GROUP THEORY

DECISION PROBLEMS AND APPLICATIONS IN CRYPTOGRAPHY

AUTHOR:

RAÚL ALEGRE

University of Zaragoza

FINAL DEGREE THESIS

2015

DEGREE IN MATHEMATICS

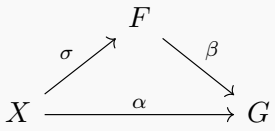
Summary (Spanish)

§1. Grupos libres y presentaciones de grupos

Sin entrar en muchos detalles, podríamos decir que la teoría combinatoria de grupos trata de describir la estructura de un grupo por medio de lo que se llama una *presentación*. Como veremos más adelante, una presentación consiste en una pareja (X, R) , donde X es un conjunto de *generadores* y R es un conjunto de *relaciones*.

Sin embargo, antes de trabajar con presentaciones es necesario introducir el concepto de *grupo libre*. Los grupos libres son los bloques básicos de la teoría combinatoria de grupos, razón por la cual dedicamos toda la atención inicial a definirlos con precisión, siguiendo el enfoque de [1].

Definición (Grupo libre). *Dado un grupo F, un conjunto no vacío X y una función $\sigma : X \longrightarrow F$, decimos que (F, σ) es* libre *en X si a cada función α de X a un grupo G le corresponde un único homomorfismo $\beta : F \longrightarrow G$ tal que $\alpha = \beta \circ \sigma$, i.e. el siguiente diagrama es conmutativo.*



Dada esta definición, nos hacemos unas preguntas muy naturales como la existencia y unicidad de los grupos libres. La respuesta queda resumida en los dos siguientes teoremas, fundamentales en el primer capítulo.

Teorema (Existencia de grupos libres). *Dado un conjunto no vacío X, existen un grupo F y una función $\sigma : X \longrightarrow F$ tales que el par (F, σ) es libre en X.*

Teorema (Unicidad de grupos libres). *Sean F_1 y F_2 grupos libres sobre X_1 y X_2 respectivamente. Entonces $F_1 \simeq F_2$ si y solo si $|X_1| = |X_2|$.*

Una vez establecida esta base, nos disponemos a estudiar la estructura de grupo libre. En este contexto surgen de forma natural los conceptos de *palabra reducida* sobre un conjunto X, fundamentales en el estudio de grupos libres. Además, nos permite estudiar diferentes ejemplos de grupos libres que aparecen en la naturaleza.

Una vez estudiados los grupos libres, establecemos la relación con grupos arbitarios por medio de las llamadas presentaciones. La idea es partir de un grupo libre y forzar ciertas igualdades entre

elementos haciendo un cociente. Es común llamar X al conjunto de generadores del grupo libre y R a un conjunto que genere normalmente el grupo por el que tomamos el cociente. Así, el nuevo grupo se denota $\langle X \mid R \rangle$.

Aunque la definición sea un poco opaca (al igual que la de grupos libres), la idea es ciertamente sencilla. Por ejemplo, tenemos las siguientes presentaciones de grupo cíclico y diédrico.

$$\mathbb{Z}_n = \langle a \mid a^n = 1 \rangle, \qquad D_n = \langle r, s \mid r^n = 1, s^2 = 1, srs = r^{-1} \rangle.$$

La aplicabilidad de las presentaciones queda recogida en el siguiente teorema.

Teorema (Existencia de presentaciones). *Todo grupo admite una presentación.*

§2. Grafos de Cayley

Cambiamos ahora el terreno de juego y pasamos a estudiar conceptos más geométricos. El objetivo que perseguimos es estudiar la estructura de los grupos a través de su relación con la geometría, la cual se ilustra de forma magistral en [2]. En particular, el objeto central de este capítulo será el *grafo de Cayley* de un grupo.

Definición (Grafo de Cayley). *Sea G un grupo con conjunto generador X. El* grafo de Cayley *de G con respecto a X es el grafo:*

- *cuyos vértices son los elementos de G, y*
- *cuyas aristas unen g y g' si y solo si $g' = gx$ para algún $x \in X$.*

Este grafo será denotado por $\Gamma_{G,X}$.

Resulta que los grupos actúan de forma natural sobre sus grafos de Cayley, siendo esta acción precisamente la conexión que buscábamos entre grupos y geometría. Esto nos permite estudiar los grupos desde una nueva perspectiva. En esta línea, encontramos la siguiente caracterización de grupos libres.

Teorema (Grupos libres y árboles). *Un grupo es libre si y solo si actúa libremente sobre un árbol.*

De aquí se deduce fácilmente que los subgrupos de grupos libres también son libres. Notar que de otra manera, este resultado no es para nada trivial.

Terminamos el capítulo con la noción de *grupo fundamental*, dando un método para construir espacios con un grupo fundamental predeterminado. Esto lo haremos tomando una presentación del grupo, construyendo el grafo de Cayley y aprovechando la acción que mencionábamos.

§3. Construyendo nuevos grupos

En este capítulo volvemos a trabajar con presentaciones de grupos, haciendo diversas manipulaciones con ellas. En particular, estudiaremos qué sucede cuando juntamos presentaciones de dos grupos y cuando añadimos algunas relaciones. Un buen compendio de estas manipulaciones se puede encontrar en [3].

De hecho, la primera construcción que estudiamos es el conocido producto directo de dos grupos. La novedad es que utilizaremos una propiedad universal para definirlo, algo que puede parecer forzado en este ejemplo pero resulta inevitable en otras construcciones. Por otra parte, es un primer ejemplo fácil de entender para ver qué pasa cuando mezclamos presentaciones de dos grupos.

Lo que sigue en el capítulo es una lista de construcciones habituales, y su caracterización en términos de presentaciones. En particular, estudiamos *productos semidirectos, productos libres, productos libres con amalgama y extensiones HNN.*

Por último, hacemos una mención a la teoría de Bass-Serre, que de nuevo se centra en describir la estructura de grupos estudiando cómo éstos actúan sobre árboles. Esto nos permitirá describir el grupo $\mathrm{SL}_2(\mathbb{Z})$ como un producto libre con amalgama de grupos cíclicos. Una referencia clásica en esta teoría es [4].

§4. Problemas de decisión y criptografía

En este último capítulo estudiamos algunas cuestiones algorítmicas que surgen de forma natural cuando trabajamos con presentaciones de grupos. En particular, estudiamos los llamados *problemas de decisión* que introdujo Max Dehn en su estudio de grupos fundamentales. Una bonita introducción histórica puede encontrarse en [5].

En concreto, presentamos el problema de la palabra (conocido como *word problem*), el problema de la conjugación (*conjugacy problem*) y el problema del isomorfismo (*isomorphism problem*). Las preguntas que plantean estos problemas son sencillas de entender, pero su solución parece escapar siempre de una respuesta simple. Esta situación nos lleva a estudiar qué significa resolver un problema, y enunciamos sin demostración que existen grupos para los cuáles los problemas mencionados son indecidibles.

Por último, describimos dos esquemas criptográficos basados en la teoría desarrollada. En particular, la seguridad de estos protocolos estará basada en la dificultad de resolver problemas similares a los descritos anteriormente. Una multitud de aplicaciones de la teoría de grupos a la criptografía puede encontrarse en [6].

Table of Contents

Chapter I

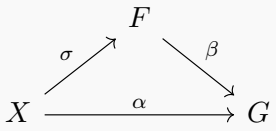
Free Groups and Group presentations

Informally speaking, combinatorial group theory is the study of groups in terms of generators and relations. In this chapter we will study free groups, the building blocks of combinatorial group theory. Then we discuss how the elements of a free group can be expressed, introducing the concept of normal form. In the last section, we make a connection between free groups and arbitrary groups introducing the concept of presentation of a group.

§1. Free groups

There are several ways to introduce free groups, the following definition is based on the so called universal properties.

Definition I.1 (Free group). *Given a group F, a nonempty set X and a function $\sigma : X \longrightarrow F$, we say that (F, σ) is* free *on X if to each function α from X to a group G there corresponds a unique homomorphism $\beta : F \longrightarrow G$ such that $\alpha = \beta \circ \sigma$, i.e. the following diagram commutes.*



Usually $X \subset F$ and $\sigma : X \hookrightarrow F$ is the inclusion. In this situation X is said to be a free basis for F, and β is the only homomorphism extending α. Let us take a look at several examples to gain insight into this definition.

Example I.1. *Consider the infinite cyclic group $F = \mathbb{Z}$, the set $X = \{1\}$ and $\sigma : \{1\} \hookrightarrow F$ to be the inclusion. Then, (F, σ) is free on X. Given any group G and a function $\alpha : \{1\} \longrightarrow G,\ 1 \longmapsto g$,*

we can consider:

$$\begin{array}{ccc} \mathbb{Z} & \xrightarrow{\beta} & G \\ n & \longmapsto & g^n. \end{array}$$

Clearly β is a homomorphism extending α. Furthermore, it is unique since any other homomorphism γ extending α satisfies $\gamma(1) = g = \beta(1)$, but this is enough to conclude $\gamma = \beta$, since $\{1\}$ generates $\mathbb{Z}$.

