

Instructor: Miklos Abert  
Scribe: Keerthi Madapusi  
June 29, 2006 .

## 5. LECTURE 5

In this lecture, all our groups will be countably generated.

### 5.1. Free Groups.

**Definition 5.1.** A group  $F$  is *generated freely* by a subset  $X \subset F$  if every map  $\phi : X \rightarrow G$ , where  $G$  is any group, extends to a unique homomorphism  $\tilde{\phi} : F \rightarrow G$  and  $\langle X \rangle = F$ .

**Definition 5.2.** A group  $F$  is *free* if it is freely generated by some generating subset  $X \subset F$ .

**Definition 5.3.** An *alphabet* is just a countable set  $X = \{a_1, a_2, \dots, a_n, \dots\}$ . It does not have to be finite.

**Definition 5.4.** A *word*  $w$  is a finite sequence of pairs

$$\{(i_r, k_r) \in \mathbb{N} \times \{-1, +1\} \mid 1 \leq r \leq s\}.$$

It might be empty.

**Definition 5.5.** Given a word  $w$  and an alphabet  $X = \{a_1, \dots, a_n, \dots\}$ , we define the *word*  $w$  in the alphabet  $X$  to be

$$w(a_1, \dots, a_n, \dots) = a_{i_1}^{k_1} a_{i_2}^{k_2} \dots a_{i_s}^{k_s}.$$

This is a purely formal string and has no algebraic meaning. For example, if

$$w = ((1, -1), (1, -1), (2, 1)),$$

then

$$w(a_1, \dots, a_n) = a_1^{-1} a_1^{-1} a_2.$$

**Definition 5.6.** Given a word  $w$  in the alphabet  $X$  in which a string of the form  $a_i a_i^{-1}$  or of the form  $a_i^{-1} a_i$ , we can get a new word  $w'$  by removing that string. If we can do this, then we will denote it by  $w \mapsto w'$ .

**Definition 5.7.** We say that two words  $w$  and  $w'$  are *related by an admissible move* if either  $w \mapsto w'$  or  $w' \mapsto w$ .

**Definition 5.8.** Two words  $w$  and  $w'$  are *equivalent* if there is a finite sequence of words  $w_1, \dots, w_r$ , with  $w_1 = w$ ,  $w_r = w'$  and for  $1 \leq i \leq r-1$ ,  $w_i$  is related to  $w_{i+1}$  by an admissible move. What this means is that two words are equivalent if we can get from one word to another by either adding or removing strings of the type  $a_i a_i^{-1}$ .

**Proposition 5.9.** This defines an equivalence relation on the set of words in  $X$ .

**Definition 5.10.** A word  $w$  is *reduced* if it does not contain any strings of the form  $a_i a_i^{-1}$  or  $a_i^{-1} a_i$ .

**Lemma 5.11.** Every equivalence class of words in  $X$  has a unique reduced representative.

**Definition 5.12.** The *concatenation*  $ww'$  of two words  $w$  and  $w'$  in  $X$  is the word in  $X$  obtained by simply putting the strings corresponding to  $w$  and  $w'$  together (in that order).

**Definition 5.13.** The *product* of two reduced words  $w$  and  $w'$  in  $X$  is defined to be the unique reduced word in the equivalence class of  $ww'$ .

**Theorem 5.14.** *The set of reduced words forms a group under the product operation defined above. This group is freely generated by  $X = \{a_1, \dots, a_r, \dots\}$ , and is denoted by  $F(a_1, \dots, a_r, \dots)$ .*

*Proof.* The uniqueness of reduced words in an equivalence class tells us that the product operation is well defined. The identity is given by the empty word. We check immediately that the operation is associative, and that it has inverses. For example, if we have a word  $a_1 a_2 a_1^{-1}$ , then its inverse is the word  $a_1 a_2^{-1} a_1^{-1}$ . It's clear that the group is then generated by the set  $\{a_1, \dots, a_r, \dots\}$ . So it only remains to prove the universal property in the definition of a freely generated group.

Suppose we have a map of sets

$$\begin{aligned} \varphi : X &\longrightarrow G \\ a_i &\mapsto g_i, \end{aligned}$$

where  $G$  is a group.

We can then define a map

$$\begin{aligned} \tilde{\varphi} : F(a_1, \dots, a_r, \dots) &\longrightarrow G \\ a_i^{k_i} \dots a_r^{k_r} &\mapsto g_i^{k_i} \dots g_r^{k_r}. \end{aligned}$$

It's easy to check that this map preserves products and inverses, but the main problem is to show that it is a map in the first place! The catch is that it might not be well defined.

