2.1 Gruppen

Wir führen jetzt eine Hierarchie von algebraischen Strukturen ein, die für die weiteren Überlegungen sehr wichtig sind. Dabei betrachten wir zunächst diejenigen, die aus einer Menge zusammen mit lediglich einer einzigen Verknüpfung bestehen:

2.1.1 Definition (Gruppoide, Halbgruppen, Monoide, Gruppen)

i) Unter einem *Gruppoid* verstehen wir eine Menge G zusammen mit einer *Verknüpfung* "$*$", d. h. mit einer Abbildung

$$* : G \times G \to G, (g, g') \mapsto g * g'.$$

ii) Sei $(G, *)$ ein Gruppoid. Ein Element $e \in G$ heißt

$$\begin{aligned} \textit{linksneutral} &:\Longleftrightarrow \quad \forall\, g \in G\colon\ e * g = g, \\ \textit{rechtsneutral} &:\Longleftrightarrow \quad \forall\, g \in G\colon\ g * e = g, \\ \textit{neutral} &:\Longleftrightarrow \quad \forall\, g \in G\colon\ g * e = e * g = g. \end{aligned}$$

iii) Ist $(G, *)$ ein Gruppoid mit neutralem Element e, $g \in G$, dann heißt $g' \in G$

$$\begin{aligned} \textit{linksinvers zu } g &:\Longleftrightarrow \quad g' * g = e, \\ \textit{rechtsinvers zu } g &:\Longleftrightarrow \quad g * g' = e, \\ \textit{invers zu } g &:\Longleftrightarrow \quad g' * g = g * g' = e. \end{aligned}$$

iv) *Halbgruppen* heißen die Gruppoide mit *assoziativer* Verknüpfung:

$$\forall\, g, g', g'' \in G\colon \quad g * (g' * g'') = (g * g') * g''.$$

v) *Monoid* heißt jede Halbgruppe mit neutralem Element.

vi) *Gruppe* nennt man ein Monoid mit Inversen:

$$\forall\, g \in G \quad \exists\, g' \in G : \quad g * g' = g' * g = e.$$

vii) *Abelsche* Gruppen sind die Gruppen mit kommutativer Verknüpfung:

$$\forall\, g, g' \in G\colon \quad g * g' = g' * g.$$

•

2.1.2 Beispiele

- $(\mathbb{N}, +)$ ist ein Monoid, aber keine Gruppe, $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +)$ sind abelsche Gruppen, ebenso $(\mathbb{Q}^*, \cdot), (\mathbb{R}^*, \cdot), (\mathbb{C}^*, \cdot)$, wenn $\mathbb{Q}^* := \mathbb{Q}\backslash\{0\}$ etc.

- Für Mengen X ist die Menge X^X aller Abbildungen von X nach X, zusammen mit der Komposition von Abbildungen, also das Paar $(X^X, \circ)$, ein Monoid.

- Die wichtigste Klasse von Beispielen ist die folgende. Sei X eine nicht leere Menge, $(G, *)$ Gruppoid, Halbgruppe, Monoid, oder Gruppe. Dann wird G^X zu Gruppoid, Halbgruppe, Monoid, Gruppe durch Einführung der *punktweisen* Verknüpfung $*'$ wie folgt:

$$\forall\ f, f' \in G^X\colon \quad (f *' f')(x) := f(x) * f'(x).$$

  Das Standardbeispiel ist hier $X := n = \{0, \ldots, n-1\}, G := \mathbb{R}$, also die Menge

$$\mathbb{R}^n = \{(x_0, \ldots, x_{n-1}) \mid x_i \in \mathbb{R}\}$$

  bei Zeilenschreibweise, bzw.

$$\mathbb{R}^n = \{\begin{pmatrix} x_0 \\ \vdots \\ x_{n-1} \end{pmatrix} \mid x_i \in \mathbb{R}\}$$

  bei Spaltenschreibweise, zusammen mit der punktweisen Addition

$$(x_0, \ldots, x_{n-1}) + (y_0, \ldots, y_{n-1}) = (x_0 + y_0, \ldots, x_{n-1} + y_{n-1}),$$

  bzw.