Example I.2. *The group $F = \mathbb{Z}$ with the inclusion is not free on $X = \{1, 2\}$. Indeed, consider $G = \mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$ and the function $\alpha : \{1, 2\} \to \mathbb{Z}_3$ given by $\alpha(1) = \alpha(2) = \overline{1}$. If we could find a homomorphism β extending α, the following would be true:*

$$\overline{1} = \alpha(2) = \beta(2) = \beta(1 + 1) = \beta(1) + \beta(1) = \alpha(1) + \alpha(1) = \overline{1} + \overline{1} = \overline{2}.$$

The problem with X is that it is not free enough. For now, it is enough to note that there is some relationship between elements of X, namely $2 = 1 + 1$.

As we will see later, free groups are those where there are no hidden relations. In some sense, the underlying structure is the simplest possible. Before we continue, let us show that free groups on a given nonempty set always exist.

Theorem I.1 (Existence of free groups). *Given a nonempty set X, there exists a group F and a function $\sigma : X \longrightarrow F$ such that (F, σ) is free on X. Furthermore, the subset $\operatorname{Im}\sigma$ generates F.*

Proof. The proof has two steps. First, we define a group F using the set X and a function $\sigma : X \longrightarrow F$. Then, we check that this group F together with σ is free on X.

Construction of (F, σ). Define the set $X^{-1} = \{x^{-1} \mid x \in X\}$, where x^{-1} is just a symbol. Let $\{X \cup X^{-1}\}^*$ denote the set of all finite sequences of elements of X and X^{-1}. For convenience, we will refer to these sequences as *words* in X. Each word $w \in \{X \cup X^{-1}\}^*$ can be written as:

$$w = x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n}, \qquad \text{where} \quad x_i \in X, \quad \varepsilon_i = \pm 1.$$

If $n = 0$, we say that w is the empty word and we write $w = 1$. Now define a product in $\{X \cup X^{-1}\}^*$ as follows:

$$w = x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n}, \quad v = y_1^{\nu_1} \dots y_m^{\nu_m} \quad \Longrightarrow \quad wv = x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n} y_1^{\nu_1} \dots y_m^{\nu_m},$$

with the convention $w1 = w = 1w$. The inverse of w is the word $w^{-1} = x_n^{-\varepsilon_n} \dots x_1^{-\varepsilon_1}$, with $1^{-1} = 1$. Finally, we need to define an equivalence relation $\sim$ in $\{X \cup X^{-1}\}^*$. We say that two words are equivalent if we can pass from one to the other inserting or deleting pairs of the form xx^{-1} or $x^{-1}x$. Clearly $\sim$ is an equivalence relation. Denote by $[u]$ the equivalence class of a word u and let F be the set of equivalence classes:

$$F = \{X \cup X^{-1}\}^* / \sim .$$

Furthermore, if $u \sim u'$ and $v \sim v'$, obviously $uv \sim u'v'$, and it makes sense define the product $[u][v] = [uv]$. This operation has the following properties.

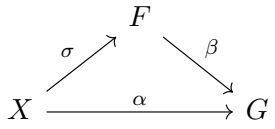
1. Associativity: $([u][v])[w] = [u]([v][w])$.
2. Existence of identity: $[1][w] = [w] = [w][1]$.
3. Existence of inverse: $[w]^{-1}[w] = [1] = [w][w]^{-1}$ with $[w]^{-1} = [w^{-1}]$.

Thus, F is a group generated by elements of the form $[x]$. Now we define σ to be:

$$\begin{array}{ccc} X & \xrightarrow{\sigma} & F \\ x & \longmapsto & [x], \end{array}$$

so that $F = \langle \operatorname{Im} \sigma \rangle$.

The group F together with σ is free on X. Suppose we are given a group G and a function $\alpha : X \longrightarrow G$. We should find a homomorphism β such that the diagram commutes.



To do so, we start defining the function $\bar{\beta}$:

$$\begin{array}{ccc} \{X \cup X^{-1}\}^* & \xrightarrow{\bar{\beta}} & G \\ x_1^{\varepsilon_1} \dots x_n^{\varepsilon_n} & \longmapsto & \alpha(x_1)^{\varepsilon_1} \dots \alpha(x_n)^{\varepsilon_n}. \end{array}$$

Now, it should be clear that $w \sim w'$ implies $\bar{\beta}(w) = \bar{\beta}(w')$, since the pairs xx^{-1} and $x^{-1}x$ map to pairs of the form gg^{-1}, which are equal to 1_G. This allows us to define:

$$\begin{array}{ccc} F & \xrightarrow{\beta} & G \\ [w] & \longmapsto & \bar{\beta}(w). \end{array}$$

Clearly $\alpha = \beta \circ \sigma$. Finally, we need to check the uniqueness of β. If γ satisfies $\alpha = \gamma \circ \sigma$, we have $\gamma([x]) = \beta([x]),\ x \in X$. However, since these elements generate F, it follows that $\gamma = \beta$. □

Since the given proof is constructive, we can write specific examples. Suppose we have the set $X = \{a\}$, then we consider the set of words $\{a, a^{-1}\}^*$, where we can find elements such as aaa^{-1} or $a^{-1}a^{-1}$. We form the group F identifying words that are the same up to cancellation of aa^{-1} or $a^{-1}a$. Thus, we write:

$$[aaa^{-1}] = [a] \qquad \text{or} \qquad [a^{-1}a^{-1}] = [a]^{-2}.$$

In general, we will be sloppy with the notation and drop the brackets, so that we just write:

$$F = \{a^n \mid n \in \mathbb{Z}\} \simeq \mathbb{Z}.$$

Therefore, the group F provided by the theorem is the same as the one we found in our first example. This suggests the idea of uniqueness of free groups in some sense. The following theorem addresses this question.

Theorem I.2 (Uniqueness of free groups). *Let F_1 and F_2 be free groups on X_1 and X_2 respectively. Then $F_1 \simeq F_2$ if and only if $|X_1| = |X_2|$.*

Proof. In order to avoid set theoretic issues, we will prove the theorem only in the case X_1 and X_2 are finite. Thus we can write

$$X_1 = \{x_1, x_2, \ldots, x_n\} \qquad X_2 = \{y_1, y_2, \ldots, y_m\}.$$

In addition, let σ_1, σ_2 be the usual maps from the corresponding set to the free group.

$\Longrightarrow$) Consider the set Hom $(F_1, \mathbb{Z}_2)$ of homomorphisms from F_1 to $\mathbb{Z}_2$. This set is a vector space over $\mathbb{Z}_2$ in the obvious way, namely:

$$\begin{array}{ccc} F_1 & \xrightarrow{\theta_1+\theta_2} & \mathbb{Z}_2 \\ x & \longmapsto & \theta_1(x)+\theta_2(x), \end{array} \qquad \begin{array}{ccc} F_1 & \xrightarrow{\lambda\theta} & \mathbb{Z}_2 \\ x & \longmapsto & \lambda\theta(x). \end{array}$$

Call this vector space V_1, now we want to find a basis. To do so, fix $x_i \in X_1$ and consider the function $\alpha_i : X \longrightarrow \mathbb{Z}_2$ given by $\alpha_i(x_i) = 1$ and $\alpha_i(x_j) = 0$ if $i \neq j$. Then there exists a homomorphism $\beta_i \in$ Hom $(F_1, \mathbb{Z}_2)$ extending α_i. We claim that the family

$$\{\beta_1, \beta_2 \ldots, \beta_n\},$$

is a basis for V_1. Indeed, any $\theta \in$ Hom $(F_1, \mathbb{Z}_2)$ can be written as:

$$\theta = t_1\beta_1 + t_2\beta_2 + \ldots + t_n\beta_n \qquad \text{where} \qquad t_i = \theta(\sigma_1(x_i)),$$

and this decomposition is unique. Hence, we conclude that

$$\dim V_1 = n = |X_1|.$$

In the same vein, the set Hom $(F_2, \mathbb{Z}_2)$ forms another vector space V_2 over $\mathbb{Z}_2$ with dimension

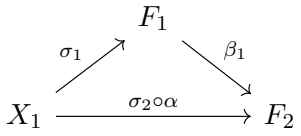
$$\dim V_2 = m = |X_2|.$$

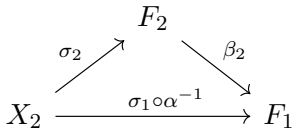
Now we use the hypothesis. If $F_1 \simeq F_2$, there is an isomorphism $F_2 \xrightarrow{\gamma} F_1$ that induces an isomorphism between V_1 and V_2 given by $\theta \in V_1 \longmapsto \theta \circ \gamma \in V_2$. Thus, the two vector spaces are isomorphic and they must have the same dimension, therefore:

$$|X_1| = |X_2|,$$

as we wanted to show.

