Einführung in die Algebra

Sebastian Bechtel, Isburg Knof, Theresa Tran

15. April 2015

1 Gruppen

Definition. Eine (innere) Verknüpfung auf einer Menge $M \neq \emptyset$ ist eine Abbildung $M \times M \to M, (a, b) \mapsto a \cdot b$.

Definition. Eine Gruppe ist eine Menge $G \neq \emptyset$ zusammen mit einer Verknüpfung $\cdot$, sodass Assoziativität (A), Existenz eines neutralen Elements (N) und Existenz inverser Elemente (I) erfüllt sind. G ist abelsch, falls Kommutativität (K) gilt.

Beispiel 1.
1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ sind abelsche Gruppen mit $+$ als Verknüpfung.
2. $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}, \mathbb{R}^*, \mathbb{C}^*$ mit Multiplikation sind abelsche Gruppen.
3. Für eine Menge M ist $\mathrm{Sym}(M)$ ist eine Gruppe, aber nicht abelsch.

Lemma 1. *a) Das neutrale Element ist eindeutig.*

b) Inverse Elemente sind eindeutig.

Beweis. a) Seien e, f neutrale Elemente, dann gilt $e = ef = f$.

b) Sei $a \in G$ und $b, b' \in G$ inverse Elemente. Dann gilt $b' = b'e = b'(ab) = (b'a)b = eb = b$.

□

Notation. multiplikativ: $a \cdot b$ oder ab, neutrales Element e oder 1, inverses Element von $a \in G$ ist a^{-1}.

Lemma 2. *Es sei $\mathcal{G} = (G, \cdot)$ eine Menge mit assoziativer Verknüpfung, einem linksneutralen Element und linksinversen Elementen, dann ist $\mathcal{G}$ eine Gruppe.*

Beweis. Sei $a \in G$ und $b \in G$ mit $ba = e$. Nach (I') gibt es $c \in G$ mit $cb = e$. Also $ab = eab = cbab = ceb = cb = e$.
Sei nun $a \in G$, es gilt $ae = a(a^{-1}a) = ea = a$. □

Lemma 3. *1.* $(a^{-1})^{-1} = a$, $(ab)^{-1} = b^{-1}a^{-1}$

2. $ab = ac$ *impliziert* $b = c$ *für alle* $a, b, c \in G$.

3. für $a, b \in G$ *gibt es genau ein* $x \in G$, *sodass* $ax = b$.

Beweis. 1. $(a^{-1})^{-1} = a$ klar. Für $a, b \in G$: $(b^{-1}a^{-1})ab = b^{-1}(a^{-1}a)b = b^{-1}eb = b^{-1}b = e$ (andere Richtung analog)

2. $ab = ac$ impliziert $a^{-1}(ab) = a^{-1}(ac)$ impliziert $b = c$

3. Setze $x = a^{-1}b$, dann erhält man $ax = a(a^{-1}b) = (aa^{-1})b = eb = b$. Die Eindeutigkeit folgt aus Punkt 2. □

Definition. Sei $a \in G$, $(G, \cdot)$ Gruppe. Für $n \in \mathbb{Z}$ definiere:

$$a^0 := e, \quad a^n := a^{n-1}a \quad \text{für } n \geq 1$$
$$a^n := \left(a^{-1}\right)^{-n} \quad \text{für } n < 0$$

Lemma 4. *Für* $a \in G$ *gelten* $a^n a^m = a^{n+m} = a^m a^n$ *und* $(a^m)^n = a^{n \cdot m}$. $ab = ba$ *impliziert* $(ab)^n = a^n b^n$.

Beispiel 2. 1. K Körper, dann ist $\mathrm{GL}_n(K)$ ein Gruppe bzgl. Matrixmultiplikation.

2. $M \neq \emptyset$ Menge, $(G, \cdot)$ Gruppe, definiere $\mathrm{Abb}(M, G) := G^M$. Für $f, g \in \mathrm{Abb}(M, G)$ ist $f \cdot g$ gegeben durch $(f \cdot g)(m) = f(m) \cdot g(m)$ für $m \in M$. Dann ist $(\mathrm{Abb}(M, G), \cdot)$ eine Gruppe.

2 Untergruppen

Definition. Sei $(G, \cdot)$ Gruppe. Eine Teilmenge $H \subset G$ heißt Untergruppe von G, falls $(H, \cdot)$ eine Gruppe ist.
Äquivalent dazu:

(i) Für $a, b \in H$ gilt $ab \in H$ (Abgeschlossenheit)

(ii) $e \in H$

(iii) Für $a \in H$ ist $a^{-1} \in H$

Satz 1. *Sei* $(G, \cdot)$ *Gruppe und* $H \subset G$ *nicht-leer. Dann gilt:* H *induziert Untergruppe von* $(G, \cdot)$ *gdw.* $ab^{-1} \in H$ *für* $a, b \in H$.

Beweis. "⇒"✓
"⇐"

- $a = b$ impliziert $e \in H$

- $e, a \in H$ impliziert $ea^{-1} \in H$ impliziert $a^{-1} \in H$
- $a, b^{-1} \in H$ impliziert $a\,(b^{-1})^{-1} \in H$ impliziert $ab \in H$ □

Beispiel 3. (a) $\{e\}, G$ induzieren je eine Untergruppe für alle Gruppen $(G, \cdot)$.

(b) K Körper. $\mathrm{SL}_n(K) = \{A \in M_n(K) : \det(A) = 1\}$ induziert Untergruppe von $\mathrm{GL}_n(K)$, die spezielle lineare Gruppe.

Definition. Eine Untergruppe heißt echt, falls sie nicht trivial ist.

Lemma 5. *Es sei $(H_j)_{j\in J}$ eine Familie von Untergruppen $H_j \subset G$. Dann ist $\bigcap_{j\in J} H_j$ eine Untergruppe von G.*

Beweis. Übung □

Definition. Es sei M eine Teilmenge von G. Die von M erzeugte Untergruppe ist der Durchschnitt aller Untergruppen, die M enthalten.

Notation. $\langle M\rangle = \bigcap_{M\subset H\subset G} H$, wobei H Untergruppe
Bemerkung. (a) $\langle\emptyset\rangle = \{e\}$

(b) Für $M \neq \emptyset$ gilt: $\langle M\rangle = \{m_1^{\varepsilon_1}\cdot ...\cdot m_n^{\varepsilon_n} : m_1, ..., m_n \in M, \varepsilon_1, ..., \varepsilon_n \in \{-1, +1\}, n \geq 0\}$

(c) Für $M = \{g\}$ gilt: $\langle g\rangle = \{g^n : n \in \mathbb{Z}\}$. Von g erzeugte zyklische Untergruppe von G.

Definition. G heißt zyklisch, falls $G = \langle g\rangle$ für ein $g \in G$ gilt.
Ist $G = \langle M\rangle$ mit M endlich, so heißt G endlich erzeugt.

