An introduction to geometric group theory
Pristina

Matthieu Dussaule

Mars 2017

This is a eight hours course that I gave at the University of Pristina. It was addressed to students with different backgrounds and knowledge (second, third and fourth year). The goal of the class was first to convince students that group theory is nice, secondly that groups can be seen as geometric objects and thirdly that it is always a good idea to find a space on which a group acts to find out information about the group itself.

The first part is about general theory of groups. The second part is about defining group with a combinatorial approach. The third part is about the geometric theory.

Exercises are really important too. There are some in the text, but I also added my exercise sheets at the end of the notes.

There are a lot a books about geometric group theory. One I chose as a reference is [2]. It is really pedagogical and offers a lot of nice perspective. There are a lot of examples and a lot of exercises too. Actually, some of my exercises are taken from this book. Another reference is the first part of [4], also translated into english ([5]). In this one, the reader really understand, I think, that actions of groups on geometric spaces (such as trees) can be very interesting!

Contents

1 Elementary theory of groups

Before introducing groups as geometric objects, we first give some basic definitions. The word elementary does not mean that everything is trivial in this paragraph. It just means that the geometric approach is not yet tackled. However, one should find in here everything that is necessary to understand the remainder of these notes. Everything is covered in the two first chapters of [3].

1.1 Groups, subgroups

Definition 1.1.1. A group is a set G together with a binary operation $\star : G \times G \to G$ that satisfies the following:

1. $\forall a, b, c \in G, (a \star b) \star c = a \star (b \star c)$,
2. $\exists e \in G, \forall a \in G, a \star e = e \star a = a$,
3. $\forall a \in G, \exists a' \in G, a \star a' = a' \star a = e$.

The first property is called associativity. The element e is called the neutral element. Sometimes we shall refer to it as the unity or the identity. It is unique. The element a' in the third property is called the inverse of a. It is also unique. It shall be denoted by a^{-1}. The group is called **abelian** if for every a and b in G, $a \star b = b \star a$.

From now on, we shall denote the binary operation $\star$ with a multiplication symbol. For example, $a \star b$ shall be denoted ab. When the group is abelian, it is standard to use the symbol $+$.

Let's give some examples!

1. The set of real numbers $\mathbb{R}$ together with the addition $+$ is a group. The neutral element is 0 and the inverse of x is $-x$.
2. The set of non-zero real numbers $\mathbb{R}^*$ together with the multiplication $\times$ is a group. The neutral element is 1 and the inverse of x is $1/x$.
3. The subset $\mathbb{R}_+^*$ of $\mathbb{R}^*$ that consists of positive real numbers is also a group together with multiplication. It has the same neutral element and the inverse of x is still $1/x$.
4. The set of integers $\mathbb{Z}$ together with addition is a group. The neutral element is 0 and the inverse of x is $-x$.
5. Let n be a positive integer and let $\mathfrak{S}_n$ be the set of bijective maps from $\{1, ..., n\}$ onto $\{1, ..., n\}$. Together with the composition of functions, it is a group.
6. More generally, if X is any set, the set $\mathrm{Bij}(X)$ of bijective maps from X onto X is a group together with the composition of functions.
7. Let n be a positive integer and let $GL_n(\mathbb{R})$ be the set of invertible matrices of size n. Together with the multiplication of matrices, it is a group.

Definition 1.1.2. If G is a finite group, then its cardinal is called its **order**.

For example the group $\mathfrak{S}_n$ is of order $n!$.

Definition 1.1.3. Let G be a group and H be a subset of G. We say that H is a **subgroup** of G if

1. $e \in H$,
2. $\forall a, b \in H, ab \in H$,
3. $\forall a \in H, a^{-1} \in H$.

If H is a subgroup of G, then H together with the operation of G is itself a group. The fact that H is a subgroup of G shall be denoted by $H < G$. For example, $(\mathbb{Z}, +) < (\mathbb{R}, +)$ and $(\mathbb{R}_+^*, \times) < (\mathbb{R}^*, \times)$.

Definition 1.1.4. If X is a subset of a group G, the smallest subgroup of G containing X is called the **subgroup generated by** X. It is denoted by $\langle X \rangle$.

Proposition 1.1.5. *The subgroup generated by X always exists.*

Proof. Take $\langle X \rangle$ as the intersection of all subgroups of G containing X. Actually, check that the intersection of a family of subgroups is a subgroup. $\square$

A **generating set** for a group G is a set X such that $\langle X \rangle = G$.

Definition 1.1.6. The order of an element $x \in G$ is the order of $\langle x \rangle$.

Definition 1.1.7. A group is said to be cyclic if it is generated by one single element, meaning that there exists $x \in G$ such that $\langle x \rangle = G$.

If G is cyclic generated by x and if G is finite, then the order of x is the order of G.

1.2 Group morphisms

Definition 1.2.1. Let G and G' be two groups. A group morphism from G to G' is a map $f : G \to G'$ such that for every $a, b \in G$, $f(ab) = f(a)f(b)$. The image of f is the set $\mathrm{Im}(f) := \{x \in G', \exists y \in G, f(y) = x\}$. The kernel of f is the set $\mathrm{Ker}(f) := \{x \in G, f(x) = e\}$.

Proposition 1.2.2. *One always has* $\mathrm{Im}(f) < G'$, $\mathrm{Ker}(f) < G$.

This proposition is really easy to prove and the reader should do it as an exercise. Actually, it is worth noticing that $\mathrm{Im}(f) < G'$. It is not always the case in some theory that the image of a morphism (when it is defined) is a sub-object. To give full meaning to this remark, one should talk about category theory. We won't.

Proposition 1.2.3. *A group morphism f is one-to-one if and only if* $\mathrm{Ker}(f) = \{e\}$.

Let's give examples!

1. The determinant $\det : GL_n(\mathbb{R}) \to \mathbb{R}^*$ is a group morphism.
2. The exponential map $\exp : \mathbb{R} \to \mathbb{R}_+^*$ is a group morphism.
3. The logarithm map $\ln : \mathbb{R}_+^* \to \mathbb{R}$ is a group morphism.

Proposition 1.2.4. *If f is a bijective group morphism, then its inverse is also a group morphism.*

Proof. Let $f : G \to G'$ be a bijective group morphism and let $g : G' \to G$ be the inverse of f. Let $a, b \in G'$. Then there are $x, y \in G$ such that $f(x) = a$, $f(y) = b$, so that $g(ab) = g(f(x)f(y)) = g(f(xy))$ since f is a group morphism. Thus, $g(ab) = xy = g(a)g(b)$. $\square$

Definition 1.2.5. A **group isomorphism** is a group morphism $f : G \to G'$ that is bijective. If $G' = G$, then f is called a **group automorphism**.

If there exists an isomorphism $f : G \to G'$, we shall say that G and G' are isomorphic and we shall denote this fact by $G \simeq G'$.

1.3 Cosets, normal subgroups and quotient groups

Let G be a group and H be a subgroup of G. Say that $x \in G$ is equivalent to $y \in G$ if there exists $h \in H$ such that $x = yh$. This defines an equivalence relation on G. The equivalence classes are the sets $xH = \{xh, h \in H\}$. They are called **left cosets**.

Remark 1.3.1. One can also define right cosets by saying that $x \sim y$ if $x = hy$. The equivalence classes are then the sets Hx.

The quotient of G by this equivalence relation is denoted by G/H. It is the set $\{xH, x \in G\}$.

Remark 1.3.2. For right cosets, one should denote the quotient by $H\backslash G$.

The quotient map $x \in G \mapsto xH \in G/H$ is denoted by π_H, or just π.

Definition 1.3.3. The **index** of H in G is the cardinal of G/H. It is denoted by $[G : H]$.

Example 1.3.4. Let $(\mathbb{Z}, +)$ be the group of integers. For $n \in \mathbb{Z}$, let $n\mathbb{Z}$ be the set $\{nk, k \in \mathbb{Z}\}$. Then, $n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$ (actually, every subgroup of $\mathbb{Z}$ is of that form). The quotient $\mathbb{Z}/n\mathbb{Z}$ is called the set of **integers modulo** n. It is of cardinal $|n|$. In other words, $n\mathbb{Z}$ is of index $|n|$ in $\mathbb{Z}$.