Take as an example the integers  $\mathbb{Z}$ . The set  $\{2, 3\}$  is a generating set for  $\mathbb{Z}$ . Define a map  $\varphi : \{2, 3\} \rightarrow \mathbb{Z}$  by  $\varphi(2) = \varphi(3) = 1$ . Then  $3 \cdot 2 - 2 \cdot 3 = 0$ , but  $3 \cdot \varphi(2) - 2 \cdot \varphi(3) = 1 \neq 0$ . So  $\varphi$  cannot be extended to a group homomorphism from  $\mathbb{Z}$  to  $\mathbb{Z}$ .

The problem in this example was that there were relations between the generators:  $2 \cdot 3 + (-3) \cdot 2 = 0$ . This problem is avoided in the case of our construction: the only way our 'map' could not be well-defined is if there was a word  $w$  equivalent to the empty word, which didn't map to the identity in  $G$ . But this cannot happen. Since  $w$  is equivalent to the empty word, and the empty word is the unique reduced word in its equivalence class, we must be able to keep performing admissible moves on  $w$  till we get the empty word. That is, we can keep taking out strings of the form  $a_i a_i^{-1}$  till there's nothing left in  $w$ . But then  $\tilde{\varphi}(w)$  has to be the identity in  $G$ . This finishes our proof.  $\square$

**Proposition 5.15.** *Every group is the homomorphic image of a free group.*

*Proof.* Let  $G$  be a group generated by some subset  $Y$ . Consider the free group  $F$  freely generated by  $Y$ . Using the universal property of  $F$ , lift the inclusion map  $Y \hookrightarrow G$  to a group homomorphism  $F \rightarrow G$ . This map must be surjective (Why?).  $\square$

**Theorem 5.16.** *Finitely generated free groups are residually finite.*

*Proof.* Let  $F$  be a free group on finitely many letters  $\{a_1, \dots, a_n\}$ . We have to prove that if  $w \neq 1$ , then there is a group homomorphism  $\varphi : F \rightarrow G$ , with  $G$  a finite group, such that  $\varphi(w) \neq 1$ . Suppose  $w = \prod_{i=1}^n a_{k_i}^{r_i}$ . By the universal property of the free group  $F$ , it's enough to construct a map

$$\begin{aligned} \psi : \{a_1, \dots, a_n\} &\rightarrow G \\ a_i &\mapsto g_i. \end{aligned}$$

such that  $w(g_1, \dots, g_n) \neq 1$ . Instead of proving this, we'll prove something stronger in the next theorem.  $\square$

**Definition 5.17.** For a prime  $p \in \mathbb{N}$ , a finite  $p$ -group is a finite group of order  $p^n$ , for some  $n \in \mathbb{N}$ .

**Theorem 5.18.** *Finitely generated free groups are residually finite 2-groups.*

*Proof.* Will be given in the next lecture. □

**Lemma 5.19.** *If  $\Gamma$  is a group, and if  $H, G \leq \Gamma$  are subgroups of finite index, then  $H \cap G$  also has finite index in  $\Gamma$ .*

*Proof.* We suppose that  $H$  and  $G$  are normal subgroups, because this is the case we'll need for the next Proposition. Then  $\Gamma/G$  and  $\Gamma/H$  are both finite groups. Consider the homomorphism

$$\begin{aligned} \varphi : \Gamma &\rightarrow \Gamma/H \times \Gamma/G \\ g &\mapsto (gH, gG). \end{aligned}$$

The kernel of  $\varphi$  is exactly  $H \cap G$ . This means that

$$\Gamma/(H \cap G) \leq \Gamma/H \times \Gamma/G$$

is a finite subgroup, and so  $H \cap G$  has finite index.

What if  $H$  and  $G$  are not normal? Hint: Consider the action of  $\Gamma$  on the coset spaces of  $H$  and  $G$ . □

**Proposition 5.20.** *For every finite group  $G$ , there exists a non-trivial element  $w \in F(a, b)$  such that for all  $a_1, a_2 \in G$ ,  $w(a_1, a_2) = 1$ .*

*Proof.* There are only finitely many homomorphisms,  $\varphi_1, \dots, \varphi_n$  from  $F(a, b)$  to  $G$ , since there are only finitely many choices in  $G$  for where  $a$  and  $b$  can be sent. Let  $H = \bigcap_{i=1}^n \ker \varphi_i$ ; then by the previous Lemma,  $H$  is a subgroup of  $G$  of finite index. In particular,  $H \neq 1$ , and so we can find a nontrivial element  $w \in H$ . But now  $\varphi_i(w) = 1 \in G$ , for all  $1 \leq i \leq n$ . With a little thought, it's easy to see that this is exactly what we wanted to prove. □

**Definition 5.21.** A *binary rooted tree* is a directed tree  $(G, E)$  with a uniquely identified vertex  $r \in G$ , called the *root*, and another subset  $L \subset G$ , not necessarily non-empty, which is called the subset of *leaves*, satisfying the following conditions:

- (1) Every vertex  $v \in G \setminus \{r\}$  has a unique parent in the tree, and  $r$  has no parent.
- (2) Every vertex  $v \in G \setminus L$  is the parent of exactly two vertices, and every vertex  $w \in L$  has no children.

