$\circ$	d_0	d_{120}	d_{240}	s_1	s_2	s_3
d_0	d_0	d_{120}	d_{240}	s_1	s_2	s_3
d_{120}	d_{120}	d_{240}	d_0	s_2	s_3	s_1
d_{240}	d_{240}	d_0	d_{120}	s_3	s_1	s_2
s_1	s_1	s_3	s_2	d_0	d_{240}	d_{120}
s_2	s_2	s_1	s_3	d_{120}	d_0	d_{240}
s_3	s_3	s_2	s_1	d_{240}	d_{120}	d_0

Tabelle 1.5: Deckabbildungen des gleichseitigen Dreiecks

1) Das Neutralelement ist d_0. Es ist id, die identische Abbildung, die jeden Punkt der Ebene auf sich selbst abbildet.
2) $(K, \circ)$ ist nicht kommutativ, wie man d. h. an $s_3 \circ d_{120} = s_2 \neq s_1 = d_{120} \circ s_3$ ablesen kann
3) Jede Spiegelung ist zu sich selbst invers (d. h. $s_i^2 = d_0$ für alle $1 \leq i \leq 3$) und zu jeder Drehung d_a ist d_{360-a} das Inverse.

1.2.3 Untergruppen

Definition 9 Es sei $(G, \circ)$ eine Gruppe und $U \subseteq G$ eine Teilmenge von G. Ist $(U, \circ)$ ebenfalls eine Gruppe, so nennt man $(U, \circ)$ eine *Untergruppe* von $(G, \circ)$, in Zeichen $U \leq G$.

Beispiel 9 Die Gruppe K der Deckabbildungen des gleichseitigen Dreiecks enthält die folgenden Untergruppen:

1) K selbst.
2) Die Gruppe der Deckdrehungen $D = \{d_0, d_{120}, d_{240}\}$.
3) Drei Untergruppen, die jeweils aus einer Spiegelung und dem Neutralelement bestehen, nämlich $S_1 = \{d_0, s_1\}$, $S_2 = \{d_0, s_2\}$ und $S_3 = \{d_0, s_3\}$.
4) Die Gruppe $\{d_0\}$, die nur aus dem Neutralelement besteht.

Jede Gruppe G hat die beiden Untergruppen G und $\{e\}$. Man nennt sie auch die trivialen Untergruppen.

Definition 10 Es sei $(G, \circ)$ und $g \in G$.

1) Man nennt $|G|$ die *Ordnung* von G.
2) Falls es ein $n \in N$ gibt mit $g^n = e$ und dieses n ist die kleinste natürliche Zahl mit dieser Eigenschaft ist, dann nennt man n die Ordnung von g und schreibt $|g| = n$. Falls es eine solches n nicht gibt, ist $|g| = \infty$.

Satz 5 *Es sei $(G, \circ)$ und $g \in G$ mit $|g| = n \in \mathbb{N}$. Dann ist $U = \{g^1, g^2, \ldots, g^n\}$ eine Untergruppe von G.*

BEWEIS Übung.

Definition 11 Es sei $(G, \circ)$ eine Gruppe und $U \leq G$ eine Untergruppe von G. Ferner sei $g \in G$. Dann nennt man die Mengen ...

1) ... $gU = \{g \circ u \mid u \in U\}$ die *Linksnebenklasse* von U bezüglich g und ...
2) ... $Ug = \{u \circ g \mid u \in U\}$ die *Rechtsnebenklasse* von U bezüglich g.

Ist $gU = Ug$, so spricht man von einer *Nebenklasse*. Man bezeichnet mit G/U die Menge der Linksnebenklassen und mit $U\backslash G$ die Menge der Rechtsnebenklassen von U in G.

