RESIDUALLY FINITE GROUPS, SIMPLE GROUPS

Definition 3.2. A group G is called *residually finite* if for every $1 \neq g \in G$ there is a homomorphism φ from G to a finite group F such that $\varphi(g) \neq 1$.

Remark 3.4. A group G is residually finite if for every $g \in G, g \neq 1$ there is a finite index subgroup H of G such that $g \notin H$ (exercise).

If a group G is residually finite then clearly any subgroup of G is also residually finite.

Proposition 3.4. *Let G be a residually finite group and let $g_1, ..., g_n$ be distinct elements of G. Then there is a homomorphism $\varphi : G \to F$ where F is finite, such that $\varphi(g_i) \neq \varphi(g_j)$ for any $1 \leq i < j \leq n$.*

Proof. If $h_1, ..., h_k$ are non trivial elements of G there are homomorphisms $\varphi_i : G \to F_i$, where F_i are finite, such that $\varphi_i(h_i) \neq 1$ for every i. It follows that

$$\varphi = (\varphi_1, ..., \varphi_k) : G \to F_1 \times ... \times F_k$$

is a homomorphism to a finite group such that $\varphi(h_i) \neq 1$ for every i. Now we apply this observation to the set of non-trivial elements $g_i g_j^{-1}$ $(1 \leq i < j \leq n)$ and we obtain a homomorphism $\varphi : G \to F$ (F finite), such that $\varphi(g_i g_j^{-1}) \neq 1$, hence $\varphi(g_i) \neq \varphi(g_j)$ for any $1 \leq i < j \leq n$. ☐

Intuitively residually finite groups are groups that can be 'approximated' by finite groups.

Matrix groups furnish examples of residually finite groups. To whow this we will need two easy lemmas. We leave the proofs to the reader.

Lemma 3.1. *Let A, B be commutative rings with 1 and let $f : A \to B$ be a ring homomorphism. Then the map $\bar{f} : SL_n(A) \to SL_n(B)$ given by $\bar{f}((a_{ij})) = (f(a_{ij}))$ is a group homorphism.*

Lemma 3.2. *Let A be a subring of $\mathbb{Q}$. Assume that there is a prime p such that for any $a/b \in A$, p does not divide b. Then the map $\phi : A \to \mathbb{Z}_p$, $\phi(a/b) = ab^{-1}$ is a ring homomorphism.*

Proposition 3.5. *$GL_n(\mathbb{Z})$ is a residually finite group.*

Proof. Indeed by lemma 3.1 if p is a prime we have a homomorphism

$$\varphi_p : GL_n(\mathbb{Z}) \to GL_n(\mathbb{Z}_p)$$

Clearly for any $g \neq 1$, $\varphi_p(g) \neq 1$ for some p. ☐

Proposition 3.6. *Any finitely generated subgroup G of $SL_n(\mathbb{Q})$ (or $GL_n(\mathbb{Q})$) is a residually finite group.*

Proof. Let $G =< g_1, ..., g_n >$. Let $p_1, ..., p_k$ be the primes that appear in the numerators or denominators of the entries of the matrices $g_1, ..., g_n$. If p is any other prime then by lemmas 3.1, 3.2 we have a homomorphism:

$$\varphi_p : G \to SL_n(\mathbb{Z}_p)$$

Clearly for any $g \in G$, $g \neq 1$, $\varphi_p(g) \neq 1$ for some prime p.

Clearly the same holds for subroups of $GL_n(\mathbb{Q})$ as we may see $GL_n(\mathbb{Q})$ as a subgroup of $SL_{n+1}(\mathbb{Q})$.

□

In fact by a similar argument one can show that the same proposition holds for any finitely generated subgroup of $GL_n(\mathbb{C})$.

Example 3.2. The group $(\mathbb{Q}, +)$ is not residually finite. Indeed if $f : \mathbb{Q} \to F$ is a homomorphism such that F is finite and $f(1) = g \neq 1$ then $g = f(1/n)^n$ for any n, which is clearly impossible in a finite group.