Proposition 1.3.5. *If G is finite, then all the cosets xH have the same cardinal.*

Proof. Let $x \in G$. Then, the map $h \in H \mapsto xh \in xH$ is bijective. In particular, the cardinal of xH is the cardinal of H. □

Corollary 1.3.6. *If G is finite, then* $\mathrm{Card}(G) = \mathrm{Card}(H)[G : H]$. *In particular, the order of H divides the order of G.*

This corollary is often referred as the Lagrange theorem.

Corollary 1.3.7. *If G is finite and if $x \in G$, then the order of x divides the order of G.*

Definition 1.3.8. If G is a group and H is a subgroup of G, then H is said to be normal in G if for every $x \in G$, $xH = Hx$ or equivalently, if $xHx^{-1} = H$.

The fact that H is a subgroup of G shall be denoted by $H \lhd G$.

Exercise 1.3.9.

1. If G is abelian, then all is subgroups are normal.
2. Let $SL_n(\mathbb{R})$ be the subgroup of $GL_n(\mathbb{R})$ that consists of invertible matrices of determinant 1. Then $SL_n(\mathbb{R}) \lhd GL_n(\mathbb{R})$.
3. More generally, if $f : G \to G'$ is a group morphism, then $\mathrm{Ker}(f) \lhd G$.

Theorem 1.3.10. *Let G be a group and H be a subgroup of G. There exists a group structure on G/H such that the quotient map π_H is a group morphism if and only if H is normal in G. In that case, the group structure on G/H is unique and the kernel of π_H is H.*

Proof. If such a group structure does exist, then the neutral element of G/H is $\pi_H(e) = eH = H$. Since $aH = H$ if and only if $a \in H$, one has $\mathrm{Ker}(\pi_H) = H$. Thus, H is normal in G (using the exercise above). Furthermore, $aHbH = \pi_H(a)\pi_H(b) = \pi_H(ab) = abH$ so that the group structure is unique.

Conversely, if H is normal, define $aHbH = abH$. This definition does not depend on the choices of a and b. Indeed, if $aH = a'H$ and $bH = b'H$, then $abH = aHb = a'Hb = a'bH = a'b'H$. This operation is associative, because of associativity in G and $aHH = aH = HaH$, so that H is neutral. Finally, $aHa^{-1}H = aa^{-1}H = H$ and the same works with $a^{-1}HaH$, so that every coset aH has an inverse, namely $a^{-1}H$. Therefore, G/H together with this operation is a group and for that structure, π_H is a group morphism. □

Remark 1.3.11. Every normal subgroup is then the kernel of some group morphism.

The following theorem is called the first isomorphism theorem (see chapter 2 of [3] for the second and the third ones). We shall use it a lot in the following.

Theorem 1.3.12. *Let G, G' be two groups and $H \lhd G$. Let $f : G \to G'$ be a group morphism. There exists a group morphism $\tilde{f} : G/H \to G'$ such that $f = \tilde{f} \circ \pi_H$ if and only if $H <$* $\mathrm{Ker}(f)$. *In that case, $\tilde{f}$ is unique.*

This property is often summarised with the following diagram.

$$\begin{tikzcd} G \arrow[r, "f"] \arrow[d, "\pi_H"'] & G' \\ G/H \arrow[ur, dashed, "\tilde{f}"'] & \end{tikzcd}$$

Proof. If $\tilde{f}$ does exist, then $\tilde{f}(xH) = f(x)$ so that is is entirely determined by f. Therefore, it is unique. Furthermore, if $h \in H$, then $\tilde{f}(hH) = f(h) = \tilde{f}(H) = f(e) = e'$, so that $H < \mathrm{Ker}(f)$.

Conversely, if $H < \mathrm{Ker}(f)$, define $\tilde{f}(xH) = f(x)$. It does not depend on the choice of x. Indeed, if $xH = x'H$, then $x = x'h$ for some $h \in H$ and thus $f(x) = f(x')f(h) = f(x')$. □

Corollary 1.3.13. *Let $f : G \to G'$ be a group morphism, then $G/\mathrm{Ker}(f) \simeq \mathrm{Im}(f)$.*

For example, $GL_n(\mathbb{R})/SL_n(\mathbb{R}) \simeq \mathbb{R}^*$.

Remark 1.3.14. One has now enough material to ask oneself some easily formulated questions with non-trivial answers. As an example, if $H \lhd G$ and if $G/H \simeq \{0\}$, then $G = H$. Conversely, if $G/H \simeq G$, is H trivial, meaning $H = \{0\}$? In general, no! Take G to be the circle $\mathbb{S}^1$ and H to be the subgroup $\{1, -1\}$ of G. Then G/H is isomorphic to $\mathbb{S}^1$. Is the answer true if G is finitely generated, meaning that there exists some finite set S such that $\langle S \rangle = G$? The answer still is no. An example is the Baumslag-Solitar group $BS(1, 2)$.

Actually, those groups such that for every $H \lhd G$ such that $G/H \simeq G$, $H = \{0\}$ have a name, they are called Hopfian groups It is equivalent to assume that every group morphism $f : G \to G$ that is onto is also one-to-one. In fact, Gilbert Baumslag and Donald Solitar considered the group $BS(1, 2)$ to show that there were non-Hopfian finitely generated groups.

1.4 Group actions

The geometric approach to group theory is all about group actions on geometric spaces. Let's give some vocabulary and basic properties about those.

Definition 1.4.1. Let G be a group and X be a set. A group action of G on X is a map $f : G \times X \to X$ such that

1. $\forall x \in X, f(e, x) = x$,
2. $\forall g, h \in G, \forall x \in X, f(g, f(h, x)) = f(gh, x)$.

We shall denote the image of (g, x) by $g \cdot x$. The properties are then

1. $\forall x \in X, e \cdot x = x$,
2. $\forall g, h \in G, \forall x \in X, g \cdot (h \cdot x) = (gh) \cdot x$.

The fact that G acts on X shall be denoted by $G \curvearrowright X$.

If $g \in G$, then the map $x \in X \mapsto g \cdot x \in X$ is a bijection of X. Indeed, one has an explicit inverse given by $x \mapsto g^{-1} \cdot x$. Denote this map by $\phi(g)$. Then $g \mapsto \phi(g)$ is a group morphism from G to $\mathrm{Bij}(X)$.

Proof. For $x \in X$ and $g, h \in G$, $\phi(gh)(x) = (gh) \cdot x = g \cdot (h \cdot x) = \phi(g)(\phi(h)(x))$, so that $\phi(gh) = \phi(g) \circ \phi(h)$. □

Conversely, if $\phi : G \to \mathrm{Bij}(X)$ is a group morphism, define $g \cdot x = \phi(g)(x)$. It is a group action of G on X. Thus, a group action is nothing else that a group morphism from G to some group $\mathrm{Bij}(X)$.

Remark 1.4.2. We shall see later that if X has geometric properties (for example X is a metric space), we shall require that the action preserves those properties, meaning that the group morphism $G \to \mathrm{Bij}(X)$ has its image in some subgroup of $\mathrm{Bij}(X)$ (for example the group of isometries of X).

Definition 1.4.3. A group action $G \curvearrowright X$ is called faithful if the morphism $G \to \mathrm{Bij}(X)$ is one-to-one. In other words, if $g \in G$ and if for every x, $g \cdot x = x$, then $g = e$.

Everything in this notes will be up-to isomorphism. Then, if one has a faithful action $G \curvearrowright X$, one can see G as a subgroup of $\mathrm{Bij}(X)$.

Definition 1.4.4. A group action $G \curvearrowright X$ is called free if for every $g \neq e$, for every $x \in X$, $g \cdot x \neq x$. In other words, every element different from the neutral element moves every point. A free action is in particular faithful.

Let's give some examples!

1. If G is a group, then G acts on itself by left translation: $g \cdot h = gh$. This action is free and hence, it is faithful. Therefore we can see G a subgroup of $\mathrm{Bij}(G)$.

