Lecture 3

I Residual finiteness of groups

IA Definition: The group Γ is residually finite if, for any $\gamma \in \Gamma$, $\gamma \neq 1$ there exists a finite group F and a homomorphism $\varphi : \Gamma \to F$ such that $\varphi(\gamma) \neq 1$.

Remark: $G \subset \Gamma$, Γ residually finite $\Rightarrow$ G residually finite.

Proposition: Free groups are residually finite.

Proof 1: Observe first that $SL(n, \mathbb{Z})$ is residually finite since any element of it can be detected in $SL(n, \mathbb{Z}/p\mathbb{Z})$ for some p, and the latter are finite. Recall further that $F(2) \hookrightarrow SL(2, \mathbb{Z})$ as in Sanov's theorem. By the above remark $F(2)$ is residually finite and thus all free groups are residually finite.

Proof 2 (Schreier's): Let $W = x_{i_1}^{\varepsilon_1} \dots x_{i_n}^{\varepsilon_n}$ a reduced word. Define a homomorphism $\varphi : F \to S_{n+1}$ such that $\varphi(x_{i_r}^{\varepsilon_r})$ is a permutation sending r to $r+1$. Thus if $\varepsilon_r = +1$, $\varphi(x_{i_r})$ sends r to $r+1$ if $\varepsilon_r = -1$ then $\varphi(x_{i_r})$ sends $r+1$ to r. This assignment is not possible if some $\varphi(a)$ is forced to send r into two distinct numbers (or if two distinct numbers are not to the same s). But this is possible only when $x_{i_r}^{\varepsilon_r} = z^{+1}$, $x_{i_{r+1}}^{\varepsilon_r} = z^{-1}$ and this is not allowed because W is reduced. Last $\varphi(W)$ sends 1 to $n+1$ and then $\varphi(W) \neq 1$. $\square$.

IB Residual finiteness and Hopfian groups

Proposition (Malcev): Finitely generated residually finite groups are Hopfian.

Proof 1: Since Γ is f.g. $\Rightarrow$ the number of normal subgroups of index k in Γ is finite, $\forall k$. Let assume $N \lhd \Gamma$ s.t. Γ is isomorphic to Γ/N. To each $H \lhd \Gamma$ of index k we associate $HN \lhd \Gamma$ which is also an index k subgroup since $\Gamma/HN \simeq (\Gamma/N)/H$. Moreover if H, H' are distinct then HN and $H'N$ are distinct as their images in Γ/N are distinct. This means that there is an injective map from the set of index k subgroups

(2) to the (subset) of index k subgroups of Γ containing N.
This map is then a bijection (since the set is finite) and so any finite index subgroup contains N. But the group is residually finite $\Rightarrow \bigcap_{\substack{H \lhd \Gamma \\ \Gamma/H \text{ finite}}} H = \{1\}$. This implies $N = \{1\}$. □

Proof 2. Let $\varphi: \Gamma \to \Gamma$ with $\ker \varphi \neq 1$ be surjective homomorphism and $\gamma \in \ker \varphi$, $\gamma \neq 1$. Let also $\pi: \Gamma \to F$ be a morphism on a finite group F. We will prove that

$$\pi(\gamma) = 1,$$ contradicting the residual finiteness.

As φ is surjective φ^n is surjective $\forall n$. Thus there exists a $\gamma_n \in \Gamma$ such that $\varphi^n(\gamma_n) = \gamma$. All γ_n are pairwise distinct because $\varphi^{n+1}(\gamma_n) = \varphi(\gamma) = 1$ and thus $\varphi^m(\gamma_n) = 1 \ \forall m > n$. If $\gamma_m = \gamma_n$ for $m > n \Rightarrow$ if $\varphi^m(\gamma_n) = 1$ and $\varphi^m(\gamma_n) = \varphi^m(\gamma_m) = \gamma$ hence $\gamma = 1$.

