1.2 Gruppen

Gruppen zählen zu den in der Mathematik und ihren Anwendungen wohl am häufigsten vorkommenden mathematischen Strukturen. Viele in der Mathematik untersuchte Objekte tragen eine »natürliche« Gruppenstruktur, wie die Beispiele im letzten Abschnitt bereits gezeigt haben. Das Wort »natürlich« bedeutet in diesem Zusammenhang, dass sich die Gruppenstruktur »von selbst ergibt« und nicht künstlich eingeführt werden muss. Gruppen finden auch außerhalb der Mathematik zum Beispiel in der Physik, der Geologie und der Chemie weitreichende Anwendungen.

1.2.1 Beispiele

In diesem Abschnitt werden exemplarisch drei Arten von Gruppen diskutiert.

Gruppen und Symmetrie: Die Diedergruppen

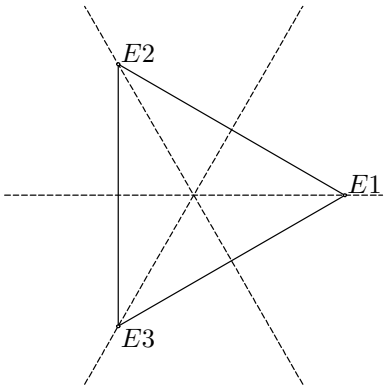

Abbildung 1: Symmetrieachsen des gleichseitigen Dreiecks

Es sei $\Delta \subset \mathbb{R}^2$ ein Dreieck mit gleich langen Seiten. Im Folgenden wird die Menge D_3 aller Spiegelungen von Δ an einer Geraden, sowie aller Drehungen von Δ um den Mittelpunkt betrachtet, die Δ deckungsgleich in sich selbst überführen. Es gilt also $D_3 \subset \mathrm{Abb}\,(\Delta)$ – siehe Beispiel 10. Das Dreieck Δ besitzt drei Symmetrieachsen, die jeweils durch eine der Ecken E_i und die gegenüberliegende Seitenmitte verlaufen – siehe Abbildung 1. An jeder dieser Achsen kann man Δ spiegeln und erhält so drei verschiedene Elemente τ_1, τ_2, τ_3 von D_3, wobei die Nummerierung so gewählt sei, dass τ_i die

Spiegelung an der durch die Ecke E_i laufenden Symmetrieachse ist – siehe Abbildung 1. Δ besitzt offensichtlich keine weiteren Symmetrieachsen, also sind auch keine weiteren Spiegelungen von Δ in sich selbst möglich.

Was die Drehungen angeht, so kann Δ um alle Winkel der Form $\frac{2\pi}{3}k$, $k \in \mathbb{Z}$, gedreht werden, wobei ein nicht negativer Winkel für eine Drehung im Gegenuhrzeigersinn und ein negativer Winkel für eine Drehung im Uhrzeigersinn steht. Betrachtet man die Wirkung der Drehungen auf das Dreieck, so ist klar, dass Drehungen um Winkel ϕ und ψ mit der Eigenschaft $\phi - \psi = 2\pi k$, $k \in \mathbb{Z}$, dieselbe Wirkung auf Δ haben:

$$\forall x \in \Delta \quad \sigma_\phi(x) = \sigma_\psi(x),$$

wobei σ_ϕ, σ_ψ die Drehungen um den Winkel ϕ und ψ sind. Weiter ist σ_0 die identische Abbildung id des Dreiecks. Insgesamt erhält man also:

$$D_3 = \{\mathrm{id}\,, \sigma_1, \sigma_2, \tau_1, \tau_2, \tau_3\},$$

wobei σ_i die Drehung um $\frac{2\pi}{3}i$ ist.

Behauptung: $(D_3, \circ)$ *ist eine Gruppe.*

Hierbei wir natürlich mit $\circ$ die Verkettung von Abbildungen bezeichnet.

Um diese Behauptung zu überprüfen, berechnet man sämtliche Verkettungen zweier Elemente aus D_3. Es ergibt sich die folgende Verknüpfungstafel:

	id	σ_1	σ_2	τ_1	τ_2	τ_3
id	id	σ_1	σ_2	τ_1	τ_2	τ_3
σ_1	σ_1	σ_2	id	τ_3	τ_1	τ_2
σ_2	σ_2	id	σ_1	τ_2	τ_3	τ_1
τ_1	τ_1	τ_2	τ_3	id	σ_1	σ_2
τ_2	τ_2	τ_3	τ_1	σ_2	id	σ_1
τ_3	τ_3	τ_1	τ_2	σ_1	σ_2	id

Die Berechnung dieser Tabelle wird durch die Tatsache vereinfacht, dass ein Element von D_3 bereits eindeutig festgelegt ist, wenn man seine Wirkung auf zwei von drei Eckpunkten von Δ kennt. Drehungen und Spiegelungen unterscheiden sich dabei dadurch, dass Spiegelungen genau eine Ecke unverändert lassen. So bildet zum Beispiel $\sigma_1 \circ \tau_1$ die Ecke 3 auf sich selbst ab, folglich muss diese Verkettung gleich id oder gleich τ_3 sein. Da die Ecke 1 nicht auf sich selbst abgebildet wird, bleibt nur τ_3 als Ergebnis. Weiter kann man bereits bekannte Identitäten benutzen um neue Verkettungen zu bestimmen:

$$\sigma_2 \circ \tau_1 = \sigma_1^2 \circ \tau_1 = \sigma_1 \circ \sigma_1 \circ \tau_1 = \sigma_1 \circ \tau_3 = \tau_2.$$

Sammelt man die anhand der Verknüpfungstafel gemachten Beobachtungen, so ergibt sich:

- Die Verkettung zweier Elemente von D_3 liegt stets in D_3 und $\circ$ ist assoziativ, weil das für alle Abbildungsverknüpfungen gilt. Folglich ist $(D_3, \circ)$ eine Halbgruppe.
- Die Betrachtung der zweiten Zeile und Spalte der Tafel zeigt, dass id ein neutrales Element ist. Folglich ist $(D_3, \circ)$ ein Monoid.
- In jeder Zeile und Spalte kommt das Element id vor, und die Positionen des Vorkommens liegen symmetrisch zur Diagonalen von links oben nach rechts unten in der Tafel. Folglich gibt es zu jedem Element eine Inverses und $(D_3, \circ)$ ist eine Gruppe.
- Die Verknüpfungstafel ist nicht symmetrisch zur oben genannten Diagnonalen, folglich ist $(D_3, \circ)$ nicht abelsch.

Die Gruppe D_3 nennt man die *Symmetriegruppe des gleichseitigen Dreiecks* oder auch die *Diedergruppe des Dreiecks*.

