§ 3 Konstruktionen von Gruppen

1. Erinnerung: normaler Abschluss

Ist G eine Gruppe, $N \subseteq G$ eine Untergruppe, dann sind äquivalent:

(i) $N \trianglelefteq G$

(ii) $gNg^{-1} = N$ für alle $g \in G$

(iii) $gNg^{-1} \subseteq N$ für alle $g \in G$

(iv) $gug^{-1} \in N$ für alle $g \in G, u \in N$

Γ (i) $\overset{\text{Def}}{\Leftrightarrow}$ (ii) $\Rightarrow$ (iii) $\Leftrightarrow$ (iv) klar

(iii) $\Rightarrow$ (ii): $gNg^{-1} \subseteq N$; $g^{-1}Ng \subseteq N \Rightarrow gNg^{-1} = N$ $\lrcorner$

Sei nun $A \subseteq G$ eine beliebige Teilmenge. Der normale Abschluss von A ist

$$\langle\langle A \rangle\rangle = \bigcap \{ N \trianglelefteq G \mid A \subseteq N \}$$

Offensichtlich gilt $A \subseteq \langle\langle A \rangle\rangle \trianglelefteq G$ und für jede Normalteiler $N \trianglelefteq G$ mit $A \subseteq N$ gilt $\langle\langle A \rangle\rangle \subseteq N$.

Andere Beschreibung des normalen Abschlusses: setze $A^* = A \cup \{1\} \cup A^{-1}$ wie in § 1.10. Dann gilt

$$\langle\langle A \rangle\rangle = \{ (g_1 a_1 g_1^{-1})(g_2 a_2 g_2^{-1}) \cdots (g_r a_r g_r^{-1}) \mid r \geq 1, a_j \in A^*, g_j \in G \}$$

denn: die rechte Seite ist eine Untergruppe, normal in G, und enthält A. Jeder Normalteiler $N \trianglelefteq G$, der A enthält, enthält auch die rechte Seite. $\square$

2. Präsentierung von Gruppen

Sei X eine Menge und sei $R \subseteq F(X)$ eine Teilmenge der freien Gruppe über X. Man schreibt

$$\langle X \mid R \rangle = F(X) / \langle\langle R \rangle\rangle$$

und nennt $\langle X \mid R \rangle$ eine Präsentierung mit Erzeugern $x \in X$ und Relatoren $r \in R$.

Idee dahinter: $\langle X \mid R \rangle$ ist die universelle Gruppe mit Erzeugendensystem X, in der die Gleichungen $r = 1$ für alle $r \in R$ gelten.

Bsp (a) $F(X) = \langle X \mid \emptyset \rangle$

(b) $k, \ell \geq 1 \rightsquigarrow \mathbb{Z}/k * \mathbb{Z}/\ell \cong \langle a, b \mid a^k, b^\ell \rangle$

(c) $\mathbb{Z} \oplus \mathbb{Z} \cong \langle a, b \mid [a, b] \rangle$

Universelle Eigenschaft von $\langle X \mid R \rangle$:
Wenn G eine Gruppe ist, $\lambda : X \to G$ eine Abbildung, und wenn für alle $r \in R$

gilt $F(\lambda)(r) = 1$, so gibt es ein eindeutiges Homomorphismus $\varphi : \langle X | R \rangle \to G$ mit

$$\begin{array}{ccc} F(X) & \xrightarrow{F(\lambda)} & G \\ & \pi \searrow \quad \nearrow \varphi & \\ & \langle X|R \rangle & \end{array} \qquad \varphi \circ \pi = F(\lambda)$$

⌜ Klar nach Homomorphiesatz, denn $\langle\langle R \rangle\rangle \subseteq \ker(F(\lambda))$ nach Voraussetzung. ⌟

Bem Jede Gruppe G läßt sich präsentieren. Ist nämlich $X \subseteq G$ ein Erzeugendensystem für G (z.B. $G = X$), so wähle $R \subseteq \ker(F(X) \to G) = N$ mit $\langle\langle R \rangle\rangle = N$, z.B. $R = N$. Es folgt

$$G \cong F(X)/N = \langle X | R \rangle .$$

3. Def Eine Gruppe G heißt endlich präsentiert (kurz: endlich präsentierbar), wenn es endliche Mengen X, $R \subseteq F(X)$ gibt mit $G \cong \langle X | R \rangle$

↑ ↑ beide endlich

Nicht jede endlich erzeugte Gruppe ist endlich präsentierbar!