$\Longleftarrow$) Assume $|X_1| = |X_2|$, so that there exists a bijection $X_1 \xrightarrow{\alpha} X_2$. Recall that the definition of free group ensures the existence of the following diagrams:

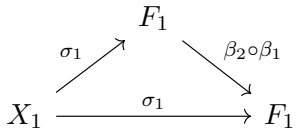




Hence

$$\beta_2 \circ (\beta_1 \circ \sigma_1) = \beta_2 \circ (\sigma_2 \circ \alpha) = (\sigma_1 \circ \alpha^{-1}) \circ \alpha = \sigma_1,$$

making the following diagram commutative



Now $\beta_2 \circ \beta_1 = \mathrm{Id}_{F_1}$ since the identity on F_1 is a homomorphism that makes the diagram commutative and it must be unique. Exchanging the roles of F_1 and F_2, we see that $\beta_1 \circ \beta_2 = \mathrm{Id}_{F_2}$. Then β_1 and β_2 are inverse isomorphisms and

$$F_1 \simeq F_2,$$

as we wanted to show. □

Now we can define the *rank* of a free group as the cardinality of any set on which it is free. Given a natural number n, we have proved that there exists a unique free group of rank n up to isomorphism. In particular, any free group of rank 1 is isomorphic to $\mathbb{Z}$. Free groups of rank 2 will appear later, but first we need to develop some ideas.

§2. A word about words

In the light of the proof of the theorems, we are going to play around with words quite often. Given this situation, we would like to know if some words are somehow more tractable than others. For example, it seems reasonable to reduce $aa^{-1}a^{-1}$ to the word a^{-1}, which is certainly easier to use. Thus, we say that a word is *reduced* if no further cancellation is possible.

Proposition I.3. *Let X be a nonempty set. Each equivalence class of words in X contains exactly one reduced word.*

Proof. Existence is trivial, just reduce the given word until no further cancellation is possible. Let R denote the set of reduced words and consider $u \in X \cup X^{-1}$. We can define a permutation $u' : R \longrightarrow R$ given by

$$u'(x_1^{\varepsilon_1} \dots x_r^{\varepsilon_r}) = \begin{cases} x_1^{\varepsilon_1} \dots x_r^{\varepsilon_r} u & \text{if} \quad u \neq x_r^{-\varepsilon_r} \\ x_1^{\varepsilon_1} \dots x_{r-1}^{\varepsilon_{r-1}} & \text{if} \quad u = x_r^{-\varepsilon_r}. \end{cases}$$

Now, we consider the group G of permutations of R, namely $G = \mathrm{Sym}\ R$ and define the function $\alpha : X \longrightarrow G$, $x \longmapsto x'$. Thus, there exists a unique homomorphism $\beta : F \longrightarrow G$ such that $\beta([x]) = x'$. Now let $v, w \in R$ and assume $v = x_1^{\varepsilon_1} \dots x_r^{\varepsilon_r}$, then $\beta([v]) = (x_1^{\varepsilon_1})' \dots (x_r^{\varepsilon_r})'$ sends the empty word to v. Similarly $\beta([w])$ sends the empty word to w. Now, if $[v] = [w]$, then $\beta([v]) = \beta([w])$ as permutations of R, then they send the empty word to the same element, yielding $v = w$. □

Thus, given an element of a free group, we can always write it as $[w]$, where w is reduced. If $[w] = [x_1]^{\varepsilon_1} \dots [x_s]^{\varepsilon_s}$, we can multiply together consecutive terms involving the same letter and drop the brackets to write

$$w = x_1^{l_1} \dots x_r^{l_r} \qquad \text{where } x_i \in X,\ r \geq 0,\ l_i \neq 0,\ x_i \neq x_{i+1}.$$

in a unique way. This expression is called the *normal form of* w. The existence of normal forms with this behaviour characterizes free groups, as we see in the next proposition.

Proposition I.4 (Characterization of free groups). *Let G be a group and X a subset of G. If every element of G can be written as $x_1^{l_1} \dots x_r^{l_r}$ where $x_i \in X$, $l_i \neq 0$, $x_i \neq x_{i+1}$ in a unique way, then G is free on X.*

Proof. Construct a free group F on X and use the defining property of free groups, with $\alpha : X \hookrightarrow G$ being the inclusion. Then there exists a unique homomorphism β such that $\beta([x]) = x$ for each $x \in X$, we claim that β is an isomorphism. Clearly β is surjective since X generates G. Injectivity follows by the existence and uniqueness of normals forms, indeed, for any $[v]$, $[w]$, we can assume that v and w are reduced and follows immediately that $\beta([v]) = \beta([w])$ implies $[v] = [w]$. □

The above proposition can be used directly to check whether a given group is free or not.

Example I.3. *Consider the group $\mathbb{Z} \times \mathbb{Z}$ and suppose it is free on X. Clearly X has at least two elements (otherwise $\mathbb{Z} \times \mathbb{Z} \simeq \mathbb{Z}$). Now take $a, b \in X$ and (writing the group operation as a product) note that $ab = ba$. Thus we have an element whose decomposition as a product of elements of X is not unique. This contradiction shows $\mathbb{Z} \times \mathbb{Z}$ is not free.*

When the group is free, a direct approach is likely to be unsuccessful, since it is difficult to prove the uniqueness of the normal form. We can solve this problem if we find a suitable action of the group on a set, as the next lemma shows.

Proposition I.5 (Ping-Pong Lemma). *Let G be a group with a generating set $X = \{a, b\}$, acting on a set S. If we can find subsets $A, B \subseteq S$ such that $A \cap B = \varnothing$ satisfying $a^n \cdot B \subseteq A$ and $b^n \cdot A \subseteq B$ for all integers $n \neq 0$, then G is free on X.*

Proof. Since X is a generating set, every element of G can be written as a reduced word in X. To show the uniqueness of this expression, it is enough to prove that no nontrivial product equals the identity. First suppose that w begins and ends with a power of a, then:

$$w = a^{n_1} b^{m_1} \dots a^{n_{r-1}} b^{m_{r-1}} a^{n_r} \qquad \text{where} \qquad n_i, m_i \neq 0.$$

We study the action of w on B.

$$\begin{aligned} w \cdot B &= a^{n_1} b^{m_1} \dots a^{n_{r-1}} b^{m_{r-1}} a^{n_r} \cdot B \subseteq a^{n_1} b^{m_1} \dots a^{n_{r-1}} b^{m_{r-1}} \cdot A \\ &\subseteq a^{n_1} b^{m_1} \dots a^{n_{r-1}} \cdot B \subseteq \dots \subseteq a^{n_1} \cdot B \subseteq A. \end{aligned}$$

Therefore $w \neq 1$. For any other word w we can find conjugates $a^{-m}wa^m$ that begin and end with a power of a (for m large enough). Since $a^{-m}wa^m \neq 1$, then $w \neq 1$. Now we can use the characterization of free groups to deduce that G is free on X. □

Now we are ready to work with some examples that appear in nature. Recall that $\mathrm{SL}_2(\mathbb{Z})$ is the group consisting of 2×2 matrices with integer entries and determinant 1.

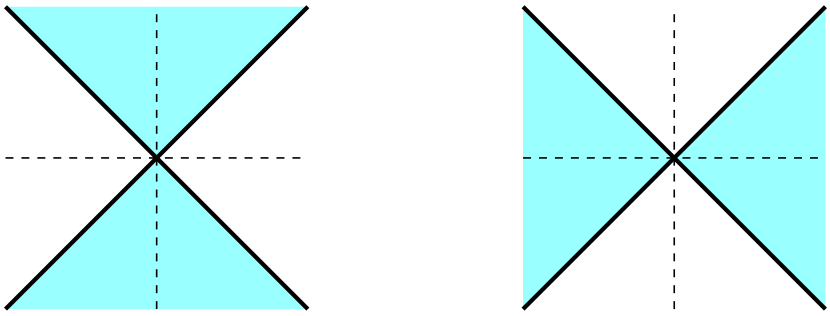
Example I.4. *The group* $\mathrm{SL}_2(\mathbb{Z})$ *has a free subgroup of rank 2. Indeed, let*

$$a = \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}, \quad b = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix},$$

and define $X = \{a, b\}$. *Then* $G = \langle X \rangle$ *is free on* X.

Proof. We will make use of the ping-pong lemma. Since G acts on the euclidean plane by left multiplication, consider the subsets A, $B \subseteq \mathbb{R}^2$ defined as:

$$A = \left\{ \begin{bmatrix} x \\ y \end{bmatrix} \in \mathbb{R}^2 \;\middle|\; |x| < |y| \right\}, \quad B = \left\{ \begin{bmatrix} x \\ y \end{bmatrix} \in \mathbb{R}^2 \;\middle|\; |x| > |y| \right\}.$$



The region A. The region B.

Figure I.1: Two disjoints subsets of the euclidean plane are indicated.

