Lecture 9.

Free Products of Groups.

Let G_i, $i \in I$, be a family of groups.

Objects: (a group G, homomorphisms $\varphi_i : G_i \to G$, $i \in I$)

Morphisms: $(G, \varphi_i) \to (G', \varphi_i')$ is a homomorphism $\chi : G \to G'$ that makes the diagrams

$$\begin{tikzcd} G \arrow[r, "\chi"] & G' \\ G_i \arrow[u, "\varphi_i"] \arrow[ur, "\varphi_i'"'] & \end{tikzcd}, \quad i \in I$$

commutative.

Universal Object: $(U, u_i : G_i \to U, i \in I)$.

For an arbitrary object $(G, \varphi_i : G_i \to G, i \in I)$

there exists a unique ~~homomorphism~~ morphism, $(U, u_i) \to (G, \varphi_i)$.

Let $G_i = \langle X_i \mid R_i(X_i) = 1 \rangle$ be presentations by generators and relations. Just as before $U = \langle \dot{\bigcup}_{i\in I} X_i \mid R_i(X_i) = 1, i \in I \rangle$ and ~~are~~ natural homomorphisms

$u_k : \langle X_k \mid R_k(X_k) = 1 \rangle \to U, k \in I,$

is a universal object.

As in the previous section a universal object is unique.

Recall that for a group G and any field F the group algebra FG consists of formal linear combinations $\sum_i \alpha_i g_i$, where $\alpha_i \in F$, $g_i \in G$.

Consider $S = \underset{i \in I}{*} FG_i$, the free product of the group algebras FG_i.

By the results of the previous section the group algebras FG_i are embedded in S and generate it as an algebra. That's why we assume that $G_i \subset S$. By lemma the set

$$U = \{1, c_1 \cdots c_n, c_k \in \bigcup_{i \in I} (G_i \setminus 1), \text{consequtive}$$

elements c_i, c_{i+1} do not lie in the same group G_j }

is a basis of S.

Note that U is a group with respect to multiplication, all groups G_i are naturally embedded in U and generate U.

<u>Lemma</u>: $U = \underset{i \in I}{*} G_i$.

Proof. Let G be a group and let $\varphi_i : G_i \to G$, $i \in I$, be homomorphisms. These homomorphisms extend to homomorphisms $\varphi_i : FG_i \to FG$ by linearity. Hence there exists a homomorphism $\chi : S \to FG$ making all appropriate diagrams commutative.

$$\begin{tikzcd} U \ni g \arrow[r, "\chi"] & FG \\ G_i \ni g \arrow[u] \arrow[ur, "\varphi_i"'] & \end{tikzcd}$$

Since $\varphi_i(g) \in G$ we conclude that $\chi(G_i) \subseteq G$. Since the subgroups G_i generate U we get $\chi(U) \subseteq G$, $\chi : U \to G$ is a homomorphism that we have been looking for. This completes the proof of the lemma.

<u>Corollary</u>: Groups G_k are embedded in the free product $\ast_{i \in I} G_i$ and generate it. Elements in $\ast_{i \in I} G_i$ have the normal form

$$1, \quad c_1 \cdots c_n, \quad n \geqslant 1, \quad c_k \in \bigcup_{i \in I} (G_i \setminus 1),$$

consequtive elements c_i, c_{i+1} do not lie in the same group G_k.

Example. The free group $Fr(m)$ of rank m is the free product of m copies of the infinite cyclic group,

$$Fr(x_1, \dots, x_m) = \langle x_1 \rangle * \langle x_2 \rangle \dots * \langle x_m \rangle.$$

Ping-Pong Lemma.

Recall that a group G acts on a set X if there is a map $G \times X \to X$, $g \times x \to gx$, such that $g_1(g_2 x) = (g_1 g_2) x$, $1x = x$ for all elements $g_1, g_2 \in G$, $x \in X$.

Lemma (Ping-Pong Lemma). Let G_1, G_2 be nonidentical subgroups that generate G with $|G_1| \geq 3$. Also let X_1 and X_2 be nonempty subsets of X such that $X_2 \not\subseteq X_1$.

