

1 Gruppen: Definition und erste Eigenschaften

Von allen algebraischen Strukturen, die man in der linearen Algebra kennenlernen, haben Gruppen die einfachste Definition. In der Tat sind viele andere algebraische Objekte von der Form "Gruppenstruktur + zusätzliche Struktur". Das bedeutet, daß Eigenschaften die für Gruppen zutreffen, dann auch für diese anderen Strukturen gelten, soweit sie eben gruppentheoretische Aussagen sind. Weiter lassen sich viele Aussagen, die man für Gruppen beweisen kann, in analoger Form auf andere Strukturen wie Vektorräume übertragen. Es gibt noch einen dritten Grund sich mit Gruppen zu beschäftigen: sie dienen dazu Symmetrieeigenschaften mathematischer Objekte zu untersuchen. Wir kommen später darauf zu sprechen.

Definition. Es sei G eine nichtleere Menge und $*$: $G \times G \rightarrow G$, $(a, b) \mapsto a * b$ eine binäre Verknüpfung. Das Paar $(G, *)$ oder kurz G heißt *Gruppe*, falls folgende Axiome erfüllt sind:

(G1) Für alle $a, b, c \in G$ gilt

$$a * (b * c) = (a * b) * c \text{ (Assoziativgesetz).}$$

(G2) Es gibt ein $e \in G$ mit

$$e * a = a \text{ für alle } a \in G \text{ (Linksneutrales Element).}$$

(G3) Für jedes $a \in G$ gibt es ein $b \in G$ mit

$$b * a = e \text{ (Linksinverses Element).}$$

Gilt zusätzlich noch

(G4) $a * b = b * a$ für alle $a, b \in G$, so heißt die Gruppe *abelsch* oder *kommutativ*.

1.1 Beispiele. (1) Die Menge $(\mathbf{Z}, +)$ der ganzen Zahlen mit der gewöhnlichen Addition als binärer Verknüpfung ist eine Gruppe: Bekanntlich gilt das Assoziativgesetz $a + (b + c) = (a + b) + c$. Linksneutral ist die 0, da $0 + a = a$ und zu a linksinvers ist $-a$, da $(-a) + a = 0$. Wegen $a + b = b + a$ ist \mathbf{Z} sogar abelsch.

(2) Es sei \mathbf{R}_+ die Menge der positiven reellen Zahlen. Mit der Multiplikation wird (\mathbf{R}_+, \cdot) zu einer kommutativen Gruppe: Denn für $a, b, c \in \mathbf{R}_+$, ist $ab \in \mathbf{R}_+$ und es gilt $a(bc) = (ab)c$. Schließlich ist 1 linksneutral und linksinvers zu a ist $a^{-1} = \frac{1}{a}$. Auch ist klar, daß \mathbf{R}_+ abelsch ist.

(3) Es sei X eine nichtleere Menge. Eine bijektive Abbildung $\pi : X \rightarrow X$ heißt auch *Permutation*. Die Komposition $\pi \circ \varphi$ von bijektiven Abbildungen π und ρ ist wieder bijektiv. Ist $\text{Sym}(X)$ die Menge der Permutationen auf X , so definiert die Komposition \circ eine binäre Verknüpfung auf $\text{Sym}(X)$. Das Paar $(\text{Sym}(X), \circ)$ ist eine Gruppe, genannt die *symmetrische Gruppe* auf X :

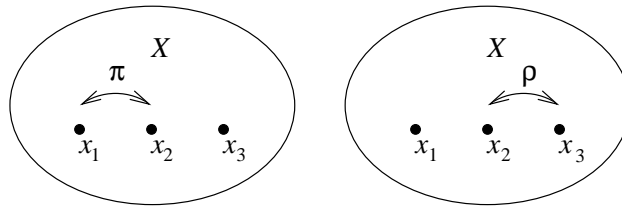
Axiom (G1) ist erfüllt, da das Assoziativgesetz für die Komposition von Abbildungen gilt. Auf X definiere die *Identität* oder *Einsabbildung* $\mathbf{1} = \mathbf{1}_X$ durch $\mathbf{1}(x) = x$ für $x \in X$. Sei $\pi \in \text{Sym}(X)$, $x \in X$, so gilt

$$\mathbf{1} \circ \pi(x) = \mathbf{1}(\pi(x)) = \pi(x), \text{ d.h. } \mathbf{1} \circ \pi = \pi$$

und $\mathbf{1}$ ist linksneutral, es gilt (G2). Sei $\pi \in \text{Sym}(X)$. Da π bijektiv ist, existiert die Umkehrabbildung $\pi^{-1} : X \rightarrow X$ mit $\pi^{-1} \circ \pi(x) = \pi^{-1}(\pi(x)) = x = \mathbf{1}(x)$ für $x \in X$. Also $\pi^{-1} \circ \pi = \mathbf{1}$ und (G3) folgt. Hat X mehr als zwei Elemente, so ist $\text{Sym}(X)$ jedoch nicht abelsch:

Seien $x_1, x_2, x_3 \in X$ drei verschiedene Elemente. Wir definieren Abbildungen $\pi : X \rightarrow X$, $\rho : X \rightarrow X$ durch

$$\pi(x) = \begin{cases} x_2, & x = x_1, \\ x_1, & x = x_2, \\ x, & \text{sonst,} \end{cases} \quad \rho(x) = \begin{cases} x_2, & x = x_3, \\ x_3, & x = x_2, \\ x, & \text{sonst.} \end{cases}$$



Da $\mathbf{1} = \pi \circ \pi = \rho \circ \rho$ liegen π und ρ in $\text{Sym}(X)$. Ferner

$$\pi \circ \rho(x_1) = \pi(x_1) = x_2, \quad \rho \circ \pi(x_1) = \rho(x_2) = x_3.$$

Also $\pi \circ \rho \neq \rho \circ \pi$.

1.2 Satz. Sei $(G, *)$ eine Gruppe.

- (a) Sei $a \in G$. Ist $b \in G$ mit $b * a = e$, so gilt auch $a * b = e$.
- (b) Das linksneutrale Element e von G eindeutig bestimmt und es gilt $e * a = a * e = a$ für alle $a \in G$.
- (c) Das linksinverse Element a^{-1} von a ist eindeutig bestimmt und es gilt $a^{-1} * a = a * a^{-1} = e$ für alle $a \in G$.

Beweis. Sei $a \in G$ und $b, c \in G$ mit $b * a = c * b = e$. Dann folgt

$$\begin{aligned} a * b &= e * (a * b) = (e * a) * b = ((c * b) * a) * b \\ &= (c * (b * a)) * b = (c * e) * b = c * b = e, \end{aligned}$$

es folgt (a).

Aus (a) folgt weiter

$$a = e * a = (a * b) * a = a * (b * a) = a * e.$$

Ist somit ebenfalls e' linksneutral, so folgern wir $e = e' * e = e * e' = e'$.

Daraus folgt (b).

Ist b' ebenfalls linksinvers zu a , so folgt mit (a):

$$b' = b' * e = b' * (a * b) = (b' * a) * b = e * b = b$$

und damit die Eindeutigkeit der Linksinversen $a^{-1} = b$. Mit (a) folgen dann alle Behauptungen von (c).

Im Folgenden schreiben wir die binäre Verknüpfung meist multiplikativ, d.h. wir schreiben ab statt $a * b$ und sprechen von der *Multiplikation* oder *Gruppenmultiplikation*, das neutrale Element wird mit 1 bezeichnet (*Eins* oder *Gruppeneins*). In abelschen Gruppen wird oft die additive Schreibweise $a + b$ für die Verknüpfung verwendet und das neutrale Element mit 0 bezeichnet. Eine nichtleere Teilmenge U der Gruppe G heißt *Untergruppe*, falls aus $a, b \in U$ stets $ab^{-1} \in U$ folgt. Dann ist U eine Gruppe und es gilt:

- (1) Sind $a, b \in U \Rightarrow ab \in U$ (U ist abgeschlossen unter der Multiplikation).

(2) Ist $a \in U \Rightarrow a^{-1} \in U$ (U ist unter Inversion abgeschlossen).

Ist nämlich $a \in U$, so $aa^{-1} = 1 \in U$ und auch $1a^{-1} = a^{-1} \in U$. Schließlich ist mit $b \in U$ auch $b^{-1} \in U$ und dann $a(b^{-1})^{-1} = ab \in U$. Hiermit folgen (1) und (2). Wegen $1 \in U$ impliziert das auch, daß U eine Gruppe ist.

Schließlich: Ist U eine nichtleere Teilmenge von G für die (1) und (2) gilt, so ist U eine Untergruppe: Sind $a, b \in U$, so folgt mit (2) dann $b^{-1} \in U$ und mit (1) schließlich $ab^{-1} \in U$.

1.3 Beispiele. (1) Jede Gruppe G hat die *trivialen* Untergruppen G und $\{1\}$.

(2) In $(\mathbf{Z}, +)$ ist die Menge $n\mathbf{Z} = \{na \mid a \in \mathbf{Z}\}$, $n \in \mathbf{Z}$ eine Untergruppe: Sei $na, nb \in n\mathbf{Z}$, so $na + (-nb) = n(a - b) \in \mathbf{Z}$.

(3) In (\mathbf{R}_+, \cdot) ist offensichtlich (\mathbf{Q}_+, \cdot) eine Untergruppe, wo \mathbf{Q}_+ die Teilmenge der rationalen Zahlen in \mathbf{R}_+ ist.

1.4 Rechtsnebenklassen. Es sei U eine Untergruppe der Gruppe G . Auf G definieren wir die Relation $\rho_U = \rho$ durch $a\rho b \Leftrightarrow ab^{-1} \in U$. Wir behaupten, daß ρ_U eine Äquivalenzrelation ist.

Zunächst beachte $aa^{-1} = 1 \in U$ für $a \in G$. Also ist $a\rho a$ (Reflexivität). Ist $a\rho b$, so $ab^{-1} \in U$ und da U eine Untergruppe ist, folgt $ba^{-1} = (ab^{-1})^{-1} \in U$, sodaß $b\rho a$ (Symmetrie) gilt. Schließlich sei $a\rho b$, $b\rho c$, d.h. $ab^{-1}, bc^{-1} \in U$ und somit $ac^{-1} = (ab^{-1})(bc^{-1}) \in U$, sodaß $a\rho c$ (Transitivität) gilt.

Für $a \in G$ ist $Ua = \{ua \mid u \in U\}$ die Äquivalenzklasse bzgl. ρ_U , die a enthält: Sei mit $[a]$ die Klasse bezeichnet, die a enthält. Ist $b \in [a]$, so $a\rho b \Rightarrow b\rho a \Rightarrow ba^{-1} = u \in U \Rightarrow b = ua \in Ua$. Also $[a] \subseteq Ua$. Umgekehrt $b = ua \in Ua$ bedeutet $ba^{-1} \in U$ und damit $b\rho a \Rightarrow a\rho b$, d.h. $Ua \subseteq [a]$.

