FREE GROUPS AND GEOMETRY

P. D. BALSDON, A. HORAWA, R. M. LENAIN, H. YANG

Group 24

Supervisor: Professor Martin Liebeck

Contents

Introduction

Mathematical objects are usually defined in an abstract, coordinate-free way, which can make them difficult to work with. A vector space over $\mathbb{R}$ is defined abstractly as a set together with two operations, but for application purposes, we often choose a basis and think about it as $\mathbb{R}^n$. Similarly, a group is defined abstractly as a set with an operation, but for many applications, it is convenient to find a *presentation* of it, that is, a set of generators and a set of relations that they satisfy.

For example, the dihedral group D_{10} is generated by two elements, σ and ϱ, that satisfy three relations: $\sigma^2 = e$, $\varrho^5 = e$, $\sigma\varrho = \varrho^{-1}\sigma$. This determines the group uniquely: the elements are any *words* in the letters σ, σ^{-1}, ϱ, ϱ^{-1}, simplified using the relations.

The *free group* on a given set of generators is the group that has no relations: its elements are any words in the generators (and their inverses). Free groups play a crucial role in group theory, since any group is a quotient of a free group by a normal subgroup that contains all the necessary relations. Therefore, if we can understand free groups and their normal subgroups, then we can understand all groups. Our project is a survey of the properties of free groups and the tools to study them.

We begin by showing that a subgroup of a free group is free. While this is a natural thing to expect (since the elements of the group do not satisfy any relations, we may expect the same to be true for the subgroups as well), it is by no means automatic. The proof is in fact fairly technical and its main idea is a graph theoretic characterisation of a free group.

Next, we study free subgroups in linear groups. Our main tool is the so-called Ping-Pong Lemma which provides a criterion for checking if two elements of a group generate a free subgroup. For example, we show that the matrices $\begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ generate a free subgroup of $\mathrm{GL}(2, \mathbb{R})$; however, the matrices $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ have a non-trivial relation between them. At this point, it is natural to ask: *how many* pairs of elements of $\mathrm{GL}(2, \mathbb{R})$ generate a free subgroup? By introducing a *measure* on the group $\mathrm{GL}(2, \mathbb{R})$, we conclude that the answer is *almost all* of them.

Finally, we present a way of studying free groups using topology. Given a free group F, we construct a topological space X whose fundamental group is F. We can then use topological properties of X to deduce algebraic properties of the group F. Most notably, *covering space* theory allows us to prove a number of results about subgroups of free groups. We prove Hall's recursive formula for the number of subgroups of index n in F and hence obtain an asymptotic approximation, also known as the *subgroup growth*.

For the sake of self-containment, we also include an appendix on group actions and an appendix on covering space theory at the end.

We would like to thank our supervisor, Professor Martin Liebeck, for suggesting different topics to pursue and helping us with the difficulties we encountered along the way.

1. Free groups and free products

In this section, we provide all the necessary background on free groups, presentations, and free products, following [Löh11, Chapter 2].

1.1. Free groups.

We start by reviewing the standard notions related to generating sets. We introduce free groups using the universal property, and prove their existence and uniqueness.

Definition 1.1.

- Let G be a group and let $S \subseteq G$. The *subgroup generated* by S (denoted $\langle S \rangle$) is the smallest subgroup (with respect to inclusion) of G that contains S. This subgroup always exists and can be expressed as follows:
$$\begin{aligned} \langle S \rangle &= \bigcap \{H \mid S \subseteq H, H \leq G\} \\ &= \{s_1^{p_1} \cdots s_n^{p_n} \mid n \in \mathbb{N}, s_1, \cdots, s_n \in S, p_1, \cdots, p_n \in \{\pm 1\}\}. \end{aligned}$$
- A group G is *finitely generated* if it contains a finite subset that generates G.
- The *rank* of a group G (denoted $\mathrm{rank}(G)$) is the smallest cardinality of a generating set for G, that is $\mathrm{rank}(G) = \min\{|X| : X \subseteq G, \langle X \rangle = G\}$. If G is finitely generated, then the rank of G is a non-negative integer.

We sometimes abuse the notation and write $\langle g, h \rangle$ instead of $\langle \{g, h\} \rangle$ and $\langle S_1, S_2 \rangle$ instead of $\langle S_1 \cup S_2 \rangle$.

Examples 1.2 (Generating sets)**.**

(1) If G is any group, then $\langle G\rangle = G$.
(2) The group $(\mathbb{Z},+)$ has two generating sets: $\langle 1\rangle = \langle 2,3\rangle = \mathbb{Z}$. Since $|\{1\}| = 1$, $\operatorname{rank}(\mathbb{Z},+) = 1$.
(3) For a non-trivial group G, we have $\operatorname{rank}(G) = 1$ if and only if G is a cyclic group.

We now introduce free groups using the universal property.

Definition 1.3 (Free groups, universal property)**.** Let S be a set. A *free group* F generated by S satisfies the following universal property: for any group G and any function $\varphi\colon S\to G$ there is a unique group homomorphism $\overline{\varphi}\colon F\to G$ extending φ, so that the following diagram commutes:

$$\begin{tikzcd}
S \arrow[r, "\varphi"] \arrow[d, hook] & G \\
F \arrow[ru, dotted, "\overline{\varphi}"'] &
\end{tikzcd}$$

where the map from S to F is the inclusion map. We call S a *free generating set* for F.

We will show that for any set S there exists a unique free group generated by S. We will first prove existence by constructing a free group as a set of words under concatenation.

Definition 1.4 (Words and reduced words)**.**

- Let S be a set. Define $A = S\cup S^{-1}$, where $S^{-1} = \{s^{-1} \mid s\in S\}$; i.e. A contains every element of S, and s^{-1} will be inverse of $s\in S$. Then we define A^* to be the set of all (finite) sequences over A; in particular this includes the empty word ε. This set A^* is the set of *words generated by* S.
- Let $n\in\mathbb{N}$ and let $s_1,\dots,s_n\in A$. The word $s_1\dots s_n\in A^*$ is *reduced* if
$$s_{j+1}\neq s_j^{-1} \text{ and } s_{j+1}^{-1}\neq s_j$$
for all $j\in\{1,\dots,n-1\}$ (in particular, ε is reduced). We write $F_{red}(S)$ for the set of reduced words in A^*.

Proposition 1.5 (Construction of a free group, existence)**.** *The set $F_{red}(S)$ of reduced words forms a free group with respect to the group law $F_{red}(S)\times F_{red}(S)\to F_{red}(S)$ given by*
$$(s_1\dots s_n, s_{n+1}\dots s_m)\mapsto (s_1\dots s_{nr}s_{n+1+r}\dots s_{n+m}),$$
where $s_1\dots s_n$ and $s_{n+1}\dots s_m$ are elements of $F_{red}(S)$, and
$$r = \max\{k\in\{0,\cdots,\min(n,m-1)\} \mid s_{n-j} = s_{n+1+j}^{-1} \textit{ and } s_{n-j}^{-1} = s_{n+1+j} \textit{ for } j = 0,\dots,k-1\}$$

Proof. We prove this is a group first.

- The group law is well-defined because the product of two reduced words is reduced.
- The empty word ε (which is reduced) is the identity under the group law.
- The inverse of a word is obtained by taking the reversed sequence and replacing letters by their inverses. (For example $(a^{-1}b^2)^{-1} = b^{-2}a$)
- It remains to prove that this group law is associative: Instead of giving a formal proof involving lots of indices, we sketch the argument graphically (Figures 1 and 2): Let $x,y,z\in F_{red}(S)$; we want to show that $(xy)z = x(yz)$. By definition, when

concatenating two reduced words, we have to remove the maximal reduction area where the two words meet.

(1) If the reduction areas of x, y and y, z have no intersection in y, then clearly $(xy)z = x(yz)$ (Figure 1).
(2) If the reduction areas of x, y and y, z have a non-trivial intersection y'' in y, then the equality $(xy)z = x(yz)$ follows by carefully inspecting the reduction areas in x and z and the neighbouring regions, as indicated in Figure 2; notice that because of the overlap in y'' , we know that x'' and z'' coincide (they both are the inverse of y'').

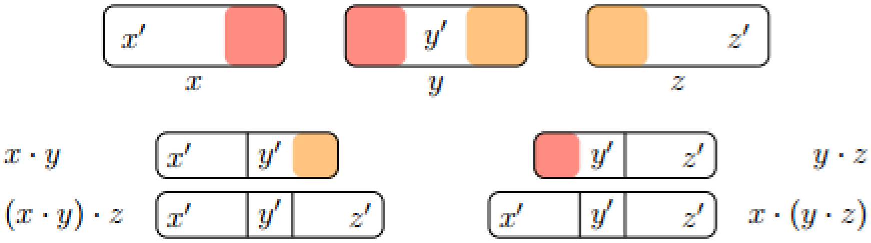


FIGURE 1. Associativity: case (1). Source: [Löh11, p. 44].

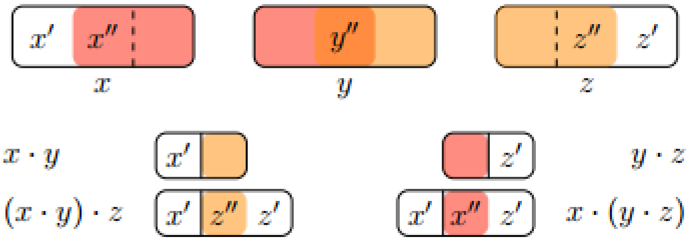


FIGURE 2. Associativity: case (2). Source: [Löh11, p. 44].

It remains to show it is a free group. To do that we verify that the universal property is satisfied. Let G be a group and let $\varphi \colon S \to G$ be a map. This defines a map $\varphi^* \colon A^* \to G$ (where A^* is the set of all words). Then

$$\overline{\varphi} = \varphi^*|_{F_{red}(S)} : F_{red}(S) \to G$$

is also a group homomorphism. Clearly, $\bar{\varphi}|_S = \varphi$ since $S \subset F_{red}(S)$. Since S generates $F_{red}(S)$, it follows that φ is the only possible homomorphism. Hence, $F_{red}(S)$ is freely generated by S. □

Remark 1.6. An alternative (but similar) construction involves defining an equivalence relation on A^* and letting the group be its equivalence classes. (For more details, see [Löh11, Theorem 2.2.7].)

We now turn to the uniqueness of free groups.

Theorem 1.7. *Let S be a set. Then, up to isomorphism, there is only one free group generated by S.*

Proof. We prove this using the universal property. Suppose there are two free groups F_1 and F_2 freely generated by S. We want to show they are isomorphic to each other. Let φ_1 and φ_2 be the inclusion map from S to F_1 and F_2 respectively (these are set theoretical maps). Because F_1 is freely generated by S, there exists a unique homomorphism $\bar{\varphi_1} : F_1 \to F_2$ such that $\bar{\varphi_1} \circ \varphi_1 = \varphi_2$, and similarly a unique homomorphism $\bar{\varphi_2} : F_2 \to F_1$ such that $\bar{\varphi_2} \circ \varphi_2 = \varphi_1$. (They are the candidates for our isomorphisms)

The composition $f_2 = \bar{\varphi_1} \circ \bar{\varphi_2} \colon F_2 \to F_2$ is a homomorphism such that:

$$f_2 \circ \varphi_2 = \bar{\varphi_1} \circ (\bar{\varphi_2} \circ \varphi_2) = \bar{\varphi_1} \circ \varphi_1 = \varphi_2$$

Note the identity map also has this property. But by the universal property, for the map $\varphi_2 : S \to F_2$, there is a unique homomorphism $f_2 : F_2 \to F_2$ such that $f_2 \circ \varphi_2(s) = \varphi_2(s)$ for also $s \in S$. Since the identity map has the property, we deduce $f_2 = \mathrm{id}_{F_2}$. Similarly, the composition $f_1 = \bar{\varphi_2} \circ \bar{\varphi_1} \colon F_1 \to F_1$ is the identity map on F_1.

So in conclusion, we have $\bar{\varphi_2} \circ \bar{\varphi_1} = \mathrm{id}_{F_1}$ and $\bar{\varphi_1} \circ \bar{\varphi_2} = \mathrm{id}_{F_2}$, this shows that they are indeed isomorphisms. □

Proposition 1.8 (Rank of free groups)**.** *Let F be a free group and $S \subset F$ be a free generating set, then* $\mathrm{rank}(F) = |S|$

Proof. We need to show if S' a generating set of F, then $|S'| \geq |S|$. By the universal property, for every function from S to C_2, there is a homomorphism from F to C_2; conversely, every homomorphism can be defined this way (since S generates F the value of a homomorphism on S determines it uniquely). Hence there are exactly $2^{|S|}$ homomorphisms from F to C_2 (since the uniqueness part from the universal property). On the other hand, if S' generates F, then there are at most $2^{|S'|}$ homomorphisms from F to C_2 (may have repeats), so $2^{|S'|}$ is an upper bound for the number of homomorphisms, which is greater than $2^{|S|}$, and hence $|S'| \geq |S|$. (This follows directly when they are finite; if they are infinite, then use Generalized Continuum Hypothesis from set theory.) □

Corollary 1.9. *All free generating sets of F have the same cardinality.*

Using this Corollary and the uniqueness of free groups, we can finally define *the* free group of rank r.

Definition 1.10 (Free group F_r)**.** Let $r \in N$ and let $S = \{x_1, \cdots, x_r\}$, where $x_1, \cdots, x_r$ are n distinct elements. Then we write F_r for *the* group freely generated by S, and call it the *free group of rank r*.

Proposition 1.11. *A group is finitely generated if and only if it is the quotient of a finitely generated free group.*

Proof. By the first isomorphism theorem, this is equivalent to the statement: a group G is finitely generated if and only if there exists a finitely generated free group F and a surjective group homomorphism $F \to G$. Note a quotient of a finitely generated group is finitely generated (the image of the generators generate the image). Conversely, let G be a finitely generated group, say generated by the finite set $S \subseteq G$. Let F be the free group generated by S, then F is finitely generated. Using the universal property of F we find a group homomorphism $\varphi \colon F \to G$ that is the identity on S (hence surjective), the $G \cong F/\ker(\varphi)$, which is what we want. □

1.2. **Presentations.** Free groups are important in group theory, because any group is a quotient of a free group by a normal subgroup. This is the so-called *presentation* of a group.

