big\},$$

nennen diese Gruppe die **symmetrische Gruppe** der Stufe n und bezeichnen ihre Elemente in der Regel mit kleinen griechischen Buchstaben. Die Elemente von S_n kann man offensichtlich am einfachsten durch eine „Wertetabelle“ angeben: Ist $\sigma \in S_n$, also $\sigma\colon \{1,\dots,n\} \to \{1,\dots,n\}$ eine bijektive Abbildung, so vereinbaren wir dafür die Schreibweise

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

Da in der unteren Reihe dieser Matrix eine **Permutation**, d. h. eine Anordnung der Zahlen $1,\dots,n$ steht, kann man S_n auch als die *Gruppe der Permutationen* von n Elementen auffassen. Für Permutationen schreibt man die Gruppenverknüpfung, also die Verkettung $\sigma \circ \tau$, auch oft ohne Verknüpfungssymbol als $\sigma\tau$.

Beispiel 2.5. Wir betrachten die symmetrische Gruppe S_3.

(a) Das neutrale Element in S_3, also die identische Abbildung auf $\{1,2,3\}$, ist $\left(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{smallmatrix}\right)$. Das Element $\sigma \in S_3$ mit $\sigma(1) = 2$, $\sigma(2) = 3$ und $\sigma(3) = 1$ ist $\sigma = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix}\right)$.

(b) Um die Verknüpfung zweier Elemente zu berechnen, z. B. $\sigma\tau$ für

$$\sigma = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{smallmatrix}\right) \quad \text{und} \quad \tau = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{smallmatrix}\right),$$

müssen wir nur verfolgen, welche Zahlen unter dieser Verkettung auf welche anderen abgebildet werden. So wird z. B. die 1 durch τ auf 3 abgebildet, und diese 3 dann durch σ auf 2. Also ist $\sigma\tau(1) = \sigma(3) = 2$ (beachte, dass in einer Verkettung stets die rechts notierte Funktion zuerst ausgeführt wird). Genauso erhalten wir $\sigma\tau(2) = \sigma(1) = 1$ und $\sigma\tau(3) = \sigma(2) = 3$, und damit

$$\sigma\tau = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{smallmatrix}\right).$$

(c) Es ist leicht, alle Elemente von S_3 konkret anzugeben: Listen wir der Reihe nach zuerst alle Permutationen σ auf mit $\sigma(1) = 1$, dann die mit $\sigma(1) = 2$ und schließlich die mit $\sigma(1) = 3$, so erhalten wir für jeden dieser Fälle zwei Möglichkeiten und damit insgesamt

$$S_3 = \left\{\left(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{smallmatrix}\right)\right\}.$$

Die Gruppe S_3 hat also die Ordnung 6.

In der Tat können wir dieses Abzählargument verallgemeinern und damit die Ordnung der symmetrischen Gruppe S_n für alle n bestimmen:

Satz 2.6. *Für alle $n \in \mathbb{N}_{>0}$ gilt $|S_n| = n!$, wobei $n!$ (gesprochen: n-**Fakultät**) als $n! := 1 \cdot 2 \cdot \cdots \cdot n$ definiert ist.*

Wir werden diesen Satz mit dem Beweisprinzip der **(vollständigen) Induktion** zeigen, das ihr inzwischen schon aus den Grundlagen der Mathematik kennen solltet. Dieses Prinzip besagt folgendes: Ist $A(n)$ eine Aussage, die von einer natürlichen Zahl n abhängt, und wollen wir zeigen, dass diese Aussage für alle $n \geq n_0$ gilt (wobei $n_0 \in \mathbb{N}$ ein vorgegebener Startwert ist), so reicht es, die folgenden beiden Aussagen zu zeigen:

- Die Aussage $A(n_0)$ ist wahr („*Induktionsanfang*“);

- für alle $n > n_0$ gilt: Wenn die Aussage $A(m)$ für alle $m < n$ gilt, dann gilt auch die Aussage $A(n)$ („*Induktionsschritt*“).