Betrachtet man statt eines gleichseitigen Dreiecks ein gleichschenkliges, nicht gleichseitiges Dreieck Δ, etwa mit den gleichlangen Seiten von der Ecke 3 ausgehend, so gibt es keine Drehungen, die Δ deckungsgleich in sich selbst abbilden, und nur die Spiegelung τ_3, die diese Eigenschaft besitzt. Die Symmetriegruppe von Δ ist in diesem Fall $(\{\mathrm{id}\,, \tau_3\}, \circ)$.

Betrachtet man ein allgemeines, unregelmäßiges Dreieck Δ, so ist dessen Symmetriegruppe gleich $(\{\mathrm{id}\,\}, \circ)$.

Die Definition der Diedergruppe D_3 lässt sich verallgemeinern: Man betrachtet ein regelmäßiges n-Eck $\Delta \subset \mathbb{R}^2$ mit $n \geq 3$ und hierzu wiederum die Menge D_n aller Drehungen und Spiegelungen, die Δ auf sich selbst abbilden. Offensichtlich gibt es neben der Identität id insgesamt $n-1$ Drehungen $\sigma_1, \ldots, \sigma_{n-1}$, wobei die Numerierung so gewählt sei, dass σ_k eine Drehung im Gegenuhrzeigersinn um den Winkel $\frac{2\pi}{n}k$ ist. Es gilt folglich

$$\sigma_k = \sigma_1^k,\ k \in \{0, \ldots, n-1\}, \tag{6}$$

wobei man entsprechend den Potenzregeln $\sigma_0 = \mathrm{id}$ setzt.

Hinsichtlich der Spiegelungen unterscheiden sich die n-Ecke abhängig davon, ob n ungerade oder gerade ist. Ist n ungerade, so besitzt Δ insgesamt n

Symmetrieachsen, die jeweils durch eine Ecke und die Mitte der gegenüberliegenden Seite verlaufen – siehe Abbildung 2. Die zugehörigen Spiegelungen werden mit $\tau_1, \ldots, \tau_n$ bezeichnet, wobei der Index die Ecke bezeichnet, durch die die Spiegelachse läuft.

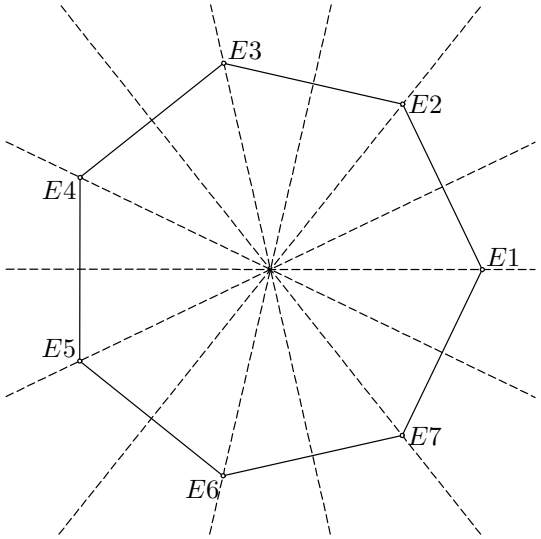

Abbildung 2: Symmetrien des 7-Ecks

Ist n gerade, so gibt es $\frac{n}{2}$ Symmetrieachsen durch jeweils gegenüberliegende Ecken, und $\frac{n}{2}$ Symmetrieachsen durch jeweils gegenüberliegende Seitenmitten. Die insgesamt n Spiegelungen $\tau_1, \ldots, \tau_n$ werden beginnend mit der Spiegelung an der Achse durch die Ecke 1 im Gegenuhrzeigersinn nummeriert – siehe Abbildung 3.

Unser Ziel ist nun die Verifizierung des folgenden Satzes:

Satz 20: *Die Menge*

$$D_n := \{\mathrm{id}\,, \sigma_1, \ldots, \sigma_{n-1}, \tau_1, \ldots, \tau_n\}$$

bildet zusammen mit der Verkettung $\circ$ von Abbildungen eine Gruppe mit $2n$ Elementen. Man bezeichnet sie als Symmetriegruppe des regelmäßigen n-Ecks.

Die im obigen Satz auftretenden Gruppen D_n nennt man allgemein *Diedergruppen.*

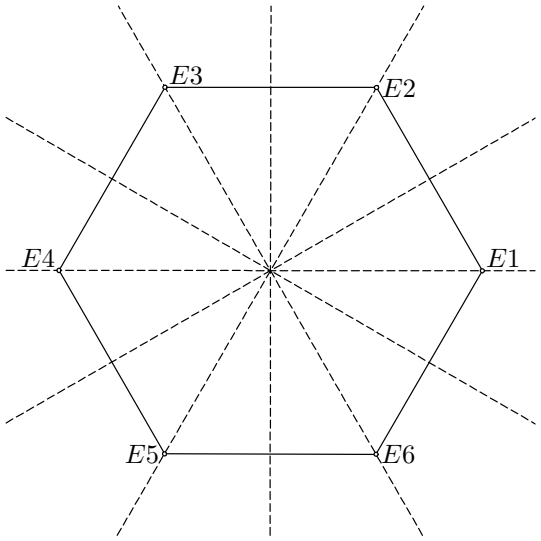

Abbildung 3: Symmetrien des 6-Ecks

Um Satz 20 zu beweisen ist nur zu zeigen, dass die Verkettung von Abbildung $\circ$ eine innere Verknüpfung von D_n liefert, dass also

$$\forall s, t \in D_n \quad s \circ t \in D_n$$

gilt. Denn das Assoziativgesetz gilt stets für die Verkettung von Abbildungen, die Abbildung id $\in D_n$ ist neutral bezüglich $\circ$ und zu jeder Drehung σ_k ist σ_{n-k}, sowie zu jeder Spiegelung τ_i die Spiegelung selbst das Inverse.

Da die Verkettung zweier Drehungen wiederum eine Drehung ist, bleibt zu untersuchen was sich bei der Verkettung zweier Spiegelungen und bei der Verkettung von Spiegelung und Drehung ergibt.

Wir betrachten zunächst die Verkettung zweier Spiegelungen (Abbildung 4): Spiegelt man einen Punkt $P \in \mathbb{R}^2$ zunächst an der Geraden h und spiegelt den erhaltenen Bildpunkt Q an der Geraden g, so kann man den erhaltenen Bildpunkt Q' aus P auch wie folgt konstruieren: Man spiegelt die Gerade h an g und betrachtet den Winkel α, den h und die gespiegelte Gerade h' einschließen. Die Drehung von P um den Schnittpunkt $h \cap g$ um den Winkel α liefert Q'.

In einem regelmäßigen n-Eck schließen die vorkommenden Spiegelachsen g und h Winkel der Form $\frac{2\pi}{2n}k$ ein. Der Winkel α besitzt also stets einen Wert $\frac{2\pi}{n}k$.