Definition 1.12 (Presentation)**.** Let S be a set, and let $R \subset (S \cup S^{-1})^*$ be a subset; let $F(S)$ be the free group generated by S. Then the group

$$\langle S|R\rangle = F(S)/\langle R\rangle^{\triangleleft}_{F(S)}$$

is said to be generated by S with the relations R; if G is a group with $G \cong \langle S|R\rangle$, then $\langle S|R\rangle$ is a *presentation* of G. Here, $\langle R\rangle^{\triangleleft}_{F(S)}$ is the smallest normal subgroup of $F(S)$ contains R. It always exists and can be expressed as:

$$\begin{aligned}\langle R\rangle^{\triangleleft}_{F(S)} &= \bigcap\{N \mid S \subset N, N \triangleleft G\} \\ &= \{g_1^{-1}s_1^{p_1}g_1 \cdots g_n^{-1}s_n^{p_n}g_n \mid n \in \mathbb{N}, s_1, \cdots, s_n \in S, p_1, \cdots, p_n \in \{\pm 1\}, g_1, \cdots, g_n \in G\}\end{aligned}$$

A group G is *finitely presented* if there exists a finite generating set S and a finite relation set R such that $G \cong \langle S|R\rangle$.

Examples 1.13 (Presentations of groups)**.**

- $\langle x|x^n\rangle \cong C_n$, for all $n \geq 1$
- $\langle x, y|x^n, y^m, xyx^{-1}y^{-1}\rangle \cong C_n \times C_m$, for all $n, m \geq 1$
- $\langle x_1, x_2, \cdots, x_r|\emptyset\rangle \cong F_r$, for all $r \geq 1$
- $\langle \rho, \sigma|\rho^n, \sigma^2, \rho\sigma\rho\sigma^{-1}\rangle \cong D_{2n}$, for all $n > 1$
- $\langle s, t|s^2, t^3, (st)^5\rangle \cong A_5$

More generally, if $G_1 \cong \langle S_1|R_1\rangle$ and $G_2 \cong \langle S_2|R_2\rangle$, then $G_1 \times G_2 \cong \langle S_1, S_2|R_1, R_2, [R_1, R_2]\rangle$, where $[R_1, R_2]$ is the *commutator.*

Theorem 1.14. *Every group has a presentation.*

Proof. Let G be a group, and consider the free group $F(G)$ generated by G. Then by the universal property of free groups, there exists a unique homomorphism $\varphi : F(G) \to G$ such that $\varphi|_G = \mathrm{id}_G$. Note this homomorphism is surjective since the identity map is surjective. And also note $\ker(\varphi) \triangleleft F(G)$, so $\langle \ker(\varphi)\rangle^{\triangleleft}_{F(S)} = \ker(\varphi)$. So by the First Isomorphism Theorem,

$$\langle G|\ker(\varphi)\rangle = {}^{F(G)}\!\big/_{\ker(\varphi)} \cong \mathrm{Im}(\varphi) = G,$$

which is a presentation for G. □

Remark 1.15. Every finite group has a finite presentation. Indeed, one can take the entire group G as the generators and the multiplication table as the relations.

Remark 1.16 (Word problem, Novikov-Boone Theorem)**.** The problem of deciding for given generators and relations whether a given word in these generators represents the trivial element in the corresponding group, is undecidable (in the sense that no such algorithm will ever exist). For more details, see Novikov-Boone Theorem [LS01, Theorem 6.3].

1.3. **Free products.** The free product of groups is a way of *multiplying* groups that does not add any new relations. For example, the free product of free groups will again be a free group.

Definition 1.17 (Free product, universal property)**.** A group G together with homomorphisms $\alpha_1 \colon G_1 \to G$ and $\alpha_2 \colon G_2 \to G$ is called a *free product* of G_1 and G_2 (denoted

$G_1 * G_2$) if the following universal property is satisfied: For any group H with homomorphisms $\varphi_1 \colon G_1 \to H$ and $\varphi_2 \colon G_2 \to H$, there is exactly one homomorphism $\varphi \colon G \to H$ of groups with $\varphi \circ \alpha_1 = \varphi \circ \alpha_2$, i.e. the following diagram commutes:

$$\begin{tikzcd}
G_1 \arrow[r, "\alpha_1"] \arrow[dr, "\varphi_1"'] & G \arrow[d, dotted, "\varphi"] & G_2 \arrow[l, "\alpha_2"'] \arrow[dl, "\varphi_2"] \\
& H &
\end{tikzcd}$$

Theorem 1.18. *Free products exist and are unique up to isomorphism.*

Proof. The uniqueness part is very similar to the proof of Theorem 1.7. It involves using universal property to find suitable isomorphisms.

For the existence part, we consider the presentation

$$G = \langle \underline{G_1} \sqcup \underline{G_2} \mid R_{G_1} \cup R_{G_2} \rangle \cong F(\underline{G_1} \sqcup \underline{G_2}) / \langle R_{G_1} \cup R_{G_2} \rangle^{\triangleleft}$$

where $\underline{G_i}$ is the *underlying set* of group G_i, and $R_{G_i} = \{ghk^{-1} | g, h, k \in \underline{G_i} \text{ such that } gh = k \in G_i\}$. The elements of $\underline{G_1}$ and $\underline{G_2}$ are treated as different letters, and hence we used the disjoint union symbol $\sqcup$. And naturally we have maps $\alpha_i : G_i \to G$, $\alpha_i(g) = N\underline{g}$.

Let H be any group with group homomorphisms $\varphi_1 \colon G_1 \to H$ and $\varphi_2 \colon G_2 \to H$. To find a homomorphism $\varphi : G \to H$, we use the universal property of free groups together with the presentation: for the map $\varphi : \underline{G_1} \sqcup \underline{G_2} \to H$,

$$\varphi(\underline{g}) = \begin{cases} \varphi_1(g) & \text{if } \underline{g} \in G_1; \\ \varphi_1(g) & \text{if } \underline{g} \in G_2, \end{cases}$$

there exists a homomorphism $\overline{\varphi} \colon G \to H$ that vanishes on the set of relations and $\overline{\varphi} \circ \alpha_1 = \varphi_1$, $\overline{\varphi} \circ \alpha_2 = \varphi_2$ by construction.

Assume that we have another homomorphism $\psi \colon G \to H$ with $\psi \circ \alpha_1 = \varphi_1$ and $\psi \circ \alpha_2 = \varphi_2$. Then $\psi|_{\underline{G_1} \sqcup \underline{G_2}} = \varphi|_{\underline{G_1} \sqcup \underline{G_2}}$. And since the image of $\underline{G_1} \sqcup \underline{G_2}$ under the projection map generates G, we see $\varphi = \psi$ and φ is indeed unique. □

Examples 1.19 (Free products)**.**

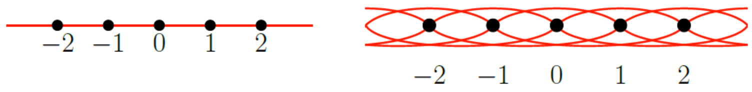
- $F_{r_1} * F_{r_2} \cong F_{r_1 + r_2}$ for any $r_1, r_2 \in \mathbb{N}$.
- $C_2 * C_2 \cong D_\infty$, where D_∞ is the infinite dihedral group.
- $C_2 * C_3 \cong \mathrm{PSL}(2, \mathbb{Z})$, where $\mathrm{PSL}(2, \mathbb{Z})$ is the modular group. (See Proposition 3.3.)

2. Subgroups of free groups are free

The goal of this section is to prove that any subgroup of a free group is free. To do that, we start by introducing Cayley graphs and considering actions of free groups on trees. For a background on group actions, see Appendix A. Throughout this section, we follow [Löh11, Chapters 3, 4] and [Ser03, Chapter 1.2].

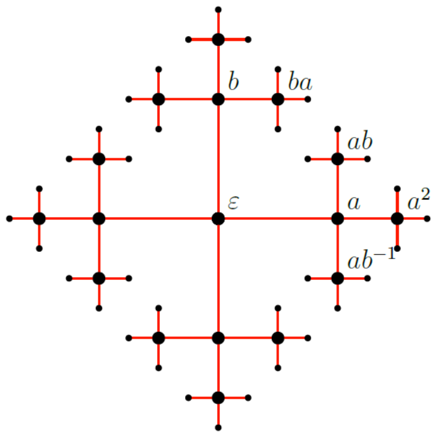
Definition 2.1. Let G be a group generated by a set $S \subseteq G$. The *Cayley Graph* of G with respect to S is $\mathrm{Cay}(G, S) = (V, E)$, where the set of vertices is $V = G$ and the set of edges is $E = \{\{g, g \cdot s\} \mid g \in G,\ s \in S \backslash \{e\}\}$.

Examples 2.2. The first examples are Cayley graphs of $\mathbb{Z}$ with respect to different generating sets, $\{1\}$ and $\{2,3\}$.



$\mathrm{Cay}(\mathbb{Z},\{1\})$ $\mathrm{Cay}(\mathbb{Z},\{2,3\})$

The second example is the Cayley graph of F_2 with respect to the generating set $\{a,b\}$.



Source for diagrams: [Löh11, p. 40].

Proposition 2.3 ([Löh11, Example 4.1.9])**.** *Let G be a group and S be a generating set for G. Then left translation action $\varphi\colon G \to \mathrm{Aut}\,(\mathrm{Cay}(G,S))$ given by $\varphi(g) = f_g$ and $f_g(h) = g \cdot h$, where the set $\mathrm{Aut}\,(\mathrm{Cay}(G,S))$ is a set of automorphisms of the Cayley graph $\mathrm{Cay}(G,S)$, is a well-defined action.*

Proof. Firstly, we show that φ is well-defined, i.e. $f_g \in \mathrm{Aut}\,(\mathrm{Cay}(G,S))$ which means that for all $x, y \in G$, x is adjacent to y if and only if $f_g(x)$ is adjacent to $f_g(y)$. Suppose x is adjacent to y in the Cayley graph; then there exists $s \in S$ such that $x = y \cdot s$. Then $f_g(y) = g \cdot y$ and

$$f_g(x) = f_g(y \cdot s) = g \cdot y \cdot s = f_g(y) \cdot s.$$

So $f_g(x)$ is adjacent to $f_g(y)$. The other implication follows the same argument with inverses.

We now show that φ is a group homomorphism, that is, $f_g \circ f_h = f_{g \cdot h}$. For any $x \in G$,

$$\left(f_g \circ f_h\right)(x) = f_g\left(f_h(x)\right) = g \cdot (h \cdot x) = (g \cdot h) \cdot x = f_{g \cdot h}(x)$$

which completes the proof. □

Proposition 2.4 ([Löh11, Prop. 4.1.10])**.** *Let G be a group and S be a generating set for G. The left translation action on the Cayley graph $\mathrm{Cay}(G,S)$ is free if and only if S does not contain any elements of order 2.*

Proof. Let us denote the left translation action by $\varphi(g) = f_g$, where $f_g(h) = g \cdot h$.

First, note that φ always acts freely on the set of verices $V = G$. Thus, we only have to consider the action φ on E.

Suppose that there exists $s \in S$ such that $s^2 = e$. Take $v \in V$, then let $v' = s \cdot v$. Since s is a generator, $\{v, v'\} \in E$. Now,

$$f_s(v) = s \cdot v = v'$$
$$f_s(v') = s \cdot v' = s \cdot s \cdot v = v$$

So, $f_s(\{v, v'\}) = \{v', v\}$, and f_s is not free.

Conversely, suppose that the action φ is not free. Then we seek to find an element in S of order 2.

Since φ is not free, but φ acts freely on V, then for some $g \in G \setminus \{e\}$ and $\{v, v'\} \in E$ we have

$$g \cdot \{v, v'\} = \{g \cdot v, g \cdot v'\} = \{v, v'\}.$$

We know that since v and v' are in an edge, for some $s \in S \cup S^{-1}$ we have $v = v' \cdot s$, and $s \neq e$. There are two cases to consider:

(1) If $g \cdot = v$ and $g \cdot v' = v'$, then $g = e$, since φ acts freely on V, a contradiction.
(2) If $g \cdot v = v'$ and $g \cdot v' = v$, then:

$$v' = g \cdot v = g \cdot v' \cdot s = v \cdot s = v' \cdot s \cdot s.$$

Thus $s^2 = e$, since φ acts freely on V. Finally, since $s \neq e$, we conclude that s has order 2.

This completes the proof. □

Theorem 2.5 ([Löh11, Theorem 4.2.1]). *A group is free if and only if it admits a free action on a (non-empty) tree.*

We will prove this by Lemmas 2.8 and 2.12, but first we need to introduce some more theory.

Theorem 2.6 ([Ser03, Prop. 1.15]). *Let F be a free group, which is freely generated by $S \subset F$. Then the corresponding Cayley graph, $X = \mathrm{Cay}(F, S)$ is a tree.*

In this proof, the elements of the basis set S both denote the group elements and edges of the Cayley graph. The use is clear form the context.

Proof. Since F is freely generated by S, we can write any element $g \in F$ uniquely as $g = s_1^{\varepsilon_1} s_2^{\varepsilon_2} \dots s_n^{\varepsilon_n}$, where $s_i \in S$ and $\varepsilon_i \in \{\pm 1\}$. Take any $g, h \in F$. Then $g = s_1^{\varepsilon_1} s_2^{\varepsilon_2} \dots s_n^{\varepsilon_n}$ and $h = t_1^{\xi_1} t_2^{\xi_2} \dots t_n^{\xi_n}$. So the vertices corresponding to g and h in the graph X are connected by the path from g to h:

$$s_n^{-\varepsilon_n}, \dots, s_1^{-\varepsilon_1}, t_1^{\xi_1}, t_2^{\xi_2}, \dots, t_n^{\xi_n}.$$

Thus we conclude that X is connected.

We now need to show that it contains no cycles. Suppose for a contradiciton that X does contain a cycle and denote it by

$$p = s_1^{\varepsilon_1}, s_2^{\varepsilon_2}, \dots, s_n^{\varepsilon_n}$$

where if $s_i = s_{i+1}$ then $\varepsilon_i = \varepsilon_{i+1}$, and $n > 2$. Then $e = s_1^{\varepsilon_1} s_2^{\varepsilon_2} \dots s_n^{\varepsilon_n}$ which is a non-trivial relation on the elements of S, contradicting the fact that S freely generates F. □

Note that in general the converse statement is not true. We therefore add another hypothesis to obtain the following theorem.