Die Äquivalenzklassen Ua heißen *Rechtsnebenklassen von G modulo U* .

Definiert man die Relation λ_U durch $a\lambda_U b \Leftrightarrow a^{-1}b \in U$, so ist auch λ_U eine Äquivalenzrelation und Äquivalenzklassen sind in diesem Fall die *Linksnebenklassen* $aU = \{au \mid u \in U\}$.

1.5 Satz. *Es sei G eine Gruppe, U eine Untergruppe und X, Y seien Rechtsnebenklassen modulo U . Dann gibt es eine Bijektion $f : X \rightarrow Y$.*

Beweis. Ist $a \in X$, $b \in Y$, so ist $X = Ua$, $Y = Ub$. Definiere

$$\begin{aligned} f : X &\rightarrow Y, \quad ua \mapsto (ua)(a^{-1}b) = ub \quad \text{und} \\ g : Y &\rightarrow X, \quad ub \mapsto (ub)(b^{-1}a) = ua. \end{aligned}$$

Dann gilt $f \circ g(ub) = f(g(ub)) = f(ua) = ub$ und $g \circ f(ua) = ua$ analog. Also ist $f \circ g = \mathbf{1}_Y$ die Identität auf Y und $g \circ f = \mathbf{1}_X$ die Identität auf X . Damit ist $g = f^{-1}$ die Umkehrabbildung zu f . Insbesondere ist f bijektiv.

Im Folgenden schreiben wir $|X| = n$ für eine Menge X , wenn n Elemente in X liegen. Hat X unendlich viele Elemente, so schreiben wir $|X| = \infty$.

Definition. Ist G eine Gruppe, so heißt $|G|$ die *Ordnung* von G . Ist U eine Untergruppe und R die Menge der Rechtsnebenklassen, so heißt

$$|G : U| = |R|$$

der *Index* von U in G .

1.6 Satz. *Es sei U eine Untergruppe der endlichen Gruppe G . Dann gilt*

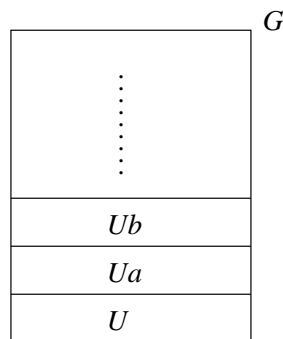
$$|G| = |U| \cdot |G : U|.$$

Beweis. Da G endlich ist, hat G auch nur endlich viele Rechtsnebenklassen, etwa X_1, \dots, X_n . Dann ist $n = |G : U|$. Ferner ist

$$G = X_1 \cup \dots \cup X_n$$

eine Partition. Es gilt

$$|G| = |X_1| + \dots + |X_n|.$$



Die Rechtsnebenklasse zu 1 sei X_1 , diese ist $X_1 = U1 = U$. Nach Satz (1.5) ist $|U| = |X_1| = |X_i|$ für alle i . Also

$$|G| = n|U| = |G : U| \cdot |U|.$$

Bemerkung. Satz (1.6) wird *Satz von Lagrange* genannt. Er besagt, daß die Ordnung jeder Untergruppe die Gruppenordnung teilt. Die Umkehrung ist jedoch im allgemeinen falsch: Es gibt endliche Gruppen G und für diese Teiler d der Gruppenordnung $|G|$, sodaß die Gruppe keine Untergruppe der Ordnung d hat.

Definition. Es sei G eine Gruppe.

(a) X, Y seien beliebige Teilmengen von G . Dann ist die Menge

$$XY = \{xy \mid x \in X, y \in Y\}$$

das *Komplexprodukt* von X und Y . Eine Rechtsnebenklasse Ua ist also das Komplexprodukt $U\{a\}$.

(b) Es sei N eine Untergruppe von G . Dann heißt N *Normalteiler* von G , falls $a^{-1}Na = N$ für alle $a \in G$ gilt. Äquivalent dazu ist die Bedingung $Na = aN$ für alle a , d.h. jede Rechtsnebenklasse ist eine Linksnebenklasse und umgekehrt.

Ist eine Gruppe G abelsch, so ist natürlich jede Untergruppe ein Normalteiler, in beliebigen Gruppen ist das im allgemeinen nicht der Fall. Ist N ein Normalteiler von G , so bezeichnen wir mit G/N die Menge der Rechtsnebenklassen.

1.7 Satz. *Sei G eine Gruppe und N ein Normalteiler. Sind $X, Y \in G/N$, so ist $XY \in G/N$. Mit dieser Multiplikation ist G/N eine Gruppe.*

Beweis. Es sei $X = Na, Y = Nb$. Wir zeigen

$$XY = NaNb = Nab = Z.$$

Ist $nab \in Nab, n \in N$, so

$$nab = (na)(1b) \in XY, \text{ was } Z \subseteq XY \text{ zeigt.}$$

Umgekehrt: Ein typisches Element aus XY hat die Gestalt n_1an_2b mit $n_1, n_2 \in N$. Wegen $Na = aN$ existiert ein $n'_2 \in N$ mit $an_2 = n'_2a$. Damit

$$n_1an_2b = n_1n'_2ab \in Nab = Z \text{ und } XY \subseteq Z$$

folgt.

Zur Verifikation der Axiome (G1)-(G3):

Für $X = Na, Y = Nb, Z = Nc$ gilt:

$$\begin{aligned} (XY)Z &= (NaNb)Nc \\ &= NabNc \\ &= N(ab)c \\ &= Na(bc) \\ &= NaNbc \\ &= Na(NbNc) \\ &= X(YZ). \end{aligned}$$

Es folgt (G1). Neutrales Element in G/N ist $N = N1$ wegen $(N1)(Na) = N(1a) = Na$ und zu Na invers ist Na^{-1} wegen $(Na^{-1})(Na) = N(a^{-1}a) = N$.

Definition. Ist N ein Normalteiler der Gruppe G , so heißt die Gruppe G/N *Faktorgruppe* oder *Quotient von G modulo N* . Quotientenbildungen sind ein wichtiges Hilfsmittel um Gruppen zu untersuchen. Auch für viele andere mathematische Strukturen sind analoge Konstruktionen von Quotientenstrukturen von fundamentaler Bedeutung.

1.8 Beispiel. Es sei wieder $G = (\mathbf{Z}, +)$, die zuvor betrachtete Gruppe der ganzen Zahlen. Es sei U eine Untergruppe, so ist U auch Normalteiler, da G abelsch ist. (Rechts) Nebenklassen haben die Form $U + a = a + U$. Wir haben bereits gesehen, dass für $n \in \mathbf{Z}$ die Menge

$$U = n\mathbf{Z} = \{nz \mid z \in \mathbf{Z}\}$$

eine Untergruppe ist.

In Satz (2.1) werden wir sogar zeigen, daß jede Untergruppe von $G = \mathbf{Z}$ diese Gestalt hat. Sei von nun an $U = n\mathbf{Z}$. Nach Definition der Relation ρ_U ist

$$a\rho_U b \Leftrightarrow a - b \in n\mathbf{Z}.$$

D.h. $a - b = nz$ und n ist Teiler der Differenz $a - b$. Umgekehrt folgt aus "n teilt $a - b$ " auch $a \rho_U b$. Damit ist $a \rho_U b$ äquivalent zu n teilt $a - b$. Statt $a \rho_U b$ schreibt man $a \equiv b \pmod{n}$ und sagt a ist *kongruent zu b modulo n* . Ist zum Beispiel $n = 5$, so ist

$$2 + 5\mathbf{Z} = \{\dots, -8, -3, 2, 7, \dots\} = \{x \in \mathbf{Z} \mid x \equiv 2 \pmod{5}\}.$$

Wir untersuchen nun die Faktorgruppe $G/U = \mathbf{Z}/n\mathbf{Z}$. Ist $n = 0$, so ist $n\mathbf{Z} = \{0\}$ die triviale Untergruppe und $a - b \in \{0\}$ bedeutet $a = b$. Also ist

$$\mathbf{Z}/0\mathbf{Z} = \{\{a\} \mid a \in \mathbf{Z}\}$$

Das ist nicht die Gruppe \mathbf{Z} aber eine "isomorphe" Gruppe, d.h. eine in mathematischem Sinne zu \mathbf{Z} völlig gleichwertige Gruppe. Wir werden bald mehr zum Isomorphiebegriff sagen. Sei von nun an $n \neq 0$. Ist $a \in \mathbf{Z}$, so zeigt die Division mit Rest, daß

$$a = qn + r \text{ ist mit } q \in \mathbf{Z}, 0 \leq r < n.$$

Damit ist

$$a + n\mathbf{Z} = r + nq + n\mathbf{Z} = r + n\mathbf{Z}.$$

Ist $0 \leq r, s < n$ und $r + n\mathbf{Z} = s + n\mathbf{Z}$, so $r \equiv s \pmod{n}$. Also teilt n die Zahl $r - s$ und wegen $|r - s| < n$ folgt $r = s$. Wir schließen:

$$\mathbf{Z}/n\mathbf{Z} = \{r + n\mathbf{Z} \mid 0 \leq r < n\} = \{\mathbf{Z} = 0 + \mathbf{Z}, 1 + \mathbf{Z}, \dots, (n - 1) + \mathbf{Z}\},$$

und erhalten als Gruppenordnung

$$|\mathbf{Z}/n\mathbf{Z}| = n.$$

Zwei exemplarische Rechnungen in $\mathbf{Z}/n\mathbf{Z}$, $n = 11$:

$$\begin{aligned} (5 + 11\mathbf{Z}) + (9 + 11\mathbf{Z}) &= 14 + 11\mathbf{Z} = 3 + 11\mathbf{Z}, \\ (7 + 11\mathbf{Z}) + (-10 + 11\mathbf{Z}) &= -3 + 11\mathbf{Z} = 8 + 11\mathbf{Z}. \end{aligned}$$

Kürzer drückt man das durch Kongruenzen aus:

$$5 + 9 = 14 \equiv 3 \pmod{11}, \quad 7 - 10 \equiv 8 \pmod{11}.$$

Zum Schluß weisen wir auf die interessante Tatsache hin, daß die Struktur der Untergruppen und der Faktorgruppen von \mathbf{Z} ganz verschieden ist: Alle

Untergruppen $n\mathbf{Z}$ von \mathbf{Z} , mit Ausnahme von $0\mathbf{Z}$, sind unendlich, alle Faktorgruppen $\mathbf{Z}/n\mathbf{Z}$, mit Ausnahme von $\mathbf{Z}/0\mathbf{Z}$, sind endlich.

Definition. Es seien G, H Gruppen. Eine Abbildung $\varphi : G \rightarrow H$ heißt *Gruppenhomomorphismus* oder kurz *Homomorphismus* von G nach H , wenn gilt

$$\varphi(ab) = \varphi(a)\varphi(b) \text{ für alle } a, b \in G.$$

Beachte, daß die Verknüpfung auf der linken Seite die Gruppenmultiplikation in G ist, die auf der rechten Seite die Gruppenmultiplikation in H ist. Homomorphismen stellen also eine Verbindung zwischen den Gruppenmultiplikationen von Gruppen her. Man nennt φ einen *Monomorphismus*, *Epimorphismus*, *Isomorphismus* je nachdem ob φ injektiv, surjektiv oder bijektiv ist.