   Corollary 1.4.5. *If G is finite, then there exists n such that $G < \mathfrak{S}_n$.*

   Proof. Let n be the order of G, so that $\mathrm{Bij}(G) \simeq \mathfrak{S}_n$. Since G acts faithfully on itself, $G < \mathfrak{S}_n$. □

2. A group G also acts on itself by conjugacy: $g \cdot h = g^{-1}hg$. This action is not faithful in general. For example, if G is abelian, the action is trivial.

3. If $H \lhd G$, then G also acts by left translation on G/H: $g \cdot xH = gxH$.

4. The group $GL_n(\mathbb{R})$ acts linearly on $\mathbb{R}^n$. It also acts on the set $\mathbb{P}(\mathbb{R}^n)$ of straight lines of $\mathbb{R}^n$ (that goes through 0). More generally, let $\mathcal{G}_{n,k}$ be the set of k-dimensional vector-subspaces of $\mathbb{R}^n$. Then $GL_n(\mathbb{R}^n)$ acts on $\mathcal{G}_{n,k}$.

Definition 1.4.6. Let G be a group, X a set, and assume that G acts on X. If $x \in X$, the **orbit** of x is the set $\omega(x) := \{g \cdot x, g \in G\}$. The **stabiliser** of x is the set $\mathrm{Stab}(x) := \{g \in G, g \cdot x = x\}$.

The orbit of x is a subset of X, the stabiliser of x is a subset of G. Actually, the stabiliser of x is a subgroup of G.

Proof. By definition, $e \cdot x = x$. If $g, h \in \mathrm{Stab}(x)$, then $gh \cdot x = g \cdot (h \cdot x) = g \cdot x = x$ and $g^{-1} \cdot x = g^{-1} \cdot (g \cdot x) = x$. □

If G acts on X, say that $x, y \in X$ are equivalent if there exists $g \in G$ such that $g \cdot x = y$. It is an equivalence relation. The equivalence classes are the orbits.

The following is a generalisation of proposition 1.3.5. The map $g\mathrm{Stab}(x) \in G/\mathrm{Stab}(x) \mapsto g \cdot x \in \omega(x)$ is well defined and is a bijection. Then, the cardinal of $\omega(x)$ is the index of $\mathrm{Stab}(x)$ in G.

In particular, if X is finite, then $\omega(x)$ is finite and therefore, $\mathrm{Stab}(x)$ is of finite index in G. If G is also finite, then $\mathrm{Card}(G) = \mathrm{Card}(\omega(x))\mathrm{Card}(\mathrm{Stab}(x))$.

Theorem 1.4.7 (The class formula)**.** *If X is finite, then denote by Ω the set of all orbits and choose one x in each $\omega \in \Omega$. Denote this set of such x by $\tilde{X}$. Then,*

$$\mathrm{Card}(X) = \sum_{x \in \tilde{X}} [G : \mathrm{Stab}(x)].$$

This theorem can be really useful. It establishes a link between the knowledge of G and its subgroups and the knowledge of X. It often allows one to understand G via its action on X. The exercise below is an illustration of this. Actually, in the following, one should keep in mind this guidind principle: Understanding a group G is understanding how it acts.

Exercise 1.4.8. Let G be a finite group and let p be a prime number such that p divides $|G|$. We are going to prove that there exists in G some element g of order exactly p: $g^p = e$ and $g^k \neq e$, if $k \leqslant p - 1$.

1. Denote by X the set $\{(g_1, ..., g_p) \in G^p, g_1 ... g_p = e\}$. Show that $|X| = |G|^{p-1}$. Thus, p divides $|X|$.

2. Show that $j \cdot (g_1, ..., g_p) := (g_{1+j}, ..., g_{p+j})$ defines a group action of $\mathbb{Z}/p\mathbb{Z}$ on X.

3. Show that the set $X^{\mathbb{Z}/p\mathbb{Z}}$ of elements $x \in X$ fixed by every element of $\mathbb{Z}/p\mathbb{Z}$ (that is $x \in X^{\mathbb{Z}/p\mathbb{Z}}$ if $\forall j \in \mathbb{Z}/p\mathbb{Z}, j \cdot x = x$) is the set $\{(x, ..., x) \in G^p, x = e$ or x is of order $p\}$. Conclude.

2 Group presentations

Before getting into the true geometric part of geometric group theory, let's give a look at the combinatorial approach. The basic idea is that one can find out everything about a group thanks to a set of generators and their relations. Relations are roughly speaking the simplifications of words written in those generators. For example, in an abelian group, the word aba^{-1} can be simplified into the word b. Therefore, one has the relation $aba^{-1} = b$, better written (as we shall see) as $aba^{-1}b^{-1} = e$.

2.1 Free groups

The cornerstone on which is built the presentation theory is the concept of free groups. We have not yet properly introduced what relations are, but one can understand free groups as groups with no relations (except trivial ones such as $aa^{-1} = e$).

Let S be any set. One has to think of S as a generating set of some group G, not yet defined. Define S^{-1} to be a disjoint copy of S, meaning that there is a bijective map $s \in S \mapsto s^{-1} \in S^{-1}$. Define some element e such that $e \notin S, e \notin S^{-1}$. Elements of S^{-1} should be seen as formal inverses of elements of S in G and e should be seen as the neutral element of G. Also define $\tilde{S} := S \sqcup S^{-1} \sqcup \{e\}$.

Definition 2.1.1. A **word** in $\tilde{S}$ is a finite sequence of elements of $\tilde{S}$. Such a word shall be written $w = s_1^{\epsilon_1}...s_n^{\epsilon_n}$, where $s_i \in S$ and $\epsilon_i = \pm 1$ (s_i^{-1} is actually the image of s_i by the map $s \mapsto s^{-1}$) OR $s_i = e$ and $\epsilon_i = 0$.

A formal power of an element of S is an element of S together with a positive integer n. Such a formal power shall be denoted by s^n. A formal power of an element of S^{-1} is an element of S^{-1} together with a positive integer n. It shall be denoted by s^{-n}. A formal power of an element of $\tilde{S}$ either is e or is a formal power of an element of S or of S^{-1}. We shall identify a power (s^{-1}, n), $n \geqslant 1$ with $(s, -n)$. Therefore, one can see a formal power of an element of $\tilde{S}$ (that is not e) as an element of S together with a non-zero integer.

Definition 2.1.2. A **reduced word** in $\tilde{S}$ is a finite sequence of powers of elements of $\tilde{S}$ $w = s_1^{\alpha_1}...s_n^{\alpha_n}$ where $s_i \in S$, $\alpha_i \in \mathbb{Z}\backslash\{0\}$ and $s_i \neq s_{i+1}$ OR $w = e$. Denote the set of reduced words in $\tilde{S}$ by $W(S)$.

A reduced word should be thought of as an element of a group G written with elements of a generating set S with all trivial simplifications: eliminating the neutral element every time it appears and eliminating the elements ss^{-1}.

Let's now give some meaning to that informal explanation. Let G be a group and let S be a generating set. **In the following, to simplify notations, we shall always assume that** $S \cap S^{-1} = \varnothing$. Define the map

$$\begin{array}{rccc} \Phi : & W(S) & \to & G \\ & w = s_1^{\alpha_1}...s_n^{\alpha_n} & \mapsto & s_1^{\alpha_1}...s_n^{\alpha_n} \end{array}$$

where the element $s_1^{\alpha_1}...s_n^{\alpha_n}$ in G is just the multiplication of elements of S and inverses of elements of S. The map Φ is onto, since S is a generating set.

Definition 2.1.3. A **free group** is a group G together with a generating set S such that the map Φ is one-to-one. We say that S is a **free basis** of G.

Theorem 2.1.4. *Let S be a set. There exists a unique (up to isomorphism) free group of free basis S. It is (abusively) denoted by $F(S)$. Furthermore, if S and S' are in bijection, then $F(S)$ is isomorphic to $F(S')$. If S is finite, of cardinal n, then $F(S)$ shall (again, abusively) be denoted by F_n.*

One can see S as a subset of $W(S)$. Since the map Φ is one-to-one, its restriction to S is also one-to-one. This restriction shall be denoted by $\Phi_S : S \hookrightarrow F(S)$.