If $(G_1 \setminus \{1\}) X_2 \subseteq X_1$ and $(G_2 \setminus \{1\}) X_1 \subseteq X_2$ then $G = G_1 * G_2$.

Proof. We need to show that any alternating product $c_1 \cdots c_n$, $n \geq 1$, $c_k \in (G_1 \cup G_2) \setminus \{1\}$, any two consequtive elements c_i, c_{i+1} do not lie in the same subgroup G_1 or G_2, is $\neq 1$.

First, consider an alternating product that begins and ends with elements from G_1, namely $a_1 b_1 a_2 b_2 \cdots b_k a_{k+1}$, where $a_1, \dots, a_{k+1} \in G_1 \setminus \{1\}$; $b_1, b_2, \dots, b_k \in G_2 \setminus \{1\}$.

We have

$$a_1 b_1 a_2 \cdots b_k a_{k+1} X_2 \subseteq a_1 b_1 a_2 \cdots b_k X_1 \subseteq \cdots$$

$$\cdots \subseteq a_1 X_2 \subseteq X_1 .$$

If $a_1 b_1 a_2 \cdots b_k a_{k+1} = 1$ then $X_2 \subseteq X_1$, a contradiction.

For products of the form

$$b_1 a_1 b_2 a_2 \cdots a_k b_{k+1}$$

choose a nonidentical element $a \in G_1$. Since we have already showed that an alternating product beginning and ending with elements from G_1 is not equal to 1,

$$a^{-1} b_1 a_1 b_2 a_2 \cdots a_k b_{k+1} a \neq 1,$$

which implies $b_1 a_1 b_2 a_2 \cdots a_k b_{k+1} \neq 1$.

For products of the form

$$a_1 b_1 a_2 b_2 \cdots a_k b_k$$

choose an element $a \in G_1$, such that $a \neq a_1$, $a \neq 1$.

Then $a^{-1}a_1 b_1 a_2 b_2 \cdots b_K a \neq 1$, therefore

$a_1 b_1 a_2 b_2 \cdots a_K b_K \neq 1$.

Similarly one may show that $b_1 a_1 b_2 a_2 \cdots a_K$ is never equal to 1. This completes the proof of the lemma.

Consider the groups

$SL_2(\mathbb{C}) = \{ a \in M_2(\mathbb{C})$, 2×2 complex matrices, such that $\det(a) = 1\}$

$SL_2(\mathbb{Z}) = \{ a \in M_2(\mathbb{Z})$, 2×2 integer matrices such that $\det(a) = 1\}$

Let z be a complex number of norm $|z| \geq 2$. Let G_1 be the subgroup of $SL_2(\mathbb{C})$ generated by the matrix $\begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix}$. Clearly, G_1

is an infinite cyclic group. Let G_2 be the subgroup of $SL_2(\mathbb{C})$ generated by the matrix $\begin{pmatrix} 1 & 0 \\ z & 1 \end{pmatrix}$.

Let $\mathbb{C}^2 = \begin{pmatrix} \mathbb{C} \\ \mathbb{C} \end{pmatrix}$. Consider the subsets

$$X_1 = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{C}^2 \;\middle|\; |x| > |y| \right\},$$

$$X_2 = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{C}^2 \;\middle|\; |x| < |y| \right\}.$$

The group $SL_2(\mathbb{C})$ acts on $\mathbb{C}^2$

<u>Lemma</u>. $(G_1 \setminus \{1\}) X_2 \subseteq X_1$, $(G_2 \setminus \{1\}) X_1 \subseteq X_2$.

<u>Proof</u>. We will check only the first inclusion.

$\begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & nz \\ 0 & 1 \end{pmatrix}$. Let $n \in \mathbb{Z}$, $n \neq 0$.

Choose an element $\begin{pmatrix} x \\ y \end{pmatrix} \in X_2$, i.e. $|x| < |y|$.

Then

$$\begin{pmatrix} 1 & nz \\ 0 & 1 \end{pmatrix}\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x+nzy \\ y \end{pmatrix},$$

$$|x+nzy| \geq |n||z||y| - |x| \geq$$
$$2|n||y| - |x| \geq 2|y| - |x| > |y|;$$

hence $\begin{pmatrix} x+nzy \\ y \end{pmatrix} \in X_1$. This completes the proof of the lemma.