Theorem 2.7 ([Ser03, Prop. 1.15])**.** *Let G be a group and S be a generating set of G such that $S \cap S^{-1} = \emptyset$. If the the Cayley graph $X = \mathrm{Cay}(G, S)$ is a tree, then G is freely generated by S.*

Proof. Suppose, for a contradiction, that S does not freely generate G. Then there is a non-trivial word (a word which does not reduce to the identity) such that its image is the point e. Choose such a word of minimal length, n, and denote it $\hat{g} = s_1^{\varepsilon_1} s_2^{\varepsilon_2} \dots s_n^{\varepsilon_n}$. Where $s_i \in S$ and $\varepsilon_i \in \{\pm 1\}$. Let P_i denote the image of the element $s_1^{\varepsilon_1} \dots s_i^{\varepsilon_i}$ in X, where $i \in \{1, 2, \dots n\}$, and let P_0 denote the image of e_G. Since $\hat{g}$ is minimal, then the P_i's are all distinct, for $i \in \{0, 1, \dots n-1\}$. (Suppose $P_i = P_j$ for some $i, j \in \{0, 1, \dots n-1\}$, then $s_{i+1}^{\varepsilon_{i+1}} \dots s_j^{\varepsilon_j}$ is a shorter element than $\hat{g}$). So, we have that $P_0 = P_n$, and the points P_i and P_{i+1} are adjacent in X. Thus we have a cycle in X, which is contradiction with X being a tree. □

We can now prove the first implication of Theorem 2.5.

Lemma 2.8. *If a group is free, then it admits a free action on a non-empty tree.*

Proof. Let F be a free group, freely generated by S; then $\mathrm{Cay}(F, S)$ is a tree by Theorem 2.6. We will show that F acts freely on $\mathrm{Cay}(F, S)$ by left translations (see Proposition 2.3). Since S is a free generating set, then none of its elements has order 2 (otherwise, $s^2 = e$ is a non-trivial relation). Then by Proposition 2.4, the left translation is a free action on the graph. □

To prove the other implication of Theorem 2.5, we need to introduce spanning trees. Recall that a *subtree* is a subgraph which is also a tree.

Definition 2.9. Let X be a connected graph, and $\varphi \colon G \to \mathrm{Aut}\,(X)$ be an action of G on X. A *spanning tree* for φ is a subtree Y of X such that $\# G(x) \cap Y = 1$ for each $x \in X$, i.e. each orbit of the action is represented by exactly one vertex of Y.

Remark 2.10. Orbits are distinct by Proposition A.7.

Theorem 2.11 ([Löh11, Theorem 4.2.4])**.** *Every action of a group on a connected graph by graph automorphisms admits a spanning tree.*

This proof involves partial and total orderings, and uses Zorn's lemma. For more details, see [Rei95, Section 1.7].

Proof. Let G be a group acting on the connected graph X. Let T_G be the set of all subtrees of X that contain at most one element from each orbit $G(v)$. We see that the subset relation, $\subseteq$, is a partial ordering on this set, and that the proper subset relation, $\subset$, is a total ordering on this set.

Any sequence $\{A_i\}_{i=1}^{\infty}$ of elements of T_G such that $A_1 \subset A_2 \subset \dots$ (a totally ordered chain) has an upper bound, $\bigcup_{i=1}^{\infty} A_i$ (where we take separately the union of the edges and the vertices). Therefore, we can apply Zorn's lemma, to obtain that there is a maximal element $T \in T_G$. This means that for all $T' \in T_G$, we have that:

$$T \not\subset T' \tag{1}$$

We claim that T is a spanning tree for the action of G on X. Firstly, since $T \in T_G$ we have that there is *at most* one element of each orbit in T. We now need to show that there is *at least* one element from each orbit in T.

Suppose contrary that there exists $v \in X$ such that no points of $G(v)$ are in T. Since X is connected, for any $u \in T$ there exists a path from u to v in the graph X. Let p be the shortest path in X that connects some vertex $u \in T$ to some vertex in $G(v)$ and let n be the length of p.

Let v' be the first point along this path such that $v' \notin T$. Consider the orbit $G(v')$ of v'. We have two possible cases: either (a) $G(v') \cap T = \emptyset$ or (b) $G(v') \cap T \neq \emptyset$.

(a) Suppose that they are disjoint and let u' denote an element in T which is connected to v'. (This exists since v' is the first element in the path that is not in T, so the element before v' in the path is in T). Then if we take the tree T, and add the edge $\{u', v'\}$ and the vertex v', we obtain a new tree, $T^\star$. Clearly, $T^\star$ has at most one element of any orbit, so $T^\star \in T_G$, and $T \subset T^\star$, which contradicts equation 1.

(b) Suppose that there is an element in $G(v') \cap T$, i.e. there exists $g \in G$ such that $g \cdot v' \in T$. Let p' denote the subpath of p connecting v' to v and m be its length. Clearly $m < n$, since the path p starts at u which is in T, whilst v' is not in T. It also clear that $m \neq 0$; otherwise, $v' = v$, and hence $G(v') = G(v)$, so there cannot be an element in the intersection of $G(v')$ and T.

Consider the path $g \cdot p$, which connects the vertex $g \cdot v'$ to $g \cdot v$. Then we have a path $g \cdot p'$ of length m connecting a vertex in T to a vertex in $G(v)$, where $0 < m < n$. This contradicts the fact that p was chosen to be the shortest path connected a vertex $u \in T$ to a vertex in $G(v)$.

This completes the proof. □

Now we have enough tools to prove the other implication of Theorem 2.5.

Lemma 2.12. *If a group admits a free action on a non-empty tree, then it is free.*

Proof. Let G be a group which acts freely on a tree, T, by graph automorphisms. Then by Theorem 2.11 there exists a spanning tree T' for this action. In this proof, we call an edge of T *essential* if one of its vertices is in T', whilst the other vertex is not. (Then by the uniqueness of paths in trees, the edge is also not in T').

The proof consists of three parts: constructing a generating set S, showing that it generates G, and showing that it freely generates G.

Step 1. Construction of S**.** Take any essential edge $f = \{u, v\}$ of T, where u is a vertex of T', and v is not a vertex of T'. Since T' is a spanning tree, there exists a group element $g_f \in G$ such that $g_f^{-1} \cdot v$ is a vertex in T'. (We can say equivalently that v is a vertex of $g_f \cdot T'$). The element g_f is uniquely determined; indeed, if we have two distinct elements of G, g_f and g'_f with this property, then $g_f \cdot v \neq g'_f \cdot v$ since G acts freely on X. So we have two distinct representatives of the orbit $G(v)$ in T', which contradicts that T' is a spanning tree.

Let $\widetilde{S} = \{g_f \in G \mid f \text{ is an essential edge of } T\}$. Then $\widetilde{S}$ has the following properties:

(1) The identity element of G is not in $\widetilde{S}$, by definition.
(2) $\widetilde{S}$ has no element of order 2:

Suppose g_f has order 2, so $g_f = g_f^{-1}$, and let $f = \{u, v\}$ be the corresponding essential edge, where $u \in T'$, and $v \in g_f \cdot T'$. Then $g_f \cdot u \in g_f \cdot T'$, and $g_f \cdot v \in T'$. So the edge $g_f \cdot f = \{g_f \cdot u, g_f \cdot v\}$ links T' to $g_f \cdot T'$. We see that the edge f also links these two trees. Since T is a tree, then these edges are the same by the uniqueness of paths. This contradicts that G acts freely on T.

(3) If $g_f = g_{f'}$, then $f = f'$:

Both of the edges f and f' connect the spanning tree T' to $g_f \cdot T'$. Then since T is a tree, we must have that $f = f'$.

(4) If $g \in \widetilde{S}$, then $g^{-1} \in \widetilde{S}$:

Let $f = \{u, v\}$ be the corresponding essential edge for g (i.e. $g = g_f$). Then $g^{-1} \cdot f = \{g^{-1} \cdot u, g^{-1} \cdot v\}$, and $g^{-1} \cdot v \in T'$, so g^{-1} is also an essential edge. We want to find the element h of G such that $h^{-1} \cdot (g^{-1} \cdot u) \in T'$. Since $u \in T'$, then clearly $h = g^{-1}$. So $g^{-1} = h = g_{(g^{-1} \cdot f)} \in \widetilde{S}$

So every element of $\widetilde{S}$ has a unique partner, namely its inverse. So we can split $\widetilde{S}$ into two sets by choosing one element from each pair to go into S and the other into S^{-1}. Then we have:

$$S \cap S^{-1} = \emptyset; \quad |S| = \frac{|\widetilde{S}|}{2}$$

Step 2. S **generates** G**.** It is enough to show that $\widetilde{S}$ generates G, since $S \cap S^{-1} = \emptyset$.

Take any $g \in G$; we want to show that g can be written as $s_1 s_2 \cdots s_n$, where $s_i \in \widetilde{S}$. Take any $v \in T'$, and let p denote the path from v to $g \cdot v$. Then the path p passes through copies of T':

$$g_0 \cdot T', \ldots, g_n \cdot T',$$

where these graphs are in the order that p passes through them, and any consecutive graphs are distinct. Note that g_0 is the identity element in G, and $g_n = g$.

Take any $j \in \{0, \ldots, n-1\}$, then $g_j \cdot T'$ and $g_{j+1} \cdot T'$ are joined by the edge $f_j = \{u_j, v_j\}$. Clearly

$$g_j^{-1} \cdot f_j = \{g_j^{-1} \cdot u, g_j^{-1} \cdot v\}$$

is an essential edge. So there exists $s_j \in \widetilde{S}$ such that $s_j^{-1} \cdot (g_j^{-1} \cdot v_j) \in T'$. We also have that $v_j \in g_{j+1} \cdot T'$, so $g_{j+1}^{-1} \cdot v_j \in T'$.

Since T' has only one element from $G(v)$, then

$$g_{j+1}^{-1} \cdot v_j = s_j^{-1} \cdot (g_j^{-1} \cdot v_j).$$

Also, since the group action is free, we can conclude that $g_{j+1}^{-1} = s_j^{-1} \cdot g_j^{-1}$, which we can rearrange to $s_j = g_j^{-1} g_{j+1}$.

Recall that $g = g_n$, $g_0 = e_G$, so we can write:

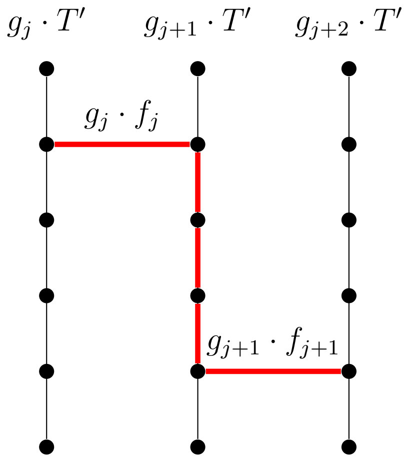
$$\begin{aligned} g &= g_0^{-1} \cdot g_n \\ &= g_0^{-1} \cdot g_1 \cdot g_1^{-1} \cdot \ldots \cdot g_{n-1}^{-1} \cdot g_n \\ &= s_0 \cdot \ldots \cdot s_{n-1} \end{aligned}$$

So, for all $g \in G$, we can generate g from elements of $\widetilde{S}$, and hence from S.

Step 3. S **freely generates** G**.** By Theorem 2.7, it suffices to show that $\mathrm{Cay}(G, S)$ does not contain any cycles. Indeed, $\mathrm{Cay}(G, S) = \mathrm{Cay}(G, \widetilde{S})$, since $\widetilde{S} = S \cup S^{-1}$.

Suppose, for a contradiction, that there is a cycle $P_0, \dots, P_{n-1}$ in $\mathrm{Cay}(G, \widetilde{S})$, where P_i corresponds to a vertex on the Cayley graph. Let g_i denote the group element who's image is P_i. Then the elements $\sigma_j = g_j^{-1} \cdot g_{j+1}$ is in $\widetilde{S}$ for all $j \in \{1, n-1\}$, since they correspond to edges on the Cayley graph. We also have that $\sigma_n = g_{n-1}^{-1} \cdot g$ is in $\widetilde{S}$, (since it corresponds to the edge that completes the cycle.)

Figure 3. Diagram for proof of Lemma 2.12



For all $j \in \{1, \dots n\}$, let f_j be an essential between T' and $\sigma_j \cdot T'$. We want to show that we can connect the vertices of $g_j \cdot T'$ and $g_{j+1} \cdot T'$ without going through any other copies of T'. For the following paragraph, it may be helpful to look at Figure 3.

Since $g_{j+1} \cdot T'$ is connected, then there is a path from all the vertices of $g_{j+1} \cdot T'$ to the vertex of $g_{j+1} \cdot f_{j+1}$ in $g_{j+1} \cdot T'$. We notice that $g_{j+1} \cdot T' = g_j \cdot (\sigma_j \cdot T')$, so since T' and $\sigma_j \cdot T'$ are connected by f_j, then $g_j \cdot T'$ is connected to $g_j \cdot (\sigma_j \cdot T') = g_{j+1} \cdot T'$ by $g_j \cdot f_j$. So we can extend the path we previously had in $g_{j+1} \cdot T'$ with the essential edge $g_j \cdot f_j$ so that we connect $g_j \cdot T'$ to $g_{j+1} \cdot T'$ without going through any other copies of T'.

We concatenate these paths together, and obtain a path from $g_0 \cdot T'$ to $g_n \cdot T'$ via the trees $g_1 \cdot T', \dots, g_n \cdot T'$. However, since $P_0, \dots, P_{n-1}$ is a cycle in the Cayley graph, then $g_n = g_0 \cdot \sigma_1 \cdot \dots \cdot \sigma_n = g_0$. Thus we see that our path in T is a cycle, which contradicts the fact that T is a tree. □

Another way to prove the lemma is to use covering space theory. We follow the ideas briefly presented in [Löh11, Remark 4.2.5].