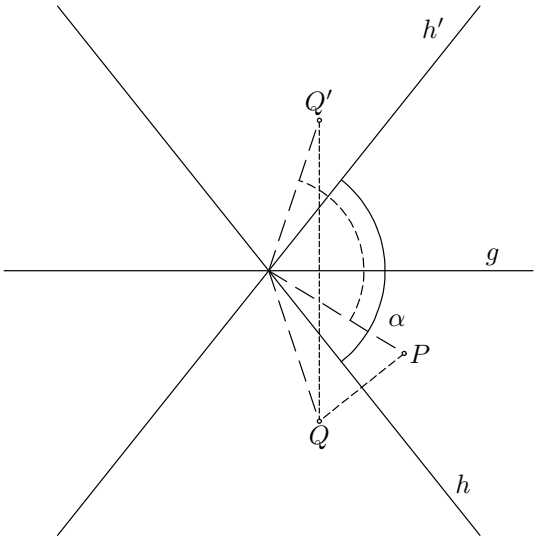

Abbildung 4: Verkettung zweier Spiegelungen

SATZ 21: *Die Verkettung $\tau_i \circ \tau_j$ zweier verschiedener Spiegelungen $\tau_i, \tau_j \in D_n$ ergibt eine Drehung $\sigma_k \in D_n$ und zwar um das doppelte des Winkels zwischen den beiden Spiegelachsen.*

Alternativ kann man Satz 21 auch so formulieren:

SATZ 22: *Die Verkettung $\sigma_k \circ \tau_i$ einer Spiegelung $\tau_i \in D_n$ mit eine Drehung $\sigma_k \in D_n$ liefert eine Spiegelung $\tau_j \in D_n$. Der Winkel zwischen den beiden Spiegelachsen ist dabei gleich dem halben Drehwinkel von σ_k.*

Wir betrachten nun die Verkettung einer Drehung mit einer Spiegelung (Abbildung 5): Dreht man einen Punkt $P \in \mathbb{R}^2$ zunächst um α, spiegelt den Bildpunkt Q dann an einer Geraden g und dreht erneut um den Winkel α, so erhält man die Spiegelung P' von P an g. Es gilt also:

SATZ 23: *Für die Drehung $\sigma_k \in D_n$ um einen Winkel $\frac{2\pi}{n}k$, $k \in \{1, \ldots, n-1\}$, und eine Spiegelung τ_i gilt:*

$$\tau_i = \sigma_k \circ \tau_i \circ \sigma_k,$$

oder äquivalent

$$\tau_i \circ \sigma_k^{n-1} = \sigma_k \circ \tau_i.$$

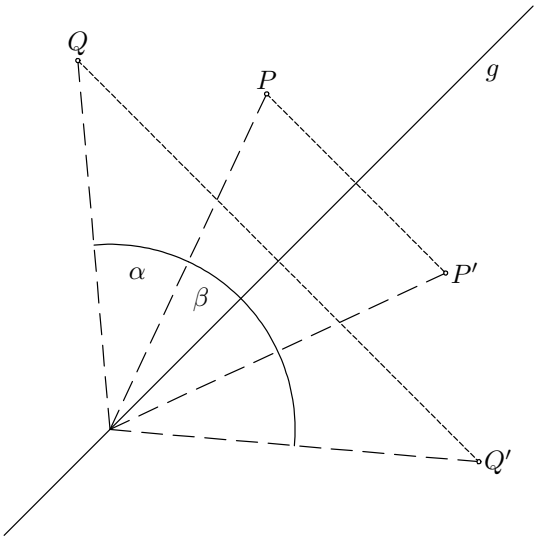

Abbildung 5: Verkettung einer Drehung mit einer Spiegelung

Damit lässt sich Satz 20 beweisen: Satz 21 zeigt, dass die Verkettung zweier Spiegelungen aus D_n wieder in D_n liegt. Satz 22 zeigt, dass die Verkettung einer Spiegelung mit einer Drehung wieder in D_n liegt. Satz 23 zeigt schließlich, dass man die Verkettung einer Drehung mit einer Spiegelung als Verkettung einer anderen Drehung mit derselben Spiegelung schreiben kann, womit man nach Satz 22 ein Element von D_n erhält.

Die in Satz 23 angegebene Beziehung zwischen Spiegelungen und Drehungen lässt sich ausnutzen um die Elemente der Gruppe D_n so darzustellen, dass man mit ihnen effizient zum Beispiel in einem Computeralgebrasystem rechnen kann:

Satz 24: *Es sei $\tau \in D_n$ eine Spiegelung und $\sigma \in D_n$ die Drehung um $\frac{2\pi}{n}$. Dann lässt sich jedes Element $s \in D_n$ eindeutig in der Form*

$$s = \tau^k \circ \sigma^\ell,\ k \in \{0, 1\}, \ell \in \{0, \ldots, n-1\} \tag{7}$$

schreiben.

Beweis: Es gelte

$$\tau^{k_1} \circ \sigma^{\ell_1} = \tau^{k_2} \circ \sigma^{\ell_2}$$

mit $k_1, k_2 \in \{0, 1\}$ und $\ell_1, \ell_2 \in \{0, \ldots, n-1\}$. Ohne Einschränkung kann man dabei $\ell_1 \leq \ell_2$ annehmen. Dann ergibt sich aus der ursprünglichen Gleichung:

$$\tau^{k_1} = \tau^{k_2} \circ \sigma^{\ell}$$

mit $\ell = \ell_2 - \ell_1 \in \{0, \ldots, n-1\}$.

Ist nun $k_1 = k_2 = 0$, so folgt $\sigma^{\ell} = \mathrm{id}$ also $\ell = 0$. Damit ist in diesem Fall die Behauptung bewiesen.

Ist $k_1 = k_2 = 1$, so liefert die Verknüpfung mit τ von links wiederum $\sigma^{\ell} = \mathrm{id}$, also die Behauptung.

Im Fall $k_1 = 1$ und $k_2 = 0$ wäre die Spiegelung τ auch eine Drehung. Dies ist unmöglich, da aus $\tau^2 = \mathrm{id}$ folgt, dass der Drehwinkel dann gleich π sein muss. Die Drehung um π besitzt aber als einzigen Fixpunkt in Δ den Punkt $(0, 0)$, kann also keine Spiegelung sein.

Der Fall $k_1 = 0$ und $k_2 = 1$ lässt sich durch Verknüpfung mit τ von links auf den gerade diskutierten zurückführen. Damit wurde insgesamt die Eindeutigkeit der Darstellung (7) bewiesen.

