1 Gruppen

1.1 Grundlegende Definitionen

Definition 1.1.1
Sei M eine Menge.

(a) Eine **Verknüpfung** auf M ist eine Abbildung $\cdot : M \times M \to M$

(b) Eine Menge M zusammen mit einer Verknüpfung $\cdot$ heißt **Magma**.

(c) Eine Verknüpfung $\cdot : M \times M \to M$ heißt **assoziativ**, wenn

$$\forall x, y, z \in M : (x \cdot y) \cdot z = x \cdot (y \cdot z)$$

(d) Eine **Halbgruppe** ist ein assoziatives Magma.

(e) $e \in M$ heißt **neutrales Element** für die Verknüpfung $\cdot$, wenn

$$\forall x \in M : x \cdot e = e \cdot x = x$$

(f) Eine Halbgruppe mit neutralem Element heißt **Monoid**.

(g) Eine **Gruppe** ist ein Monoid $(G, \cdot)$, in dem es zu jedem $x \in G$ ein $x' \in G$ gibt mit

$$x \cdot x' = x' \cdot x = e$$

x' heißt dann **zu** x **inverses Element.**

Bemerkung 1.1.2
Sei $(M, \cdot)$ ein Magma.

(a) In M gibt es höchstens ein neutrales Element.

Beweis: Sind e, e' neutrale Elemente, so ist $e = e \cdot e' = e'$ ■

(b) Ist M Monoid, so gibt es zu $x \in M$ höchstens ein inverses Element.

Beweis: Seien x', x'' zu x invers, so ist $x' = (x'' \cdot x) \cdot x' = x'' \cdot (x \cdot x') = x''$ ■

Definition + Bemerkung 1.1.3

Sei $(M, \cdot)$ ein(e) $\left\{ \begin{array}{l} Magma \\ Halbgruppe \\ Monoid \\ Gruppe \end{array} \right\}$

(a) $U \subseteq M$ heißt Unter-$\left\{ \begin{array}{l} \vdots \end{array} \right\}$, wenn $U \cdot U \subseteq U$ und $(U, \cdot)$ selbst ein(e) $\left\{ \begin{array}{l} \vdots \end{array} \right\}$ ist.

(b) $U \subseteq M$ Unterhalbgruppe $\Leftrightarrow U \cdot U \subseteq U$

(c) $U \subseteq M$ Untermonoid $\Leftrightarrow U \cdot U \subseteq U$ und $e \in U$

(d) $U \subseteq M$ Untergruppe $\Leftrightarrow U \neq \emptyset$ und $\forall x, y \in U : x \cdot y^{-1} \in U$

Beweis: "$\Leftarrow$":
Sei $x \in U \Rightarrow e = x \cdot x^{-1} \in U \Rightarrow$ mit x ist auch x^{-1} in $U \Rightarrow$ mit x, y ist auch $xy = x(y^{-1})^{-1} \in U$ ■

Bemerkung 1.1.4

Sei $(M, \cdot)$ Monoid. Dann ist $M^x := \{x \in M : \text{es gibt inverses } x^{-1} \text{ zu } x \in M\}$ eine Gruppe.

Beweis:
$e \in M^x$, da $e \cdot e = e$, also $M^x \neq \emptyset$. Sind $x, y \in M^x$, so ist $x \cdot y \in M^x$, da $xy \cdot (y^{-1}x^{-1}) = e \Rightarrow \cdot$ ist Verknüpfung auf $M^x \Rightarrow (M^x, \cdot)$ ist Gruppe. ■

Definition + Bemerkung 1.1.5

Seien $(M, \cdot), (M', *)$ $\left\{ \begin{array}{l} \vdots \end{array} \right\}$

(a) Eine Abbildung $f : M \to M'$ heißt **Homomorphismus**, wenn $\forall\, x, y \in M$:

$$f(x \cdot y) = f(x) * f(y) \qquad \text{(i)}$$

Hat M ein neutrales Element, so muß außerdem gelten:

$$f(e) = e' \qquad \text{(ii)}$$

(b) Ist $f : G \to G'$ Abbildung von Gruppen, die (i) erfüllt, so ist f Homomorphismus.

Beweis: $f(e) = f(e \cdot e) = f(e) * f(e) \overset{\cdot f(e)^{-1}}{\Rightarrow} e' = f(e)$ ■

(c) Ein Homomorphismus $f : M \to M'$ heißt **Isomorphismus**, wenn es einen Homomorphismus $g : M' \to M$ gibt, mit $f \circ g = id_{M'}$ und $g \circ f = id_M$

(d) Jeder bijektive Homomorphismus ist Isomorphismus.

Beweis: Sei $f : M \to M'$ bijektiver Homomorphismus und $g : M' \to M$ die Umkehrabbildung. z.z.: g ist Homomorphismus.
Seien $x, y \in M'$. Schreibe $x = f(\hat{x}), y = f(\hat{y})$ für passende $\hat{x}, \hat{y} \in M \Rightarrow$
$g(x \cdot y) = g(f(\hat{x}) \cdot f(\hat{y})) = g(f(\hat{x} \cdot \hat{y})) = \hat{x} \cdot \hat{y} = g(f(\hat{x})) \cdot g(f(\hat{y})) = g(x) \cdot g(y)$
■

(e) Die Komposition von Homomorphismen ist wieder ein Homomorphismus.

Definition 1.1.6
Sei $f : M \to M'$ Hom von $\left\{ \begin{array}{l} \cdot \\ \cdot \end{array} \right\}$.

(a) Bild$(f) := \{f(x) : x \in M\} \subseteq M'$ ist ein Unter-$\left\{ \begin{array}{l} \cdot \\ \cdot \end{array} \right\}$.

Beweis: Sind $x, x' \in M$, so ist $f(x) * f(x') = f(x \cdot x') \in$ Bild(f). Sind M, M' Monoide, so gilt: $f(e) = e' \in$ Bild(f). Sind M, M' Gruppen, so gilt: $f(x)^{-1} = f(x^{-1}) \in$ Bild(f), da $f(x \cdot x^{-1}) = f(e) = e' = f(x) * f(x^{-1})$ ■

(b) Sind M, M' Monoide/Gruppen, so ist Kern$(f) := \{x \in M : f(x) = e'\}$ Untermonoid/-gruppe von M.

Beweis: $x, y \in$ Kern$(f) \Rightarrow f(xy) = f(x) * f(y) = e' * e' = e' \Rightarrow xy \in$ Kern$(f), e \in$ Kern(f) ✓
$x \in$ Kern$(f) \Rightarrow f(x^{-1}) = f(x)^{-1} = (e')^{-1} = e' \Rightarrow x^{-1} \in$ Kern(f) ■

(c) Sind G, G' Gruppen, so ist f genau dann injektiv, wenn Kern$(f) = \{e\}$

1.2 Beispiele und Konstruktionen

(1) Sei M eine Menge.
$M^M := \{f : M \to M$ Abbildung $\}$ ist mit der Verknüpfung $\cdot$ ein Monoid. $(M^M)^X = \{f : M \to M$ bijektiv $\} =: \text{Perm}(M) = S_M$.
insbesondere: $M = \{1, \ldots, n\} : S_{\{1,\ldots,n\}} = S_n$ Ist $(M, \cdot)$ ein $\left\{ \begin{array}{l} \cdot \\ \cdot \end{array} \right\}$, so ist $End(M) := \{f \in M^M : f$ Hom.$\}$ ein Untermonoid von M^M und
$Aut(M) :=$ Perm$(M) \cap$ End(M) Untergruppe von Perm(M)

(2a) Sei X Menge, M ein(e) $\left\{ \begin{array}{l} \cdot \\ \cdot \end{array} \right\}$. Dann ist $M^X = \{f : X \to M$ Abbildung $\}$ mit der Verknüpfung $(f \cdot g)(x) = f(x) \cdot g(x)$ ein(e) $\left\{ \begin{array}{l} \cdot \\ \cdot \end{array} \right\}$

(2b) Ist $(M, \cdot)$ Halbgruppe, $(H, +)$ kommutative Halbgruppe, so ist Hom$(M, H) := \{f \in H^M : f$ Homomorphismus$\}$ eine kommutative Unterhalbgruppe von H^M.
denn: Sind $f, g : M \to H$ Homomorphismen, so ist $\forall x, y \in M$:

$(f+g)(x\cdot y) = f(x\cdot y)+g(x\cdot y) = f(x)+f(y)+g(x)+g(y) = f(x)+g(x)+f(y)+g(y) = (f+g)(x)+(f+g)(y)$

(3) Sei I eine Indexmenge. Für jedes $i \in I$ sei $(M_i, \cdot)$ ein(e) $\left\{ \begin{array}{c} \cdot \\ \cdot \end{array} \right\}$.

a) $\prod_{i\in I} M_i$ ist mit komponentenweiser Verknüpfung ein(e) $\left\{ \begin{array}{c} \cdot \\ \cdot \end{array} \right\}$.

b) Sind M_i Monoide, so ist

$$\bigoplus_{i\in I} M_i := \{(x_i)_{i\in I} \in \prod_{i\in I} M_i, x_i = e_i \text{ ffa.} i\}$$

ein Monoid.

Definition + Bemerkung 1.2.1

(a) $\prod$ heißt **direktes Produkt**
$\bigoplus$ heißt **direkte Summe**

(b) Ist I endlich, so ist $\prod M_i \cong \bigoplus M_i$

(c) Sei M ein(e) $\left\{ \begin{array}{c} \cdot \\ \cdot \end{array} \right\}$ und für jedes $i \in I : g_i : M \to M_i$ ein Homomorphismus. Dann gibt es genau einen Homomorphismus $G : M \to \prod_{i\in I} M_i$, so dass $g_i = pr_i \circ G$, wobei $pr_i : \prod_{j\in I} M_j \to M_i$ Projektion.

Beweis: Setze $G(m) := (m_j)_{j\in I}$ mit $m_j = g_j(m)$ für $m \in M$. G ist Homomorphismus. ✓
G ist eindeutig, da $pr_i(G(m)) = g_i(m)$ sein muss. ■

(d) Ist $(M, +)$ ein kommutatives Monoid, und für jedes $i \in I$ $f_i : M_i \to M$ ein Homomorphismus, so gibt es genau einen Homomorphismus

$$F : \bigoplus_{j\in I} M_j \to M, \text{ so dass für jedes } i \in I : f_i = F \circ \nu_i, \text{ wobei } \nu_i : M_i \to \bigoplus_{j\in I} M_j$$

$$m \mapsto (m_j)_{j\in I}, \text{ wobei } m_j = \begin{cases} m & i = j \\ e_j & \text{sonst} \end{cases}$$

Beweis: Setze $F((m_j)_{j\in I}) = \sum_{j\in I} f_j(m_j)$

Brauche: $F((e,\dots,e,m_i,e,\dots,e)) = F(\nu_i(m_i)) \stackrel{!}{=} f_i(m_i)$
$\Rightarrow \quad F((e,\dots,e,m_i,e,\dots,e,m_j,e,\dots,e)) = f_i(m_i) + f_j(m_j) = F((e,\dots,e,m_i,e,\dots,e)) + F((e,\dots,e,m_j,e,\dots,e))$ ■

(4) Sei S eine Menge ("Alphabet") $F^a(S) := \bigcup_{n=1}^{\infty} S^n$ ist Halbgruppe mit Verknüpfung "Nebeneinanderschreiben" $(x_1, \ldots, x_n) \cdot (y_1, \ldots, y_m) := (x_1, \ldots, x_n, y_1, \ldots, y_m)$
$\in S^n \quad \in S^m \quad \in S^{n+m}$
$F^a(S)$ heißt freie Halbgruppe oder "Worthalbgruppe" über S.

Definiert man $S^0 := \{\varepsilon\}$, dann ist $F_0^a(S) := \bigcup_{n=0}^{\infty} S^n$ ein Monoid mit neutralem Element ε, dem „leeren Wort". Für $S = \{1\}$ ist $F_0^a(S) = (\mathbb{N}_0, +)$.

Bemerkung 1.2.2

Ist $(H, \cdot)$ Halbgruppe, $f : S \to H$ eine Abbildung, so gibt es genau einen Homomorphismus $\varphi : F^a(S) \to H$ mit $\varphi(s) = f(s)$ für alle $s \in S$, wobei man S als $S^1 \subset F^a(S)$ auffasst.

Beweis: Für $(x_1, \ldots, x_n) \in S^n$ muss gelten: $\varphi(x_1, \ldots, x_n) = \varphi(x_1) \cdot \cdots \cdot \varphi(x_n) = f(x_1) \cdot \cdots \cdot f(x_n)$. Also ist φ eindeutig und existiert, da es so definiert werden kann. ■

Bemerkung + Definition 1.2.3

Sei $(M, \cdot)$ ein Monoid und $(G, \cdot)$ eine Gruppe

(a) Für $x \in M$ ist $\varphi_x : \mathbb{N}_0 \to M$, $n \mapsto x^n$ ein Homomorphismus.

(b) Für $g \in G$, so ist $\varphi_g : \mathbb{Z} \to G$, $n \mapsto g^n$ ein Gruppenhomomorphismus.

(c) $\langle g \rangle := \text{Bild}(\varphi_g)$ heißt die von g erzeugte **zyklische Untergruppe** von G.

(d) G heißt zyklisch, wenn es ein $g \in G$ gibt mit $\langle g \rangle = G$.

(e) $|\langle g \rangle| \in \mathbb{N} \cup \{\infty\}$ heißt **Ordnung** von g

(f) Ist G endlich, so heißt $|G|$ die **Ordnung** von G.

Definition + Bemerkung 1.2.4 (Satz von Cayley)

(a) Für $g \in G$ heißt die Abbildung $\tau_g : G \to G$, $h \mapsto gh$ die *Linksmultiplikation* mit g.

(b) Für jedes $g \in G$ ist τ_g bijektiv, da $\tau_{g^{-1}}$ die Umkehrabbildung ist.

(c) Die Abbildung:

$$\begin{aligned} \tau \quad : \quad & G \to \text{Perm}(G) \\ & g \mapsto \tau_g \end{aligned}$$

ist ein injektiver Gruppenhomomorphismus.

Beweis:

(1) $\tau_g \in \text{Perm}(G) : \tau_g$ ist bijektiv mit Umkehrabbildung $\tau_{g^{-1}}$

(2) τ ist Homomorphismus: $\tau(g_1g_2) = \tau(g_1) \circ \tau(g_2)$, denn: $\forall x \in G : \tau(g_1 \circ g_2)(x) = (g_1g_2)x = g_1(g_2x) = \tau_{g_1}(\tau_{g_2}(x)) = (\tau_{g_1} \circ \tau_{g_2})(x)$

(3) $\text{Kern}(\tau) = \{e\}$, denn ist $\tau(g) = id_g$, so ist $\forall x \in G : \tau_g(x) = gx = x$, also $g = e$ ■

Definition + Bemerkung 1.2.5

Sei G Gruppe, $g \in G$

(a) Die Abbildung $c_g : G \to G, x \mapsto gxg^{-1}$ ist ein **Automorphismus**, sie heißt **Konjugation** mit g.

Beweis: c_g ist Homomorphismus: $c_g(x_1x_2) = g(x_1x_2)g^{-1}$
$c_g(x_1)c_g(x_2) = (gx_1g^{-1})(gx_2g^{-1}) = c_g(x_1) \cdot c_g(x_2)$
c_g ist bijektiv: Die Umkehrabbildung ist $c_{g^{-1}}$ ■

(b) Die Abbildung $c : G \to \text{Aut}(G), g \mapsto c_g$ ist ein Gruppenhomomorphismus.

Beweis: $\forall x \in G : c(g_1g_2)(x) = (g_1g_2)x(g_1g_2)^{-1} = g_1(g_2xg_2^{-1})g_1^{-1} = (c(g_1) \circ c(g_2))(x)$ ■

(c) Die Elemente von $\text{Bild}(c) =: \text{Aut}_i(G)$ heißen **innere Automorphismen** von G.

(d) $Z(G) := \text{Kern}(c)$ heißt **Zentrum** von G. Es ist $Z(G) = \{g \in G : \forall x \in G : gx = xg\}$

(e) Eine Untergruppe $N \subseteq G$ heißt **Normalteiler** in G, wenn $\forall g \in G : c_g(N) \subseteq N$. Äquivalent: $\forall g \in G, x \in N : gxg^{-1} \in N$

(f) Ist $f : G \to G'$ Gruppenhomomorphismus, so ist $\text{Kern}(f)$ Normalteiler in G.

Beweis: Sei $x \in \text{Kern}(f), g \in G$. Dann ist $f(gxg^{-1}) = f(g)\underbrace{f(x)}_{e'}f(g)^{-1} = e'$.
■

(g) $\text{Aut}_i(G)$ ist Normalteiler in $\text{Aut}(G)$

Beweis: Sei $\varphi \in \text{Aut}(G), g \in G$: z.z.: $\varphi \cdot c_g \cdot \varphi^{-1} \in \text{Aut}_i(g)$.
Es ist $(\varphi \cdot c_g \cdot \varphi^{-1})(x) = \varphi(c_g(\varphi^{-1}(x))) = \varphi(g \cdot \varphi^{-1}(x) \cdot g^{-1}) = \varphi(g) \cdot \varphi(\varphi^{-1}(x)) \cdot \varphi(g^{-1}) = \varphi(g) \cdot x \cdot \varphi(g)^{-1} = c_{\varphi(g)}(x) \Rightarrow \varphi \circ c_g \circ \varphi^{-1} = c_{\varphi(g)} \in \text{Aut}_i(G)$ ■

Definition + Bemerkung 1.2.6

Sei G Gruppe, $H \subseteq G$ Untergruppe.

(a) Für $g \in G$ heißt $g \cdot H = \{g \cdot h : h \in H\} = \tau_g(H)$ **Linksnebenklasse** von G bzgl. H und $H \cdot g = \{h \cdot g : h \in H\}$ **Rechtsnebenklasse**

(b) Für $g_1, g_2 \in G$ gilt: $g_1H \cap g_2H \neq \emptyset \Leftrightarrow g_1H = g_2H$

Beweis: Sei $y = g_1h_1 = g_2h_2 \in g_1H \cap g_2H$ und $h1, h2, h \in H \Rightarrow g_1 = g_2h_2h_1^{-1} \Rightarrow g_1h = g_2h_2h_1^{-1} \in g_2H \Rightarrow g_1H \subseteq g_2H$, die Umkehrung folgt analog. ■

(c) H ist genau dann Normalteiler, wenn $\forall g \in G : g \cdot H = H \cdot g$

Beweis: $gH = Hg \Leftrightarrow H = gHg^{-1}$ ■

(d) Alle Nebenklassen von G bzgl. H sind gleichmächtig.

Beweis: $\tau_g : \underbrace{H}_{e \cdot H} \to g \cdot H, h \mapsto g \cdot h$ ist bijektiv. ■

(e) Die Anzahl der Linksnebenklassen bzgl. H ist gleich der Anzahl der Rechtsnebenklassen. Sie heißt **Index** $[G : H]$ von H in G.

Beweis: Die Zuordnung

$$\begin{array}{lcl} \{\text{Linksnebenklasse}\} & \to & \{\text{Rechtsnebenklasse}\} \\ g \cdot H & \mapsto & H \cdot g^{-1} \end{array}$$

ist **wohldefiniert** und bijektiv.

Wohldefiniertheit: ist $g_1H = g_2H$, also $g_2 = g_1h$ für ein $h \in H \Rightarrow Hg_2^{-1} = H(g_1h)^{-1} = H \cdot h^{-1}g_1^{-1} = Hg_1^{-1}$ ■

(f) **Satz von Lagrange:** Ist G endlich, so ist

$$[G : H] = \frac{|G|}{|H|}$$

Beweis: G ist disjunkte Vereinigung der $[G : H]$ Linksnebenklassen bzgl. H. Diese haben alle $|H|$ Elemente. ■

1.3 Quotientenbildung

Definition + Bemerkung 1.3.1
Sei $f : M \to M'$ eine Abbildung von Mengen.

(a) Die Relation $\sim_f$ auf $M : x \sim_f y \Leftrightarrow f(x) = f(y)$ ist eine Äquivalenzrelation.

(b) Für $x \in M$ sei $\bar{x} := [x]_f := \{y \in M : y \sim_f x\} = \{y \in M : f(y) = f(x)\}$. Es ist $\bar{x} = f^{-1}(f(x))$

Weiter sei $\bar{M} := M/\sim_f := \{\bar{x} : x \in M\}$

(c) $\bar{f} : \bar{M} \to \text{Bild}(f)$, $\bar{x} \mapsto f(x)$ ist eine bijektive Abbildung.

Definition 1.3.2
Ist $(M, \cdot)$ und $(M', *)$ ein $\left\{ \begin{array}{c} \cdot \\ \cdot \end{array} \right\}$, und $(M, \cdot) \to (M', *)$ ein Homomorphismus, so wird durch $\bar{x} \cdot \bar{y} := \overline{x \cdot y}$ eine Verknüpfung auf $\bar{M}$ definiert. So wird $(\bar{M}, \cdot)$ auch zu einem $\left\{ \begin{array}{c} \cdot \\ \cdot \end{array} \right\}$.

Beweis: z.z.: $\cdot$ ist wohldefiniert. Seien also $x' \in \bar{x}, y' \in \bar{y}$ zu zeigen: $\overline{x' \cdot y'} = \overline{x \cdot y}$ dh. $f(x' \cdot y') = f(x \cdot y)$ dh. $f(x') = f(x), f(y') = f(y)$ Es ist $f(x' \cdot y') = f(x') * f(y') = f(x) * f(y) = f(x \cdot y)$ ■

Definition + Bemerkung 1.3.3
Sei $f : G \to G'$ Gruppenhomomorphismus.

(a) $\bar{G} = G/\sim_f$ ist die Menge der Linksnebenklassen bzgl. $\text{Kern}(f)$ also ist für jedes $g \in G$: $[g]_f = g \cdot \text{Kern}(f) = \text{Kern}(f) \cdot g$.

(b) $\bar{G} = G/\text{Kern}(f)$ heißt **Faktorgruppe** von G bzgl. $\text{Kern}(f)$.

Beweis: Seien $x, y \in G$. Dann gilt: $\bar{x} = \bar{y} \Leftrightarrow f(x) = f(y) \Leftrightarrow f(x) \cdot f(y^{-1}) = e' \Leftrightarrow xy^{-1} \in \text{Kern}(f) \Leftrightarrow y = (xy^{-1})^{-1}x \in \text{Kern}(f) \cdot x \Leftrightarrow x^{-1}y \in \text{Kern}(f) \Leftrightarrow y = x(x^{-1}y) \in x \cdot \text{Kern}(f) \Leftrightarrow y \cdot \text{Kern}(f) = x \cdot \text{Kern}(f)$ ■

Beispiel: $\exp : (\mathbb{R}, +) \to (\mathbb{C}^\times, \cdot)$, $t \mapsto e^{2\pi i t}$ ist ein Gruppenhomomorphismus. Es ist $\exp(t_1) = \exp(t_2) \iff 1 = e^{2\pi i(t_2 - t_1)} \iff t_2 - t_1 \in \mathbb{Z}$, also ist $\text{Kern}(\exp) = \mathbb{Z}$.

Die Abbildung $[0, 1) \to \mathbb{R}/\mathbb{Z}$, $t \mapsto [t]_f$ ist bijektiv, spiegelt aber die Eigenschaften dieser Gruppe nicht wieder. Besser geeignet ist die Bijektion $\mathbb{R}/\mathbb{Z}$, $\bar{t} \mapsto e^{2\pi i t}$.

Bemerkung 1.3.4
Sei G Gruppe. Es ist $N \subseteq G$ Normalteiler, genau dann, wenn es eine Gruppe G' mit einem surjektivem Gruppenhomomorphismus $f : G \to G'$ und $N = \text{Kern}(f)$ gibt.

Beweis: Die Richtung $\Longleftarrow$ folgt aus 1.2.5 f). Sei $G' := \{x \cdot N, x \in G\}$ $(\subseteq \mathcal{P}(G))$
Für $x, y \in G$ setze $(x \cdot N)(y \cdot N) = (xy \cdot N)$
Behauptung: $(G', \cdot)$ ist Gruppe, **denn:**

(i) Die Verknüpfung ist wohldefiniert: Seien $x, x', y, y' \in G$ mit $x \cdot N = x' \cdot N,\ y \cdot N = y' \cdot N$. Dann gibt es $n, m \in N$ mit $x' = xn, y' = ym \Rightarrow x', y' = x(ny)m$. Da N Normalteiler ist, gibt es $n' \in N$ mit $ny = yn' \Rightarrow x'y' = xyn'm \Rightarrow x'y' \cdot N = xy \cdot N$

(ii) alle übrigen Eigenschaften "vererben" sich von G auf G'
$f : G \to G',\ x \mapsto x \cdot N$ ist surjektiver Gruppenhomomorphismus mit Kern(f) = N
■

Definition + Bemerkung 1.3.5

Sei G Gruppe, $N \subset G$ Normalteiler. Die Gruppe G' aus dem vorherigen Beweis heißt Faktorgruppe von G nach N, und wir schrieben $G' = G/N$ („G modulo N"). Sie ist gleich der Faktorgruppe $G/\operatorname{Kern}(f)$ für das f aus der vorherigen Bemerkung (ii).

Satz 1

(a) Sei $f : M \to M'$ eine Abbildung. $\bar{M} := M/\sim_f$ und $p : M \to \bar{M}, x \mapsto \bar{x}$ die Restklassenabbildung. Dann exisitiert genau eine Abbildung $\bar{f} : \bar{M} \to M'$ mit $f = \bar{f} \circ p$. Es ist p surjektiv und $\bar{f}$ injektiv.

(b) Ist $f : M \to M'$ ein Homomorphismus von $\left\{ \begin{array}{l} \cdot \\ \cdot \end{array} \right\}$, so ist $\bar{M}$ auch ein $\left\{ \begin{array}{l} \cdot \\ \cdot \end{array} \right\}$ und p, $\bar{f}$ sind Homomorphismen.

(c) **Homomorphiesatz**
Ist $f : G \to G'$ ein Gruppenhomomorphismus, so ist $G/\operatorname{Kern}(f) \cong \operatorname{Bild}(f)$

(d) **Universelle Abbildungseigenschaft (UAE) der Faktorgruppe**
Sei G Gruppe, $N \subseteq G$ Normalteiler. Dann gibt es zu jedem Gruppenhomomorphismus $f : G \to G'$ mit $N \subseteq \operatorname{Kern}(f)$ genau einen Gruppenhomomorphismus $f_N : G/N \to G'$ mit $f = f_N \circ p_N$, wobei p_N die Restklassenabbildung ist.

Beweis:

(a) $\bar{f}(\bar{x}) = f(x)$, wie in 1.3.1 c)

(c) $\bar{f} : G/\operatorname{Kern}(f) \to \operatorname{Bild}(f)$ ist injektiv, ein Gruppenhomomorphismus nach a), b) und 1.3.3. Also ist $\bar{f}$ ein bijektiver Homomorphismus, also eine Isomorphie.

(d) Setze $f_N(x \cdot N) := f(x)$
f_N ist wohldefiniert: Ist $gN = g'N$, so ist $(g')^{-1}g \in N \subseteq \text{Kern}(f)$, also $f((g')^{-1}g) = e' \implies f(g') = f(g)$. Die Eindeutigkeit von $\bar{f}$, sowie dass $\bar{f}$ ein Homomorphismus ist, ist klar. ■

1.4 Abelsche Gruppen

Bemerkung 1.4.1 (a) Jede zyklische Gruppe ist isomorph zu $\mathbb{Z}$ oder zu $\mathbb{Z}/n\mathbb{Z}$ für genau ein $n \in \mathbb{N} \setminus \{0\}$.

Beweis: Sei $G = \langle g \rangle$, $\varphi_g : \mathbb{Z} \to G,\ n \mapsto g^n$ (siehe 1.2.3)
φ_g ist surjektiver Gruppenhomomorphismus.
Nach Satz 1 ist $G \cong \mathbb{Z}/\text{Kern}(\varphi_g)$
Da jede Untergruppe von $\mathbb{Z}$ von der Form $H = n\mathbb{Z}$ für ein $n \in \mathbb{N}$ ist, folgt die Behauptung. ■

(b) Jede Untergruppe einer zyklischen Gruppe ist zyklisch.

Beweis: Sei $G = \langle g \rangle$ zyklisch, $H \subseteq G$ Untergruppe. Ist $H = \{e\}$, so ist $H = \langle e \rangle$ zyklisch. Anderenfalls sei $n := \min\{k \in \mathbb{N} \setminus \{0\} : g^k \in H\}$.

Behauptung: $\langle g^n \rangle = H$, denn sonst gibt es ein $m > 0$ mit $g^m \in H \setminus \langle g^n \rangle$. Sei m minimal mit dieser Eigenschaft. Dann ist $0 < m - n < m$. Aber: $g^{m-n} = g^m g^{-n} \in H \implies g^{m-n} \in \langle g^n \rangle \implies g^m = g^{m-n} g^n \in \langle g^n \rangle$ Wid! ■

Definition + Bemerkung 1.4.2

(a) Die Abbildung $\varphi : \mathbb{N} \setminus \{0\} \to \mathbb{N},\ n \mapsto \varphi(n) := |\{k \in \{1, \ldots, n\} : \text{ggT}(k, n) = 1\}|$ heißt **Eulersche φ -Funktion**.

(b) $\varphi(1) = 1 = \varphi(2)$, $\varphi(p) = p - 1$ für p Primzahl, $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$, falls m, n teilerfremd, $\varphi(p^k) = p^{k-1}(p - 1)$, für p Primzahl.

(c) Für jedes $n \in \mathbb{N} \setminus \{0\}$ gilt: $n = \sum_{d|n} \varphi(d)$

Beweis: $n = |G| = \sum_{d|n} |\{x \in G, \text{ord}(x) = d\}| \overset{(d)}{=} \sum_{d|n} \varphi(d)$ ■

(d) Ist G zyklische Gruppe der Ordnung n, so gilt für jeden Teiler d von n: $|\{x \in G : \text{ord}(x) = d\}| = \varphi(d)$

Beweis: Sei $G = \langle g \rangle$. Für $x = g^k \in G$ ist $\text{ord}(x) = \frac{n}{\text{ggT}(k,n)}$. Also ist $\text{ord}(x) = d \Leftrightarrow \text{ggT}(k,n) = \frac{n}{d} \implies |\{g \in G \mid \text{ord}(g) = d\}| = |\{l \in \{1,\dots,n\} \mid \text{ggT}(l,d) = 1\}| = \varphi(d)$. ■

Beispiel:

(1)
$$\{e^{\frac{2\pi i k}{n}} : n \in \mathbb{N} \setminus \{0\}, 0 \le k < n\}$$
ist zyklische Untergruppe von $\mathbb{C}^*$ der Ordnung n. (n-te Einheitswurzel)

(2) Sei $V = \{id, \tau, \sigma_1, \sigma_2\}$ mit τ = Drehung im $\mathbb{R}^2$ $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$,
σ_1 = Spiegelung an der x-Achse $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$,
σ_2 = Spiegelung an der y-Achse $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$. V ist abelsche Gruppe, aber **nicht** zyklisch. V heißt **Kleinsche Vierergruppe** $V \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$

(3)
$$\begin{array}{ccccc} \mathbb{Z}/6\mathbb{Z} & \cong & \mathbb{Z}/2\mathbb{Z} & \oplus & \mathbb{Z}/3\mathbb{Z} \\ \{1, a, a^2, a^3, a^4, a^5\} & & \{1, \sigma\} & & \{1, \tau, \tau^2\} \\ a & \mapsto & (\sigma, \tau) & & \end{array}$$

Definition + Bemerkung 1.4.3

Sei G Gruppe, $A \subseteq G$ Teilmenge.

(a) $\langle A \rangle := \bigcap_{\substack{H \subseteq G \text{ Ugr.} \\ A \subseteq H}} H$ heißt die **von A erzeugte Untergruppe von G**.

Beweis: z.z.: $\langle A \rangle = \bigcap_{\substack{H \subseteq G \text{ Ugr.} \\ A \subseteq H}} H$ ist Untergruppe in G.

(i) $\forall H \subseteq G$, H Untergruppe: $e \in H \Rightarrow e \in \langle A \rangle \Rightarrow \langle A \rangle \neq \emptyset$

(ii) Seien $x, y \in \langle A \rangle$, H Untergruppe von G mit $A \subseteq H \Rightarrow x, y \in H \overset{H \text{ Ugr.}}{\Rightarrow} xy^{-1} \in H \Rightarrow xy^{-1} \in \langle A \rangle$. $\Rightarrow \langle A \rangle$ Untergruppe von G.

■

(b) $\langle A\rangle = \{g_1^{\varepsilon_1}\cdots g_n^{\varepsilon_n}, n\in\mathbb{N}, g_i\in A, \varepsilon_i\in\{\pm 1\}\}$

Definition + Proposition 1.4.4
Sei $(A,+)$ eine abelsche Gruppe, $X\subseteq A$.

(a) A heißt **freie abelsche Gruppe** mit Basis X, wenn gilt: $A=\langle X\rangle$ und für alle paarweisen verschiedenen Elemente $x_1,\dots,x_n\in X$ ist $\sum_{i=1}^n n_i x_i = 0$, $n_i\in\mathbb{Z}$, nur dann möglich ist, wenn alle $n_i = 0$ sind.
Jedes $a\in A$ hat dann eine eindeutige Darstellung $a=\sum_{x\in X} n_x x$ mit $n_x\in\mathbb{Z}$, $n_x\neq 0$ nur für endlich viele $x\in X$.

Beweis: $A\to\mathbb{Z}^X : \sum n_x x\mapsto (n_x)_{x\in X}$ ist Isomorphismus. ■

(b) $\mathbb{Z}$ ist frei mit Basis $\{1\}$.

(c) A ist frei mit Basis X genau dann, wenn $A\cong\bigoplus_{x\in X}\mathbb{Z}$.

(d) Ist A frei mit Basis X, und X endlich, so heißt $|X|$ der Rang von A.

(e) (UAE der freien abelschen Gruppe)
Ist A frei mit Basis X, dann gibt es zu jeder abelschen Gruppe A' und jeder Abbildung $f: X\to A'$ genau einen Homomorphismus $\varphi: A\to A'$ mit $\forall x\in X: \varphi(x)=f(x)$

Beweis: Setze $\varphi(\sum_{x\in X} n_x x) := \sum_{x\in X} n_x f(x)$ ■

Beispiel: (wichtig!) X endlich, $X=\{x_1,\dots,x_n\}$. Dann ist $\mathbb{Z}^X\cong\mathbb{Z}^n$
$\mathbb{Z}^n$ ist "so etwas ähnliches" wie ein Vektorraum *("freier Modul")*. Insbesondere lassen sich die Gruppenhomomorphismen $\mathbb{Z}^n\to\mathbb{Z}^m$ durch eine $m\times n$-Matrix mit Einträgen in $\mathbb{Z}$ beschreiben.

Beispiel: Ist $(\mathbb{Q},+)$ frei? $(\mathbb{Q},+)$ ist nicht frei von Rang 1, sonst wäre $\mathbb{Q}=r\mathbb{Z}$ für ein $r\in\mathbb{Q}$.

Sei also $(\mathbb{Q},+)$ frei mit Basis X und $x_1\neq x_2\in X$. Es gilt $x_i=\frac{n_i}{m_i}$, $n_i,m_i\in\mathbb{Z}$. Dann ist $n_2m_1x_1 - n_1m_2x_2 = 0$, also sind x_1,x_2 linear abhängig.

Satz 2 (Elementarteilersatz)
Jede Untergruppe einer freien abelschen Gruppe von endlichem Rang n ist frei mit Rang $r\leq n$. Genauer:

Sei H eine Untergruppe von $\mathbb{Z}^n$ ($n\in\mathbb{N}\setminus\{0\}$). Dann gibt es eine Basis $\{x_1,\dots,x_n\}$ von $\mathbb{Z}^n$, ein $r\in\mathbb{N}$ mit $0\leq r\leq n$ und $a_1,\dots,a_r\in\mathbb{N}\setminus\{0\}$ mit a_i teilt a_{i+1} für $i=1,\dots,r-1$, so dass $a_1x_1,\dots,a_rx_r$ eine Basis von H ist. Die a_i sind eindeutig bestimmt.

Beweis: 1. Schritt: H ist endlich erzeugt: Induktion über n:
$n = 1 : \checkmark$
$n > 1$: Sei $e_1, \ldots, e_n$ Basis von $\mathbb{Z}^n$, $\pi : \mathbb{Z}^n \to \mathbb{Z}$, $\sum_{i=1}^{n} a_i e_i \mapsto a_n$
(Projektion auf letze Komponente).

1. Fall: $\pi(H) = \{0\} \Rightarrow H \subseteq \mathbb{Z}^{n-1}$, also endlich erzeugt nach **IV**.
2. Fall: $\pi(H) = l\mathbb{Z}$ für ein $l \in \mathbb{N} \setminus \{0\}$ Sei $y \in H$ mit $\pi(y) = l$
Beh.: $H \cong \langle y \rangle \oplus (H \cap \mathrm{Kern}(\pi))$ Dann folgt die Behauptung von Schritt 1, da $\mathrm{Kern}(\pi) \cong \mathbb{Z}^{n-1}$, $H \cap \mathrm{Kern}(\pi)$ Untergruppe von $\mathbb{Z}^{n-1}$, existiert also nach **IV** $\Rightarrow$
Bew. der Beh..: $\langle y \rangle \cap (H \cap \mathrm{Kern}(\pi)) = \{0\}$ nach Definition von $y \Rightarrow$ Summe direkt.
Sei $z \in H$ mit $\pi(z) = k \cdot l$ für ein $k \in \mathbb{Z} \Rightarrow z - ky \in H \cap \mathrm{Kern}(\pi) \Rightarrow$ Beh.

2. Schritt: Sei $y_1, \ldots, y_r$ Erzeugendensystem von H. Nach Schritt 1 kann $r \leq n$ erreicht werden. Schreibe $y_j = \sum_{i=1}^{n} a_{ij} e_i$. Dann ist $A := (a_{ij}) \in \mathbb{Z}^{n \times r}$ eine Darstellungsmatrix der Einbettung $H \hookrightarrow \mathbb{Z}^n$ bzgl. der Basen $\{y_1, \ldots, y_r\}$ von H und $\{e_1, \ldots, e_n\}$ von $\mathbb{Z}^n$. Zeilen- und Spaltenumformungen entsprechen Basiswechseln in H bzw. $\mathbb{Z}^n$.
Vorsicht: Dabei dürfen nur **ganzzahlige** Basiswechselmatrizen benutzt werden, deren inverse Matrix ebenfalls ganzzahlige Einträge hat!
Ziel: Bringe A durch elementare Zeilen- und Spaltenumformungen auf Diagonalgestalt:
$\widetilde{A} = \begin{pmatrix} a_1 & & 0 \\ & \ddots & \\ 0 & & a_r \end{pmatrix}$ mit $a_i \in \mathbb{Z}$ und a_i teilt a_{i+1} $\forall\, i = 1, \ldots, r-1$

3. Schritt: Das geht! Ganzzahliger Gauß-Algorithmus, „Elementarteileralgorithmus“.

(i) Suche den betragsmäßig kleinsten Matrixeintrag $\neq 0$ und bringe diesen nach a_{11}. Dazu braucht man höchstens eine Zeilen- und eine Spaltenumformung.

(ii) Stelle fest, ob alle a_{i1} $(i = 2, \ldots, n)$ durch a_{11} teilbar sind. Falls nicht, teile a_{i1} mit Rest durch a_{11} : $a_{i1} = q a_{11} + r$ mit $0 < r < |a_{11}|$. Ziehe dann von der i-ten Zeile das q-fache der ersten ab. Die neue i-te Zeile beginnt nun mit $\widetilde{a_{i1}} = r \Rightarrow$ Zurück zu (i)

(iii) Sind schließlich alle a_{i1} durch a_{11} teilbar, so wird die erste Spalte zu

$$\begin{pmatrix} a_{11} \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

gemacht, indem man von der i-ten Zeile das $\frac{a_{i1}}{a_{11}}$-fache der ersten Zeile abzieht.

Gegebenenfalls zurück zu (i).

(iv) Genauso wird die erste Zeile zu $(a_{11}, 0, \ldots, 0)$

(v) Gibt es jetzt noch einen Matrixeintrag, der nicht durch a_{11} teilbar ist, schreibe $a_{ij} = qa_{11} + r$ mit $0 < r < |a_{11}|$ Ziehe von der i-ten Zeile das q-fache der ersten ab. Die neue i-te Zeile lautet dann:

$$(-qa_{11}, a_{i2}, \ldots, a_{ij}, \ldots, a_{ir})$$

(da $a_{i1} = 0, a_{1k} = 0$ für $1 < k \leq r$)
Addiert man zur j-ten Spalte die erste, so ist das neue Element $\widetilde{a_{ij}} = a_{ij} - qa_{11} = r \Rightarrow$ Zurück zu (i)

(vi) Nach endlich vielen Schritten erhalte Matrix

$$\begin{pmatrix} a_{11} & 0 & \ldots & 0 \\ 0 & & & \\ \vdots & & A' & \\ 0 & & & \end{pmatrix},$$

in der alle Einträge von A' durch a_{11} teilbar sind. Wende nun den Algorithmus auf A' an.

Noch zu zeigen: Die Eindeutigkeit der a_i:

r ist eindeutig, da r der Rang von H ist.

Ist $x_1, \ldots, x_n$ Basis von $\mathbb{Z}^n$, und $a_1x_1, \ldots, a_rx_r$ eine Basis von H wie im Satz, so ist $H \subseteq \mathbb{Z}^r$ und $\mathbb{Z}^r/H \cong \bigoplus_{i=1}^r \mathbb{Z}/a_i\mathbb{Z}$, denn $\varphi : \mathbb{Z}^r \to \oplus_{i=1}^r \mathbb{Z}/a_i\mathbb{Z}$, $x_i \mapsto e_i := (0, \ldots, s_i, \ldots, 0)$, ($s_i$ Erzeuger von $\mathbb{Z}/a_i\mathbb{Z}$) ist ein surjektiver Homomorphismus.

$\text{Kern}(\varphi) \supseteq \langle\{a_1x_1, \ldots, a_rx_r\}\rangle = H$, sowie $\text{Kern}(\varphi) \subseteq H$, denn für $y \in \text{Kern}(\varphi)$, $y = \sum_{i=1}^r b_ix_i$ gilt: $\varphi(y) = \sum_{i=1}^r b_ie_i = (b_1s_1, \ldots, b_rs_r) = (0, \ldots, 0)$, also gilt $a_i \mid b_i$, $i = 1, \ldots, r$, also $y \in H$. Nach dem Homomorphiesatz gilt also: $\mathbb{Z}^r/H \cong \bigoplus_{i=1}^r \mathbb{Z}/a_i\mathbb{Z}$.

Zu zeigen ist nun: Für $T := \bigoplus_{i=1}^r \mathbb{Z}/a_i\mathbb{Z} \cong \bigoplus_{i=1}^s \mathbb{Z}/b_i\mathbb{Z} =: \tilde{T}$ mit $a_i \mid a_{i+1}$, $i = 1, \ldots, r-1$ und $b_i \mid b_{i+1}$, $i = 1, \ldots, s-1$ gilt: $r = s$ und $a_i = b_i$, $i = 1, \ldots, r$.

Für $z \in T$ gilt: $ord(z) \mid a_r$, denn mit $z = (z_1, \ldots, z_n)$, $z_i \in \mathbb{Z}/a_i\mathbb{Z}$ gilt $a_r \cdot z = (a_rz_1, \ldots, a_rz_r) = (0, \ldots, 0)$. Genauso: $ord(z) \mid b_s$. T enhält das Element $(0, \ldots, 0, s_r) = e_r$ und $ord(e_r) = a_r$, also gilt $a_r \mid b_s$ und $b_s \mid a_r$, also $a_r = b_s$. Die Behauptung folgt dann per Induktion über r ∎

Ergänzung:

(1) In der Situation von Satz 2 heißen die a_{ii} $i = 1, \ldots, r$ die **Elementarteiler** von H.

(2) Ist $A = (h_1, \ldots, h_r) \in \mathbb{Z}^{n \times r}$, so erzeugen die Spalten $h_1, \ldots, h_r$ eine Untergruppe von $\mathbb{Z}^n$. A ist Darstellungsmatrix der Einbettung $H \hookrightarrow \mathbb{Z}^n$.
Die Elementarteiler von H heißen auch Elementarteiler von A.

Folgerung 1.4.5 (Struktursatz für endlich erzeugte abelsche Gruppen)
Jede endlich erzeugte abelsche Gruppe A ist die direkte Summe von zyklischen Gruppen:

$$A \cong \mathbb{Z}^r \oplus \bigoplus_{i=1}^{m} \mathbb{Z}/a_i\mathbb{Z}$$

mit $r, m, a_1, \ldots, a_m \in \mathbb{N}$, $\forall i : a_i \geq 2$, a_i teilt a_{i+1} für $i = 1, \ldots, m-1$. Dabei sind r, m und die a_i eindeutig bestimmt.

Beweis: Sei $x_1, \ldots, x_n$ ein Erzeugendensystem von A.
Nach 1.4.4 gibt es einen surjektiven Gruppenhomomorphismus $\varphi : \mathbb{Z}^n \to A$ mit $\varphi(e_i) = x_i$, für $i = 1, \ldots, n$.
Nach Homomorphiesatz (Satz 1) ist dann $A \cong \mathbb{Z}^n/\mathrm{Kern}(\varphi)$.
Nach Satz 2 gibt es $m \in \mathbb{N}, m \leq n$, eine Basis $\{z_1, \ldots, z_n\}$ von $\mathbb{Z}^n$ und Elementarteiler $a_1, \ldots, a_m$ mit a_i teilt a_{i+1} für $i = 1, \ldots, m-1$, so dass $\{a_1 z_1, \ldots, a_m z_m\}$ Basis von $\mathrm{Kern}(\varphi)$ ist. Dann ist $A \cong \mathbb{Z}^n/\mathrm{Kern}(\varphi) \cong \left(\bigoplus_{i=1}^{n} z_i\mathbb{Z}\right) / \left(\bigoplus_{i=1}^{m} a_i z_i \mathbb{Z}\right) \cong \bigoplus_{i=1}^{m} (z_i\mathbb{Z}/a_i z_i\mathbb{Z}) \oplus \bigoplus_{i=m+1}^{n} z_i\mathbb{Z} \cong \bigoplus_{i=1}^{m} \mathbb{Z}/a_i\mathbb{Z} \oplus \mathbb{Z}^{n-m}$

Ist $a_1 = 1$, so lassen wir die $\mathbb{Z}/1\mathbb{Z} = \{e\}$ weg.

■

1.5 Freie Gruppen

Definition + Bemerkung 1.5.1

Sei F eine Gruppe und $X \subseteq F$

(a) F heißt **freie Gruppe mit Basis X**, wenn jedes $y \in F$ eine eindeutige Darstellung $y = x_1^{\varepsilon_1} \cdot \ldots \cdot x_n^{\varepsilon_n}$ hat, in der

- $n \geq 0$ (für $n = 0$ ist y das "leere Wort", es ist das neutrale Element in F)
- $x_i \in X$ für $i = 1, \ldots, n$
- $\varepsilon_i \in \{+1, -1\}$ für $i = 1, \ldots, n$
- $x_{i+1}^{\varepsilon_{i+1}} \neq x_i^{-\varepsilon_i}$ für $i = 1, \ldots, n-1$

(b) Ist F frei mit Basis X, so gilt für jedes $x \in X$: $x^{-1} \notin X$.

(c) Ist F frei mit Basis X, so ist F torsionsfrei, das heißt: $ord(x) = \infty$ für jedes $x \in F$, $x \neq e$.

(d) $(\mathbb{Z}, +)$ ist frei mit Basis $\{1\}$ oder Basis $\{-1\}$

(e) Ist F frei mit Basis X und $|X| \geq 2$, so ist F nicht abelsch.

Beweis: Seien $x_1, x_2 \in X : x_1 \neq x_2 \Rightarrow x_1 x_2 x_1^{-1} x_2^{-1} \neq e \Rightarrow x_1 x_2 \neq x_2 x_1$ ■

Satz 3

(a) Zu jeder Menge X gibt es eine freie Gruppe $F(X)$ mit Basis X.

(b) Zu jeder Gruppe G und jeder Abbildung $f : X \to G$ gibt es genau einen Gruppenhomomorphismus $\phi : F(X) \to G$ mit $\phi(x) = f(x)$ für alle $x \in X$.

(c) Jede Gruppe "ist" (d.h. ist isomorph zu einer) Faktorgruppe einer freien Gruppe.

(d) $F(X) \cong F(Y) \Leftrightarrow |X| = |Y|$

Beweis:

(a) Sei $X^{\pm} = X \times \{1, -1\}$ und $i : X^{\pm} \to X^{\pm}$ die Abbildung: $i(x, \varepsilon) = (x, -\varepsilon)$. Die Abbildung i ist bijektiv und $i^2 = id$.
Schreibweise: $(x, 1) =: x$, $(x, -1) =: x^{-1} \Rightarrow i(x) = x^{-1}$, $i(x^{-1}) = x$
Ein Element $g = (x_1, \ldots, x_n) \in F_0^a(X^{\pm})$ (freie Worthalbgruppe) heißt **reduziert**, wenn $x_{\nu+1} \neq i(x_\nu)$ für $\nu = 1, \ldots, n-1$. Sei $F(X)$ die Menge der reduzierten Wörter in $F_0^a(X^{\pm})$
Def.: Zwei Wörter in $F_0^a(X^{\pm})$ heißen **äquivalent**, wenn sie durch endliches Einfügen oder Streichen von Paaren der Form $(x, i(x)), x \in X^{\pm}$ auseinander hervorgehen.
Bsp.: $x_1 \sim x_1 x_2 x_2^{-1} \sim x_1 x_2 x_3^{-1} x_3 x_2^{-1}$
Beh.: In jeder Äquivalenzklasse gibt es genau ein reduziertes Wort. Dann definiere Verknüpfung auf $F(X) : (x_1, \ldots, x_n) \star (y_1, \ldots, y_m)$ sei **das** reduzierte Wort in der Äquivalenzklasse von $(x_1, \ldots, x_n, y_1, \ldots, y_m)$. Dieses Produkt ist **assoziativ**: Für $x, y, z \in F(X)$ ist $(xy)z$ das eindeutig bestimmte reduzierte Wort in der Klasse von $(x_1, \ldots, x_n, y_1, \ldots, y_m, z_1, \ldots, z_l)$, und das gleiche gilt für $x(yz)$.
neutrales Element: $e = ()$
inverses Eement zu $(x_1, \ldots, x_n)$ ist $(i(x_n), i(x_{n-1}), \ldots, i(x_1)) \Rightarrow F(X)$ ist Gruppe.
$F(X)$ ist frei mit Basis X nach Konstruktion.
Bew. der Beh.: In jeder Klasse gibt es ein reduziertes Wort: **ja**!
Eindeutigkeit: Seien x, y reduziert und äquivalent. Dann gibt es ein Wort w, aus

dem sowohl x als auch y durch Streichen hervorgehen. Zu zeigen also: Jede Reihenfolge von Streichen führt zum selben reduzierten Wort.
Induktion über die Länge $l(w)$:
$l(w) = 0$ ✓
$l(w) = 1$ ✓
Sei $l(w) \geq 2$; Ist w reduziert, so ...
Enthält w genau ein Paar $(x_\nu, i(x_\nu))$, so muß dies als erstes gestrichen werden. Es entsteht w' mit $l(w') = l(w) - 2 \overset{\text{IV}}{\Rightarrow}$ Beh. Enthält w Paare $(x_\nu, i(x_\nu))$ und $(x_\mu, i(x_\mu))$, so gibt es zwei Fälle: (Sei oBdA $\mu > \nu$)
$\mu = \nu + 1$: $x_\nu i(x_\nu) x_\nu$ Dann führen beide Streichungen zum selben Wort.
$\mu \geq \nu + 2$: Streichen beider Paare, erhalte w'' mit $l(w'') = l(w) - 4 \overset{\text{IV}}{\Rightarrow}$ Beh.

(b) Sei $f : X \to G$ eine Abbildung. Für $w = x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n}$ setze

$$\phi(w) = f(x_1)^{\varepsilon_1} \cdot \cdots \cdot f(x_n)^{\varepsilon_n} .$$

Dies muss eindeutig so sein, und so wird ein Homomorphismus definiert.

(c) Sei $S \subseteq G$ ein Erzeugendensystem (d.h. die einzige Untergruppe H von G mit $S \subseteq H$ ist G selbst). Sei $F(S)$ die freie Gruppe mit Basis S, $f : S \to G$ die Inklusion und $\phi : F(S) \to G$ der Homomorphismus aus (b). ϕ ist surjektiv, weil $\phi(F(S))$ Untergruppe ist, die S enthält. Also ist nach Homomorphiesatz $G \cong F(S)/\operatorname{Kern}(\phi)$

Beispiele:

a) G zyklisch von Ordnung $n \in \mathbb{N}$, dann ist $G \cong \mathbb{Z}/n\mathbb{Z}$.

b) $\mathbb{Z}^2 := \mathbb{Z} \times \mathbb{Z}$, $S = \{(0,1) =: x, (1,0) =: y\}$. Der Homomorphismus $\varphi : F(S) \to \mathbb{Z}^2$, $x \mapsto (0,1)$, $y \mapsto (1,0)$ bildet $w = x^{n_1} y^{m_1} \cdots x^{n_d} y^{m_d} \in F(S)$ auf $\varphi(w) = (\sum_{i=1}^d n_i, \sum_{i=1}^d m_i)$ ab, also ist $\operatorname{Kern}\varphi = \{w = x^{n_1} y^{m_1} \cdots x^{n_d} y^{m_d} \in F(S) \mid \sum_{i=1}^d n_i = \sum_{i=1}^d m_i = 0\} = \langle\{w_1 w_2 w_1^{-1} w_2^{-1}, w_1, w_2 \in F(S)\}\rangle = G^{\text{ab}}$. $\operatorname{Kern}\varphi$ ist kleinster Normalteiler von $F(\{x,y\})$, der $xyx^{-1}y^{-1}$ enthält, daher ist $\mathbb{Z}^2 \cong F(\{x,y\})/\langle xyx^{-1}y^{-1}\rangle_{\text{NT}}$.

(d) Erstmal ist klar, dass für jede Abbildung $g : X \to Y$ ein eindeutiger Gruppenhomomorphismus $\varphi_g : F(X) \to F(Y)$ mit $\varphi_g(x) = g(x)$ für alle $x \in X$ existiert. (Dies folgt aus (b), wenn die Abbildung $X \to F(Y)$, $x \mapsto g(x)$ als f eingesetzt wird.)

"$\Leftarrow$" Sei $f : X \to Y$ bijektive Abbildung. Dazu gibt es Gruppenhomomorphismen $\varphi_f : F(X) \to F(Y)$ sowie $\varphi_{f^{-1}} : F(Y) \to F(X)$. Es ist sowohl $\varphi_{f^{-1}} \circ \varphi_f|_X = id_X$ als auch $id_{F(X)}|_X = id_X$, also folgt aus der Eindeutigkeit (b), dass $\varphi_{f^{-1}} \circ \varphi_f = id_{F(X)}$. Analog; $\varphi_f \circ \varphi_{f^{-1}} = id_{F(Y)}$. Also ist φ_f ein Isomorphismus.
"$\Rightarrow$" Die Anzahl der Gruppenhomomorphismen von $F(X)$ in $\mathbb{Z}/2\mathbb{Z}$ ist gleich der Anzahl der Abbildungen von X nach $\{0,1\}$ (wegen (b)), und diese ist $|2^X| = |\mathcal{P}(X)|$
Sei $|X| \neq |Y|$, dann ist $|\mathcal{P}(X)| \neq |\mathcal{P}(Y)|$. ■

1.6 Kategorien und Funktoren

Definition 1.6.1

Eine **Kategorie** $\mathcal{C}$ besteht aus einer Klasse $Ob\,\mathcal{C}$ von Objekten und für je zwei Objekte $A, B \in Ob\ \mathcal{C}$ aus einer Menge $Mor_{\mathcal{C}}(A, B)$ von **Morphismen** von A nach B, für die folgende Eigenschaften erfüllt sind.

(i) Für jedes $A \in Ob\,\mathcal{C}$ gibt es ein Element $id_A \in Mor_{\mathcal{C}}(A, A)$

(ii) Für je drei Objekte $A, B, C \in Ob\,\mathcal{C}$ gibt es eine Abbildung $\circ$:

$$\begin{array}{ccccc} Mor(B,C) & \times & Mor(A,B) & \to & Mor(A,C) \\ (g & , & f) & \mapsto & g \circ f \end{array}$$

mit

$$\begin{array}{rcll} g \circ id_A & = & g & \text{für alle } g \in Mor(A,B) \\ id_B \circ f & = & f & \text{für alle } f \in Mor(A,B) \\ (h \circ g) \circ f & = & h \circ (g \circ f) & \text{für alle } f \in Mor(A,B), g \in Mor(B,C), h \in Mor(C,D) \end{array}$$

Beispiel:

(1) Mengen mit Abbildungen

(2) Mengen mit bijektiven Abbildungen

(3) K-Vektorräume mit k-linearen Abbildungen

(4) Halbgruppen mit Homomorphismen

(5) Monoide mit Homomorphsimen

(6) Magmen mit Homomorphismen

(7) Gruppen mit Homomorphismen

(8) abelsche Gruppen mit Homomorphismen

(9) topologische Räume mit stetigen Abbildungen

Definition 1.6.2

Seien $\mathcal{A}$ und $\mathcal{B}$ Kategorien.

(a) Ein **kovarianter Funktor** $F : \mathcal{A} \to \mathcal{B}$ besteht aus einer Abbildung $F : Ob\ \mathcal{A} \to Ob\ \mathcal{B}$, sowie für je zwei Objekte $X, Y \in Ob\ \mathcal{A}$ aus einer Abbildung $F : Mor_{\mathcal{A}}(X, Y) \to Mor_{\mathcal{B}}(F(X), F(Y))$, so dass gilt:

(i) $F(id_X) = id_{F(X)}$ für alle $X \in Ob\,\mathcal{A}$

(ii) $F(g \circ f) = F(g) \circ F(f)$ für alle $f \in Mor_{\mathcal{A}}(A, B), g \in Mor_{\mathcal{A}}(B, C)$

(b) Ein **kontravarianter** Funktor $F : \mathcal{A} \to \mathcal{B}$ ist ebenso wie in (a) definiert. Ausnahme: $F : Mor_{\mathcal{A}}(X, Y) \to Mor_{\mathcal{B}}(F(Y), F(X))$, ... und $F(g \circ f) = F(f) \circ F(g)$

Beispiel:

(1) V : Gruppen $\to$ Mengen, $(G, \cdot) \mapsto G$, $V(f) = f$ ist der „Vergissfunktor“

(2) a) Im : Mengen $\to$ Mengen, $Im(X) = \mathcal{P}(X)$, für $f : X \to Y$ ist $Im(f) : \mathcal{P}(X) \to \mathcal{P}(Y)$, $Im(f)(U) = f(U)$, $U \in \mathcal{P}(X)$ ist kovariant.

b) Urb : Mengen $\to$ Mengen, $Urb(X) = \mathcal{P}(X)$, für $f : X \to Y$ ist $Urb(f) : \mathcal{P}(Y) \to \mathcal{P}(X)$, $Urb(f)(V) = f^{-1}(V)$, $V \in \mathcal{P}(Y)$ ist kontravariant.

(3) Sei $\mathcal{C}$ Kategorie, X ein Objekt in $\mathcal{C}$. Definiere Funktoren $\mathcal{C} \to$ Mengen durch
$\mathrm{Hom}(X, \cdot) : Y \mapsto Mor_{\mathcal{C}}(X, Y)$ (kovariant)
$\mathrm{Hom}(\cdot, X) : Y \mapsto Mor_{\mathcal{C}}(Y, X)$ (kontravariant)
Für $f \in \mathrm{Mor}(Y, Z)$ ist $\mathrm{Hom}(X, \cdot)(f) : Mor(X, Y) \to Mor(X, Z)$ gegeben durch $g \mapsto f \circ g$ und $\mathrm{Hom}(\cdot, X)(f) : Mor(Z, X) \to Mor(Y, X)$, $g \mapsto g \circ f$

(4) Sei X Menge, F_X: Gruppen $\to$ Mengen. $G \mapsto Abb(X, G) = Mor_{Mengen}(X, G)$ ist kovarianter Funktor (also Komposition des Vergissfunktors und des Homomorphismen-Funktors $\mathrm{Hom}(X, \cdot)$).

Definition 1.6.3

Sei $\mathcal{C}$ eine Kategorie, X, Y Objekte in $\mathcal{C}$. $f \in Mor_{\mathcal{C}}(X, Y)$ heißt **Isomorphismus**, wenn es $g \in Mor_{\mathcal{C}}(Y, X)$ gibt, so dass $g \circ f = id_X$ und $f \circ g = id_Y$.

Definition 1.6.4

Seien $\mathcal{A}$, $\mathcal{B}$ Kategorien und $F, G : \mathcal{A} \to \mathcal{B}$ kovariante Funktoren. F und G heißen **isomorph**, wenn es zu jedem Objekt $A \in Ob\,\mathcal{A}$ einen Isomorphismus $\alpha_A : F(A) \to G(A)$, also $\alpha_A \in Mor_{\mathcal{B}}(F(A), G(A))$ gibt, so dass für alle Morphismen $f : A \to A'$ in $\mathcal{A}$ das folgende Diagramm kommutiert:

$$\begin{array}{ccc} F(A) & \xrightarrow{\alpha_A} & G(A) \\ {\scriptstyle F(f)}\downarrow & & \downarrow{\scriptstyle G(f)} \\ F(A') & \xrightarrow[\alpha_{A'}]{} & G(A') \end{array}$$

Also: $G(f) \circ \alpha_A = \alpha_{A'} \circ F(f)$.

Sind die α_A nur Morphismen (also nicht notwendigerweise Isomorphismen), so heißt $\alpha : F \to G$ eine **natürliche Transformation** von Funktoren.

Proposition 1.6.5

Sei X eine Menge, $F(X)$ die freie Gruppe mit Basis X. Dann sind die Funktoren F_X und $Hom(F(X), \cdot) : \underline{\text{Gruppen}} \to \underline{\text{Mengen}}$ isomorph.

Beweis: Nach Satz 3 gibt es für jede Gruppe G eine bijektive Abbildung $\alpha_G : F_X(G) = Abb(X, G) \to Hom(F(X), G)$, $f \mapsto \varphi = \hat{f}$. Sei $\rho : G \to G'$ ein Gruppenhomomorphismus. Dann kommutiert:

$$\begin{array}{ccc} F_X(G) & \xrightarrow{\alpha_G} & Hom(F(X), G) \\ {\scriptstyle F_X(\rho)}\downarrow & & \downarrow{\scriptstyle Hom(F(X),\cdot)(\rho)} \\ F_X(G') & \xrightarrow[\alpha_{G'}]{} & Hom(F(X), G') \end{array}$$

Denn für $f \in F_X(G)$ ist $\alpha_G(f) = \hat{f}$ und $\big((Hom(F(X), \cdot)(\rho)\big)(\hat{f}) = \rho \circ \hat{f}$ sowie $F_X(\rho)(\hat{f}) = \rho \circ f$ und $\alpha_{G'}(\rho \circ f) = \widehat{g \circ f}$. Beides ist **der** eindeutig bestimmte Gruppenhomomorphismus $F(X) \to G'$, der auf X die Abbildung $g \circ f$ ist. ■

Definition + Bemerkung 1.6.6

1. Sei $\mathcal{C}$ eine Kategorie und $F : \mathcal{C} \to \underline{\text{Mengen}}$ ein kovarianter Funktor. Ein Objekt $U \in \mathcal{C}$ heißt **darstellendes Objekt** für F, wenn F isomorph zu $Hom(U, \cdot)$ ist.

   Analog gilt das für kontravariante Funktoren, wenn F isomorph zu $Hom(\cdot, U)$ ist.

2. F heißt **darstellbar**, wenn es ein darstellendes Objekt für F gibt.

3. Ist F darstellbar, so sind je zwei darstellende Objekte für F isomorph.

Beweis: Seien U, W darstellende Objekte für F. Dann gibt es einen Isomorphismus von Funktoren $\alpha := h_U := Hom(U, \cdot) \to Hom(W, \cdot)$, insbesondere also bijektive Abbildungen $\alpha_U : Mor(U, U) \to Mor(W, U)$ und $\alpha_W : Mor(U, W) \to Mor(W, W)$. Sei $\varphi := \alpha_U(id_U)$, $\psi := \alpha_W^{-1}(id_W)$. Zu zeigen: $\varphi \circ \psi = id_U$, $\psi \circ \varphi = id_W$.

Das kommutative Diagramm aus Definition 1.6.4 für den Morphismus ψ ist:

$$\begin{array}{ccc} Mor(U, U) & \xrightarrow{\alpha_U} & Mor(W, U) \\ {\scriptstyle h_U(\psi)}\downarrow & & \downarrow{\scriptstyle h_W(\psi)} \\ Mor(U, W) & \xrightarrow[\alpha_W]{} & Mor(W, W) \end{array}$$

Also gilt

$$\begin{aligned} id_W &= \alpha_W(\psi) \\ &= \alpha_W(\psi \circ id_U) \\ &= (\alpha_W \circ h_U(\psi))(id_U) \\ &= (h_W(\psi) \circ \alpha_U)(id_U) \\ &= h_W(\psi)(\varphi) \\ &= \psi \circ \varphi \end{aligned}$$

und analog folgt $\varphi \circ \psi = id_U$. ■

1.7 Gruppenaktionen und die Sätze von Sylow

Definition + Bemerkung 1.7.1

Sei G eine Gruppe, X eine Menge.

(a) Eine **Aktion** (Wirkung) von G auf X ist ein Gruppenhomomorphismus $\rho : G \to \mathrm{Perm}(X)$. G **operiert** dann auf X.

(b) Die Aktionen von G auf X entsprechen bijektiv den Abbildungen: $G \times X \to X,\ (g, x) \mapsto gx$, für die gilt

(i) $ex = x$ für alle $x \in X$

(ii) $(g_1 g_2)x = g_1(g_2 x)$ für alle $g_1, g_2 \in G,\ x \in X$

Beweis: Sei $\rho : G \to \mathrm{Perm}(X)$ ein Homomorphismus. Dann erfüllt $G \times X \to X,\ (g, x) \mapsto \rho(g)(x)$ die Eigenschaften (i) und (ii), denn $\rho(e) = id_X$ und $\rho(g_1 g_2)(x) = \rho(g_1)(\rho(g_2)(x))$.

Ist umgekehrt $\mu : G \times X \to X$ mit (i), (ii) gegeben, so sei für $g \in G$ die Abbildung $\rho(g) : X \to X$ definiert durch $\rho(g)(x) = \mu(g, x)$. $\rho(g)$ ist bijektiv, da $\rho(g^{-1})$ die Umkehrabbildung ist:

$$\begin{aligned} \rho(g^{-1})(\rho(g)(x)) &= \mu(g^{-1}, \mu(g, x)) \\ &= g^{-1} \cdot (g \cdot x) \\ &= (g^{-1} \cdot g) \cdot x \\ &= e \cdot x \\ &= x \end{aligned}$$

Dann ist $\rho : G \to \mathrm{Perm}(X),\ g \mapsto \rho(g)$ wegen (ii) ein Homomorphismus. ■

Beispiel:

a) $G \times G \to G,\ (g_1, g_2) \mapsto g_1 g_2$ ("Linksmultiplikation") ist eine Gruppenaktion.

b) $(g, h) \mapsto h \cdot g$ ist im Allgemeinen keine Gruppenaktion, aber $(g, h) \mapsto hg^{-1}$ ist eine.

c) $G \times G \to G,\ (g, h) \mapsto ghg^{-1}$ ("Konjugation") ist eine Gruppenaktion.

d) Ist X eine beliebige Menge, so operiert S_n auf X^n durch Vertauschen der Komponenten: $\sigma(x_1, \ldots, x_n) = (x_{\sigma^{-1}(1)}, \ldots, x_{\sigma^{-1}(n)})$.

(c) Eine Aktion ρ heißt **effektiv** (oder **treu**), wenn $\mathrm{Kern}(\rho) = \{e\}$.
Allgemein heißt $\mathrm{Kern}(\rho)$ **Ineffektivitätskern** ("Nichtsnutz") der Aktion.

Beispiel:

a) ist effektiv

c) Der Ineffektivitätskern ist das Zentrum $Z(G)$

d) ist effektiv für $|X| \geq 2$

(d) Für $x \in X$ heißt $Gx := \{gx : g \in G\}$ die **Bahn** von x unter G.

(e) X ist disjunkte Vereinigung von G-Bahnen.

Beweis: Durch $x \sim y \iff \exists g \in G : y = gx$ wird eine Äquivalenzrelation definiert, deren Äquivalenzklassen gerade die G-Bahnen sind. ■

(f) Für $x \in X$ heißt $G_x := \{g \in G : gx = x\}$ die **Fixgruppe** von x unter G (auch **Stabilisator** oder **Isotropiegruppe** von x genannt). Dies ist eine Untergruppe von G.

(g) Für $x \in X,\ g \in G$ ist $G_{gx} = gG_x g^{-1}$

Proposition 1.7.2 (Bahnbilanz)

Sei X endliche Menge, G Gruppe, die auf X operiert. Sei $x_1, \ldots, x_n$ ein Vertretersystem der G-Bahnen in X. (dh. aus jeder G-Bahn genau ein Element). Dann gilt:

$$|X| = \sum_{i=1}^{r} [G : G_{x_i}]$$

Beweis: Nach 1.7.1 ist $|X| = \sum_{i=1}^{r} |Gx_i|$. Zu zeigen bleibt also: $|Gx_i| = [G : G_{x_i}]$.

Beh.:

$$\alpha_i = \begin{cases} Gx_i & \to & G/G_{x_i} \\ gx_i & \mapsto & gG_{x_i} \end{cases}$$

ist bijektive Abbildung, denn:

- α_i ist wohldefiniert: Ist $g \cdot x_i = h \cdot x_i$, so ist $(h^{-1}g)x_i = x_i$, also $h^{-1}g \in G_{x_i} \implies g \in hG_{x_i} \implies gG_{x_i} \cap hG_{x_i} \neq \emptyset \implies gG_{x_i} = hG_{x_i}$
- α_i ist injektiv. Ist $gG_{x_i} = hG_{x_i}$, so ist $g \in hG_{x_i} \implies h^{-1}g \in G_{x_i} \implies (h^{-1}g)x_i = x_i \implies g \cdot x_i = h \cdot x_i$
- α_i ist offensichtlich surjektiv.

■

Satz 4 (Sylow)

Sei G endliche Gruppe, $|G| = n$, p eine Primzahl. Sei $n = p^k m$ mit $k \geq 0$ und $p \nmid m$. Dann gilt:

(a) G enthält eine Untergruppe S der Ordnung p^k. Jede solche Untergruppe heißt **p-Sylowgruppe** von G.

(b) Je zwei p-Sylowgruppen sind konjugiert.

(c) Die Anzahl s_p der p-Sylowgruppen in G erfüllt: $s_p \mid m$ und $s_p \equiv 1 \mod p$.

Beweis: $k = 0 : \checkmark$ Sei also $k \geq 1$.

(a) Sei $\mathcal{M} = \{M \subseteq G : |M| = p^k\} \subset \mathcal{P}(G)$.
Es ist $|\mathcal{M}| = \binom{n}{p^k} = \binom{p^k m}{p^k}$
Beh.1: $p \nmid |\mathcal{M}|$
G operiert auf $\mathcal{M}$ durch die Linksmultiplikation $gM = \{gx : x \in M\} \in \mathcal{M} \Rightarrow |\mathcal{M}|$ ist Summe der Bahnlängen. Wegen Beh.1 gibt es eine Bahn GM_0 mit $p \nmid |GM_0|$.
$\overset{1.7.2}{\Rightarrow} |GM_0| = [G : G_{M_0}] = \frac{|G|}{|G_{M_0}|} = \frac{p^k m}{|G_{M_0}|} \Rightarrow p^k \mid |G_{M_0}|$.
Andererseits ist $|G_{M_0}| \leq p^k = |M_0|$, denn für $x \in M_0$ ist $g \mapsto gx$ injektive Abbildung $G_{M_0} \to M_0 \Rightarrow |G_{M_0}| = p^k$, dh. G_{M_0} ist p-Sylowgruppe.
Bew. von Beh.1:

$$\binom{p^k m}{p^k} = \prod_{i=0}^{p^k - 1} \frac{p^k m - i}{p^k - i}$$

Schreibe jedes dieser i in der Form $p^{\nu_i} m_i$, mit $p \nmid m_i (0 \leq \nu_i < k) \Rightarrow \frac{p^k m - i}{p^k - i} = \frac{m p^{k-\nu_i} - m_i}{p^{k-\nu_i} - m_i} \Rightarrow$ weder Zähler noch Nenner sind durch p teilbar. $\Rightarrow$ Beh.

(b) Sei $S \subseteq G$ p-Sylowgruppe.
$\mathcal{S} := \{S' \leq G : S' = gSg^{-1}$ für ein $g \in G\}$
Beh.2: $p \nmid |\mathcal{S}|$.
Bew.2: G operiert auf $\mathcal{S}$ durch Konjugation. Diese Aktion ist transitiv, d.h. es gibt nur eine Bahn. Die Fixgruppe von S' unter dieser Aktion ist $N_{S'} := \{g \in G : gS'g^{-1} = S'\}$
$N_{S'}$ heißt der **Normalisator** von S' in G.
(S' ist Normalteiler in $N_{S'}$ und maximal mit dieser Eigenschaft.)
$\Rightarrow |\mathcal{S}| = [G : N_S] = \frac{|G|}{|N_S|} = \frac{p^k m}{|N_S|}$
S ist Untergruppe von $N_S \Rightarrow p^k \mid |N_S| \Rightarrow |\mathcal{S}|$ ist Teiler von m.
Sei $\widetilde{S}$ eine p-Sylowgruppe in G. zu zeigen: $\widetilde{S} \in \mathcal{S}$.
$\widetilde{S}$ operiert auf $\mathcal{S}$ (da $\widetilde{S} \subset G$). Sei nun $s_1, \ldots, s_r$ ein Vertretersystem der Bahnen.

$$\Rightarrow |\mathcal{S}| = \sum_{i=1}^{r} [\widetilde{S} : \widetilde{S_{s_i}}] = \sum_{i=1}^{r} \frac{p^k}{|\widetilde{S_{s_i}}|} \overset{\text{Beh.2}}{\Rightarrow} \text{Es gibt ein } i \text{ mit } \widetilde{S} = \widetilde{S_{s_i}}$$

Dann ist $\widetilde{S} \subseteq N_{S_i}$.
Beh.3: Dann ist $\widetilde{S} \subseteq S_i$, also $\widetilde{S} = S_i$, da beide p^k Elemente haben.
Bew.3: S_i ist Normalteiler in N_{s_i}, $\widetilde{S}$ ist Untergruppe in $N_{s_i} \Rightarrow \widetilde{S}S_i$ ist Untergruppe von N_{s_i} (Übung)
Wäre $\widetilde{S} \not\subseteq S_i$, dann wäre $\widetilde{S}S_i \supsetneq S_i$, also $|\widetilde{S}S_i| = p^k d$ mit $d > 1$. (und $p \nmid d$)
$\overset{\text{Übung}}{\Rightarrow} \widetilde{S}S_i/S_i \cong \widetilde{S}/\widetilde{S} \cap S_i \Rightarrow |\widetilde{S}S_i| = \frac{|S_i||\widetilde{S}|}{|\widetilde{S} \cap S_i|} = \frac{p^{2k}}{|\widetilde{S} \cap S_i|} = p^l$ für ein $l \in \mathbb{N}$. $p^l = p^k d$, $d \neq 1 \Rightarrow \lightning$!

(c) $s_p = |\mathcal{S}| \Rightarrow s_p \mid m$ und $\mathcal{S} = \sum_{i=1}^{r} [\widetilde{S} : \widetilde{S}_{S_i}]$
$[\widetilde{S} : \widetilde{S}_{S_i}] = 1 \Leftrightarrow \widetilde{S} = \widetilde{S}_{S_i} \overset{Beh.3}{\Leftrightarrow} \widetilde{S} = S_i$, also genau **einmal**. Alle anderen Summanden sind durch p teilbar. ■

Folgerung 1.7.3

Ist G eine endliche Gruppe und p eine Primzahl, die die Gruppenordnung $|G|$ teilt, so enthält G ein Element von Ordnung p.

Beweis: Sei $|G| = p^k m$ mit $p \nmid m$, $k \geq 1$. $S \subseteq G$ eine p-Sylowgruppe und $x \in S$, $x \neq e$. $\overset{1.2.6}{\Rightarrow}$ ord(x) ist Teiler von $|S| = p^k \Rightarrow$ ord$(x) = p^d$ für ein d, $1 \leq d \leq k \Rightarrow x^{p^{d-1}}$ hat dann Ordnung p. ■

Beispiel: Wieviele Gruppen G gibt es mit $|G| = 15$? Mindestens eine: $G = \mathbb{Z}/15\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$.

Nach Sylow gibt es nicht 5 3-elementigen Untergruppen, da $5 \equiv 1 \mod 3$ nicht gilt, und nicht 3, da $3 \nmid s_3$. also gibt es nur eine S_3 und ebenso nur eine S_5.

Daher gibt es genau zwei Elemente der Ordnung 3 und vier Elemente der Ordnung 5. Übrig gleiben 8 Elemente, die Ordnung 15 haben müssen, also ist $G \cong \mathbb{Z}/15\mathbb{Z}$.

1.8 Symmetrische und alternierende Gruppen

Definition + Bemerkung 1.8.1

Sei $n \geq 0$.

(a) $S_n = \text{Perm}(\{1, \ldots, n\})$ heißt *symmetische Gruppe*.

(b) $|S_n| = n!$

(c) $\xi \in S_n$ heißt **Zyklus** wenn es ein k gibt (mit $1 \leq k \leq n$) und paarweise verschiedene Elemente $i_1, \cdots, i_k$ von $\{1, \ldots, n\}$ mit $\xi(i_\nu) = i_{\nu+1}$ für $\nu = 1, \ldots, k-1$, $\xi(i_k) = i_1$ und $\xi(j) = j$ für $j \notin \{i_1, \ldots, i_k\}$. In diesem Fall heißt ξ ein k-**Zyklus**, und k wird die **Länge** dieses Zykels ξ genannt.

(d) Jedes $\sigma \in S_n$ lässt sich als Produkt von paarweise disjunkten Zykeln schreiben (wobei zwei Zykeln als disjunkt gelten, wenn jedes Element von $\{1, \ldots, n\}$ von mindestens einem der beiden unverändert gelassen wird). Diese Darstellung ist eindeutig bis auf die Reihenfolge.

(e) 2-Zykel heißen auch Transpositionen.

(f) Jeder k-Zyklus ist Produkt von $k-1$ Transpositionen:

$$(1\ 2 \cdots k) = (1\ 2) \circ (2\ 3) \circ \cdots \circ (k-1\ k)$$

(g) $\sigma \in S_n$ heißt *gerade*, wenn es als Produkt einer geraden Anzahl von Transpositionen geschrieben werden kann, anderenfalls *ungerade*.

(h) sign : $S_n \to \{+1, -1\}$,

$$\text{sign}(\sigma) = \begin{cases} +1, & \sigma \text{ gerade} \\ -1, & \sigma \text{ ungerade} \end{cases}$$

ist ein Homomorphismus.

$A_n := \text{Kern}(\text{sign}) = \{\sigma \in S_n \mid \sigma \text{ gerade}\}$ heißt *alternierende Gruppe*.

Bemerkung 1.8.2 (a) Je zwei k-Zykel in S_n sind konjugiert.

Beweis: Für $\sigma \in S_n$ ist $\sigma(1\ 2\ \cdots\ k)\sigma^{-1} = (\sigma(1)\ \sigma(2)\ \cdots\ \sigma(k))$, also kann man jedes k-Zykel so darstellen. ■

(b) Daraus folgt: Zwei Permutationen in S_n sind genau dann konjugiert, wenn sie die gleiche „Zykelstruktur" haben (d. h. derart jeweils als Produkte disjunkter Zykel dargestellt werden können, dass die Längen der Zykel in der Darstellung der ersten Permutation gleich den Längen der entsprechenden Zykel in der Darstellung der zweiten Permutation sind).

Bemerkung 1.8.3 (a) In A_4 kann die vorangehende Bemerkung nicht stimmen: (1 2 3) und (3 2 1) sind nicht konjugiert.

(b) Für $n \geq 5$ sind je zwei 3-Zykel in A_n konjugiert.

Beweis:

(a) Ausprobieren

(b) $(1\ 3\ 2) = \sigma(1\ 2\ 3)\sigma^{-1}$ mit $\sigma = (1\ 2)(4\ 5)$
$(i\ j\ k) = \sigma(1\ 2\ 3)\sigma^{-1}$ mit $\sigma = (1\ i\ 2\ j)(3\ k)$ für $i, j, k > 3$. Weitere Fälle: Übung. ■

Bemerkung 1.8.4
Jede gerade Permutation ist als Produkt von 3-Zykeln darstellbar

Beweis: $(1\ 2)(3\ 4) = (1\ 2\ 3)(2\ 3\ 4)$, $(1\ 2)(2\ 3) = (1\ 2\ 3)$ ■

Satz 5
Für $n \neq 4$ enthält A_n nur die Normalteiler $\{1\}$ und A_n

Beweis: In A_4 ist $\{\text{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (2\ 3)(1\ 4)\}$ Normalteiler, $A_1 = A_2 = \{\text{id}\}$ und $A_3 = \mathbb{Z}/3\mathbb{Z}$.

Sei also $n \geq 5$ und $N \neq \{\text{id}\}$ ein Normalteiler von A_n.

Es genügt zu zeigen: N enthält einen 3-Zyklus, denn nach 1.8.3 sind dann alle 3-Zykel in N und nach 1.8.4 ist damit $N = A_n$.

Es genügt auch zu zeigen, dass N das Produkt von zwei Transpositionen enthält, denn ist $\sigma = (1\ 2)(3\ 4) \in N$, so ist auch $(3\ 4\ 5) = \sigma(\tau\sigma^{-1}\tau) \in N$, mit $\tau = (1\ 2)(3\ 5)$.

Das Ziel ist also zu zeigen, dass N ein Element σ enthält mit $\sigma(i) \neq i$ für höchstens vier i, denn dann ist $\sigma \in A_4$, also 3-Zykel oder Produkt von zwei Transpositionen.

Für $\sigma \in A_n$ sei $k_\sigma := |\{i : \sigma(i) \neq i\}|$. Wähle $\sigma \in N \setminus \{\mathrm{id}\}$ so dass $k_\sigma \leq k_\alpha$ für alle $\alpha \in N \setminus \{\mathrm{id}\}$.

Annahme: $k_\sigma \geq 5$. 1. Fall: σ enthält einen Zyklus der Länge ≥ 3, also $\sigma(1) = 2$, $\sigma(2) = 3$, $\sigma(4) \neq 4$, $\sigma(5) \neq 5$. Sei $\alpha := \sigma^{-1}(3\ 4\ 5)\sigma(3\ 5\ 4) \in N$. Ist $\sigma(i) = i$, so ist $\alpha(i) = i$ für $i \geq 6$. Außerdem ist $\alpha(1) = 1$ und $\alpha(2) = \sigma^{-1}(4) \neq 2$, also ist $\alpha \neq \mathrm{id}$ und $k_\alpha < k_\sigma$.

2. Fall: σ ist Produkt von disjunkten Transpositionen (mind. 4). Ohne Einschränkung der Allgemeinheit ist $\sigma = (12)(34)(56)(78)\widetilde{\sigma}$ mit $\widetilde{\sigma} \in A_n$, $\widetilde{\sigma}(i) = i$ für $i = 1, \ldots, 8$ $\alpha = \sigma^{-1}(345)\sigma(354)$ erfüllt $\alpha(i) = i$, falls $\sigma(i) = i$, und $\alpha(1) = 1 \Rightarrow k_\alpha < k_\sigma$

Also enthält N ein σ, das höchstens vier i nicht gleich lässt. Damit ist $N = A_n$ gezeigt. ■

1.9 Kompositionsreihen

Vorüberlegung: G Gruppe, $N \trianglelefteq G$ Normalteiler und G/N die Faktorgruppe. Läßt sich nun G aus N und G/N rekonstruieren? Nicht unbedingt, wie das Beispiel D_n zeigt. D_n hat als Normalteiler $\mathbb{Z}/n\mathbb{Z}$, und $D_n/(\mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/2\mathbb{Z}$, aber $D_n \ncong \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Definition 1.9.1

Sei $(*) \ldots \to G_{i-1} \overset{\alpha_{i-1}}{\to} G_i \overset{\alpha_i}{\to} \ldots$ eine Sequenz (Folge) von Gruppen und Gruppenhomomorphismen.
$(*)$ heißt **exakt** an der Stelle i, wenn $\mathrm{Kern}(\alpha_i) = \mathrm{Bild}(\alpha_{i-1})$.
Die Sequenz $(*)$ heißt **exakt**, wenn sie an jeder Stelle exakt ist.

Beispiel:

$$0 \to \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$$

und

$$0 \to \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \to 0$$

sind exakt. Allgemein ist die Sequenz

$$1 \to N \to G \to G/N \to 1 \quad (*)$$

exakt, wann immer G eine Gruppe und N ein Normalteiler von G sind.

Die Aufgabe, Gruppen zu klassifizieren zerfällt in zwei Teilaufgaben:

(1) Geg.: N und G/N. Welche Möglichkeiten gibt es für G?

(2) Welche "unzerlegbaren" Gruppen gibt es?

Definition 1.9.2

Sei G eine Gruppe.

(a) Eine Reihe der Form

$$G = G_0 \triangleright G_1 \triangleright G_2 \triangleright \cdots \triangleright G_n = \{e\} \quad (**)$$

(mit $n \in \mathbb{N}$) heißt **Normalreihe**, wenn G_{i+1} Normalteiler in G_i ist ($i = 0, \ldots, n-1$) und $G_{i+1} \neq G_i$.

(b) Die Faktorgruppen G_i/G_{i+1} in einer Kompositionsreihe $G_0 \triangleright G_1 \triangleright G_2 \triangleright \cdots \triangleright G_n$ heißen die **Faktoren** (oder **Faktorgruppen**) dieser Kompositionsreihe.

(c) G heißt **einfach**, wenn $G \triangleright \{e\}$ die einzige Normalreihe ist, das hießt: G besitzt nur die trivialen Normalteiler G und $\{e\}$ und $G \neq \{e\}$.

(d) Eine Normalreihe heißt **Kompositionsreihe**, wenn sie sich nicht verfeinern läßt, dh. wenn G_i/G_{i+1} einfach ist für $i = 0, \ldots, n-1$

Bemerkung 1.9.3

(a) $\mathbb{Z}/n\mathbb{Z}$ ist einfach $\Leftrightarrow$ n ist Primzahl.

(b) Eine abelsche Gruppe G ist einfach $\Leftrightarrow$ $G \cong \mathbb{Z}/p\mathbb{Z}$ für eine Primzahl p.

(c) $\mathbb{Z}$ besitzt keine Kompositionsreihe.

(d) Jede endliche Gruppe besitzt eine Kompositionsreihe.

(e) Ist G endlich, $(**)$ eine Normalreihe, so gilt:

$$|G| = \prod_{i=0}^{n-1} [G_i : G_{i+1}] = \prod_{i=0}^{n-1} \frac{|G_i|}{|G_{i+1}|}$$

(f) Es ist eine Kompositionsreihe:

$$S_4 \triangleright A_4 \triangleright D_2 = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \triangleright \mathbb{Z}/2\mathbb{Z} \triangleright \{1\}$$

(g) Für $n \geq 5$ ist eine Kompositionsreihe:

$$S_n \triangleright A_n \triangleright \{1\}$$

Satz 6 (Jordan-Hölder)

Sei G eine Gruppe, und seien

$$G = G_0 \rhd G_1 \rhd \cdots \rhd G_m = \{1\}$$

$$G = H_0 \rhd H_1 \rhd \cdots \rhd H_l = \{1\}$$

Kompositionsreihen für G.

Dann ist $m = l$ und es gibt eine Permutation $\sigma \in \mathrm{Perm}(\{0, \ldots, m-1\})$ mit $G_i/G_{i+1} \cong H_{\sigma(i)}/H_{\sigma(i)+1}$ für $i = 0, \ldots, m-1$.

Beweis: Induktion über m:

$m = 1$: Dann ist G einfach, also auch $l = 1$

$m > 1$: Sei $\bar{G} := G/G_1, \pi : G \to \bar{G}$ die Restklassenabbildung.
$\Rightarrow \bar{H}_i = \pi(H_i)$ ist Normalteiler in $\bar{H}_{i-1}$ für $i = 1, \ldots, l$, denn für $\bar{h}_i \in \bar{H}_i$, $\bar{g} \in \bar{H}_{i-1}$ ist $\bar{g}\bar{h}_i\bar{g}^{-1} = \pi(gh_ig^{-1}) \in \bar{H}_i$ (da $gh_ig^{-1} \in H_i$).
Nach Voraussetzung ist $\bar{G}$ einfach, also $\bar{H}_0 = \bar{G}$, $\bar{H}_1 = \bar{G}$ oder $\bar{H}_1 = \{1\}$, usw.
$\Rightarrow \exists j \in \{0, \ldots, l-1\}$ mit $\bar{H}_0 = \cdots = \bar{H}_j = \bar{G}, \{1\} = \bar{H}_{j+1} = \cdots = \bar{H}_l$.
Sei $C_i := H_i \cap G_1$, $i = 0, \ldots, l$.

Beh.1:

$$G_1 = C_0 \rhd C_1 \rhd \cdots \rhd C_j \rhd C_{j+2} \rhd \cdots \rhd C_l = \{1\}$$

ist Kompositionsreihe für G_1 wenn $j \leq l-2$, bzw.

$$G_1 = C_0 \rhd C_1 \rhd \cdots \rhd C_j = \{1\}$$

ist Kompositionsreihe für G_1 wenn $j = l-1$.
Aber

$$G_1 \rhd G_2 \rhd G_3 \rhd \cdots \rhd G_m = \{1\}$$

ist ebenfalls Kompositionsreihe. $\overset{\text{IV}}{\Rightarrow} m - 1 = l - 1$, also $m = l$ und es gibt $\sigma : \{0, \ldots, j, j+2, \ldots, l-1\} \to \{1, \ldots, l-1\}$ bijektiv mit

$$C_i/C_{i+1} \cong G_{\sigma(i)}/G_{\sigma(i)+1} \text{ für } i \in \{0, \ldots, j, j+2, \ldots, l-1\}.$$

Beh.2

(a) $C_j = C_{j+1}$

(b) $C_i/C_{i+1} \cong H_i/H_{i+1}$ für $i \neq j$

(c) $H_j/H_{j+1} \cong \bar{G} = G/G_1$

Beh.1 folgt aus Beh.2:
C_{i+1} ist Normalteiler in C_i $(i = 0, \ldots, l-1)$, denn für $x \in C_{i+1} = H_{i+1} \cap G_1$ und $y \in C_i = H_i \cap G_1$ ist $yxy^{-1} \in H_i \cap G_1 = C_i$.
C_{j+2} ist Normalteiler in C_j wegen Beh.2(a).
C_{i-1}/C_i sind wegen Beh.2(b) einfach und $\neq \{1\}$ $(i \neq j+1)$

Bew. von Beh.2:

(a) $\bar{H}_{j+1} = \{1\}$, dh. $H_{j+1} \subseteq \operatorname{Kern}\pi = G_1 \Rightarrow C_{j+1} = H_{j+1}$. $C_j = H_j \cap G_1$ ist Normalteiler in H_j. (weil G_1 Normalteiler in G ist)
Da $\bar{H}_j = \bar{G} \neq \{1\}$, ist $C_j \neq H_j \Rightarrow H_{j+1} = C_{j+1} \trianglelefteq C_j \triangleleft H_j$, und weil H_j/H_{j+1} einfach ist, folgt $C_j = H_{j+1} = C_{j+1}$

(b) Für $i \geq j+1$ ist $\bar{H}_i = \{1\}$, also $H_i \subseteq G_1$ und damit $C_i = H_i$.
Für $i < j$ ist $\bar{H}_{i+1} = \bar{G} = G/G_1 \Rightarrow H_{i+1} \cdot G_1 = G_1 \cdot H_{i+1} = G$

$$C_i/C_{i+1} = C_i/(H_{i+1} \cap C_i) \overset{\text{Übung}}{\cong} C_i \cdot H_{i+1}/H_{i+1}$$

zu zeigen also: $C_i \cdot H_{i+1} = H_i$
denn: „$\subseteq$“: ✓
„$\supseteq$“: Da $G_1 H_{i+1} = G$ ist, gibt es zu $x \in H_i$ ein $h \in H_{i+1}$ und $g \in G_1$ mit $x = gh \Rightarrow g = xh^{-1} \in H_i \cdot H_{i+1} \subseteq H_i$, also $g \in H_i \cap G_1 = C_i$ und folglich $x = gh \in C_i H_{i+1}$.

(c) $H_{j+1} \subseteq G_1 \Rightarrow H_j/H_{j+1} = H_j/C_{j+1} \overset{(a)}{=} H_j/C_j = H_j/H_j \cap G_1 \cong H_j G_1/G_1 = G/G_1$

■

Definition + Bemerkung 1.9.4

(a) Eine Gruppe heißt **auflösbar**, wenn sie eine Normalreihe mit abelschen Faktorgruppen besitzt.

(b) Eine endliche Gruppe ist genau dann auflösbar, wenn die Faktoren in ihrer Kompositionsreihe zyklisch von Primzahlordung sind.

Beweis: „$\Longleftarrow$“: Klar

„$\Longrightarrow$“: Sei

$$G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_m = \{1\}$$

eine Normalreihe mit G_i/G_{i+1} abelsch für $i = 0, \ldots, m-1$. Verfeinere sie zur

Kompositionsreihe

$$G = G_0 = H_{0,0} \triangleright H_{0,1} \triangleright \cdots \triangleright H_{0,d_0} = G_1 = H_{1,0} \triangleright \cdots \triangleright H_{1,d_1} = G_2 \triangleright \cdots \triangleright G_m = \{1\}$$

Dabei ist

$$H_{i,j}/H_{i,j+1} \cong H_{i,j}/G_{i+1}/H_{i,j+1}/G_{i+1} \subseteq G_i/G_{i+1}/H_{i,j+1}/G_{i+1}$$

also ist $H_{i,j}/H_{i,j+1}$ isomorph zu einer Untergruppe einer Faktorgruppe einer abelschen Gruppe, also selbst auch abelsch. ■

Beispiel:

- $D_n = \{1, \tau, \ldots, \tau^{n-1}, \sigma, \sigma\tau, \ldots, \sigma\tau^{n-1}\} \triangleright \{1, \tau, \ldots, \tau^{n-1}\} \cong \mathbb{Z}/n\mathbb{Z} \triangleright \{1\}$, also ist D_n auflösbar.
- Für $n \geq 5$ ist $S_n \triangleright A_n \triangleright \{1\}$ Kompositionsreihe, also ist S_n nicht auflösbar.

Proposition 1.9.5

Sei $1 \to G' \to G \to G'' \to 1$ kurze exakte Sequenz von Gruppen, das heißt: G' ist Normalteiler zu G und $G'' = G/G'$. Dann ist G auflösbar genau dann, wenn G' und G'' auflösbar sind.

Beweis: „ $\Longrightarrow$ “: Sei

$$G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_m = \{1\}$$

eine Normalreihe mit G_i/G_{i+1} abelsch für $i = 0, \ldots, m-1$. Dann ist

$$G' = G_0 \cap G' \triangleright G_1 \cap G' \triangleright \cdots \triangleright G_m \cap G' = \{1\}$$

nach Weglassen von Wiederholungen eine Normalreihe für G'. Die Faktorgruppen

$$G_i \cap G'/G_{i+1} \cap G' \cong G_{i+1} \cdot (G_i \cap G')/G_{i+1} \subseteq G_i/G_{i+1}$$

sind abelsch.

$$G'' = G_0/(G_0 \cap G') \triangleright G_1/(G_1 \cap G') \triangleright \cdots \triangleright G_m/(G_m \cap G') = \{1\}$$

ist ebenso nach Weglassen von Wiederholungen eine Normalreihe für G'' mit abelschen Faktorgruppen.

„ $\Longleftarrow$ “: Ist

$$G' = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_m = \{1\}$$

eine Normalreihe für G' mit abelschen Faktoren,

$$G'' = H_0 \triangleright H_1 \triangleright \cdots \triangleright H_n = \{1\}$$

eine solche für G'' und $\pi : G \to G/G' = G''$ die Restklassenabbildung, dann ist

$$G = \pi^{-1}(H_0) \triangleright \pi^{-1}(H_1) \triangleright \cdots \triangleright \pi^{-1}(H_n) = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_m = \{1\}$$

eine Normalreihe für G, da $\pi^{-1}(H_{i+1})$ Normalteiler in $\pi^{-1}(H_i)$ ist und $\pi^{-1}(H_i)/\pi^{-1}(H_{i+1}) \cong H_i/H_{i+1}$ abelsch ist. ■