Alternative proof of Lemma 2.12. Suppose G acts freely on a tree T. Since the action is free, for each $t \in T$ there exists a neighbourhood U such that $g_1(U) \cap g_2(U) \neq \emptyset$ implies $g_1 = g_2$ for any $g_1, g_2 \in G$, so we can use Theorem B.4 to obtain a covering map $p \colon T \to T/G$ and

$$G \cong \frac{\pi_1(T/G)}{p_*(\pi_1(T))} \cong \pi_1(T/G),$$

since a tree is contractible. Finally, since T is a tree, T/G is a tree with some of the vertices identifies, i.e. a graph. There exists a spanning tree for the graph T/G with the action of G by Theorem 2.11, so if we contract it, we conclude that T/G is homotopically equivalent to a bouquet of circles. Then $G \cong \pi_1(T/G)$ is a free group by Seifert-van Kampen theorem [Hat02, Theorem 1.20]. □

Lemmas 2.8 and 2.12 together yield Theorem 2.5. The main theory of the section now follows as a corollary to Theorem 2.5.

Corollary 2.13 ([Löh11, Corollary 4.3.1])**.** *Subgroups of free groups are free.*

Proof. Let F be a free group, and H be a subgroup of F. Then F acts freely on a tree by Theorem 2.5. Then clearly H also acts freely on this tree, so again by Theorem 2.5, H is free. □

One can also prove this result directly using covering space theory. We follow the ideas briefly presented in [Löh11, Remark 4.3.3].

Alternative proof of Corollary 2.13. Suppose G is a subgroup of a free group F_r. Note that F_r is the fundamental group of a bouquet X of r circles, so by Theorem B.2, G corresponds to a connected pointed covering $p\colon \tilde{X} \to X$ of X. Since X can be thought of as a graph, the covering space $\tilde{X}$ is a connected graph. Then there exists a spanning tree for $\tilde{X}$ with the action of G by Theorem 2.11, so by contracting the spanning tree, $\tilde{X}$ is homotopically equivalent to a bouquet of circles. Therefore $G \cong \pi_1(\tilde{X})$ is a free group by the Seifert-van Kampen theorem [Hat02, Theorem 1.20]. □

We can also calculate the rank of the subgroup, given its index.

Corollary 2.14 (Schreir index formula, [Löh11, Corollary 4.3.2])**.** *Let F be a free group of rank r_F, and H be a subgroup of F with finite index k. Denote the rank of H as r_H, then*

$$r_H = k(r_F - 1) + 1$$

Proof. Let $T = \mathrm{Cay}(F, S)$, where S freely generates F. So T is a tree by Theorem 2.6. From the proof of Lemma 2.12, we see that the rank of H is $\frac{E}{2}$, where E denotes the number of essential edges of the action of H on on T.

We will determine E by a counting argument. Let T' be a spanning tree for the action H on T. Then since the index $[F : H] = k$, we see that T' has k vertices. Let $d_T(v)$ denote the number of edges a vertex has, for all $v \in T$, and let $V(T')$ denote the set of vertices of T'. We calculate the sum of the number of edges that the vertices of T' have in two different ways.

The tree T' has k vertices, so it has $k-1$ internal edges. Each edge is counted twice when we sum over the tree, so we obtain that:

$$\sum_{v \in V(T')} d_T(v) = 2 \cdot (k-1) + E.$$

We also notice that because S freely generates F, every vertex has $2 \cdot |S| = 2 \cdot r_F$ edges. So we obtain

$$\sum_{v \in V(T')} d_T(v) = 2 \cdot r_F \cdot k.$$

Putting these two results together, we obtain that $E = 2 \cdot r_F \cdot k - 2(k-1)$, so

$$r_H = r_F \cdot k - k + 1 = k(r_F - 1) + 1$$

which completes the proof. □

Corollary 2.15. *The free group $F_2 = \langle a, b \rangle$ contains a free subgroup of rank r.*

Proof. For $r = 1$, $\langle a \rangle$ is a subgroup of F_2 of rank 1. For $r \geq 2$, by the Shreier index formula 2.14 it is enough to find a subgroup of index $k = r - 1$. Define

$$G = \{w \in F_2 \mid \text{sum of the powers of the generators in } w \text{ is } k\}$$

where we interpret w as a reduced word in a and b. (For example, the sum of the powers in a^2ba^{-1} is 2.) First, note that G is a subgroup of F_2:

- If the sum of the powers in w is nk, then the sum of the powers in w^{-1} is $-nk$.
- If the sum of the powers in w_1, w_2 is n_1k, n_2k, respectively, then the sum of the powers in w_1w_2 is $(n_1 + n_2)k$.

Moreover, $F_2/G = \{G, aG, a^2G, \ldots, a^{k-1}G\}$, which shows that $[F_2 : G] = k$. □

Remark 2.16 (Kurosh subgroup theorem)**.** A more general result states that any subgroup of a free product of groups is a free product of groups. For more details, see [CFR11, Theorem 14.8.8].

3. The Ping-Pong Lemma

This section is devoted to the Ping-Pong Lemma, a result that allows us to check if a group is a free product of two groups.

Theorem 3.1 (Ping-Pong Lemma)**.** *Let G be a group acting on a set X. Let H_1 and H_2 be two subgroups of G, such that $|H_1| \geq 3$. If there are non-empty subsets $X_1, X_2 \subseteq X$ such that $X_2 \not\subseteq X_1$ and*

$$h(X_2) \subseteq X_1, \quad \text{for all } h \in H_1 \setminus \{e\} \tag{2}$$

$$h(X_1) \subseteq X_2, \quad \text{for all } h \in H_2 \setminus \{e\} \tag{3}$$

then $\langle H_1, H_2 \rangle \cong H_1 * H_2$.

Proof. We have to show that elements in Γ do not satisfy any other relation, i.e. if w is a non-empty reduced word formed by letters in $H_1\backslash\{e\}$ and $H_2\backslash\{e\}$, then w is not the identity. We then have four cases:

(i) Suppose w starts and ends with an element of $H_1\backslash\{e\}$. Say

$$w = a_1b_1a_2b_2 \ldots b_{k-1}a_k, \quad \text{for } a_i \in H_1\backslash\{e\} \text{ and } b_i \in H_2\backslash\{e\}.$$

Then we have

$$\begin{aligned} w(X_2) = a_1b_1 \ldots b_{k-1}a_k(X_2) &\subseteq a_1b_1 \ldots a_{k-1}b_{k-1}(X_1) \text{ by (2)} \\ &\subseteq a_1b_1 \ldots a_{k-1}(X_2) \text{ by (3)} \\ &\ldots \\ &\subseteq a_1(X_2) \subseteq X_1 \end{aligned}$$

We assumed $X_2 \not\subseteq X_1$, therefore $w \neq e$.

(ii) Suppose that $w = a_1b_1a_2 \ldots b_k$. Then define a to be any element in $H_1\backslash\{e, a_1^{-1}\}$. One can now use a same argument as part (i) with awa^{-1} to show

$$awa^{-1}(X_2) \subseteq X_1$$

which implies $awa^{-1} \neq e$. Therefore $w \neq e$ since awa^{-1} starts and ends with an element of $H_1 \backslash \{e\}$.

(iii) Suppose that $w = b_1 a_2 b_2 \dots a_k$. Similarly as before, define a to be any element in $H_1 \backslash \{e, a_k^{-1}\}$, and use a same argument as part (i) with awa^{-1} to show

$$awa^{-1}(X_2) \subseteq X_1$$

which implies $w \neq e$.

(iv) Suppose that $w = b_1 a_2 \dots b_k$, let $a \in H_1 \backslash \{e\}$ and use the same argument as part (i) to show $w \neq e$. □

The following corollary presents a special case of the Ping-Pong Lemma which is easier to apply in practice.

Corollary 3.2. *Let G be a group acting on a set X and let $g_1, g_2 \in G$ such that $o(g_1) \geq 3$. If there exist non-empty subsets $X_1, X_2 \subseteq X$ such that $X_2 \not\subseteq X_1$ and for any $n \neq 0$*

$$g_1^n(X_2) \subseteq X_1,$$
$$g_2^n(X_1) \subseteq X_2,$$

then $\langle g_1, g_2 \rangle \cong \langle g_1 \rangle * \langle g_2 \rangle$.

Proof. Let $H_1 = \langle g_1 \rangle$ and $H_2 = \langle g_2 \rangle$ and apply the Ping-Pong Lemma 3.1 to obtain the result. □

Throughout the rest of the section, we present various applications of the Ping-Pong Lemma.

Proposition 3.3 ([Alp93])**.** *The modular group* $\mathrm{PSL}(2, \mathbb{Z})$ *is isomorphic to the free product of cyclic groups $C_2 * C_3$.*

In order to prove this theorem we first need the following lemma from [Con].

Lemma 3.4. *The matrices*

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \; B = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

generate $\mathrm{SL}(2, \mathbb{Z})$.

Proof. Take any

$$T = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z}).$$

Then for $n \in \mathbb{Z}$:

$$A^n T = \begin{pmatrix} a + cn & b + nd \\ c & d \end{pmatrix}, \; BT = \begin{pmatrix} -c & -d \\ a & b \end{pmatrix}$$

We are going to apply a version of the division algorithm. If $c = 0$, then $a = d = \pm 1$ since $\det(T) = 1$. Suppose now $c \neq 0$. If $|a| < |c|$, let $T' = BT$ (this exchanges rows, with a sign change), and use the following argument. If $|a| \geq |c|$, define

$$a = cq + r \text{ (i.e. } a - qc = r)$$

such that $0 \leq r < |c|$. This is possible by the division algorithm. Now

$$A^{-q} = \begin{pmatrix} 1 & -q \\ 0 & 1 \end{pmatrix}, \ A^{-q}T = \begin{pmatrix} a-qc & b-qd \\ c & d \end{pmatrix} = T^{(1)}$$

where $a - qc < |c|$. Now apply B on the left to $T^{(1)}$. If $a - qc = r = 0$, proceed to the next step. If not, repeat this part of the algorithm with $T^{(1)}$. By the division algorithm, we will eventually get $r = 0$. We obtain a matrix of the form

$$MT = \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z}), \ M \in \langle A, B \rangle$$

Therefore $\det(MT) = 1$ which implies $x = z = \pm 1$, so $MT = \pm A^y$ which gives the desired result $T \in \langle A, B \rangle$, since M is invertible. □

We can now prove the previously stated theorem.

Proof of Theorem 3.3. Define two matrices in $\mathrm{SL}(2, \mathbb{Z})$ as follows:

$$A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \ B = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

By Lemma 3.4, A and B generate $\mathrm{SL}(2, \mathbb{Z})$. Therefore their images (say $\tilde{A}$ and $\tilde{B}$) in $\mathrm{PSL}(2, \mathbb{Z}) = \mathrm{SL}(2, \mathbb{Z})/\langle \pm I \rangle$ generate $\mathrm{PSL}(2, \mathbb{Z})$. This group acts on $\hat{\mathbb{C}}$ by Möbius transformations:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot z = \frac{az + b}{cz + d}$$

where by $[X]$ we denote the equivalence class of the matrix $X \in \mathrm{SL}(2, \mathbb{Z})$ in $\mathrm{PSL}(2, \mathbb{Z})$. Let

$$C = AB = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}.$$

Then B and C generate $\mathrm{SL}(2, \mathbb{Z})$, since $A = CB^{-1}$, so letting $\tilde{C}$ be the image of C, $\tilde{B}$ and $\tilde{C}$ also generate $\mathrm{PSL}(2, \mathbb{Z})$.

Now, let P be the set of positive irrational numbers and N be the set of negative irrational numbers, which gives $P, N \subset \mathbb{R} \subset \hat{\mathbb{C}}$. Note that $\tilde{C}$ has order 3 and $\tilde{B}$ has order 2 in $\mathrm{PSL}(2, \mathbb{Z})$. Therefore, it is enough to check that $\tilde{B}^n(P) \subseteq N$ for $n = 1$ and $\tilde{C}^n(N) \subseteq P$ for $n = 1, -1$. The elements $\tilde{B}$, $\tilde{C}$ and $\tilde{C}^{-1}$ act on $\hat{\mathbb{C}}$ as follows:

$$\tilde{B} \colon z \mapsto \frac{-1}{z}, \quad \tilde{C} \colon z \mapsto \frac{z-1}{z}, \quad \tilde{C}^{-1} \colon z \mapsto \frac{1}{1-z}.$$

Hence

$$\tilde{B}(P) \subseteq N, \quad \tilde{C}(N) \subseteq P, \quad \tilde{C}^{-1}(N) \subseteq P$$

so Corollary 3.2 implies

$$\langle \tilde{B}, \tilde{C} \rangle \cong \langle \tilde{B} \rangle * \langle \tilde{C} \rangle \cong C_2 * C_3$$

since $\tilde{B}$ has order 2 and $\tilde{C}$ has order 3. □

The Ping-Pong Lemma 3.1 also allows us to check that $\mathrm{SL}(2, \mathbb{R})$ contains a free group of rank 2 as a subgroup.

Proposition 3.5. *The subgroup of* $\mathrm{SL}(2,\mathbb{R})$ *generated by*

$$A = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}, \; B = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$$

is free of rank 2.

Proof. To use Corollary 3.2, we let $\mathrm{SL}(2,\mathbb{R})$ act on $\mathbb{R}^2$ by linear transformations, and define:

$$X_1 = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \text{ such that } |x| > |y| \right\} \subset \mathbb{R}^2$$

$$X_2 = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \text{ such that } |x| < |y| \right\} \subset \mathbb{R}^2$$

$$g_1 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$$

$$g_2 = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$$

Note that

$$g_1^n = \begin{pmatrix} 1 & 2n \\ 0 & 1 \end{pmatrix}, \quad g_2^n = \begin{pmatrix} 1 & 0 \\ 2n & 1 \end{pmatrix}.$$

Hence, for $n \neq 0$ and $v = (x, y)^T \in X_2$:

$$g_1^n v = \begin{pmatrix} x + 2ny \\ y \end{pmatrix}$$

Now $|x + 2ny| \; \geq |2ny| - |x| \; > |2ny| - |y| \; \geq |y|$ since $v \in X_2$, thus $g_1^n v \in X_1$. Similarly one can prove that for $n \neq 0$, $g_2^n(X_1) \subseteq X_2$. Therefore, by Corollary 3.2,

$$\langle g_1, g_2 \rangle \cong \langle g_1 \rangle * \langle g_2 \rangle \cong F_2,$$

since these two matrices are of infinite order. □

Remark 3.6. If we let $A = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$ and $B = \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix}$, for any $|t| \geq 2$, then we can adjust the above argument to show that $\langle A, B \rangle \cong F_2$.

However, not every pair of matrices of this form generates a free group.