Wenn φ ein Isomorphismus ist, so ist auch die Umkehrabbildung φ^{-1} ein Isomorphismus (siehe 1.10)). Es gibt also eine eindeutige Korrespondenz zwischen den Elementen von G und H und wegen $\varphi(ab) = \varphi(a)\varphi(b)$ wird die Gruppenmultiplikation respektiert. Anschaulich gesprochen: In beiden Gruppen gelten die gleichen "Rechenregeln". Von einem abstrakten Standpunkt aus werden die Gruppen G und H nicht unterschieden und symbolisch drückt man diesen Sachverhalt durch $G \simeq H$ aus. Aus mathematischer Sicht interessiert normalerweise weniger eine Gruppe in einer speziellen Darstellung, sondern man ist an den Eigenschaften des *Isomorphietyps* dieser Gruppe interessiert, also den Eigenschaften, die alle Gruppen haben, die zur betrachteten Gruppe isomorph sind.

1.9 Beispiele. (1) Es sei G eine Gruppe. Die Identität $\mathbf{1} = \mathbf{1}_G : G \rightarrow G, a \mapsto a$ ist offenbar ein Isomorphismus. Die Abbildung $\varphi : G \rightarrow \{1\}, a \mapsto 1$ für alle $a \in G$ ist ein Epimorphismus aber kein Monomorphismus, wenn $|G| > 1$ ist.

(2) Es sei $G = (\mathbf{Z}, +)$ die additive Gruppe der ganzen Zahlen, $H = (\mathbf{Z}/0\mathbf{Z}, +)$ die Faktorgruppe modulo dem trivialen Normalteiler $0\mathbf{Z} = \{0\}$. Durch $\varphi : G \rightarrow H$ mit $\varphi(a) = \{a\}$ ist ein Homomorphismus erklärt, denn

$$\varphi(a + b) = \{a + b\} = \{a\} + \{b\} = \varphi(a) + \varphi(b).$$

Offensichtlich ist φ bijektiv. Also ist G zu H isomorph und vom gruppentheoretischen Standpunkt aus beschreiben $(\mathbf{Z}, +)$ und $(\mathbf{Z}/0\mathbf{Z}, +)$ das gleiche Objekt.

Die hier gemachte Beobachtung gilt auch allgemein: Ist $N = \{1\}$ der triviale Normalteiler der Gruppe G , so ist $G \simeq G/N$.

(3) Sei wieder $G = (\mathbf{Z}, +)$ und H eine beliebige Gruppe. Für ein festes $a \in H$ definiere $\varphi : G \rightarrow H$ durch $\varphi(n) = a^n$. Wegen

$$\varphi(m+n) = a^{m+n} = a^m a^n = \varphi(m)\varphi(n)$$

ist φ ein Gruppenhomomorphismus.

(4) Es sei $G = (\mathbf{R}, +)$ die additive Gruppe der reellen Zahlen und $H = (\mathbf{R}_+, \cdot)$ die multiplikative Gruppe der positiven reellen Zahlen. Die neutralen Elemente sind 0 bzw. 1. Definiere $\varphi : G \rightarrow H$ durch $\varphi(x) = e^x$ (Exponentialfunktion). Nach den Rechenregeln der Exponentialfunktion gilt:

$$\varphi(x+y) = e^{x+y} = e^x e^y = \varphi(x)\varphi(y).$$

Also ist φ ein Homomorphismus. Man weiß, daß φ eine Umkehrabbildung $\varphi^{-1} = \log$, den Logarithmus, besitzt. In dem diesem Beispiel folgenden Satz (1.11) wird gezeigt, dass die Umkehrabbildung eines Isomorphismus selbst ein Isomorphismus ist. Das bestätigt die folgende, wohlbekannte Rechenregel des Logarithmus:

$$\varphi^{-1}(xy) = \log(xy) = \log(x) + \log(y) = \varphi^{-1}(x) + \varphi^{-1}(y).$$

Somit gilt $(\mathbf{R}, +) \simeq (\mathbf{R}_+, \cdot)$, die additive Gruppe der reellen Zahlen ist isomorph zur multiplikativen Gruppe der positiven reellen Zahlen.

Weitere Bezeichnungen. Es sei G eine Gruppe. Ein Homomorphismus $\varphi : G \rightarrow G$ heißt *Endomorphismus*. Ist φ bijektiv, so ist φ ein *Automorphismus*. Seien G, H Gruppen, $\varphi : G \rightarrow H$ ein Homomorphismus. Wir definieren *Kern* und *Bild* von φ als

$$\text{Ker}(\varphi) = \{a \in G \mid \varphi(a) = 1\}, \quad \text{Im}(\varphi) = \{\varphi(a) \mid a \in G\}.$$

Anders ausgedrückt: $\text{Ker}(\varphi) = (\varphi)^{-1}(1)$, $\text{Im}(\varphi) = \varphi(G)$.

1.10 Satz. *Es sei $\varphi : G \rightarrow H$ ein Gruppenhomomorphismus. Dann gilt:*

- (a) $\varphi(1) = 1$ und $\varphi(a)^{-1} = \varphi(a^{-1})$ für $a \in G$.
- (b) $\text{Ker}(\varphi)$ ist eine Untergruppe von G und $\text{Im}(\varphi)$ ist eine Untergruppe von H .
- (c) φ ist genau dann ein Monomorphismus, wenn $\text{Ker}(\varphi) = \{1\}$ gilt.
- (d) Ist φ ein Isomorphismus, so ist die Umkehrabbildung $\varphi^{-1} : H \rightarrow G$ ein Isomorphismus.

Beweis. (a) $\varphi(1) = \varphi(1^2) = \varphi(1)\varphi(1)$. Multipliziert man mit $\varphi(1)^{-1}$, so folgt $1 = \varphi(1)$. Weiter ist für $a \in G$:

$$1 = \varphi(1) = \varphi(a^{-1}a) = \varphi(a^{-1})\varphi(a),$$

was $\varphi(a^{-1}) = \varphi(a)^{-1}$ zeigt.

(b) Seien $a, b \in \text{Ker}(\varphi)$. Zeige $ab^{-1} \in \text{Ker}(\varphi)$:

Aus (a) folgt $\varphi(ab^{-1}) = \varphi(a)\varphi(b)^{-1} = 1 \cdot 1^{-1} = 1$, was $ab^{-1} \in \text{Ker}(\varphi)$ impliziert.

Seien $x, y \in \text{Im}(\varphi)$. Zeige $xy^{-1} \in \text{Im}(\varphi)$:

Es existieren $a, b \in G$ mit $\varphi(a) = x$, $\varphi(b) = y$. Mit (a) folgt $\varphi(b^{-1}) = y^{-1}$ und daher

$$xy^{-1} = \varphi(a)\varphi(b^{-1}) = \varphi(ab^{-1}) \in \text{Im}(\varphi).$$

(c) Angenommen $\text{Ker}(\varphi) = \{1\}$. Sei $\varphi(a) = \varphi(b)$. Dann $1 = \varphi(a)\varphi(b)^{-1} = \varphi(a)\varphi(b^{-1}) = \varphi(ab^{-1})$. Also $ab^{-1} \in \text{Ker}(\varphi) = \{1\}$ und damit $1 = ab^{-1}$ bzw. $a = b$. Daher ist φ injektiv.

Nun nehme an, daß φ injektiv ist. Dann hat das Einselement in H als Urbild unter φ nur das Einselement von G . Also $\text{Ker}(\varphi) = \{1\}$.

(d) Seien $x, y \in H$. Zeige $\varphi^{-1}(xy) = \varphi^{-1}(x)\varphi^{-1}(y)$:

Es existieren $a, b \in G$ mit $\varphi(a) = x$, $\varphi(b) = y$. Also $\varphi(ab) = \varphi(a)\varphi(b) = xy$ und $\varphi^{-1}(x) = a$, $\varphi^{-1}(y) = b$ sowie $\varphi^{-1}(xy) = ab$. Es folgt

$$\varphi^{-1}(xy) = ab = \varphi^{-1}(x)\varphi^{-1}(y).$$

1.11 Beispiel. Es sei G eine Gruppe, $g \in G$ sei fest gewählt. Definiere $\alpha(g) : G \rightarrow G$ durch $\alpha(g)(a) = gag^{-1}$. Diese Abbildung nennt man *Konjugation mit g* . Zunächst gilt für $a, b \in G$:

$$\begin{aligned}
\alpha(g)(ab) &= g(ab)g^{-1} \\
&= (ga) \cdot 1 \cdot (bg^{-1}) \\
&= (ga)(g^{-1}g)(bg^{-1}) \\
&= (gag^{-1})(gbg^{-1}) \\
&= \alpha(g)(a) \cdot \alpha(g)(b).
\end{aligned}$$

Damit ist $\alpha(g)$ Homomorphismus, also Endomorphismus. Wegen

$$\alpha(g^{-1}) \circ \alpha(g)(a) = \alpha(g^{-1})(\alpha(g)(a)) = g^{-1}(gag)g^{-1} = a$$

ist $\alpha(g^{-1}) = \alpha(g)^{-1}$ die Umkehrabbildung von $\alpha(g)$ und somit ist $\alpha(g)$ ein Automorphismus.

Ist die Gruppe G abelsch, so ist natürlich jeder der Automorphismen $\alpha(g)$ die Identität 1_G . In nicht abelschen Gruppen gibt es jedoch Automorphismen der Gestalt $\alpha(g)$, die nicht die Identität sind.

Bemerkung. Sind $\varphi : G \rightarrow H$, $\psi : H \rightarrow K$ Homomorphismen, so ist wegen

$$\begin{aligned}
\psi \circ \varphi(ab) &= \psi(\varphi(ab)) \\
&= \psi(\varphi(a)\varphi(b)) \\
&= \psi(\varphi(a))\psi(\varphi(b)) \\
&= \psi \circ \varphi(a) \cdot \psi \circ \varphi(b)
\end{aligned}$$

auch die Komposition $\psi \circ \varphi : G \rightarrow K$ ein Homomorphismus.

Auf der Menge $\text{End}(G)$ der Endomorphismen von G ist somit die Komposition von Homomorphismen eine binäre Verknüpfung. Bezeichnet man mit $\text{Aut}(G)$ die Menge der Automorphismen von G , so ist $\text{Aut}(G)$ mit der Komposition sogar eine Gruppe, die *Automorphismengruppe von G* . Beachte, daß die Existenz der Inversen aus Satz (1.11.c) folgt und die Identität natürlich das neutrale Element von $\text{Aut}(G)$ ist.