$$\begin{pmatrix} x_0 \\ \vdots \\ x_{n-1} \end{pmatrix} + \begin{pmatrix} y_0 \\ \vdots \\ y_{n-1} \end{pmatrix} = \begin{pmatrix} x_0 + y_0 \\ \vdots \\ x_{n-1} + y_{n-1} \end{pmatrix}.$$

- Die *symmetrische Gruppe* auf einer Menge X wird definiert als die Menge

$$S_X := \{\pi\colon X \rightarrowtail\!\!\!\!\!\rightarrow X\},$$

  zusammen mit der Hintereinanderausführung als Verknüpfung:

$$(S_X, \circ).$$

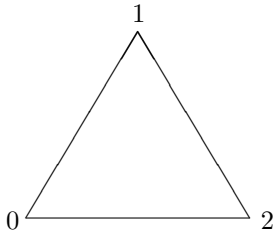
  Z. B. ist — in naheliegender Schreibweise, bei der die Bilder unter die Urbilder geschrieben werden —

$$S_3 = \{\begin{pmatrix} 012 \\ 012 \end{pmatrix}, \begin{pmatrix} 012 \\ 102 \end{pmatrix}, \begin{pmatrix} 012 \\ 210 \end{pmatrix}, \begin{pmatrix} 012 \\ 021 \end{pmatrix}, \begin{pmatrix} 012 \\ 120 \end{pmatrix}, \begin{pmatrix} 012 \\ 201 \end{pmatrix}\}.$$

  S_X ist leicht als Gruppe nachzuweisen, falls $|X| > 2$ ist diese Gruppe *nicht abelsch,* denn es gilt z. B.

$$\begin{pmatrix} 012 \\ 210 \end{pmatrix} \circ \begin{pmatrix} 012 \\ 021 \end{pmatrix} = \begin{pmatrix} 012 \\ 201 \end{pmatrix}, \text{aber } \begin{pmatrix} 012 \\ 021 \end{pmatrix} \circ \begin{pmatrix} 012 \\ 210 \end{pmatrix} = \begin{pmatrix} 012 \\ 120 \end{pmatrix},$$

und diese Nichtvertauschbarkeit ist natürlich nicht von der Numerierung der Elemente von X sondern nur von deren Anzahl abhängig. S_3 ist also eine nicht abelsche Gruppe. Man kann sie sich als *Symmetriegruppe* des regelmäßigen Dreiecks



vorstellen. Denn die Drehungen und Spiegelungen induzieren auf der Menge $\{0,1,2\}$ der Nummern der Ecken gerade die angegebenen Permutationen. Z.B. induziert die Drehung um 120 Grad *gegen den Uhrzeigersinn* die Permutation

$$\begin{pmatrix} 012 \\ 120 \end{pmatrix},$$

wenn wir $f(x) = y$ interpretieren als "y tritt an die Stelle von x".

$\diamond$

Es gelten die (echten!) Inklusionen

$$\text{Gruppoide} \supset \text{Halbgruppen} \supset \text{Monoide} \supset \text{Gruppen} \supset \text{abelsche Gruppen}.$$

In der Regel werden wir die *multiplikative Schreibweise* verwenden, also $*$ durch $\cdot$ ersetzen (und diesen Multiplikationspunkt oft einfachheitshalber sogar weglassen). Höchstens im kommutativen Fall werden wir die *additive Schreibweise* benutzen, also $+$ anstelle von $*$.
Es ist leicht zu zeigen, daß es in einem Gruppoid *höchstens ein neutrales Element* gibt: Für neutrale Elemente $e, e' \in G$ gilt nämlich $e = e * e'$, weil e' neutral ist, und die Neutralität von e ergibt daraus $e * e' = e'$. Bei multiplikativer Schreibweise werden wir dieses Element ggf. als 1 (oder genauer als 1_G) bezeichnen, bei additiver Schreibweise als 0 oder 0_G.
Ebenso mühelos zeigt man, daß Elemente von Monoiden *höchstens ein Inverses* besitzt, denn für zwei Inverse g' und g'' von g gilt offensichtlich

$$g' = e * g' = (g'' * g) * g' = g'' * (g * g') = g'' * e = g''.$$

Das Inverse wird ggf. mit g^{-1} bzw. $-g$ bezeichnet.