Die Idee ist also, dass wir nur die erste Aussage $A(n_0)$ wirklich direkt zeigen. Beim Beweis jeder weiteren Aussage $A(n)$ für $n > n_0$ können wir dann voraussetzen, dass wir alle „vorhergehenden“ Aussagen $A(m)$ für $m < n$ schon gezeigt haben (wobei man in der Praxis oft nur die Aussage $A(n-1)$ für den direkt vorhergehenden Wert benötigt). Mit anderen Worten zeigen wir zuerst $A(n_0)$ direkt, beim Beweis von $A(n_0+1)$ können wir dann $A(n_0)$ bereits als bekannt voraussetzen, beim Beweis von $A(n_0+2)$ können wir $A(n_0)$ und $A(n_0+1)$ bereits voraussetzen, und so weiter. Man bezeichnet dabei die Voraussetzung, dass $A(m)$ für $m < n$ schon bekannt ist, als *Induktionsannahme* oder *Induktionsvoraussetzung*. Beachtet dabei bitte insbesondere, dass das Wort „Voraussetzung“ auch nach der neuen deutschen Rechtschreibung nur mit einem „r“ geschrieben wird.

Dass das Beweisprinzip der Induktion funktioniert, liegt offensichtlich daran, dass man alle natürlichen Zahlen irgendwann erreicht, wenn man auf diese Art beliebig oft „eins weiter zählt“.

Aber kehren wir nun zurück zum Beweis des obigen Satzes:

Beweis von Satz 2.6. Wir werden mit Induktion über $n \in \mathbb{N}_{>0}$ die folgende Aussage zeigen: Sind $M = \{x_1, \dots, x_n\}$ und $N = \{y_1, \dots, y_n\}$ zwei n-elementige Mengen, so gibt es genau $n!$ Bijektionen $f\colon M \to N$. (Offensichtlich folgt aus dieser Aussage sofort der Satz, indem man $M = N = \{1, \dots, n\}$ setzt.)

Induktionsanfang: Es ist klar, dass es genau eine Bijektion $f\colon \{x_1\} \to \{y_1\}$ gibt. Da $1! = 1$ ist, ist die Behauptung im Fall $n = 1$ also richtig.

Induktionsschritt: Wir können annehmen, dass wir bereits wissen, dass es zwischen zwei beliebigen $(n-1)$-elementigen Mengen genau $(n-1)!$ Bijektionen gibt (Induktionsannahme). Um zu untersuchen, wie viele Bijektionen $f\colon M \to N$ es zwischen zwei n-elementigen Mengen $M = \{x_1, \dots, x_n\}$ und $N = \{y_1, \dots, y_n\}$ gibt, unterscheiden wir nun n Fälle, je nachdem auf welches Element x_1 abgebildet wird:

1. Fall: $f(x_1) = y_1$. Dann muss f die Menge $\{x_2, \dots, x_n\}$ bijektiv auf $\{y_2, \dots, y_n\}$ abbilden, und jede solche Bijektion liefert auch eine Bijektion $f\colon M \to N$. Nach Induktionsannahme gibt es also genau $(n-1)!$ Bijektionen $f\colon M \to N$ mit $f(x_1) = y_1$.

2. Fall: $f(x_1) = y_2$. Dann bildet f die Menge $\{x_2, \dots, x_n\}$ bijektiv auf $\{y_1, y_3, y_4, \dots, y_n\}$ ab. Wie im 1. Fall erhalten wir nach Induktionsannahme also noch einmal $(n-1)!$ Bijektionen.

Die anderen Fälle $f(x_1) = y_3, \dots, f(x_1) = y_n$ sind offensichtlich analog, liefern also ebenfalls jeweils $(n-1)!$ Bijektionen. Insgesamt erhalten wir also $n \cdot (n-1)! = n!$ Bijektionen, was zu zeigen war. □

Aufgabe 2.7. Es seien $n \in \mathbb{N}_{>0}$, $\sigma \in S_n$ und $i \in \{1, \dots, n\}$. Ferner sei $k \in \mathbb{N}_{>0}$ die kleinste Zahl, so dass

$$\sigma^k(i) \in \{i, \sigma(i), \sigma^2(i), \dots, \sigma^{k-1}(i)\}.$$

Beweise, dass dann $\sigma^k(i) = i$ gilt.