Proof. To prove this theorem, one should take $F(S)$ as the set of reduced words $W(S)$ and define an operation as follows. If w_1 and w_2 are two reduced words, first define $\overline{w_1 w_2}$ to be the concatenation of the words w_1 and w_2. If the last letter of w_1 is the same as the first letter of w_2, then simplify $\overline{w_1 w_2}$ by eliminating those and keep on doing that until the word is reduced. Define $w_1 w_2$ to be this reduced word. To actually show that

this operation exists and defines a group structure on $W(S)$ is rather long and fastidious. We shall use a trick, often called the van der Waerden trick.

Let G be the group $\mathfrak{S}(W(S))$, that is the group of bijective maps $W(S) \to W(S)$. We shall define $F(S)$ as a subgroup of G. Let $w = s_1^{\alpha_1}...s_n^{\alpha_n} \in W(S)$. We say that w starts with $s \in S$ if $s_1 = s$ and $\alpha_1 > 0$. In that case, we write $w = sw'$ where $w' = s_1^{\alpha_1 - 1}...s_n^{\alpha_n}$ if $\alpha_1 > 1$ and $w' = s_2^{\alpha_2}...s_n^{\alpha_n}$ otherwise. Similarly, we say that w starts with $s^{-1} \in S^{-1}$ if $s_1 = s$ and $\alpha_1 < 0$. In that case we write $w = s^{-1}w'$.

If $s \in S$, define $\sigma(s)(w) = sw$ if w does not start with s and $\sigma(s)(w) = w'$ if w starts with s and $w = sw'$. In both cases, $\sigma(s)(w)$ is a reduced word. If $s^{-1} \in S^{-1}$, define $\sigma(s^{-1})(w) = s^{-1}w$ if w does not start with s^{-1} and $\sigma(s^{-1})(w) = w'$ if w starts with s^{-1} and $w = s^{-1}w'$. By definition, $\sigma(s) \circ \sigma(s^{-1}) = \sigma(s^{-1}) \circ \sigma(s) = Id$ so that $\sigma(s), \sigma(s^{-1}) \in G$. Moreover, the map $\sigma : S \to G$ is one-to-one and we shall now identify S with $\sigma(S)$. Let $F(S)$ be the subgroup of G generated by S.

Let's show that $F(S)$ is free of free basis S. Let $w = s_1^{\alpha_1}...s_n^{\alpha_n}$ be a reduced words in $\tilde{S}$ and $\Phi(s_1^{\alpha_1}...s_n^{\alpha_n}) = g$ be its image in $F(S)$. Assume that $w \neq e$ and prove that $g \neq Id \in F(S)$. In fact, since $g \in \mathfrak{S}(W(S))$, we can evaluate g on e, seeing e as an element of $W(S)$. A simple induction on $|\alpha_1| + ... + |\alpha_n|$ shows that $g(e) = w$ Since $w \neq e$, $g \neq Id$.

This concludes the existence part of the theorem. For uniqueness, assume that G and G' are free of free basis S. Then there are bijective maps $\Phi : W(S) \to G$ and $\Phi' : W(S) \to G'$. The map $\Phi^{-1} \circ \Phi'$ is in fact a group morphism from G' to G. Since it is bijective, it is an isomorphism.

Finally, if S and S' are in bijection, then so are $W(S)$ and $W(S')$, so that a reduced word in $\tilde{S}$ is a reduced word in $\tilde{S'}$. Since all we did was defined up to bijective maps, $F(S)$ and $F(S')$ are isomorphic. □

A powerful tool for proving that some group G is a free group is the ping-pong lemma.

Theorem 2.1.5 (Ping-pong lemma)**.** *Let G be a group acting on a set X. Let S be a generating set of G. Assume that there are non-empty disjoint sets $(X_s)_{s \in S}$ such that*

$$\forall s, t \in S, s \neq t, \forall n \in \mathbb{Z}^*, s^n X_t \subset X_s.$$

Then, the group G is free with free basis S: $G \simeq F(S)$.

We leave the proof as an exercise.

Exercise 2.1.6. To prove the ping-pong lemma, take $g = s_1^{\alpha_1}...s_n^{\alpha_n} \in G$. Assume that g is reduced. It only has to be shown that $g \neq e$. There are two cases. Either $s_n = s_1$ or $s_n \neq s_1$.

1. Assume that $s_1 = s_n = s$. Denote by $Y_s = \bigcup_{t \neq s} X_t$. Show that if $x_0 \in Y_s$, then $g \cdot x_0 \in X_s$. Deduce that $g \neq e$.

2. Assume that $s_1 = s \neq t = s_n$ Show that there exists $x \in G$ such that $x \neq s_1^{-\alpha_1}$ and $x^{-1} \neq s_n^{-\alpha_n}$ By considering xgx^{-1}, show that $g \neq e$.

2.2 A universal property

The following theorem can be used as an alternative definition for $F(S)$.

Theorem 2.2.1. *Let S be a set and $F(S)$ be a free group of free basis S. Let G be a group and let $f : S \to G$ be a map. Then, there exists a unique group morphism $\tilde{f} : F(S) \to G$ such that $\tilde{f} \circ \Phi_s = f$ (recall that Φ_S is the restriction to S of the map $\Phi : W(S) \to F(S)$).*

This theorem can be summarised with the following diagram.

$$\begin{tikzcd} S \arrow[rr, "f"] \arrow[dr, "\Phi_S"'] & & G \\ & F(S) \arrow[ur, dashed, "\tilde{f}"'] & \end{tikzcd}$$

Proof. If $\tilde{f} \circ \Phi_S = f$, then $\tilde{f}(w) = \tilde{f}(s_1^{\alpha_1}...s_n^{\alpha_n}) = \tilde{f}(s_1)^{\alpha_1}...\tilde{f}(s_n)^{\alpha_n} = f(s_1)^{\alpha_1}...f(s_n)^{\alpha_n}$, so that $\tilde{f}$ is uniquely determined by f. Conversely, since $\Phi : W(S) \to F(S)$ is a bijective map, this formula defines $\tilde{f}$. It is well defined because $F(S)$ is free and it is a group morphism. □

Such a property is called a universal property in the category language, and $F(S)$ is called a universal object, since it satisfies a universal property. Be careful! A universal property is NOT a definition. In general, one has to show that a universal object DOES exist. It is not always an easy thing to do.

The converse of this theorem is true.

Theorem 2.2.2. *Let F be a group and $\varphi_S : S \to F$ a map such that for every group G and for every map $f : S \to G$, there exists a unique group morphism $\tilde{f} : F \to G$ such that $\tilde{f} \circ \varphi_S = f$. Then, $F(S)$ is isomorphic to F.*

Proof. First use the universal property with $F(S)$: there exists a (unique) group morphism $f_1 : F(S) \to F$ such that $f_1 \circ \Phi_S = \varphi_S$. Then, use it with F: there exists a (unique) group morphism $f_2 : F \to F(S)$ such that $f_2 \circ \varphi_S = \Phi_S$. Thus, the morphism $g = f_1 \circ f_2 : F \to F$ satisfies $g \circ \varphi_S = \varphi_S$. That means that it is a solution of the universal property applied to F onto F itself. However, the identity also satisfies this universal property. By uniqueness, one finds that $f_1 \circ f_2 = Id$. Similarly $f_2 \circ f_1$, so that f_1 and f_2 are isomorphisms. □

Remark 2.2.3. Actually, we proved that the isomorphism $F(S) \to F$ is unique (since f_1 and f_2 are unique).

Let G be a group and S be a generating set. Then, the inclusion is a map $S \to G$. Therefore, one deduces from the universal property that there exists a group morphism $\pi_S : F(S) \to G$ such that $\pi_S(s) = s$. Since S is a generating set, π_S is onto, so that, by the first isomorphism theorem,

$$F(S)/\mathrm{Ker}(\pi_S) \simeq G.$$

Conclusion: every group is the quotient of some free group!

2.3 Presentations: generating sets and relations

Definition 2.3.1. Let G be a group and let H be a subgroup of G. The **subgroup normally generated by** H is the smallest subgroup of G containing H. It is denoted by $\langle\langle H \rangle\rangle$.