1.12 Satz. *Es sei $\varphi : G \rightarrow H$ ein Gruppenhomomorphismus. Dann ist $\text{Ker}(\varphi)$ ein Normalteiler von G .*

Beweis. Setze $N = \text{Ker}(\varphi)$. Wir zeigen $a^{-1}Na \subseteq N$ für $a \in G$: Ein typisches Element aus $a^{-1}Na$ hat die Form $x = a^{-1}na$ mit $n \in N$. Dann

$$\varphi(x) = \varphi(a^{-1})\varphi(n)\varphi(a) = \varphi(a)^{-1} \cdot 1 \cdot \varphi(a) = 1$$

und $x \in \text{Ker}(\varphi) = N$. Es folgt die Behauptung.

Dann gilt auch $a^{-1}Na = N$ für alle $a \in G$: Es ist nämlich auch $aNa^{-1} \subseteq N$ und damit $N = a^{-1}(aNa^{-1})a \subseteq a^{-1}Na$.

1.13 Satz. *Es sei $\varphi : G \rightarrow H$ ein Gruppenhomomorphismus. Dann gilt*

$$G/\text{Ker}(\varphi) \simeq \text{Im}(\varphi).$$

Beweis. Nach Satz (1.12) ist $N = \text{Ker}(\varphi)$ ein Normalteiler von G . Daher kann man die Faktorgruppe G/N bilden.

(1) Ist X eine Rechtsnebenklasse und $x, y \in X$, so gilt $\varphi(x) = \varphi(y)$:

Sei $X = Na$, $a \in G$ geeignet. Dann ist $x = n_1a$, $y = n_2a$ mit $n_1, n_2 \in N = \text{Ker}(\varphi)$. Also

$$\varphi(x) = \varphi(n_1a) = \varphi(n_1)\varphi(a) = 1 \cdot \varphi(a) = \varphi(a)$$

und genauso ist $\varphi(y) = \varphi(a) = \varphi(x)$.

(2) Definiere $f : G/N \rightarrow H$ durch

$$f(X) = \varphi(a) \text{ für } X = Na.$$

Nach (1) wird damit jeder Nebenklasse genau ein Element aus H zugeordnet, d.h. f ist eine Abbildung.

Wir bemerken an dieser Stelle, daß wir damit gezeigt haben, daß f wohldefiniert ist. Damit ist gemeint:

Will man auf einer Menge von Äquivalenzklassen eine Abbildung dadurch definieren, indem man das Bild der Äquivalenzklasse als das Bild eines Repräsentanten beschreibt, so ist immer nachzuprüfen, daß diese Definition des Bildes der Äquivalenzklasse unabhängig von der Wahl des Repräsentanten ist.

(3) f ist ein Homomorphismus:

$$f(NaNb) = f(Nab) = \varphi(ab) = \varphi(a)\varphi(b) = f(Na)f(Nb).$$

(4) f ist surjektiv:

Ist $x = \varphi(a) \in \text{Im}(\varphi)$, so $f(Na) = \varphi(a) = x$.

(5) f ist injektiv:

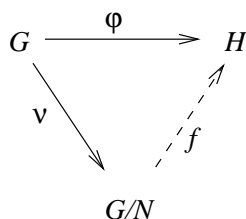
Angenommen $f(Na) = f(Nb)$. Dann $\varphi(a) = \varphi(b)$. Also $1 = \varphi(a)\varphi(b)^{-1} = \varphi(ab^{-1})$ und $ab^{-1} \in \text{Ker}(\varphi) = N$. Es folgt $a \in Nb$ und $Na = Nb$.

Bemerkungen. (a) Satz (1.13) ist von fundamentaler Bedeutung und wird *Homomorphiesatz* genannt. Unter anderem hat er folgende Konsequenz: Kennt man alle Normalteiler einer Gruppe G , so sind auch alle ihre epimorphen Bilder bekannt. In diesem Fall ist nämlich $\text{Im}(\varphi) = H$ und $G/\text{Ker}(\varphi) \simeq H$.

(b) Ist N ein Normalteiler der Gruppe G , so wird durch $\nu : G \rightarrow G/N, a \mapsto Na$ ein Epimorphismus definiert (die Homomorphieeigenschaft folgt aus der Art wie die Multiplikation auf G/N erklärt ist). Dieser Epimorphismus heißt der *natürliche* Epimorphismus von G auf G/N . Für die Abbildung f aus dem Beweis von Satz (1.13) gilt somit

$$f \circ \nu(a) = \varphi(a)$$

für $a \in G$. Diesen Sachverhalt beschreibt man auch durch ein kommutatives Diagramm.



Kommutative Diagramme sind Systeme von Pfeilen. Die Pfeile stehen für Abbildungen. Das Durchlaufen von Pfeilen bedeutet Komposition von Abbildungen und "kommutativ" heißt, daß jeder Weg längs Pfeilen, der zwei Punkte verbindet, stets die gleiche Abbildung darstellt.

(c) Es sei $\varphi : G \rightarrow H$ ein Gruppenepimorphismus. Der Homomorphiesatz stellt eine eindeutige Korrespondenz der Untergruppen $\text{Ker } \varphi \leq U \leq G$ zwischen $\text{Ker } \varphi$ und G mit den Untergruppen von H her:

Ist nämlich $V \leq H$, so ist das *Urbild* von V

$$U = \varphi^{-1}(V) = \{g \in G \mid \varphi(g) \in V\}$$

eine Untergruppe (die Routineverifikation sei dem Leser überlassen), die zwischen $\text{Ker } \varphi$ und G liegt. Da φ ein Epimorphismus ist, gilt auch $\varphi(U) = V$. Umgekehrt: Gilt $\text{Ker } \varphi \leq U \leq G$ und setzt man $V = \varphi(U)$, so $U \leq \varphi^{-1}(V)$. Es gilt sogar $U = \varphi^{-1}(V)$, denn ist $\varphi(u) = \varphi(x)$, $u \in U$, $x \in \varphi^{-1}(V)$, so $xu^{-1} \in \text{Ker } \varphi$, und daher $x \in (\text{Ker } \varphi)u \subseteq U$. Es folgt die Behauptung.

2 Struktursätze

Will man eine mathematische Theorie verstehen, so ist es immer wichtig einige typische Beispiele gut zu kennen. In diesem Abschnitt untersuchen wir zwei Beispiellklassen von Gruppen. Die erste Klasse besteht aus den zyklischen Gruppen. Diese Gruppen sind aus gruppentheoretischer Sicht völlig verstanden, insbesondere kennt man die Struktur der Untergruppen. Zyklische Gruppen sind gewissermaßen die unkompliziertesten Gruppen. Als zweite Serie von Gruppen betrachten wir die symmetrischen Gruppen auf endlichen Mengen. Hier kommen wir nicht zu einer vollständigen Beschreibung der Untergruppenstruktur, wir geben uns mit der Bestimmung der Ordnung zufrieden. In der Tat sind die symmetrischen Gruppen aus gruppentheoretischer Sicht so kompliziert wie nur möglich: Es gibt nämlich einen Satz, der besagt, daß jede endliche Gruppe G Untergruppe einer symmetrischen Gruppe auf $|G|$ Symbolen ist.

2.1 Satz. *Es sei U eine Untergruppe der additiven Gruppe \mathbf{Z} der ganzen Zahlen. Dann gibt es ein $0 \leq n \in \mathbf{Z}$ mit $U = n\mathbf{Z}$.*

Beweis. Ist $U = \{0\}$, so ist $U = 0\mathbf{Z}$. Sei also $U \neq \{0\}$. Mit $x \in U$ ist auch $-x \in U$. Insbesondere gibt es ein $0 < x \in U$. Sei n die kleinste positive Zahl, die in U liegt.

Behauptung: $U = n\mathbf{Z}$.

Sei $m \in U$ beliebig. Division mit Rest ergibt

$$m = qn + r$$

mit $q, r \in \mathbf{Z}$ und $0 \leq r < n$.

Nun ist für $q > 0$ die Zahl qn die q -fache Summe von n , dh. $qn \in U$. Ist $q < 0$, so ist $qn = -|q|n$ und liegt ebenfalls in U . Damit ist

$$r = m - qn \in U.$$

Nach der Wahl von n folgt $r = 0$. Also $m = qn \in n\mathbf{Z}$. Es folgt $U \subseteq n\mathbf{Z}$. Nach der obigen Überlegung ist andererseits auch $n\mathbf{Z} \subseteq U$. Es folgt die Behauptung.

Bemerkung. Nach Satz 2.1 liegt eine komplette Auflistung aller Untergruppen der Gruppe \mathbf{Z} vor. In der Praxis gelingt es nur sehr selten die vollständige Liste aller Untergruppen einer Gruppe herzustellen.

Definition. Eine Gruppe H heißt *zyklisch*, falls es einen Epimorphismus: $\varphi : \mathbf{Z} \rightarrow H$ gibt, also $H = \text{Im}(\varphi)$. Nach dem Isomorphiesatz (1.13) und (2.1) gilt

$$H = \text{Im}(\varphi) \simeq \mathbf{Z}/n\mathbf{Z},$$

wobei $\text{Ker}(\varphi) = n\mathbf{Z}$, $0 \leq n \in \mathbf{Z}$ ist. Entweder ist $n = 0$ und damit $H \simeq \mathbf{Z}/0\mathbf{Z} \simeq \mathbf{Z}$ und $|H| \simeq \infty$ oder $n > 0$ und $|H| = |\mathbf{Z}/n\mathbf{Z}| = n$.

2.2 Satz. *Es sei G eine zyklische Gruppe der Ordnung $n < \infty$. Dann existiert ein $g \in G$ mit*

$$G = \{g^m | m \in \mathbf{Z}\} = \{1 = g^0, g^1, \dots, g^{n-1}\}.$$

Jedes solche g heißt *erzeugendes Element* von G . Insbesondere ist G abelsch.

Beweis. Es sei $\varphi : \mathbf{Z} \rightarrow G$ ein Epimorphismus mit $\text{Ker}(\varphi) = n\mathbf{Z}$, $n \geq 0$. Setze $g = \varphi(1)$. Ist $m \geq 0$, so

$$\varphi(m) = \varphi(1 + \dots + 1) = \varphi(1) \cdots \varphi(1) = g^m,$$

wobei die Summe der Einsen bzw. das Produkt der $\varphi(1)$ sich jeweils über m Terme erstreckt. Ist $m < 0$, so

$$\varphi(m) = \varphi(-1) \cdots \varphi(-1) = (g^{-1})^{|m|} = g^m.$$

Das zeigt $G = \{g^m | m \in \mathbf{Z}\}$. Ist $g^m = 1$, so folgt $\varphi(m) = 1$ und $m \in \text{Ker}(\varphi) = n\mathbf{Z}$. Damit ist genau dann $g^m = 1$, wenn n ein Teiler von m ist. Sei h ein beliebiges Element aus G und $k \in \mathbf{Z}$ mit $h = \varphi(k) = g^k$. Division mit n liefert ganze Zahlen q, r mit $k = qn + r$, $0 \leq r < n$. Es folgt

$$h = g^k = g^{qn+r} = g^{qn} g^r = g^r.$$

Damit ergibt sich $G = \{g^r | 0 \leq r < n\}$. Da G die Ordnung n hat, sind alle Elemente in der Menge auf der rechten Seite paarweise verschieden. Die Gruppe G ist auch abelsch, da sie das Bild einer abelschen Gruppe ist. Es folgen alle Behauptungen.