Beispiel 10 Aus der Verknüpfungstafel der Deckabbildungen des gleichseitigen Dreiecks (Abb. 1.5) kann man für die Untergruppe der Deckdrehungen $D = \{d_0, d_{120}, d_{240}\}$ ablesen, dass $s_1D = \{s_1, s_2, s_3\} = Ds_1$. Links- und Rechtsnebenklasse bezüglich s_1 sind also identisch, d. h. eine Nebenklasse liegt vor. Dasselbe gilt auch für die anderen Spiegelungen, d. h. es ist $s_iD = \{s_1, s_2, s_3\} = Ds_i$ für alle $1 \leq i \leq 3$.

Ebenso kann man ablesen, dass $d_{120}D = \{d_0, d_{120}, d_{240}\}$ ist, d. h. in diesem Fall ist die Nebenklasse $d_{120}D$ mit der Untergruppe D identisch. Dies gilt allgemein: Die Untergruppe U ist immer auch eine der Nebenklassen von U.

Als weiteres Beispiel kann man ablesen, dass für $S_1 = \{d_0, s_1\}$ und s_2 gilt, dass $s_2S_1 = \{s_2, d_{120}\}$ und $S_1s_2 = \{s_2, d_{240}\}$ ist, d. h. Links- und Rechtsnebenklasse sind in diesem Fall nicht identisch. Analog sieht man, dass $s_3S_1 = \{s_3, d_{240}\}$ und $S_1s_3 = \{s_3, d_{120}\}$ gilt. Wie zu erwarten, lässt ein Element der Gruppe die Untergruppe unverändert $s_1S_1 = \{d_0, d_{120}\} = S_1s_1$.

Außerdem ist für $S_1 = \{d_0, s_1\}$ ersichtlich: $s_1S_1 = \{d_0, s_1\} = S_1$, $s_2S_1 = \{s_2, d_{120}\}$ und $s_3S_1 = \{s_3, d_{240}\}$. Damit kommt jedes Element aus G in einer Nebenklasse von S_1 vor, und zwar so, dass jedes Element in genau einer Nebenklasse liegt. Betrachtet man außerdem die Nebenklassen, welche durch die Drehungen induziert werden, nämlich $d_0S_1 = \{d_0, s_1\} = S_1$, $d_{120}S_1 = \{s_2, d_{120}\}$ und $d_{240}S_1 = \{s_3, d_{240}\}$, so findet man keine neuen Nebenklassen. Bei den identischen Nebenklassen, z. B. $s_2S_1 = d_{120}S_1$, fällt auf, dass $d_{120}^{-1} \circ s_2 = d_{240} \circ s_2 = s_1 \in S_1$ und $s_2^{-1} \circ d_{120} = s_2 \circ d_{120} = s_1 \in S_1$ gilt.

Lemma 1 *Es sei $(G, \circ)$ eine Gruppe und $U \leq G$ eine Untergruppe von G. Dann gilt für alle $g, h \in G$:*

1) $gU = U \Leftrightarrow g \in U$
2) $gU = hU \Leftrightarrow h^{-1}g \in U$
3) $gU \cap hU \neq \emptyset \Leftrightarrow gU = hU$
4) $|U| = |gU| = |hU|$

Die Nebenklassen von U bilden also eine Partition von G, d. h. sie induzieren eine Äquivalenzrelation auf G: Jedes Element von G liegt in genau einer Nebenklasse von U. Außerdem sind alle Nebenklassen gleichmächtig zueinander.