Example 3.7. The subgroup of $\mathrm{SL}(2,\mathbb{R})$ generated by the matrices

$$A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \; B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

is not free. Indeed,

$$ABA^{-1}BAB^{-1} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

is a non-trivial relation between A and B. It turns out that these matrices generate $\mathrm{SL}(2,\mathbb{Z})$

Remark 3.8. One can find matrices A and B of the form described in Remark 3.6 with $|t| < 2$ that do generate a free group. Indeed, suppose t is any transcendental number with $|t| < 2$ (for example, $t = \pi/4$), meaning that it is not the root of any non-zero polynomial with integer coefficients. Any word in A, A^{-1}, B, B^{-1} is of the form

$$\begin{pmatrix} p_1(t) & p_2(t) \\ p_3(t) & p_4(t) \end{pmatrix}$$

where p_i is a polynomial with integer coefficients. If there was a non-trivial relation between A and B, then we would have $p_2(t) = p_3(t) = 0$ and at least one of p_2 and p_3 would be non-trivial, which would contradict transcendentality of t. Therefore, $\langle A, B\rangle \cong F_2$.

Another example from [dlH00] shows how to construct a subgroup isomorphic to F_r in the modular group.

Proposition 3.9. *Let $r \in \mathbb{N}$ and let $D_1, D_2, \dots, D_{2r}$ be $2r$ closed discs in $\hat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$. For any $k \in \{1, 2, \dots, 2r\}$, let $h_k \in \mathrm{PSL}(2,\mathbb{C})$ be such that $h_k(\hat{\mathbb{C}} \setminus D_{2k-1}) \subseteq D_{2k}$ (existence is assumed here). Then*

$$\langle h_1, h_2, \dots, h_r\rangle \cong F_r.$$

Proof. For $k = 1, \dots, r$, let $X_k = D_{2k-1} \cup D_{2k}$. By construction, $h_1^n(X_2) \subset X_1$ and $h_2^n(X_1) \subset X_2$ for $n \neq 0$ and $X_1 \neq X_2$, so we can apply Corollary 3.2 to X_1 and X_2 to show that

$$\langle h_1, h_2\rangle \cong \langle h_1\rangle * \langle h_2\rangle \cong F_2$$

Now, apply the Ping-Pong Lemma 3.1 to $X_1 \cup X_2$ and X_3 with the subgroups $\langle h_1, h_2\rangle$ and $\langle h_3\rangle$ to obtain:

$$\langle h_1, h_2, h_3\rangle \cong \langle h_1, h_2\rangle * \langle h_3\rangle \cong \langle h_1\rangle * \langle h_2\rangle * \langle h_3\rangle \cong F_3.$$

Continuing in this way, we show that

$$\langle h_1, h_2, \dots, h_r\rangle \cong \langle h_1\rangle * \langle h_2\rangle * \cdots * \langle h_r\rangle \cong F_r$$

which completes the proof. □

4. Free subgroups in linear groups

The main goal of this section is to show that *almost all* n-tuples of elements of $\mathrm{GL}(n,\mathbb{C})$ generate free groups. For that sake, we review the notions of solubility and the Haar measure.

4.1. **Solubility.**

In this subsection, we recall the definition of solubility and prove that free groups of rank at least 2 are not soluble following [Rot95, p. 102–103].

Definition 4.1. A group G is called *soluble* if there are normal subgroups

$$\{e\} = G_0 \lhd G_1 \lhd \cdots \lhd G_k = G$$

such that G_{j+1}/G_j is abelian.

Proposition 4.2. *Let G be a group and $N \lhd G$. Then G is soluble if and only if both N and G/N are soluble. More generally, any subgroup and any factor group of a soluble group are soluble.*

Proof. Suppose G is soluble, then there is a composition series

$$\{e\} = G_0 \lhd G_1 \lhd \cdots \lhd G_k = G$$

such that G_{j+1}/G_j is abelian. Then the series

$$\{e\} = \{e\} \cap N = G_0 \cap N \lhd G_1 \cap N \lhd \cdots \lhd G_k \cap N = G \cap N = N$$

is a composition series for N (recall that the intersection $S \cap N$ is a normal subgroup of S), and each factor is abelian because

$$(G_{i+1} \cap N)/(G_i \cap N) = (G_{i+1} \cap N)/(G_{i+1} \cap G_i \cap N) \cong (G_{i+1} \cap N)G_i/G_i < G_{i+1}/G_i$$

by the Second Isomorphism Theorem and since subgroups of an abelian group are abelian.

Let G/N be a quotient group; then note that $G_{j+1}N/N \lhd G_jN/N$, so that

$$\{e\} = G_0N/N \lhd G_1N/N \lhd \cdots \lhd G_{k-1}N/N \lhd G_kN/N = G/N.$$

Moreover, $(G_iN/N)/(G_{i-1}N/N) \cong G_iN/G_{i-1}N$ is abelian by the Third Isomorphism Theorem.

Conversely, suppose N and G/N are soluble with $\{e\} = N_0 \lhd N_1 \lhd \cdots \lhd N_k = N$ and $\{e\} = K_0 \lhd K_1 \lhd \cdots \lhd K_k = G/N$ and let $\varphi : G \to G/N$ be the quotient map. Then

$$\{e\} = N_0 \lhd N_1 \lhd \cdots \lhd N_k = N \lhd \varphi^{-1}(K_0) \lhd \cdots \lhd \varphi^{-1}(N_k) = G$$

is a composition series for G with abelian factor groups. □

Theorem 4.3. *A free group F_r is soluble if and only if $r = 1$.*

Proof. If $r = 1$, then $F_r \cong \mathbb{Z}$, which is abelian. Then $\{e\} \lhd F_r$ is a composition series for F_r with abelian factors.

Conversely, assume for a contradiction F_r for some $r > 1$. Since the free group of rank 2 contains the free group of rank r for each r by Corollary 2.15, we only need to show F_2 is not soluble by Proposition 4.2. Recall that by Proposition 1.11 every finitely generated group is a quotient of a free group. One can show that A_5 can be generated by 2 elements (see Examples 1.13), so $A_5 \cong F_2/N$ for some $N \lhd F_2$. Since A_5 is not soluble, F_2 is not soluble by Proposition 4.2. The proof is complete. □

Corollary 4.4. *A subgroup of a soluble group cannot be isomorphic to a free group of rank greater than* 1.

Proof. By Proposition 4.2, a subgroup of a soluble group is soluble. But F_r is not soluble for $r \geq 2$, hence it cannot be a subgroup. □

4.2. **Almost all subgroups of GL$(n, \mathbb{C})$ are free.** We now turn to the main theorem of the section. To make rigorous sense of measuring subsets in a group, we introduce the Haar Measure following [AM07, Chapter 2].

Recall that a *topological group* is a topological space and a group such that the group's binary operation and inverse function are both continuous. Moreover, a topological space is *locally compact* if every point has a compact neighbourhood, and it is *Hausdorff* if every two distinct point have non-intersecting neighbourhoods.

Definition 4.5 (Haar Measure)**.** Let G be a locally compact Hausdorff topological group. A measure μ is called a left *Haar measure* if $\mu(xE) = \mu(E)$ for every x in G and every measurable $E \subset G$.

By Haar's Theorem, such a (non-trivial) measure always exists and is unique up to a multiplicative factor.

Examples 4.6 (Examples of Haar measures)**.**

- A Haar measure on $(\mathbb{R}, +)$ is the Lebesgue measure.
- A Haar measure on $(\mathbb{R}^*, \times)$ is given by $\mu(E) = \int_E \frac{1}{|t|} dt$.

- A Haar measure on $G = \mathrm{GL}(n, \mathbb{R})$ is given by $\mu(E) = \int_E \frac{1}{|\det(X)|^n} dX$, where dX denotes the Lebesgue measure on $\mathbb{R}^{n\times n}$.
- Similarly, a Haar measure on $\mathrm{GL}(n, \mathbb{C})$ is given by $\mu(E) = \int_E \frac{1}{|\det(X)|^{2n}} dX$.

Theorem 4.7. *For each $r > 0$, and for almost all r-tuples $(g_1, \ldots, g_r)$ of elements of $G = \mathrm{GL}(n, \mathbb{C})$, the group generated by $g_1, \ldots, g_r$ is free on these r elements. ('Almost all' is to be interpreted in terms of Haar measure on G^r.)*

Proof. Let w be a free word in F_r (for example, $r = 2$ and $w = a^2b$). Such a word defines an analytic map, which we also call $w\colon G^r = G \times \cdots \times G \to G$ (in our case, $w(g_1, g_2) = g_1^2 g_2$).

The set of r-tuples which are generators of free subgroups of rank r is

$$X = G^r \setminus \bigcup_{\substack{w\in F_r\\ w\neq e}} w^{-1}(e)$$

In other words, the set of free generators is equal to the set of all r-tuples except those that give a relation. Since F_2 is countable and F_r can be thought as a subset of F_2 (as it is isomorphic to a subgroup of F_2 by Corollary 2.15), we conclude that F_r is countable for $r \geq 1$. Now, taking the measure of both sides and using the countable additivity property for measures, we get:

$$\mu(X) = \mu(G^r) - \sum_{\substack{w\in F_r\\ w\neq e}} \mu(w^{-1}(e))$$

For any analytic mapping from a connected analytic manifold M to an analytic manifold N, the pre-image of a point in N is either the whole of M or has measure zero in M. Thus, if we show the pre-image of the identity is not the entire G^r, then we will have $\mu(w^{-1}(e)) = 0$ for any $w \neq e$ in F_r, and hence we will show that $\mu(X) = \mu(G^r)$.

To show the pre-image is not G^r, we first note that $\mathrm{GL}(n, \mathbb{C})$ contains a free subgroup of rank r. Indeed, by Proposition 3.5 the matrices $\begin{pmatrix}1 & 2\\ 0 & 1\end{pmatrix}$ and $\begin{pmatrix}1 & 0\\ 2 & 1\end{pmatrix}$ generate a free subgroup of rank 2 of $\mathrm{GL}(2, \mathbb{Z}) \leq \mathrm{GL}(2, \mathbb{C})$. One can easily generalize this to matrices

$$\mathrm{diag}\left(\begin{pmatrix}1 & 2\\ 0 & 1\end{pmatrix}, I_{n-2}\right) \text{ and } \mathrm{diag}\left(\begin{pmatrix}1 & 0\\ 2 & 1\end{pmatrix}, I_{n-2}\right) \in \mathrm{GL}(n, \mathbb{C})$$

that generate a free group of rank 2 in $\mathrm{GL}(2, \mathbb{Z})$. Therefore, by Corollary 2.15, $\mathrm{GL}(2, \mathbb{Z})$ contains a free subgroup of rank r. Finally, note that $w^{-1}(e) = G^r$ if and only if the relation w is satisfied throughout G. However, G has a free subgroup, so no relation will be satisfied. □

Remark 4.8 (General form of Theorem 4.7)**.** The result is true if we replace $G = \mathrm{GL}(n, \mathbb{C})$ with any connected, finite-dimensional, non-soluble Lie group. For the proof of the general case, see [Eps71].

Remark 4.9. One natural question to ask at this point is: given $a_1, \cdots, a_r \in \mathrm{GL}(n, \mathbb{C})$ such that $\langle a_1, \cdots, a_r\rangle$ is a free group of rank r, is there a way to choose a $a_{r+1} \in \mathrm{GL}(n, \mathbb{C})$ such that $\langle a_1, \cdots, a_{r+1}\rangle$ is a free group of rank $r + 1$?

For $n = 1$, this is impossible since $(\mathbb{C}, \times)$ is abelian, which is soluble, and subgroup of a soluble group cannot be free of rank greater than 1 by Theorem 4.3. Note that if we can prove for $m = 2$, then we can use the method from Theorem 4.7 to generalize the result to any $m \geq 2$.

For $r = 1$, the condition of $\langle a_1, \cdots, a_r \rangle$ *is a free group of rank* r is the same as saying no power of a_1 is the identity matrix. In this case, the answer is yes. We can use the fact that conjugation does not change the free group to either diagonalise or put the matrix into the *reflected* Jordan form (in the sense of the 1's are below the diagonal). Then construct a matrix with 1's on the diagonal and a *transcendental* number over the field generated by adjoining the eigenvalues, and show they form a free group of rank 2. For more details, see [Lie15].

For $r \geq 2$, the answer is still yes [Bel15]. Note it is sufficient to answer it in $\mathrm{SL}(2, \mathbb{C})$. One can define a ring $R = \mathbb{C}[t_1, t_2, t_3, t_4]/(t_1 t_4 - t_2 t_3 - 1)$, and let $T = \begin{pmatrix} t_1 & t_2 \\ t_3 & t_4 \end{pmatrix} \in SL(2, \mathbb{C})$ and show $\langle a_1, \cdots, a_r, T \rangle$ is free. Then for any non-trivial word $w = w(a_1 \cdots, a_{r+1})$ in F_{r+1}, then the equation $w(a_1 \cdots, a_r, T) = I$ is a system of polynomial equations in t_1, t_2, t_3, t_4, which defines a proper sub-variety V_w of $\mathrm{SL}(2, \mathbb{C})$. But $\mathrm{SL}(2, \mathbb{C})$ cannot be expressed as a countable union of proper sub-varieties, and hence there exists a matrix $a_{r+1} \in \mathrm{SL}(2, \mathbb{C})$ that does not lie in any V_w, then $\langle a_1, \cdots, a_{r+1} \rangle$ is a free.

Corollary 4.10. *If $a_1, \cdots, a_r \in \mathrm{GL}(n, \mathbb{C})$ and $\langle a_1, \cdots, a_r \rangle$ is a free group of rank r, then for almost all $a_{r+1} \in \mathrm{GL}(n, \mathbb{C})$, the subgroup $\langle a_1, \cdots, a_{r+1} \rangle$ is a free group of rank $r + 1$. (Here again, almost all is interpreted in terms of Haar measure.)*

Proof. The proof follows the same argument as the proof of Theorem 4.7. □

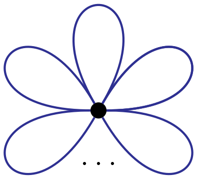
5. Fixed index subgroups

In this section, we will study subgroups of free groups F_r and the modular group $C_2 * C_3$ with a fixed index n. We will provide two methods of counting these groups, one using algebraic topology and one using group actions. We will then apply these results to study the asymptotic growth of the number of subgroups of index n.