Bemerkung. Satz (2.2) zeigt: 1) Eine zyklische Gruppe der Ordnung n ist zu $\mathbf{Z}/n\mathbf{Z}$ isomorph. 2) Zu jeder natürlichen Zahl $n > 0$ existiert eine zyklische Gruppe der Ordnung n , nämlich $\mathbf{Z}/n\mathbf{Z}$.

2.3 Beispiel. Es sei G eine zyklische Gruppe der Ordnung 11 und g ein erzeugendes Element. Dann ist $G = \{1 = g^0, g, \dots, g^{10}\}$. Multiplikation von g^a mit g^b erfolgt gemäß der Rechenregeln für den Umgang mit Potenzen. In unserem Fall sind Exponenten modulo 11 zu lesen. Also

$$g^5 g^9 = g^{14} = g^3 \text{ oder } g^{10} g = g^{11} = 1.$$

Insbesondere ist g^{11-a} , das Inverse von g^a .

2.4 Satz.

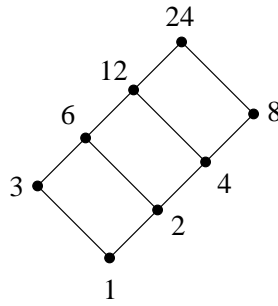
- (a) *Es sei $n \geq 1$ eine natürliche Zahl. Die Untergruppen H von \mathbf{Z} , die $n\mathbf{Z}$ enthalten, haben die Form $H = d\mathbf{Z}$ mit einem Teiler d von n .*
- (b) *Es sei G eine zyklische Gruppe der Ordnung n . Dann gibt es zu jedem Teiler d von n genau eine Untergruppe der Ordnung d von G . Diese Untergruppe ist zyklisch.*

Beweis. (a) Sei $d\mathbf{Z}$ eine Untergruppe von \mathbf{Z} , die $n\mathbf{Z}$ enthält. Dann existiert ein $k \in \mathbf{Z}$, mit $kd = n$. Es folgt die Behauptung.

(b) Es sei $\varphi : \mathbf{Z} \rightarrow G$ ein Epimorphismus und $g = \varphi(1)$ sei ein erzeugendes Element von G . Sei $n = kd$. Definiere einen Homomorphismus $\phi : G \rightarrow G$ durch $\phi(g^r) = (g^r)^k = g^{rk}$ und setze $H = \text{Im}(\phi)$. Damit ist $\varphi \circ \phi : \mathbf{Z} \rightarrow H$ ein Epimorphismus. Angenommen $m \in \text{Ker}(\varphi \circ \phi)$. Dann $\varphi(\phi(m)) = g^{mk} = 1$ und n ist, wie wir im Beweis von (2.2) gesehen haben, ein Teiler von mk , d.h. d ist ein Teiler von m . Daher $\text{Ker}(\varphi \circ \phi) = d\mathbf{Z}$ und der Homomorphiesatz zeigt: $H \simeq \mathbf{Z}/d\mathbf{Z}$ ist zyklisch der Ordnung d .

Nach Bemerkung (c) zum Homomorphiesatz induziert φ eine eindeutige Korrespondenz zwischen den Gruppen, die zwischen $n\mathbf{Z}$ und \mathbf{Z} liegen mit den Untergruppen von G . Nach (a) hat $\mathbf{Z}/n\mathbf{Z}$ höchstens so viele Untergruppen, wie n Teiler hat. Daher gibt es zu jedem Teiler d von n genau eine Untergruppe der Ordnung d .

Bemerkung. Das folgende Diagramm zeigt die Untergruppenstruktur einer zyklischen Gruppe der Ordnung 24:



Definition. Es sei G eine Gruppe und $a \in G$. Die kleinste natürliche Zahl n mit $a^n = 1$ nennen wir die *Ordnung* von a und schreiben $|a| = n$; gilt $a^n \neq 1$ für jede natürliche Zahl n , so sagen wir, daß a *unendliche Ordnung* hat und schreiben $|a| = \infty$. Betrachten wir wieder den Homomorphismus $\varphi : \mathbf{Z} \rightarrow G$, $m \mapsto a^m$, so gilt $\text{Im}(\varphi) \simeq \mathbf{Z}/n\mathbf{Z}$, falls $|a| = n$ und $\text{Im}(\varphi) \simeq \mathbf{Z}$, falls $|a| = \infty$.

2.5 Satz. *Es sei G eine endliche Gruppe. Dann gilt $a^{|G|} = 1$ für alle $a \in G$.*

Beweis. Definiere wie in der Definition $\varphi(m) = a^m$ und $U = \text{Im}(\varphi)$. Sei $\text{Ker}(\varphi) = n\mathbf{Z}$, so $n > 0$, da $U \simeq \mathbf{Z}/n\mathbf{Z}$ endlich ist und nach Satz (2.2) ist

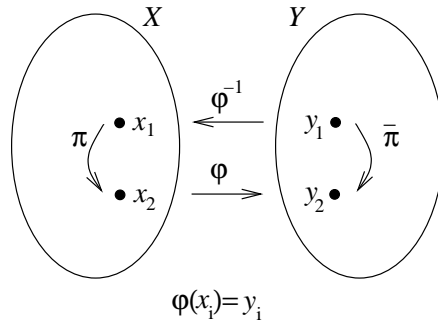
$$U = \{1 = a^0, a, \dots, a^{n-1}\}$$

und damit $a^n = a^{|U|} = 1$. Nach dem Satz von Lagrange folgt $a^{|G|} = (a^{|U|})^{|G:U|} = 1$.

Für den Rest dieses Abschnitts wollen wir uns mit den symmetrischen Gruppen beschäftigen. Das nächste Resultat zeigt, daß die Struktur der symmetrischen Gruppe $\text{Sym}(X)$ nur von der Kardinalität $|X|$ der Menge X abhängt.

2.6 Satz. *Es seien X, Y Mengen und $\varphi : X \rightarrow Y$ eine Bijektion. Dann ist $\text{Sym}(X) \simeq \text{Sym}(Y)$.*

Beweis. Wir definieren eine Abbildung $\bar{\pi} : \text{Sym}(X) \rightarrow \text{Sym}(Y)$ durch $\bar{\pi} = \varphi \circ \pi \circ \varphi^{-1}$ für $\pi \in \text{Sym}(X)$.



Als Komposition bijektiver Abbildungen ist $\bar{\pi} = \varphi \circ \pi \circ \varphi^{-1}$ bijektiv, also eine Permutation auf Y . Die Abbildung $\pi \mapsto \bar{\pi}$ ist auch ein Homomorphismus denn:

$$\overline{\pi_1 \circ \pi_2} = \varphi \circ \pi_1 \circ \pi_2 \circ \varphi^{-1} = \varphi \circ \pi_1 \circ \varphi^{-1} \circ \varphi \circ \pi_2 \circ \varphi^{-1} = \bar{\pi}_1 \circ \bar{\pi}_2.$$

Definiert man die Abbildung $\sim : \text{Sym}(Y) \rightarrow \text{Sym}(X)$ durch $\tilde{\sigma} = \varphi^{-1} \circ \sigma \circ \varphi$ für $\sigma \in \text{Sym}(Y)$, so folgt aus Symmetriegründen, daß diese Abbildung ebenfalls ein Homomorphismus ist. Offensichtlich sind die Abbildungen $-$ und \sim zueinander invers und daher sind beide Isomorphismen. Wir haben $\text{Sym}(X) \simeq \text{Sym}(Y)$.

Bemerkung. Ist X eine Menge mit n Elementen, so zeigt unser Satz, daß die Symmetrische Gruppe $\text{Sym}(X)$ isomorph ist und zur symmetrischen Gruppe auf der Menge $\{1, \dots, n\}$. Da man nur am Isomorphietyp einer Gruppe interessiert ist, darf man $X = \{1, \dots, n\}$ annehmen. Wir schreiben dann auch $\text{Sym}(n)$ statt $\text{Sym}(\{1, \dots, n\})$.

2.7 Satz. *Es gilt $|\text{Sym}(n)| = n!$.*

Beweis. Es sei $X = \{1, \dots, n\}$. Ist $\pi : X \rightarrow X$ injektiv, so gilt $|\pi(X)| = n = |X|$ und damit ist π sogar bijektiv, also eine Permutation. Um $|\text{Sym}(n)|$ zu berechnen müssen wir demnach die injektiven Abbildungen $\pi : X \rightarrow X$ abzählen. Man überlegt sich sofort, daß eine Abbildung π genau dann injektiv ist, wenn sie die folgenden n Bedingungen erfüllt.

- (1) $\pi(1) \in X$.

- (2) $\pi(2) \in X - \{\pi(1)\}$
- (3) $\pi(3) \in X - \{\pi(1), \pi(2)\}$
- \vdots \vdots
- (n) $\pi(n) \in X - \{\pi(1), \dots, \pi(n-1)\}$

Definiert man $\pi : X \rightarrow X$ dadurch, daß man $\pi(1) \in X$ beliebig, $\pi(2) \in X - \{\pi(1)\}$ beliebig $\dots, \pi(n) \in X - \{\pi(1), \dots, \pi(n-2)\}$ beliebig wählt, so erhält man eine injektive Abbildung und jede injektive Abbildung wird auf diese Weise konstruiert.

Für $\pi(1)$ hat man n Wahlen, für $\pi(2)$ hat man $n - 1$ Wahlen, \dots für $\pi(n)$ hat man $n - (n - 1) = 1$ Wahlen.

$$\text{Also } |\text{Sym}(n)| = n \cdot (n - 1) \cdots 1 = n!.$$

Bemerkung. Wie am Anfang dieses Abschnitts erwähnt sind die symmetrischen Gruppen aus gruppentheoretischer Sicht komplizierte Gruppen. Insbesondere ist $\text{Sym}(n)$ für $n \geq 3$ nicht zyklisch. Damit lassen sich die Elemente dieser Gruppe nicht als Potenzen eines erzeugenden Elementes schreiben. Gibt es vielleicht Teilmengen $X \subseteq \text{Sym}(n)$, die mehr als ein Element enthalten, sodaß die Elemente aus G Produkte von Elementen aus X sind? Nun diese Frage hat eine triviale Antwort: Man nehme $X = G$. Eigentlich meinen wir: Kann man eine besonders "schöne" Menge X mit der gewünschten Eigenschaft finden. "Schön" könnte heißen, daß X nur wenige Elemente hat, oder nur Elemente einer bestimmten Sorte. Mit dieser Frage im Zusammenhang mit der symmetrischen Gruppe beschäftigen wir uns im nächsten Abschnitt. Als Vorbereitung auf diese Frage verallgemeinern wir den Begriff des erzeugenden Elementes.