Exercise 2.3.2. The subgroup normally generated by H is the set of elements of G of the form $g_1 h_1 g_1^{-1} ... g_n h_n g_n^{-1}$, with $g_i \in G$ and $h_i \in H$.

Definition 2.3.3. If G is a group and X is any subset of G, then the **subgroup normally generated by** X is the subgroup normally generated by $\langle X \rangle$. It is denoted by $\langle\langle X \rangle\rangle$.

Let G be a group and let S be a generating set. Then, there exists a group morphism $\pi_S : F(S) \to G$ and $G \simeq F(S)/\mathrm{Ker}(\pi_S)$.

Definition 2.3.4. A **relation** is an element of $\mathrm{Ker}(\pi_S)$. A system of relations is a set $R \subset \mathrm{Ker}(\pi_S)$ such that $\langle\langle R \rangle\rangle = \mathrm{Ker}(\pi_S)$.

If R is a system of relations, then G is entirely determined by S and R up to isomorphism, since G is isomorphic to $F(S)/\langle\langle R \rangle\rangle$. We shall denote this fact by $G \simeq \langle S | R \rangle$. Such a writing is called a **presentation** of G.

Let's give examples (actually, exercises)!

1. The group of integers $\mathbb{Z}$ is generated by one element. Actually, it is free of free basis this element. Therefore, $\mathbb{Z} \simeq \langle x | \varnothing \rangle$.

2. More generally, $F(S) \simeq \langle S | \varnothing \rangle$.

3. The group $\mathbb{Z}^2$ has the presentation $\langle x, y | xyx^{-1}y^{-1} \rangle$.

4. The group $\mathfrak{S}_n$ has the presentation $\langle x_1, ..., x_n | x_i^2, x_i x_j x_i^{-1} x_j^{-1} (|j-i| \geqslant 2), x_i x_{i+1} x_i x_{i+1}^{-1} x_i^{-1} x_{i+1}^{-1} \rangle$.

Sometimes, it is easier to write elements of R as equalities. For example, one can write $xy = yx$ instead of $xyx^{-1}y^{-1}$ in the presentation of $\mathbb{Z}^2$.

Conversely, let S be any set and R any subset of $F(S)$. Define $\langle S|R \rangle$ to be $F(S)/\langle\langle R \rangle\rangle$.

Of course, a same group can have as many presentation as one wants. For instance, it suffices to add a generator s and to add the relation $s = e$, or more generally $s = g$, for any $g \in G$. Actually, given two presentations $\langle S_1|R_1 \rangle$, $\langle S_2|R_2 \rangle$, asking if the two groups are isomorphic is a really difficult question to answer. Another difficult question is whether some group has a finite presentation (meaning that S and R are both finite).

This approach to group theory gave birth to what is called combinatorial group theory. It was initiated by Walther Dyck (who invented free groups in 1882). A good reference for combinatorial group theory is [1]. It is not what those notes are about, but in some sense, it leads to a geometric theory that we shall now explore.

3 Cayley graphs

We saw that a group can be defined with a set of generators and relations between those. From that, we shall introduce some geometric object, namely the Cayley graph of a group. Basically, the idea is to draw the presentation $\langle S|R \rangle$ by connecting vertices with generators and adding relations to connect vertices. It shall be made precise in a few moment. First, we shall give some general definitions about graph theory.

3.1 Graphs and trees

We only need some naive graph theory in the following. Nevertheless, to do things properly, we introduce here some vocabulary.

Definition 3.1.1. A **graph** is a set V of vertices together with a set $E \subset V \times V$ of edges such that if $(v_0, v_1) \in E$, then $(v_1, v_0) \in E$. In that case, we say that v_0 and v_1 are connected by an edge and that v_1 is a neighbour of v_0.

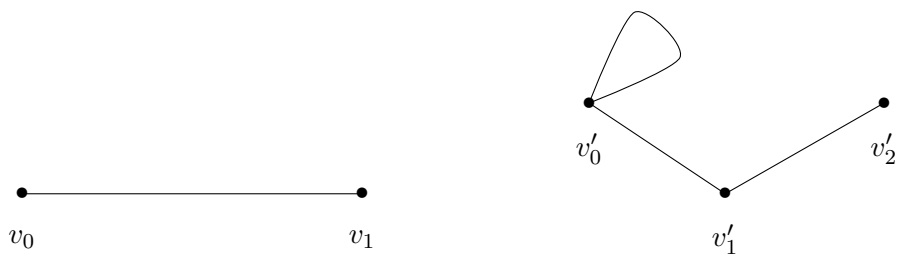
Remark 3.1.2. We made a choice here of doubling every edge. It is not always the case in literature and one could define graphs without requiring that $(v_0, v_1) \in E$ if and only if $(v_1, v_0) \in E$. However, it shall be useful in the following.

In this definition, it seems that our graphs are non-oriented. It is not true! Defining edges like that, one can orient them as follows.

Definition 3.1.3. If $e = (v_1, v_2) \in E$, define $\partial_0(e) = v_0$ and $\partial_1(e) = v_1$ and define $\overline{e} = (v_1, v_0)$. Call $\partial_0(e)$ the origin of e and $\partial_1(e)$ its end.

Thus, we do deal with oriented graphs, but require that every edge is doubled, for later purpose. It is actually really important to deal with oriented graphs, as we shall see.

For example, the first graph below can be defined as $V = \{v_0, v_1\}$ and $E = \{(v_0, v_1), (v_1, v_0)\}$. The second one can be defined as $V' = \{v'_0, v'_1, v'_2\}$ and $E' = \{(v'_0, v'_0), (v'_0, v'_1), (v'_1, v'_0), (v'_1, v'_2), (v'_2, v'_1)\}$. Actually, we did not draw every edge in the figure, for simplicity. We just put one edge between two vertices (that are connected by an edge). We shall do the same every time we draw graphs. However, **as an abstract graph**, every edge is doubled.



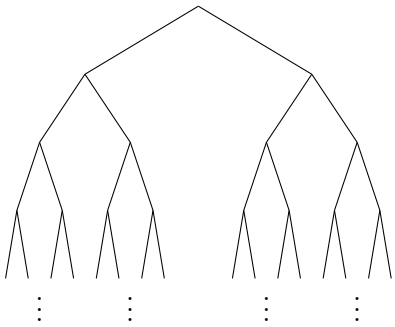
Definition 3.1.4. We say that two vertices v, v' are connected if there exists a finite sequence of vertices $(v_0 = v, v_1, ..., v_n = v')$ such that $(v_i, v_{i+1}) \in E$. We say that the graph is connected if every two vertices are connected.

Definition 3.1.5. A **loop** is a finite sequence of vertices $(v_0, ..., v_n)$ such that $v_0 = v_n$, $(v_i, v_{i+1}) \in E$ and $v_i \neq v_{i+2}$ (meaning that there is no back-tracking).

Definition 3.1.6. A **tree** is a connected graph without a loop.

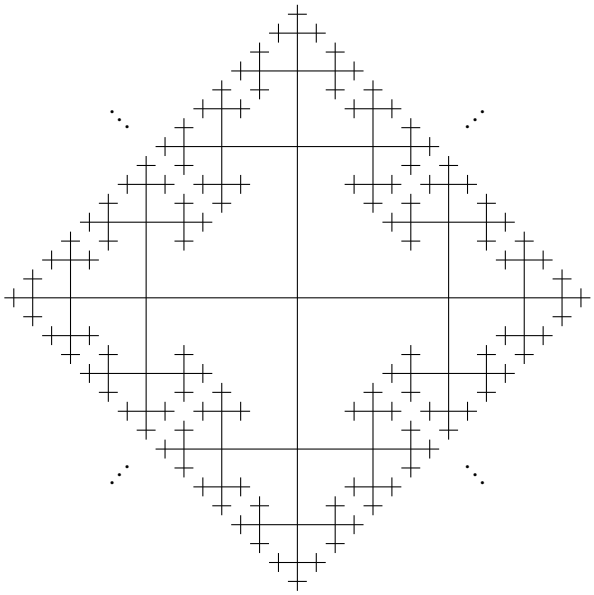
Let's give examples!