By the Ping-Pong Lemma the subgroup generated by $\begin{pmatrix} 1 & z \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ z & 1 \end{pmatrix}$ in $SL_2(\mathbb{C})$ is the free group ~~of~~ $F_2(2)$ of rank 2.

If $z \in \mathbb{Z}$ then we get an embedding

$$F_2(2) \hookrightarrow SL_2(\mathbb{Z}).$$

Exercise. The commutator subgroup $[F_2(2), F_2(2)]$ is a free group of countable rank, so $F_2(\infty) \hookrightarrow SL_2(\mathbb{Z})$.

Def. A group G is called residually finite if there exists a family of homomorphisms $\varphi_i : G \to G_i$, $|G_i| < \infty$, and $\bigcap_i \operatorname{Ker} \varphi_i = (1)$.

In other words:

$$\bigcap_H \{ H \lhd G, |G:H| < \infty \} = (1).$$

For any two distinct elements $a, b \in G$, $a \neq b$, there exists a homomorphism φ_i that distinguishes between them: $\varphi_i(a) \neq \varphi_i(b)$.

Let p be a prime number.

Def. A group G is called <u>residually - p</u> if there exists a family of homomorphisms $\varphi_i : G \to G_i$, G_i is a finite p-group i.e. $|G_i| = p^k, k \geq 1$, and $\bigcap_i \operatorname{Ker} \varphi_i = (1)$.

Equivalently:

$$\bigcap_H \{ H \triangleleft G, |G:H| = p^k, k \geq 1 \} = (1).$$

The homomorphism $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ gives ris to the homomorphism

$SL_n(\mathbb{Z}) \to SL_n(\mathbb{Z}/p\mathbb{Z})$. The kernel $SL_n^1(\mathbb{Z}, p)$ is called a **congruence subgroup**. It consists of invertible matrices $(a_{ij})_{n\times n}$ such that all $a_{ii} = 1$ mod p and all a_{ij}, $i \neq j$, are divisible by p, so $(a_{ij})_{n\times n} \in I_n + p\,M_n(\mathbb{Z})$.

Example. $SL_n^1(\mathbb{Z}, p)$ is a residually-p group.

Indeed, let $SL_n^1(\mathbb{Z}, p^k)$ be the kernel of the homomorphism $SL_n(\mathbb{Z}) \to SL_n(\mathbb{Z}/p^k\mathbb{Z})$, so

$$SL_n^1(\mathbb{Z}, p^k) = \{ g \in SL_n(\mathbb{Z}) \mid g = I_n + p^k M_n(\mathbb{Z}) \}.$$

Clearly,

$$\bigcap_{k\geq 1} SL_n^1(\mathbb{Z}, p^k) = (1)$$

Let $g \in SL_n^1(\mathbb{Z}, p)$, $g = I_n + pa$, $a \in M_n(\mathbb{Z})$.

Then

$$g^{p^k} = (I_n + pa)^{p^k} = I_n + \sum_{i=1}^{p^k} \binom{p^k}{i} p^i a^i$$

Each $\binom{p^k}{i} p^i$ is divisible by p^k. Hence

$g^{p^k} \in SL_n^1(\mathbb{Z}, p^k)$ and therefore

$SL_n^1(\mathbb{Z}, p)/SL_n^1(\mathbb{Z}, p^k)$ is a finite p-group.

<u>Example</u>. For any prime p the free group $F_r(2)$ is residually $-p$.

<u>Proof</u>. The subgroup generated by

$\begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ p & 1 \end{pmatrix}$ in $SL_2(\mathbb{Z})$ is isomorphic to $Fr(2)$. The matrices $\begin{pmatrix} 1 & p \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ p & 1 \end{pmatrix}$ lie in $SL_2^1(\mathbb{Z}, p)$. Hence

$$Fr(2) \hookrightarrow SL_2^1(\mathbb{Z}, p),$$

hence $Fr(2)$ is residually-p.