4. Algorithmische Probleme

Sei $\langle X|R\rangle$ endlich präsentiert. Fragen:

- gibt es einen Algorithmus, der für jedes $w \in F(X)$ feststellt, ob $w \in \langle\langle R \rangle\rangle$?
  (Wortproblem)
- gibt es einen Algorithmus, der feststellt ob
  $\langle X|R\rangle = \{1\}$?
- gibt es einen Algorithmus, der feststellt, ob $\langle X|R\rangle$ endlich ist ?

Im allgemeinen lautet die Antwort in allen drei Fällen **nein** !

(P. Novikov 1955: das Wortproblem ist nicht lösbar)

Für manche Gruppen sind die drei Fragen aber beantwortbar, z.B. für freie Gruppen (klar) und für endlich erzeugte abelsche Gruppen.

5. Def Sei $\mathcal{E}$ eine gruppentheoretische Eigenschaft, z.B. $\mathcal{E}$ = "endlich", oder $\mathcal{E}$ = "endliche p-Gruppe".

Eine Gruppe G heißt residuell $\mathcal{E}$, wenn es für jedes $g \in G - \{1\}$ eine Gruppe H gibt, die Eigenschaft $\mathcal{E}$ besitzt, so wie ein Homomorphismus $\varphi: G \to H$ mit $\varphi(g) \neq 1$

Bsp (a) Jede Gruppe mit Eigenschaft $\mathcal{E}$ ist auch residuell $\mathcal{E}$; z.B. G endlich $\Rightarrow$ G residuell endlich

(b) $\mathbb{Z}$ ist residuell endlich, s.o. Denn: $z \in \mathbb{Z} - \{0\}$ wähle Primzahl p mit $p > |z|$ $\Rightarrow$ $z \not\equiv 0 \pmod p$ d.h. $\varphi(z) \neq 0$ in $\mathbb{Z}/p$

6. Satz Ist $G = \langle X \mid R \rangle$ endlich präsentiert und residuell endlich, so ist das Wortproblem in G lösbar.

Beweis: Sei $w \in F(X)$. Wir müssen algorithmisch feststellen, ob gilt $w \in \langle\langle R \rangle\rangle$.

Dazu starten wir gleichzeitig zwei Programme.

Program 1 zählt alle Elemente in $\langle\langle R \rangle\rangle$ auf und stoppt, wenn w dabei vorkommt.

Program 2 zählt alle endlichen Gruppen H auf, sowie alle Abbildungen $\chi : X \to H$ mit $R \leq \ker(F(\chi))$ und stoppt, wenn $F(\chi)(w) \neq 1$.

Da $\langle X | R \rangle$ residuell endlich ist, bricht eines der beiden Programme nach endlicher Zeit ab. Dann stoppt der Algorithmus. □

Wir bleiben noch kurz bei residuellen Eigenschaften.

7. Satz Jede residuell endliche (endlich erzeugte) Gruppe ist hopfsch.

[Erinn.: G hopfsch $\Leftrightarrow$ jeder Epimorphismus $\varphi : G \twoheadrightarrow G$ ist bijektiv/isomorphismus]]

Beweis Angenommen, das ist falsch. Sei G res. endlich, sei $\Psi : G \twoheadrightarrow G$ ein Epimorphismus mit $\Psi(g) = 1$ für ein $g \in G - \{1\}$.

Da G residuell endlich ist, gibt es $N \trianglelefteq G$ mit $[G : N] < \infty$ und $g \notin N$.

Die Menge $\mathrm{Hom}(G, G/N) = \{ \Psi : G \to G/N \mid \Psi \text{ Homom.} \}$ ist endlich, weil G/N endlich ist und

und G von der endlich Ring X erzeugt wird. Sei $m = \#\,\mathrm{Hom}(G, G/N)$, mit $\mathrm{Hom}(G, G/N) = \{\varphi_1, \dots, \varphi_m\}$ und $\varphi_1(x) = xN$ mit $\varphi_1(g) \neq 1$. Sei $s: G \to G$ Schnitt zu φ, d.h. $\varphi \circ s = id_G$.