1. The n-ary rooted tree is an infinite tree. Every vertex has $n+1$ neighbours except for one vertex that has n neighbours and that is called the root. Here is a representation of the binary tree.

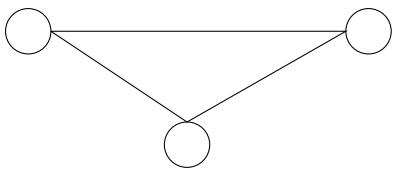


   It contains an infinite number of copies of itself, and has very rich symmetry.

2. The n-ary regular tree is also an infinite tree. Every vertex has exactly n neighbours. It is denoted by $\mathbb{T}_n$. Here is a representation of $\mathbb{T}_4$.



3. A complete graph is a graph (V, E) such that every two vertices are connected by an edge. It can never be a tree. Here is a complete graph with three vertices.



We defined the structure of graph. Let's define morphisms that preserve this structure.

Definition 3.1.7. A **graph morphism** between two graphs (V, E) and (V', E') is a map $f : V \to V'$ such that if v_0 and v_1 are connected by an edge in V, then $f(v_0)$ and $f(v_1)$ are connected by an edge in V'.

A **graph isomorphism** is a graph morphism that is bijective. In that case the inverse of the map is also a graph morphism. A **graph automorphism** is a graph isomorphism from one graph to itself.

Definition 3.1.8. Let (V, E) be a graph and let G be a group that acts on V. The action of V is called a **graph action** if whenever v and v' are connected by an edge, for every $g \in G$, $g \cdot v$ and $g \cdot v'$ are also connected by an edge. In other words, the bijective map $v \mapsto g \cdot v$ is a graph automorphism for every $g \in G$.

3.2 Cayley graphs of a group

When we defined the free group $F(S)$ for some generating set S, we required that S and S^{-1} were disjoint sets, for simplicity. In the following, we shall deal with generating sets of pre-existing groups. Such an assumption is then impossible: for example, if $s \in S$ is of order 2, then $s = s^{-1}$. We slightly change our hypothesis and require that $S = S^{-1}$, meaning that if $s \in S \subset G$, then $s^{-1} \in S$. We say that the generating set S is **symmetric**. We then work with S directly instead of $\tilde{S} = S \cup S^{-1}$.

Definition 3.2.1. Let G be a group, and S a symmetric generating set. The **Cayley graph** of G, associated to S, is the graph $\Gamma_{G,S}$ defined as follows:

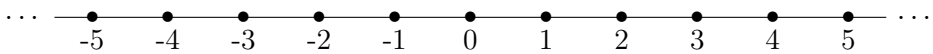
1. $V = G$ (every vertex represents an element of G),
2. $(g, g') \in E$ if there exists $s \in S$ such that $g' = gs$ (we can go from one vertex to another by multiplying the first one on the right by a generator).

Remark 3.2.2. Since S is symmetric, it is true that is $(g, g') \in E$ if and only if $(g', g) \in E$.

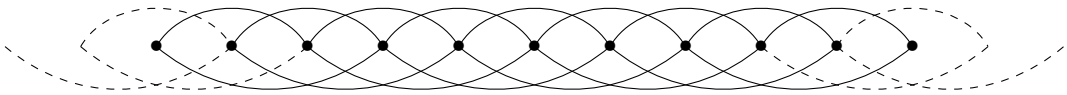
Remark 3.2.3. One could define a Cayley graph by requiring that $(g, g') \in E$ if there exists $s \in S$ such that $g' = sg$, that is choosing multiplication on the left. As we shall see, the group G acts on its Cayley graph, and we do want a left action, so that we chose right multiplication in the definition of the Cayley graph.

Let's give examples!

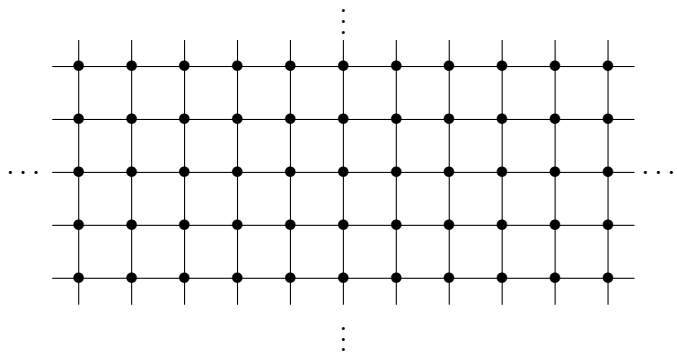
1. Let $G = \mathbb{Z}$ and choose the generating set $S = \{-1, 1\}$. Then, two integers are connected by and edge in the Cayley graph if and only if they differ by 1.



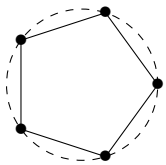
2. Let $G = \mathbb{Z}$ again, but choose the generating set $S = \{-3, -2, 2, 3\}$.



3. Let $G = \mathbb{Z}^2$ and choose the generating set $\{(-1, 0)(0, -1), (1, 0), (0, 1)\}$.

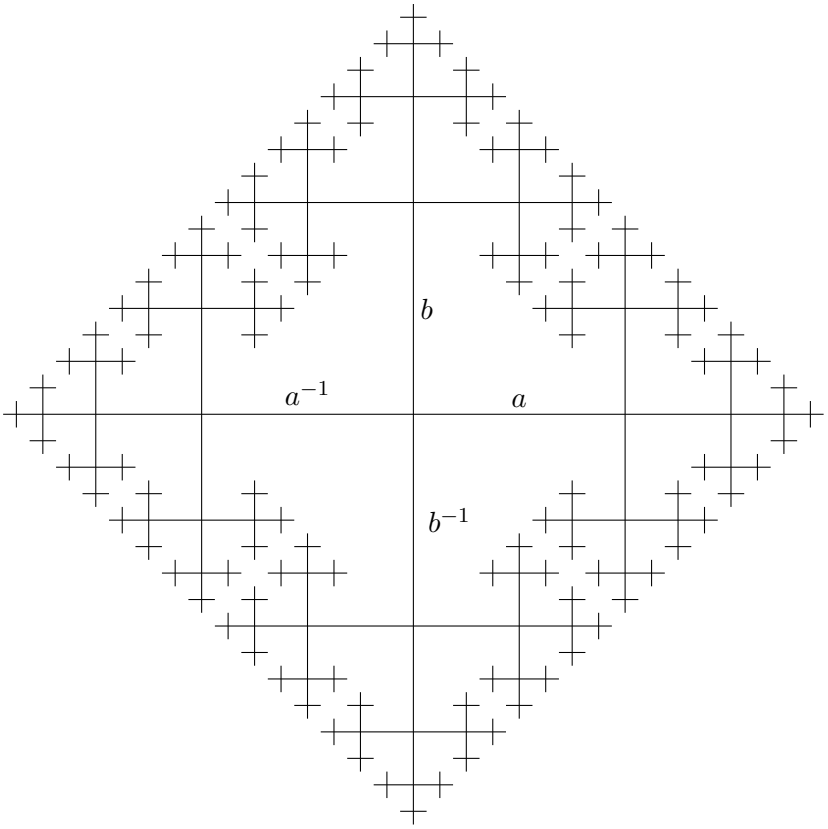


4. Let G be a finite cylic group $\mathbb{Z}/n\mathbb{Z}$. For example, take $G = \mathbb{Z}/5\mathbb{Z}$ and choose the generating set $\{-1, 1\}$. The Cayley graph can be represented as a regular n-gon.



5. Take any group G and choose S to be G. The corresponding Cayley graph is a complete graph with set of vertices G.

6. Let G be a free group $F(S)$ and choose the generating set $S \cup S^{-1}$. For example, take $G = F_2$ and denote by $\{a, b\}$ a free basis. Then, take S to be $\{a^{-1}, b^{-1}, a, b\}$. As we shall see, the corresponding Cayley graph is a tree. The Cayley graph of F_2 is actually the tree $\mathbb{T}_4$:



As illustrated by the examples of $\mathbb{Z}$ with two different generating sets, the choice of S really matters. However, in some sense, from a distant point-of-view, the two Cayley graphs look the same. We shall properly state what we mean by that later.