Hilfreich ist noch, daß man zum Nachweis der Gruppeneigenschaft von $(G, \cdot)$ manche Rechnung einsparen kann, wenn man folgendes Resultat berücksichtigt:

2.1.3 Satz *Halbgruppen $(G, \cdot)$ mit linksneutralem Element und diesbezüglichen Linksinversen sind Gruppen.*

Beweis: Sei e ein linksneutrales Element von G, g' linksinvers zu g bzgl. e.
i) Wir zeigen zunächst, daß g' auch rechtsinvers ist bzgl. e : Es gibt auch zu g' ein Linksinverses bzgl. e, es sei mit g'' bezeichnet. Hierfür gilt:

$$gg' = e(gg') = (g''g')(gg') = g''(g'g)g' = g''eg' = g''g' = e.$$

ii) Das Element e ist auch rechtsneutral:

$$ge = g(g'g) = (gg')g =_{i)} eg = g.$$

□

Die oben eingeführte *Verknüpfung* $*$ ist, genauer gesagt, eine *zweistellige* Abbildung:

$$G^2 \to G, (g, g') \mapsto g * g'.$$

Allgemeiner kann man *n-stellige* Verknüpfungen als Abbildungen $* : G^n \to G$ einführen und auf diese Weise dann die Existenz von Inversen als einstellige Abbildung auffassen:

$$G^1 \to G, g \mapsto g^{-1},$$

und die Existenz eines neutralen Elements mit der Existenz der folgenden nullstelligen Abbildung identifizieren: (denn $G^0 = G^\emptyset = \{\emptyset\}$):

$$G^0 \to G, \emptyset \mapsto e,$$

denn $G^0 = G^\emptyset = \{\emptyset\}$. Davon werden wir gleich anhand der nächsten Definition Gebrauch machen:

2.1.4 Definition (Unterstruktur) Ist G (genauer: die Menge G mit den vorgegebenen Verknüpfungen, der zweistelligen Verknüpfung $*$ und (gegebenenfalls) den ein- oder nullstelligen) ein Gruppoid, eine Halbgruppe ..., dann versteht man unter einem *Untergruppoid,* einer *Unterhalbgruppe,* ... eine Teilmenge $U \subseteq G$, so daß die Einschränkung der Verknüpfungen auf U^2 bzw. auf U^1 oder U^0 ihr Bild in U haben. Wir kürzen das mit

$$U \leq G$$

ab, wenn klar ist, welche Art algebraischer Struktur gemeint ist. •

2.1.5 Bemerkung *Zum Beweis von $U \leq G$ genügt der Nachweis, daß die Einschränkungen der die Struktur auf G definierenden Abbildungen auf U^2, U^1 bzw. auf U^0 nicht aus U hinausführen.*

Wir brauchen tatsächlich nicht mehr zu fordern, denn die geforderten Eigenschaften wie Assoziativität, Inversivität oder Neutralität übertragen sich automatisch von G nach U. Es folgt auch beispielsweise, daß Untergruppen ebenfalls nicht leer sind und dasselbe neutrale Element besitzen wie die Obergruppe! Wichtig ist vor allem diese unmittelbare Konsequenz:

2.1.6 Folgerung *Jeder Durchschnitt von Untergruppoiden, -halbgruppen, -monoiden oder -gruppen ist ebenfalls Untergruppoid, -halbgruppe, -monoid, -gruppe.*