BEWEIS

1) Es gelte $gU = U$. Dann gibt es ein $u \in U$ mit $g \cdot u \in U$. Es sei $u' = g \cdot u$ für dieses u. Dann ist $g = u' \cdot u^{-1}$. Da $u' \cdot u^{-1} \in U$ ist, ist also $g \in U$. Nun sei umgekehrt $g \in U$. Dann gilt $gU \subseteq U$, da Untergruppen abgeschlossen sind. Aus demselben Grund gilt auch $g^{-1}U \subseteq U$. Dann ist aber $U = g(g^{-1}U) \subseteq gU \subseteq U$, also $U = gU$.
2) Als Anwendung von 1) ergibt sich $gU = hU \Leftrightarrow h^{-1}gU = U$. Das ist genau dann der Fall, wenn $h^{-1}g \in U$ erfüllt ist.
3) Falls $gU = hU$, so ist $gU \cap hU = gU \neq \emptyset$. Falls umgekehrt $gU \cap hU \neq \emptyset$ ist, dann gibt es ein $k \in gU \cap hU$. Folglich gibt es $u, u' \in U$ mit $k = g \circ u$ und $k = h \circ u'$, also $g \circ u = h \circ u'$ bzw. $h^{-1} \circ g = u' \circ u^{-1} \in U$. Nach 2) ist daher $gU = hU$.
4) Man betrachte die Abbildungen $a : U \to gU : x \mapsto g \circ x$ und $b : U \to Ug : x \mapsto x \circ g$. Da G regulär ist, sind a und b bijektiv, d. h. es ist $|U| = |gU| = |hU|$.

Definition 12 Es sei $(G, \circ)$ eine Gruppe und $U \leq G$ eine Untergruppe von G. Dann nennt man die Anzahl der verschiedenen Nebenklassen von U in G

$$[G : U] := |\{gU \mid g \in G\}| = |\{Ug \mid g \in G\}|$$

den *Index* von U in G.

Satz 6 (Satz von Lagrange) *Es sei $(G, \circ)$ eine Gruppe und $U \leq G$ eine Untergruppe von G. Dann gilt*

$$|G| = [G : U] \cdot |U|$$

Insbesondere gilt: Wenn G endlich ist, dann sind $|U|$ und $[G : U]$ Teiler von $|G|$.

BEWEIS Nach Lemma 1 bilden die Nebenklassen G/U von U eine Äquivalenzrelation mit gleichmächtigen Äquivalenzklassen auf G. Es sei $R \subseteq G$ ein Repräsentantensystem von G/U, d. h. R enthält aus jeder Nebenklasse von G/U genau ein Element r, d. h. es ist $|R| = [G : U]$. Dann ist

$$G = \bigcup_{r \in R} rU$$

Da diese Vereinigung nach Lemma 1 disjunkt ist, gilt $|G| = |R| \cdot |U|$, also $|G| = [G : U] \cdot |U|$.

Bemerkung 3 In Beispiel 9 hat man gesehen: Die Gruppe K der Deckabbildungen hat die Ordnung $|K| = 6$. Die Untergruppen haben die Ordnungen $1, 2, 3$ und 6. Nach dem Satz von Lagrange ist klar, dass es Untergruppen zu anderen Ordnungen nicht geben kann, da 6 keine weiteren Teiler hat. Der Satz von Lagrange sagt für endliche Gruppen G allerdings nur aus: Wenn eine Untergruppe U existiert, so ist $|U|$ ein Teiler von $|G|$, nicht aber, dass es zu jedem Teiler von $|G|$ tatsächlich eine Untergruppe U von G gibt. Dass das bei den Deckabbildungen K des gleichseitigen Dreiecks so ist, ist ein Sonderfall, und nicht die Regel.

Außerdem sieht man an Beispiel 9: Die Untergruppe D der Ordnung $|D| = 3$ hat zwei Nebenklassen (nämlich D selbst und $\{s_1, s_2, s_3\}$), die Untergruppen der Spiegelungen haben jeweils die Ordnung 2 und jeweils drei Nebenklassen. Insgesamt ergibt

sich als Produkt von Gruppenordnung und Anzahl der Nebenklassen also stets die Gruppenordnung $|G| = 6$.

Korollar 1 *Es sei $(G, \circ)$ eine endliche Gruppe und $g \in G$, so ist $|g|$ ein Teiler von $|G|$.*

Korollar 2 (Kleiner Satz von Fermat) *Es sei $(G, \circ)$ eine endliche Gruppe. Dann gilt $g^{|G|} = e$ für jedes $g \in G$.*

Definition 13 (Kern eines Homomorphismus) Es seien $(G, \circ)$ und $(H, *)$ Gruppen. Ist $\varphi : G \to H$ ein Homomorphismus, so nennt man

$$Kern(\varphi) := \{g \in G \mid \varphi(g) = e_H\}$$

den *Kern* von φ, d. h. die Menge aller Elemente von G, die φ auf das Neutralelement von H abbildet.