Notice that the Cayley graph of G is locally finite if and only if the generating set S is finite. We say that G is **finitely generated** if there exists a finite generating set S (we already used this definition at the end of our discussion about Hopfian groups). It does not mean that every generating set is finite (for example, if G is infinite, you can always choose G as a generating set). It does not even imply that the subgroups of G are finitely generated!

Proposition 3.2.4. *Let G be a group and S be a symmetric generating set and let $\Gamma_{G,S}$ be the corresponding Cayley graph. Then $\Gamma_{G,S}$ is a tree if and only if there exists $S' \subset S$ such that $S = S' \sqcup S'^{-1}$ and G is free of free basis S'.*

Proof. Assume that $G \simeq F(S')$. Every Cayley graph is connected, so that one only has to prove that $\Gamma_{G,S}$ has no loop. Let $(g, gs_1, ..., gs_1...s_n)$ be a path with $s_i \in S$. If $s_i \neq s_{i+1}^{-1}$ (no backtracking), the word $s_1...s_n$ is reduced. Since G is free, $gs_1...s_n \neq g$, otherwise, one could multiply by g^{-1} and get $s_1...s_n = e$.

Conversely, assume that $\Gamma_{G,S}$ is a tree. and define S' to be a subset of S such that $S' \cap S'^{-1} = \varnothing$ and $S' \cup S'^{-1} = S$, so that S' also generates G. Thus, one has $G \simeq F(S')/\mathrm{Ker}(\pi'_S)$. Let $w \in F(S')$ be such that $\pi'_S(w) = e \in G$. Assume that w is reduced and choose such a w of minimal length, that is if $w = s_1...s_n$, with $s_i \in S' \cup S'^{-1} = S$, then w minimises n. Since $\pi_S(w) = e$, the path $(e, es_1, ..., es_1...s_n)$ starts and ends with the same vertex in $\Gamma_{G,S}$. If there were more than one vertex, it would be a loop, since the word is reduced (and therefore, there is no backtracking), hence the path is trivial, and $w = e \in F(S')$. That means that π'_S is one-to-one, so that $G \simeq F(S')$. □

Remark 3.2.5. What we actually proved here is that loops in the Cayley graph correspond to relations in the group. It gives sense to the phrase "drawing the presentation $\langle S|R\rangle$".

Proposition 3.2.6. *Let G be a group, S be a symmetric generating set. Let $\Gamma_{G,S}$ be the corresponding Cayley graph. The group G acts on $\Gamma_{G,S}$ by $g \cdot v = gv$. It is a free graph action. Moreover for every vertices $v, v' \in \Gamma_{G,S}$, there exists $g \in G$ such that $g \cdot v = v'$ (the action is called transitive).*

Proof. The action on vertices is the same as the left translation action of G on itself. Thus, it is free. If $v, v' \in G$, then they are connected by an edge if and only if there exists $s \in S$ such that $v' = vs$. In that case, $g \cdot v' = gv' = gvs = (g \cdot v)s$, so that $g \cdot v$ and $g \cdot v'$ are also connected by an edge. If $v, v' \in G$, then $v'v^{-1} \cdot v = v'$. □

3.3 Metric structures on graphs

To properly state that two Cayley graphs of the same group with different choices of generating sets do look the same, we have introduce some geometric vocabulary. First we realise graphs as (geo)metric spaces. Recall that if $e = (v, v')$ is an edge, then $\overline{e}$ is the edge (v', v), $\partial_0(e) = v$ and $\partial_1(e) = v'$.

Let $\Gamma = (V, E)$ be a graph. The **geometric realisation** of Γ is the space

$$\mathcal{G} = (V \sqcup E \times [0,1])/(e,0) \sim \partial_0(e), (e,1) \sim \partial_1(e), (\overline{e}, t) \sim (e, 1-t).$$

Take the discrete topology on V, the discrete topology on E, the product topology on $E \times [0,1]$ and the sum topology on $V \sqcup E \times [0,1]$. Finally take the quotient topology on $\mathcal{G}$. This is called the **cellular topology of** $\mathcal{G}$.

Define also a distance on $\mathcal{G}$ as follows. Declare that each edge is isometric to $[0,1]$, meaning that if $x = \overline{(e,t)} \in \mathcal{G}$, $y = \overline{(e,s)} \in \mathcal{G}$, then $d(x,y) = |t-s| = d(y,x)$. If $\gamma : [0,1] \to \mathcal{G}$ is continuous for the cellular topology, then $\gamma([0,1])$ is compact. Therefore, there is only a finite number of vertices $\overline{v}$ in $\gamma([0,1])$. Denote them by $\overline{v_1} = \gamma(t_1)$,...,$\overline{v_k} = \gamma(t_k)$. Moreover, $\gamma(0)$ is of the form $\overline{(e,t_0)}$ and $\overline{v_1}$ of the form $\overline{(e,1)}$ or $\overline{(e,0)}$ with the same e, so that $d(\gamma(0), \overline{v_1})$ is well defined. Similarly, $d(\overline{v_k}, \gamma(1))$ is well defined. The **length** of $\gamma([0,1])$ is then $k + d(\gamma(0), v_1) + d(v_k, \gamma(1))$. If $x, y \in \mathcal{G}$, define the **graph distance** between x and y to be

$$d(x,y) = \inf\{\mathrm{length}(\gamma), \gamma : [0,1] \to \mathcal{G} \text{ continuous}, \gamma(0) = x, \gamma(1) = y\}.$$

The topology defined by that distance is weaker than the cellular topology and is not always the same. It is if the graph is locally finite. Anyway, the topology we shall use is the one induced by this distance.

If G is a group, S a symmetric generating set and if $\Gamma_{G,S}$ is the corresponding Cayley graph, then G can be embedded into its Cayley graph, identifying an element of G with the corresponding vertex. The restriction to G of the graph distance is called the **word metric**. The distance between $g, g' \in G$ is then exactly the minimal number of generators $s_1, ..., s_n \in S$ that one needs to write $g' = gs_1...s_n$.

Exercise 3.3.1. Prove that it is indeed a distance.

We now give a definition that measures the "closeness" of two metric spaces. First recall the following.

Definition 3.3.2. Let (X, d), (X', d') be two metric spaces and let $f : (X, d) \to (X', d')$ be a map. The map f is called an **isometry** if

$$\forall x, y \in X, d(x, y) = d'(f(x), f(y)).$$

Such a map is always one-to-one. Moreover, if it is onto, then its inverse is also an isometry.

Definition 3.3.3. Two metric spaces (X, d) and (X', d') are called isometric if there exists an onto isometry $f : X \to X'$.

Two metric spaces are "close" if there almost exists an onto isometry between them:

Definition 3.3.4. Let (X, d), (X', d') be two metric spaces and let $f : (X, d) \to (X', d')$ be a map. The map f is called a **quasi-isometry** if there exists $\lambda \geqslant 1$ and $c \geqslant 0$ such that

$$\forall x, y \in X, \frac{1}{\lambda} d(x, y) - c \leqslant d'(f(x), f(y) \leqslant \lambda d(x, y) + c.$$

Definition 3.3.5. Let (X, d), (X', d') be two metric spaces and let $f : (X, d) \to (X', d')$ be a map. The map f is called **quasi-onto** if there exists $D \geqslant 0$ such that

$$\forall x' \in X', \exists x \in X, d'(f(x), x') \leqslant D.$$

Up to some thickening, a quasi-isometry is an isometry and a quasi-onto map is onto.

Lemma 3.3.6. *If there exists a quasi-onto quasi-isometry $f : X \to X'$, then there exists a quasi-onto quasi-isometry $g : X' \to X$.*

Definition 3.3.7. Twp metric spaces (X, d) and (X', d') are called quasi-isometric if there exists a quasi-onto quasi-isometry $f : X \to X'$.

Lemma 3.3.8. *This defines an equivalence relation on metric spaces*

Exercise 3.3.9. Prove lemma 3.3.6 and lemma 3.3.8.

Remark 3.3.10. The action of G on $\Gamma_{G,S}$ is by isometries, meaning that for every $g \in G$ $v \mapsto g \cdot v$ is an isometry of $\Gamma_{G,S}$. Since the action is free, one can see G as a subgroup of the set of isometries of $\Gamma_{G,S}$ (check that this is a group!). It is not in general the whole group of isometries. Therefore, in some sense, $\Gamma_{G,S}$ has much more symmetry than G.