Definition. (i) Die Ordnung einer Gruppe G ist $ord(G) = |G|$.

(ii) Die Ordnung eines Elements $g \in G$ ist $ord(g) = ord(\langle g\rangle)$.

(iii) Ist $ord(g)$ endlich, dann hat g endliche Ordnung.

Notation. (n, s) bezeichnet den größten gemeinsamen Teiler.

Satz 2. *Sei G Gruppe, $g \in G$*

1. *g hat nicht endliche Ordnung $\iff$ alle Potenzen von g sind verschieden*
2. *g hat endliche Ordnung $\iff \exists m > 0 : g^m = e$*
   Dann gilt:
   (a) $n := ord(g) = \min\{m > 0 : g^m = e\}$
   (b) $g^m = e \iff m = nk$ *für ein* $k \in \mathbb{Z}$
   (c) $\langle g\rangle = \{e, g^1, ..., g^{n-1}\}$
3. $ord(g^s) = \frac{n}{(n,s)}$ *für* $n = ord(g)$ *endlich*

Beweis. 1. Wir nehmen an: Für $i, j \in \mathbb{Z}$, oBdA $j > i$ gilt $g^i = g^j$. Dann gilt $g^{j-i} = g^j(g^i)^{-1} = e$. Es sei dann n die kleinste positive Zahl, die $g^n = e$ erfüllt. Sei $m \in \mathbb{Z}$ beliebig. Der Divisionsalgorithmus liefert: $m = kn + r$ für $0 \leq r < n$ und $k, r \in \mathbb{Z}$.

   Dann gilt: $g^m = g^{kn+r} = g^{kn}g^r = (g^n)^k g^r = eg^r = g^r$. Daraus folgt $\langle g \rangle = \{g^m : m \in \mathbb{Z}\} = \{g^r : r = 0, ..., n-1\}$. Besonders gilt $ord(g) = n$ ist endlich. ⌈ Dies zeigt $\Rightarrow$, $\Leftarrow$ klar, dann ist $\langle g \rangle = \{g^m : m \in \mathbb{Z}\}$ unendlich ⌋

2. Alle g^r mit $0 \leq r \leq n-1$ sind verschieden, da: $g^i = g^j \Rightarrow g^{j-i} = e \Rightarrow j - i = kn$ mit $k \in \mathbb{Z} \Rightarrow i \equiv j \pmod{n} \Rightarrow i = j$ falls $0 \leq i, j \leq n-1$. Dies liefert g^r mit $0 \leq r \leq n-1$ sind paarweise verschieden und es gilt: $ord(g) = n$. ⌈a und c⌋ Aus dem Divisionsalgorithmus folgt (b): $g^m = e \Leftrightarrow e = g^{kn+r} = g^r$ mit $m = kn + r, 0 \leq r < n \Leftrightarrow r = 0$. Also $m = kn$ mit $k \in \mathbb{Z}$.

3. Es sei $m = ord(g^s), n = ord(g)$. Aus $(g^s)^m = e$ folgt (siehe 2), dass n ein Teiler von sm ist. Dies liefert: $\frac{n}{(s,n)} | \frac{s}{(s,n)} m$. Somit $\frac{n}{(s,n)} | m$. Nun möchten wir noch zeigen: $m | \frac{n}{(s,n)}$. $(g^s)^{\frac{n}{(s,n)}} = (g^n)^{\frac{s}{(s,n)}} = e^{\frac{s}{(s,n)}} = e$. Daraus folgt $m | \frac{n}{(s,n)}$ (wegen 2). Also gilt $m = \frac{n}{(s,n)}$. □

Lemma 6. *Wir können alle Untergruppen einer zyklischen Gruppe beschreiben mit $G = \langle g \rangle, H \subset G$, es sei $h \in H, h \neq e$. Dann gilt: $h = g^k$.*

Beweis. Wir setzen: $m = min\{k > 0 : g^k \in H\}$.
⌈ Existiert: $G = \langle g \rangle = \langle g^{-1} \rangle, h = g^k, k < 0$, dann ersetzen wir h durch h^{-1}⌋
Wir wollen zeigen: $\langle g^m \rangle = H$

1. $\langle g^m \rangle \subset H$ gilt wegen $g^m \in H$

2. Es sei $j \in \mathbb{Z}$ mit $g^j \in H$. Divisionsalgorithmus liefert $j = lm + r$ mit $0 \leq r < m$: $g^j \in H \Rightarrow g^r = g^{-lm} g^{lm+r} = (g^m)^{-l} g^j$. Also $g^r \in H$. Aus der Minimalität von M folgt $r = 0$. Dies liefert $g^j = (g^m)^l \in \langle g^m \rangle$ und somit gilt: $H \subset \langle g^m \rangle$ und die zwei Untergruppen stimmen überein.

□

Ähnlich kann man zeigen:

Satz 3. *Alle Untergruppen einer zyklischen Gruppe sind zyklisch. Ist $ord(G) = n$ endlich und m ein Teiler von n, so ist $H = \langle g^{\frac{n}{m}} \rangle$ die einzige Untergruppe der Ordnung m.*

Definition. Sei H eine Untergruppe der Gruppe G. Dann kann man die folgende Äquivalenzrelation definieren:
$(x, y) \in G^2 : x \sim_H y \Leftrightarrow x = yh$ für ein $h \in H$
⌈Äquivalenzrelation wegen Gruppenaxiomen für H⌋

Definition. Die Äquivalenzklassen bzgl. $\sim_H$ heißen Linksnebenklassen.

Notation. Für $a \in G, aH = \{ah : h \in H\}$

Bemerkung. Es gelten folgende Eigenschaften:

- Die Abbildung $H \to aH, h \mapsto ah$ ist eine Bijektion. Besonders gilt: $|aH| = |H|$ für alle $a \in G$.
  ⌈Die Abbildung ist bijektiv, da sie umkehrbar ist: $aH \to H, b \mapsto a^{-1}b$ ist die Umkehrfunktion⌋
- $aH \neq bH \Rightarrow aH \cap bH = \emptyset$, d.h. sie sind disjunkt.
  ⌈$x \in aH \neq bH \Rightarrow x = ah_1 = bh_2$ für $h_1, h_2 \in H \Rightarrow a = bh_2h_1^{-1} \in bH \Rightarrow ah = b(h_2h_1^{-1}h) \in bH$ für alle $h \in H \Rightarrow aH \subset bH$. Ähnlich gilt $bH \subset aH$. Daraus folgt $aH = bH$.⌋

Definition. $G/H = \{aH : a \in G\}$ ist die Menge der Linksnebenklassen.
Der Index von H ist die Mächtigkeit von G/H, d.h. Index $[G : H] := |G/H|$