02

Neben der Schreibweise für Permutationen als Wertetabelle wie in Notation 2.4 ist noch eine weitere Schreibweise nützlich und auch oft platzsparender. Hierfür benötigen wir den Begriff eines Zykels.

Notation 2.8 (Zykel)**.** Es sei $n \in \mathbb{N}_{>0}$.

(a) Für $k \in \mathbb{N}_{>0}$ seien $a_1, \dots, a_k$ verschiedene Zahlen zwischen 1 und n. Die Permutation $\sigma \in S_n$ mit

$$\sigma(a_1) = a_2,\ \sigma(a_2) = a_3,\ \dots,\ \sigma(a_{k-1}) = a_k,\ \sigma(a_k) = a_1$$
$$\text{und} \quad \sigma(a) = a \text{ für alle } a \notin \{a_1, \dots, a_k\},$$

also die die Zahlen $a_1, \dots, a_k$ zyklisch vertauscht und alle anderen Zahlen fest lässt, wird mit $(a_1\ a_2\ \cdots\ a_k)$ bezeichnet. Eine solche Permutation heißt ein k-**Zykel**. Als Spezialfall davon werden 2-Zykel $(a_1\ a_2)$ — also Permutationen, die genau zwei Zahlen a_1 und a_2 miteinander vertauschen und alle anderen fest lassen — **Transpositionen** genannt.

(b) Zwei Zykel $(a_1 \ \cdots \ a_k)$ und $(b_1 \ \cdots \ b_l)$ in S_n heißen **disjunkt**, wenn keine Zahl zwischen 1 und n in beiden Zykeln vorkommt.

Bemerkung 2.9.

(a) Offensichtlich gilt $(a_1 \ a_2 \ \cdots \ a_k) = (a_2 \ \cdots \ a_k \ a_1)$: Beide Zykel beschreiben die Permutation, die a_i auf a_{i+1} für $i < k$, und a_k auf a_1 abbilden. Man sagt: Die Einträge eines Zykels können *zyklisch vertauscht* werden, ohne die Permutation zu ändern. So ist z. B. in S_4

$$(1\ 2\ 4) = (2\ 4\ 1) = (4\ 1\ 2) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}.$$

Eine beliebige Vertauschung der Einträge eines Zykels liefert in der Regel jedoch eine andere Permutation: Im Vergleich zu obigem Zykel ist z. B.

$$(2\ 1\ 4) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix} \neq (1\ 2\ 4).$$

(b) Sind die Zykel $\sigma = (a_1 \ \cdots \ a_k)$ und $\tau = (b_1 \ \cdots \ b_l)$ disjunkt, so gilt $\sigma\tau = \tau\sigma$: Beide Verkettungen bilden a_i auf a_{i+1} für $i < k$, a_k auf a_1, b_i auf b_{i+1} für $i < l$, und b_l auf b_1 ab. Man sagt: Disjunkte Zykel vertauschen miteinander. Für Zykel, die nicht disjunkt sind, gilt dies natürlich nicht: So ist z. B. in S_3

$$(1\ 2)(1\ 3) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \quad \text{aber} \quad (1\ 3)(1\ 2) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

(beachte, dass wie bei Abbildungen üblich zuerst die rechte und dann die linke Permutation angewendet wird — so bildet z. B. die Verkettung $(1\ 2)(1\ 3)$ die Zahl 3 auf 2 ab, denn die 3 wird zuerst durch die rechte Transposition auf 1 abgebildet, und diese 1 dann durch die linke Transposition auf 2). Also ist $(1\ 2)(1\ 3) \neq (1\ 3)(1\ 2)$ in S_3.

(c) Als Spezialfall ist in Notation 2.8 (a) auch $k = 1$, also ein 1-Zykel zugelassen. Die zugehörige Permutation ist dann aber natürlich gerade die Identität.