Definition. (a) Es sei G eine Gruppe. Eine Teilmenge X heißt *Erzeugendensystem* von G , falls sich jedes Element aus G als Produkt der Form $x_1 \cdots x_n$ schreiben läßt, wobei x_i oder x_i^{-1} in X liegt.

(b) Ist Y eine Teilmenge und $\langle Y \rangle$ die Menge aller Produkte der Form $y_1 \cdots y_n$ mit y_i oder y_i^{-1} in Y , so sieht man leicht ein, daß $\langle Y \rangle$ eine Untergruppe von

G ist. $\langle Y \rangle$ heißt das *Erzeugnis der Menge* Y . Insbesondere ist Y Erzeugendensystem von G , wenn $\langle Y \rangle = G$ gilt.

2.8 Beispiele. (a) Es sei $G = \{1 = g^0, \dots, g^{11}\}$ die zyklische Gruppe der Ordnung 12 mit einem erzeugenden Element g . Wir können also $G = \langle g \rangle$ schreiben. Nach (2.4) ist $\langle g^4 \rangle$ eine Untergruppe der Ordnung 3, $\langle g^3 \rangle$ eine Untergruppe der Ordnung 4. Schließlich gilt noch

$$G = \langle g^3, g^4 \rangle :$$

Sei R die rechte Seite, so ist R eine Untergruppe von G und nach dem Satz von Lagrange teilt $|R|$ die Zahl 12. Andererseits sind $\langle g^4 \rangle$ und $\langle g^3 \rangle$ Untergruppen von R . Damit sind wieder nach Lagrange 3 und 4 Teiler von $|R|$. Es folgt $|R| = 12$ und somit $G = R$.

(b) Es sei $G = \text{Sym}(3)$. Wir wissen bereits aus §1, daß G nicht abelsch ist, also auch nicht zyklisch. Damit braucht man wenigstens zwei Elemente um G zu erzeugen. Wir definieren zwei Permutationen durch

$$\begin{aligned} \tau : 1 \mapsto 2, 2 \mapsto 1, 3 \mapsto 3, \\ \sigma : 1 \mapsto 1, 2 \mapsto 3, 3 \mapsto 2. \end{aligned}$$

Klar ist, $\tau \neq \sigma$ und da die Untergruppe $U = \langle \sigma, \tau \rangle$ auch die Identität enthält, ist $|U| \geq 3$. Andererseits ist $\tau^2 = \mathbf{1}$. Damit hat τ die Ordnung 2. Nach (2.5) folgt: 2 teilt $|U|$. Damit gilt sogar $|U| \geq 4$. Schließlich ist $|U|$ ein Teiler von $|\text{Sym}(3)| = 3! = 6$. Wir folgern $U = \text{Sym}(3)$ und $\{\tau, \sigma\}$ ist ein Erzeugendensystem von G .

Bemerkung. Man beachte, daß durch Verwendung des Satzes von Lagrange es nicht nötig war, die Elemente aus der Gruppe G als Produkte der erzeugenden Elemente konkret hinzuschreiben. Das wäre in beiden Fällen natürlich auch möglich gewesen.

3 Permutationsgruppen

Dieses Kapitel handelt von Untergruppen von symmetrischen Gruppen, sogenannten Permutationsgruppen. Nachdem die Begriffe "Bahn" und "Stabilisator" erklärt sind, wird in Satz (3.2) eine fundamentale Beziehung beschrieben: die gruppeninterne Größe $|G : G_x| = \text{Index des Stabilisators}$ ist gleich

der externen Größe $|B|$ =Bahnlänge. Diese einfache Beobachtung erweist sich als grundlegend für die Gruppentheorie. Wir wenden dieses Resultat an und geben einen neuen Beweis der Ordnungsformel für $\text{Sym}(n)$. Bei der Behandlung der Zyklenzerlegung von Permutationen wird (3.2) ebenfalls von Nutzen sein. Wichtig für die lineare Algebra ist der Signumshomomorphismus. Man benötigt ihn dort bei der Behandlung der Determinante linearer Operatoren. Wir beenden das Kapitel mit Anwendungen der Gruppentheorie auf Symmetriebetrachtungen.

Definition. Es sei X eine nichtleere Menge und G eine Untergruppe der symmetrischen Gruppe $\text{Sym}(X)$ auf X . Man nennt das Paar (G, X) oder einfach G eine *Permutationsgruppe (auf der Menge X)*.

Im Folgenden schreiben wir auch $\pi\tau$ statt $\pi \circ \tau$ für $\pi, \tau \in G$.

3.1 Satz. *Es sei (G, X) eine Permutationsgruppe.*

- (a) *Wir definieren auf X die Relation \sim , indem wir $x \sim y$ setzen, falls ein $\pi \in G$ existiert mit $y = \pi(x)$. Dann ist \sim eine Äquivalenzrelation auf X .*
- (b) *Für $x \in X$ setze $G_x = \{\pi \in G \mid \pi(x) = x\}$. Dann ist G_x eine Untergruppe von G .*

Beweis. (a) Wegen $\mathbf{1} \in G$ und $\mathbf{1}(x) = x$ für $x \in X$, folgt $x \sim x$ für alle $x \in X$. Gilt $x \sim y$, so existiert ein $\pi \in G$ mit $\pi(x) = y$. Wendet man π^{-1} an, so erhält man $x = \pi^{-1}(y)$. Da π^{-1} Element von G ist, folgt $x \sim y$. Sei $x \sim y, y \sim z$. Dann existieren $\pi, \sigma \in G$ mit $y = \pi(x), z = \sigma(y)$. Damit folgt $z = \sigma(y) = \sigma(\pi(x)) = \sigma \circ \pi(x)$. Wegen $\sigma \circ \pi \in G$ hat man $x \sim z$ und (a) ist gezeigt.

(b) Wegen $\mathbf{1}(x) = x$ ist $\mathbf{1} \in G_x$. Seien $\pi, \sigma \in G_x$, also $\pi(x) = \sigma(x) = x$. Damit gilt auch $\sigma^{-1}(x) = x$, was $\sigma^{-1} \in G_x$ bedeutet. Also haben wir

$$\pi \circ \sigma^{-1}(x) = \pi(\sigma^{-1}(x)) = \pi(x) = x.$$

Damit gilt $\pi \circ \sigma^{-1} \in G_x$ und G_x ist eine Untergruppe von G .

Definition. Es sei (G, X) eine Permutationsgruppe und \sim die Äquivalenzrelation aus dem vorstehenden Satz. Es sei $x \in X$ und B die Äquivalenzklasse, die x enthält. Nach Definition ist

$$B = \{\pi(x) \mid \pi \in G\}.$$

Man nennt B eine *Bahn von G auf X* (die Bahn, die x enthält).

Ist B eine endliche Menge, so heißt die Anzahl $|B|$ der Elemente der Bahn die *Bahnlänge* von B . Für $\pi \in G$ sind die Elemente $x \in X$ mit $\pi(x) = x$ die *Fixpunkte* von π . Die Gruppe G_x aus dem Satz besteht also gerade aus den Elementen von G , die x als Fixpunkt haben. Man nennt G_x den *Stabilisator von x* .

Beispiel. Es $X = \{1, 2, 3\}$ und π die Permutation, die 1 und 2 vertauscht und 3 festläßt. Sei G die von π erzeugte zyklische Untergruppe von $\text{Sym}(X)$. Wegen $\pi^2 = \mathbf{1}$ ist $G = \{\mathbf{1}, \pi\}$ und $|G| = 2$. Jedes Element aus X ist fix unter $\mathbf{1}$ und 3 ist der einzige Fixpunkt von π . Ferner hat G die Bahnen $\{1, 2\}$ und $\{3\}$. Schließlich gilt $G_1 = G_2 = \{\mathbf{1}\}$, $G_3 = G$. Die folgende Beziehung zwischen den Elementen einer Bahn und den Nebenklassen eines Stabilisators ist fundamental.

3.2 Satz. *Es sei (G, X) eine Permutationsgruppe, B eine Bahn von G und $x \in B$.*

- (a) *Wähle $\pi_i \in G$ derart, daß die $\pi_i(x)$, $i \in I$ die verschiedenen Elemente von B sind. Also $B = \{\pi_i(x) \mid i \in I\}$ und $\pi_i(x) \neq \pi_j(x)$ für $i \neq j$. Dann ist*

$$G = \bigcup_{i \in I} \pi_i G_x$$

die Linksnebenklassenzerlegung von G modulo dem Stabilisator G_x .

- (b) *Es sei X endlich. Dann gilt*

$$|B| = |G : G_x|.$$

D.h. die Bahnlänge $|B|$ ist gleich dem Index $|G : G_x|$ des Stabilisators von x in G für jedes $x \in B$.

Beweis. (a) Sei $\pi \in G$. Dann liegt $\pi(x)$ in B und es existiert ein $i \in I$ mit $\pi(x) = \pi_i(x)$. Also $\pi_i^{-1} \circ \pi(x) = x$ was $\pi_i^{-1} \circ \pi \in G_x$ zeigt. Es folgt $\pi \in \pi_i G_x$. Damit gilt

$$G = \bigcup_{i \in I} \pi_i G_x.$$

Wir zeigen noch, daß diese Nebenklassen paarweise verschieden sind. Angenommen $\pi_i G_x = \pi_j G_x$. Dann existieren $\sigma_1, \sigma_2 \in G_x$ mit $\pi_i \circ \sigma_1 = \pi_j \circ \sigma_2$ und daher

$$\pi_i(x) = \pi_i(\sigma_1(x)) = \pi_i \circ \sigma_1(x) = \pi_j \circ \sigma_2(x) = \pi_j(\sigma_2(x)) = \pi_j(x).$$

Nach Wahl der π_i folgt $i = j$ und damit die Behauptung.

(b) Es sei $B = \{\pi_1(x), \dots, \pi_n(x)\}$, so ist nach (a)

$$G = \bigcup_{i \in I} \pi_i G_x$$

eine Nebenklassenzerlegung und daher

$$|G : G_x| = n = |B|.$$

3.3 Beispiel. Definiere $\pi, \sigma \in \text{Sym}(5)$ durch

$$\pi : 1 \mapsto 2, 2 \mapsto 1, 3 \mapsto 3, 4 \mapsto 5, 5 \mapsto 4$$

und

$$\sigma : 1 \mapsto 1, 2 \mapsto 2, 3 \mapsto 4, 4 \mapsto 5, 5 \mapsto 3.$$

Man verifiziert sofort: $|\pi| = 2$, $|\sigma| = 3$ und $\pi^{-1}\sigma\pi = \sigma^{-1}$. Das zeigt $\langle \sigma \rangle \trianglelefteq G$, wo $G = \langle \pi, \sigma \rangle$. Daher $|G| = 6$. Die Bahnen von G sind $B_1 = \{1, 2\}$ und $B_2 = \{3, 4, 5\}$. Schließlich erhält man als Stabilisatoren $G_1 = \langle \sigma \rangle$ und $G_3 = \langle \pi \rangle$. In Übereinstimmung mit Satz (3.2) ergibt sich

$$|B_1| = 2 = |G : G_1|, \quad |B_3| = 3 = |G : G_3|.$$

Ein neuer Beweis von (2.7): $|\text{Sym}(n)| = n!$.

