§3 Finitely presented groups and residually finite groups

1. **Def** Let R be a subset of a group G. The <u>normal closure</u> of R is the normal subgrp

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

Hence $R \subseteq \langle R\rangle \leq \langle\langle R\rangle\rangle \trianglelefteq G$

Put $R^* = R \cup \{e\} \cup R^{-1}$. Then

$$\langle\langle R\rangle\rangle = \{ g_1 r_1 g_1^{-1} \cdot g_2 r_2 g_2^{-1} g_3 r_3 g_3^{-1} \cdots g_n r_n g_n^{-1} \mid r_1, \dots, r_n \in R^*, \ g_1, \dots, g_n \in G, \ n \geq 1 \}$$

⌈ The RHS is a subgrp containing R and is normal in G. Every normal subgrp $N \trianglelefteq G$ with $R \subseteq N$ contains the RHS. ⌋

2. **Def** Let X be a set, $R \subseteq F(X)$ a subset. Put

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

This is called a <u>presentation</u> with <u>generators</u> $x \in X$ and <u>relators</u> $r \in R$.

<u>Examples</u> (a) $\langle X \mid \emptyset \rangle = F(X)$

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

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

[Use universal property!]

The map $X \to \langle X \mid R \rangle$ has the following <u>universal property</u>. If H is a grp and if $\varphi : X \to H$ is a map and if $F(\varphi)(r) = e$ for all $r \in R$, then there is a <u>unique</u> homomorphism $F_R(\varphi) : \langle X \mid R \rangle \to H$ such that the diagram commutes.

$$\begin{tikzcd} X \arrow[r] \arrow[dr, "\varphi"'] & \langle X \mid R \rangle \arrow[d, "F_R(\varphi)"] \\ & H \end{tikzcd}$$

<u>Remark</u> Every grp is of the form $\langle X \mid R \rangle$.

Let G be a grp, let $X \subseteq G$ be a generating set, put $R = \ker(F(X) \twoheadrightarrow G) \rightsquigarrow$ the induced homomorphism $\langle X \mid R \rangle \to G$ is an <u>isomorphism</u>.

3. Def A group G is finitely presentable if there is a finite set $X \subseteq G$ of generators and a finite set $R \subseteq F(X)$ of relators such that the map

$$\langle \underset{\text{finite}}{X} \mid \underset{\text{finite}}{R} \rangle \longrightarrow G$$

is an isomorphism.

There are finitely generated grps which are not finitely presentable.

4. Suppose that $\langle X \mid R \rangle$ is a finitely presented group. We may ask the following algorithmic questions.

- The word problem. Is there a general algorithm that decides (in finite time!) for $w \in F(X)$ if $w \in \langle\langle R \rangle\rangle$?

- Is there an algorithm that decides if $\langle X \mid R \rangle = \{e\}$?

- Is there an algorithm that decides if $\langle X \mid R \rangle$ is finite?

The answer is in general no.

P. Novikov 1955: The word problem is undecidable.

But: for some classes of groups these questions are decidable, eg for free groups and for finitely generated abelian groups.

5. Def Let $\mathcal{P}$ be a property that groups may or may not have, eg being "finite" or "free" or "abelian" or "solvable". A group G has virtually property $\mathcal{P}$ if G has a subgp $H \leq G$ of finite index which has property $\mathcal{P}$.

Ex G is finite $\Leftrightarrow$ G is virtually trivial (!)

G has residually property $\mathcal{P}$ or is residually $\mathcal{P}$ if for every $g \in G - \{e\}$ there is a gp H with property $\mathcal{P}$ and a homomphism $\varphi: G \to H$ with $\varphi(g) \neq e$

Ex (1) If G has property $\mathcal{P}$, then G is residually $\mathcal{P}$

(2) The grp $(\mathbb{Z},+)$ is residually finite.

If $k \in \mathbb{Z}$, $k \neq 0$ choose $l > |k|$. Then the image of k in $\mathbb{Z} \to \mathbb{Z}/l$ is nontrivial.

6. Proposition Let $G = \langle X \mid R \rangle$ be a finitely presented group. If G is residually finite, then the word problem is solvable for $\langle X \mid R \rangle$.

Pf Let $w \in F(X)$. We need to know if $w \in \langle\langle R \rangle\rangle$. For this, we start two "algorithms."

"Algorithm 1" enumerates all elts in $\langle\langle R \rangle\rangle$ and stops if w turns up.

"Algorithm 2" enumerates all finite groups H and all maps $\varphi: X \to H$ with $F(\varphi)(R) = \{e\}$ and stops if $F(\varphi)(w) \neq e$

Since $\langle X \mid R \rangle$ is residually finite, one of these two algorithm will terminate in finite time.