Es folgt: $\varphi_j \circ \varphi = \varphi_k \circ \varphi \Rightarrow \varphi_j \circ \varphi \circ s = \varphi_k \circ \varphi \circ s$

$\Rightarrow \varphi_j = \varphi_k \Rightarrow j = k$,

also $\mathrm{Hom}(G, G/N) = \{\varphi_1 \circ \varphi, \dots, \varphi_m \circ \varphi\}$.

Ab. $\varphi_j \circ \varphi(g) = \varphi_j(1)$ für alle j ↯ mit $\varphi_1(g) \neq 1$ □

Wir wissen jetzt, dass F_m residuell endlich und damit hopfsch ist.

8. Lemma Sei R ein kommutativer Ring, sei $m \geq 1$. Dann ist

$$U(m,R) = \left\{ \begin{pmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \in R^{m \times m} \right\}$$

eine Gruppe. Ist $\# R = p^l$, p Primzahl, so ist $U(m,R)$ eine p-Gruppe.

Beweis Sei $g, h \in U(m,R)$

$$g = \mathbb{1} + g_0 \qquad g_0 = \begin{pmatrix} 0 & & * \\ & \ddots & \\ 0 & & 0 \end{pmatrix} \qquad \Rightarrow g_0^m = 0 = h_0^m$$
$$h = \mathbb{1} + h_0 \qquad h_0 = \begin{pmatrix} 0 & & * \\ & \ddots & \\ 0 & & 0 \end{pmatrix}$$

Es folgt $gh = (\mathbb{1} + g_0)(\mathbb{1} + h_0) = \mathbb{1} + g_0 + h_0 + g_0 h_0 \in U(m,R)$

mit formaler Rihe

$$(\mathbb{1} + g_0)\underbrace{(\mathbb{1} - g_0 + g_0^2 - g_0^3 + \dots \pm g_0^m)}_{\in U(m,R)} = \mathbb{1}$$

$\Rightarrow U(m,R)$ Gruppe und $\# U(m,R) = (\# R)^{\frac{m(m-1)}{2}}$ □

9. Satz Sei X eine hölderige Menge, sei p eine Primzahl. Dann ist $F(X)$ residuell eine p-Gruppe, insbesondere ist $F(X)$ residuell endlich.

Beweis Sei p Primzahl, sei $w \in F(X) - \{1\}$.

Seien $x_1, \dots, x_n \in X$ die verschiedenen in w vorkommenden Buchstaben aus X, $x_i \neq x_j$ für $i \neq j$

$$w = x_{i_1}^{k_1} \cdots x_{i_r}^{k_r} \qquad k_j \in \mathbb{Z} - \{0\}, \quad i_j \neq i_{j+1}$$

$\{i_1, \dots, i_r\} = \{1, \dots, n\}$. Wähle $N \geq 1$ so, dass

$p^N \nmid k_1 \cdots k_r$ (hier Teile) $\Rightarrow k_1 \cdots k_r \not\equiv 0 \bmod p^N$.

Setze $R = \mathbb{Z}/p^N$.

Sei $\varepsilon_{ij} \in R^{(r+1)\times(r+1)}$ die Matrix, die nur an der Stelle (i,j) einen Eintrag 1 hat (sonst 0),

$$\varepsilon_{ij} = \begin{matrix} \\ i \\ \\ \\ \\ j \end{matrix} \begin{pmatrix} 0 & & 0 \\ & 1 & \\ 0 & & 0 \end{pmatrix} \Rightarrow \varepsilon_{ij} \cdot \varepsilon_{kl} \overset{(*)}{=} \begin{cases} \varepsilon_{il} & \text{wenn } j = k \\ 0 & \text{sonst} \end{cases}$$

Definiere für $j = 1, \dots, n$

$$g_j = \prod_{i_\ell = j} (\mathbb{1} + \varepsilon_{\ell, \ell+1}) \in U(r+1, R)$$