Da die Mengen D_n und $\{\tau^k \circ \sigma^{\ell} : k \in \{0, 1\}, \ell \in \{0, \ldots, n-1\}\}$ beide $2n$ Elemente besitzen – letztere nach dem gerade Bewiesenen – sind sie gleich. Hieraus folgt die behauptete Darstellung (7) der Elemente von D_n. □

Will man mit Hilfe von Gruppen konkrete Probleme lösen, so muss man in der Lage sein in einer gegebenen Gruppe $(G, \cdot)$ effizient zu rechnen. Arbeitet man beispielsweise in der Diedergruppe D_{101}, weil man mit ihrer Hilfe einen Schlüsseltausch nach Diffie-Hellman durchführen will, so möchte man vielleicht das Gruppenelement

$$(\sigma_{67} \circ \tau_{13} \circ \sigma_{34} \circ \tau_{55})^{42} \tag{8}$$

berechnen, wobei in diesem Ausdruck die in Satz 20 eingeführte Notation verwendet wird. Das wird man normalerweise nicht per Hand, sondern mit einem Computer erledigen, unabhängig davon stellen sich aber folgende Fragen:

- In welcher Form will man das Ergebnis erhalten?
- Wie findet man dieses Ergebnis systematisch?

Die beiden Fragen hängen natürlich zusammen.

Eine einfache Antwort auf die erste Frage ist die folgende: Man nummeriert die Elemente der Gruppe G in einer im Prinzip beliebigen Weise,

$G = \{g_1, g_2, \ldots, g_n\}$. Ein Verfahren zur Berechnung eines Ausdrucks wie zum Beispiel (8) soll dann die Nummer $e \in \{1, \ldots, n\}$ desjenigen Gruppenelements liefern, das als Ergebnis der Auswertung des betrachteten Ausdrucks entsteht. Die Auswertung des Ausdrucks selbst kann in diesem Fall nur mit Hilfe einer Verknüpfungstafel erfolgen, was auch die zweite Frage beantwortet. Dieses Vorgehen ist allerdings bei großen Gruppen sehr unhandlich, weil man die dann große Verknüpfungstafel vollständig speichern muss um sie für die Ergebnissuche nutzen zu können.

Eine effizientere Form der Darstellung eines Ergebnisses wurde für die Diedergruppe D_n mit Satz 24 vorgestellt. Zur Darstellung eines beliebigen Gruppenelements werden hier nur die *zwei* Elemente τ und σ benötigt. Die Variation der Exponenten in den Termen $\tau^k \circ \sigma^\ell$ liefert dann alle Elemente von D_n. Man beachte hierbei, dass $n \in \mathbb{N}$ beliebig groß sein kann. Die erste Frage kann man für die Gruppe D_n also auch so beantworten: Das Ergebnis soll wieder in der Form $\tau^k \circ \sigma^\ell$ geliefert werden. Die zweite Frage ist dann allerdings schwieriger zu beantworten, da man Ausdrücke der Form (8) systematisch in die Standardform $\tau^k \circ \sigma^\ell$ umformen können muss. Dank der Gleichungen $\sigma \circ \tau = \tau \circ \sigma^{n-1}$, $\tau^2 = \mathrm{id}$ und $\sigma^n = \mathrm{id}$ ist das stets und systematisch möglich:

Satz 25: *Das folgende Verfahren ermittelt für jeden Ausdruck*

$$(\tau^{k_1} \circ \sigma^{\ell_1}) \circ (\tau^{k_2} \circ \sigma^{\ell_2}) \circ \ldots \circ (\tau^{k_r} \circ \sigma^{\ell_r}),\ k_i \in \{0, 1\},\ \ell_i \in \{0, \ldots n-1\},$$

nach endlich vielen Schritten die Standardform

$$\tau^k \circ \sigma^\ell,\ k \in \{0, 1\},\ \ell \in \{0, \ldots n-1\}$$

von Elementen der Diedergruppe D_n.

1. *Setze $T := (\tau^{k_1} \circ \sigma^{\ell_1}) \circ (\tau^{k_2} \circ \sigma^{\ell_2}) \circ \ldots \circ (\tau^{k_r} \circ \sigma^{\ell_r})$, wobei mit T der angegebene, noch nicht ausgerechnete Term gemeint ist.*

2. *Fasse alle unmittelbar nebeneinander stehenden Faktoren τ beziehungsweise alle unmittelbar nebeneinander stehenden Faktoren der Form σ^b zusammen.*

   Ersetze Potenzen τ^a, $a > 1$, und σ^b, $b > n-1$, gemäß der Gleichungen $\tau^2 = \mathrm{id}$ und $\sigma^n = \mathrm{id}$.

3. *Besitzt der Term T die Standardform, so stoppe das Verfahren mit dem Term T als Ergebnis.*

   Besitzt T nicht die Standardform, gehe zu Schritt 4.

4. *Sei $\sigma^a \circ \tau$ der von links betrachtet erste in T vorkommende Teilterm dieser Form.*

   Ersetze diesen Teilterm in T durch den Term $\tau \circ \sigma^{a(n-1)}$ – nach der Gleichung $\sigma \circ \tau = \tau \circ \sigma^{n-1}$ gilt $\sigma^a \circ \tau = \tau \circ \sigma^{a(n-1)}$ in D_n.

5. *Fasse alle unmittelbar nebeneinander stehenden Faktoren τ beziehungsweise alle unmittelbar nebeneinander stehenden Faktoren der Form σ^b zusammen.*

   Ersetze Potenzen τ^a, $a > 1$, und σ^b, $b > n-1$, gemäß der Gleichungen $\tau^2 = \mathrm{id}$ und $\sigma^n = \mathrm{id}$.

6. *Besitzt der Term T die Standardform, so stoppe das Verfahren mit dem Term T als Ergebnis.*

   Besitzt T nicht die Standardform, gehe zu Schritt 2.

Beweis: Es ist nur zu zeigen, dass das angegebene Verfahren nach endlich vielen Schritten zum Ende kommt. Um dies zu sehen betrachtet man die Länge $L(T)$ des jeweils umzuformenden Terms T, wobei $L(T)$ definiert ist als Anzahl der Faktoren aus D_n, die in T vorkommen.

Durch die im Schritt 2 vorgenommenen Termumformungen wird die Länge des Terms kleiner oder bleibt gleich.

Durch den Schritt 4 wird die Länge von T nicht geändert.

Im Term T *vor* Durchführung von Schritt 4 stehen Gruppenelemente der Form τ und σ^b stets abwechselnd nebeneinander, da die Schritte 2 beziehungsweise 5 genau solche Terme erzeugen. Folglich steht *nach* Durchführung von Schritt 4 entweder unmittelbar links von $\tau \circ \sigma^{a(n-1)}$ ein τ, oder unmittelbar rechts von $\tau \circ \sigma^{a(n-1)}$ ein σ^b. Insgesamt verkürzt sich der Term T im Schritt 5 mindestens um 1.