Then stop. $\square$

Residually finite grps have good properties.

7. <u>Proposition</u> Every finitely generated residually finite group is hopfian.

<u>pf</u> Suppose not. Let $\varphi : G \twoheadrightarrow G$ be a surjective homomorphism, with $\varphi(g) = e$, $g \neq e$. Then is $N \trianglelefteq G$ with $g \notin N$ and $[G:N] < \infty$.

The set $\mathrm{Hom}(G, G/N)$ is finite (because G/N is finite and because G is finitely generated!).

Put $\mathrm{Hom}(G, G/N) = \{\psi_1, \dots, \psi_m\}$, $\psi_1 = \pi : G \to G/N$, $\# \mathrm{Hom}(G, G/N) = m$. Let $s : G \to G$ be a section for φ, $\varphi \circ s = \mathrm{id}_G$.

Now: $\psi_j \circ \varphi = \psi_k \circ \varphi \Rightarrow \psi_j \circ \varphi \circ s = \psi_j = \psi_k \circ \varphi \circ s = \psi_k$

$\Rightarrow j = k$, hence $\mathrm{Hom}(G, G/N) = \{\psi_1 \circ \varphi, \dots, \psi_m \circ \varphi)$

But $\psi_j \circ \varphi(g) = \psi_j(e)$ for all $j = 1, \dots, m$ ↯ $\square$

#

Next we want to show that the free grp F_m is residually finite.

8. <u>Lemma</u> Let R be a commutative ring.

For $m \geq 2$ put $\mathcal{U}(m,R) = \left\{ \begin{pmatrix} 1 & & * \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \in R^{m \times m} \right\}$

Then $\mathcal{U}(m,R)$ is a group. If $\# R = p^\ell$ for some prime number p, then $\mathcal{U}(m,R)$ is a <u>p-group</u> (every elt has order p^k, for some k)

<u>pf</u> Let $g, h \in \mathcal{U}(m,R)$ $\quad g = \mathbb{1} + g_0$, $\quad h = \mathbb{1} + h_0$

$$g_0 = \begin{pmatrix} 0 & & * \\ & \ddots & \\ 0 & & 0 \end{pmatrix} \qquad h_0 = \begin{pmatrix} 0 & & * \\ & \ddots & \\ 0 & & 0 \end{pmatrix}$$

$$\Rightarrow g_0^m = 0 = h_0^m$$

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

$$(\mathbb{1} + g_0)\underbrace{\underbrace{(\mathbb{1} - g_0 + g_0^2 - g_0^3 \cdots \qquad)}_{m+1 \text{ summands}}}_{\in \mathcal{U}(m,R)} = \mathbb{1}$$

hence g has an inverse and $\mathcal{U}(m,R)$ is a group.

The order of $\mathcal{U}(m,R)$ is $\# R^{\frac{m(m-1)}{2}}$ if R is finite.

$\square$

It is easy to see that the free abelian grp $FA(X)$ is residually finite: if $h = \sum_{x \in X} k_x \hat{x} \neq 0$ pick $z \in X$ with $k_z \neq 0$, choose $N \gg 1$ with $|k_x| < N$. Put $\varphi : FA(X) \to \mathbb{Z}/N$, $\varphi(\sum_{x\in X} l_x \hat{x}) = l_z + N\mathbb{Z} \in \mathbb{Z}/N$

$\rightsquigarrow \varphi(h) \neq 0$.

9. Proposition Let p be a prime. Then the free grp $F(X)$ is residually a finite p-group. In particular, F_m is residually finite.

pf Let $e \neq w \in W = F(X)$, let $x_1, \dots, x_n \in X$ be the different letters appearing in w, $x_i \neq x_j$ for $i \neq j$. Hence $w = x_{i_1}^{k_1} \cdots x_{i_r}^{k_r}$ ($\to i_e \neq i_{e+1}$)

$k_1, \dots, k_r \neq 0$, $\{i_1, \dots, i_r\} = \{1, \dots, n\}$ $(r \geq n)$

Choose $N \gg 1$ so that $p^N \nmid k_1 \cdots k_r$ and put $R = \mathbb{Z}/N$. Consider $U(r+1, R)$.