Theorem 3.2. *Let G be a residually finite group admitting a finite presentation $\langle S|R \rangle$. Then G has a solvable word problem.*

Proof. Given a word $w \in F(S)$ we enumerate in parallel homomorphisms $f : G \to S_n$ (where S_n are the groups of permutations of $\{1, ..., n\}$) and the elements of $\langle\langle R \rangle\rangle$. Eventually either for some f, $f(w) \neq 1$, hence $w \neq 1$ in G, or we will have that $w \in \langle\langle R \rangle\rangle$ and so $w = 1$ in G. □

Theorem 3.3. *The free group F_n is residually finite.*

Proof. Since F_n is a subgroup of F_2 it is enough to show that F_2 is residually finite. One way to show this is to prove that F_2 is isomorphic to a subgroup of $GL_2(\mathbb{Z})$ (exercise). We give here a different proof. Let $w \in F_2 =< a, b >$ be a reduced word of length k. Let B be the set of reduced words of length less or equal to k. We consider the group of permutations of B, $Symm(B)$. We define now two permutations α, β of $Symm(B)$: If $|v| \leq k - 1$ we define $\alpha(v) = av$ and we extend α to the words of length k in any way. Similarly if $|v| \leq k - 1$ we define $\beta(v) = bv$ and we extend β in the words of length k in any way. We define now a homomorphism

$$\varphi : F_2 \to Symm(B), \ \varphi(a) = \alpha, \varphi(b) = \beta$$

Clearly $\varphi(w)(e) = w$ so $\varphi(w) \neq 1$. □

Definition 3.3. We say that a group G is *Hopf* if every epimorphism $\varphi : G \to G$ is 1-1.

Theorem 3.4. *If a finitely generated group G is residually finite then G is Hopf.*

Proof. Assume that G is residually finite but not Hopf. Let $f : G \to G$ be an onto homomorphism and let $1 \neq g \in ker\, f$. Let F be a finite group and let $\varphi : G \to F$ be a homomorphism such that $\varphi(g) \neq 1$.

Since f is onto there is a sequence $g_0 = g, g_1, ..., g_n, ...$ such that $f(g_n) = g_{n-1}$ for any $n \geq 1$. This implies that the homomorphisms

$$\varphi \circ f^{(n)} : G \to F$$

are all distinct since for any $n \geq 1$

$$\varphi \circ f^{(n)}(g_n) \neq 1,\ \varphi \circ f^{(n)}(g_k) = 1 \text{ for } k < n$$

This is a contradiction since G is finitely generated and so there are only finitely many homomorphisms from G to F. □

Corollary 3.1. *If A is a generating set of n elements of the free group of rank n, F_n, then A is a free basis of F_n.*

Proof. Let X be a free basis of F_n and let $\varphi : X \to A$ be a 1-1 function. Then φ extends to a homomorphism $\varphi : F_n \to F_n$. Since A is a generating set φ is onto. However F_n is residually finite and hence Hopf. It follows that φ is an isomorphism and A a free basis of F_n. □

Definition 3.4. A non-trivial group G is called *simple* if the only normal subgroups of G are $\{1\}$ and G.

Theorem 3.5. *Let $G = \langle S | R \rangle$ be a finitely presented simple group. Then G has a solvable word problem.*

Proof. Let w be a word in S. We remark that if $w \neq 1$ in G then $\langle\langle w \rangle\rangle = G$, so $\langle\langle w \cup R \rangle\rangle = F(S)$.

We enumerate in parallel the elements of $\langle\langle w \cup R \rangle\rangle$ and of $\langle\langle R \rangle\rangle$ in $F(S)$. If $w = 1$ then eventually w will appear in the list of $\langle\langle R \rangle\rangle$, while if $w \neq 1$ the set S will eventually appear in the list of $\langle\langle w \cup R \rangle\rangle$. □