(If this is too complicated, just remember the picture from Lecture).

**Definition 5.22.** A vertex  $v$  in a binary rooted tree is in the  $n^{\text{th}}$  *level*, or the  $n^{\text{th}}$  *generation*, if the unique path from  $r$  to  $v$  has length  $n$ .

**Definition 5.23.** A binary rooted tree is called an  $n^{\text{th}}$  *level tree* if every leaf  $v \in L$  is in the  $n^{\text{th}}$  level. Up to isomorphism of graphs (what is an isomorphism of graphs? See the definition of an automorphism below), there is only one such rooted tree. We denote this tree by  $T_n$ .

**Definition 5.24.** A binary rooted tree is infinite if  $L = \emptyset$ . Again, up to isomorphism, there is a unique such tree. We denote it by  $T_\infty$ .

**Lemma 5.25.** *The infinite binary rooted tree really is infinite! That is, it has infinitely many vertices.*

*Proof.* Suppose not; then we can find a vertex  $v$  that has maximal level. But  $v \notin L$ , because  $L = \emptyset$ . What happens now?  $\square$

**Definition 5.26.** An *automorphism* of a graph  $(G, E)$  is a bijection  $\varphi : G \rightarrow G$  which preserves edges in the following sense: If  $v_1, v_2 \in G$  are two vertices in  $G$  such that  $\{v_1, v_2\} \in E$  (that is, they form an edge), then  $\{\varphi(v_1), \varphi(v_2)\}$  is also in  $E$ .

**Definition 5.27.** The *automorphism group*  $\text{Aut}(G)$  of a graph  $(G, E)$  is the group of all its automorphisms, with the group operation being given by composition of automorphisms. The identity map on  $(G, E)$  gives the identity in  $\text{Aut}(G)$ .

**Proposition 5.28.** For any  $m \in \mathbb{N} \cup \{\infty\}$ ,  $\text{Aut}(T_m)$  acts transitively on the  $n^{\text{th}}$  generation vertices, for  $n \leq m$ .

*Proof.* By induction on  $n$ : for  $n = 1$ , we can just flip the two vertices that are first generation. Suppose  $\text{Aut}(T_m)$  acts transitively on the  $(n - 1)^{\text{th}}$  generation vertices, and let  $v_1$  and  $v_2$  be two  $n^{\text{th}}$  generation vertices, with parents  $w_1$  and  $w_2$ . There is some  $\varphi \in \text{Aut}(T_m)$  that takes  $w_1$  to  $w_2$ . If  $\varphi(v_1) = v_2$ , we're done; otherwise, we just need one more flip to take  $\varphi(v_1)$  to  $v_2$ .  $\square$

**Proposition 5.29.** Suppose  $m \in \mathbb{N} \cup \{\infty\}$ ; then for any  $n \leq m$ , there is a canonical copy of  $T_n$  sitting inside  $T_m$ : just take all the vertices in  $T_m$  that are in the  $n^{\text{th}}$  generation or older. Then the restriction map

$$\text{Aut}(T_m) \rightarrow \text{Aut}(T_n)$$

is a surjective group homomorphism.

**Proposition 5.30.**

$$|\text{Aut}(T_n)| = 2^{2^n - 1}.$$

In particular,  $\text{Aut}(T_n)$  is a 2-group.

*Proof.* By induction on  $n$ : if  $n = 1$ , the only automorphism of  $T_1$  is the flip. So  $|\text{Aut}(T_1)| = 2$ . Now, we have a surjective map

$$\text{Aut}(T_n) \rightarrow \text{Aut}(T_{n-1}).$$

What is the kernel of this homomorphism? It consists of all the automorphisms of  $T_n$ , which flip only the  $n^{\text{th}}$  generation vertices, and keep the rest of the vertices fixed. There are  $2^{2^n - 1}$  such flips (Why?); so we see that

$$|\text{Aut}(T_n)| = 2^{2^n - 1} |\text{Aut}(T_{n-1})| = 2^{2^n - 1 + 2^{n-1} - 1} = 2^{2^n - 1}.$$

We used the induction hypothesis to plug in the value for  $|\text{Aut}(T_{n-1})|$ .  $\square$

**Definition 5.31.** The *boundary*  $B(T_\infty)$  of the infinite binary rooted tree is the set of all infinite paths in  $T_\infty$  originating at the root  $r$ .