Elementary calculations show that, for each integer n:

$$a^n = \begin{bmatrix} 1 & 0 \\ 2n & 1 \end{bmatrix}, \quad b^n = \begin{bmatrix} 1 & 2n \\ 0 & 1 \end{bmatrix}.$$

Therefore

$$a^n \cdot \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} x \\ 2nx + y \end{bmatrix}, \qquad b^n \cdot \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} x + 2ny \\ y \end{bmatrix}.$$

Now recall that given $|n| \geq 1$.

$$\begin{aligned} |x| > |y| \quad &\Longrightarrow \quad |2nx + y| \geq 2|n||x| - |y| > (2|n| - 1)|x| \geq |x|, \\ |x| < |y| \quad &\Longrightarrow \quad |x + 2ny| \geq 2|n||y| - |x| > (2|n| - 1)|y| \geq |y|, \end{aligned}$$

yielding

$$a^n \cdot B \subseteq A, \qquad b^n \cdot A \subseteq B \qquad \text{for all integers } n \neq 0.$$

It follows from the ping-pong lemma that G is free on X. □

For the next example, recall that a Möbius transformation is a permutation of the set $\hat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ of the form:

$$z \mapsto \frac{az+b}{cz+d} \qquad \text{where} \quad a, b, c, d \in \mathbb{C} \quad \text{satisfy} \quad ad - bc \neq 0.$$

The set of Möbius transformations forms a group, usually denoted as $\mathrm{Aut}(\hat{\mathbb{C}})$.

Example I.5. *The group of Möbius transformations has a free subgroup of rank 2. Consider* $\alpha, \beta \in \mathrm{Aut}(\hat{\mathbb{C}})$ *defined as:*

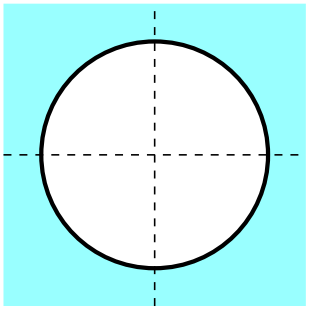
$$\alpha(z) = z + 2, \qquad \beta(z) = \frac{z}{2z+1}, \qquad z \in \hat{\mathbb{C}},$$

and define $X = \{\alpha, \beta\}$. *The group* $G = \langle X \rangle$ *is free on* X.

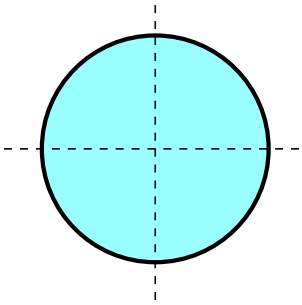
Proof. The group G acts trivially on $\hat{\mathbb{C}}$. The proof in similar to the last example, considering the sets

$$A = \{z \in \mathbb{C} \mid |z| > 1\}, \qquad B = \{z \in \mathbb{C} \mid |z| < 1\}.$$

□



The region A.



The region B.

Figure I.2: Two disjoints subsets of $\hat{\mathbb{C}}$ are indicated.

Remark

The similarities between these two examples are not an accident. There exists a trivial correspondence between Möbius transformations and 2×2 matrices with nonzero determinant. Namely:

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \longmapsto \left(z \mapsto \frac{az+b}{cz+d} \right).$$

It is easily seen that this correspondence is an epimorphism. It is not injective since M and λM map to the same Möbius transformation for any $0 \neq \lambda \in \mathbb{C}$. Then the first isomorphism theorem applies to deduce:

$$\mathrm{Aut}(\hat{\mathbb{C}}) \simeq \mathrm{PGL}_2(\mathbb{C}),$$

where $\mathrm{PGL}_2(\mathbb{C})$ is called projective general linear group.

§3. Group presentations

We promised that free groups would help us to describe other groups. However, so far free groups have been studied on their own. Now we introduce the relation between free groups and arbitrary groups, but before we introduce the main result, we provide an illustrative example.

Example I.6. *We know that $\mathbb{Z}\times\mathbb{Z}$ is not free on $X=\{a,b\}$, where $a=(1,0)$, $b=(0,1)$. However $\mathbb{Z}\times\mathbb{Z}$ behaves as the free group F on X with the additional constraint $ab=ba$.*

In fact, if we let $N\triangleleft F_2$ denote the normal closure of $aba^{-1}b^{-1}$ in F, the quotient F/N has the desired behaviour, since in this group $(ab)N=(ba)N$. Thus one can show $\mathbb{Z}\times\mathbb{Z}\simeq F/N$, and this construction suggests to write:

$$\mathbb{Z}\times\mathbb{Z}=\langle a,b\mid ab=ba\rangle.$$

The situation in the example is quite common, so it deserves a general definition.

Definition I.2 (Group presentation). *Let F be a free group on a nonempty set X, and R a subset of F. Let N denote the normal closure of R in F. Then we define the* group generated by X with relations R *to be F/N. This group is denoted*

$$\langle X\mid R\rangle.$$

If $G\simeq\langle X\mid R\rangle$, we say that $\langle X\mid R\rangle$ is a presentation for G.

We usually do not distinguish between a group and its presentation, so we will write $G=\langle X\mid R\rangle$. If X and R are both finite, we say that G is finitely presented, and we will write

$$G=\langle x_1,\, x_2,\ldots,\, x_n\mid r_1,\, r_2,\,\ldots,\, r_m\rangle.$$

Usually, relations of the form "$\tilde{w}w^{-1}$" will be written as "$\tilde{w}=w$".

Note that the relations in $\langle X\mid R\rangle$ allow different spellings for the same element. Sometimes we want to emphasize that two (possibly different) words represent the same element, and we will write $w=_G w'$.

Which groups can be described using a presentation? The following theorem generalizes the previous example and justifies the importance of free groups.

Theorem I.6. *Every group can be expressed as the quotient of a free group. In particular, every group admits a presentation.*

Proof. Denote the group by G and take a generating set X (note that always exists one, as we can take the whole G). Now we construct the free group on X and define $\alpha : X \hookrightarrow G$ to be the inclusion. The defining property of free groups says that there exists a unique homomorphism β such that $\alpha = \beta \circ \sigma$. Since X is a generating set, β is surjective, and the first isomorphism theorem yields

$$G \simeq F/\ker\beta.$$

Thus, G is a quotient of F. Now take a set R that normally generates $\ker\beta$ and we have the desired presentation (once again, we can take R to be the whole $\ker\beta$). □

Informally speaking, R codifies the relations that should hold in the group G. Several examples will help to understand this notation.

Example I.7. *In $\mathbb{Z}\times\mathbb{Z}$, the crucial constraint is $ab = ba$, so we define $R = \{aba^{-1}b^{-1}\}$. Then a presentation is*

$$\mathbb{Z}\times\mathbb{Z} = \langle a, b \mid aba^{-1}b^{-1}\rangle \qquad or \qquad \mathbb{Z}\times\mathbb{Z} = \langle a, b \mid ab = ba\rangle.$$

Example I.8. *In $\mathbb{Z}_n$, let $a = \overline{1}$ and write the group operation as a product. Then a^n equals the identity and we have the presentation:*

$$\mathbb{Z}_n = \langle a \mid a^n = 1\rangle.$$

Example I.9. *Consider the dihedral group. This group is generated by two elements, a rotation r and a symmetry s. The properties of these elements are codified in the presentation*

$$D_n = \langle r, s \mid r^n = 1,\ s^2 = 1,\ srs = r^{-1}\rangle.$$

Example I.10. *The quaternion group can be presented as*

$$Q = \langle i, j, k \mid i^2 = j^2 = k^2 = ijk\rangle,$$

where the identity is denoted 1, the common element $i^2 = j^2 = k^2 = ijk$ is denoted -1 and the elements i^3, j^3, k^3 are denoted $-i, -j, -k$ respectively.

Example I.11. *The Baumslag-Solitar group $BS(m, n)$ is defined to be*

$$\mathrm{BS}(m, n) = \langle a, t \mid t^{-1}a^m t = a^n\rangle.$$

Example I.12. *Any group of the form*

$$G = \langle X \mid r = 1\rangle,$$

is called a one relator *group. $\mathbb{Z}\times\mathbb{Z}$, $\mathbb{Z}_n$ and $\mathrm{BS}(m, n)$ are one relator groups.*

Example I.13. *A presentation without relations yields a free group. Thus*

$$G = \langle X \mid \varnothing\rangle,$$

is free of rank $|X|$.

Chapter II

Cayley graphs

§1. Introduction

In this chapter we discuss some aspects of geometric group theory and their relation to combinatorial group theory. In particular, we will focus our attention on the interplay between groups and graphs.

Given a group G with a generating set X, we can construct a graph $\Gamma_{G,X}$ called the Cayley graph. It turns out that the group acts naturally on the graph, making possible to study the properties of the former when the latter is known. In addition, these graphs give a characterization for free groups. Finally, we will see how Cayley graphs can be used to construct spaces with a desired fundamental group.