5.1. Counting using covering spaces.

Let G be a group and let X be a topological space (satisfying sufficient connectedness conditions; see Appendix B) such that $\pi_1(X) \cong G$. Combining theorems B.2 and B.3 from Appendix B reduces the problem of finding subgroups of fixed index to finding pointed path-connected coverings with a fixed number of sheets.

To apply the theorems to $G = F_r$, we need to construct a space whose fundamental group is F_r. Since $\pi_1(S^1) \cong \mathbb{Z}$ and $F_r \cong \mathbb{Z}^{*r}$, we can apply the Seifert-van Kampen theorem [Hat02, Theorem 1.20] to the join $S^1 \vee S^1 \vee \ldots \vee S^1$ of r circles (also known as the *bouquet of r circles*)



to obtain

$$\pi_1(\underbrace{S^1 \vee S^1 \vee \dots \vee S^1}_{r \text{ times}}) \cong F_r.$$

Altogether, we obtain the following corollary from the two theorems.

Corollary 5.1. *There is a one-to-one correspondence between subgroups of F_r of index n and connected n-sheeted pointed covering spaces of the join of r circles, i.e. connected directed coloured graphs with:*

(1) n vertices,
(2) r colours of the directed edges,
(3) the in-degree and the out-degree in any colour equal to 1, for any vertex,
(4) a chosen base vertex.

We have therefore reduced the problem of counting the number of subgroups of F_r of index n to a purely combinatorial exercise. We can now prove a general recursive formula for $a_n(F_r)$, where we denote the number of subgroups of G of index n by $a_n(G)$. Note that $a_1(G) = 1$ for any group G, so we just need to express $a_n(F_r)$ in terms of $a_k(F_r)$ for $k \in \{1, 2, \dots, n-1\}$.

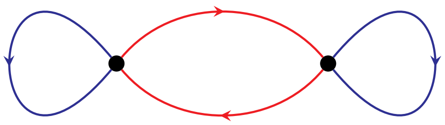
Theorem 5.2 (Hall's formula, [Hal49, Theorem 5.1])**.** *For $r \geq 2$, $n \geq 1$, we have*

$$a_n(F_r) = n(n!)^{r-1} - \sum_{k=1}^{n-1} [(n-k)!]^{r-1} a_k(F_r).$$

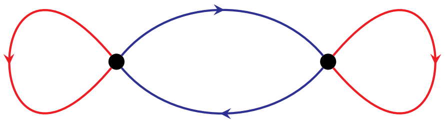
Before the proof of the theorem, we give two examples where we can write down the covering spaces and the groups explicitly.

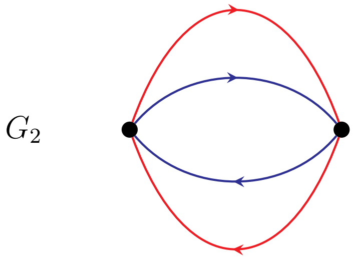
Example 5.3 ($n = 2$, $r = 2$)**.** We want to find all the 2-sheeted connected pointed coverings of $S^1 \vee S^1$. We start by writing all of the coverings down. The two colours, red and blue, correspond to the two circles in $S^1 \vee S^1$. Note that since the graphs have 2 vertices, it does not matter which one is the base point; this is consistent with the fact that any subgroup of index 2 is normal.

G_1

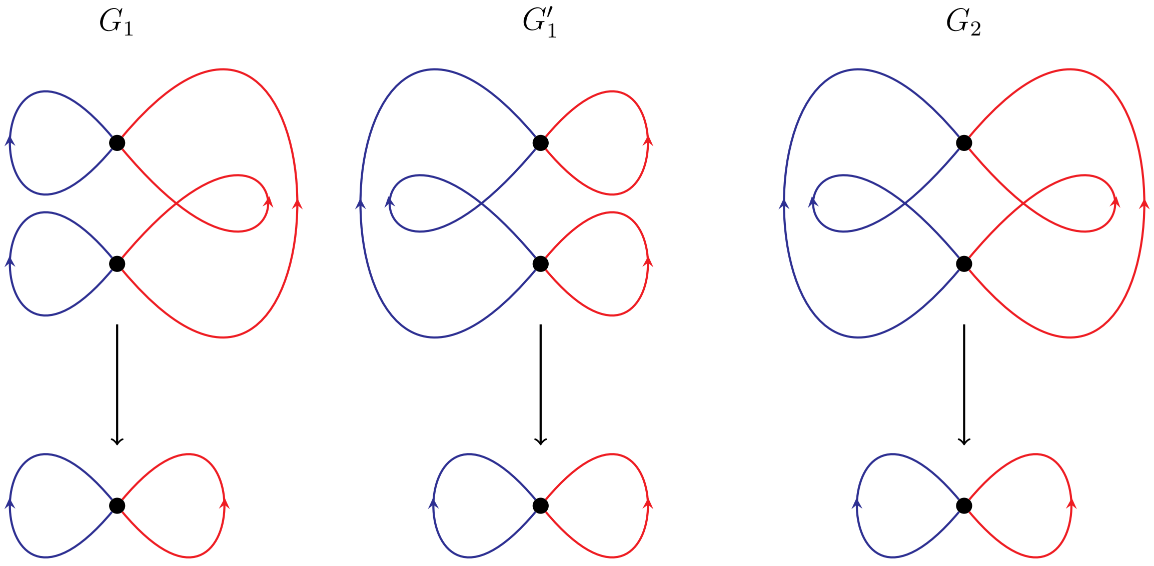


G_1'





To clarify how these graphs form covering spaces for $S^1 \vee S^1$, we can also sketch them in a way that makes the projection maps obvious.



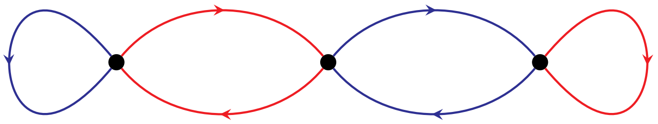
We have three different graphs corresponding to the three subgroups of index 2 in F_2. The elements of the corresponding groups will be cycles in the graphs. If we denote the generators corresponding to the colours red and blue by r and b, respectively, and find the *generating* cycles, we obtain that the three subgroups of index 2 in $F_2 = \langle b, r | \rangle$ are

$$G_1 = \langle b, r^2, rbr \rangle, G_1' = \langle r, b^2, brb \rangle, G_2 = \langle b^2, r^2, br \rangle$$

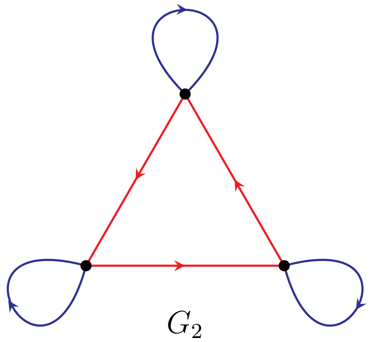
As expected, all these subgroups are free (Corollary 2.13) and they have rank 3 (Schreier index formula 2.14). Moreover, the result is consistent with Hall's formula 5.2, since

$$3 = 2 \cdot 2 - 1 = 2(2!)^{2-1} - a_1(F_2)$$

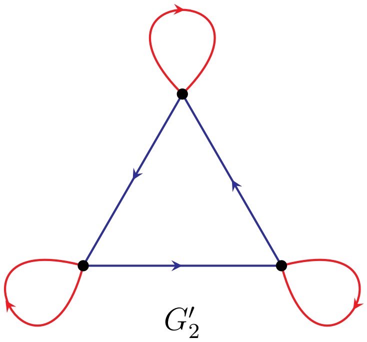
Example 5.4 ($n = 3$, $r = 2$)**.** We want to find all the 3-sheeted connected pointed coverings of $S^1 \vee S^1$. We start by writing all of the coverings without base points down. The two colours, red and blue, correspond to the two circles in $S^1 \vee S^1$.



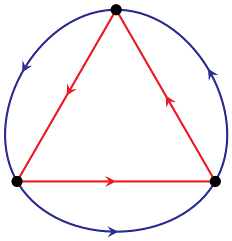
G_1



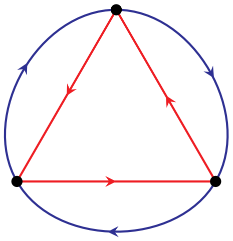
G_2



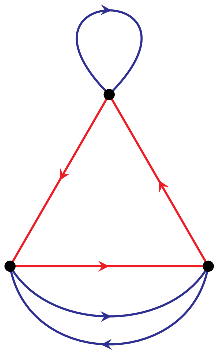
G_2'



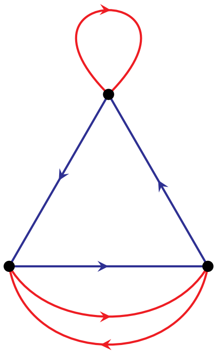
G_3



G_3'



G_4



G_4'

By inspection, we can see that these are all the possible graphs satisfying (1)–(3) from Corollary 5.1. Each one of them corresponds to a conjugacy class of subgroups of index 3 in F_2 by Theorem B.3. We will denote the generators corresponding to the colours red and blue by r and b, respectively. The elements of the corresponding groups will be cycles that start and end at the base point. By considering different placements of the base points and by finding the *generating* cycles, we obtain the following table:

graph	choices of base point	the corresponding conjugate subgroups of index 3
G_1	3	$\langle b, r^2, rb^2r, rbrbr\rangle$, $\langle r, b^2, br^2b, brbrb\rangle$, $\langle r^2, b^2, rbr, brb\rangle$
G_2	1	$\langle r^3, b, rbr^2, r^2br\rangle$
G_2'	1	$\langle b^3, r, brb^2, b^2rb\rangle$
G_3	1	$\langle b^3, r^3, br^{-1}, rb^{-1}\rangle$
G_3'	1	$\langle b^3, r^3, br, rb\rangle$
G_4	3	$\langle r^3, b^2, br^{-1}, r^2br\rangle$, $\langle r^3, b^2, br, rbr^2\rangle$, $\langle r^3, b, rbr, rb^{-1}r\rangle$
G_4'	3	$\langle b^3, r^2, rb^{-1}, b^2rb\rangle$, $\langle b^3, r^2, rb, brb^2\rangle$, $\langle b^3, r, brb, br^{-1}b\rangle$

As expected, all these subgroups are free (Corollary 2.13) and they have rank 5 (Schreier index formula 2.14).

These are all the subgroups of index 3 in $F_2 = \langle b, r|\rangle$. Therefore:

$$a_3(F_2) = 3 + 1 + 1 + 1 + 1 + 3 + 3 = 13$$

which is consistent with Hall's formula 5.2:

$$a_3(F_2) = 3(3!) - \sum_{k=1}^{2}[(3-k)!]a_k(F_r) = 18 - 2 \cdot a_1(F_2) - a_2(F_2) = 18 - 2 - 3 = 13,$$

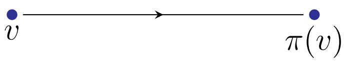
where we can use Example 5.3 or the formula again to obtain $a_2(F_2) = 3$.

By Theorem B.2, each of the graphs corresponds to a different conjugacy class of subgroups, so we can also deduce that the number of conjugacy classes is 7 and the number of normal subgroups is 4.

We now turn to the proof of Theorem 5.2. We omit the original proof of the theorem, and present instead a proof that relies on covering space theory. We will also present a more elementary proof using permutation representations in Section 5.2.

Proof of Theorem 5.2. The main idea of the proof is to count the number N of **any** (connected or not) graphs satisfying conditions (1)–(4) from Corollary 5.1 with a chosen base point and an order on the set of the vertices, say $\{1, 2, \dots, n\}$.

Note that condition (3) implies that the set of (directed) edges in one colour induces a permutation of the n vertices. Explicitly, the permutation π maps any vertex $v \in \{1, 2, \dots, n\}$ to the unique vertex connected to it, i.e.



Therefore, we have n choices for the base point, and for any edge colour we have $n!$ independent arrangements of the edges in that colour.

$$N = n(n!)^r.$$

We will now count the number N in a different way, using the numbers $a_k(F_r)$ for $k = 1, 2, \dots, n$, therefore proving the desired result. We first choose the base point (n choices). Let us fix k and count the number of graphs satisfying conditions (1)–(4) with the property that the base point lies in a connected component on exactly k vertices:

choose $k-1$ ordered points that will be in the connected component with the base point	$\frac{(n-1)!}{(n-k)!}$ choices
for the k points, choose which covering with a base point they correspond to	$a_k(F_r)$ choices
for the $n-k$ points, arrange them in any way	$[(n-k)!]^r$ choices

In total, we obtain:

$$n \cdot (n!)^r = N = n \cdot \sum_{k=1}^{n} \left(\frac{(n-1)!}{(n-k)!} \cdot a_k(F_r) \cdot [(n-k)!]^r \right),$$

and the result follows by rearranging. □

The advantage of using covering theory is that one can write find a set of generators for the subgroups (which we know are free by Corollary 2.13). We turn our attention particularly to subgroups of index $n = 2$. From the formula in Theorem 5.2, we immediately see that

$$a_2(F_r) = 2^r - 1. \tag{4}$$

We strengthen this result below by writing down the subgroups explicitly.