Bemerkung.
- $|G| = [G : H]|H|$
- Analog ist $a \sim_H b$ mit $a, b \in G \Leftrightarrow a = hb$ für ein $h \in H$ ("rechtsäquivalent bzgl. H") eine Äquivalenzrelation. Rechtsnebenklassen: $Ha = \{ha : h \in H\}$ mit $a \in G$
  Bijektion: Für $a \in G$ $aH \to Ha, x \mapsto a^{-1}xa$

Definition. $H\backslash G$ ist die Menge der Rechtsnebenklassen. Dann gilt: $|H\backslash G| = |G/H|$
⌈Bijektion: $H\backslash G \to G/H, Hb \mapsto b^{-1}H$⌋

Lemma 7. *Die Funktion*

$$H\backslash G \xrightarrow{f} G/H$$
$$Hb \to b^{-1}H$$

ist eine Bijektion

Beweis. 1) f ist wohldefiniert:
Gilt $Hb_1 = Hb_2$ für $b_1, b_2 \in G$ das heißt $b_1 \ _H\sim b_2$
existiert ein $h \in H$ mit $b_1 = hb_2$
$b^{-1} * H = (hb_2)^{-1} * H = b_2^{-1} * h * H = b_2^{-1} * H$
2) f ist Bijektion, da sie wohldefiniert ist:

$$G/H \xrightarrow{g} H\backslash G$$
$$Ha \to Ha^{-1}$$

ist wohldefiniert, ähnlich zu (1).
$g \circ f = Id_{H\backslash G}$ weil $G \circ f(Hb) = gb^{-1}H = H(b^{-1})^{-1} = Hb$
$f \circ g = Id_{G/H}$ analog. □

Satz 4. *Es seien H,K Untergruppen von G mit $K \subset H \subset G$. Dann gilt:*

$$[G : K] = [H : K] * [G * H]$$

Beweis. Wir nehmen an, dass $[G : H] = m$ und $[H : K] = n$ endlich sind. Dann gibt es $a_1, ..., a_n \in H$, so dass $H/K = \{a_1K, ..., a_nK\}$ und $b_1, ..., b_m \in G$ mit $G\backslash H = \{b_1H, ..., b_mH\}$

Dann gilt:

$$G = \bigcup_{\substack{i=1...m \\ j=1...n}} b_i a_j K$$

mit $b_i a_j K$ paarweise disunkt.

$b_{i_1} a_{j_1} K = b_{i_2} a_{j_2} K$ mit $i_1, i_2 \in \{1, ..., n\}$ und $j_1, j_2 \in \{1, ..., m\}$
$\Rightarrow b_{i_1} H$ und $b_{i_2} H$ sind nicht disjunkt.
$\Rightarrow b_{i_1} H = b_{i_2} H$
Dann gilt: $b_{i_1} a_{j_1} K = b_{i_1} a_{j_2} K$
$\overset{*b^{-1}}{\Rightarrow} a_{j_1} K = a_{j_2} K \Rightarrow a_{j_1} = a_{j_2}$
Also: Es gibt genau $m * n$ Linksnebenklassen von K in G.

$$\bigcup_{\substack{i=1...m \\ j=1...n}} b_i a_j K = \bigcup_i b_i (\bigcup_j a_j K) = \bigcup_i b_i H = G$$

□

Bemerkung. Der Beweis lässt sich zum Fall von unendlichem Index erweitern. Dies liefert eine Bijektion $G/H \times H/K \to G/K$

Korollar 1. *Satz von Lagrange*
Es gilt $|G| = [G : H] * |H|$ für jede Untergruppe H von G. Besonders gilt: $|H|$ teilt $|G|$ und $ord(g)$ ist ein Teiler von $|G|$ für jedes $g \in G$.

Beweis. $K = \{e\}$ im vorigen Satz. □

Beispiel 4. G endlich mit $|G| = p$ Primzahl. Dann existiert ein $g \in G$ mit $g \neq e$
$ord(g) = p \Rightarrow < g >$ besteht aus genau p Elementen.
Also $< g >= G$ und G ist die von g erzeugte zyklische Gruppe.

3 Normalen Untergruppen und Gruppenhomomorphismen

Satz 5. *Es sei G eine Gruppe unf $H \in G$ eine Untergruppe.*
Die folgenden Bedingungen sind äquivalent:
(i) es gilt: $bH = Hb$ für alle $b \in G$
(ii) es gilt: $b^{-1}Hb = H$ für alle $b \in G$
(iii) es gilt: $b^{-1}hb = H$ für alle $b \in G$ und $h \in H$

Definition. Eine Untergruppe H, die eine der Bedingungen (i)-(iii) erfüllt, nennt man eine normale Untergruppe (oder Normalteiler) von G.

Beweis. (i)⇒(ii)
Es sei $b \in G$ mit$bH = Hb$ Dann gilt für alle $x \in b^{-1}Hb$:
$x = b^{-1}hb \Rightarrow bx = hb \in Hb = bH$ mit $h \in H$
⇒ es gibt ein $h' \in H$ mit $bx = bh'$
$\Rightarrow b^{-1}xb = b$ also $x = b^{-1}bh' = h' \in H$
$\Rightarrow b^{-1}Hb \subset H$
Für $h' \in H$ gilt: $bh' \in bH = Hb$ Daraus folgt: $bh' = hb$ für ein $h \in h$ und $h' = b^{-1}hh' = b^{-1}hb \in b^{-1}Hb$ also $H \subset b^{-1}Hb$
(ii) *Rightarrow* (iii) ist klar.
(iii) *Rightarrow* (i)
Für $b \in G$, $h \in$ gilt:
$bh = bh(b^{-1}b) = ((b^{-1})^{-1}hb^{-1})b \in Hb$
(iii) für $b^{-1} \in G$ $hb = bb^{-1}hb \in bH$
Daraus folgt: $bH = Hb$ □

Bemerkung. Ist N normal, so gilt:
$(aN)(bN) = abN$

Beweis. $(aN)(bN) = (Na)(bN) = N(ab)N = (abN)N = abN$ □

Beispiele:
(1) Die trivialen Untergruppen $\{e\}$, G sind normal.

Definition. Eine Gruppe G sodass $\{e\}$ und G die einzigen normalen Untergruppen sind, nennt man einfache Gruppe.