Of course, the whole relation between groups and geometry will be possible thanks to the formalism of group presentations we have developed so far.

§2. Cayley Graphs

In this section we start with a group G with a generating set X. The goal is to translate the group structure into a graph called Cayley graph.

Definition II.1 (Cayley graph). *Let G be a group with generating set X. The* Cayley Graph *of G with respect to X is the graph whose:*

- *vertices are the elements of G, and*
- *edges join g and g' if and only if $g' = gx$ for some $x \in X$.*

We denote this graph $\Gamma_{G,X}$.

Usually, $\Gamma_{G,X}$ has labels on both the vertices and the edges. The following examples should clarify these ideas.

Example II.1. *The Cayley Graph of the group $G = \mathbb{Z}$ with generating set $X = \{1\}$ is*

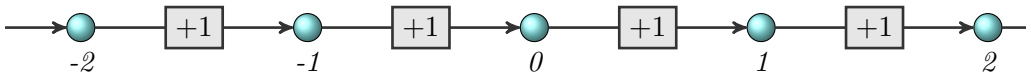
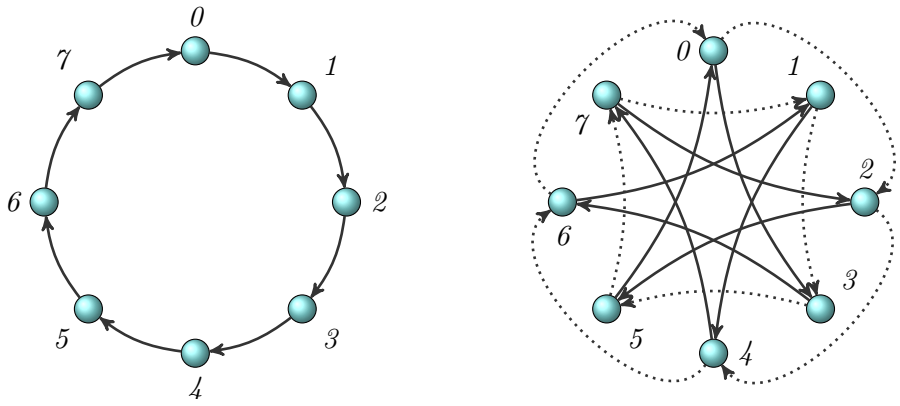


Figure II.1: Cayley Graph $\Gamma_{\mathbb{Z},\{1\}}$.

In order to make cleaner graphs, we will not write the labels on the edges. Instead, we will plot the edges using different patterns to denote different generators.

Example II.2. *The Cayley Graph depends on the generating set. Consider $G = \mathbb{Z}_8$ and the generating sets $X = \{1\}$, $Y = \{2, 3\}$. The two Cayley Graphs are shown.*



$\Gamma_{G,X}$. $\Gamma_{G,Y}$.

Figure II.2: Cayley graphs with different generating sets.

Example II.3. *Consider the Dihedral group D_6 with generating set $X = \{r, s\}$.*

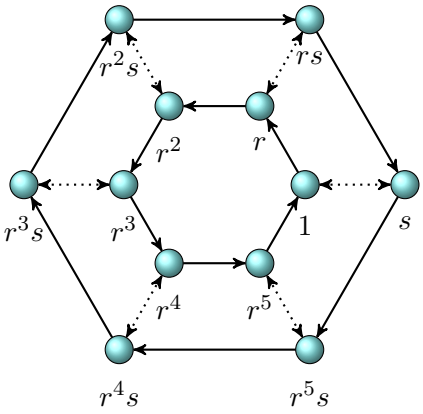


Figure II.3: Cayley Graph of a dihedral group.

§3. Group actions on graphs

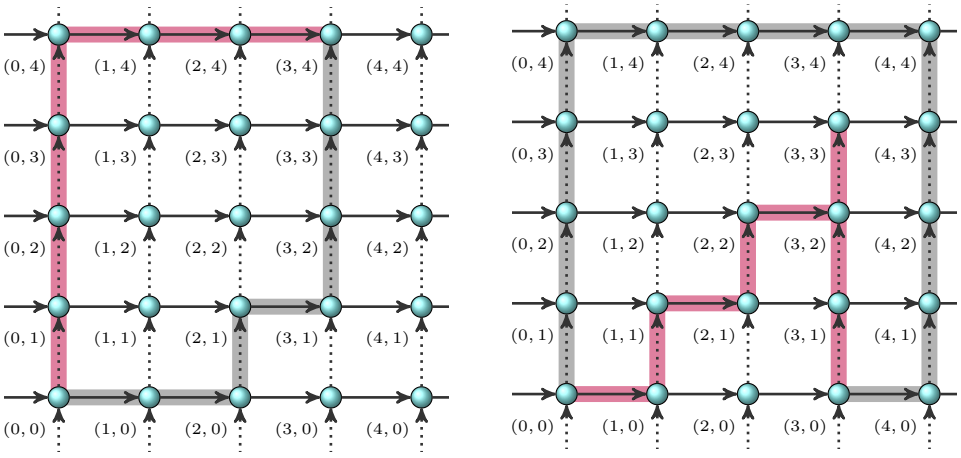
We said we could take advantage of the relation between groups and geometry. This section tries to make this connection a little more precise.

Theorem II.1 (Cayley's Better Theorem). *Every finitely generated group can be faithfully represented as a symmetry group of a connected, directed, locally finite graph.*

Proof. (Sketch) The difficult part is to find the graph, but we already defined it. Consider a Cayley graph and define the action of G by left multiplication (i.e. the element g moves the vertex h to the vertex gh). With this definition, the ends of an edge are preserved since they are defined by right multiplication and the action is well defined. Now the proof is straightforward. □

Given a group $G = \langle X \mid R \rangle$, this result allows us to identify a word $w \in G$ with a path in the Cayley graph $\Gamma_{G,X}$. It is enough to follow the vertices given by the word.

Example II.4. *Consider $G = \langle a, b \mid ab = ba \rangle$. The Cayley graph looks like a grid, as shown in the figure. We can think of a and b as $(1,0)$ and $(0,1)$, and we recover $\mathbb{Z} \times \mathbb{Z}$. Several paths are shown in the figure. Note that different words w, w' result in different paths ending in the same point precisely when $w =_G w'$.*



The words a^2bab^3 and b^4a^3. *The words $(ab)^3b^{-3}$ and $b^4a^4b^{-4}a^{-1}$.*

Figure II.4: Cayley Graph of $\mathbb{Z} \times \mathbb{Z}$ with respect to $\{(1,0),(0,1)\}$.

As wee see, this relationship between words and paths allows us to decide whether or not two words are the same as elements of the group (if the Cayley graph has been given). Just construct the two paths and check if they end in the same vertex.

§4. Free groups and graphs

Our next goal is to give a characterization of free groups in terms of their action on graphs. Before we introduce the main result, let us show how is the Cayley graph of a free group of rank 2.

Example II.5. *Consider the set $X = \{a, b\}$ and the free group $G = \langle X \mid \varnothing \rangle$. The Cayley graph is a tree where every vertex has valence 4.*

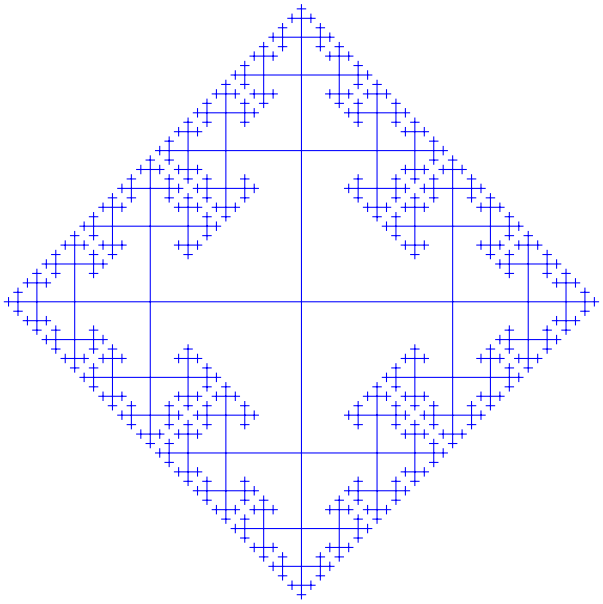


Figure II.5: Cayley graph of the free group of rank 2.

The fact that a free group has a tree as its Cayley graph it is no surprise. Indeed, any reduced word in a free group is not equal to the identity. As a consequence, any possible path in the corresponding Cayley graph is not a cycle. Finally, we note that trees are precisely the graphs without cycles. Recall that a group acts freely on its Cayley graph, the preceding comments motivate the main result of this section, which we quote without proof.

Theorem II.2 (Characterization of free groups). *A group G is free if and only if it acts freely on a tree.*

The converse requires more advanced tools and a clever use of (a generalization of) ping-pong lemma. This characterization shows how to take advantage of the interplay between groups and graphs. Indeed, an immediate consequence is the following.