Proposition 5.5. *Any subgroup G of F_r of index 2 can be obtained as follows: fix $k \in \{0, 1, \ldots, r-1\}$ and choose k generators $a_1, \ldots, a_k$ of F_r so that $F_r = \langle a_1, \ldots, a_k, b_1, \ldots, b_l | \rangle$ where $l = r - k$; then G is freely generated by*

$$a_1, \ldots, a_k,$$

$$b_1^2, \ldots, b_l^2,$$

$$b_1b_2, b_1b_3, \ldots, b_1b_l,$$

$$b_1a_1b_1, b_1a_2b_1, \ldots, b_1a_kb_1.$$

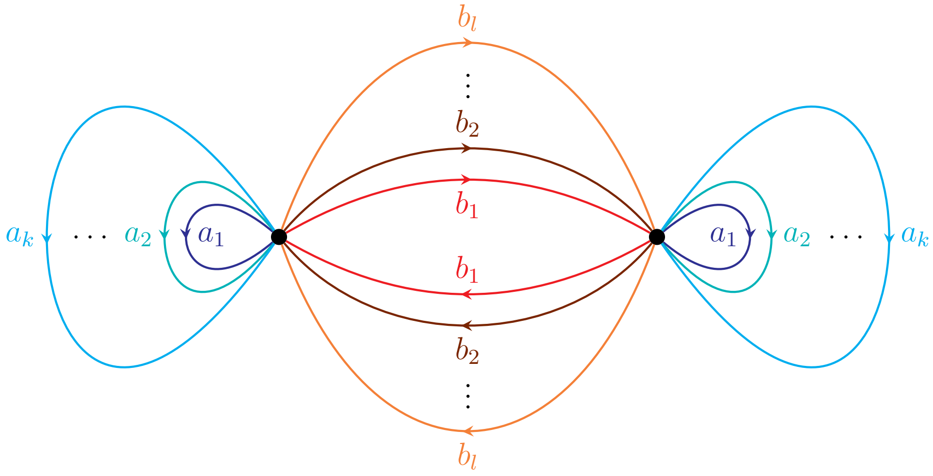
Note that this is consistent with equation (4); the total number of subgroups of F_r of index 2 is:

$$\sum_{k=0}^{r-1} \binom{r}{k} = \sum_{k=0}^{r} \binom{r}{k} - 1 = 2^r - 1.$$

Moreover, the number of free generators for each of these groups is $k + l + (l-1) + k = 2(k+l) - 1 = 2n - 1$, which is consistent with the Scheier index formula 2.14.

Proof. Recall that a subgroup G of index 2 of F_r corresponds to a connected graph on 2 vertices satisfying the conditions (1)–(4) from Corollary 5.1. Note that if one of the vertices has a loop of a given colour, then so does the other. Let $k \in \{0, 1, \ldots, r-1\}$ be the number of loops on a vertex and $a_1, \ldots, a_k$ be the colours of the loops. Then all the other edges in $l = r - k$ colours, $b_1, \ldots, b_l$, have to connect the two vertices.

In general, the graph will hence look as follows.



The elements of the group G will now correspond to cycles (paths that start and end at the same vertex of the graph). We identify the colous $a_1, \dots, a_k, b_1, \dots, b_l$ with the generators of the free group with multiplication corresponding to composition of paths. We note that the paths

$$a_1, \dots, a_k,$$

$$b_1^2, \dots, b_l^2,$$

$$b_1 b_2, b_1 b_3, \dots, b_1 b_l,$$

$$b_1 a_1 b_1, b_1 a_2 b_1, \dots, b_1 a_k b_1$$

are all cycles in the graph (so they correspond to elements of G) and there are no relations between them. Let us denote the group generated by these cycles $H \subseteq G$ and show that $H = G$. A cycle of the graph starting at the base point is a disjoint union of cycles that only visit the base point twice (at the start and at the end of the cycle). Therefore, it is enough to show that a general element

$$b_i a b_j$$

where a is a word in $a_1, \dots, a_k$, is a product of the cycles. The proof goes by induction on the number of letters of a. For a 1-letter word a, we have that $b_1 a b_1 \in H$, so:

$$b_i a b_j = b_i^2 (b_1 b_i)^{-1} (b_1 a b_1)(b_1^2)^{-1}(b_1 b_j) \in H.$$

Moreover, if $b_i a b_j \in H$ and a' is a 1-letter word, then by the above argument we have $b_j a' b_j \in H$, so:

$$b_i a a' b_j = (b_i a b_j)(b_j)^{-2}(b_j a' b_j) \in H.$$

This completes the proof. □

5.2. **Counting using permutation representations.** We now turn to another method of finding the numbers $a_n(G)$, following [LS03, Chapters 1, 2]. We revisit Hall's recursive formula 5.2 and generalize it to any free product of groups.

Our main tool in this section is the permutation representation of a group. There is a correspondence between subgroups H of index n of a group G and transitive permutation representations $\varphi\colon G \to \mathrm{Sym}(n)$ of G (homomorphisms from G to $\mathrm{Sym}(n)$ such that $\varphi(G)$ acts transitively on $\{1, \dots, n\}$):

- Given a subgroup H of index n, let us label the set of cosets G/H with numbers $1, 2, \dots, n$ so that H has the label 1. This gives rise to $(n-1)!$ distinct transitive actions $\varphi\colon G \to \mathrm{Sym}(n)$ that satisfy $H = \mathrm{Stab}_G(1)$, the stabilizer of 1.
- Given a transitive action $\varphi\colon G \to \mathrm{Sym}(n)$, the stabilizer $\mathrm{Stab}_G(1)$ of 1 is a subgroup of index n.

Therefore, if $a_n(G)$ is the number of subgroups of G of index n, then we can reduce the problem of finding $a_n(G)$ to the problem of finding the number $t_n(G)$ of transitive permutation representations:

$$a_n(G) = t_n(G)/(n-1)! \tag{5}$$

Now, we express the numbers $t_n(G)$ recursively in terms of the number

$$h_n(G) = \#\mathrm{Hom}(G, \mathrm{Sym}(n))$$

of all homomorphisms from G to $\mathrm{Sym}(n)$.

Lemma 5.6 ([LS03, Lemma 1.1.3])**.** *Let G be a group. Then*

$$h_n(G) = \sum_{k=1}^{n} \binom{n-1}{k-1} t_k(G) h_{n-k}(G).$$

Proof. Let us first calculate the number

$$h_{n,k} = \#\{\varphi\colon G \to \mathrm{Sym}(n) \mid \#G(1) = k\}$$

where we denote the orbit of 1 in the action by $G(1)$, for each k. There are:

- $\binom{n-1}{k-1}$ ways to choose the other members of $G(1)$,
- $t_k(G)$ ways to act on the orbit $G(1)$ (the action is transitive, since $G(1)$ is an orbit),
- $h_{n-k}(G)$ ways to act on the complement $\{1, 2, \dots, n\} \setminus G(1)$.

Therefore:

$$h_{n,k}(G) = \binom{n-1}{k-1} t_k(G) h_{n-k}(G).$$

Finally:

$$h_n(G) = \sum_{k=1}^{n} h_{n,k}(G) = \sum_{k=1}^{n} \binom{n-1}{k-1} t_k(G) h_{n-k}(G),$$

which completes the proof. □

This lemma immediately yields Hall's formula 5.2.

Alternative proof of Theorem 5.2. First, we can rearrange the formula in Lemma 5.6 to get:

$$t_n(G) = h_n(G) - \sum_{k=1}^{n-1} \binom{n-1}{k-1} t_k(G) h_{n-k}(G) \tag{6}$$

Moreover, note that for $G = F_r$, we can map the generators to any elements of a symmetric group, so

$$h_{n-k}(F_r) = [(n-k)!]^r. \tag{7}$$

Altogether:

$$\begin{aligned} a_n(F_r) &= t_n(F_r)/(n-1)! && \text{(by equation (5))} \\ &= \tfrac{h_n(F_r)}{(n-1)!} - \sum_{k=1}^{n-1} \tfrac{1}{(n-k)!(k-1)!} t_k(F_r) h_{n-k}(F_r) && \text{(by equation (6))} \\ &= n(n!)^r - \sum_{k=1}^{n-1} [(n-k)!]^{r-1} a_k(F_r) && \text{(by equations (5) and (7))} \end{aligned}$$

which completes the proof. □

Even though the proof might seem very different from the one given before, it relies on the same idea. In the proof of Lemma 5.6, we fix k and use the numbers $a_k(G)$ to calculate the number of actions such that the orbit of 1 has k elements. In the previous proof, this corresponds exactly to choosing the connected component of the covering graph on k vertices that contains the base point.

By adjusting the arguments above, one can generalize Hall's formula 5.2 to any product of free groups. As before, we use the notation

$$h_n(G) = \#\mathrm{Hom}(G, \mathrm{Sym}(n)).$$

Theorem 5.7 ([Dey65, Theorem 6.10])**.** *Let $G = H_1 * H_2$ be the free product of the groups H_1 and H_2. Then*

$$a_n(G) = \frac{1}{(n-1)!} h_n(H_1) h_n(H_2) - \sum_{k=1}^{n-1} \frac{1}{(n-1)!} h_{n-k}(H_1) h_{n-k}(H_2) a_k(G).$$

The formula can also be easily generalized to the free product of any finite number of groups. One can hence obtain Hall's formula 5.2 as a corollary by applying the theorem to $F_r \cong \underbrace{\mathbb{Z} * \mathbb{Z} * \cdots * \mathbb{Z}}_{r \text{ times}}$.

However, we can also apply this theorem to other groups that arise as free products. We have already seen an example of such a group, the modular group $\mathrm{PSL}(2,\mathbb{Z})$ which is isomorphic to $C_2 * C_3$ by Proposition 3.3.

Corollary 5.8. *Let $\mathrm{PSL}(2,\mathbb{Z})$ be the modular group. Then*

$$a_n(\mathrm{PSL}(2,\mathbb{Z})) = \frac{1}{(n-1)!} h_n(C_2) h_n(C_3) - \sum_{k=1}^{n-1} \frac{1}{(n-1)!} h_{n-k}(C_2) h_{n-k}(C_3) a_k(G),$$

where for $l = 1, 2, \ldots, n$:

$$h_l(C_2) = \sum_{0 \le r \le l/2} \frac{l!}{r!(l-2r)!2^r}, \quad h_l(C_3) = \sum_{0 \le r \le l/3} \frac{l!}{r!(l-3r)!3^r}.$$

Proof. We apply Theorem 5.7 to $\mathrm{PSL}(2,\mathbb{Z}) \cong C_2 * C_3$ and obtain the numbers $h_l(C_2)$ and $h_l(C_3)$ using [New76, Equation (10)]. □

5.3. **Subgroup growth.** This subsection presents basic results about subgroup growth, following [LS03, Chapter 2] and [New76].

We first use Hall's formula 5.2 to study the growth of subgroups of index n in F_r.

Theorem 5.9 ([LS03, Theorem 2.1])**.** *Let $r \geq 2$. As $n \to \infty$, we have:*

$$a_n(F_r) \sim n \cdot (n!)^{r-1}.$$

Proof. Let us first show that $\frac{t_n(F_r)}{h_n(F_r)} \to 1$ as $n \to \infty$. This will essentially mean that *most* of the r-tuples of permutations generate transitive subgroups. Let us hence bound the number of the intransitive actions:

$$\begin{aligned} h_n(F_r) - t_n(F_r) &= \sum_{k=1}^{n-1} \tbinom{n-1}{k-1} t_k(F_r) h_{n-k}(F_r) && \text{(by equation (6))} \\ &\leq \sum_{k=1}^{n-1} \tbinom{n-1}{k-1} h_k(F_r) h_{n-k}(F_r) && \text{(by } t_k(F_r) \leq h_k(F_r)\text{)} \\ &\leq \sum_{k=1}^{n-1} \tbinom{n-1}{k-1} (k!)^r (n-k)!^r && \text{(by equation (7))} \\ &= (n!)^r \sum_{k=1}^{n-1} \tbinom{n}{k}^{-r-1} \frac{k}{n} \\ &\leq (n!)^r \sum_{k=1}^{[n/2]} \tbinom{n}{k}^{-r-1} && \text{(by } \tbinom{n}{k} = \tbinom{n}{n-k}\text{)} \end{aligned}$$

Now, we just have to bound $\binom{n}{k}$ for $1 \leq k \leq n/2$. We have:

$$\binom{n}{k} = (n-k-1) \cdot \frac{n-k+2}{k-k+2} \cdot \frac{n-k+3}{k-k+3} \cdot \dots \cdot \frac{n}{k} \geq (n-k+1) \left(\frac{n}{k}\right)^{k-1} \geq 2^{k-2} n.$$

Since $r \geq 2$, this yields:

$$h_n(F_r) - t_n(F_r) \leq (n!)^r \sum_{k=1}^{[n/2]} 2^{-k+2} \frac{1}{n} < \frac{4}{n} (n!)^r = \frac{4}{n} h_n(F_r).$$

Rearranging, we obtain

$$1 \geq \frac{t_n(F_r)}{h_n(F_r)} \geq 1 - \frac{4}{n},$$

so taking the limit as $n \to \infty$, we have shown that

$$\frac{t_n(F_r)}{h_n(F_r)} \to 1.$$

Therefore by equation (5):

$$a_n(F_r) = \frac{t_n(F_r)}{(n-1)!} \sim \frac{h_n(F_r)}{(n-1)!} = n \cdot (n!)^{r-1},$$

which completes the proof. □

A similar analysis yields a stronger result about the number $m_n(G)$ of maximal subgroups of index n of $G = F_r$. In this case, maximal subgroups will correspond to primitive actions (i.e.

actions that do not preserve any non-trivial partitions). As before, if $p_n(G)$ is the number of primitive permutation representations of G, then

$$m_n(G) = p_n(G)/(n-1)! \tag{8}$$

Surprisingly, the asymptotic growth of the maximal subgroups of index n of F_r is the same as the growth of all the subgroups of index n.