Satz 7 *Es seien $(G, \circ)$ und $(H, *)$ Gruppen und $\varphi : G \to H$ ein Homomorphismus. Ferner seien $U \leq G$ und $V \leq H$ Untergruppen von G bzw. H und $g \in G$. Dann gilt:*

1) *$\varphi(e_G) = e_H$, also $e_G \in Kern(\varphi)$.*
2) *$\varphi(g^n) = \varphi(g)^n$ für alle $n \in \mathbb{Z}$, d. h. Bilder von Potenzen sind Potenzen der Bilder.*
3) *$\varphi(U) \leq H$, d. h. Untergruppen von G werden auf Untergruppen von H abgebildet.*
4) *$\varphi^{-1}(V) \leq G$, d. h. Urbilder von Untergruppen von H sind Untergruppen von G.*
5) *$Kern(\varphi) \leq G$, d. h. der Kern von φ ist eine Untergruppe von G.*
6) *Genau dann, wenn $Kern(\varphi) = \{e_G\}$ gilt, ist φ injektiv.*

BEWEIS

1) Es gilt $\varphi(e_G) = \varphi(e_G \circ e_G) = \varphi(e_G) * \varphi(e_G) = e_H * e_H = e_H$.
2) Beweis durch vollständige Induktion für $n \in \mathbb{N}_0$. Für negative Exponenten gilt dann $e_H = \varphi(e_G) = \varphi(g^n \circ g^{-n}) = \varphi(g^n) * \varphi(g^{-n}) = \varphi(g)^n * \varphi(g^{-n})$. Daraus ergibt sich $\varphi(g)^{-n} = \varphi(g^{-n})$.
3) Es sei $V = \varphi(U)$. Zu zeigen ist, dass V abgeschlossen ist und das Neutralelement enthält: Für $e_G \in U$ gilt $\varphi(e_G) = e_H$ nach Teil 1), also ist $e_H \in V$. Für $u \in U$ gilt $e_H = \varphi(e_G) = \varphi(u \circ u^{-1}) = \varphi(u) * \varphi(u^{-1})$, also $\varphi(u)^{-1} = \varphi(u^{-1}) \in V$. Für $u, v \in U$ gilt $\varphi(u) * \varphi(v) = \varphi(u \circ v) \in V$.
4) Analog zu 3).
5) Da $\varphi(Kern(\varphi)) = \{e_H\} \leq H$ eine Untergruppe von H ist, ist nach 4) der Kern von φ eine Untergruppe von G.
6) Nach 1) ist $e_G \in Kern(\varphi)$. Wenn φ injektiv ist, so enthält $Kern(\varphi)$ keine weiteren Elemente, also ist $Kern(\varphi) = \{e_G\}$. Nun sei umgekehrt $Kern(\varphi) = \{e_G\}$. Dann gilt nach Definition eines Homomorphismus und nach Teil 2) für alle $g, h \in G$ mit $\varphi(g) = \varphi(h)$ (also mit $\varphi(g) * \varphi(h)^{-1} = e_H$):

$$\varphi(g \circ h^{-1}) = \varphi(g) * \varphi(h^{-1}) = \varphi(g) * \varphi(h)^{-1} = e_H$$

Daher ist $g \circ h^{-1} \in Kern(\varphi)$. Da aber $Kern(\varphi) = \{e_G\}$ ist, gilt $g \circ h^{-1} = e_G$, also $g = h$, d. h. die Urbilder sind identisch und φ ist damit injektiv.

1.2.4 Permutationsgruppen

Definition 14 (Permutation) Es sei M eine eine endliche Menge und $\pi : M \to M$ eine bijektive Abbildung, so nennt man π eine *Permutation* von M und $Sym(M)$ bezeichnet die Menge aller Permutationen von M.