Theorem II.3 (Nielsen-Schreier Theorem). *Every subgroup of a free group is free.*

§5. Fundamental Groups

We end this chapter studying how presentations of groups can be used to construct topological spaces with a certain fundamental group.

Definition II.2. *The* fundamental group *of a path connected topological space X is the group whose elements are the equivalence classes of loops under the equivalence relation of homotopy. We denote it by $\pi_1(X)$.*

The spaces we are going to be dealing with are sort of two dimensional extensions of graphs, in particular, we are going to use 2 dimensional cell complexes. A later example will show the basic features of their construction. However, we give first the main result.

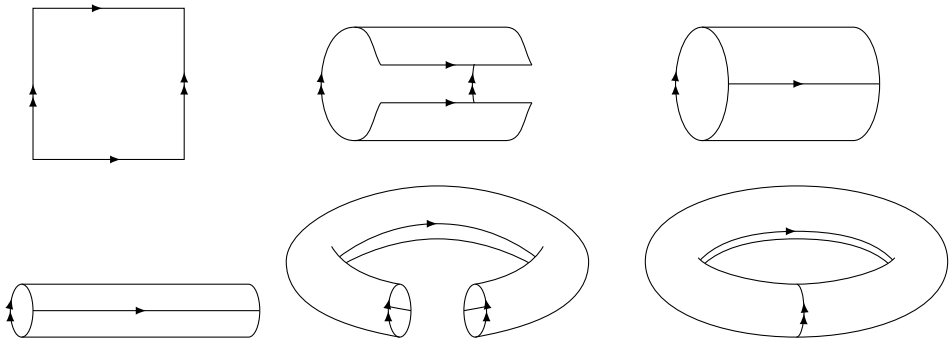
Proposition II.4. *For every group G there is a two dimensional cell complex X_G whose fundamental group is G, i.e. $\pi_1(X_G) = G$.*

Example II.6. *Consider $G = \mathbb{Z} \times \mathbb{Z} = \langle a, b \mid aba^{-1}b^{-1} = 1 \rangle$. We outline the construction of X_G.*

1. *Construct the Cayley graph as in (a).*
2. *Each relation is associated with a cycle in the Cayley graph. Starting on each vertex, we add 2-cells corresponding to the cycles as in (b).*
3. *Since we have an action of the group on the Cayley graph, we can take the corresponding quotient and obtain a space like the one in (c), where every vertex is identified, as well as edges corresponding to the same generator. However, the action extends naturally to the 2-cells, so we have to attach them identifying the edges shown in (d).*

(a) *(b)* *(c)* *(d)*

The following diagram helps to visualize how the attaching yields a torus. Then, the fundamental group of a torus is $\mathbb{Z} \times \mathbb{Z}$.



Chapter III

Constructing new groups

In this chapter we take advantage of the machinery developed in the first chapter to construct new groups. In particular, we will study what happens when we "mix" different presentations in a variety of ways. In addition, we will discuss how we can write the elements of the groups in each case.

§1. Normal forms

Suppose we are given a presentation of a group $G = \langle X \mid R \rangle$. When the group is not free, each word will have several spellings in terms of the generators, and this might cause some confusion. However, if we agree on a particular spelling, such a problem does not appear. We will call that particular spelling a normal form.

Normal forms are important in practice. For example, they are needed for several cryptographic schemes, where often one needs to check whether two words are the same. We will see later how hard this problem can be in general, however, if we agree on a normal form the solution is trivial once we are able to recognize the particular spelling.

Example III.1. *In free groups, we already focused our attention in a particular spelling. Of course, we are talking about the normal form defined in the first chapter.*

Example III.2. *In a group $G = \langle X \mid R \rangle$, we define an arbitrary order between elements of X. Now, for each element $g \in G$ take the set of words w such that $w =_G g$ and w has minimal length (these are called geodesic words). Finally, among these words, take the first one regarding the lexicographic order induced by the order in X. This particular choice is called* short-lex *normal form.*

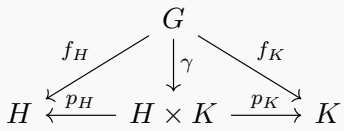
For example, in $\mathbb{Z} \times \mathbb{Z} = \langle a, b \mid ab = ba \rangle$, we can define the order $a < b$. Now, the geodesics word of a particular element are $a^i b^j$ and $b^j a^i$, and the short-lex normal form is $w = a^i b^j$.

§2. Direct product

Although this construction may be familiar to the reader, we will introduce it here in a new fashion. As we did with free groups, we can define the direct product of two groups by means of a universal property.

Definition III.1. *Let H, K, D be groups. We say that D is the direct product of H and K if there are homomorphisms $p_H : D \to H$, $p_K : D \to K$ such that: for each group G and homomorphisms $f_H : G \to H$, $f_K : G \to K$ there exists a unique homomorphism $\gamma : G \to D$ such that $f_H = p_H \circ \gamma$ and $f_K = p_K \circ \gamma$.*

In this situation, we write $D = H \times K$. The following diagram summarizes the definition.



The well-known construction of direct product $H \times K$ fits this definition. Moreover, a diagram chase using uniqueness shows the direct product is unique. However, now we want to see how group presentations help us to describe this group. Recall that the commutator of two subsets A, B of a group is

$$[A, B] = \{aba^{-1}b^{-1} \mid a \in A, b \in B\}.$$

Proposition III.1. *If $H = \langle X \mid R \rangle$, $K = \langle Y \mid S \rangle$, then*

$$H \times K = \langle X,\ Y \mid R,\ S,\ [X, Y] \rangle.$$

Proof. Let $D = \langle X,\ Y \mid R,\ S,\ [R, S] \rangle$. Now note that, since words in X and Y commute, every element w in D is a word in X, Y which can be written as $w = uv$, where u, v are words in X and Y respectively. Now define the homomorphisms $p_H : D \to H$, $p_K : D \to K$ as follows:

$$p_H(w) = u, \quad p_K(w) = v, \qquad \text{where} \quad w = uv.$$

Now suppose we are given a group G and homomorphisms $f_H : G \to H$, $f_K : G \to K$. Then we can define $\gamma : G \to D$ to be:

$$\gamma(g) = uv \qquad \text{where} \quad u = p_H(g),\ v = p_K(g),$$

where u and v are expressed as words in X and Y. Clearly, γ satisfies $f_H = p_H \circ \gamma$ and $f_K = p_K \circ \gamma$. Uniqueness is an immediate consequence of the commutativity of the diagram. □

In this case, there is not too much to say about normal forms. Using the commuting relations, every word can be written as $w = uv$ in a unique way, where u is a word in X and v is a word in Y. Of course, u and v will be expressed in the corresponding normal form of the groups H and K.

Remark

What about semi direct-products? There is not an easy way to mimic the last definition. In fact, there is a universal property for semi-direct products, but it explains how the elements behave, rather than the groups. Thus, we can not write a commutative diagram to introduce it.

However, group presentations still provide a nice description, which is encapsulated in the following proposition.

Proposition III.2. *Let $N = \langle X \mid R \rangle$, $H = \langle Y \mid S \rangle$, $\phi : H \longrightarrow \text{Aut } N$. Then*

$$H \rtimes_\phi K = \langle X,\ Y \mid R,\ S,\ \phi(h)(n) = hnh^{-1} \text{ for all } n \in N,\ h \in H \rangle.$$

The given commuting relations lead to the same comments regarding normal forms.

Example III.3. *The dihedral group D_n is a semi-direct product of $\mathbb{Z}_n$ and $\mathbb{Z}_2$. In fact, we have the presentations*

$$\mathbb{Z}_n = \langle r \mid r^n = 1 \rangle, \quad \mathbb{Z}_2 = \langle s \mid s^2 = 1 \rangle,$$

and we can let $\phi : \mathbb{Z}_2 \longrightarrow \text{Aut } \mathbb{Z}_n$ be the homomorphism defined by $\phi(s)(r) = r^{-1}$. Then we have

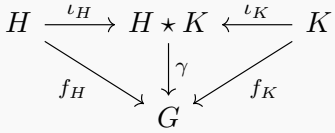
$$\mathbb{Z}_n \rtimes_\phi \mathbb{Z}_2 = \langle r, s \mid r^n = 1, s^2 = 1, srs = r^{-1} \rangle = D_n.$$

§3. Free product

The direct product is a natural construction. However, it is not the "freest" group containing the two initial groups. This is due to the commuting relations that appear in the presentation. This suggest the idea of a new construction which we call free product.

Definition III.2. *Let H, K, F be groups. We say that F is the free product of H and K if there are homomorphisms $\iota_H : H \to F$, $\iota_K : K \to F$ such that: for each group G and homomorphisms $f_H : H \to G$, $f_K : K \to G$ there exists a unique homomorphism $\gamma : F \to G$ such that $f_H = \gamma \circ \iota_H$ and $f_K = \gamma \circ \iota_K$.*

In this situation, we write $F = H \star K$. The following diagram summarizes the definition.