Da $L(T)$ endlich ist, muss stoppt das Verfahren nach höchstens $L(T)$ Durchführungen der Schritte 3 und 5. □

Als Beispiel für die Anwendung dieses Verfahrens berechnet man in der

Gruppe D_6 das Produkt $(\tau \circ \sigma^5) \circ (\tau \circ \sigma^5) \circ (\sigma^3) \circ (\tau)$.

$$\begin{array}{rcll}
(\tau \circ \sigma^5) \circ (\tau \circ \sigma^5) \circ (\sigma^3) \circ (\tau) & = & (\tau \circ \sigma^5) \circ (\tau \circ \sigma^8) \circ (\tau) & \text{(Schritt 3)} \\
& = & (\tau \circ \sigma^5) \circ (\tau \circ \sigma^2) \circ (\tau) & \text{(Schritt 3)} \\
& = & \tau \circ (\sigma^5 \circ \tau) \circ \sigma^2 \circ \tau & \text{(Schritt 4)} \\
& = & \tau \circ (\tau \circ \sigma^{25}) \circ \sigma^2 \circ \tau & \text{(Schritt 4)} \\
& = & \tau^2 \circ \sigma^{27} \circ \tau & \text{(Schritt 5)} \\
& = & \sigma^3 \circ \tau & \text{(Schritt 5)} \\
& = & \tau \circ \sigma^{15} & \text{(Schritt 4)} \\
& = & \tau \circ \sigma^3 & \text{(Schritt 5)}
\end{array}$$

Verfahren wie das in Satz 25 beschriebene hängen natürlich von der betrachteten Gruppe G ab, und von der gewählten Standardform für Elemente von G. Dennoch bilden solche Verfahren im Prinzip die Basis von Computeralgebrasystemen, also Programmen, die symbolisch und nicht numerisch rechnen.

Einheitswurzeln und Einheitskreis: Zyklische Gruppen

Satz 26: *Für jedes $n \in \mathbb{N}$ ist die Menge*

$$\mu_n := \{z \in \mathbb{C} : z^n = 1\}$$

zusammen mit der Multiplikation komplexer Zahlen als innerer Verknüpfung eine abelsche Gruppe. Sie besitzt n Elemente und es gilt

$$\mu_n = \{\zeta^k : k \in \{0, \ldots, n-1\}\},\ \zeta_n := \cos(\frac{2\pi}{n}) + i \sin(\frac{2\pi}{n}).$$

Die Elemente von μ_n nennt man n-te Einheitswurzeln.

Beweis: Das Assoziativ- und das Kommutativgesetz gelten in μ_n, weil sie in $\mathbb{C}$ gelten. Sind $z, w \in \mu_n$, so gilt $(zw)^n = z^n w^n = 1 \cdot 1 = 1$, also ist $zw \in \mu_n$. Für jedes $z \in \mu_n$ ist $(z^{-1})^n = (z^n)^{-1} = 1^{-1} = 1$, womit auch die Inversen in μ_n vorhanden sind.

Im Weiteren wird die Exponential- oder Polardarstellung

$$z = re^{i\phi} = rcos(\phi) + i \sin(\phi)$$

komplexer Zahlen verwendet. Mit ihrer Hilfe sieht man sofort, dass $z^n = 1$ nur dann gelten kann, wenn $r = 1$ und $n\phi$ ein Vielfaches von 2π ist.

Das angegebene Element ζ_n lässt sich in Exponentialschreibweise als $\zeta_n = e^{i\frac{2\pi}{n}}$ schreiben. Da die Winkel

$$k\frac{2\pi}{n},\ k \in \{0, \ldots, n-1\},$$

keine Vielfachen von 2π sind, ist n die kleinste natürliche Zahl, für die $\zeta_n^n = 1$ gilt. Daher gilt $\zeta_n \in \mu_n$, und die Potenzen $\zeta_n^0, \zeta_n^1, \ldots, \zeta_n^{n-1}$ sind alle verschieden: Wäre nämlich $\zeta_n^k = \zeta_n^\ell$ mit $\ell > k$, so wäre $\zeta_n^{\ell-k} = 1$, was wegen $\ell - k < n$ ein Widerspruch ist.

Aus $\zeta_n \in \mu_n$ folgt $\zeta_n^k \in \mu_n$ für alle $k \in \mathbb{Z}$, was die Inklusion $\supseteq$ in der dritten Aussage des Satzes beweist. Da das Polynom $X^n - 1$ höchstens n Nullstellen besitzt, kann auch μ_n höchstens n Elemente haben und die zweite Aussage des Satzes ist ebenfalls bewiesen. □

Die Gruppen μ_n teilen sich die interessante Eigenschaft, dass das Rechnen in diesen Gruppen durch die Potenzregeln 16 und 18 vollständig festgelegt ist, da jedes Gruppenelement Potenz des Elements ζ_n ist.

In der Diskussion der Diedergruppe kommt ebenfalls eine Gruppe vor, die diese Eigenschaft besitzt: Die Menge $\{\mathrm{id}, \sigma_1, \ldots, \sigma_{n-1}\}$ der verschiedenen Drehungen eines regelmäßigen n-Ecks bilden zusammen mit der Verkettung $\circ$ als innerer Verknüpfung eine Gruppe. Bei der verwendeten Nummerierung der Drehungen ist σ_k die Drehung um den Winkel $\frac{2\pi}{n}k$ und daher gilt $\sigma_k = \sigma_1^k$.

Tatsächlich bilden Gruppen mit der gerade betrachteten Eigenschaft eine für die Gruppentheorie wichtige Klasse von Gruppen und bekommen deshalb einen eigenen Namen:

Definition 27: *Eine Gruppe $(G, \cdot)$ heißt zyklisch, falls es ein Element $g \in G$ gibt, für welches*

$$G = \{g^k : k \in \mathbb{Z}\}$$

gilt. Mit anderen Worten: Die Elemente von G bestehen aus den Potenzen eines einzigen Elements, sowie deren Inversen.

Das Element g nennt man einen Erzeuger von G und schreibt $G = \langle g \rangle$.

Zyklische Gruppen müssen nicht endlich sein: Die Gruppe $(\mathbb{Z}, +)$ etwa ist eine unendliche zyklische Gruppe, denn das Element $g = 1$ besitzt die Eigenschaft, dass sich jedes $h \in \mathbb{Z}$ in der Form $h = g + g \ldots + g$ (k Summanden) oder als $h = -(g + g \ldots + g)$ (k Summanden) schreiben lässt. Beachtet man, dass hier die Verknüpfung additiv und nicht multiplikativ geschrieben ist, so zeigt dies, dass $(\mathbb{Z}, +)$ zyklisch ist.

Ist $(G, \cdot)$ eine endliche zyklische Gruppe, so kann benötigt man für das Auflisten aller Gruppenelemente durch einen Erzeuger keine negativen Exponenten:

FESTSTELLUNG 28: *Für eine endliche zyklische Gruppe $(G, \cdot)$ mit Erzeuger g gilt*

$$G = \{g^k : k \in \{0, \ldots, n-1\}, \quad n = |G|,$$

und n ist die kleinste natürliche Zahl, für die $g^n = 1$ gilt.

BEWEIS: Die Inklusion $\supseteq$ ist klar.