Let ε_{ij} denote the $(r+1)\times(r+1)$ - Matrix with entry $(i,j) = 1$, 0 else

$$
\begin{array}{cc}
 & \\
i & \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{pmatrix} \in R^{(r+1)\times(r+1)} \\
 & j
\end{array}
$$

$$\rightsquigarrow \varepsilon_{ij} \cdot \varepsilon_{kl} = \begin{cases} \varepsilon_{il} & \text{if } j = k \\ 0 & \text{else} \end{cases}$$

For $j = 1, \dots, n$ put

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

these matrices commute, because $i_\ell \neq i_{\ell+1}$

and note that $g_j^{k_j} = \mathbb{1} + k_j \sum_{i_\ell = j} \varepsilon_{\ell,\ell+1}$

<u>Example</u> $\omega = x_2 x_1^{-3} x_2^2$

$$g_1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ & 1 & 1 & 0 \\ & & 1 & 0 \\ 0 & & & 1 \end{pmatrix} \qquad g_2 = \begin{pmatrix} 1 & 1 & 0 & 0 \\ & 1 & 0 & 0 \\ & & 1 & 1 \\ 0 & & & 1 \end{pmatrix}$$

Put now
$$\begin{aligned} \varphi : X &\longrightarrow U(r+1, R) \\ x_j &\longmapsto g_j \\ \varphi(y) &= \mathbb{1} \quad \text{for } y \neq x_1, \dots, x_n \end{aligned}$$

<u>Claim: $F(\varphi)(\omega) \neq \mathbb{1}$</u> let $e_j = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} - j$

$$F(\varphi)(\omega) = g_{i_1}^{k_1} \cdots g_{i_r}^{k_r}$$

$$g_{i_s}^{k_s}(e_{s+1}) = \Big(\mathbb{1} + k_s \sum_{i_l = i_s} \varepsilon_{l,l+1}\Big) e_{s+1}$$

need to be equal, else zero!

$$= e_{s+1} + k_s e_s$$

$$g_{i_s}^{k_s}(e_{s+1+m}) = \Big(\mathbb{1} + k_s \sum_{i_l = i_s} \varepsilon_{l,l+1}\Big) e_{s+1+m}$$

$m \geq 1$ $\quad = \text{linear combination of } e_{s'},\ s' > s$

Hence $F(\varphi)(w)(e_{r+1}) = k_1 k_2 \cdots k_r e_1 + \text{others} \neq e_r$

$\square$

<u>Corollary</u> The groups F_m are hopfian.

10. <u>Def</u> Let X be a set. A subset $Y \subseteq F(X)$ is called a <u>basis</u> of the free group if the following equivalent conditions are satisfied.

(1) The natural map $F(Y) \xrightarrow{F(\varphi)} F(X)$ given by the inclusion $\varphi : Y \hookrightarrow F(X)$ is an isomorphism

(2) For every element $w \in F(X)$, there are <u>unique</u> elements $y_1, \dots, y_n \in Y$ and integers $k_1, \dots, k_n \neq 0$, with $y_j \neq y_{j+1}$ for $j = 1, \dots, n-1$, such that

$w = y_1^{k_1} \cdots y_n^{k_n}$.

⌜ The equivalence of the two conditions follows from the explicit construction of $F(Y)$ as reduced words in Y, cp. § 2.7 ⌟

11. Proposition Let X be a finite set, let $Y \subseteq F(X)$ be a subset. The following are equivalent:

(i) Y is a basis for $F(X)$.

(ii) $\#X = \#Y$ and Y generates $F(X)$.

Pf (i) $\Rightarrow$ (ii) is clear by the above and § 2.11.

(ii) $\Rightarrow$ (i): Let $X = \{x_1, .., x_m\}$, $Y = \{y_1, .., y_m\}$, $\#X = \#Y = m$. Define $\varphi(x_i) = y_i \rightsquigarrow$ get homomorphism

$$F(\varphi): F(X) \longrightarrow F(X)$$

which is surjective, since Y generates $F(X)$.

Since $F(X)$ is hopfian, $F(\varphi)$ is an isomorphism. $\square$

11. Lemma Suppose that G is a finitely generated grp, and that $n \geq 1$. Then the set

$$\{H \leq G \mid H \text{ subgrp}, [G:H]=n\}$$ is finite

(possibly empty). If it is nonempty, then

$$\bigcap \{H \leq G \mid H \text{ subgrp}, [G:H]=n\} = N$$ is a characteristic subgrp of finite index in G.

Recall: A subgroup $K \leq G$ is characteristic in K if $\alpha(K) = K$ for every automorphism $\alpha \in \mathrm{Aut}(G)$.
Every characteristic subgrp is normal. For example, $\mathrm{Cen}(G)$ is characteristic in G. (-> homework)

Pf Since G is finitely generated, the set $\mathrm{Hom}(G, \mathrm{Sym}(n))$ is finite. Put
$\Lambda = \{H \leq G \mid [G:H]=n\}$, assume $\Lambda \neq \phi$.