As usual, the universal property may not be very illustrative. However, it can be shown in a similar fashion that free products admit the following description in terms of generators and

relations.

Proposition III.3. *If $H = \langle X \mid R\rangle$, $K = \langle Y \mid S\rangle$, then*

$$H \star K = \langle X,\ Y \mid R,\ S\rangle.$$

How can we write the elements in this group? Every element can be written uniquely as an alternating expression of the form $h_1k_1 \dots h_mk_m$ with $h_i \neq 1$, $k_i \neq 1$ when present. Here uniqueness means

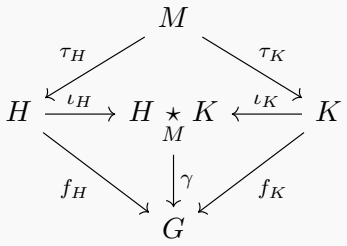
$$h_1k_1 \dots h_mk_m =_{H\star K} h'_1k'_1 \dots h'_nk'_n \quad \Longrightarrow \quad n = m,\ h_i =_H h'_i,\ k_i =_K k'_i.$$

§4. Free products with amalgamation

The following construction will be a generalization of the free product. Suppose M is a group isomorphic to subgroups of H and K, then we would like to construct a product where these subgroups are identified.

Definition III.3. *Let H, K, M, L be groups and $\tau_H : M \longrightarrow H$, $\tau_K : M \longrightarrow K$ be monomorphisms. We say that L is the* free product of H and K with amalgamated subgroup M *if there are homomorphisms $\iota_H : H \to L$, $\iota_K : L \to L$ satisfying $\iota_H \circ \tau_H = \iota_K \circ \tau_K$ such that: for each group G and homomorphisms $f_H : H \to G$, $f_K : K \to G$ satisfying $f_H \circ \tau_H = f_K \circ \tau_K$ there exists a unique homomorphism $\gamma : L \to G$ such that $f_H = \gamma \circ \iota_H$ and $f_K = \gamma \circ \iota_K$.*

In this situation, we write $L = H \underset{M}{\star} K$. The following diagram summarizes the definition.



Letting $A = \tau_H(M)$, $B = \tau_K(M)$ (the subgroups isomorphic to M), we can denote the product as $H \underset{A=B}{\star} K$. As usual, let's see a presentation for this new group.

Proposition III.4. *If $H = \langle X \mid R\rangle$, $K = \langle Y \mid S\rangle$, $M = \langle Z \mid T\rangle$ then*

$$H \underset{M}{\star} K = \langle X,\ Y \mid R,\ S,\ \tau_H(z) = \tau_K(z) \text{ for all } z \in Z\rangle.$$

Normal forms in these groups are not trivial at all. It is required to choose some particular transversals W, Z for the right cosets of A and B in H and K respectively. Then every product can be written uniquely as $ah_1k_1 \dots h_mk_m$, where $a \in A$, $h_i \in H$, $k_i \in K$.

Example III.4. *Consider the free groups $H = \langle a \mid \varnothing \rangle$, $K = \langle b \mid \varnothing \rangle$, $M = \langle c \mid \varnothing \rangle$ with the monomorphisms $\tau_H : M \longrightarrow H$, $\tau_K : M \longrightarrow K$ given by $\tau_H(c) = a^3$, $\tau_K(c) = b^2$. Then we have $A = \langle a^3 \rangle$, $B = \langle b^2 \rangle$.*

$$H \underset{A=B}{\star} K = \langle a, b \mid a^3 = b^2 \rangle.$$

Remark

Free products with amalgamation can be used to compute some fundamental groups. The Seifert-van Kampen theorem makes this idea concrete.

Theorem III.5 (Seifert-van Kampen). *Let X be a path connected topological space. Suppose $X = U_1 \cup U_2$, where U_1, U_2 are open, path connected sets such that $U_1 \cap U_2$ is open and path connected. Then the fundamental group $\pi_1(X)$ admits the following expression.*

$$\pi_1(X) = \pi_1(U_1) \underset{\pi_1(U_1 \cap U_2)}{\star} \pi_1(U_2).$$

§5. HNN extensions

We end this sequence of definitions with another common construction. The setting is the following: we have a group G with two subgroups A, B with an explicit isomorphism between them. We want to extend G so that the isomorphism becomes an *inner* automorphism. We will achieve this introducing a new letter and adding some relations.

Definition III.4. *Let $G = \langle X \mid R \rangle$ be a group with subgroups A, B such that there exists an isomorphism $\varphi : A \longrightarrow B$. The* HNN extension of G with respect to associated subgroups A and B *is the group denoted $G\star_\varphi$ and defined by*

$$G\star_\varphi = \langle X,\ p \mid R, p^{-1}ap = \varphi(a) \text{ for all } a \in A \rangle.$$

The new generator p is called the stable letter.

Many similarities arise between HNN extensions (named after G. Higman, B.H. Neumann, and H. Neumann) and free products with amalgamation. The main results about HNN extensions are consequences of a technical lemma known as Britton Lemma. In particular, it gives a normal form similar to those studied in free products with amalgamation (more details may be found on [3]).

§6. The structure of $\mathrm{SL}_2(\mathbb{Z})$

We end this chapter with a mention to Bass Serre theory. This theory aims to describe the structure of groups analyzing their action on trees. In particular, groups are described using iterated free products with amalgamation and HNN extensions.

As an example, we will describe the group $\mathrm{SL}_2(\mathbb{Z})$ finding a tree on which it acts to obtain the groups as a free product with amalgamation. To do so, we need a previous definition.

Definition III.5. *Let G be a group acting on a graph Γ. A* fundamental domain *for Γ mod G is a subgraph of Γ isomorphic to the quotient of Γ by the action of G.*

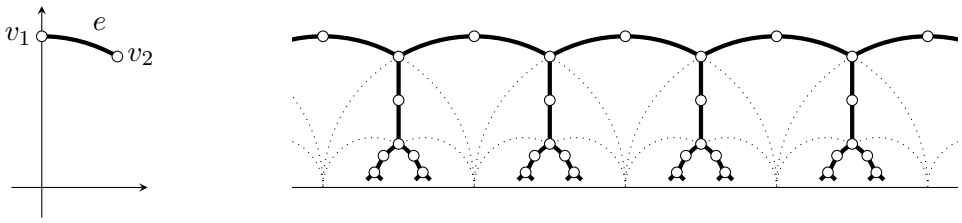
Recall that a segment is an edge and its two ends. Now we state the main result.

Proposition III.6. *Let G be a group acting on a tree Γ. Let a segment T in Γ be a fundamental domain for Γ mod G. Let G_1, G_2 and G_e be the stabilizers of the vertex and the edge of T respectively. Then $G \simeq G_1 \underset{G_e}{\star} G_2$.*

With this idea in mind, let $G = \mathrm{SL}_2(\mathbb{Z})$. It is well known that G acts on the upper half of the complex plane as follows:

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

Now consider the points $v_1 = e^{i\pi/2}$, $v_2 = e^{i\pi/3}$ and the arc e of the circle $|z| = 1$ between them. If we let T be this segment, we can construct a graph attaching all the translates of T under the action of G. Trivially T will be a fundamental domain and the graph turns out to be a tree.



(a) (b)

Figure III.1: Geometric realization of a tree out of a segment.

Now it is a simple exercise to compute the stabilizers of v_1, v_2 and the edge e, to find $G_1 = \mathbb{Z}_4$, $G_2 = \mathbb{Z}_6$ and $G_e = \mathbb{Z}_2$. This finally allows to obtain the structure of $\mathrm{SL}_2(\mathbb{Z})$ as a free product with amalgamation.

$$\mathrm{SL}_2(\mathbb{Z}) = \mathbb{Z}_4 \underset{\mathbb{Z}_2}{\star} \mathbb{Z}_6.$$

Chapter IV

Decision problems and applications to cryptography

This chapter will introduce the problems that led to the development of combinatorial group theory. In particular, we will focus our attention on the so-called decision problems. The history behind these problems leads us to algebraic topology, however we are mainly interested in the applications of these problems in cryptography.

§1. Decision Problems and undecidability

Essentially, a decision problem is to determine if a given object has a particular property. Max Dehn raised the three following decision problems about finitely presented groups.

Definition IV.1 (The word problem). *Let $G = \langle X \mid R \rangle$ be a finitely presented group. Is there an algorithm which decides whether or not a given word w respresents the identity in G?*

Definition IV.2 (The conjugacy problem). *Let $G = \langle X \mid R \rangle$ be a finitely presented group. Is there an algorithm which decides whether or not any pair of words u, v represent conjugate elements in G?*

Definition IV.3 (The isomorphism problem). *Is there an algorithm which decides whether or not any pair of finitely presented groups are isomorphic?*

These problems arose naturally in Dehn's work of fundamental groups. Is a given loop contractible? (word problem) are two given loops freely homotopic? (conjugacy problem) are two given surfaces

homeomorphic? (isomorphism problem) (homeomorphic surfaces have the same fundamental group, but the converse is not true).