Von besonderer Bedeutung ist es, ökonomische Verfahren zu entwickeln, mit denen eine Teilmenge $M \subseteq G$ daraufhin überprüft werden kann, ob sie eine Unterstruktur ist oder nicht. Zunächst einmal genügt natürlich die Überprüfung, ob die Einschränkungen der Verknüpfungen — von G^2, G^1, G^0 auf M^2, M^1, M^0 — aus M hinausführen oder nicht. Man kann dies bei Gruppen aber auch "in einem Aufwasch" verifizieren:

2.1.7 Satz *Sei $(G, \cdot)$ eine Gruppe, $\emptyset \neq U \subseteq G$. Dann gilt:*

i) $U \leq G \Longleftrightarrow [u, u' \in U \Longrightarrow u \cdot (u')^{-1} \in U]$.

ii) Ist U endlich, dann gilt $U \leq G \Longleftrightarrow [u, u' \in U \Longrightarrow u \cdot u' \in U]$.

iii) $U, U' \leq G \Longrightarrow [U \cdot U' \leq G \Longleftrightarrow U \cdot U' = U' \cdot U]$. *Dabei bedeutet $U \cdot U'$ das sogenannte* Komplexprodukt *von U mit U' :*

$$U \cdot U' := \{u \cdot u' \mid u \in U, u' \in U'\}.$$

Beweis: i) ist leicht nachzuprüfen:

a) Ist U eine Untergruppe, dann liegt mit u' auch dessen Inverses u'^{-1} in U und natürlich auch, zu jedem $u \in U$, das Produkt uu'^{-1}.

b) Liegt, umgekehrt, mit $u, u' \in U$ auch das Produkt uu'^{-1} in U, dann gilt das auch für $u' = u$, so daß $1_G = uu^{-1} \in U$ richtig ist. Setzen wir jetzt $u := 1_G$, dann folgt auch $u'^{-1} \in U$, die Inversen liegen also ebenfalls in U. Diese Teilmenge ist auch *multiplikativ abgeschlossen:* 1_G liegt in U, mit u' also auch u'^{-1} und deshalb, mit $u, u' \in U$, auch deren Produkt uu'. U ist demnach eine Untergruppe.

Für ii) beachten wir, daß es, wegen der Endlichkeit von G, für $u' \in U$ natürliche Zahlen $m \neq n$, etwa $m > n$, gibt mit $u'^n = u'^m$, also, wenn etwa $m > n$: $u'^{m-n} = e$, so daß eine Potenz von u' gleich dem Inversen von u' ist. Jetzt folgt aus i) die Behauptung.

iii) ist Übungsaufgabe.

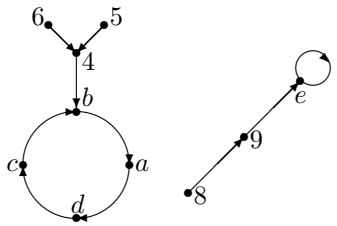
□

Sehen wir uns jetzt noch ein Beispiel etwas genauer an, die symmetrischen Gruppen auf endlichen Mengen, die bereits eingeführt worden sind. Es sollen einige Bezeichnungsweisen eingeführt werden, die den Umgang mit den Elementen symmetrischer Gruppen erleichtern.

2.1.8 Definition (Endofunktionen, Zyklen, disjunkte Zyklen)

- Bevor wir *bijektive* Abbildungen einer endlichen Menge X, also Elemente der symmetrischen Gruppe S_X, betrachten, wollen wir uns einmal *beliebige* Abbildungen $f \in X^X$ ansehen. Zunächst ein Beispiel, eine Abbildung

$f \in X^X$, wobei $X := \{4, 5, 6, 8, 9, a, b, c, d, e\}$, solche Funktionen heißen *Endofunktionen* auf X. Wir skizzieren uns diese Funktion durch einen *gerichteten Graphen,* die Pfeile geben an, welches Element von X worauf abgebildet wird. Hier ist ein Beispiel:

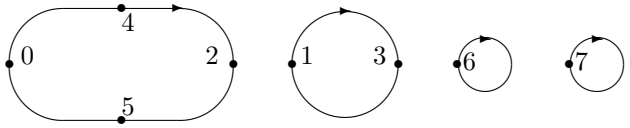


Es ist klar, daß eine Endofunktion einer *endlichen* Menge diese in zwei Teilmengen einteilt, von denen die eine Teilmenge aus den Elementen x besteht, die von einer geeigneten Potenz f^n auf sich selbst abgebildet werden: $f^n(x) = x$, für geeignetes n. Diese Punkte liegen also auf (gerichteten) *Kreisen* oder auch *Zyklen.*

- Ist die Abbildung dagegen *bijektiv,* dann müssen *alle* $x \in X$ auf solchen Kreisen liegen, hier ist ein Beispiel, ein Element π der symmetrischen Gruppe auf $X := \{0, 1, 2, 3, 4, 5, 6, 7\}$:

$$\pi := \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 3 & 5 & 1 & 2 & 0 & 6 & 7 \end{pmatrix}.$$

Visualisierung durch Zyklen ergibt folgendes Bild (die Pfeilrichtung deutet die Abbildungsrichtung an):



- Elemente $\pi \in S_X$, die höchstens einen Kreis aus mehr als einem Element enthalten heißen *zyklisch, Zyklus* oder genauer $r-$*Zyklus,* wenn r die Anzahl der Elemente dieses Zyklus ist. Das ist genau dann der Fall, wenn es — bei geeigneter Numerierung der Elemente von X — $x_0, \ldots, x_{r-1} \in X$ gibt mit

$$\pi = \begin{pmatrix} x_0 & x_1 & \ldots & x_{r-2} & x_{r-1} & x_r & \ldots & x_{|X|-1} \\ x_1 & x_2 & \ldots & x_{r-1} & x_0 & x_r & \ldots & x_{|X|-1} \end{pmatrix}.$$

Wir schreiben dann auch kurz

$$\pi = (x_0 \ldots x_{r-1})(x_r) \ldots (x_{|X|-1}),$$

oder gar nur

$$\pi = (x_0 \ldots x_{r-1}),$$

wenn klar ist, auf welcher Gesamtmenge π wirkt.

- Zwei Zyklen $\pi = (x_{i_0} \dots x_{i_{r-1}})$ und $\rho = (x_{j_0} \dots x_{j_{s-1}})$ in S_X heißen *disjunkt*, wenn r oder s gleich 1 ist oder, bei $r, s \neq 1$,

$$\{x_{i_0}, \dots, x_{i_{r-1}}\} \cap \{x_{j_0}, \dots, x_{j_{s-1}}\} = \emptyset.$$

•

Schreiben wir als Beispiel erneut die Elemente der symmetrischen Gruppe auf der Menge 3 hin, diesmal unter Verwendung der gerade eingeführten Notation für Zyklen:

$$S_3 = \{1, (01), (02), (12), (012), (021)\}.$$

2.1.9 Hilfssatz

i) Disjunkte Zyklen sind vertauschbare Abbildungen.

ii) Ist X eine endliche Menge, dann ist jedes $\pi \in S_X$ darstellbar als Komposition verschiedener und bis auf die Reihenfolge eindeutig bestimmter disjunkter Zyklen.

iii) $(x_{i_0} \dots x_{i_{r-1}}) = (x_{i_1} \dots x_{i_{r-1}} x_{i_0}) = (x_{i_2} \dots x_{i_{r-1}} x_{i_0} x_{i_1}) = \dots$.

iv) $(x_{i_0} \dots x_{i_{r-1}})^{-1} = (x_{i_{r-1}} x_{i_{r-1}} \dots x_{i_0})$,

v) $(x_{i_0} \dots x_{i_{r-1}}) = (x_{i_0} x_{i_1})(x_{i_1} x_{i_2}) \dots (x_{i_{r-1}} x_{i_{r-1}})$.

Beweis: trivial.