Es sei $X = \mathbf{N}_n = \{1, \dots, n\}$ und $G = \text{Sym}(X) = \text{Sym}(n)$. Wir machen Induktion nach n .

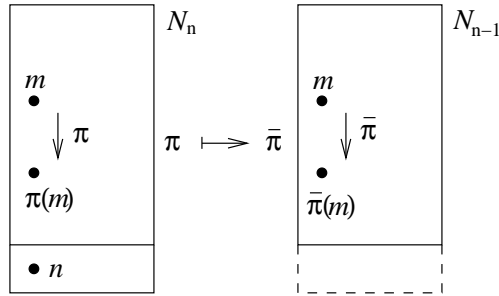
$n = 1$: $|\text{Sym}(1)| = |\{\mathbf{1}\}| = 1 = 1!$.

$n - 1 \Rightarrow n$: Zunächst gilt für den Stabilisator G_n von n :

(1)

$$\text{Sym}(n - 1) \simeq G_n.$$

Dazu definiere eine Abbildung $- : G_n \rightarrow H = \text{Sym}(n - 1)$ durch $\pi \mapsto \bar{\pi}$, wo $\bar{\pi}$ die Einschränkung der Permutation π auf $Y = \mathbf{N}_{n-1}$ ist. Wegen $\pi(n) = n$ permutiert π die Elemente von Y untereinander, d.h. $\bar{\pi}$ ist in der Tat aus H .



Für $\sigma \in H$ definiere die Permutation $\hat{\sigma}$ auf X durch

$$\hat{\sigma}(x) = \begin{cases} \sigma(x), & x \in Y, \\ n, & x = n. \end{cases}$$

Dann gilt $\hat{\sigma} \in G_n$. Man sieht leicht, daß die beiden Abbildungen $-$ und \wedge zueinander invers sind und beide Homomorphismen sind. Es folgt Aussage (1). Konsequenz dieser Aussage und der Induktion ist (2)

$$|G_n| = (n - 1)!$$

Es ist X eine G -Bahn: Sind nämlich $x, y \in X$, $x \neq y$,
So definiere

$$\pi(z) = \begin{cases} y, & z = x, \\ x, & z = y, \\ z, & \text{sonst.} \end{cases}$$

Offenbar ist π eine Permutation mit $\pi(x) = y$. Dann ist $x \sim y$ im Sinne der Äquivalenzrelation aus 3.1. Aus (3.2) folgt

$$n = |X| = |G : G_n|.$$

Aus (2) und dem Satz von Lagrange ergibt sich

$$|G| = |G : G_x| |G_x| = n(n - 1)! = n!$$

3.4 Zyklen. Es sei $X = \mathbf{N}_n = \{1, \dots, n\}$. Eine Permutation π aus $\text{Sym}(n)$ beschreibt man oft durch ein zweireihiges Schema der Gestalt

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

Zum Beispiel schreibt sich die Permutation

$$\pi : 1 \mapsto 2, 2 \mapsto 3, 3 \mapsto 1$$

als

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

Produkte $\pi\varphi = \pi \circ \varphi$ werden durch Auflösen von rechts berechnet, also

$$\begin{aligned} \pi\varphi &= \begin{pmatrix} 1 & \cdots & \varphi(m) & \cdots & n \\ \pi(1) & \cdots & \pi(\varphi(m)) & \cdots & \pi(n) \end{pmatrix} \begin{pmatrix} 1 & \cdots & m & \cdots & n \\ \varphi(1) & \cdots & \varphi(m) & \cdots & \varphi(n) \end{pmatrix} \\ &= \begin{pmatrix} 1 & \cdots & m & \cdots & n \\ \pi(\varphi(1)) & \cdots & \pi(\varphi(m)) & \cdots & \pi(\varphi(n)) \end{pmatrix}. \end{aligned}$$

Konkret:

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

Wir entwickeln jetzt eine sehr viele bequemere und aussagekräftigere Darstellung von Permutationen. Es sei $G = \langle \pi \rangle$ die von π erzeugte zyklische Gruppe. Eine Bahn B von G wird π -Zyklus oder *Zyklus von π* genannt, die Bahnlänge $|B|$ heißt *Zykluslänge*. Die Zyklen der Länge 1 bilden offenbar die Menge $Fix(\pi)$ der Fixpunkte von π . Das Komplement $Tr(\pi) = X - Fix(\pi)$ heißt der *Träger* von π und dieser ist die Vereinigung von Zyklen, deren Länge größer als 1 ist. Eine Permutation π heißt *k-Zyklus*, $k > 1$, falls der Träger $Tr(\pi)$ ein π -Zyklus der Länge k ist. 2-Zyklen nennt man *Transpositionen*.

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 1 & 3 \end{pmatrix}$$

hat die Zyklen $\{1, 2, 4\}$, $\{3, 5\}$ und $X = \mathbf{N}_5$ ist der Träger von π . Die Permutation

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

hat die Zyklen $\{1\}$, $\{2, 4\}$, $\{3\}$ und $Tr(\tau) = \{2, 4\}$ ist ein 2-Zyklus. Also ist τ eine Transposition. Die Identität hat offenbar nur die Zyklen $\{x\}$, $x \in X$ und $Fix(\mathbf{1}) = X$, $Tr(\mathbf{1}) = \emptyset$.

Beachte, daß wir etwas ungenau den Begriff Zyklus für Mengen (= Bahnen) wie auch für Permutationen verwenden. Aus dem Zusammenhang wird sich jedoch problemlos ergeben, in welchem Sinne dieser Begriff verwendet wird.

3.5 Satz. *Es seien π, ρ Permutationen aus $\text{Sym}(n)$.*

- (a) *Es sei $\text{Tr}(\pi) \cap \text{Tr}(\rho) = \emptyset$. Dann gilt $\pi\rho = \rho\pi$.*
- (b) *Sei B ein π -Zyklus der Länge k und $x \in B$. Dann gilt $B = \{x, \pi(x), \dots, \pi^{k-1}(x)\}$.*
- (c) *Es seien B_1, \dots, B_r die π -Zyklen der Länge > 1 . Dann existieren Zyklen $\rho_1, \dots, \rho_r \in \text{Sym}(n)$ mit $\text{Tr}(\rho_i) = B_i$, $1 \leq i \leq r$, mit $\pi = \rho_1 \cdots \rho_r$. Es gilt $\rho_i \rho_j = \rho_j \rho_i$ für alle $1 \leq i, j \leq r$.*
- (d) *Die Produktdarstellung von π mit disjunkten Zyklen wie in (c) ist eindeutig. D.h. sind ρ'_1, \dots, ρ'_s Zyklen mit $\text{Tr}(\rho'_i) \cap \text{Tr}(\rho'_j) = \emptyset$ für $i \neq j$ und $\pi = \rho'_1 \cdots \rho'_s$, so ist $r = s$ und $\rho_i = \rho'_i$ bei geeigneter Numerierung.*

Beweis. Setze $X = \mathbf{N}_n$.

(a) Wegen $\text{Tr}(\pi) \cap \text{Tr}(\rho) = \emptyset$ ist $X = \text{Fix}(\pi) \cup \text{Fix}(\rho)$. Sei $x \in X$, zum Beispiel $x \in \text{Fix}(\pi)$. Ist auch $x \in \text{Fix}(\rho)$, so $\pi\rho(x) = \pi(x) = x = \rho(x) = \rho\pi(x)$. Ist $x \in \text{Tr}(\rho)$, so ist auch $\rho(x) \in \text{Tr}(\rho) \subseteq \text{Fix}(\pi)$. Daher gilt

$$\rho(\pi(x)) = \rho(x) = \pi(\rho(x)).$$

Aus Symmetriegründen folgt $\rho\pi(x) = \pi\rho(x)$ für alle $x \in X$, also $\pi\rho = \rho\pi$.

(b) Ist s die Ordnung von π , so ist $\langle \pi \rangle = \{\mathbf{1}, \pi, \dots, \pi^{s-1}\}$. Damit folgt $B = \{\pi^i(x) \mid 0 \leq i < s\}$. Wähle $0 < \ell \in \mathbf{Z}$ so klein wie möglich, sodaß die Elemente $x, \pi(x), \dots, \pi^{\ell-1}(x)$ paarweise verschieden sind. Dann $\pi^\ell(x) = \pi^r(x)$ mit $0 \leq r < \ell$. Wende auf diese Gleichung π^{-r} an. Dann ist $\pi^{\ell-r}(x) = x$. Nach Wahl von ℓ folgt $r = 0$. Hieraus folgt, daß $B = \{\pi^i(x) \mid 0 \leq i < \ell\}$ ist und damit die Behauptung.

(c) Offenbar ist $\text{Tr}(\pi) = B_1 \cup \dots \cup B_r$ eine Partition. Für jedes $1 \leq i \leq r$ definiere eine Abbildung $\rho_i : X \rightarrow X$ durch:

$$\rho_i(x) = \begin{cases} \pi(x), & x \in B_i, \\ x, & \text{sonst.} \end{cases}$$

Man stellt sofort fest, daß ρ_i ein Zyklus der Länge k_i mit Träger $\text{Tr}(\rho_i) = B_i$ ist. Insbesondere folgt aus (a) $\rho_i \rho_j = \rho_j \rho_i$ für alle i, j . Sei $x \in X$. Ist

$x \in \text{Fix}(\pi) \subseteq \text{Fix}(\rho_i)$ für alle i , so folgt

$$\rho_1 \cdots \rho_r(x) = x = \pi(x).$$

Ist $x \in B_i$, so $x, \pi(x) = \rho_i(x) \in B_i$ d.h. $x, \pi(x) \in \text{Fix}(\rho_j)$, für $j \neq i$. Damit folgt

$$\rho_1 \cdots \rho_i \rho_{i+1} \cdots \rho_r(x) = \rho_1 \cdots \rho_i(x) = \rho_1 \cdots \rho_{i-1}(\pi(x)) = \pi(x).$$

Wir haben $\pi = \rho_1 \cdots \rho_r$.

(d) Wegen $\text{Tr}(\rho'_i) \cap \text{Tr}(\rho'_j) = \emptyset$ für $i \neq j$ ist $\pi(x) = \rho'_i(x)$ für $x \in \text{Tr}(\rho'_i)$ (gleiche Rechnung wie in der vorletzten Zeile von (c)). Damit sind $\text{Tr}(\rho'_1), \dots, \text{Tr}(\rho'_s)$ die π -Zyklen der Länge > 1 . Es folgt $r = s$ und $\text{Tr}(\rho'_i) = B_i$ bei geeigneter Nummerierung. Damit gilt auch $\rho_i = \rho'_i$ nach (b).