Wegen $i_\ell \neq i_{\ell+1}$ kommutiert die Matrix in dem Produkt, (wegen $(*)$ ∇_0)

und

$$g_{ij}^m = \mathbb{1} + m \sum_{i_\ell = j} \varepsilon_{\ell, \ell+1}$$

Bsp $w = x_2 x_1^{-3} x_2$ $\quad r=3,\ n=2$

$$g_1 = \begin{pmatrix} 1 & & & \\ & 1 & 1 & \\ & & 1 & \\ & & & 1 \end{pmatrix} \qquad g_2 = \begin{pmatrix} 1 & 1 & & \\ & 1 & & \\ & & 1 & 1 \\ & & & 1 \end{pmatrix}$$

Definiere $\lambda: X \to U(r+1, R)$ durch $\lambda(x_j) = g_j$

$\lambda(y) = \mathbb{1}$ wenn $y \neq x_1, \dots, x_n$. Beh: $F(\lambda)(w)$

$= g_{i_1}^{k_1} \cdots g_{i_r}^{k_r} \neq \mathbb{1}$. $\qquad e_j = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \leftarrow j$

Denn: $\left(\mathbb{1} + k_j \sum_{i_\ell = i_j} \varepsilon_{\ell,\ell+1}\right) e_{j+1} = e_{j+1} + k_j e_j \qquad (1 \le j \le r)$

$\left(\mathbb{1} + k_j \sum_{i_\ell = i_j} \varepsilon_{\ell,\ell+1}\right) e_{j+1+s} = e_{j+1+s} \qquad (1 \le j < r,\ s \ge 1)$

Lin. Kombination von $e_{j+1}, e_{j+2}, \dots e_r$

Es folgt: $g(e_{r+1}) = \underbrace{k_1 \cdots k_r}_{\neq 0 \bmod p^N} \cdot e_1 + a_2 e_2 + \dots + a_{r+1} e_r$

$\Rightarrow g \neq \mathbb{1}$. $\square$

10. Korollar Ist X endlich, so ist $F(X)$ kopfsch

Beweis: Folgt aus §3.9 und §3.7 □

Def Eine Teilmenge $Y \subseteq F(X)$ heißt Basis, wenn eine der beid Folgend äquivalente Bedingungen erfüllt ist:

(i) Der durch $i: Y \hookrightarrow F(X)$ induziert Homomorphismus $F(i): F(Y) \to F(X)$ ist ein Isomorphismus

(ii) Für jedes $w \in F(X)$ gibt es eindeutig bestimmt Elemente $y_1, \dots, y_r \in Y$ und Zahlen $k_1, \dots, k_r \in \mathbb{Z} - \{0\}$, mit $y_j \neq y_{j+1}$ für $1 \leq j < r$, so dass $w = y_1^{k_1} \cdots y_r^{k_r}$

[Die Äquivalenz von (i) und (ii) Folgt aus der konkreten Beschreibung der Elemente von $F(Y)$ in §2.5 als reduzierte Wörter]

Satz Ist X endlich, $Y \subseteq F(X)$ Teilmenge, dann sind äquivalent: (i) Y ist Basis

(ii) $\#Y = \#X$ und Y erzeugt $F(X)$.

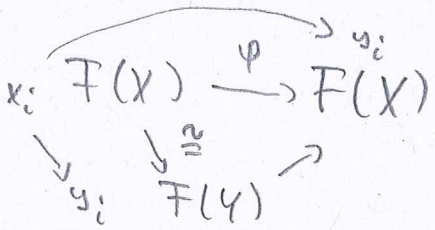
Beweis (i) $\Rightarrow$ (ii) klar mit §2.13

(ii) $\Rightarrow$ (i) $\#X = m = \#Y$ $X = \{x_1, \dots, x_m\}$

$Y = \{y_1, \dots, y_m\}$ def. $\varphi: F(X) \to F(X)$

durch $\varphi(x_i) = y_i$ $\Rightarrow$ φ surjektiv (weil

$Y \in \mathcal{Z}S$) $\Rightarrow$ φ Isomorphismus



□

11. **Lemma** Sei G endlich erzeugt, sei $n \geq 1$.