□

2.1.10 Definition (Zyklenschreibweise, Listenschreibweise) Die Darstellung von $\pi \in S_X$ als Produkt disjunkter Zyklen nennt man die *Zyklenschreibweise,* bei Weglassen der 1-Zyklen auch die *verkürzte Zyklenschreibweise.* Ist $\pi \in S_n$ und

$$\pi = \prod_{\nu=0}^{z(\pi)-1} (j_\nu \pi j_\nu \dots \pi^{l_\nu - 1} j_\nu) \qquad (*)$$

die Zyklenschreibweise für π ($z(\pi)$ steht also für die Anzahl der zyklischen Faktoren, l_ν für deren Längen), dann wird diese eindeutig, wenn wir noch fordern

a) $\forall\, n \in \mathbb{N}$: $j_\nu \leq \pi^n j_\nu$,

b) $j_0 < j_1 < \dots$.

In diesem Fall heißt $(*)$ auch die *Standardzyklenschreibweise.*
Neben dieser Zyklenschreibweise wird noch die *Listenschreibweise* benutzt, insbesondere in Computerprogrammen. Hier schreibt man einfach für $\pi \in S_n$ die Folge der Funktionswerte:

$$\pi = [\pi 0, \pi 1, \dots, \pi(n-1)].$$

Bijektionen von Mengen auf sich selbst heißen *Permutationen,* Gruppen, die aus Permutationen einer Menge X bestehen, also Untergruppen von S_X, X geeignet, heißen entsprechend *Permutationsgruppen,* $|X|$ heißt dabei der *Grad* der Permutation $\pi \in S_X$ bzw. der Untergruppe $U \leq S_X$. •

Eine weitere Definition von grundlegender Bedeutung ist das sogenannte Erzeugnis einer Teilmenge:

2.1.11 Definition (Erzeugnis) Als *Erzeugnis* $\langle T\rangle$ einer Teilmenge T eines Gruppoids, einer Halbgruppe, eines Monoids, einer Gruppe G bezeichnet man die kleinste Unterstruktur von G, die T umfaßt, also, wegen 2.1.6, den Durchschnitt aller Untergruppoide, Unterhalbgruppen, Untermonoide, Untergruppen, die T enthalten:

$$\langle T\rangle := \bigcap_{U:T\subseteq U\leq G} U.$$

•

Weil das Erzeugnis von T als *kleinste* Unterstruktur definiert ist, die T umfaßt, geht man beim Nachweis, daß eine Teil*menge* U die von T erzeugte Unterstruktur ist, am besten wie folgt vor:

2.1.12 Hilfssatz *Ist G Gruppoid, Halbgruppe, Monoid oder Gruppe, $T\subseteq G$ und U eine Teilmenge von G, dann genügt zum Beweis von $\langle T\rangle = U$ der Nachweis von*

1. *U ist Unterstruktur von G,*
2. *T liegt in U,*
3. *U liegt in jeder Unterstruktur, die T umfaßt.*

□

2.1.13 Beispiele

- Das Erzeugnis von z in der abelschen Gruppe $(\mathbb{Z},+)$ wird kurz mit $\langle z\rangle$ (anstelle von $\langle\{z\}\rangle$) bezeichnet. Es gilt

  $$\langle z\rangle = \{0,\pm z,\pm 2z,\ldots\}.$$

  Das Erzeugnis von $\emptyset$ in dieser Gruppe ist

  $$\langle\emptyset\rangle = \{0\}.$$

- Ganz allgemein bezeichnet man das Erzeugnis eines Elements g in einer Gruppe G mit $\langle g\rangle$, es gilt offenbar

  $$\langle g\rangle = \{1, g^{\pm 1}, g^{\pm 2}, g^{\pm 3},\ldots\}.$$

  Diese Untergruppe heißt *die von g erzeugte zyklische Untergruppe von G.*

◇

Zur Untersuchung und Anwendung von Gruppen ist sehr oft die Kenntnis eines *möglichst kleinen* Erzeugendensystems hilfreich, wir wollen ein solches für die symmetrischen Gruppen S_n angeben.