Bemerkung 4 Da jede endliche Menge M mit $|M| = n$ gleichmächtig ist zur Menge $\{1, 2, \ldots, n\}$, wird im weiteren $M = \{1, 2, \ldots, n\}$ vorausgesetzt, d. h. es werden fortan nur Permutation der ersten n natürlichen Zahlen betrachtet.

Definition 15 Es sei $M = \{1, 2, \ldots, n\}$ und $\pi \in Sym(M)$, dann nennt man

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

die Matrixdarstellung von π. Genauso wie Deckabbildungen werden Permutationen als Rechtsoperatoren geschrieben, d. h. $(n)\pi$ ist das Bild von n unter π

Beispiel 11 Es sei $M = \{1, 2, 3, 4\}$ und

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

Dann gilt $(1)\pi = 3$, $(2)\pi = 2$, $(3)\pi = 4$ und $(4)\pi = 1$ bzw.

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

und

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

Es wird nämlich (von links nach rechts zu lesen) vom ersten π die 4 auf die 1 und vom zweiten π die 1 auf die 3 abgebildet, also insgesamt die 4 auf die 3, d. h. es gilt $(4)\pi^2 = (4)(\pi \circ \pi) = ((4)\pi)\pi) = (1)\pi = 3$. Geht man die übrigen drei Zahlen 1, 2 und 3 durch, so ergibt sich insgesamt

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

Dabei ist $\circ$ (wie gewohnt) die Verkettung oder Hintereinanderausführung von Abbildungen.

Satz 8 *Es sei $M = \{1, 2, \ldots, n\}$. Dann ist $(Sym(M), \circ)$ eine Gruppe.*

BEWEIS
1) Inverse: Da alle Elemente von $Sym(M)$ bijektiv sind, existiert zu jedem $\pi \in Sym(M)$ eine Umkehrabbildung $\pi^{-1} \in Sym(M)$. Das ist das Inverse zu π, da für alle $m \in M$ gilt $(m)(\pi \circ \pi^{-1}) = ((m)\pi)\pi^{-1}) = m$ und $(m)(\pi^{-1} \circ \pi) = ((m)\pi^{-1})\pi) = m$.
2) Assoziativität: Die Assoziativität gilt allgemein für die Verkettung von Funktionen.
3) Neutralelement: Das Neutralelement ist die identische Abbildung.
4) Abgeschlossenheit: Es seien $\pi, \rho \in Sym(M)$. Da π und ρ bijektiv sind, gibt es nach 1) zu ihnen die Umkehrabbildungen π^{-1} und ρ^{-1}. Dann ist $\rho^{-1} \circ \pi^{-1}$ die Umkehrabbildung zu $\pi \circ \rho$, da für alle $m \in M$ gilt $(m)\rho \circ \pi \circ \pi^{-1} \circ \rho^{-1} = (((((m)\pi)\rho)\rho^{-1})\pi^{-1}) = ((m)\pi)\pi^{-1} = m$.

Satz 9 (Satz von Cayley) *Es sei G eine endliche Gruppe mit $|G| = n$. Dann gibt es eine Untergruppe $U \leq Sym(n)$, sodass G isomorph zu U ist.*

BEWEIS Man betrachte für jedes $g \in G$ die Abbildung $\lambda_g : G \to G : x \mapsto g \circ x$. Da Gruppen regulär sind, ist λ_g bijektiv. Ferner gilt für alle $g, h \in G$:

$$(\lambda_g \circ \lambda_h)(s)\lambda_g(\lambda_h(x)) = g \circ (h \circ x) = (g \circ h) \circ x = \lambda_{g \circ h}(x)$$

Damit ist die Abbildung $\lambda : G \to Sym(G) : g \mapsto \lambda_g$ ein Homomorphismus. Zu zeigen ist noch, dass λ injektiv ist. Es gelte $\lambda_g = id$. Dann ist $g = \lambda_g(e) = id(e) = e$, d. h. es ist $Kern(\lambda) = \{e\}$. Nach Satz 7 ist λ damit injektiv.