Dann ist die Menge $\{H \leq G \mid H \text{ Untergrp}, [G:H] = n\}$

endlich (eventuell leer). Wenn es $H \leq G$

gibt mit $[G:H] = n$, so ist

$$\bigcap \{H \leq G \mid H \text{ Untergrp mit } [G:H] = n\}$$

eine charakteristische (also normale) Untergruppe von endlich Index in G.

Beweis Sei $U = \{H \leq G \mid H \leq G \text{ Untergrp}, [G:H] = n\}$,

mit $U \neq \emptyset$. Für jedes $H \in U$ wähle eine

Bijektion $\alpha_H: G/H \to \{1, \dots, n\}$ mit $\alpha_H(H) = 1$

Über α_H und die Linkswirkung von G auf G/H

erhalten wir einen Homomorphismus $\varphi_H: G \to \mathrm{Sym}(n)$

Da G endlich erzgt ist, ist die Menge $\mathrm{Hom}(G, \mathrm{Sym}(U))$ endlich. Ist nun $K, H \in U$, $H \neq K$, so existiert $h \in H - K$. Es folgt

$\varphi_K(h)(1) \neq 1$ (weil $hK \neq K$), dagegen

$\varphi_H(h)(1) = 1$ (weil $hH = H$), also

$\varphi_H \neq \varphi_K$.

Sei nun $U = \{H_1, \ldots, H_r\}$. Allgemein gilt für Untergruppen A, B einer Gruppe G, dass

$$[G : A \cap B] \leq [G:A] \cdot [G:B] \qquad (\text{ü A!})$$

es folgt induktiv, dass für $N = H_1 \cap \ldots \cap H_r$ gilt $[G:N] \leq n^r$. Klar: ist $\alpha \in \mathrm{Aut}(G)$, so ist $\alpha(U) = U \Rightarrow \alpha(N) = \alpha(\cap U) = \cap U = N$, d.h. $N \trianglelefteq G$ ist charakteristische Untergruppe.

12. <u>Satz</u> Ist G endlich erzgt und residuell endlich, so ist auch $\mathrm{Aut}(G)$ residuell endlich.

Beweis. Sei $\alpha \in \mathrm{Aut}(G) - \{id_G\}$. Es gibt also ein $g \in G$ mit $\alpha(g) \neq g$ $\Rightarrow \alpha(g) g^{-1} \neq 1$. Wähle $H \leq G$ Untergruppe mit $\alpha(g) g^{-1} \notin H$ und $[G:H] = n < \infty$

Das geht, weil G residuell endlich ist:

Sei $\mathcal{H} = \{K \leq G \mid K \text{ Untergrp}, [G:K] = n\}_{H}$ (abs. $H \in \mathcal{H}$)
und sei $M = \bigcap \mathcal{H}$ so $[G:M] < \infty$ nach §3.11. Für alle $\beta \in Aut(G)$ gilt $\beta(\mathcal{H}) = \mathcal{H}$, also $\beta(M) = M$. Insbesondere ist $M \trianglelefteq G$ und für jedes β ist $\bar{\beta}: G/M \to G/M$, $xM \mapsto \beta(xM) = \beta(x)M$ ein Automorphismus. Die Abbildung $Aut(G) \to Aut(G/M)$, $\beta \mapsto \bar{\beta}$ ist ein Homomorphismus. Da G/M endlich ist, ist auch $Aut(G/M)$ endlich. Wegen $\alpha(g) \notin H \supseteq M$ falls $\bar{\alpha} \neq id_{G/M}$ $\square$

Folglich sind die Gruppen

$Aut(\mathbb{Z}^m) = GL_m\mathbb{Z}$

$Aut(F_m)$

residuell endlich

Bem.
- Produkte von residuell endlichen Gruppen sind residuell endlich
- Untergruppen von res. endl. Gruppen sind res. endl.

} i.A.

- Quotienten oder Bilder von res. endlichen Gruppen sind nicht unbedingt residuell endlich.