Theorem 5.10 ([LS03, Theorem 2.1])**.** *Let $r \geq 2$. As $n \to \infty$, we have:*

$$m_n(F_r) \sim n \cdot (n!)^{r-1}.$$

Proof. The proof is similar to the proof of Theorem 5.9. We will show that $\frac{p_n(F_r)}{h_n(F_r)} \to 1$. To count the number of the inprimitive actions of F_r on $\{1, 2, \ldots, n\}$, let us count the number of actions that preserve a nontrivial partition into equal parts, each of size $a = n/b$. For any of the b parts, we have $a!$ permutations, and we have $b!$ permutations of the parts, so there are $(a!)^b b!$ such permutations. For each of the generators of F_r, we choose one of the elements it is mapped to under the homomorphism, giving a total of

$$((a!)^b b!)^r$$

such actions of F_r. (In fact, any such action is a homomorphism $F_r \to \mathrm{Sym}(a) \wr \mathrm{Sym}(b)$.) Moreover, the number of partitions into equal parts of size a is

$$\frac{1}{b!}\binom{ab}{a}\binom{a(b-1)}{a}\cdots\binom{2a}{a}\binom{a}{a} = \frac{n!}{(a!)^b b!}.$$

Thus, if we denote the number of divisors of n by $d(n)$, the number of imprimitive actions of F_r on $\{1, 2, \ldots, n\}$ is:

$$\begin{aligned} t_n(F_r) - p_n(F_r) &\leq \sum_{a \cdot b = n} \tfrac{n!}{(a!)^b b!} \cdot ((a!)^b b!)^r \\ &< d(n) \cdot n! \cdot ((a!)^b b!)^{r-1} \end{aligned}$$

We now use the upper bound $(a!)^b b! < (ab-1)!$ for $a \geq 3$, $b \geq 2$. (Since we are only interested in the limit as $n \to \infty$ and $ab = n$, we may assume that $a \geq 3$, $b \geq 2$.) We prove it by induction on $b \geq 2$. For $b = 2$, we simply note that for $a \geq 3$:

$$2 \cdot a! < (a-1+2) \cdot (a-1+3) \cdot \cdots \cdots (a-1+a) = (a+1) \cdot (a+2) \cdot \cdots \cdot (2a-1)$$

which immediately implies that $2 \cdot (a!)^2 < (2a-1)!$. For the induction step, note that:

$$\begin{aligned} (a(b+1)-1)! &= (ab+a-1)! \\ &= (ab-1)! \cdot (ab)(ab+1)\ldots(ab+a-1) \\ &> (a!)^b b! \cdot \underbrace{(ab)(ab+1)\ldots(ab+a-1)}_{>a! \cdot (b+1)} \\ &> (a!)^{b+1}(b+1)! \end{aligned}$$

so we are done. Therefore:

$$0 \leq \frac{t_n(F_r) - p_n(F_r)}{h_n(F_r)} < d(n) \cdot n! \cdot ((n-1)!)^{r-1}/(n!)^r = d(n)n^{-(r-1)} \to 0$$

as $n \to \infty$, since $r \geq 2$ and $d(n) = o(n)$ (see [Apo76, p. 296]). Hence

$$\lim_{n\to\infty} \frac{p_n(F_r)}{h_n(F_r)} = \lim_{n\to\infty} \frac{t_n(F_r)}{h_n(F_r)}$$

and the theorem follows from Theorem 5.9. □

Finally, we state a theorem about the subgroup growth of $\mathrm{PSL}(2, \mathbb{Z}) = C_2 * C_3$.

Theorem 5.11 ([New76, Theorem 4])**.** *Let* $\mathrm{PSL}(2,\mathbb{Z})$ *be the modular group. Then*

$$a_n(\mathrm{PSL}(2,\mathbb{Z})) \sim \frac{a_n(C_2)a_n(C_3)}{(n-1)!} \sim \frac{1}{\sqrt{12\pi e^{1/2}}}\exp\left(\frac{n}{6}\log n - \frac{n}{6} + n^{1/2} + n^{1/3} + \frac{1}{2}\log n\right)$$

The proof relies on Theorem 5.7 and Corollary 5.8, but it is more involved, so we omit it here.

Appendix A. Group Actions

In this appendix, we review the necessary notions from group actions.

Definition A.1. An *automorphism* is an isomorphism from a group to itself, (or equally a graph to itself). We write $\mathrm{Aut}\,(X)$ for the set of all automorphisms of X.

Proposition A.2. *The set* $\mathrm{Aut}\,(X)$ *forms a group under composition of automorphisms. Here* X *can either denote a group,* G*, or a graph* (V,E)*.*

Proof.

(1) **Closure:** Take $f_1, f_2 \in \mathrm{Aut}\,(X)$ then $f_1 \circ f_2$ is a composition of isomorphisms, so is clearly an isomorphism.
(2) **Associativity:** Composition of functions is associative, so clearly this holds.
(3) **Identity:** The trivial isomorphism, the identity map $\mathrm{Id}_X\colon X \to X$ such that $\mathrm{Id}_X(x) = x$ is our identity.
(4) **Inverses:** Take $f \in \mathrm{Aut}\,(X)$ then since f is an isomorphism f^{-1} also is, so $f^{-1} \in \mathrm{Aut}\,(X)$ and $f^{-1}\circ f = f \circ f^{-1} = \mathrm{Id}_X$

□

Definition A.3. Let G be a group, and let X be a graph. An *action* of G on X is a group homomorphism $\varphi\colon G \to \mathrm{Aut(X)}$. In other words, for each $g \in G$, there is an automorphism $\varphi(g) = f_g\colon X \to X$ such that:

$$f_g \circ f_h = f_{g\cdot h}$$

for any $g, h \in G$.

Definition A.4. Let G be a group, let (V,E) be a graph. An action $\varphi\colon G \to \mathrm{Aut}\,(V,E)$ is *free* if for all $g \in G \setminus \{e\}$ we have:

$$\varphi(g)(v) \neq v,$$
$$\varphi(g)\left(\{v,v'\}\right) \neq \{v,v'\},$$

for any $v \in V$, $\{v,v'\} \in E$.

Example A.5. Let G be a group, so $G = (X,\cdot)$. The *left translation action* is:

$$G \to \mathrm{Aut}\,(X)$$
$$g \mapsto f_g, \text{ where } f_g(h) = g\cdot h$$

Definition A.6 (Orbits)**.** Let G be a group acting on X. We define the *orbit* of $x \in X$ to be the set

$$G(x) = \{g\cdot x \mid g \in G\}\,.$$

Proposition A.7. *Suppose* G *acts on* X*, then for any* x_1, x_2 *in* X *we write* $x_1 \sim x_2$ *if and only if* x_1 *is in* $G(x_2)$*. This is an equivalence relation.*

Proof.

(1) **Reflexivity** Clearly $x_1 \sim x_1$ since $e \in G$, and hence $x_1 = e \cdot x_1 \in G(x_1)$
(2) **Symmetry** Suppose $x_1 \sim x_2$, then there is a $g \in G$ such that $g \cdot x_2 = x_1$. Then clearly $g^{-1} \in G$ and $g^{-1} \cdot x_1 = x_2$, so $x_2 \in G \cdot x_1$ and $x_2 \sim x_1$
(3) **Transitivity** Suppose $x_1 \sim x_2$ and $x_2 \sim x_3$. Then there exists $g, h \in G$ such that $g \cdot x_2 = x_1$ and $h \cdot x_3 = x_2$. Then clearly $h^{-1}g^{-1} \cdot x_2 = x_3$, so $x_3 \in G(x_1)$ and hence $x_3 \sim x_1$.

□

Appendix B. Covering space theory

In this appendix, we review the necessary covering space theory following [Hat02, Section 1.3].

Definition B.1. Let (X, x_0) be a pointed topological space. A *pointed covering space* of (X, x_0) is a space $(\tilde{X}, \tilde{x_0})$ together with a map $p\colon \tilde{X} \to X$ such that:

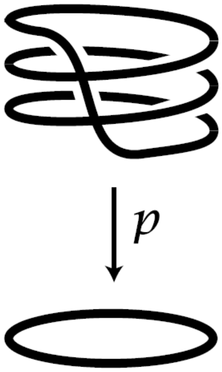
(1) each point $x \in X$ has a neighbourhood $U \subseteq X$ such that $p^{-1}(U)$ is a union of disjoint open sets in $\tilde{X}$ (we refer to these open sets as *sheets*),
(2) $p(\tilde{x_0}) = x_0$.

We may sometimes drop the base points $x_0, \tilde{x_0}$ (and condition (2)) and refer to $\tilde{X}$ as a *covering space* for X.

If the number of sheets is finite, say n, then $\tilde{X}$ is an *n-sheeted covering space* for X.

Finally, we denote by $p_*\colon \pi_1(\tilde{X}, \tilde{x_0}) \to \pi_1(X, x_0)$ the homomorphism induced by the map $p\colon : \tilde{X} \to X$.

A standard example is a 3-sheeted covering of the circle. Source of diagram: [Hat02, p. 56].



The reason that covering theory plays an important tool in geometric group theory is that there is a one-to-one correspondence between subgroups of a group and coverings of spaces. As we can see in Section 5, this can turn algebraic problems into purely combinatorial exercises.

Theorem B.2 ([Hat02, Theorem 1.38])**.** *Suppose (X, x) is a pointed topological space satisfying sufficient connectedness conditions*[*]*. Then the following mappings are bijections:*

$$\begin{tikzcd} \left\{\begin{array}{c}\textit{pointed coverings of } (X,x_0) \textit{ up to}\\ \textit{base-point preserving isomorphism}\end{array}\right\} \arrow[r, leftrightarrow] & \left\{\begin{array}{c}\textit{subgroups}\\ H \leq \pi_1(X,x_0)\end{array}\right\} \\ p\colon (\tilde{X},\tilde{x_0}) \to (X,x_0) \arrow[r, mapsto] & p_*(\pi_1(\tilde{X},\tilde{x_0})) \end{tikzcd}$$

$$\begin{tikzcd} \left\{\begin{array}{c}\textit{coverings of } X \textit{ up to}\\ \textit{isomorphism}\end{array}\right\} \arrow[r, leftrightarrow] & \left\{\begin{array}{c}\textit{conjugacy classes of}\\ \textit{subgroups } H \leq \pi_1(X,x_0)\end{array}\right\} \\ p\colon \tilde{X} \to X \arrow[r, mapsto] & {[p_*(\pi_1(\tilde{X},\tilde{x_0}))]} \end{tikzcd}$$

In the second bijection, $x_0 \in X$ and $\tilde{x_0} \in \tilde{X}$ are any points, and we denote the conjugacy class of a subgroup H by $[H]$.

Moreover, the index of the subgroups correspond to the number of sheets of the covering.

Theorem B.3 ([Hat02, Prop. 1.32])**.** *Suppose $p\colon (\tilde{X}, \tilde{x_0}) \to (X, x_0)$ is a covering, where X and $\tilde{X}$ are path-connected. Then the number of sheets of the covering is equal to the index of $p_*(\pi_1(\tilde{X}, \tilde{x_0}))$ in $\pi_1(X, x_0)$.*

Finally, if G is a group acting (suitably) on a space X, then X is a covering space for the orbit space X/G.

Theorem B.4 ([Hat02, Prop. 1.40])**.** *Suppose an action of G on a path-connected and locally path-connected topological space X satisfies the following property: each $x \in X$ has a neighbourhood U such that $g_1(U) \cap g_2(U) \neq \emptyset$ implies $g_1 = g_2$ for any g_1, g_2. Then the quotient map $p\colon X \to X/G$ is a covering space and*

$$G \cong \frac{\pi_1(X/G)}{p_*(\pi_1(X))}.$$

References

[Alp93] Roger C. Alperin, *Notes: $PSL_2(Z) = Z_2 * Z_3$*, Amer. Math. Monthly **100** (1993), no. 4, 385–386, doi:10.2307/2324963. MR 1542320

[AM07] Hossein Abbaspour and Martin Moskowitz, *Basic Lie theory*, World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2007, doi:10.1142/6462. MR 2364699 (2008i:22001)

[Apo76] Tom M. Apostol, *Introduction to analytic number theory*, Springer-Verlag, New York-Heidelberg, 1976, Undergraduate Texts in Mathematics. MR 0434929 (55 #7892)

[Bel15] Jim Belk, *Free subgroups of linear groups*, June 2015, answer on Stack Exchange, http://math.stackexchange.com/questions/1320634/free-subgroup-of-linear-groups.

[CFR11] Celine Carstensen, Benjamin Fine, and Gerhard Rosenberger, *Abstract algebra*, Sigma Series in Pure Mathematics, vol. 11, Heldermann Verlag, Lemgo; Walter de Gruyter GmbH & Co. KG, Berlin, 2011, Applications to Galois theory, algebraic geometry and cryptography. MR 2777985

[Con] Keith Conrad, *Notes:* $\mathrm{SL}(2, \mathbb{Z})$, as seen June 12, 2015, http://www.math.uconn.edu/~kconrad/blurbs/grouptheory/SL%282,Z%29.pdf.

[Dey65] I. M. S. Dey, *Schreier systems in free products*, Proc. Glasgow Math. Assoc. **7** (1965), 61–79 (1965). MR 0188279 (32 #5718)

[*] To be precise, X is path-connected, locally path-connected, semilocally simply-connected. The definitions of the latter two can be found in [Hat02, p. 70–72]. Needless to say, all the spaces we will consider do satisfy these properties trivially, which is why we omit the details here.

[dlH00] Pierre de la Harpe, *Topics in geometric group theory*, Chicago Lectures in Mathematics, University of Chicago Press, Chicago, IL, 2000. MR 1786869 (2001i:20081)

[Eps71] D. B. A. Epstein, *Almost all subgroups of a Lie group are free*, J. Algebra **19** (1971), 261–262. MR 0281776 (43 #7491)

[Hal49] Marshall Hall, Jr., *Subgroups of finite index in free groups*, Canadian J. Math. **1** (1949), 187–190. MR 0028836 (10,506a)

[Hat02] Allen Hatcher, *Algebraic topology*, Cambridge University Press, Cambridge, 2002. MR 1867354 (2002k:55001)

[Lie15] Martin W. Liebeck, *Free generators in linear groups*, June 2015, preprint.

[Löh11] Clara Löh, *Geometric group theory*, March 2011, notes, as seen June 8, 2015, http://www.mathematik.uni-regensburg.de/loeh/teaching/ggt_ws1011/lecture_notes.pdf.

[LS01] Roger C. Lyndon and Paul E. Schupp, *Combinatorial group theory*, Classics in Mathematics, Springer-Verlag, Berlin, 2001, Reprint of the 1977 edition. MR 1812024 (2001i:20064)

[LS03] Alexander Lubotzky and Dan Segal, *Subgroup growth*, Progress in Mathematics, vol. 212, Birkhäuser Verlag, Basel, 2003, doi:10.1007/978-3-0348-8965-0. MR 1978431 (2004k:20055)

[New76] Morris Newman, *Asymptotic formulas related to free products of cyclic groups*, Math. Comp. **30** (1976), no. 136, 838–846. MR 0466047 (57 #5930)

[Rei95] Miles Reid, *Undergraduate commutative algebra*, London Mathematical Society Student Texts, vol. 29, Cambridge University Press, Cambridge, 1995, doi:10.1017/CBO9781139172721. MR 1458066 (98c:13001)

[Rot95] Joseph J. Rotman, *An introduction to the theory of groups*, fourth ed., Graduate Texts in Mathematics, vol. 148, Springer-Verlag, New York, 1995, doi:10.1007/978-1-4612-4176-8. MR 1307623 (95m:20001)

[Ser03] Jean-Pierre Serre, *Trees*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2003, Translated from the French original by John Stillwell, Corrected 2nd printing of the 1980 English translation. MR 1954121 (2003m:20032)