(2) jede Untergruppe einer abelschen Gruppe ist normal.
(3) $SL_n(K)$ ist normale Untergruppe von $GL_n(K)$ (K Körper)

Definition. Es seien $(G, \cdot_G)$ und $(H, \cdot_H)$ Gruppen. Ein Gruppenhomomorphismus von G in H ist eine Abbildung $f : G \to H$, so dass gilt:
$f(a \cdot_G b) = f(a) \cdot_H f(b)$ für alle $a, b \in G$

Eigenschaften
(i) $f(e_G) = e_H$.
Für $g \in G$ beliebig gilt:
$f(g) = f(e_G \cdot_G g) = f(e_G) \cdot_H f(g)$
$\Rightarrow f(e_G) = f(e_G) \cdot_H (f(g) \cdot_H f(g)^{-1}) = f(g) \cdot_H f(g)^{-1} = e_H$
(ii) $f(g^{-1}) = g(g)^{-1}$ für alle $g \in G$
$e_H = f(e_G) = f(g \cdot_G g^{-1}) = f(g) \cdot_H f(g^{-1}) \Rightarrow f(g^{-1}) = f(g)^{-1}$
(iii) Seien $a_1 : G_1 \to G_2$ und $a_2 : G_2 \to G_3$ Gruppenhomomorphismen, dann ist $a_1 \circ a_2 : G_1 \to G_3$ ein Gruppenhomomorphismus.

Beispiele
(1) Für jedes $g \in G$ ist
$\mathbb{Z} \to G$
$n \to g^n$
ein Gruppenhomomorphismus.
(2) (Exponentialabbildung)
$(\mathbb{R}, +) \to (\mathbb{R}^*, \cdot)$
$x \to e^x$
ist ein gruppenhomomorphismus.
(3) Für $(G, +)$ ablegt ist
$G \to G$
$a \to na = a + ... + a$(n-mal)
ein Gruppenhomomorphismus.

Definition. Ist N eine normale Untergruppe von G, so ist G/N eine Gruppe, die man als Faktorgruppe von G bezüglich N bezeichnet (oder von N in G). Die natürliche Projektion
$G \to G/N$
$a \to aN$
ist dann ein surjektiver Gruppenhomomorphismus.

Definition. G, H Gruppen, $f : G \to H$ ein Gruppenhomomorphismus.
Bild von f: $im(f) = \{f(g), g \in G\}$
Kern von f: $ker(f) = \{g \in G, f(g) = e_H\}$

Lemma 8. *Für einen Gruppenhomomorphismus $f : G \to H$ gilt:*
(i) im(f) ist eine Untergruppe von H.// (ii) ker(f) ist eine normale Untergruppe von G.

Beweis. (i) folgt aus Eigenschaften (i) und (ii) für Gruppenhomomorphismen.
(ii) für $a, b \in ker(f) : f(ab^{-1}) = f(a)f(b^{-1} = e_H$
$\Rightarrow ab^{-1} \in ker(f)$ □

Definition. A, B, C Gruppen, $f : G \to H$ Gruppenhomomorphismus.
Das Bild von f ist: $im(f) = \{f(g)|g \in G\} \subseteq H$.
Der Kern von f ist: $ker(f) = \{g \in G|f(g) = e_H\} \subseteq G$.

Lemma 9. *Für jeden Gruppenhomomorphismus $f : G \to H$ gilt:*

(i) $im(f)$ ist eine Untergruppe von H.

(ii) $ker(f)$ ist eine normale Untergruppe von G.

(iii) f injektiv (bzw. surjektiv) $\Leftrightarrow ker(f) = e_G$ (bzw. $im(f) = H$).

Beweis. (i) $im(f)$ ist wegen der Definition von Gruppenhomomorphismen unter $\cdot_H$ abgeschlossen, enthält $e_H = f(e_G)$ (Eigenschaft (i)) und die Inversen aller seiner Elemente (Eigenschaft (ii)).

(ii) Für alle $a, b \in ker(f)$ gilt:

$$f(ab^{-1}) = f(a)f(b^{-1}) = f(a)(f(b))^{-1} = ee^{-1} = e.$$

Somit ist $ker(f)$ eine Untergruppe.
Für jedes $g \in ker(f)$ und $x \in G$ gilt:

$$f(x^{-1}gx) = f(x^{-1})f(g)f(x) = f(x^{-1})ef(x) = f(x^{-1})f(x) = f(x^{-1}x) = f(e) = e.$$

Also ist $x^{-1}gx \in ker(f)$ und somit ist $ker(f)$ ein Normalteiler.

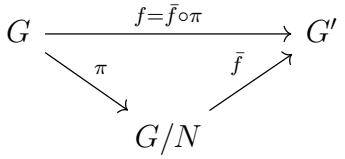
(iii) Subjektivität: offentsichtlich. Injektivität: vgl. Übung 2, Aufgabe 1.

□

Bemerkung.
- Ein bijektiver Homomorphismus wird Isomorphismus genannt. Die Umkehrfunktion ist dann wieder ein Isomorphismus.
- Ein Gruppenhomomorphismus $G \to G$ heißt Endomorphismus von G.
- Ein Gruppenisomorphismus $G \to G$ heißt Automorphismus von G.

Definition. G/N heißt Faktorgruppe von N in G, wenn N normale Untergruppe von G ist.
Gruppenstruktur: $aN \cdot bN = abN$, $eN = N$ neutrales Element
Die natürliche Projektion $\pi : G \to G/N, a \mapsto aN$ ist ein surjektiver Gruppenhomomorphismus mit $ker(\pi) = N, im(\pi) = G/N$.

Satz 6 (Homomorphiesatz)**.** *Es sei $f : G \to G'$ ein Gruppenhomomorphismus und N ein Normalteiler von G. Ist N im $ker(f)$ enthalten, so gibt es genau einen Gruppenhomomorphismus $\bar{f} : G/N \to G'$, so dass das folgende Diagramm kommutiert:*



Bemerkung. Es gilt $ker(\bar{f}) = \pi(ker(f))$ und $im(\bar{f}) = im(f)$.

Korollar 2. *Wenn $f : G \to G'$ ein surjektiver Homomorphismus ist, dann ist $\bar{f} : G/ker(f) \to G'$ ein Isomorphismus.*

Beweis des Satzes. Aus dem kommutativen Diagramm folgt, dass $\bar{f}(aN) = f(a)$ sein sollte für jedes $aN \in G/N$.
Wir zeigen zuerst, dass $\bar{f}$ wohldefiniert ist. Es seien $a, b \in G$ mit $aN = bN$. Dann gilt $a \sim_N b$ und also $b^{-1}a \in N$. Daraus folgt

$$f(a) = f(ea) = f(b(b^{-1}a)) = f(b)f(b^{-1}a) \overset{b^{-1}a \in N \subseteq ker(f)}{=} f(b)e = f(b).$$

Die Abbildung $\bar{f} : G/N \to G'$ existiert somit und ist offensichtlich ein Gruppenhomomorphismus, denn

$$\bar{f}(abN) = f(ab) = f(a)f(b) = \bar{f}(aN)\bar{f}(bN)$$

for all $a, b \in G$. □

Beweis der Bemerkung.

- $aN \in ker(\bar{f}) \overset{Def.\ von\ \bar{f}}{\Leftrightarrow} a \in ker(f) \overset{Def.\ von\ \pi}{\Leftrightarrow} aN \in \pi(ker(f))$
- $im(f) = im(\bar{f} \circ \pi) = \bar{f}(im(\pi)) \overset{\pi\ surj.}{=} \bar{f}(G/N) = im(\bar{f})$

□

Satz 7 (1. Isomorphiesatz)**.** *Es seien G eine Gruppe, $H \subseteq G$ eine Untergruppe und N ein Normalteiler von G. Dann ist $NH = \{nh | n \in N, h \in H\}$ Untergruppe von G und $N \cap H$ ein Normalteiler von H. Ferner ist $H/(N \cap H) \to (NH)/N, a(N \cap H) \mapsto aN$ ein Isomorphismus.*

Beweis. Es seien $n_1, n_2 \in N, h_1, h_2 \in H$. Dann gilt:

$$(n_1h_1)(n_2h_2)^{-1} = n_1h_1h_2^{-1}n_2^{-1} = n_1(h_1h_2^{-1}n_2^{-1}) = \cdots$$

[Da N normal, gilt $h_1h_2^{-1}N = Nh_1h_2^{-1}$. Es gibt also ein $n_3 \in N$ mit $h_1h_2^{-1}n_2^{-1} = n_3h_1h_2^{-1}$.]

$$\cdots = (n_1n_3)(h_1h_2^{-1}) \in NH.$$

Daraus folgt, dass NH Untergruppe von G ist.
Nun betrachten wir $f : H \to (NH)/N, a \mapsto aN = Na$. f ist ein surjektiver Gruppenhomomorphismus mit $ker(f) = N \cap H$. Aus dem Homomorphiesatz (+ Korollar) folgt dann, dass $\bar{f} : H/(N \cap H) \to (NH)/N$ ein Isomorphismus ist. □

Satz 8 (2. Isomorphiesatz)**.** *Es seien M, N normale Untergruppen einer Gruppe G. Gilt $N \subseteq M$, so ist M/N eine normale Untergruppe von G/N und die Abbildung $(G/N)/(M/N) \to G/M, (aN)M/N \mapsto aM$ ist ein Isomorphismus.*

Beweis. $f : G/N \to G/M, aN \mapsto aM$ (wohldefiniert wegen $N \subseteq M$) ist surjektiver Gruppenhomomorphismus mit $ker(f) = M/N$. Die Aussage folgt dann aus dem Korollar zum Homomorphiesatz. □

Notation. Seien A, B, C Gruppen, $\alpha : A \to B$, $\beta : B \to C$ Gruppenhomomorphismen.

- Falls $im(\alpha) = ker(\beta)$, so sagt man, dass die Folge $A \xrightarrow{\alpha} B \xrightarrow{\beta} C$ bei B exakt ist.
- α ist surjektiv, falls $A \xrightarrow{\alpha} B \longrightarrow \{e\}$ bei B exakt ist.
  $b \mapsto e$
- α ist injektiv, falls $\{e\} \longrightarrow A \xrightarrow{\alpha} B$ bei A exakt ist.
  $e \mapsto e_A$
- Notation: $\{e\} =: 1$. Eine exakte Folge der Form

  $$1 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \longrightarrow 1$$

  (d.h. α injekiv, β surjekiv und $im(\alpha) = ker(\beta)$), heißt kurze exakte Folge.

Beispiel 5 (für kurze exakte Folgen)**.**

- $1 \longrightarrow N \xrightarrow{\alpha} G \xrightarrow{\beta} G/N \longrightarrow 1$ ist exakt für jeden Normalteiler N von G.
- Für G abelsch ($\{e\} =: 0$):
  $0 \longrightarrow H \xrightarrow{\alpha} G \xrightarrow{\beta} G/H \longrightarrow 0$ ist exakt für jede Untergruppe H von G.

4 Produkte von Gruppen

Definition. Es sei $(G_i)_{i\in I}$ eine Familie von Gruppen. Das äußere direkte Produkt der Familie ist das kartesische Produkt $\prod_{i\in I} G_i$ mit der Verknüpfung $(a_i)_{i\in I}(b_i)_{i\in I} = (a_i b_i)_{i\in I}$. Neutrales Element: $(e_i)_{i\in I}$ mit $e_i \in G_i$ neutral.

Notation. $G_1 \times G_2 \times \cdots \times G_n$ für endliche Produkte.
$G_1 \oplus G_2 \oplus \cdots \oplus G_n$ für endliche Produkte, G_i abelsch [additiv].

Lemma 10. *Für jedes $i_0 \in I$ ist die Teilmenge*

$$\overline{G_{i_0}} = \{(b_i)_{i\in I} \in \prod_{i\in I} G_i | b_i = e_i \text{ für } i \neq i_0\}$$

ein Normalteiler von $\prod_{i\in I} G_i$, isomorph zu G_{i_0}.

Beweis. $\overline{G_{i_0}}$ ist der Kern des Gruppenhomomorphismus

$$p_{i_0} : \prod_{i\in I} G_i \to \prod_{i\in I-\{i_0\}} G_i, (b_i)_{i\in I} \mapsto (b_i)_{i\in I-\{i_0\}}.$$

Ferner ist

$$j_{i_0} : G_{i_0} \to \prod_{i\in I} G_i, a \mapsto (b_i)_{i\in I} \text{ mit } b_{i_0} = a \text{ und } b_i = e_i \text{ für } i \neq i_0.$$

Das Bild ist $\overline{G_{i_0}}$ und j_{i_0} ist injektiv, weil

$$(b_i)_{i\in I} = (e_i)_{i\in I} \Leftrightarrow b_i = e_i \text{ für alle } i \in I.$$

□

Bemerkung.
- $1 \longrightarrow G_{i_0} \xrightarrow{j_{i_0}} \prod_{i\in I} G_i \xrightarrow{p_{i_0}} \prod_{i\in I-\{i_0\}} G_i \longrightarrow 1$ ist kurze exakte Folge.
- Der Beweis liefert $\overline{G_{i_0}} \cap \langle \bigcup_{i\in I-\{i_0\}} G_i \rangle = \{e\}$.

Definition. Sei G eine Gruppe und $(N_i)_{i\in I}$ eine Familie von normalen Untergruppen, so dass gilt:

(i) $G =< \cup_{i\in I} N_i >$

(ii) $N_{i_0} \cap < \cup_{i\in I\setminus\{i_0\}} N_i >= \{e\}$ für jedes $i_0 \in I$.

Dann ist G das innere Produkt von $(N_i)_{i\in I}$.

Lemma 11. *Es sei G das innere Produkt von $(N_i)_{i\in I}$. Dann gilt $ab = ba$ für $a \in N_i, b \in N_j$ mit $i \neq j$.*

Beweis. Man rechnet:

$$ab\,(ba)^{-1} = aba^{-1}b^{-1} = (aba^{-1})b^{-1} = a(ba^{-1}b^{-1}) \in N_i \cap N_j$$

Somit folgt $ab\,(ba)^{-1} = e$, also $ab = ba$. □

Wir werden uns demnächst nur mit endlichen Produkten beschäftigen.

Lemma 12. *Sei G Gruppe, $N_1, \ldots, N_r$ normale Untergruppen von G. Dann ist G genau dann das innere Produkt von $N_1, \ldots, N_r$, wenn gilt:*

(i)' $G = N_1 \ldots N_r$

(ii)' Die Darstellung $a = n_1 \ldots n_r$ mit $n_j \in N_j$ ist für jedes $a \in G$ eindeutig bestimmt.

Beweis. (i) äquivalent (i)': folgt aus

$$< \bigcup_{i=1}^{r} N_i >= \{a_1^{\xi_1} \ldots a_k^{\xi_k} : a_j \in N_1 \cup \cdots \cup N_r, \xi_j = \pm 1\}$$

und der Tatsache, dass die N_j normale Untergruppen sind die für paarweise verschiedene $j \neq j'$ kommutieren.

(ii)' impliziert (ii): oBdA gelte $i_0 = 1$. Wir möchten zeigen, dass

$$N_1 \cap < N_2 \cup \cdots \cup N_r >= N_1 \cap (N_2 \ldots N_r) = \{e\}$$

Sei $x \in N_1 \cap < N_2 \dots N_r >$. Dann gilt $x = n_1 \in N_1$ und $x = n_2 \dots n_r$ mit $n_i \in N_i$ für $i \geq 2$. Also $x = n_1 e \dots e = e n_2 \dots n_r$, somit $n_i = e$ für alle i, also $x = e$.

(ii) impliziert (ii)': Aus $n_1 \dots n_r = n_1' \dots n_r'$ mit $n_i, n_i' \in N_i$ folgt

$$(n_1')^{-1} n_1 = (n_2' \dots n_r') (n_2 \dots n_r)^{-1} = \{e\}$$

Die letzte Gleichheit gilt nach (ii). Also folgt $n_i = n_i'$. Vertauschen der Reihenfolge liefert dies für $i \neq 1$. □

Satz 9. *Das innere Produkt G von normalen Untergruppen $N_1, \dots, N_r$ ist zum äußeren Produkt $N_1 \times \dots \times N_r$ kanonisch isomorph. Folgerung: Wir brauchen nicht zwischen den $\overline{G_i} = N_i$ und den G_i zu unterscheiden.*

Beweis. Wir definieren

$$N_1 \times \dots \times N_r \xrightarrow{\pi} G, \quad (n_1, \dots, n_r) \mapsto n_1 \dots n_r$$

Da das Bild von π die Untergruppe $N_1 \dots N_r \overset{(i)'}{=} G$ ist, ist π surjektiv. Aus (ii)' folgt, dass π auch injektiv ist. π ist auch Gruppenhomomorphismus:

$$\begin{aligned} &\pi((m_1, \dots, m_r) \cdot (n_1, \dots, n_r)) \\ = \pi((m_1 n_1, \dots, m_r n_r)) = m_1 n_1 \dots m_r n_r &= m_1 \dots m_r n_1 \dots n_r \\ &\pi(\bar{m}) \pi(\bar{n}) \end{aligned}$$

Dabei gilt die vorletzte Gleichheit, weil wir Elemente aus verschiedenen Untergruppen vertauschen dürfen. □

Definition. Für N, H Gruppen ist eine Gruppenerweiteruung von N durch eine kurze, exakte Folge von Gruppen

$$1 \longrightarrow N \longrightarrow G \longrightarrow H \longrightarrow 1$$

gegeben, wobei i injektiv, p surjektiv, im $i = \ker p$ ($G/H \cong H$).

Beispiel 6. $G = N \times H$ Diese ist i.A. nicht die einzige Gruppenerweiterung.

Definition. Es seien G eine Gruppe, $N \subseteq G$ Normalteiler von G und $H \subseteq G$ beliebige Untergruppe, so dass gilt:

$$G = NH \quad \text{und} \quad N \cap H = \{e\}$$

Dann ist G das semidirekte Produkt von N und H, Notation: $G = N \rtimes H$.

Bemerkung. Jedes $a \in G$ hat eine eindeutige Darstellung $a = nh$ mit $n \in N, h \in H$. Dies liefert eine Bijektion

$$N \times H \to G = N \rtimes H, (n, h) \mapsto nh$$

Satz 10. *Für jedes $h \in H$ ist die Konjugationsabbildung*

$$\gamma_h : N \to N, \quad n \mapsto hnh^{-1}$$

ein Automorphismus von N. Dies ergibt den Homomorphismus

$$H \xrightarrow{\gamma} Aut(N), h \mapsto \gamma_h$$

Beweis. γ ist Homomorphismus:

$$\begin{aligned}\gamma_{h_1h_2}(n) &= (h_1h_2)n\,(h_1h_2)^{-1} = h_1h_2nh_2^{-1}h_1^{-1} \\ &= h_1\gamma_{h_2}(n)h_1^{-1} = (\gamma_{h_1} \circ \gamma_{h_2})(n)\end{aligned}$$

für $n \in N$. □

Bemerkung. (1) Das semidirekte Produkt von N und H wird von $\gamma : H \to \mathrm{Aut}(N)$ eindeutig festgelegt. Es gilt nämlich:

$$(n_1h_1)(n_2h_2) = n_1(h_1n_2h_1^{-1})h_1h_2 = n_1\gamma_{h_1}(n_2)h_1h_2$$

wobei

$$n_1\gamma_{h_1}(n_2) \in N, h_1h_2 \in H$$

.

(2) Umgekehrt definiert $\gamma : H \to \mathrm{Aut}(N)$ immer ein semidirektes Produkt $N \rtimes H$:

$$\begin{aligned}G &= (N \times H, \cdot_\gamma) \\ (n_1, h_1) \cdot_\gamma (n_2, h_2) &= (n_1\gamma_{h_1}(n_2), h_1h_2)\end{aligned}$$

ist Gruppe mit neutralem Element (e_N, e_H) und inversen Elementen

$$(n, h)^{-1} = (\gamma_{h^{-1}}(n^{-1}), h^{-1})$$

Definiere:

$$\begin{aligned}N^* &:== \{(n, e_H) : n \in N\} \cong N, \\ H^* &:== \{(e_N, h) : h \in H\} \cong H\end{aligned}$$

N^*, H^* sind Untergruppen von G, isomorph zu N bzw. H.

$$\pi : G \longrightarrow H, \quad (n, h) \mapsto h$$

ist ein Homomorphismus mit $\ker \pi = N^*$, also ist N^* normale Untergruppe.
Das $N^* \cap H^* = \{e\}$ ist klar.

$$(n, h) = (n, e_H) \cdot_\gamma (e_N, h)$$

liefert $G = N^*H^*$.

Definition. Eine kurze exakte Folge

$$1 \longrightarrow N \xrightarrow{i} G \underset{s}{\overset{p}{\rightleftarrows}} H \longrightarrow 1$$

spaltet, falls ein Homomorphismus $s : H \to G$ existiert, mit $p \circ s = \mathrm{id}_H$. p heißt ein Schnitt von p.

Für $G = N \rtimes H$ Gruppenerweiterung:

$$1 \longrightarrow N \xrightarrow{i} G \xrightarrow{p} H \longrightarrow 1$$

wobei $i : N \to G, n \mapsto (n, e_H), p : G \to H, (n, h) \mapsto h$ ist $j : H \to G, h \mapsto (e_N, h)$ Schnitt. H ist Untergruppe. Man rechnet $(p \circ j)(h) = p(e_N, h) = h$

Satz 11. *Es sei*

$$1 \longrightarrow N \xrightarrow{i} G \xrightarrow{p} H \longrightarrow 1$$

eine Gruppenerweiterung, die mit einem Schnitt $s : H \to G$ spaltet. Dann ist G das semidirekte Produkt von N und H, definiert durch

$$\gamma : H \to Aut(N), \quad h \mapsto \gamma_h$$

Beweis. Wir setzen $\rho : N \rtimes H \to G, (n, h) \mapsto i(n)s(h)$. Zeige, dass ρ Homomorphismus ist:

$$\begin{aligned} &\rho((n_1, h_1) \cdot (n_2, h_2)) = \rho(n_1\gamma_{h_1}(n_2), h_1h_2) \\ &= i(n_1)i(\gamma_{h_1}(n_2))s(h_1)s(h_2) = i(n_1)s(h_1)i(n_2)s(h_1)^{-1}s(h_1)s(h_2) \\ &= \rho(n_1, h_1)\rho(n_2, h_2). \end{aligned}$$

Es bleibt zu zeigen, dass ρ bijektiv ist.

1. Injektivität

   Sei $(n, h) \in \ker(\rho)$. Dann gilt

   $i(n) \cdot s(h) = e_G \Rightarrow e_H = p(e_G) = p(i(n) \cdot s(h)) = p(i(n)) \cdot p(s(h))$.

   Aber $p(i(n)) = e_H$ wegen der kurzen exakten Folge und $p(s(h)) = h$. Also $e_H = h$.

   Damit ist $i(n) \cdot s(h) = i(n) \cdot s(e_H) = i(n) \cdot e_G = i(n)$. Da $(n, h) \in \ker(\rho)$ folgt $i(n) = e_G$ und somit $n = e_N$, da i injektiv ist.

   Daraus folgt $\ker(\rho) = \{(e_N, e_H)\}$. Somit ist ρ injektiv.

2. Surjektivität

   Sei $a \in G$ beliebig. Wir setzen: $b := a \cdot (s(p(a))^{-1}$. Wegen der Schnitteigenschaft von s ist $p \circ s = \mathrm{id}_H$ und somit

$p(b) = p(a) \cdot (p \circ s)(p(a)^{-1}) = p(a) \cdot p(a)^{-1} = e_G$. Daraus folgt $b \in \ker(p) = \mathrm{im}(i)$. Und somit $\exists n \in N$ mit $i(n) = b$. Dies liefert:

$\rho(n, p(a)) = b \cdot s(p(a)) = a \cdot s(p(a))^{-1} s(p(a)) = a.$

□

Beispiel 7. (a) Für einen beliebigen Körper K zerfällt (bzw. spaltet)

$$1 \longrightarrow SL_n(K) \longrightarrow GL_n(K) \xrightarrow{\det} K^* \longrightarrow 1.$$

Das heißt $GL_n(K) = SL_n(K) \rtimes K^*$.

(b) Es sei N eine beliebige abelsche Gruppe und $H := (\{\pm 1\}, \cdot)\,[\cong (\mathbb{Z}/2\mathbb{Z}, +)]$. Für $h \in H$ sei γ_h definiert als $\gamma_h : N \to N, \gamma_h(n) := n^h$.

Dann heißt $D_n := N \rtimes H$ verallgemeinerte Diedergruppe. Diese hat die Verknüpfung $(n_1, \epsilon_1) \cdot (n_2, \epsilon_2) = (n_1 n_2^{\epsilon_1}, \epsilon_1 \epsilon_2)$. Es ist $N \cong N \times \{1\}$ eine normale Untergruppe von D_N mit Index $[D_N : N] = 2$.

(c) Spezialfall: $N = \mathbb{Z}/k\mathbb{Z}$, $D_{2k} := D_{\mathbb{Z}/k\mathbb{Z}}$ heißt Diedergruppe der Ordnung $2k$. Dann ist D_{2k} die Symmetriegruppe des regelmäßigen k-Gons. Die Untergruppe $N \subset D_{2k}$ ist gerade die Menge der Drehungen.

Ist G eine von zwei Elementen $n, h \in G$ erzeugt, also $G = \langle n, h \rangle$, mit $ord(n) = k$ ($\cong$ Drehung) und $ord(h) = 2$ ($\cong$ Spiegelung) und außerdem $h^{-1} n h = n^{-1}$, so gilt $G \cong D_{2k}$.

5 Die symmetrische Gruppe

Definition. Für eine Menge $M \neq \emptyset$ bildet S_M als Menge aller Bijektionen von $M \to M$ mit Verkettung von Funktionen als Verknüpfung und der Identität als neutrales Element eine Gruppe, die *symmetrische Gruppe von M*. Die Elemente von S_M heißen *Permutationen*.

Satz 12 (Satz von Cayley)**.** *Jede Gruppe G ist isomorph zu einer Untergruppe von S_G.*

Beweis. Für jedes Element $a \in G$ ist die Linkstranslation um a, also $\lambda_a : G \to G, b \mapsto a \cdot b$ eine Permutation.

Die Abbildung $\lambda : G \to S_G, a \mapsto \lambda_a$ ist ein Homomorphismus, denn für $a, b, h \in G$ gilt

$$\lambda_{ab}(h) = abh = a(bh) = a\lambda_b(h) = \lambda_a(\lambda_b(h)) = (\lambda_a \circ \lambda_b)(h).$$

Es sei $a \in \ker(\lambda)$. Dann gilt $\lambda_a = \mathrm{id}_G \Rightarrow ah = h$ für alle $h \in G$ und damit

$$a = a \cdot e = \lambda_a(e) = e \Rightarrow \ker(\lambda) = \{e\}.$$

Also ist λ injektiv und somit $G \cong \mathrm{im}(\lambda)$. □

Definition. Es sei $M \neq \emptyset$ eine Menge und σ eine Permutation von M.