Let now $\pi_n = \pi \circ \varphi^n : \Gamma \to F$. We have

$$\pi_n(\gamma_n) = \pi \circ \varphi^n(\gamma_n) = \pi(\gamma).$$

$$\pi_m(\gamma_n) = \pi \circ \varphi^m(\gamma_n) = \pi(1) = 1 \quad \forall m > n.$$

If $\pi(\gamma) \neq 1$ then π_m are distinct morphism $\Gamma \to F$. Indeed if $\pi_m(\gamma_n) = \pi_n(\gamma_m)$ then $\pi(\gamma) = 1$. But there are only finitely many morphism $\Gamma \to F$ (fixed F) because Γ is finitely generated. This contradiction proves the claim.

Corollary: The non-Hopfian groups $BS(1,2) \times BS(1,2)$ and $B(2,3)$ are NOT residually finite.

Remark: There exist also Hopfian groups which are not residually finite. In fact any infinite simple group is Hopfian, but it is not residually finite.

Corollary (Nielsen) Let $S \subset F(n)$ be a set of generators with n elements. Then S is a free set of generators of $F(n)$ the free group of rank n.

Proof Let T be a free set of generators with n elements, $\varphi: T \to S$ a bijection and $\psi: F(n) \to F(n)$ be the map induced between the free groups. Then ψ is surjective, $F(n)$ is Hopfian $\Rightarrow$ ψ is an isomorphism $\square$

II A Malcev's theorem. Statement

The $SL(n,\mathbb{Z})$ residual finiteness can be extended to much more general groups:

Theorem (Malcev) A finitely generated subgroup of $GL_n(A)$ where A is a commutative ring is residually finite.

II B Noetherian rings

Def. A (commutative) ring is Noetherian if every ideal in it is finitely generated. Equivalently, if we have an ascending sequence of ideal

$$I_1 \subset I_2 \subset \dots \subset I_n \subset \dots$$

then this becomes stationary i.e. for large n $I_n = I_{n+1} = \dots$

Ex 1) $\mathbb{Z}$ is Noetherian.

2) $U \subset \mathbb{Z}[x]$ be the subring of polynomials $\{a_0 + a_1 x + \dots + a_n x^n,\ a_i \equiv 0 (2)\}$

The ideal of those polynomials f with $a_0 = 0$ is generated by the set

$$\{2x, 2x^2, \dots, 2x^n, \dots\}$$

and no proper subset can generate it.

Hilbert basis theorem If A is Noetherian ring then $A[x]$ is Noetherian.

Proof Let $I \subset A[x]$ be an ideal, and I_k be the set of elements of A which occur as leading coefficients of elements of I degree k i.e.

$$I_k = \{a \in A;\ ax^k + a_1 x^{k-1} + \dots + a_k \in I \text{ for some } a_i\}$$

Then $I_0 \subset I_1 \subset \dots$ is an ascending sequence of ideals of A.

Note A Noetherian $\Rightarrow \exists n$ s.t. $I_n = \bigcup_{j=0}^{\infty} I_j$.

Let then I_k be generated by $\{a_{k1}, \dots, a_{km_k}\} \subset A$ and set

$f_{kj} \in A[x]$ be $f_{kj} = a_{kj} x^k + \alpha_1 x^{k-1} + \dots$

Lemma: $\{f_{kj},\ \text{for } k \le n,\ j \le m_k\}$ is a generating system for I as $A[x]$-ideal.

Proof: Let $g(x) = bx^k + \dots \in I$. If $k \le n$ then

(4) write $(*)$ $b = \sum \lambda_j a_{nj} \Rightarrow$

$g(x) - \sum \lambda_j f_{kj}$ has degree $< k$ and we can continue reducing the degree until the degree reduces to 0.

If $k > n$ then

$g(x) - \sum \lambda_j f_{nj} x^{k-n}$ has degree $< k$

and continue reducing. $\square$

Corollary: 1) $\mathbb{Z}[x_1, \dots, x_n]$ is Noetherian.