Definition. Es sei $\pi \in \text{Sym}(n)$ und $\pi = \rho_1 \cdots \rho_r$ die eindeutige Produktdarstellung von π durch Zyklen ρ_i mit $\text{Tr}(\rho_i) \cap \text{Tr}(\rho_j) = \emptyset$ für $i \neq j$. Diese Produktdarstellung heißt *Zyklendarstellung* oder *Zyklenschreibweise* der Permutation π .

Sind B_1, \dots, B_s die Zyklen von π und gilt

$$B_i = \{x_i, \pi(x_i), \dots, \pi^{k_i-1}(x_i)\},$$

so schreibt man

$$\pi = (x_1, \pi(x_1), \dots, \pi^{k_1-1}(x_1)) \cdots (x_s, \pi(x_s), \dots, \pi^{k_s-1}(x_s)).$$

Zyklen der Länge 1 kann man bei dieser Darstellung hinschreiben oder einfach weglassen. Also

$$\begin{aligned} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 10 & 3 & 2 & 4 & 1 & 7 & 6 & 9 & 8 & 5 \end{pmatrix} &= (1, 10, 5)(4)(2, 3)(6, 7)(8, 9) \\ &= (1, 10, 5)(2, 5)(6, 7)(8, 9). \end{aligned}$$

Berechnet man Produkte von Permutationen in Zyklendarstellung wie zuvor durch Rechtsauflösung, so erhält man das Produkt auch in der Zyklendarstellung. Zum Beispiel:

$$\begin{aligned} (1, 2)(3, \overrightarrow{9}, \overrightarrow{10})(4, 11)(5, 6)(7, 8) \cdot (1, 11)(2, 4)(\overrightarrow{3}, \overrightarrow{9})(5, 7)(6, 8) \\ = (1, 4)(2, 11)(\overrightarrow{3}, \overrightarrow{10})(5, 8)(6, 7). \end{aligned}$$

3.6 Satz. *Jede Permutation aus $\text{Sym}(n)$ ist das Produkt von Transpositionen.*

Beweis. Es sei $\pi \in \text{Sym}(n)$. Wir beweisen den Satz durch Induktion nach $|Tr(\pi)| = m$. Gilt $m = 0$, so $X = \mathbf{N}_n = \text{Fix}(\pi)$, d.h. $\pi = \mathbf{1}$ und π ist das leere Produkt von Transpositionen (aber auch $\mathbf{1} = \tau^2$ für jede Transposition). Ist $m = 2$, so ist π selbst eine Transposition. Sei also $m \geq 3$ und $a, b \in Tr(\pi)$ mit $\pi(a) = b$. Für die Transposition $\tau = (a, b)$ gilt $Tr(\tau) = \{a, b\} \subseteq Tr(\pi)$ und somit $\text{Fix}(\pi) \subseteq \text{Fix}(\tau)$. Ferner $\tau\pi(a) = \tau(b) = a$. Somit gilt $\text{Fix}\{\pi\} \cup \{a\} \subseteq \text{Fix}(\tau\pi)$. Insbesondere $|Tr(\tau\pi)| < m$. Nach Induktion existieren Transpositionen τ_1, \dots, τ_r mit $\tau\pi = \tau_1 \cdots \tau_r$. Multipliziere von links mit $\tau = \tau^{-1}$ und man erhält mit $\pi = \tau\tau_1 \cdots \tau_r$ die gewünschte Produktdarstellung.

3.7 Satz. *Die Identität $\mathbf{1} \in \text{Sym}(n)$ ist nicht das Produkt einer ungeraden Anzahl von Transpositionen.*

Beweis. Angenommen $\mathbf{1}$ lasse sich doch als Produkt einer ungeraden Anzahl k von Transpositionen schreiben und
(*)

$$\mathbf{1} = \tau_1 \cdots \tau_k$$

sei eine solche Darstellung, wobei k minimal gewählt sei. Ferner sei $\tau_k = (a, b)$.

Dann existiert ein $i < k$ mit $a \in Tr(\tau_i)$:

Anderenfalls wäre a Fixpunkt von $\tau_1 \cdots \tau_{k-1}$ und daher $b = \mathbf{1}(b) = \tau_1 \cdots \tau_k(b) = \tau_1 \cdots \tau_{k-1}(a) = a$, ein Widerspruch.

Wir nehmen nun weiter an, daß die Produktdarstellung (*) so gewählt ist, daß die Anzahl der τ_i mit $a \in Tr(\tau_i)$ minimal ist. Sei $j < k$ und $\tau_j = (a, c)$. Wegen

$$(a, c)(d, e) = (d, e)(a, c) \text{ und } (a, c)(c, d) = (c, d)(a, d)$$

können wir τ_j nach "hinten schieben" und annehmen, daß $a \in Tr(\tau_{k-1})$ ist.

Sei etwa $\tau_{k-1} = (a, c)$. Wäre $b = c$, so $\tau_k = \tau_{k-1}$ und aus (*) folgt

$$\mathbf{1} = \tau_1 \cdots \tau_k = \tau_1 \cdots \tau_{k-2} \tau_k^2 = \tau_1 \cdots \tau_{k-2},$$

ein Widerspruch zur Wahl von k . Ist $b \neq c$, so gilt

$$\tau_{k-1}\tau_k = (a, c)(a, b) = (b, c)(a, c) = \tau'_{k-1}\tau'_k.$$

In (*) eingesetzt erhalten wir

(**)

$$\mathbf{1} = \tau_1 \cdots \tau_{k-2} \tau'_{k-1} \tau'_k$$

und in (**) gibt es weniger Transpositionen, die a im Träger haben, als in (*). Aber in (*) sollte die Anzahl der Transpositionen, die a im Träger haben, schon minimal sein, ein Widerspruch. Es folgt die Behauptung.

3.8 Das Signum. Es sei $\pi \in \text{Sym}(n)$ und $\pi = \tau_1 \cdots \tau_m$, $\pi = \tau'_1 \cdots \tau'_r$ seien Produktdarstellungen von π mit Transpositionen.

Es gilt

$$m \equiv r \pmod{2}.$$

Denn wegen $\tau_i^{-1} = \tau_i$ ist $\mathbf{1} = \tau'_1 \cdots \tau'_r \tau_m \cdots \tau_1$ und mit dem vorstehenden Satz folgt, daß $m + r$ gerade ist, was $m \equiv r \pmod{2}$ bedeutet.

Definition. Ist $\pi \in \text{Sym}(n)$ und $\pi = \tau_1 \cdots \tau_r$ eine Produktdarstellung mit Transpositionen, so ist

$$\text{sgn } \pi = (-1)^r$$

das *Signum* von π . Das Signum hängt, wie wir gerade gesehen haben, nicht von der Produktdarstellung ab.

3.9 Satz. Die Signumsabbildung $\text{sgn} : \text{Sym}(n) \rightarrow \{-1, 1\}$ ist ein Homomorphismus, d.h.

$$\text{sgn}(\pi\rho) = \text{sgn } \pi \cdot \text{sgn } \rho.$$

Beweis. π sei Produkt von r Transpositionen und ρ sei Produkt von s Transpositionen. Dann ist $\pi\rho$ das Produkt von $r + s$ Transpositionen. Also

$$\text{sgn}(\pi\rho) = (-1)^{r+s} = (-1)^r (-1)^s = \text{sgn } \pi \cdot \text{sgn } \rho.$$

Bezeichnung. Der Kern der Signumsabbildung heißt die *alternierende Gruppe* $\text{Alt}(n)$ vom Grad n .

Folgerung. Es sei $n \geq 2$. Dann gilt

$$|\text{Alt}(n)| = \frac{n!}{2}.$$

Beweis. Nach Definition ist $\text{sgn}(1, 2) = -1$ und somit ist das Signum ein Epimorphismus auf $\{1, -1\}$. Nach dem Homomorphiesatz gilt

$$\text{Sym}(n)/\text{Alt}(n) \simeq \{1, -1\}.$$

Es folgt die Behauptung.

Bemerkungen. Neben unserer Definition des Signums gibt es auch andere. Am häufigsten wird das Signum durch die Formel

$$\text{sgn } \pi = \prod_{i < j} \frac{\pi(j) - \pi(i)}{j - i}$$

definiert. Der Vorteil dieser Definition ist die konkrete Formel. Nachteilig ist, daß diese Formel für die praktische Berechnung ganz ungeeignet ist. Die Zyklendarstellung liefert dagegen sofort als "Abfallprodukt" das Signum, wie die folgende Proposition zeigt.

3.10 Proposition. *Es sei $\pi \in \text{Sym}(n)$ und die Zyklenerlegung habe genau r Zyklen der Längen k_1, \dots, k_r . Dann gilt,*

$$\text{sgn } \pi = (-1)^{n-r} = (-1)^{k_1-1} \dots (-1)^{k_r-1} = (-1)^{a(\pi)},$$

wo $a(\pi)$ die Anzahl der Zyklen gerader Länge ist.

Beweis. Es sei $\pi = (a_1, \dots, a_p)$ ein p -Zyklus. Dann gilt

$$\pi = (a_1, a_2)(a_2, a_3) \cdots (a_{p-2}, a_{p-1})(a_{p-1}, a_p).$$

D.h. $\text{sgn } \pi = (-1)^{p-1}$ und insbesondere $\text{sgn } \pi = 1$, wenn p ungerade ist. Im allgemeinen Fall ist dann $\text{sgn } \pi = (-1)^{k_1-1} \dots (-1)^{k_r-1} = (-1)^{n-r}$. Es folgt die Behauptung.

3.11 Satz von Cayley. Es sei G eine endliche Gruppe. Definiere auf der Menge $X = G$ für $g \in G$ die Permutation $\pi(g) \in \text{Sym}(X)$ durch $\pi(g)x = gx$. M.a.W. die Permutation $\pi(g)$ bewirkt die Linksmultiplikation der Elemente aus $X = G$ mit dem Element g . Die Abbildung $\pi : G \rightarrow \text{Sym}(X), g \mapsto \pi(g)$ ist wegen

$$\pi(gh)x = (gh)x = g(hx) = \pi(g)(\pi(h)x) = \pi(g) \circ \pi(h)x$$

ein Homomorphismus. Aus $\pi(g)1 = 1$ folgt $g = 1$, was $\text{Ker}(\pi) = \{1\}$ zeigt. Also ist π ein Monomorphismus und $\text{Im}(\pi) \simeq G$. Aus (2.6) folgt:

Satz (Cayley). *Es sei G eine endliche Gruppe der Ordnung n . Dann ist G zu einer Untergruppe von $\text{Sym}(n)$ isomorph.*

Leider ist dieser Satz kein wirksames Hilfsmittel, um endliche Gruppen zu studieren. Er zeigt nur, daß die symmetrischen Gruppen mit wachsendem Grad immer komplizierter werden.