For each $H \in \Lambda$ choose a bijection

$$\alpha_H : G/H \longrightarrow \{1, \ldots, n\}, \text{ with } \alpha_H(H) = 1$$

From the G action on G/H we get a G action on $\{1, \ldots, n\}$ via α_H as homomorphism

$f_H : G \to \mathrm{Sym}(n)$.

If $H, K \in \Lambda$, $H \neq K$, then there is some $h \in H - K$ (because then $H \not\subseteq K$). Hence

$$\left.\begin{array}{l} f_K(h)(1) \neq 1 \\ f_H(h)(1) = 1 \end{array}\right\} \Rightarrow f_H \neq f_K \text{ for } K \neq H.$$

Hence Λ is finite.

For subgrps $A, B \leq G$ one has always

$$[G : A \cap B] \leq [G:A] \cdot [G:B] \quad (\to \text{homework}).$$

It follows inductively for

$L = \bigcap \Lambda$ that $[G:L] \leq n^m$, $m \# \Lambda$.

If φ is an automorphism of G, then $\varphi(H) \in \Lambda$ for all $H \in \Lambda$. Hence $\varphi(L) = L$.

$\square$

12. Proposition Let G be a finitely generated group. If G is residually finite, then $\mathrm{Aut}(G)$ is also residually finite.

pf Let $\alpha \in \mathrm{Aut}(G)$, $\alpha \neq id_G$. Hence there is $g \in G$ with $\alpha(g) \neq g$. $\leadsto$ $\alpha(g)g^{-1} \neq e$.

Choose $H \leq G$ of finite index, with $\alpha(g)g^{-1} \notin H$.

Put $n = [G:H]$ and $\Delta = \{ K \leq G \mid [G:K] = n \}$.

Consider $M = \bigcap \Delta$. Then M is characteristic in G (see above), and $[G:M] < \infty$.

Each automorphism $\beta \in \mathrm{Aut}(G)$ induces an automorphism $\bar{\beta} : G/M \to G/M$ via

$$\bar{\beta}(aM) = \beta(aM) = \beta(a)M.$$

Since G/M is finite, $\mathrm{Aut}(G/M)$ is finite as well.

We have $\alpha(g)g^{-1} \notin H \geq M$, hence $\bar{\alpha} \neq id_{G/M}$.

Hence
$$\mathrm{Aut}(G) \longrightarrow \mathrm{Aut}(G/M)$$
$$\beta \longmapsto \bar{\beta}$$

is a homomorphism with $\bar{\alpha} \neq id_{G/M}$ $\leadsto$

$\mathrm{Aut}(G)$ is residually finite. $\square$

13. <u>Lemma</u> We have $\mathrm{Aut}(\mathbb{Z}^m) \cong GL_m\mathbb{Z}$

$= \{ a \in \mathbb{Z}^{m\times m} \mid \det(a) = \pm 1 \}$

<u>Pf</u> Suppose that $\alpha \in \mathrm{Aut}(\mathbb{Z}^m)$. Let a be

the matrix whose columns are the vectors $\alpha(e_1), \dots, \alpha(e_m)$

$e_j = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} - j$. Then $\alpha\left(\sum_{k=1}^{m} x_k e_k\right) = \sum_{k=1}^{m} \alpha(x_k e_k)$

$x_1, \dots, x_k \in \mathbb{Z}$

$= \sum_{k=1}^{m} x_k \alpha(e_k) = a \begin{pmatrix} x_1 \\ \vdots \\ x_k \end{pmatrix}$ ⇝ α determined by

the matrix $a \in \mathbb{Z}^{m\times m}$. The matrix for α^{-1} is

b ⇝ $ab = \mathbb{1} = ba \Rightarrow \underbrace{\det(a)}_{\in\mathbb{Z}} \underbrace{\det(b)}_{\in\mathbb{Z}} = 1$ ⇝ $\det(a) = \pm 1$

⇝ $\mathrm{Aut}(\mathbb{Z}^m) \subseteq GL_m(\mathbb{Z})$. Conversely, if $a \in GL_m(\mathbb{Z})$,

then $a^{-1} \in GL_m(\mathbb{Z})$ (by <u>Cramer's rule</u>)

⇝ $GL_m(\mathbb{Z})$ is a group, every $a \in GL_m\mathbb{Z}$ induces

an automorphism of $\mathbb{Z}^m$ via $\begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix} \mapsto a\begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix}$. □

<u>Corollary</u> The group $GL_m\mathbb{Z}$ is residually finite.