(d) Es gilt

$$(a_k \ \cdots \ a_2 \ a_1)(a_1 \ a_2 \ \cdots \ a_k) = \mathrm{id},$$

da diese Verkettung von Zykeln offensichtlich jedes a_i für $i = 1, \ldots, k$ auf sich selbst abbildet (und alle anderen Zahlen in $\{1, \ldots, n\}$ ohnehin durch beide Permutationen unverändert bleiben). Also ist der „umgekehrte" Zykel $(a_k \ \cdots \ a_2 \ a_1)$ genau das Inverse von $(a_1 \ a_2 \ \cdots \ a_k)$. Insbesondere sind Transpositionen damit zu sich selbst invers, da

$$(a_1 \ a_2)^{-1} = (a_2 \ a_1) \overset{\text{(a)}}{=} (a_1 \ a_2).$$

Mit Hilfe von Zykeln können wir jetzt auch beliebige Permutationen einfacher schreiben:

Konstruktion 2.10 (Zykelzerlegung)**.** Wir wollen sehen, dass sich jede Permutation $\sigma \in S_n$ als Verkettung disjunkter Zykel schreiben lässt. Dazu betrachten wir einmal als Beispiel die Permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 7 & 1 & 6 & 5 & 3 & 2 \end{pmatrix} \in S_7.$$

Wir versuchen nun, in dieser Permutation einen Zykel zu finden. Dazu starten wir mit einer beliebigen Zahl in $\{1, \ldots, n\}$, z. B. mit 1, und verfolgen sie bei fortlaufender Anwendung von σ:

$$1 \overset{\sigma}{\longmapsto} 4 \overset{\sigma}{\longmapsto} 6 \overset{\sigma}{\longmapsto} 3 \overset{\sigma}{\longmapsto} 1.$$

Da es nur endlich viele Zahlen von 1 bis n gibt, ist klar, dass wir hierbei irgendwann einmal wieder auf eine Zahl stoßen mussten, die wir vorher in der Reihe schon einmal hatten. Nach Aufgabe 2.7 muss dies sogar wieder die Ausgangszahl sein, im Beispiel oben also die 1. Die Abbildung σ lässt sich auf den Zahlen, die in dieser Kette vorkommen, also durch einen Zykel beschreiben — in unserem Fall durch den 4-Zykel $(1\ 4\ 6\ 3)$.

Um die Abbildung σ auch auf den anderen Zahlen korrekt zu beschreiben, müssen wir jetzt auf die gleiche Art noch Zykel konstruieren, die diese anderen Zahlen enthalten. Starten wir z. B. als Nächstes mit 2, so erhalten wir den Zykel

$$2 \overset{\sigma}{\longmapsto} 7 \overset{\sigma}{\longmapsto} 2,$$

also die Transposition $(2\ 7)$ (beachte, dass wir hierbei auch wirklich keine Zahl erhalten können, die schon im vorher betrachteten Zykel enthalten war, weil σ injektiv ist). Die einzige Zahl, die wir nun bisher noch nicht betrachtet haben, ist die 5 — die aber von σ auf sich selbst abgebildet wird und somit den 1-Zykel (5) bildet. Insgesamt können wir σ daher als die Verkettung

$$\sigma = (1\ 4\ 6\ 3)(2\ 7)(5)$$

schreiben. Da der letzte 1-Zykel (5) natürlich nach Bemerkung 2.9 (c) die Identität ist, können wir diesen nun noch weglassen und erhalten

$$\sigma = (1\ 4\ 6\ 3)(2\ 7).$$

Es ist klar, dass man mit diesem Verfahren jede Permutation als Vereinigung disjunkter Zykel schreiben kann (genau genommen müsste man dies jetzt formal beweisen, aber ein solcher formaler Beweis würde hier nur verwirren und keine neuen Erkenntnisse bringen — daher möchte ich euch und mir das ersparen). Man nennt dies eine **Zykelzerlegung** von σ.

Anhand der Konstruktion sieht man auch, dass die Zykelzerlegung einer Permutation eindeutig ist bis auf

(a) zyklisches Vertauschen der Einträge in den Zykeln (siehe Bemerkung 2.9 (a)): Wir hätten im Beispiel oben z. B. auch $\sigma = (6\ 3\ 1\ 4)(7\ 2)$ schreiben können;

(b) Vertauschen der Zykel (siehe Bemerkung 2.9 (b)): Wir hätten die Permutation oben auch als $\sigma = (2\ 7)(1\ 4\ 6\ 3)$ schreiben können;

(c) Hinzufügen bzw. Weglassen von 1-Zykeln (siehe Bemerkung 2.9 (c)): Dies haben wir oben im Beispiel schon gesehen.