Beispiel 12 Betrachten wir noch einmal die Deckabbildungen des gleichseitigen Dreiecks aus dem Beispiel 8, aber zu Anfang nur die Untergruppe der Deckdrehungen, um die Darstellung etwas kürzer zu halten:

$\circ$	d_0	d_{120}	d_{240}
d_0	d_0	d_{120}	d_{240}
d_{120}	d_{120}	d_{240}	d_0
d_{240}	d_{240}	d_0	d_{120}

Tabelle 1.6: Gruppe D Deckdrehungen des gleichseitigen Dreiecks

Wenn man die Ecken eines gleichseitigen Dreiecks mit den Zahlen 1, 2 und 3 durchnummeriert, so kann man jeder Drehung aus D eine entsprechende Permutation der der Eckpunkte des Dreiecks zuordnen (durch die Permutation der Eckpunkte ist die Deckabbildung des Dreiecks eindeutig charakterisiert):

$$d_0 \mapsto \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$

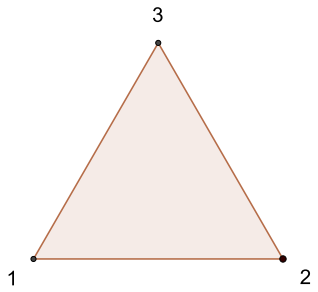

Abbildung 1.2: Gleichseitiges Dreieck mit den Eckpunkten 1, 2 und 3

$$d_{120} \mapsto \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$
$$d_{240} \mapsto \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

Auf diese Weise hat man einen Isomorphismus zwischen der Gruppe $(D, \circ)$ der Deckdrehungen des gleichseitigen Dreiecks und einer Untergruppe U von $Sym(3)$ hergestellt. Der Vergleich der beiden Verknüpfungstafeln lässt die Isomorphie erkennen:

$\circ$	$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$
$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$
$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$
$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$	$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$

Tabelle 1.7: Isomorphe Untergruppe U von $Sym(3)$

Auf diese Weise kann man den Isomorphismus auf die gesamte Gruppe K der Deckabbildungen des gleichseitigen Dreiecks erweitern:

$$d_0 \mapsto \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$$
$$d_{120} \mapsto \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$
\begin{aligned}
d_{240} &\mapsto \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \\
s_1 &\mapsto \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \\
s_2 &\mapsto \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \\
s_3 &\mapsto \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}
\end{aligned}
$$

Dieser Isomorphismus ist allerdings nicht derjenigen, von dem im Satz von Caley die Rede ist, denn K hat die Ordnung 6, d. h. nach dem Satz von Caley wird ein Isomorphismus zu einer Untergruppe in $Sym(6)$, und nicht in $Sym(3)$ konstruiert. Aus dem Beweis zum Satz von Caley ist diese Konstruktion direkt ablesbar. Man nummeriert die Gruppenelemente durch und liest ab, wie jede Verknüpfung mit einem Gruppenelement von links (in der Spalte links) die Elemente der Gruppe permutiert. In der folgenden Verknüpfungstafel ist die Nummerierung eingetragen:

$\circ$	d_0 (1)	d_{120} (2)	d_{240} (3)	s_1 (4)	s_2 (5)	s_3 (6)
d_0 (1)	d_0 (1)	d_{120} (2)	d_{240} (3)	s_1 (4)	s_2 (5)	s_3 (6)
d_{120} (2)	d_{120} (2)	d_{240} (3)	d_0 (1)	s_2 (5)	s_3 (6)	s_1 (4)
d_{240} (3)	d_{240} (3)	$d_0(1)$	$d_{120}(2)$	s_3 (6)	s_1 (4)	s_2 (5)
s_1 (4)	s_1 (4)	s_3 (6)	s_2 (5)	d_0 (1)	d_{240} (3)	d_{120} (2)
s_2 (5)	s_2 (5)	s_1 (4)	s_3 (6)	d_{120} (2)	d_0 (1)	d_{240} (3)
s_3 (6)	s_3 (6)	s_2 (5)	s_1 (4)	d_{240} (3)	d_{120} (2)	d_0 (1)