2.1.14 Hilfssatz *Die symmetrische Gruppe S_n hat die Ordnung*

$$|S_n| = n! := 1 \cdot 2 \cdots n$$

(dabei ist zu beachten, daß das leere Produkt *als 1 definiert wird, also $|S_0| = 0! := 1$ behauptet wird) und die folgenden Erzeugendensysteme:*

$$S_n = \langle (01), (12), \ldots, (n-2, n-1) \rangle = \langle (01), (0, \ldots, n-1) \rangle.$$

Beweis: Die Behauptung über die Ordnung ergibt sich durch Induktion nach n :
i) Die Induktionsbasis ist $|S_0| = 1 = 0!$, was offensichtlich richtig ist, denn die einzige Bijektion auf der leeren Menge ist die leere Abbildung.
ii) Zum Vollzug des Induktionsschlusses von n auf $n+1$ betrachten wir die möglichen Bilder des Punktes n in der Menge $n+1 = \{0, \ldots, n\}$ unter Bijektionen auf der Menge $n+1$. Er kann die $n+1$ verschiedenen Werte $0, \ldots, n$ annehmen, wir erhalten also

$$|S_{n+1}| = (n+1) \cdot |S_n| = (n+1) \cdot n! = (n+1)!,$$

wie behauptet.
Es bleiben noch die Behauptungen über die Erzeugendensysteme nachzuweisen. Zunächst zeigen wir, daß alle zyklischen Permutationen als Produkte von *Transpositionen* (das sind die Bijektionen, die genau zwei Punkte vertauschen und alle anderen auf sich selbst abbilden) schreiben lassen:

$$(i_0 \ldots i_{r-1}) = (i_0 i_1)(i_1 i_2) \ldots (i_{r-2} i_{r-1}).$$

Jetzt braucht nur noch gezeigt zu werden, daß man von den Transpositionen eigentlich nur die von *benachbarten Punkten* benötigt, was sich aus folgender Gleichung ergibt:

$$(j, k+1) = (k, k+1)(j, k)(k, k+1).$$

Damit ist bewiesen, daß die symmetrische Gruppe von den Transpositionen $(i, i+1)$ benachbarter Ziffern erzeugt wird.
Es bleibt schließlich noch zu verifizieren, daß auch das angegeben System aus nur *zwei* Elementen genügt. Hierzu bemerken wir, daß

$$(i, i+1) = (0, \ldots, n-1)^i (01) (0, \ldots, n-1)^{-i}$$

gilt, also jede Transposition benachbarter Ziffern aus (01) mit Hilfe der Permutation $(0, \ldots, n-1)$ konstruiert werden kann.

□

Beispielsweise ist

$$S_4 = \langle (01), (12), (23) \rangle = \langle (01), (0123) \rangle.$$

Aufgabe 2.1.1
Sei $(G, *)$ eine Gruppe. Zeigen Sie, daß für jedes $g \in G$ die Abbildungen

a) $l_g: G \to G,\ x \mapsto g * x$, sowie

b) $\kappa_g: G \to G,\ x \mapsto g * x * g^{-1}$,

bijektiv sind. (Kennzeichnen Sie jeweils, an welcher Stelle Sie welches Gruppenaxiom verwenden!).

Aufgabe 2.1.2

Sei $\pi := \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 10 & 4 & 1 & 7 & 8 & 9 & 11 & 2 & 3 & 0 & 5 & 6 \end{pmatrix} \in S_{12}$.

a) Schreiben Sie π als Produkt disjunkter Zykel.

b) Berechnen Sie $\pi^{-1}, \pi^3, \pi^4, \pi^{1997}$.

Aufgabe 2.1.3

Sei $(G, *)$ eine Gruppe und A, B zwei Untergruppen von G. Zeigen Sie:

Das Komplexprodukt $A * B$ ist genau dann eine Untergruppe von G, wenn gilt $A * B = B * A$.

Aufgabe 2.1.4

Geben Sie alle Untergruppen von S_3 an (keine Begründung)..