Wegen der Endlichkeit von G gibt es $k, \ell \in \mathbb{N}$, $\ell > k$ mit $g^\ell = g^k$. Es gilt dann $g^{\ell-k} = 1$ und folglich gibt es eine kleinste natürliche Zahl $m \in \mathbb{N}$ für die $g^m = 1$ gilt. Die Potenzen $g^0, g^1, \ldots, g^m$ sind dann alle verschieden, womit $m \leq n$ folgt. Da g ein Erzeuger ist, muss andererseits $m \geq n$ gelten, womit die Feststellung bewiesen ist. □

In einer zyklischen Gruppe mit mehr als zwei Elementen gibt es immer mehr als einen Erzeuger: In $(\mathbb{Z}, +)$ ist neben 1 auch -1 ein Erzeuger. Es ist leicht nachzuweisen, dass diese beiden Elemente die einzigen Erzeuger sind.

Ist G eine endliche zyklische Gruppe, so kann man alle Erzeuger angeben, wenn man einen kennt:

SATZ 29: *Es sei $(G, \cdot)$ eine endliche zyklische Gruppe mit Erzeuger g. Dann besteht die Menge*

$$\{g^k : k \in \{1, \ldots, n-1\}, \mathrm{ggT}(k, n) = 1\}$$

genau aus den Erzeugern von G. Insbesondere gibt es für $n > 2$ mehr als einen Erzeuger.

BEWEIS: Für $k \in \{1, \ldots, n-1\}$ sei $m := \frac{n}{\mathrm{ggT}(k,n)}$. Dann teilt n das Produkt km, womit $1 = g^{km} = (g^k)^m$ gilt. Ist also $\mathrm{ggT}(k, n) \neq 1$, so kann g^k kein Erzeuger der Gruppe G sein.

Nun gelte $\mathrm{ggT}(k, n) = 1$ und es sei $m \in \mathbb{N}$ die kleinste natürliche Zahl für die $(g^k)^m = 1$ ist. Dann muss km durch n teilbar sein. Nach Voraussetzung ist also n ein Teiler von m. Da m minimal gewählt wurde, ist folglich sogar $m = n$ und die Behauptung ist bewiesen. □

Die Einheitswurzelgruppen μ_n bestehen aus komplexen Zahlen, deren Betrag gleich 1 ist. Geometrisch betrachtet liegen diese Zahlen alle auf dem Einheitskreis

$$S^1 := \{z \in \mathbb{C} : |z| = 1\}$$

und bilden jeweils ein regelmäßiges n-Eck, das eine Ecke im Punkt $1 + 0i$ besitzt. Angesichts dieser Situation sind zwei Fragen naheliegend:

- Bildet die Vereinigungsmenge $\mu := \bigcup_{n\in\mathbb{N}} \mu_n$ eine Gruppe?
- Ist S^1 eine Gruppe?

Natürlich soll in beiden Fällen die komplexe Multiplikation die innere Verknüpfung sein.

Satz 30: *Der Einheitskreis $S^1 \subset \mathbb{C}$ bildet mit der Multiplikation komplexer Zahlen eine abelsche Gruppe mit überabzählbar vielen Elementen. Insbesondere ist S^1 keine zyklische Gruppe.*

Die Teilmenge $\mu \subset S^1$ aller Einheitswurzeln bildet mit der Multiplikation komplexer Zahlen eine nicht zyklische, abelsche Gruppe mit abzählbar unendlich vielen Elementen.

Beweis: Für $z, w \in S^1$ gilt $|zw| = |z|\,|w| = 1$, also $zw \in S^1$. Weiter folgt aus $1 = |zz^{-1}| = |z|\,|z^{-1}|$, dass auch $z^{-1} \in S^1$ gilt. Damit ist S^1 eine abelsche Gruppe. Die Exponentialdarstellung $e^{i\phi}$ komplexer Zahlen in S^1 zeigt die Überabzählbarkeit, da das Winkelintervall $[0, 2\pi)$ überabzählbar ist.

Eine zyklische Gruppe ist (fast) nach Definition endlich oder abzählbar unendlich.

Für $z, w \in \mu$ gilt $z \in \mu_m$ und $w \in \mu_n$ für gewisse $m, n \in \mathbb{N}$. Damit ist $(zw)^{mn} = 1$, also $zw \in \mu_{mn} \subset \mu$. Weiter ist $z^{-1} \in \mu_n \subset \mu$, womit μ eine abelsche Gruppe ist.

Die Vereinigung abzählbar vieler, endlicher Mengen ist abzählbar. Dies wurde zum Beispiel in der Vorlesung »Beweisen und Argumentieren« unter dem Stichwort »Hilbert's Hotel« bewiesen.

μ ist nicht zyklisch, da zu jedem $z \in \mu$ ein $n \in \mathbb{N}$ existiert, für das $z^n = 0$ gilt. Damit kommt kein $z \in \mu$ als Erzeuger von μ in Frage. □

Permutationen: Symmetrische Gruppen

Es sei M eine nicht leere Menge. Im Beispiel 10 wurde das Monoid $(\mathrm{Abb}\,(M), \circ)$ der Selbstabbildungen von M eingeführt. Seine invertierbaren Elemente, also die bijektiven Selbstabbildungen, bilden nach Feststellung 17 eine Gruppe. Um diese Gruppe geht es im vorliegenden Abschnitt.

DEFINITION 31: *Es sei M eine nicht leere Menge. Die Gruppe*

$$S(M) := \mathrm{Abb}\,(M)^\times = \{f : M \to M : f \text{ ist bijektiv.}\}$$

wird als (volle) symmetrische Gruppe von M bezeichnet.

Im Spezialfall $M = \{1, 2, \ldots, n\}$, $n \in \mathbb{N}$, schreibt man auch S_n anstelle von $S(M)$. Die Elemente von S_n nennt man Permutationen (der Zahlen $1, 2, \ldots, n$).

Aus algorithmischer Sicht kann man mit den Elementen der Gruppe $(S_n, \circ)$ gut umgehen, da jedes $\sigma \in S_n$ durch eine endliche Wertetabelle der Form

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix},$$

also durch ein n-Tupel, angegeben werden kann. Ist zum Beispiel:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \quad \sigma' = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix},$$

so kann man leicht

$$\sigma' \circ \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

errechnen.

An dieser Darstellung kann man auch ablesen, dass S_n insgesamt

$$n! = 2 \cdot 3 \cdot 4 \cdots (n-1) \cdot n$$

Elemente besitzt: Man zeigt dies durch vollständige Induktion nach n. Der Induktionsanfang bei $n = 1$ ist klar, da S_1 nur ein Element besitzt. Im Induktionsschritt betrachtet man die Gruppe S_{n+1}. Für die Wahl des Bildes $\sigma(1)$ der 1 einer Permutation σ hat man $n+1$ Möglichkeiten. Ist $\sigma(1)$ gewählt, so permutiert σ die Zahlen $2, \ldots, n+1$. Also gibt es bei festem $\sigma(1)$ nach Induktionsannahme $n!$ Permutationen der Zahlen $2, \ldots, n+1$. Insgesamt ergibt dies $(n+1) \cdot n! = (n+1)!$ Permutationen in der Gruppe S_{n+1}.