Tabelle 1.8: Deckabbildungen des gleichseitigen Dreiecks durchnummiert

Aus der nummerierten Verknüpfungstafel lässt sich der Isomorphismus, der aus dem Beweis zum Satz von Caley folgt, direkt ablesen:

$$
\begin{aligned}
d_0 &\mapsto \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} \\
d_{120} &\mapsto \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 5 & 6 & 4 \end{pmatrix} \\
d_{240} &\mapsto \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 2 & 6 & 4 & 5 \end{pmatrix} \\
s_1 &\mapsto \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 6 & 5 & 1 & 3 & 2 \end{pmatrix}
\end{aligned}
$$

$$s_2 \mapsto \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 6 & 2 & 1 & 3 \end{pmatrix}$$
$$s_3 \mapsto \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}$$

Hieran erkennt man zweierlei:

1) Der Isomorphismus nach $Sym(n)$ ist nicht eindeutig. Man hätte die Gruppenelemente auch anders durchnummieren können, d. h. es gibt u. U. mehrere zu einer Gruppe G mit $|G| = n$ isomorphe Untergruppen in $Sym(n)$.
2) Wenn $|G| = n$ ist, dann gibt es u. U. auch in kleineren Permutationsgruppen $Sym(k)$ mit $k < n$ isomorphe Untergruppen zu G. Das wurde oben anhand der Gruppe K der Deckabbildungen des gleichseitigen Dreiecks ersichtlich: Es ist $|K| = 6$, aber K ist isomorph zu $Sym(3)$.

Bemerkung 5 Der Satz von Caley sagt aus: Wenn man endliche Gruppen untersuchen möchte, braucht man sich nur mit Permutationsgruppen zu beschäftigen, da alle endlichen Gruppen isomorph zu einer (in der Regel mehreren) Permutationsgruppe(n) sind.

1.2.5 Normalteiler

Definition 16 Es sei $N \leq G$ eine Untergruppe der Gruppe $(G, \circ)$. Dann ist N ein *Normalteiler* von G (in Zeichen $N \trianglelefteq G$), wenn $gN = Ng$ für alle $g \in G$ gilt, d. h. wenn alle Links- und Rechtsnebenklassen von N identisch sind.

Beispiel 13 In Beispiel 10 kann man für die Untergruppe der Deckdrehungen $D = \{d_0, d_{120}, d_{240}\}$ erkennen, dass $s_1 D = \{s_1, s_2, s_3\} = Ds_1$ gilt. Links- und Rechtsnebenklasse bezüglich s_1 sind also identisch. Dasselbe gilt auch für die anderen Spiegelungen, d. h. es ist $s_i D = \{s_1, s_2, s_3\} = Ds_i$ für alle $1 \leq i \leq 3$. Für Elemente d_i aus D ergibt sich als Nebenklasse $d_i D = Dd_i = D$. Also sind Links- und Rechtsnebenklassen zu D stets identisch, d. h. D ist ein Normalteiler der Gruppe der Deckabbildungen des gleichseitigen Dreiecks. Die drei Untergruppen der Spiegelungen sind keine Normalteiler, da – wie man ebenfalls in Beispiel 10 sieht – bei Ihnen Links- und Rechtsnebenklassen nicht identisch sind.

1.3 Ringe

1.3.1 Grundbegriffe über Ringe

Definition 17 (Ring) Es sei R eine nichtleere Menge und $+ : (R \times R) \to R$ und $\cdot : (R \times R) \to R$ Verknüpfungen von R. Das Tripel $(R, +, \cdot)$ heißt Ring, wenn gilt:

1) Das Paar $(R, +)$ ist eine kommutative Gruppe, d. h. es gilt: