2. Gruppen

2.1 Definition und erste Beispiele, Untergruppen, Gruppenhomomorphismen

2.1.1 Def Eine Gruppe ist eine Menge G zusammen mit einer Verknüpfung (d.h. einer Abb)

$$* : G \times G \longrightarrow G : (x, y) \longmapsto x * y,$$

so daß folgende Eigenschaften gelten:

1) (Assoziativität) $\forall\, x, y, z \in G$:

$$(x * y) * z = x * (y * z)$$

Wir schreiben dann $x * y * z$

2) (Existenz des Neutralen)

$$\exists\, e \in G : \quad e * x = x \quad \forall\, x \in G$$

3) (Existenz von Inversen)

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

Man nennt x' das Inverse von x und schreibt x^{-1}.

Wir bezeichnen die Gruppe mit $(G, *)$ oder auch nur G, falls $*$ aus dem Kontext klar ist.

Gilt zusätzlich

4) (Kommutativität) $x * y = y * x$
$\forall\, x, y \in G$,

so heißt G <u>abelsch</u> oder <u>kommutativ</u>.

<u>Bsp</u> 1) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ sind abelsche Gruppen. 0 ist neutrales, $-x$ das Inverse zu x.

2) $(\mathbb{Q}\setminus\{0\}, \cdot)$, $(\mathbb{R}\setminus\{0\}, \cdot)$ sind abelsche Gruppen. 1 ist neutrales, $\frac{1}{x}$ das Inverse zu x.

3) Ist M eine Menge, so ist
$\mathrm{Sym}(M) := \{f : M \to M,\ f \text{ bijektiv}\}$
mit der Komposition von Abb eine Gruppe. Es gilt Assoziativität (Analysis), id_M ist Neutrales, die Umkehrabb (Analysis) das Inverse.
Enthält M mehr als 2 Elemente, so ist $\mathrm{Sym}(M)$ nicht abelsch:
Seien x_1, x_2, x_3 in M, definiere

$$f : M \to M : \begin{cases} x_1 \longmapsto x_2 \\ x_2 \longmapsto x_3 \\ x_3 \longmapsto x_1 \\ x \longmapsto x \end{cases} \quad \forall\, x \neq x_1, x_2, x_3$$

$$g: M \to M: \begin{cases} x_1 \mapsto x_2 \\ x_2 \mapsto x_1 \\ x \mapsto x \end{cases} \quad \forall\, x \neq x_1, x_2$$

Dann ist $f \circ g(x_1) = f(x_2) = x_3$

$g \circ f(x_1) = g(x_2) = x_1$

also ist $f \circ g \neq g \circ f$.

Ist $M = \{1, \dots, n\}$, so schreiben wir $S_n := \mathrm{Sym}(M)$ und bezeichnen sie als Permutationsgruppe oder symmetrische Gruppe und ihre Elemente als Permutationen.

Mehr zur Permutationsgruppe S_n:

Wir beschreiben ein Element $\sigma \in S_n$ wie folgt:

$$\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \dots & \sigma(n) \end{pmatrix}$$

2.1.2 Def:

Eine Permutation σ, für die es $\{a_1, \dots, a_k\} \dot\cup \{b_1, \dots, b_{n-k}\} = \{1, \dots, n\}$

gibt mit

$$b = \begin{pmatrix} a_1 & a_2 & a_3 & \cdots & a_{k-1} & a_k & b_1 & \cdots & b_{n-k} \\ a_2 & a_3 & a_4 & \cdots & a_k & a_1 & b_1 & \cdots & b_{n-k} \end{pmatrix}$$

heißt **k-Zykel**.

Wir schreiben kurz $b = (a_1\ a_2 \cdots a_k)$.

$((a_1\ a_2 \cdots a_k) = (a_2\ a_3 \cdots a_k\ a_1)$ etc.)

Ein 2-Zykel heißt **Transposition**.

Eine Transposition $(i\ j)$ vertauscht genau zwei Zahlen i und j und hält die anderen fest.

Eine Transposition $(i\ i+1)$ heißt **Nachbartransposition**.

Bsp

$S_2 = \{id, (12)\}$

$S_3 = \{id, (12), (13), (23), (123), (132)\}$

2.1.3 Satz $|S_n| = n! := n \cdot (n-1) \cdots 1$

Beweis: Um eine Permutation σ festzulegen, müssen wir Bilder für alle Zahlen $1, \dots, n$ festlegen. Für 1 gibt es n Möglichkeiten, für 2 $n-1$ (denn $\sigma(1)$ geht nicht) usw. Also gibt es insgesamt $n!$ Möglichkeiten, die alle Elemente der S_n liefern. □

2.1.4 Prop

Jede Permutation kann als Produkt von disjunkten Zyklen geschrieben werden.

Bsp $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 5 & 6 & 1 & 2 & 8 & 7 \end{pmatrix} \in S_8$

Verfolge die Zahlen:

$1 \mapsto 3 \mapsto 5 \mapsto 1$

$2 \mapsto 4 \mapsto 6 \mapsto 2$

$7 \mapsto 8 \mapsto 7$

$\sigma = (135)(246)(78)$.

Beweis von 2.1.4: Konstruktiv:

Für $i \in \{1, \dots, n\}$ ist i in einem Zykel, man kann ihn mit i beginnend aufschreiben: $(i \quad b(i) \quad b^2(i) \dots b^{k-1}(i))$ bis man k findet mit $b^k(i) = i$.

Es ist nicht möglich, daß $b^k(i) = b^j(i)$ für $0 < j < k$, denn da b bijektiv ist, folgt dann $b^{k-j+1}(i) = i$ und man hätte schon früher geendet.

Betrachte ein j, das nicht im ersten Zykel liegt und fahre fort. □

Zykel der Länge 1 lassen wir weg:

$(12)(36)(4)(5) = \begin{pmatrix} 1 & 2 & 3 & 6 & 4 & 5 \\ 2 & 1 & 6 & 3 & 4 & 5 \end{pmatrix}$

$= (12)(36)$

2.1.5 Lemma Sei $(G, *)$ eine Gruppe.

1. Das neutrale Element ist eindeutig bestimmt und hat die Eigenschaft $x * e = x \quad \forall x \in G$.
2. Sei $x \in G$. Das Inverse x^{-1} ist eindeutig bestimmt und es fällt

$x * x^{-1} = e$.

3. Für $x, y \in G$ gilt $(x^{-1})^{-1} = x$ und $(x * y)^{-1} = y^{-1} * x^{-1}$.

Übung.

Notation: Als Verknüpfungssymbol verwenden wir oft „$\cdot$" und schreiben dann 1 für das Neutrale und x^{-1} oder $\frac{1}{x}$ für Inverse. Verwenden wir „$+$", schreiben wir 0 bzw. $-x$. Dies ist nur eine Schreibweise, angelehnt an die üblichen Bsp.

Notation: Sei $(G, \cdot)$ eine Gruppe, $x \in G$. Wir setzen $x^0 := e$ und für $i \in \mathbb{N}$ rekursiv $x^i := x \cdot x^{i-1}$, und $x^{-i} = (x^{-1})^i$.

Man sieht leicht, daß $x^i \cdot x^j = x^{i+j}$, $(x^i)^j = x^{ij}$.

2.1.6 Def Die Ordnung $|G|$ einer Gruppe ist die Anzahl ihrer Elemente, falls G endlich ist, und ∞ sonst.

2.1.7 Def Erfüllt G nur 2.1 (1), so heißt G Halbgruppe (Bsp: $(\mathbb{N}_{>0}, +)$), erfüllt G 2.1 (1) und (2), so heißt G Monoid (Bsp: $(\mathbb{N}, +)$).

2.1.8 Bsp (freie Gruppen)
Sei $A = \{a, b, c, \dots\}$ eine endliche Menge. Ein Wort über dem Alphabet A ist eine endliche Folge $w = a_1 \cdots a_n$ mit $n \in \mathbb{N}_{>0}$, $a_i \in A$. Ist w' ein weiteres Wort, so definiert Hintereinanderschreiben eine assoziative Verknüpfung $\circ$ auf der Menge aller Wörter G. Wir erhalten eine Halbgruppe. Fügen wir das leere Wort

e hinzu, ist $(G, \circ)$ Monoid.
Fügen wir weitere Buchstaben $a^{-1}, b^{-1}, \ldots$
mit der Regel $aa^{-1} = a^{-1}a = e$,
$bb^{-1} = b^{-1}b = e, \ldots$ zu, so erhalten
wir die <u>freie Gruppe erzeugt von A.</u>

Zum Beispiel ist $(\mathbb{Z}, +)$ die freie
Gruppe erzeugt von $\{1\}$.

2.1.9 Def Sei $(G, \cdot)$ eine Gruppe.
$U \subset G$ heißt <u>Untergruppe</u>, falls $(U, \cdot)$
(mit der Einschränkung $\cdot|_{U \times U}$)
wieder eine Gruppe ist

2.1.10 Proposition: (Untergruppenkriterium)
Sei $(G, \cdot)$ Gruppe und $\emptyset \neq U \subset G$.

U ist Untergruppe $\Leftrightarrow$
$\forall x, y \in U: xy \in U$ und $x^{-1} \in U$.

Beweis:

"$\Rightarrow$" Damit $(U, \cdot)$ Gruppe ist, muß $\cdot|_{U\times U} : U \times U \to U$ gelten, also $xy \in U$ für $x, y \in U$. N.V. existieren die Inversen in U. Da die Inversen in G eindeutig sind, ist x^{-1} (das Inverse in G) in U.

"$\Leftarrow$" Da $xy \in U$ $\forall x, y \in U$ ist $\cdot|_{U\times U} : U \times U \to U$. Assoziativität gilt, da sie in G gilt. Da $U \neq \emptyset$ $\exists x \in U$, n.V. $\exists$ damit auch $x^{-1} \in U$, und dann $x^{-1} \cdot x = e \in U$. Da e Neutrales in G ist, ist es das auch in U. Die Inversen existieren n.V. in U. □

Bsp 1) $(\{-1, 1\}, \cdot)$ ist Untergruppe von $(\mathbb{Q}\setminus\{0\}, \cdot)$.

2) $\mathbb{Z} \subset \mathbb{Q}$, $\mathbb{Z} \subset \mathbb{R}$, $\mathbb{Q} \subset \mathbb{R}$ jeweils mit $+$ sind Untergruppen.

3) Sei $n \in \mathbb{Z}$, setze $n\mathbb{Z} := \{nz \mid z \in \mathbb{Z}\}$ die Menge aller durch n teilbaren Zahlen. $(n\mathbb{Z}, +)$ ist Untergruppe von $(\mathbb{Z}, +)$ (Übung).

2.1.11 Def Seien $(G, \cdot)$, $(H, *)$ Gruppen, $f: G \to H$ eine Abbildung. f heißt ((Gruppen-) Homo-) Morphismus (strukturerhaltende Abb), falls

$$\forall x, y \in G \quad f(x \cdot y) = f(x) * f(y).$$

Bsp 1) $a \in \mathbb{R}$, $f_a: (\mathbb{R}, +) \to (\mathbb{R}, +)$:

$$x \longmapsto ax$$

$$f_a(x+y) = a(x+y) = ax + ay = f_a(x) + f_a(y)$$

$\Rightarrow f_a$ ist Morphismus.

2) Sei $(G, \cdot)$ eine Gruppe, $g \in G$.

Die Rechtstranslation

$$R_g: G \to G: x \longmapsto xg$$

und die Linkstranslation

$$L_g: G \to G: x \longmapsto gx$$

sind keine Gruppenhomomorphismen für $g \neq e$, denn z.B.

$L_g(g \cdot g) = g^3$, $L_g(g) \cdot L_g(g) = g^4$,
wäre $g^3 = g^4$, so würde durch Mult
mit $(g^3)^{-1}$ folgen $e = g$ ↯.

3) Die Konjugation mit g

$i_g: G \longrightarrow G: x \longmapsto g^{-1} x g$

ist ein bijektiver Morphismus:

$i_g(x \cdot y) = g^{-1} x \cdot y \cdot g = g^{-1} x e y g$

$= g^{-1} x g g^{-1} y g = i_g(x) \cdot i_g(y)$

Surjektiv: $g x g^{-1}$ ist Urbild von x,
denn $i_g(g x g^{-1}) = g^{-1} g x g^{-1} g = e x e = x$

Injektiv: Sei $g^{-1} x g = g^{-1} y g$, dann
folgt nach Mult von links mit g
und von rechts mit g^{-1} $x = y$.

2.1.12 Lemma

Seien $f_1: (G_1, \circ) \longrightarrow (G_2, *)$
$f_2: (G_2, *) \longrightarrow (G_3, \times)$
Gruppenhomomorphismen, dann ist auch
$f_2 \circ f_1: (G_1, \circ) \longrightarrow (G_3, \times)$ ein
Gruppenhomomorphismus.

Beweis: $f_2 \circ f_1(g \circ h) = f_2(f_1(g \circ h)) =$

$f_2(f_1(g) * f_2(h)) = f_2(f_1(g)) \times f_2(f_1(h))$.

□

2.1.13 Def Sei $f: (G, \cdot) \to (H, *)$ ein Morphismus.

1) f heißt Monomorphismus, falls f injektiv.
2) " Epimorphismus, falls f surjektiv.
3) " Isomorphismus, falls f bijektiv
4) " Endomorphismus, falls $G = H$.
5) " Automorphismus, falls f Endo- + Isomorphismus ist.

Existiert für Gruppen G, H ein Isomorphismus, so schreiben wir $G \cong H$, G ist isomorph zu H.
Isomorphie ist eine Äquivalenzrelation (siehe 2.1.12 + 2.1.14).

Bsp Die Konjugation i_g ist ein Automorphismus.

2.1.14 Proposition: Sei $f: (G, \cdot) \to (H, *)$ ein Morphismus.

1) $f(e_G) = e_H$
2) $f(x^{-1}) = f(x)^{-1} \quad \forall x \in G$

3) Ist f bijektiv, so ist $f^{-1}: H \to G$ ein Morphismus.

4) Ist $\emptyset \neq U \subset G$ Untergruppe, so ist auch $f(U) \subset H$ Untergruppe.

5) Ist $\emptyset \neq V \subset H$ Untergruppe, so ist auch $f^{-1}(V) \subset G$ Untergruppe.

6) $\operatorname{Im} f$ ist Untergruppe von H.

7) $\operatorname{Ker} f := f^{-1}(e_H)$, der Kern von f, ist Untergruppe von G.

Beweis:

1) $f(e_G) = f(e_G \cdot e_G) = f(e_G) * f(e_G)$, durch Multiplikation mit $f(e_G)^{-1}$ erhält man $f(e_G) = e_H$.

2) $f(x^{-1} \cdot x) = f(e_G) = e_H = f(x^{-1}) \cdot f(x)$, aus der Eindeutigkeit der Inversen folgt $f(x)^{-1} = f(x^{-1})$.

3) Ist f bijektiv, so existiert die Umkehrabb $f^{-1}: H \to G$.
Seien $u, v \in H$, setze $x = f^{-1}(u)$, $y = f^{-1}(v)$, dann gilt

$$f^{-1}(u * v) = f^{-1}(f(x) * f(y)) =$$
$$f^{-1}(f(x \cdot y)) = id_G(x \cdot y) =$$

$x \cdot y = f^{-1}(u) \cdot f^{-1}(v)$.

4) Seien $u, v \in f(U) \Rightarrow$
$\exists\, x, y \in U : f(x) = u,\ f(y) = v$.
Da U Untergruppe ist, gilt
$xy \in U \Rightarrow f(xy) = f(x) * f(y) =$
$u * v \in f(U)$.
Auch $x^{-1} \in U$ und damit $f(x^{-1}) \overset{2)}{=}$
$f(x)^{-1} = u^{-1} \in f(U)$.
Da $U \neq \emptyset$ ist $f(U) \neq \emptyset$, damit
ist das Untergruppenkriterium 1.8.4
erfüllt und $f(U) \subset H$ ist Untergruppe

5) genauso

6) folgt aus 4), da G Untergruppe von G ist.

7) folgt aus 5), da $(\{e_H\}, *)$ Untergruppe von H ist. □

2.1.15 Lemma

Sei $f : (G, \circ) \longrightarrow (H, *)$ Morphismus,
f injektiv $\Leftrightarrow$ $\ker f = \{e_G\}$

Beweis: „$\Rightarrow$" Da $f(e_G) = e_H$, ist $e_G \in \ker f$. Für $x \in \ker f$ gilt $f(x) = e_H \Rightarrow f(x) = f(e_G)$

$\Rightarrow x = e_G$, da f injektiv

$\Rightarrow \ker f = \{e_G\}$.

„$\Leftarrow$" Seien $x, y \in G$ mit $f(x) = f(y)$

$\Rightarrow e_H = f(x) * f(y)^{-1} =$

$f(x) * f(y^{-1}) = f(x \cdot y^{-1})$

$\Rightarrow x \cdot y^{-1} \in \ker f = \{e_G\}$

$\Rightarrow x y^{-1} = e_G \Rightarrow x = y$.

□

2.2 Faktorgruppen

2.2.1 Def Sei G eine Gruppe und $\sim$ eine Äquivalenzrelation auf G.
$\sim$ heißt mit der Gruppenstruktur verträglich, falls $\forall x, y, z \in G$:
$x \sim y \Rightarrow zx \sim zy$.

2.2.2 Def Sei $U \subset G$ eine Untergruppe.

Für U definieren wir eine Äquivalenzrelation auf G durch

$$x \sim y \quad :\Longleftrightarrow \quad x^{-1}y \in U$$

für $x, y \in G$.

2.2.3 Lemma Die Relation $\sim$ ist eine mit der Gruppenstruktur verträgliche Äquivalenzrelation.
Eine Äquivalenzklasse ist

$$[x] = x \cdot U := \{x \cdot u \mid u \in U\}$$

Beweis:

Reflexivität: $x \sim x$, da $x^{-1}x = e \in U$

Symmetrie: $x \sim y \Rightarrow x^{-1}y \in U \Rightarrow$

$$(x^{-1}y)^{-1} = y^{-1}(x^{-1})^{-1} = y^{-1}x \in U$$

$$\Rightarrow y \sim x$$

Transitivität: $x \sim y,\ y \sim z \Rightarrow$

$x^{-1}y,\ y^{-1}z \in U \Rightarrow (x^{-1}y)\cdot(y^{-1}z) =$

$$x^{-1}(yy^{-1})z = x^{-1}ez = x^{-1}z \in U$$

$$\Rightarrow x \sim z$$

Verträglich: $x \sim y \Rightarrow x^{-1}y \in U \Rightarrow$

$x^{-1}z^{-1}zy = (zx)^{-1}zy \in U \Rightarrow$

$zx \sim zy$.

Sei $[x]$ eine Äquivalenzklasse,

$y \in [x] \Rightarrow x \sim y \Rightarrow x^{-1}y \in U$,

setze $u := x^{-1}y$, dann ist $y = xu$

$\Rightarrow [x] \subset x \cdot U$.

Sei $y \in x \cdot U \Rightarrow y = x \cdot u$ für ein

$u \in U \Rightarrow x^{-1}y = u \in U \Rightarrow$

$y \in [x]$

$\Rightarrow [x] = x \cdot U$. □

Die Menge aller Äquivalenzklassen wird mit G/U bezeichnet,

$x \cdot U$ heißt Restklasse von x modulo U.

Bsp: $G = \mathbb{Z}$, $U = n\mathbb{Z}$, $G/U = \mathbb{Z}/n\mathbb{Z}$

Eine Äquivalenzklasse $[x]$ ist die Restklasse $\{y \mid y \equiv x \bmod n\}$.

$\mathbb{Z}/n\mathbb{Z}$ erbt die Gruppenstruktur von $\mathbb{Z}$, i.e. die Verknüpfung $[a] + [b] = [a+b]$ ist wohldefiniert.

Das funktioniert nicht für beliebige U, sondern nur für Normalteiler:

2.2.4 Def Eine Untergruppe $U \subset G$ heißt normal oder Normalteiler falls

$\forall x \in G, u \in U$ gilt

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

Dies ist äquivalent zu:

$\forall x \in G, u \in U$ gilt

$$xux^{-1} \in U.$$

Ist G abelsch, so ist jede Untergruppe Normalteiler.

Bsp 1) $n\mathbb{Z}$ ist Normalteiler.

2) $U = \{id, (12)\} \subset S_3$ ist kein Normalteiler, denn für $b = (23) \in S_3$ gilt $b \circ (12) \circ b^{-1} = (23)(12)(23)$

$$= (13) \notin U$$

2.2.5 Satz

Sei $(G, \cdot)$ eine Gruppe.

1) Eine Untergruppe $U \subset G$ ist Normalteiler $\Longleftrightarrow$ auf G/U ist die Operation

$$[x] \cdot [y] = [xy] \in G/U$$

wohldefiniert.

2) Ist $U \subset G$ Normalteiler, dann ist $(G/U, \cdot)$ mit der in 1) definierten Verknüpfung eine Gruppe mit Neutralem $[e] = U$, für Inverse gilt $[x]^{-1} = [x^{-1}]$.

Man nennt G/U die <u>Faktorgruppe</u> von G nach U.

Die Restklassenabbildung

$$\pi : G \longrightarrow G/U : x \longmapsto [x]$$

ist ein Gruppenhomomorphismus mit $\ker(\pi) = U$.

Beweis:

1) „$\Rightarrow$" Sei U ein Normalteiler, $[x], [y] \in G/U$. Sei $x' \in [x]$, $y' \in [y]$ $\Rightarrow$ $x' = xu$, $y' = yv$ für $u, v \in U$.

$\Rightarrow$ $x'y' = xuyv$.

Wir wollen zeigen, $x'y' \in [x \cdot y] = xyU$, also $xuyv \in xyU$. Da $v \in U$ ist dies äquivalent zu

$xuy \in xyU \Leftrightarrow uy \in yU$

Das gilt, da U Normalteiler ist.

„$\Leftarrow$" Sei $x \in G$, $u \in U$.

$$U = e \cdot U = [e] = [x \cdot x^{-1}]$$

$$\overset{\text{n.V.}}{=} [x] \cdot [x^{-1}] = [x \cdot u] \cdot [x^{-1}]$$

$$= [x \cdot u \cdot x^{-1}]$$

also ist $xux^{-1} \in U$ und U ist Normalteiler.

2) Wegen 1) ist die Operation wohldefiniert.

$[e] \cdot [x] = [e \cdot x] = [x]$, also ist $[e] = U$ Neutrales.

$[x^{-1}] \cdot [x] = [x^{-1} x] = [e]$,

also ist $[x^{-1}]$ Inverses zu x.

$$\pi(x \cdot y) = [x \cdot y] = [x] \cdot [y]$$
$$= \pi(x) \cdot \pi(y)$$

$$\ker(\pi) = \{x \in G \mid [x] = [e] = U\}$$
$$= U.$$

□

Bsp $n\mathbb{Z} \subset \mathbb{Z}$ ist Normalteiler

Die Addition in $\mathbb{Z}/n\mathbb{Z}$ ist wohldefiniert.

Wir schreiben $\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z}$.

2.2.6 Satz (Homomorphiesatz)

Ist $f: G \to H$ ein Morphismus, dann gilt:

1) $\ker(f)$ ist Normalteiler von G

2) Die durch f induzierte Abb.

$$\tilde{f}: G/\ker f \longrightarrow \operatorname{Im} f:$$
$$[x] \longmapsto f(x)$$

ist wohldefiniert und ein Isomorphismus.

Beweis:

1) Sei $u \in \ker(f)$, $x \in G$ $\Rightarrow$

$$f(xux^{-1}) = f(x) f(u) f(x)^{-1}$$
$$= f(x) e_H f(x)^{-1} = f(x) f(x)^{-1} = e_H$$

$\Rightarrow xux^{-1} \in \ker(f)$

Damit ist $\ker(f)$ Normalteiler.

2) Sei $[x] = [x'] \in G/\ker f$

$\Rightarrow x \sim x' \Rightarrow x^{-1}x' \in \ker f$

$\Rightarrow e_H = f(x^{-1}x') = f(x)^{-1} f(x')$

$\Rightarrow f(x) = f(x')$

Also ist $\tilde{f}$ wohldefiniert.

$\tilde{f}([x]\cdot[y]) = \tilde{f}([xy]) = f(xy) = f(x)\,f(y) = \tilde{f}([x])\,\tilde{f}([y])$

also ist $\tilde{f}$ Morphismus.

$\tilde{f}$ ist offensichtlich surjektiv.

Seien $[x], [y] \in G/\ker f$ mit

$f(x) = \tilde{f}([x]) = \tilde{f}([y]) = f(y)$

$\Rightarrow e_{\#} = f(x)^{-1} f(y) = f(x^{-1})f(y)$

$= f(x^{-1}y) \Rightarrow x^{-1}y \in \ker f$

$\Rightarrow x \sim y \Rightarrow [x] = [y]$, also

ist $\tilde{f}$ injektiv. □

2.3 Erzeugnisse und zyklische Gruppen

2.3.1 Def Sei G eine Gruppe, $S \subset G$ eine Teilmenge.

Dann ist

$$\langle S \rangle := \bigcap_{\substack{S \subseteq U \subseteq G \\ U \text{ Untergruppe}}} U$$

die von S erzeugte Untergruppe.

2.3.2 Lemma:

$\langle S \rangle = \{$ Wörter in S bzw. den Inversen der Elemente von $S\}$

Beweis:

„$\subseteq$", da die rechte Seite Untergruppe U mit $S \subseteq U$ ist

„$\supseteq$", die rechte Seite ist in jeder Untergruppe, die S enthält, und daher auch im Schnitt. □

Bsp

1) $GL_n(K)$ (die Gruppe der invertierbaren $n \times n$-Matrizen über einem Körper K) wird erzeugt von Elementarmatrizen, da man jede Matrix vollen Rangs mit Elementarmatrizen (elementaren Zeilenumformungen) auf die reduzierte Zeilenstufenform, also die

Einheitsmatrix $\mathbb{1}_n$, bringen kann.

2) $\mathbb{Z}$ wird von 1 erzeugt.

3) S_n wird von Nachbartranspositionen erzeugt (siehe ggf. Lineare Algebra 1).

4) $\mathbb{Z}/n\mathbb{Z}$ wird von $[1]$ erzeugt.

2.3.3 Def Sei G eine Gruppe,

$K = \{ \underbrace{(ab)(ba)^{-1}}_{= aba^{-1}b^{-1}} / a, b \in G \}$ ist

die Menge der Kommutatoren in G,

$[G,G] := \langle K \rangle$ die von K erzeugte Kommutatorengruppe.

Bemerkung: $[G,G] = \{e\} \Leftrightarrow G$ abelsch

2.3.4 Lemma $[G,G]$ ist ein Normalteiler.

Beweis: Sei $g \in G$, $u = aba^{-1}b^{-1} \in [G,G]$.
Dann gilt

$$gug^{-1} = gaba^{-1}b^{-1}g^{-1} =$$

$$ga(g^{-1}g)b(g^{-1}g)a^{-1}(g^{-1}g)b^{-1}g^{-1} =$$

$$gag^{-1}\,gbg^{-1}\,ga^{-1}g^{-1}\,gb^{-1}g^{-1} =$$

$$gag^{-1}\,gbg^{-1}\,(gag^{-1})^{-1}\,(gbg^{-1})^{-1} \in [G,G].$$

Mit Produkten von Kommutatoren verfährt man analog. □

2.3.5 Korollar Sei G eine Gruppe, U ein Normalteiler.
G/U ist abelsch $\iff$ $U \supset [G,G]$
Insbesondere ist $G/[G,G]$ abelsch.

Beweis: $[a][b] = [b][a]$ $\forall a,b$ $\iff$
$[a][b][a]^{-1}[b]^{-1} = [e]$ $\forall a,b$ $\iff$
$[aba^{-1}b^{-1}] = [e]$ $\forall a,b$ $\iff$
$U = e \cdot U = [e] \supset \langle K \rangle = [G,G]$ □

2.3.6 Def

Eine Gruppe G heißt <u>zyklisch</u>, falls $\exists\, g \in G : G = \langle g \rangle$

<u>Bsp</u>: $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$ sind zyklisch.

2.3.7 Def

Sei $g \in G$, $\operatorname{ord}(g) := |\langle g \rangle|$ heißt die <u>Ordnung</u> von g.

<u>Bsp</u>:

1) Für $[2] \in \mathbb{Z}/6\mathbb{Z}$ ist $\operatorname{ord}([2]) = 3$, denn $\langle [2] \rangle = \{[0], [2], [4]\}$

2) Die Ordnung eines k-Zykels in S_n ist k.

2.3.8 Satz (Lagrange)
Sei G eine endliche Gruppe, U eine Untergruppe. Dann gilt

$$|G| = |U| \cdot |G/U|$$

Insbesondere ist die Ordnung einer Untergruppe ein Teiler der Gruppenordnung.

Beweis: Die Äquivalenzrelation für U (siehe Def. 2.2.2) zerlegt G disjunkt in $|G/U|$ Äquivalenzklassen. Wegen 2.2.3 hat jede Klasse die Form $x \cdot U$, also $|x \cdot U| = |U|$ Elemente. □

2.3.9 Korollar Sei G endlich, $g \in G$. Dann gilt $\operatorname{ord}(g) \mid |G|$.

2.3.10 Korollar Sei G eine Gruppe von Primzahlordnung. Dann ist G zyklisch.

Beweis: Sei $g \in G \setminus \{e\}$. Da $\langle g \rangle \subset G$ Untergruppe ist, folgt $\text{ord}(g) = |\langle g \rangle| \mid |G|$ $\overset{\text{Primzahl}}{\Rightarrow}$ $|\langle g \rangle| = |G| \Rightarrow \langle g \rangle = G$. □

2.3.11 Satz Sei G zyklisch.
Falls G unendliche Ordnung hat, so ist $G \cong \mathbb{Z}$.
Falls $|G| = m$, so ist $G \cong \mathbb{Z}_m$.

Beweis:
Sei $G = \langle g \rangle$.
Setze $f(n) := g^n$, dann ist $f: \mathbb{Z} \longrightarrow G$ ein Gruppenhomomorphismus (denn $f(n+m) = g^{n+m} = g^n \cdot g^m = f(n) \cdot f(m)$).
f ist surjektiv.
Damit ist $\ker(f) \subset \mathbb{Z}$ eine Untergruppe, also $\ker(f) = m\mathbb{Z}$ für ein m.

Falls $m=0$ ist $G \cong \mathbb{Z}$, falls $m \neq 0$ ist $G \cong \mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m$.

Der erste Fall tritt ein genau dann, wenn $|G| = \infty$, der zweite genau dann, wenn G endlich. □

2.3.12 Satz Sei G zyklisch. Jede Untergruppe von G ist zyklisch.

Beweis: Sei $G = \langle g \rangle$ und $U = \{e\}$. Sei

$a := \min \{ j \in \mathbb{N} \setminus \{0\} \mid g^j \in U \}$.

Beh: $U = \langle g^a \rangle$

"$\supset$" klar.

"$\subset$" Sei $u \in U$. Da $u \in G$

$\exists b \in \mathbb{Z}: u = g^b$.

Schreibe b nach Division mit Rest als $b = q \cdot a + r$ mit $0 \leq r < a$.

Dann gilt $u = g^b = g^{q \cdot a + r} =$

$g^{qa} \cdot g^r = (g^a)^q \cdot g^r \Rightarrow$

$g^r = u \cdot (g^a)^{-q} \in U$

$\Rightarrow \quad r = 0 \quad \Rightarrow \quad u = (g^a)^q \in \langle g^a \rangle$.

□

2.3.13 Satz (Untergruppen zyklischer Gruppen)

Sei G eine Gruppe, $g \in G$.

1) $\operatorname{ord}(g) = \min\{n \in \mathbb{N}_{>0} \mid g^n = e\}$

Insbesondere $g^{\operatorname{ord}(g)} = e$,

$\langle g \rangle = \{e, g, g^2, \dots, g^{\operatorname{ord}(g)-1}\}$

2) $g^n = e \iff \operatorname{ord}(g) \mid n$

3) Hat g endliche Ordnung und ist $j \in \mathbb{N}$, so gilt

$$\operatorname{ord}(g^j) = \frac{\operatorname{ord}(g)}{ggT(\operatorname{ord}(g), j)}$$

4) Hat g endliche Ordnung n und ist $d \in \mathbb{N}$, $d \mid n$, so sind die Elemente von Ordnung d mit $d \mid d$ in der von g erzeugten zyklischen Untergruppe genau die $g^{k \cdot \frac{n}{d}}$ mit $k \in \mathbb{N}$.

Dabei hat $g^{k \cdot \frac{n}{d}}$ Ordnung d

$\Leftrightarrow \quad ggT(k, d) = 1.$

5) Ist G zyklisch der Ordnung n, so gibt es zu jedem Teiler $d | n$ genau eine Untergruppe U_d der Ordnung d.

Beweis:

1) $\langle g \rangle$ ist zyklisch, mit 2.3.7 ergibt sich $\langle g \rangle \cong \begin{cases} \mathbb{Z} \\ \mathbb{Z}_m \end{cases}$

Falls $\langle g \rangle \cong \mathbb{Z}$, so ist $ord(g) = \infty$ und $\{ n \in \mathbb{N}_{>0} \mid g^n = e \}$ ist unbeschränkt, da $f: \mathbb{Z} \to G: 1 \mapsto g$ Isomorphismus ist und $g^n = f(n) \neq e$ für $n \neq 0$.

Falls $\langle g \rangle \cong \mathbb{Z}_m$, so ist $ord(g) = m$ und $\mathbb{Z}_m \longrightarrow G: [1] \longmapsto g$ ist Isomorphismus.

Da $m = \min \{ n \mid \overbrace{[1] + \dots + [1]}^{n \text{ Summanden}} = 0 \}$ ist auch $m = \min \{ n \mid g^n = e \}$.

2) „$\Rightarrow$" $g^n = e \Rightarrow \min\{j \mid g^j = e\} \leq n$
$\Rightarrow \operatorname{ord}(g) \leq n$. Sei $\operatorname{ord}(g) = m$, schreibe
$n = q \cdot m + r$, $0 \leq r < m$ (Division mit Rest).
Dann ist $e = g^n = g^{q \cdot m + r} = (g^m)^q \cdot g^r$
$= e \cdot g^r$, da $r < m$ und $g^r = e$ folgt
$r = 0 \Rightarrow n = q \cdot m \Rightarrow m \mid n \Rightarrow$
$\operatorname{ord}(g) \mid n$.
„$\Leftarrow$" $\operatorname{ord}(g) \mid n \Rightarrow \exists\, q: n = q \cdot \operatorname{ord}(g)$
$\Rightarrow g^n = g^{q \cdot \operatorname{ord}(g)} = (g^{\operatorname{ord}(g)})^q = e$

3) Sei $m = \operatorname{ord}(g)$. Sei $j \in \mathbb{N}$
und $d = ggT(m, j)$

Beh: $\frac{m}{d} = \min\{k \in \mathbb{N}_{>0} \mid (g^j)^k = e\}$
$= \operatorname{ord}(g^j)$

Da $(g^j)^{\frac{m}{d}} = (g^m)^{\frac{j}{d}} = e$ ist
$\frac{m}{d} \in \{k \mid (g^j)^k = e\}$
$\Rightarrow \operatorname{ord}(g^j) \leq \frac{m}{d}$.

Sei $r \in \{k \mid (g^j)^k = e\} \Rightarrow$

$(g^j)^r = e \Rightarrow g^{jr} = e$

$\Rightarrow m \mid jr \Rightarrow jr$ ist ein gemeinsames Vielfaches von m und j. Damit folgt

$$\frac{mj}{d} = kgV(m,j) \mid jr.$$

Insbesondere $\frac{m}{d} \mid r$.

$\Rightarrow \frac{m}{d} \mid \min\{k \mid (g^j)^k = e\}$

$\Rightarrow \frac{m}{d} \mid ord(g^j)$

Da auch $ord(g^j) \leq \frac{m}{d} \Rightarrow$

$\frac{m}{d} = ord(g^j)$.

4) Sei d ein Teiler von n, d' ein Teiler von d und $g^j \in \langle g \rangle$ ein Element der Ordnung

$$d' = \frac{n}{ggT(n,j)}.$$

$$\Rightarrow \frac{n}{ggT(n,j)} \mid d \Rightarrow \frac{n}{d} \mid ggT(n,j)$$

Da $ggT(n,j) \mid j$ folgt $\frac{n}{d} \mid j$

$\Rightarrow \exists k: j = k \cdot \frac{n}{d}$.

Damit ist $g^j = g^{k\frac{n}{d}}$ in der gewünschten Form dargestellt.

Sei umgekehrt ein Element der Form $g^{k \cdot \frac{n}{d}}$ gegeben, wir wollen zeigen, daß $ord(g^{k\frac{n}{d}}) \mid d$.

Es gilt $ord(g^{k\frac{n}{d}}) = \frac{n}{ggT(n, k\frac{n}{d})}$,

und $\frac{n}{d} \mid ggT(n, k\frac{n}{d})$

$\Rightarrow \frac{n}{ggT(n, k\frac{n}{d})} \mid d$

$\Rightarrow ord(g^{k\frac{n}{d}}) \mid d$.

Es gilt $ord(g^{k\frac{n}{d}}) = d \iff$

$\frac{n}{ggT(n, k\frac{n}{d})} = d \iff \frac{n}{d} = ggT(n, k\frac{n}{d})$

$= ggT(d \cdot \frac{n}{d}, k \cdot \frac{n}{d}) \iff$

$ggT(k, d) = 1$.

5) Zu jedem Teiler d/n betrachte $U_d := \langle g^{\frac{n}{d}} \rangle$. Diese Untergruppe hat Ordnung d, da

$$ord(g^{\frac{n}{d}}) = \frac{n}{ggT(n, \frac{n}{d})} = d.$$

Wegen 4) sind alle Elemente der Ordnung d (da d/d) von der Form $g^{k\frac{n}{d}}$ und damit in U_d enthalten.

Sei U' eine Untergruppe der Ordnung d. Wegen 2.3.8 ist U' zyklisch $\Rightarrow \exists\, h \in G$, $ord(h) = d$, $U' = \langle h \rangle$.

Dann ist aber $h \in U_d \Rightarrow U' \subset U_d \Rightarrow U' = U_d$.

□

2.3.14 Def Sei G eine Gruppe. Wir definieren auf $\{U \mid U$ ist Untergruppe von $G\}$ eine Teilordnung durch $U \leq U' :\Leftrightarrow U \subset U'$

Wir stellen diese Relation als Diagramm (Verband) dar.

Für $n \in \mathbb{N}_{>0}$ definieren wir auf $\{d \mid d \mid n\}$ eine Teilordnung durch $d \leq d' :\Leftrightarrow d \mid d'$.

2.3.15 Korollar

Der Untergruppenverband einer zyklischen Gruppe der Ordnung n ist gleich dem der Teiler von n.

Beweis:

Sei $G = \langle g \rangle$. Jede Untergruppe ist von der Form $U_d = \langle g^{\frac{n}{d}} \rangle$

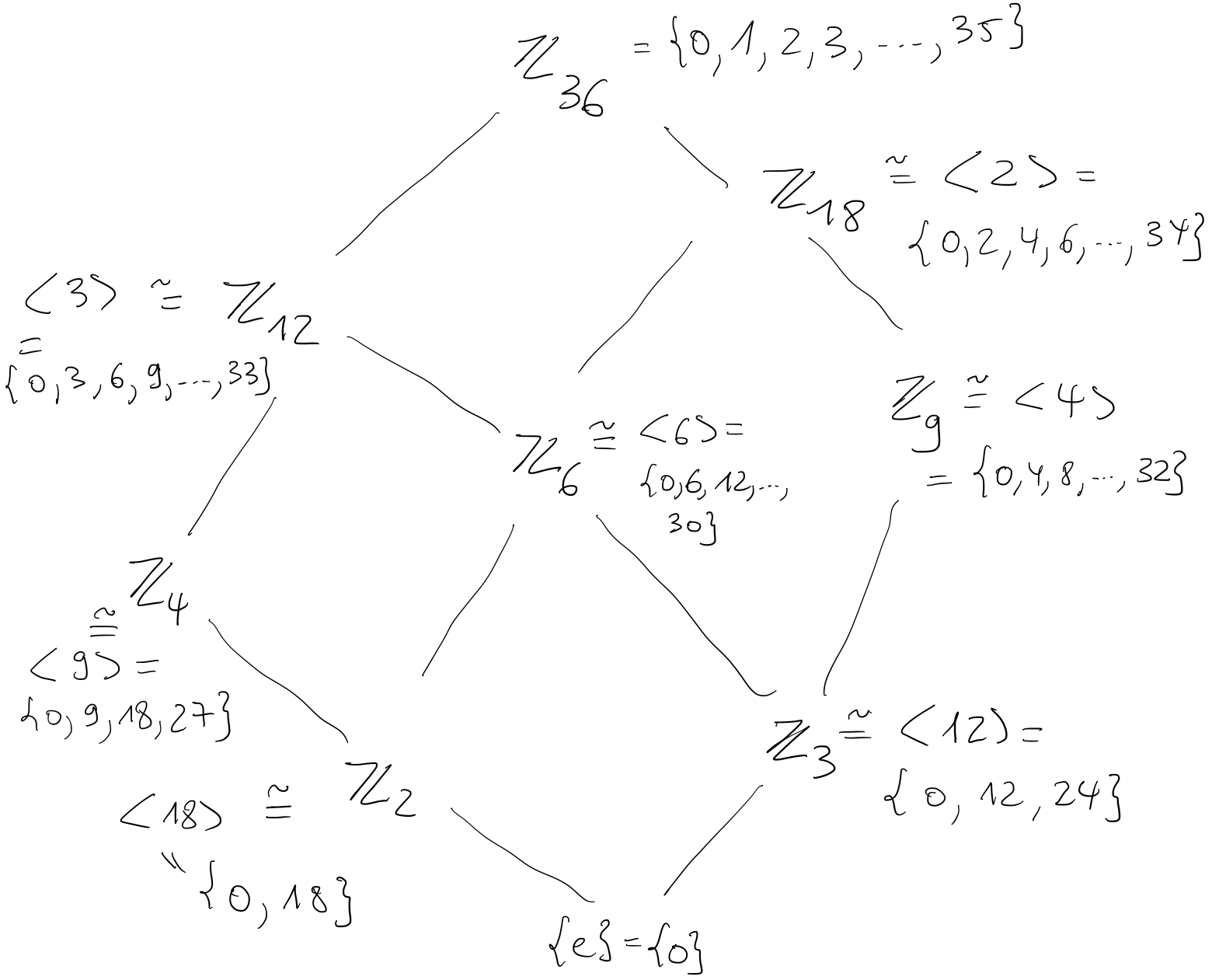
$= \{ g^{k \cdot \frac{n}{d}} \mid k \in \mathbb{N} \}$.

Daher gilt $U_d \subset U_{d'} \iff$

$\frac{n}{d}$ ist ein Vielfaches von $\frac{n}{d'}$

$\iff d \mid d' \iff d \leq d'$ □

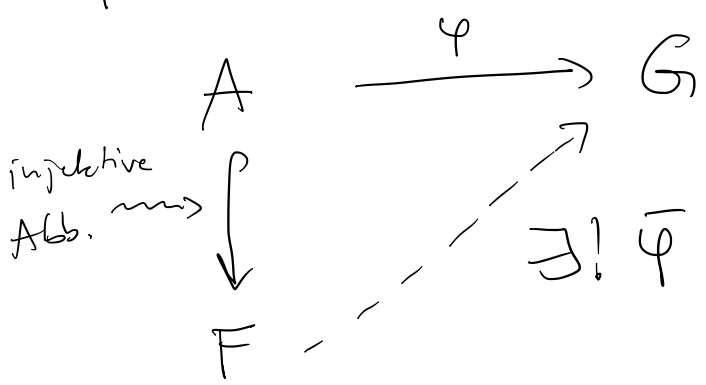
Bsp Der Untergruppenverband von $\mathbb{Z}_{36}$ ist



2.4 Freie Gruppen und Relationen

Wir verallgemeinern / abstrahieren Bsp. 2.1.8:

2.4.1 Def Sei A eine endliche Menge.
Eine Gruppe F heißt *frei erzeugt von A*, falls F folgende universelle Eigenschaft erfüllt:
$\forall$ Gruppe G und Abb $\varphi: A \to G$
$\exists!$ Morphismus $\bar{\varphi}: F \to G$, der φ erweitert:



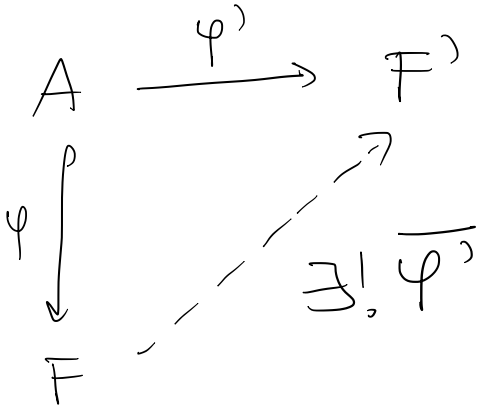
Eine Gruppe heißt frei, wenn eine Menge $A \subset F$ existiert, die F frei erzeugt.

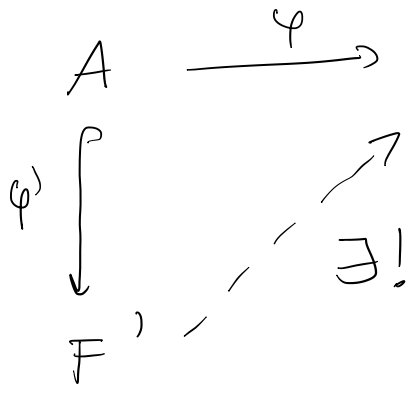
Bsp $\mathbb{Z}$ ist frei, $\mathbb{Z}$ wird frei erzeugt von 1. $\mathbb{Z}$ wird nicht von $\{2,3\}$ frei erzeugt, aber $\mathbb{Z} = \langle 2,3 \rangle$.

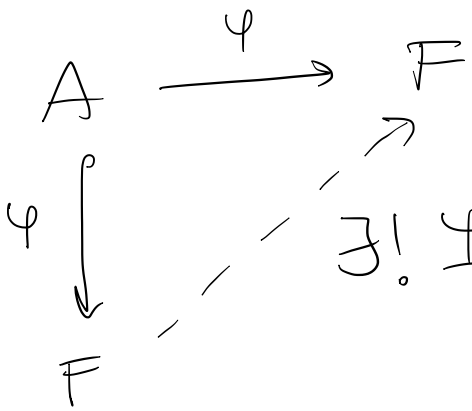
Insbesondere enthält nicht jede erzeugende Teilmenge eine frei erzeugende Teilmenge.

2.4.2 Prop (freie Gruppe, Eindeutigkeit)
Sei A eine endliche Menge. Dann existiert höchstens eine frei von A erzeugte Gruppe F (bis auf kanonische Isomorphie).

Beweis: Seien F, F' frei erzeugt von A.







$\Psi = id_F$ lässt das Diagramm kommutieren,
$\Psi = \bar{\varphi} \circ \bar{\varphi}'$ auch,
aus der Eindeutigkeit von Ψ folgt
$id_F = \bar{\varphi} \circ \bar{\varphi}'$. Genauso $id_{F'} = \bar{\varphi}' \circ \bar{\varphi}$.
$\Rightarrow F \cong F'$. □

Kanonisch: die Isomorphismen $F \to F'$, $F' \to F$ sind id auf S und sind die einzigen Isomorphismen, die $id|_S$ erweitern, wegen der Eindeutigkeit in der universellen Eigenschaft.

2.4.3 Satz (freie Gruppe, Existenz)

Sei A eine endliche Menge. Dann existiert eine von A frei erzeugte Gruppe.

Beweis: Wir zeigen, dass die Gruppe aus Bsp. 2.18 die universelle Eigenschaft erfüllt:

F = Menge der Wörter in A und $A^{-1}/\sim$

$= \{a_1 \cdots a_n \mid n \in \mathbb{N}, a_i \in A \cup A^{-1}\}/\sim$

wobei $\forall$ Wörter x, y, $a \in A$:

$$xaa^{-1}y \sim xy, \quad xa^{-1}ay \sim xy$$

Hintereinanderschreiben ist assoziativ, das leere Wort ε ist neutrales, in umgekehrter Reihenfolge schreiben und invertieren liefert Inverse. $A \subset F$.

Sei G eine weitere Gruppe, $\varphi: A \to G$ eine Abb.

Wir konstruieren rekursiv eine Abb φ^* von der Menge der Wörter durch:

$$\varepsilon \longmapsto e$$
$$a \cdot x \longmapsto \varphi(a) \cdot \varphi^*(x)$$
$$a^{-1} \cdot x \longmapsto \varphi(a)^{-1} \cdot \varphi^*(x)$$

$\forall a \in A$, Wort x.

Nach Def ist φ^* kompatibel mit der Äquivalenzrelation $\sim$ auf der Menge der Wörter, und liefert damit $\overline{\varphi} : F \longrightarrow G$, die Morphismus ist. □

2.4.4 Korollar Sei F frei erzeugt von A, dann ist $\langle A \rangle = F$.

Beweis: Die freie Gruppe aus Bsp. 2.18 bzw. Satz 2.4.3 ist von A erzeugt, und sie ist eindeutig. □

2.4.5 Prop Sei F eine freie Gruppe. Alle freien Erzeugendensysteme haben die gleiche Anzahl, den Rang von F.

Beweis: F sei frei erzeugt von A, $|A| = n$. Die Menge der Homomorphismen $F \to \mathbb{Z}_2$, $\mathrm{Hom}(F, \mathbb{Z}_2)$, erfüllt $|\mathrm{Hom}(F, \mathbb{Z}_2)| = 2^n$, also hängt n nur von F ab und nicht von A. □

Wir schreiben F_n für die von n Elementen frei erzeugte Gruppe.

Bsp $F_1 \cong \mathbb{Z}$

Bem 1) $\mathbb{Z} \times \mathbb{Z} = \mathbb{Z}^2$ ist nicht frei erzeugt von $\binom{1}{0}, \binom{0}{1}$, denn $\binom{1}{0} + \binom{0}{1} = \binom{0}{1} + \binom{1}{0}$ ist eine Relation, die zusätzlich zu den Inversen $\binom{1}{0} + \binom{-1}{0} = e$ ... erfüllt ist.

Man kann z. B. nicht $\binom{1}{0} \mapsto (12)$, $\binom{0}{1} \mapsto (13) \in S_3$ abbilden, denn sonst

$\binom{1}{0} + \binom{0}{1} \mapsto (12) \circ (13) \neq (13) \circ (12) \leftarrow \binom{0}{1} + \binom{1}{0}$

nicht wohldefiniert.

In der Tat ist $\mathbb{Z}^2$ nicht frei.

2) Endliche Gruppen sind nicht frei, da ein Element g endliche Ordnung hat, also $\exists r: g^r = e$ und somit gibt es eine zusätzliche Relation. Man kann nicht $g \longmapsto 1 \in \mathbb{Z}$ abbilden, da

$g^r = e \longmapsto 0 \neq r = 1 + \cdots + 1$ nicht wohldefiniert.

$g^r = g \circ \cdots \circ g \longmapsto$

2.4.6 Korollar Eine Gruppe G ist endlich erzeugt $\Leftrightarrow$ $G \cong F_n / N$ für eine freie Gruppe F_n und einen Normalteiler N.

Beweis: „$\Leftarrow$" klar

„$\Rightarrow$" Sei $G = \langle A \rangle$, $|A| = n < \infty$.

Mit der universellen Eigenschaft finden wir $\Pi: F_n \longrightarrow G$, der surjektiv ist, da $G = \langle A \rangle$.

Setze $N = \ker(\Pi)$, dann folgt aus dem Homomorphiesatz $G \cong F_n / N$. □

2.4.7 Def

Sei G eine Gruppe, $A \subset G$.
$\langle A \rangle^{\triangleleft}$ ist der kleinste Normalteiler von G, der A enthält:

$$\langle A \rangle^{\triangleleft} = \bigcap_{\substack{A \subset N \subset G, \\ N \text{ Normalteiler}}} N .$$

2.4.8 Lemma

$$\langle A \rangle^{\triangleleft} = \{ g_1 \alpha_1^{\varepsilon_1} g_1^{-1} \circ \cdots \circ g_m \alpha_m^{\varepsilon_m} g_m^{-1} \mid m \in \mathbb{N},\ \varepsilon_i \in \{\pm 1\},\ g_i \in G,\ \alpha_i \in A \}$$

Siehe Lemma 2.3.2.

2.4.9 Def (Erzeuger und Relatoren)

$$\langle A \mid R \rangle := F / \langle R \rangle^{\triangleleft},$$

wobei F die frei von A erzeugte Gruppe ist, ist die Gruppe erzeugt von A mit Relatoren R.
$\langle A \mid R \rangle$ heißt Präsentation der Gruppe.

Bsp

1) $\langle x \mid x^n \rangle \cong \mathbb{Z}_n$

2) $\langle x, y \mid xyx^{-1}y^{-1} \rangle \cong \mathbb{Z}^2$

↝ man schreibt manchmal auch $xyx^{-1}y^{-1} = e$ oder $xy = yx$

$$x \longmapsto \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$
$$y \longmapsto \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

3) $\langle x, y \mid xyx^{-1} = y^2,\ yxy^{-1} = x^2 \rangle$

$= \{e\}$:

$$x = x(y(x^{-1}x)y^{-1}) = (xyx^{-1})xy^{-1}$$
$$= y^2xy^{-1} = y(yxy^{-1}) =$$
$$yx^2 \Rightarrow e = yx \Rightarrow$$
$$y = x^{-1}$$
$$y^{-2} = x^2 = yxy^{-1} = yy^{-1}y^{-1} = y^{-1}$$
$$\Rightarrow y = e \Rightarrow x = e.$$

4) $\langle a, b \mid a^2 = b^2 = (ab)^3 = e \rangle \cong S_3$:

$a \longmapsto (12)$, $b \longmapsto (13)$

$ab \longmapsto (12)(13) = (132)$, es gilt $(132)^3 = e$, dies ist verträglich mit der Relation $(ab)^3 = e$.

Die Gruppe $G = \langle a, b \mid a^2 = b^2 = (ab)^3 = e \rangle$ besteht aus Wörtern in a, b, wobei a und b abwechselnd hintereinander kommen.

Es gilt $(bab)^2 = babbab = e$

und $(aba)(bab) = (ab)^3 = e$

$\Rightarrow aba = (bab)^{-1} = bab$.

Möglichkeiten für Wörter außer a, b, e:

I. $abab \cdots ab$ II $abab \cdots aba$

III $baba \cdots ba$ IV $baba \cdots bab$

I Höchstens 2 Wiederholungen, da $(ab)^3 = e$.
Aber $abab = babb = ba$.
Also nur ab.

II $ababa = aabaa = b$
Also nur aba.

III Nur ba, IV $bab = aba$

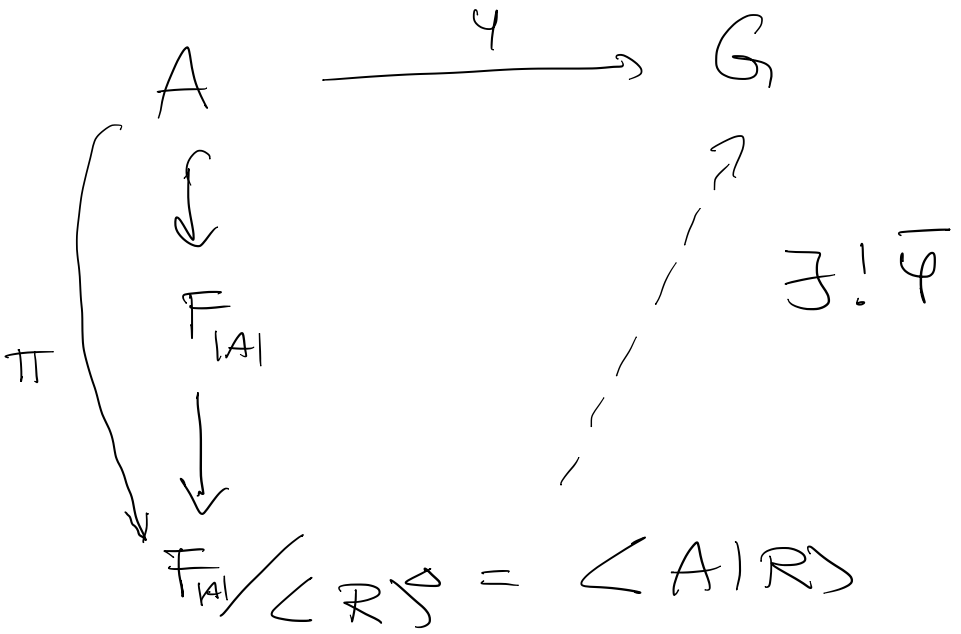
$\Rightarrow G = \{e, a, b, ab, ba, aba\}$

Die Zuordnung $a \mapsto (12)$,
$b \mapsto (13)$ liefert einen
Isomorphismus $G \longrightarrow S_3$

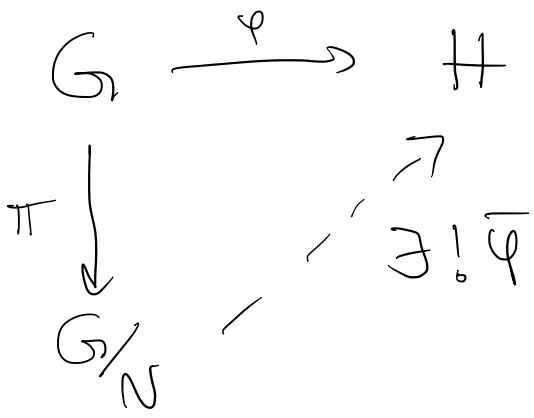
$$G = \{ e \;,\; a \;,\; b \;,\; ab \;,\; ba \;,\; aba \}$$
$$\downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow \quad \downarrow$$
$$S_3 = \{ id \;,\; (12) \;,\; (13) \;,\; (132) \;,\; (123) \;,\; (23) \}$$

Bem: Folgende universelle Eigenschaft
gilt für Gruppen, die durch
Erzeuger und Relationen gegeben sind:
$\forall$ Gruppen G, Abb $\varphi: A \to G$
mit $\varphi^*(r) = e$ in G $\forall r \in R$
(wobei φ^* den auf den Wörtern
konstruierten Morphismus aus Satz
2.4.3 (Existenz freie Gruppe) bezeichnet)
$\exists!$ Gruppenhomomorphismus
$\overline{\varphi}: \langle A \mid R \rangle \longrightarrow G$ mit

$\bar{\varphi} \circ \pi = \varphi$:



Dies folgt aus der universellen Eigenschaft für freie Gruppen, und für Faktorgruppen:
G/N, $\pi: G \to G/N$ erfüllen folgende universelle Eigenschaft: $\forall$ Gruppen H, Morphismen $\varphi: G \to H$ mit $N \subset \ker(\varphi)$ $\exists!\ \bar{\varphi}: G/N \to H$ mit $\bar{\varphi} \circ \pi = \varphi$:



Die universelle Eigenschaft für Faktorgruppen zeigt man wie beim Homomophie-satz, indem wir $\bar{\varphi}([g]) = \bar{\varphi}(g \cdot N) = \varphi(g)$ setzen.