Für das Rechnen mit Permutationen gibt es allerdings eine wesentlich bessere Methode als die Nutzung der Wertetabellendarstellung; sie wird im Folgenden entwickelt.

DEFINITION 32: *Für eine Permutation $\sigma \in S_n$ sei*

$$B(\sigma) := \{k : \sigma(k) \neq k\}.$$

Zwei Permutationen $\sigma, \tau \in S_n$ heißen disjunkt, falls $B(\sigma) \cap B(\tau) = \emptyset$ gilt.

Als ersten Schritt hin zu der angestrebten Rechenmethode beweist man:

FESTSTELLUNG 33: *Es seien $\sigma, \tau \in S_n$ disjunkte Permutationen, dann gilt: $\sigma \circ \tau = \tau \circ \sigma$.*

BEWEIS: Die behauptete Identität ist eine Gleichheit von Abbildungen, kann also punktweise für jedes $k \in \{1, \ldots, n\}$ überprüft werden.

Es sei $k \in B(\sigma)$. Dann gilt $k \notin B(\tau)$ und daher

$$(\sigma \circ \tau)(k) = \sigma(\tau(k)) = \sigma(k).$$

Es ist folglich $(\tau \circ \sigma)(k) = \sigma(k)$ zu zeigen. Aus $\sigma(k) \neq k$ folgt $\sigma(\sigma(k)) \neq \sigma(k)$, wegen der Injektivität von σ. Also ist $\sigma(k) \in B(\sigma)$ und damit $\sigma(k) \notin B(\tau)$, das heißt es gilt $\tau(\sigma(k)) = \sigma(k)$, wie angestrebt. □

Die am leichtesten zu verstehenden Permutationen $\sigma \in S_n$ sind diejenigen, die eine bestimmte Teilmenge der Zahlen $\{1, \ldots, n\}$ zyklisch vertauschen: Für $i \neq j$ ist zum Beispiel die Permutation $\sigma(i) = j$, $\sigma(j) = i$, $\sigma(k) = k$ für alle $k \neq i$, $k \neq j$, von dieser Art. Mit drei verschiedenen Zahlen i, j, k kann man die Permutation $\sigma(i) = j$, $\sigma(j) = k$, $\sigma(k) = i$, $\sigma(\ell) = \ell$ für alle $\ell \neq i$, $\ell \neq j$, $\ell \neq k$, bilden. Ganz allgemein:

DEFINITION 34: *Eine Permutation $\sigma \in S_n$ heißt zyklisch oder genauer r-Zykel, falls $B(\sigma)$ aus r verschiedenen Zahlen $k_1, \ldots, k_r$ besteht, für die gilt:*

$$\sigma(k_i) = k_{i+1}, i = 1, \ldots, r, \quad \sigma(k_r) = k_1.$$

Die Permutation σ wird in diesem Fall auch mit dem Symbol $(k_1, \ldots, k_r)$ bezeichnet.

Einen 2-Zykel nennt man auch Transposition.

Bemerkung: In dem Symbol $(k_1, \ldots, k_r)$ kann man die Ziffern k_i zyklisch vertauschen, die dadurch bezeichnete Permutation ändert sich nicht.

Das Rechnen mit zyklischen Permutationen unter Verwendung des oben eingeführten Symbols ist sehr einfach: Man arbeitet die einzelnen Permutationen eines Produkts wie für Abbildungen üblich von rechts nach links ab. Dabei muss man nur diejenigen Zahlen betrachten, die in mindesten einer der (zyklischen) Faktoren vorkommen; alle anderen werden vom Produkt festgelassen. Das folgende Beispiel zeigt das Prinzip:

$$\sigma := (3, 5, 7) \circ (1, 2, 7, 4) \circ (6, 8, 9)$$

Man beginnt mit der Zahl 1:

$$\sigma(1) = ((3,5,7) \circ (1,2,7,4) \circ (6,8,9))(1) = ((3,5,7) \circ (1,2,7,4))(1) = (3,5,7)(2) = 2$$
$$\sigma(2) = ((3,5,7) \circ (1,2,7,4) \circ (6,8,9))(2) = ((3,5,7) \circ (1,2,7,4))(2) = (3,5,7)(7) = 3$$
$$\sigma(3) = ((3,5,7) \circ (1,2,7,4) \circ (6,8,9))(3) = ((3,5,7) \circ (1,2,7,4))(3) = (3,5,7)(3) = 5$$
$$\sigma(4) = ((3,5,7) \circ (1,2,7,4) \circ (6,8,9))(4) = ((3,5,7) \circ (1,2,7,4))(4) = (3,5,7)(1) = 1$$
$$\sigma(5) = ((3,5,7) \circ (1,2,7,4) \circ (6,8,9))(5) = ((3,5,7) \circ (1,2,7,4))(5) = (3,5,7)(5) = 7$$
$$\sigma(6) = ((3,5,7) \circ (1,2,7,4) \circ (6,8,9))(6) = ((3,5,7) \circ (1,2,7,4))(8) = (3,5,7)(8) = 8$$
$$\sigma(7) = ((3,5,7) \circ (1,2,7,4) \circ (6,8,9))(7) = ((3,5,7) \circ (1,2,7,4))(7) = (3,5,7)(4) = 4$$
$$\sigma(8) = ((3,5,7) \circ (1,2,7,4) \circ (6,8,9))(8) = ((3,5,7) \circ (1,2,7,4))(9) = (3,5,7)(9) = 9$$
$$\sigma(9) = ((3,5,7) \circ (1,2,7,4) \circ (6,8,9))(9) = ((3,5,7) \circ (1,2,7,4))(6) = (3,5,7)(6) = 6$$

Es wird sich zeigen, dass zyklische Permutationen die Bausteine sind, aus denen sich alle Permutationen zusammensetzen. Zunächst sammelt man jedoch einige grundlegende Eigenschaften dieses Permutationstyps:

FESTSTELLUNG 35: *Für zyklische Permutationen gilt:*

1. *Ist σ ein r-Zykel, so gilt für jedes $k \in B(\sigma)$*

$$B(\sigma) = \{k, \sigma(k), \sigma^2(k), \ldots, \sigma^{r-1}(k)\}.$$

2. $(k_1, \ldots, k_r)^r = \mathrm{id}$ *und* $(k_1, \ldots, k_r)^s \neq \mathrm{id}$ *für alle* $s \in \{1, \ldots, r-1\}$.

3. $(k_1, \ldots, k_r)^{-1} = (k_r, \ldots, k_1)$.

4. $(k_1, \ldots, k_r) = (k_1, \ldots, k_i) \circ (k_i, \ldots, k_r)$.