Example IV.1. *Consider the quaternion group $Q = \langle i, j, k \mid i^2 = j^2 = k^2 = ijk \rangle$. It is well known that $i^4 = 1$, but this is not an immediate consequence of the presentation. An instance of the word problem is to determine whether or not $i^4 = 1$. The proof is ad-hoc: it is easy to check that $ij = k$ and $ki = j$, yielding $j = iji$. Now*

$$i^2 = j^2 = (iji)^2 = iji^2ji = ijj^2ji = ij^4i = i^6 \quad \Longrightarrow \quad i^4 = 1.$$

These problems fall into the domains of theory of algorithms and recursive functions. Thus, we will not be able to give all the details of the answers. However, we give some basic definitions.

Definition IV.4. *A set of objects is* recursive *is there is an algorithm for deciding membership in the set. Similarly, a set of objects is* recursively enumerable *if there is an algorithm for listing all the elements in the set.*

Clearly, a set S (living in some bigger set) is recursive if and only if S and its complement are recursively enumerable. Now we can formulate the word problem (for example) as follows.

The word problem. Let G be a finitely presented group. Is the set $\{w \in G \,|\, w =_G 1\}$ recursive?

In our finitely presented case, we can solve a part of the problem. The set $\{w \in G \mid w =_G 1\}$ is recursively enumerable, since we can list all the words corresponding to the identity writing products of relations, their conjugates and inverses. Thus, if we are given a word w such that $w =_G 1$, it will be eventually listed. However, if $w \neq_G 1$, we have a problem. There is no way to know if the word will appear later in our list or not, no matter how long we wait.

If we were able to list all the elements in $\{w \in G \mid w \neq_G 1\}$, the set $\{w \in G \mid w =_G 1\}$ would be recursive and the problem would be solved. However, there is no reason to make that assumption. If $\{w \in G \mid w =_G 1\}$ is not recursive, we say that the problem is undecidable.

Note that verifying $w = 1$ is equivalent to verifying if w is conjugate to 1. In particular, a group with undecidable word problem has undecidable conjugacy problem. The existence of such groups was shown by Nokivov and Boone in 1959.

Theorem IV.1 (Undecidability of the word and conjugacy problems). *There exists a finitely presented group whose word problem is undecidable. As a consequence, its conjugacy problem is undecidable.*

Which groups have a decidable word problem? A lot of research has been done to answer this question. There are many known properties that imply solvability of the word problem. For example, one relator groups, residually finite groups, nilpotent groups or metabelian groups have solvable word problem.

Remark

Once again, we are going to take advantage of the Cayley Graph to solve a problem about the group. As we know, to each word there corresponds a path in Cayley Graph, and this path is a cycle when the word is the identity. Thus, the following proposition is immediate.

Proposition IV.2. *A finitely presented group has solvable word problem if and only if we know a Cayley Graph.*

For the sake of completeness, we give a negative solution to the last problem.

Theorem IV.3 (Undecidability of the isomorphism problem). *The isomorphism problem for finitely presented groups is undecidable.*

This theorem is a consequence of a theorem by Adian and Rabin in 1958, which established that almost any property of finitely presented groups is undecidable.

§2. Applications to cryptography

In this section we outline the description of a couple of cryptographic schemes whose theoretical background relies on the concepts we have been dealing with. Recall that the most widely used protocols are based in the difficulty of solving mathematical problems, such as factorization of integers (*RSA*) or the "discrete log" problem (*ElGamal cryptosystem*).

A protocol based on the conjugacy search problem

Let G be a group with solvable word problem. From now on, we write w^a to denote the conjugation $a^{-1}wa$, where $w, a \in G$. The protocol is based on the following problem.

Conjugacy search problem. Given conjugate elements $v, w \in G$, find $a \in G$ such that $w^a = v$.

Note that this is not a decision problem, since we know that the elements are conjugate. Indeed, the problem is recursively solvable, since we can list all the elements conjugate to w until v appears. However, this approach in infeasible in practice, making this problem interesting from the complexity theory point of view. In fact, using a *search* variant of a well known decision problem is a quite common approach.

In the parlance of the field, we would say that the map $a \longmapsto w^a$ is a *one-way function*. As a consequence, we can build a cryptographic protocol based on conjugation. In particular, we explain now a key exchange protocol between Alice and Bob.

1. An element $w \in G$ is published.
2. Alice picks a private $a \in G$ and sends w^a to Bob.
3. Bob picks a private $b \in G$ and sends w^b to Alice.
4. Alice computes $(w^b)^a = w^{ba}$ and Bob computes $(w^a)^b = w^{ab}$.

This protocol is due to Ko, Lee, et. al. [7]. If a and b are chosen such that $ab = ba$, the two parties will have computed the same element $K = w^{ab} = w^{ba}$, so that they have a shared key. Note that this key can not be computed if one does not know either a or b. In addition, several questions arise, which groups should be used? How do we choose commuting elements? In [6] we can find some requirements the group G should satisfy. In particular, the creators of the protocol used *Braid groups*, which turn out to have some commuting subgroups.

A protocol based on the word problem

The following protocol is due to Shpilrain and Zapata. In this protocol, Alice decrypts with probability very close to 1 a binary sequence Bob has sent.

1. A pool of group presentations with efficiently solvable word problem is considered public.
2. Alice picks a group presentation Γ, modifies it by means of isomorphism-preserving transformations to get Γ' and eliminates some relations to get $\hat{\Gamma}$. The new presentation $\hat{\Gamma}$ is sent to Bob (and should be considered public).
3. Bob sends its binary sequence as follows. For each "1" in the sequence, he sends a word $w = 1$ in $\hat{\Gamma}$ and for each "0", he sends a long, random word w in $\hat{\Gamma}$.
4. Alice receives the words w and treats them as elements of Γ' (rather than $\hat{\Gamma}$), now applies the isomorphism to get back to the original presentation Γ, where she solves the word problem.

There are several points to be made regarding this protocol. For example, which groups can we take? We have mentioned several examples of group with solvable word problem, but the creators suggest to consider the so-called *small cancellation groups*. Secondly, how is Alice supposed to diffuse the presentation into another one? The answer is given by Tiezte transformations. In addition, Alice should take the initial presentation (with solvable word problem) to another one where the word problem is undecidable. Lastly, if $w = 1$ in $\hat{\Gamma}$, then the same is true in Γ'. However, if $w \neq 1$ in $\hat{\Gamma}$, we can say nothing about w in Γ'. This is why we say that Alice decrypts correctly with probability close to 1. The idea is to choose w long enough, so that (with overwhelming probability) w is not a product of relations, conjugates and their inverses in Γ'.

It is worth noting that one can not decrypt the sequence without knowledge of the original presentation Γ. This is true because decryption in $\hat{\Gamma}$ implies solving the word problem. A further analysis of the security may be found in [6].

Bibliography

[1] Derek Robinson. *A Course in the Theory of Groups*. Graduate Texts in Mathematics. Springer-Verlag New York.

[2] John Meier. *Groups, Graphs and Trees*. Cambridge University Press, 2008.

[3] Charles F. Miller III. *Combinatorial Group Theory*. 2004.

[4] Jean-Pierre Serre. *Trees*. Springer-Verlag Berlin Heidelberg, 1980.

[5] Gilbert Baumslag. *Topics in Combinatorial Group Theory*. Lectures in Mathematics. ETH Zürich. Birkhäuser Basel, 1993.

[6] Alexander Ushakov Alexei Myasnikov, Vladimir Shpilrain. *Group-based cryptography*. Advanced Courses in Mathematics - CRM Barcelona. Birkhäuser Basel, 2008.

[7] Jung Hee Cheon Jae Woo Han Ju-sung Kang Choonsik Park Ki Hyoung Ko, Sang Jin Lee. *New Public-Key Cryptosystem Using Braid Groups*. 2000.

[8] Schupp Paul E. Lyndon, Roger C. *Combinatorial Group Theory*. Classics in Mathematics. Springer-Verlag Berlin Heidelberg, 2001.

[9] D. L. Johnson. *Presentations of Groups*. Cambridge University Press, 1977.

[10] D. L. Johnson. *Topics in the Theory of Group Presentations*. Cambridge University Press, 1980.

[11] Donald Solitar Wilhelm Magnus, Abraham Karrass. *Combinatorial Group Theory: Presentations of Groups in Terms of Generators and Relations*. Dover Publications Inc, 2005.

[12] Clara Löh. *Geometric group theory, an introduction*. 2015.

[13] A. Raghuram & B. Sury. *Groups acting on trees*.

[14] Billy Wonderly. *Combinatorial Group Theory: An Introduction*. 2012.