(Natürlich müsste man eigentlich auch diese Eindeutigkeitsaussage formal beweisen; auch dies wollen wir aus den oben genannten Gründen hier jedoch nicht tun.)

Unter den Zykeln sind vor allem die Transpositionen besonders wichtig, da wir jetzt sehen wollen, dass man aus ihnen durch geeignete Verkettungen jedes Element der symmetrischen Gruppe S_n bilden kann. Anschaulich ist dies einfach die Aussage, dass sich jede Permutation der Zahlen $1,\dots,n$ dadurch erhalten lässt, dass man mehrfach nacheinander zwei geeignete Zahlen miteinander vertauscht.

Lemma 2.11 (Verkettungen von Transpositionen)**.** *Es sei $n \in \mathbb{N}_{>0}$.*

(a) *Jeder k-Zykel in S_n ist eine Verkettung von $k-1$ Transpositionen.*

(b) *Jede Permutation in S_n ist eine Verkettung von Transpositionen.*

Beweis.

(a) Offensichtlich gilt

$$(a_1\ a_2\ \cdots\ a_k) = (a_1\ a_2)(a_2\ a_3)\cdots(a_{k-1}\ a_k),$$

da die Permutationen auf beiden Seiten jedes a_i für $i < k$ auf a_{i+1} und a_k auf a_1 abbilden (sowie alle anderen Zahlen in $\{1,\dots,n\}$ unverändert lassen).

(b) Dies folgt sofort aus (a), da jede Permutation nach Konstruktion 2.10 eine Verkettung von Zykeln ist. □

Die Darstellung einer Permutation als Verkettung von Transpositionen ist natürlich keinesfalls eindeutig. So gilt z. B. in S_4

$$\mathrm{id}_{S_4} = (1\ 2)(1\ 2) = (1\ 3)(3\ 4)(1\ 3)(1\ 4) = (1\ 4)(1\ 3)(2\ 4)(3\ 4)(1\ 2)(2\ 3),$$

wie man leicht durch explizite Berechnung jeder dieser Verkettungen überprüfen kann. Überraschenderweise haben aber alle solchen Darstellungen einer gegebenen Permutation σ trotz der vielen Wahlmöglichkeiten eines gemeinsam: Wie wir jetzt zeigen werden, ist die Anzahl der Transpositionen abhängig von σ entweder immer eine gerade Zahl (so wie im Fall der Identität oben, für die wir Darstellungen mit 2, 4 und 6 Transpositionen angegeben haben) oder immer eine ungerade Zahl. Bei der Untersuchung der symmetrischen Gruppe ist es ein sehr wichtiges Unterscheidungsmerkmal für die Permutationen, ob diese Anzahl gerade oder ungerade ist.

Lemma 2.12. *Es sei $n \in \mathbb{N}_{>0}$.*

(a) *Für alle $\sigma \in S_n$ bezeichne $c_\sigma \in \mathbb{N}_{>0}$ die Anzahl der Zykel (inklusive aller 1-Zykel) in der Zykelzerlegung von σ wie in Konstruktion 2.10. Dann gilt*

$$c_{\tau\sigma} = c_\sigma \pm 1$$

für jede Transposition τ.

(b) *Sind*

$$\sigma = \tau_1 \cdots \tau_r \quad \text{und} \quad \sigma = \tilde{\tau}_1 \cdots \tilde{\tau}_s$$

zwei Darstellungen derselben Permutation $\sigma \in S_n$ als Verkettung von Transpositionen $\tau_1, \dots, \tau_r$ bzw. $\tilde{\tau}_1, \dots, \tilde{\tau}_s$, so sind r und s entweder beide gerade oder beide ungerade.

Beweis.

(a) Es sei $\sigma = \sigma_1 \cdots \sigma_m$ die Zerlegung von σ in disjunkte Zykel $\sigma_1, \dots, \sigma_m$ wie in Konstruktion 2.10, so dass also $m = c_\sigma$ gilt. Ferner sei $\tau = (a_1\ b_1)$ mit verschiedenen $a_1, b_1 \in \{1, \dots, n\}$.