5. $(k_1, \ldots, k_r) = (k_1, k_2) \circ \ldots \circ (k_{r-1}, k_r)$.

BEWEIS: Zu 1.: Ist $\sigma = (k_1, \ldots, k_r)$, so gilt für $k = k_i$: $k_j = \sigma^{j-i}(k)$ für alle $j > i$, also insbesondere $k_r = \sigma^{r-i}(k)$. Es folgt $k_1 = \sigma^{r-i+1}(k)$, $k_2 = \sigma^{r-i+2}(k)$, ..., $k_{i-1} = \sigma^{r-1}(k)$.

Zu 2.: Wegen der Gleichungen $\sigma(k_i) = k_{i+1}$ und $\sigma(k_r) = k_1$ ist die Identität $\sigma^r = \mathrm{id}$ klar. Ist aber $s < r$ eine natürliche Zahl, so gilt $\sigma^s(k_1) = k_{s+1} \neq k_1$, womit $\sigma^s \neq \mathrm{id}$ gilt.

Zu 3.: Man berechnet die Bilder der Verkettung $\sigma := (k_1, \ldots, k_r) \circ (k_r, \ldots, k_1)$ Zahl für Zahl. Ist $k \neq k_i$, $i = 1, \ldots, r$, so wird k sowohl von $(k_1, \ldots, k_r)$ als auch von $(k_r, \ldots, k_1)$ unverändert gelassen; also $\sigma(k) = k$ in diesem Fall.

Eine Zahl k_i für $i \neq 1$ wird von $(k_r, \ldots, k_1)$ auf k_{i-1} abgebildet; letztere wird von $(k_1, \ldots, k_r)$ auf k_i abgebildet. Also $\sigma(k_i) = k_i$. Schließlich wird k_1 von $(k_r, \ldots, k_1)$ auf k_r und letztere von $(k_1, \ldots, k_r)$ auf k_1 abgebildet. Es folgt $\sigma = \mathrm{id}$.

Zu 4.: Man rechnet diese Identität analog zum Punkt 3 Zahl für Zahl nach.

Zu 5.: Folgt durch wiederholte Anwendung von Punkt 4. Ein Beweis wird als durch Induktion nach r geführt – Übungsaufgabe. □

Nun also zu der Aussage zyklische Permutationen seien die Bausteine der Permutationen:

SATZ 36: *Jede Permutation $\sigma \in S_n$ lässt sich als Produkt*

$$\sigma = \sigma_1 \circ \sigma_2 \circ \ldots \circ \sigma_m \tag{9}$$

zyklischer Permutationen σ_i schreiben, wobei je zwei Permutationen $\sigma_i \neq \sigma_j$ disjunkt sind. Bis auf die Reihenfolge der σ_i ist die Zykeldarstellung (9) durch σ eindeutig bestimmt.

BEWEIS: Mit Hilfe des folgenden, programmierbaren Verfahrens, kann man eine Zykeldarstellung (9) von σ ermitteln.

1. $Z := \{1, 2, \ldots, n\}$, $t := 1$.
2. Wähle ein $k \in Z$, etwa das kleinste Element, und berechne $\sigma(k), \sigma^2(k), \ldots$ bis zu der ersten natürlichen Zahl $e \in \mathbb{N}$, für die $\sigma^e(k) = k$ gilt.
3. Ist $e > 1$, so setze $\sigma_t := (k, \sigma(k), \sigma^2(k), \ldots, \sigma^{e-1}(k))$.
4. Ersetze Z durch $Z \setminus \{k, \sigma(k), \sigma^2(k), \ldots, \sigma^{e-1}(k)\}$.
5. Ist $Z \neq \emptyset$, so ersetze t durch $t + 1$ und gehe zu Schritt 2.
6. Ist $Z = \emptyset$: Beende das Verfahren mit $\sigma_1, \ldots, \sigma_m$ als Ergebnis.

Das Verfahren liefert disjunkte Permutationen: Es sei $k \in B(\sigma_i) \cap B(\sigma_j)$. Dann gilt nach Punkt 1 von Feststellung 35 $B(\sigma_i) = B(\sigma_j)$. Dies ist nach Konstruktion (Schritte 2 und 4) nur für $i = j$ möglich.

Das Produkt der σ_i ist σ: Zu $k \in \{1, \ldots, n\}$ gibt es wegen der Disjunkheit der σ_i genau einen Index j mit $k \in B(\sigma_j)$. Nach Schritt 2 gilt dann

$$(\sigma_1 \circ \sigma_2 \circ \ldots \circ \sigma_m)(k) = \sigma_j(k) = \sigma(k).$$

Die Darstellung (9) ist eindeutig: Es gelte

$$\sigma_1 \circ \sigma_2 \circ \ldots \circ \sigma_m = \tau_1 \circ \tau_2 \circ \ldots \circ \tau_r, \tag{10}$$

mit paarweise disjunkten Zykeln σ_i und paarweise disjunkten Zykeln τ_i. Es sei $k \in B(\sigma_m)$. Dann gibt es genau ein j mit $k \in B(\tau_j)$ und Punkt 1 von Feststellung 35 liefert $B(\sigma_m) = B(\tau_j)$ also $\sigma_m = \tau_j$. Verknüpft man die Gleichung (10) von rechts mit σ_m^{-1} und berücksichtigt die Vertauschbarkeit disjunkter Permutationen (Feststellung 33), so ergibt sich die Gleichung

$$\sigma_1 \circ \sigma_2 \circ \ldots \circ \sigma_{m-1} = \tau_1 \circ \tau_2 \circ \ldots \circ \tau_{j-1} \circ \tau_{j+1} \circ \ldots \circ \tau_r.$$

Die Argumentation lässt sich nun wiederholen. □

Das folgende Beispiel illustriert den im Beweis von Satz 36 beschriebenen Algorithmus:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 4 & 3 & 2 & 7 & 6 & 9 & 1 & 10 & 5 & 8 \end{pmatrix}$$

Für $k = 1$ erhält man die zyklische Permutation $\sigma_1 := (1, 4, 7)$. Nach diesem Schritt ist also $Z = \{2, 3, 5, 6, 8, 9, 10\}$ und man kann mit $k = 2$ fortsetzen. Dies liefert $\sigma_2 = (2, 3)$ und damit $Z = \{5, 6, 8, 9, 10\}$. Setzt man mit $k = 5$ fort, ergibt sich $\sigma_3 = (5, 6, 9)$ und $Z = \{8, 10\}$. Schließlich erhält man $\sigma_4 = (8, 10)$ und damit $m = 4$. Die Zykeldarstellung von σ lautet

$$\sigma = (1, 4, 7) \circ (2, 3) \circ (5, 6, 9) \circ (8, 10).$$

Das Rechnen mit Permutationen ist aufgrund von Satz 36 und(!) seinem konstruktiven Beweis sehr gut in Software realisierbar.