1. Der Träger von σ ist $\text{supp}(\sigma) := \{m \in M : \sigma(m) \neq m\}$.
2. Ein Zyklus der Länge l ist eine Permutation $\sigma \in S_M$ mit $l = |supp(\sigma)|$, so dass

$$supp(\sigma) = \{m_1, m_2, \ldots, m_l\} \text{ mit } \sigma(m_j) = m_{j+1},\ 1 \leq j < l,\ \sigma(m_l) = m_1.$$

   Für einen solchen Zyklus schreiben wir $\sigma = (m_1 m_2 \ldots m_l)$.
3. 2-Zyklen werden Transpositionen genannt.

Bemerkung. Sind $\sigma, \tau \in S_M$ mit $supp(\sigma) \cap supp(\tau) = \emptyset$, so gilt $\sigma \circ \tau = \tau \circ \sigma$.

Definition. Im Spezialfall $M = \{1, 2, \ldots, n\}$ schreibt man $S_n := S_M$. Ein Element $\sigma \in S_n$ schreibt man als

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

Beispiel 8. $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix} \in S_4$. σ ist der 3-Zyklus $(143) = (431) = (314)$.

Satz 13. *(a) Jede Permutation $\sigma \in S_n, \sigma \neq Id$, kann als Produkt von Zyklen mit disjunkten Trägern geschrieben werden. Diese Darstellung ist bis auf die Reihenfolge der Faktoren eindeutig bestimmt.*

(b) Für einen beliebigen l-Zyklus $(m_1 m_2 \ldots m_l) \in S_n$ und $\sigma \in S_n$ gilt

$$\sigma \circ (m_1 m_2 \ldots m_l) \circ \sigma^{-1} = (\sigma(m_1)\sigma(m_2) \ldots \sigma(m_l)).$$

(c) Die symmetrische Gruppe S_n wird von den Transpositionen erzeugt.

Beweis. (a) Es sei $\sigma \in S_n, \sigma \neq \text{id}$. Für $m_1, m_2 \in \{1, \ldots, n\} =: M$ definieren wir

$$m_1 \sim m_2 :\Leftrightarrow m_1 = \sigma^l(m_2) \qquad \text{für ein } l \in \mathbb{Z}.$$

Dann ist $\sim$ eine Äquivalenzrelation auf M. Es sei $M = K_1 \cup K_2 \cup \cdots \cup K_r$ die Zerlegung von M in disjunkte Äquivalenzklassen. Wir betrachten $a_j \in K_j$ beliebig. Es sei l_j die kleinste positive Zahl mit $\sigma^{l_j}(a_j) = a_j$. Das liefert uns

$$a_j, \sigma(a_j), \sigma^2(a_j), \ldots, \sigma^{l_j - 1}(a_j) \in K_j$$

und diese Elemente sind paarweise verschieden. Aus der Definition folgt, dass $\sigma \restriction_{K_j} = (a_j \sigma(a_j) \ldots \sigma^{l_j-1}(a_j)) \in S_{K_j}$ ein Zyklus der Länge l_j ist. Wenn wir dies für alle $j = 1, \ldots, r$ tun, erhalten wir:

$$\sigma = (a_1 \ldots \sigma^{l_1 - 1}(a_1))(a_2 \ldots \sigma^{l_2 - 1}(a_2)) \ldots (a_r \ldots \sigma^{l_1 - r}(a_r)).$$

Dies ist genau die gesuchte Darstellung, wenn man zudem $(a_j) := \mathrm{id}$ für $l_j = 1$ definiert.

Eindeutigkeit: Es sei für $s \in \mathbb{N}$ $\sigma = \tau_1\tau_2 \dots \tau_s$ eine andere Darstellung. Dann ist $\sigma \restriction_{supp(\tau_k)} = \tau_k$ für alle k ein Zyklus. Damit ist $supp(\tau_k) = K_j$ für ein $j = 1, \dots, r$ und somit ist τ_k gerade ein solcher Zyklus wie in unserer Konstruktion. Diese ist also eindeutig.

(b) Es sei $\sigma \in S_n$ und $(m_1 \dots m_k)$ ein Zyklus. Dann gilt

$$(\sigma(m_1 \dots m_k)\sigma^{-1})(\sigma(m_\alpha)) = (\sigma(m_1 \dots m_k))(m_\alpha) = \sigma(m_{\alpha+1}) \text{ mit } m_{k+1} := m_1.$$

Für $m \notin \{m_1, \dots, m_k\}$ gilt $(\sigma(m_1 \dots m_k)\sigma^{-1})(\sigma(m)) = (\sigma(m_1 \dots m_k))(m) = \sigma(m)$. Daraus folgt $\sigma \circ (m_1 m_2 \dots m_l) \circ \sigma^{-1} = (\sigma(m_1)\sigma(m_2) \dots \sigma(m_l))$.

(c) Wegen (a) genügt es zu zeigen, dass für alle $k \in \mathbb{N}$ alle k-Zyklen Produkte von Transpositionen sind. Für einen beliebigen Zyklus gilt

$$(m_1 \dots m_k) = (m_1 m_2)(m_2 m_3) \dots (m_{k-1} m_k).$$

Beispiel: $(1234) = (12)(23)(34)$. Graphisch veranschaulicht:

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

Anmerkung: Es reichen deutlich weniger Transpositionen aus, um S_n zu erzeugen. □

Definition. Für $\sigma \in S_n$ ist das Signum von σ definiert als

$$sgn(\sigma) := \prod_{i<j} \frac{\sigma(i) - \sigma(j)}{i - j} \qquad (\in \{\pm 1\}).$$

Permutationen $\sigma \in S_n$ mit $sgn(\sigma) = 1$ (bzw. -1) heißen gerade (bzw. ungerade) Permutationen.

Lemma 13. *Die Abbildung $sgn : S_n \to \{\pm 1\}$ ist ein Gruppenhomomorphismus.*

Beweis. Es seien $\sigma, \tau \in S_n$ beliebig. Dann gilt

$$
\begin{aligned}
sgn(\sigma\tau) &= \prod_{i<j} \frac{\sigma\tau(i) - \sigma\tau(j)}{i-j} = \prod_{i<j} \frac{\sigma\tau(i) - \sigma\tau(j)}{\tau(i) - \tau(j)} \cdot \prod_{i<j} \frac{\tau(i) - \tau(j)}{i-j} \\
&= \left(\prod_{\substack{i<j, \\ \tau(i)<\tau(j), \\ i':=\tau(i), j':=\tau(j)}} \frac{\sigma\tau(i) - \sigma\tau(j)}{\tau(i) - \tau(j)} \cdot \prod_{\substack{i<j, \\ \tau(j)<\tau(i), \\ i':=\tau(j), j':=\tau(i)}} \frac{\sigma\tau(i) - \sigma\tau(j)}{\tau(i) - \tau(j)} \right) \cdot sgn(\tau) \\
&= \prod_{i'<j'} \frac{\sigma(i') - \sigma(j')}{i' - j'} \cdot sgn(\tau) \\
&= sgn(\sigma) \cdot sgn(\tau).
\end{aligned}
$$

□