14. Remarks (1) If $(G_i)_{i\in I}$ is a family of residually finite groups, then the product $\prod_{i\in I} G_i$ is residually finite (→ homework)

(2) If G is residually finite and if $H \leq G$ is a subgrp, then H is residually finite (This is clear)

(3) If G is residually finite and if $N \trianglelefteq G$ is a normal subgrp, then G/N need not be residually finite (otherwise every grp would be residually finite, since free groups are residually finite).

15. Proposition Coproducts of residually finite groups are residually finite.

For the proof we use two auxiliary results.

Lemma A Suppose that G is residually finite and that $g_1, \ldots, g_m \in G - \{e\}$. Then there is a normal subgrp $N \trianglelefteq G$ of finite index, with $g_1, \ldots, g_m \notin N$.

pf Let $N_i \trianglelefteq G$ of finite index, with $g_i \notin N_i$. Put $N = N_1 \cap \dots \cap N_m \trianglelefteq G$. Then $[G:N] < \infty$ ($\rightarrow$ homework) and $g_1, \dots, g_m \notin N$ $\square$

<u>Lemma B</u> Suppose that $(G_i)_{i\in I}$ is a <u>finite</u> family of <u>finite</u> groups. Then $\coprod_{i \in I} G_i = G$ is residually finite.

pf Let $\mathcal{W} = G$ denote the set of reduced words, put $\mathcal{W}_m = \{ w \in \mathcal{W} \mid w = g_1 \cdots g_k \ , k \leq m \}$

Then $\mathcal{W}_m$ is finite. Put $l(\underbrace{g_1 \cdots g_k}_{\text{reduced word}}) = k$

We define an action

$G_j \times \mathcal{W}_m \to \mathcal{W}_m$ as follows:

$$g(w) = \begin{cases} w & \text{if } l(gw) = m+1 \\ gw & \text{else} \end{cases}$$

multiplication in G

This is indeed an action: the identity in G_j acts trivially (✓)

$g(w) = w \iff w = g_1 \cdots g_m \ , \ g_1 \notin G_j$

$\iff \tilde{g}(w) = w$ for all $\tilde{g} \in G_j - \{e\}$

$\boxed{\text{Case } g(\omega) \neq \omega}$

If $\ell(\omega) < m \Rightarrow (g\tilde{g})(\omega) = g(\tilde{g}(\omega))$ (✓)

If $\ell(\omega) = m$, $\omega = g_1 \cdots g_m$, $g_1 \in G_j$

$\Rightarrow (g\tilde{g})(\omega) = (g\tilde{g}g_1)\, g_2 \cdots g_m$ (✓)

We obtain a homomorphism $G_j \to \mathrm{Sym}(\mathcal{W}_m)$,

whence a homomorphism $\coprod_{j\in I} G_j \xrightarrow{\varphi_m} \mathrm{Sym}(\mathcal{W}_m)$

If $w \in \mathcal{W}$, $\ell(w) = m \geq 1$, then

$w(()) = w$ for the action $\coprod_{j\in I} G_j \times \mathcal{W}_m \to \mathcal{W}_m$

empty word

$\Rightarrow \varphi_m(w) \neq \mathrm{id}_{\mathcal{W}_m} \Rightarrow \coprod_{j\in I} G_j$ is residually finite $\square$

pf of Prop §3.15

Let $w \in \mathcal{W} = \coprod_{j\in I} G_j$, $w \neq ()$.

$\Rightarrow w = g_{i_1} \cdots g_{i_m}$ reduced word, $m \geq 1$

Put $H_j = \{e\}$ for $j \neq i_1, \dots, i_m$

For $j \in \{i_1, \dots, i_m\}$ choose $N_j \trianglelefteq G_j$ of finite index in such a way that $g_{i_k} \notin N_j$ for all $i_k = j$

(by Lemma A). Put $H_j = G_j / N_j$ and consider the diagram

$$\begin{tikzcd}
\coprod_{i \in I} G_i \arrow[rr, "\exists!"', "\psi"] & & \coprod_{i \in I} H_i \\
G_j \arrow[u] \arrow[urr, "\varphi_j"] \arrow[rr, "\pi_j"] & & H_j \arrow[u]
\end{tikzcd}$$

$$\psi(w) = \psi(g_{i_1} \cdots g_{i_m}) = \varphi_{i_1}(g_{i_1}) \cdots \varphi_{i_m}(g_{i_m}) \neq e$$

By Lemma B, there is a finite gp H and a homomorphism $f : \coprod_{i \in I} H_i \longrightarrow H$ with $f(\psi(w)) \neq e$

$\square$