Da sowohl a_1 als auch b_1 in genau einem Zykel der Zerlegung vorkommen, können zwei Fälle auftreten:

- Die Zahlen a_1 und b_1 liegen im gleichen Zykel. Nach Konstruktion 2.10 (a) und (b) können wir die Zykel in der Zerlegung dann so anordnen, dass a_1 und b_1 im ersten Zykel σ_1 vorkommen, und a_1 die erste Zahl dieses Zykels ist. Es ist also

$$\sigma = \underbrace{(a_1\ \cdots\ a_k\ b_1\ \cdots\ b_l)}_{=\sigma_1}\, \sigma_2 \cdots \sigma_m$$

für gewisse $a_2, \dots, a_k, b_2, \dots, b_l$. Wie man analog zu Lemma 2.11 (a) sofort nachrechnet, ist dann

$$\begin{aligned} \tau\sigma &= (a_1\ b_1)(a_1\ \cdots\ a_k\ b_1\ \cdots\ b_l)\, \sigma_2 \cdots \sigma_m \\ &= (a_1\ \cdots\ a_k)(b_1\ \cdots\ b_l)\, \sigma_2 \cdots \sigma_m. \end{aligned}$$

Da dies nun die Zykelzerlegung von $\tau\sigma$ ist, und sie aus $m+1$ Zykeln besteht, ist also $c_{\tau\sigma} = c_\sigma + 1$.

- Die Zahlen a_1 und b_1 liegen in verschiedenen Zykeln. Dann können wir die Zykelzerlegung so umschreiben, dass a_1 die erste Zahl im Zykel σ_1 und b_1 die erste Zahl im Zykel σ_2 ist, und wir erhalten durch Nachrechnen diesmal die Zykelzerlegung

$$\begin{aligned} \tau\sigma &= (a_1\ b_1)\, \underbrace{(a_1\ \cdots\ a_k)}_{=\sigma_1}\, \underbrace{(b_1\ \cdots\ b_l)}_{=\sigma_2}\, \sigma_3 \cdots \sigma_m \\ &= (a_1\ \cdots\ a_k\ b_1\ \cdots\ b_l)\, \sigma_3 \cdots \sigma_m \end{aligned}$$

von $\tau\sigma$ mit $m-1$ Zykeln. Damit ergibt sich in diesem Fall $c_{\tau\sigma} = c_\sigma - 1$.

(b) Nach Voraussetzung gilt

$$\begin{aligned}\mathrm{id} &= \sigma^{-1}\sigma \\ &= (\tau_1 \cdots \tau_r)^{-1}\, \tilde{\tau}_1 \cdots \tilde{\tau}_s \\ &= \tau_r^{-1} \cdots \tau_1^{-1}\, \tilde{\tau}_1 \cdots \tilde{\tau}_s \qquad \text{(Lemma 1.10 (b))} \\ &= \tau_r \cdots \tau_1\, \tilde{\tau}_1 \cdots \tilde{\tau}_s\, \mathrm{id}. \qquad \text{(Bemerkung 2.9 (d))}\end{aligned}$$

Die Anzahl der Zykel in der Zykelzerlegung einer Permutation wechselt aber nach (a) bei jeder Verkettung von links mit einer Transposition von gerade auf ungerade und umgekehrt. Da wir ausgehend von der Identität nach einer Verkettung mit $r+s$ Transpositionen wieder die Identität erhalten, muss diese Anzahl $r+s$ von Transpositionen also gerade sein. Damit sind r und s entweder beide gerade oder beide ungerade. □

Definition 2.13 (Signum von Permutationen)**.** Es sei $n \in \mathbb{N}_{>0}$ und $\sigma \in S_n$. Nach Lemma 2.11 (b) können wir σ als Verkettung $\sigma = \tau_1 \cdots \tau_r$ einer gewissen Anzahl r von Transpositionen schreiben. Das **Signum** oder **Vorzeichen** von σ ist dann definiert als

$$\operatorname{sign}\sigma := (-1)^r = \begin{cases} 1 & \text{falls } r \text{ gerade,} \\ -1 & \text{falls } r \text{ ungerade.} \end{cases}$$

Beachte, dass dies nach Lemma 2.12 (b) auch wirklich nur von der gegebenen Permutation σ und nicht von der gewählten Darstellung als Verkettung von Transpositionen $\sigma_1, \ldots, \sigma_r$ abhängt.