2) $F[x_1, \dots, x_n]$ is Noetherian $\forall$ F field.

3) A quotient of a Noetherian ring $\Rightarrow$ Noetherian.

Thus every finitely generated ring (i.e. the quotient of $\mathbb{Z}[x_1, \dots, x_n]$ by some ideal) is Noetherian.

II C Krull intersection theorem.

Def. If I, J are ideals then IJ is the product ideal i.e. the ideal generated by xy, $x \in I$, $y \in J$. Write $I^\infty = \bigcap_{j=1}^{\infty} I^j$.

Theorem (Krull) If A is Noetherian, I, J ideals such that $J \subset I^\infty$ then $I \cdot J = J$.

Proof We have to show that $J \subset I \cdot J$.

Let $\{b_1, \dots, b_n\}$ generate I as ideal. Let also

$B = A + Ix + I^2x^2 + \dots + I^n x^n + \dots \subset A[x]$

$\tilde{J} = J + Jx + Jx^2 + \dots + Jx^n + \dots \subset B$, since $J \subset I^n \; \forall n$.

Lemma: B is Noetherian, $\tilde{J} \subset B$ is an ideal.

Pf of lemma: The map $\phi : A[y_1, \dots, y_n] \to B$, $\phi(y_i) = b_i x$ is obviously surjective and hence B is a quotient of the Noetherian ring $A[y_1, \dots, y_n]$. Moreover $\tilde{J}$ is an ideal in $A[x]$ hence in the subring $B \subset A[x]$. $\square$

By Hilbert basis theorem $\tilde{J}$ is finitely generated as B-ideal by $\{f_1, \dots, f_k\} \subset \tilde{J}$. The f_j are polynomials in x of

degrees $\leq m$. Left $\alpha x^{m+1} \in \tilde{J}$ with $\alpha \in J$. Then

$$\alpha x^{m+1} = \sum g_i(x) f_i(x), \quad g_i \in B$$

and $f_i \in J$ has degree $\leq m$. Let $g_i(x) = \sum \lambda_{is} x^s$

Then taking the coefficients of $x^{m+1} \Rightarrow f_i(x) = \sum \delta_{it} x^t$.

$$\alpha = \sum_{\substack{s+t=m+1 \\ s>0 \\ t<m+1}} \lambda_{is} \delta_{it} \in I \cdot J.$$

and $\delta_{it} \in J$, $\lambda_{is} \in I$ (since $\lambda_{is} \in I$ for $s>0$)

Hence $J \subset IJ$ as claimed □

II D Maller's lemma

Theorem If K is a field which is finitely generated as a ring then K is a finite field.

Proof The main step is the following

Lemma: If E is a finite extension of the field F and E is finitely generated as a ring, then so is F.

Pf. of Lemma: Induction on the degree of the extension reduces the pb to a simple extension $E = F(x)$. Let $f(x) = x^d + a_{d-1}x^{d-1} + \dots + a_0$ be the minimal polynomial of x and $\{y_1, \dots, y_m\}$ be a generating system for E as a ring. Therefore

$$y_i = \sum_{j=0}^{d} b_{ij} x^j, \quad b_{ij} \in F$$

Let R be the subring of E generated by b_{ij}, a_i. Any $z \in F$ can be written as an integer polynomial in the y_i and hence as a polynomial in x with coeff in R. Now $a_i \in R$ so that this polynomial has degree $< d$ in R, namely $z = \sum_{j=0}^{d-1} r_j x^j$.

Now $z, r_j \in F$, $1, x, \dots, x^{d-1}$ form a basis of E as a F-vector space so $r_0 = z$ and $r_j = 0$, $j > 0$ and so $z \in R$. Hence $R = F$ and F is finitely generated as a ring □

Proof of the theorem K is a finitely generated extension

of its prime field F and so K has a transcendence basis $x_1, \dots, x_n$ and K is a finite extension of $E = F(x_1, \dots, x_n)$. By the lemma above $F(x_1, \dots x_n)$ is finitely generated as a ring.