(Sonst wäre nach §2.7 jede Gruppe residuell endlich $\frac{\nabla}{0}$) (Welche Gruppe ist nicht res. endl.?)

13. Satz Sei $(G_i)_{i\in I}$ eine Familie von residuell endlichen Gruppen. Dann ist auch das Koprodukt $\ast_{i\in I} G_i$ residuell endlich.

Wir benötigen zuerst eine Hilfsaussage

Lemma A Wenn G residuell endlich ist und $g_1,\dots,g_r \in G-\{1\}$, so gibt es $N \trianglelefteq G$ mit $[G:N]<\infty$ und $g_1,\dots,g_r \notin N$.

Beweis: Wähle $N_i \trianglelefteq G$ mit $g_i \notin N_i$, $[G:N_i]<\infty$, setze $N = N_1 \cap \dots \cap N_r$. Es folgt $g_i \notin N$ und $[G:N] < \infty$ □

Lemma B Koprodukte von Familien endlicher Gruppen sind residuell endlich.

Beweis: Sei $(G_i)_{i\in I}$ Familie von endlichen Gruppen, sei $W = \ast_{i\in I} G_i$. Nach Satz 12 besteht W aus reduzierten Wörtern.

Setze $W_m = \{ w = (g_1, i_1, \dots, g_{k_1} i_k) \mid k \le m \} \subseteq W$

$\Rightarrow W_m$ endlich für jedes $m \in \mathbb{N}$.

Setze $|w| = k$ wenn $w = (g_1, \dots, i_k)$

Für jedes $j \in I$ und $m \in \mathbb{N}$ definiert

$$G_j \times W_m \to W_m \quad \text{durch} \quad w = (i_1, \dots, i_k)$$

$$g(w) = \begin{cases} w & \text{wenn } |(g,j)*w| = m+1 \\ (g,j)*w & \text{sonst} \end{cases}$$

Das ist eine Wirkung, denn: das Neutralelement $1 \in G$ wirkt trivial (klar)

$$g(w) = w \iff |w| = m \text{ und } i_1 \neq j$$
$$\iff g'(w) = w \text{ für alle } g' \in G \quad (*)$$

$g(w) \neq w$: $\Rightarrow$ $|w| < m$ oder $|w| = m$

$|w| < m \Rightarrow g'(g(w)) = (g'g)(w)$ $(*)$

$|w| = m \Rightarrow i_1 = j \Rightarrow g'(g(w)) = (g'g)(w)$ $(*)$

Wir erhalten also Homomorphismen $G_j \to \mathrm{Sym}(W_m)$ für jedes j und damit $*_{i \in I} G_i \to \mathrm{Sym}(W_m)$.

Sei jetzt $w \in W - \{0\}$, also $|w| = m > 0$

Es folgt $w(0) = w$ für die Wirkung von w via

$$W \times W_m \to W_m$$

also hat w nicht triviales Bild in der endlichen Gruppe $\mathrm{Sym}(W_m)$ $\square$

Beweis des Satzes. Sei $w \in \mathcal{W}$,

$w = (g_1, i_1, \dots, i_r)$. Es existiert Homomorphismus

$\varphi_j : G_j \to H_j$, H_j endlich, (*) so dass (Lemma 4)

jedes g_k gilt $\varphi_{i_k}(g_k) \neq 1$. Betrachte

$$\begin{array}{ccc} *_{i\in I} G_i & \xrightarrow{\exists!\ \Psi} & *_{i\in I} H_i \\ \uparrow & \nearrow & \uparrow \\ G_j & \longrightarrow & H_j \end{array}$$

$$\Rightarrow \quad \Psi(w) = (\varphi_{i_1}(g_1), i_1, \dots, \varphi_{i_r}(g_r), i_r) \neq ()$$

Lemma B $\Rightarrow$ es gibt K endlich, $*_{i\in I} H_i \xrightarrow{\varphi} K$ Hom.

mit $\varphi(\Psi(w)) \neq 1$ □

Korollar Freie Gruppen sind residuell endlich. □

Denn $\mathbb{Z}$ ist residuell endlich.

(*) $H_j = \{1\}$ für alle $j \in I - \{i_1, \dots, i_r\}$