Eine unmittelbare, aber sehr wichtige Folgerung aus dieser Definition ist, dass das Vorzeichen *multiplikativ* ist, d. h. dass das Vorzeichen einer Verkettung $\sigma\tau$ von Permutationen gleich dem Produkt der Vorzeichen von σ und τ ist.

Satz 2.14 (Multiplikativität des Signums)**.** *Für alle $n \in \mathbb{N}_{>0}$ und $\sigma, \tau \in S_n$ gilt*

$$\operatorname{sign}(\sigma\tau) = \operatorname{sign}\sigma \cdot \operatorname{sign}\tau.$$

Beweis. Es seien $\sigma = \sigma_1 \cdots \sigma_r$ und $\tau = \tau_1 \cdots \tau_s$ für gewisse Transpositionen $\sigma_1, \ldots, \sigma_r, \tau_1, \ldots, \tau_s$. Dann ist $\sigma\tau = \sigma_1 \cdots \sigma_r \tau_1 \cdots \tau_s$ ein Produkt von $r+s$ Transpositionen, und damit folgt sofort

$$\operatorname{sign}(\sigma\tau) = (-1)^{r+s} = (-1)^r \cdot (-1)^s = \operatorname{sign}\sigma \cdot \operatorname{sign}\tau.$$ □

Beispiel 2.15.

(a) Transpositionen haben offensichtlich das Signum -1. Allgemeiner besagt Lemma 2.11 (a), dass ein k-Zykel Signum $(-1)^{k-1}$ hat, also dass sein Signum genau dann -1 ist, wenn k gerade ist.

(b) Wegen der Multiplikativität des Signums aus Satz 2.14 können wir das Signum einer beliebigen Permutation mit Hilfe von (a) leicht aus ihrer Zykelzerlegung berechnen. So gilt z. B. für die Beispielpermutation $\sigma = (1\ 4\ 6\ 3)(2\ 7) \in S_7$ aus Konstruktion 2.10

$$\operatorname{sign}\sigma \overset{2.14}{=} \operatorname{sign}(1\ 4\ 6\ 3) \cdot \operatorname{sign}(2\ 7) \overset{\text{(a)}}{=} (-1) \cdot (-1) = 1.$$

Allgemein hat eine Permutation σ demzufolge genau dann Signum -1, wenn die Anzahl der Zykel *gerader* Länge in ihrer Zykelzerlegung *ungerade* ist.

Aufgabe 2.16. Wir betrachten die Permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 2 & 6 & 1 & 4 \end{pmatrix} \in S_6$.

(a) Berechne σ^2 und σ^{-1}.

(b) Bestimme die Zykelzerlegung von σ.

(c) Man schreibe σ als Verkettung von Transpositionen. Was ist das Vorzeichen von σ?

Aufgabe 2.17. Beim im Bild (A) unten dargestellten „Schiebepuzzle“ sind mit den Zahlen 1 bis 15 beschriftete Würfel zufällig so in einem 4×4-Quadrat angeordnet, dass das Feld rechts unten frei bleibt.

Man kann nun nacheinander Würfel von links, rechts, oben oder unten in den jeweils freien Platz schieben und so z. B. von (A) aus die Position (B) erreichen, indem man den Würfel 2 nach unten schiebt. Ziel des Spiels ist es, durch solche Züge letztlich die vollständig geordnete Position (C) zu erreichen.

14	10	15	1
6	7	8	9
5	4	3	2
13	12	11	

(A)

14	10	15	1
6	7	8	9
5	4	3	
13	12	11	2

(B)

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

(C)

Wir wollen die möglichen Positionen des Puzzles im Folgenden als Permutationen in S_{16} auffassen, indem wir die Zahlen von links oben nach rechts unten lesen und den freien Platz dabei mit 16 bezeichnen. Die Zielposition (C) ist also z. B. gerade die Identität in S_{16}.

(a) Berechne das Signum der Ausgangsposition (A).

(b) Zeige, dass jeder mögliche Spielzug das Signum der Spielposition ändert.

(c) Beweise, dass es nicht möglich ist, von Position (A) aus das Ziel (C) zu erreichen.