If $n=0$ then $E = F$; if F has prime characteristic then F is finite hence K is finite. if F has zero characteristic then $F = \mathbb{Q}$, but $\mathbb{Q}$ is not finitely generated as a ring because there are ∞-many primes in $\mathbb{Z}$.

if $n > 0$ then K is $A(x)$ where A is a rational function field in $n-1$ indeterminates over F. But if A is any field $A(x)$ can't be finitely generated as a ring because $K[x]$ has infinitely many monic irreducible polynomials.

II E Proof of Maker's Theorem

First step is to consider $GL_1(A)$, namely

Proposition Let A be a finitely generated ring and $a \in A \setminus \{0\}$. Then there exists an ideal J of A such that

$$a \notin J \text{ and } A/J \text{ is a finite ring.}$$

Proof Let us show that

Lemma if A is Noetherian ring then ~~for every~~ the intersection over all powers of the maximal ideals $M \subset A$ (i.e. M such that A/M is a field) ~~we have~~ is zero i.e.

$$\bigcap_{\substack{M \subset A \\ M \text{ maximal}}} M^\infty = 0.$$

Pf of Lemma: Take $a \in A$, $a \neq 0$ and set

$$\mathrm{Ann}(a) = \{ x \in A ; xa = 0 \} \quad \text{annihilator of } a.$$

Then $\mathrm{Ann}(a) \subset A$ is an ideal and $1 \notin \mathrm{Ann}(a)$. There exists a maximal ideal $M \supset \mathrm{Ann}(a)$. We claim that there is an n such that $a \notin M^n$, Otherwise we

would have $\langle a\rangle \subset M^\infty$, where $\langle a\rangle$ is the ideal generated by $\langle a\rangle$.
By Krull intersection theorem $M\cdot\langle a\rangle = \langle a\rangle$ and thus
there exists $m \in M$ s.t. $ma = a$ i.e.
$(1-m)a = 0$, hence $1-m \in \mathrm{Ann}(a) \subset M$.
But $m \in M$, $1-m \in \mathrm{Ann}(a) \Rightarrow 1 \in M$, contradiction. □

Pf. of proposition By Lemma above there is a maximal ideal
M of A an $n \geq 1$ s.t. $a \notin M^n$. We claim that
A/M^n is finite.
if $n=1$ then A/M is a field which is finitely generated
and hence by the Malcev's lemma II D A/M is finite.
If $n>1$ remark that M^n is an ideal of a Noetherian
ring (A is a quotient of $\mathbb{Z}[x_1,\dots,x_m]$) and hence
generated by finitely many elements. Also M^n/M^{n+1} is
a A/M-module i.e. a finite dimensional space over
the finite field A/M, and hence a finite set. Thus
$\mathrm{card}(A/M^{n+1}) = \mathrm{card}(A/M^n)\cdot\mathrm{card}(M^n/M^{n+1})$
and this proves induction step. □

Proposition if A is a finitely generated commutative ring then
$GL_n(A)$ is residually finite.

Proof. if $a \in GL_n(A)$, $a \neq 1$ then the matrix a has some entries
different from those of identity. But A has an ideal J
with A/J finite s.t. $a \neq 1$ modulo J by previous proposition.
Thus $GL_n(A) \to GL_n(A/J)$ sends a into a non trivial
element of the finite group $GL_n(A/J)$. □

General case if the group Γ is generated by $g_1,\dots,g_k$ let
K be the subring of A generated by entries of the matrices $\{g_i^{\pm 1}\}$.
Then K is a finitely generated ring, $GL_n(K) \subset GL_n(A)$
and $\Gamma \subset GL_n(K)$. By above $GL_n(K)$ is finite $\Rightarrow$ Γ resid. finite □