3.4 Equivalence of Cayley graphs

It is now possible to prove that two Cayley graphs with different (finite) generating sets look the same.

Let G be a group and S a generating set. Let $\Gamma_{G,S}$ be the corresponding Cayley graph. Then the inclusion of G into $\Gamma_{G,S}$ is a quasi-onto quasi-isometry. It is actually an isometry since the word metric is the restriction of the graph metric of $\Gamma_{G,S}$. It is quasi-onto because every point on an edge is at distance at most 1 of a vertex.

Theorem 3.4.1. *Let G be a finitely generated group and let S, S' be two **finite** symmetric generating sets. Denote by d, d' the corresponding word metrics. Then $Id : (G, d) \to (G, d')$ is a quasi-isometry.*

Proof. Let $\Lambda = \max\{d(e, s'), s' \in S'\}$ and $\Lambda' = \max\{d'(e, s), s \in S\}$. If $d'(g, h) = n$, then $h = gs'_1 ... s'_n$, $s'_i \in S'$. Write s'_i as a word w_i in S so that $h = gw_1 ... w_n$. Then $d(g, h) = d(e, w_1 ... w_n) \leqslant \Lambda n = \Lambda d'(g, h)$. Similarly, $d'(g, h) \leqslant \Lambda' d(g, h)$. Let $\lambda = \max(\Lambda, \Lambda')$. Then,

$$\frac{1}{\lambda} d(g, h) \leqslant d'(g, h) \leqslant \lambda d(g, h).$$

□

Corollary 3.4.2. *Let G be a finitely generated group and let S, S' be two **finite** symmetric generating sets. Let $\Gamma_{G,S}$ and $\Gamma_{G,S'}$ be the corresponding Cayley graphs. Then, for the graph metrics, $\Gamma_{G,S}$ and $\Gamma_{G,S'}$ are quasi-isometric.*

References

[1] Roger C. Lyndon and Paul E. Schupp. *Combinatorial Group Theory*. Reprint of the 1977 edition. Classics in Mathematics. Springer, 2001.

[2] John Meier. *Groups, Graphs and Trees*. London Mathematical Society Student Texts 73. Cambridge University Press, 2008.

[3] Joseph J. Rotman. *An Introduction to the Theory of Groups*. Graduate Texts in Mathematics. Springer, 1995.

[4] Jean-Pierre Serre. *Arbres, amalgames,* SL_2. Third edition. Astérisque 46. Société Mathématique de France, 1983.

[5] Jean-Pierre Serre. *Trees*. Translated by J. Stillwell. Springer, 1980.

EXERCISES

Elementary theory of groups

To get warmed up

Exercise 1 Let G be a group.
a) Show that the neutral element e is unique.
b) Show that if $a \in G$, then its inverse a^{-1} is unique.

Exercise 2 Show that if G is a group and H is a subgroup of G, then H is itself a group.

Exercise 3 Let G, G' be two groups and $f : G \to G'$ a group morphism.
a) Show that $f(e) = e'$
b) Show that for every $a \in G$, $f(a^{-1}) = f(a)^{-1}$.

Exercise 4 Let G, G' be two groups and $f : G \to G'$ a group morphism. Show that the map f is one-to-one if and only if $\mathrm{Ker}(f) = \{e\}$.

Exercise 5 Let G be a group. Denote by $Z(G)$ the set of elements $g \in G$ that commute with every element h of G, i.e. $g \in Z(G)$ if $\forall h \in G, gh = hg$. Show that $Z(G)$ is a subgroup of G. It is called the center of G.

Exercise 6 Let G be a group and let $g, h \in G$.
a) Show that $(gh)^{-1} = h^{-1}g^{-1}$.
b) Show that $(ghg^{-1})^{-1} = gh^{-1}g^{-1}$.
c) Show that for all $n \in \mathbb{Z}$, $(ghg^{-1})^n = gh^ng^{-1}$.

Normal subgroups and quotient groups

Exercise 7 Show that if G is abelian, then all its subgroups are normal.

Exercise 8 Denote by $GL_n(\mathbb{K})$ the set of invertible matrices of size n and by $SL_n(\mathbb{K})$ the set of those matrices with determinant 1.
a) Show that $SL_n(\mathbb{K})$ is a normal subgroup of $GL_n(\mathbb{K})$.
b) Show that the quotient group $GL_n(\mathbb{K})/SL_n(\mathbb{K})$ is isomorphic to $\mathbb{K}^*$.

Exercise 9 Let G, G' be two groups and $f : G \to G'$ a group morphism. Show that $\mathrm{Ker}(f)$ is a normal subgroup of G.

Exercise 10 Let G be a group and H a subgroup of G of index 2. Show that H is a normal subgroup of G.

Exercise 11 Let G, G' be two groups and $f : G \to G'$ a group morphism. Assume that G is finite. Show that $|G| = |\mathrm{Ker}(f)| \times |\mathrm{Im}(f)|$.

Cyclic groups

Exercise 12

a) If $n \in \mathbb{Z}$, denote by $n\mathbb{Z}$ the set of integers of the form nk. Show that $n\mathbb{Z}$ is a normal subgroup of $\mathbb{Z}$.

b) Determine all the subgroups of $\mathbb{Z}$.

Hint: Use euclidean division.

Exercise 13 Let G be a **cyclic** group.

a) Show that there exists a group morphism $f : \mathbb{Z} \to G$ that is onto.

b) Show that either G is isomorphic to $\mathbb{Z}$ or there exists $n \in \mathbb{Z}$ such that G is isomorphic to $\mathbb{Z}/n\mathbb{Z}$.

Exercise 14 Find all the automorphisms of $\mathbb{Z}$.

The derived subgroup

Exercise 15 Let G be a group. If $g, h \in G$, define their commutator by $[g, h] := g^{-1}h^{-1}gh$. The derived subgroup (sometimes called commutator subgroup) of G is the subgroup $D(G)$ generated by all the commutators $[g, h]$, for $g, h \in G$.

a) Show that the derived subgroup of G is normal.

Hint: Use exercise 6.

b) Show that $G/D(G)$ is abelian.

c) Show that $D(G)$ is the smallest normal subgroup of G such that the quotient is abelian.

Group actions

Exercise 16 Let G be a group of order p^k, acting on a finite set X. Denote by X^G the set of (globally) fixed elements, i.e. $x \in X^G$ if $\forall g \in G$, $g \cdot x = x$. Show that $|X| = |X^G|$ modulo p.

Hint: Use the class formula.

Exercise 17 [A theorem of Cauchy] Let G be a finite group and let p be a prime number such that p divides $|G|$. We are going to prove that there exists in G some element g of order exactly p: $g^p = e$ and $g^k \neq e$, if $k \leqslant p - 1$.

a) Denote by X the set $\{(g_1, ..., g_p) \in G^p, g_1...g_p = e\}$. Show that $|X| = |G|^{p-1}$. Thus, p divides $|X|$.

b) Show that $j \cdot (g_1, ..., g_p) := (g_{1+j}, ..., g_{p+j})$ defines a group action of $\mathbb{Z}/p\mathbb{Z}$ on X.

c) Show that $X^{\mathbb{Z}/p\mathbb{Z}} = \{(x, ..., x) \in G^p, x = e \text{ or } x \text{ is of order } p\}$ and conclude, using exercise 16.

Exercise 18

a) Let G be a group of order p. Show that G is isomorphic to $\mathbb{Z}/p\mathbb{Z}$.

b) Let G be a group of order p^k. Using exercise 16, show that $Z(G)$ is not trivial.

c) Let G be a group of order p^2. Show that G is abelian.

Exercise 19 [A Burnside formula] Let G be a finite group acting on a finite set X. Denote by Ω the set of all orbits. Denote by A the set $\{(g, x) \in G \times X, g \cdot x = x\}$.

a) Show that $|A| = \sum_{\omega \in \Omega} \sum_{x \in \omega} |\mathrm{Stab}_x| = |\Omega||G|$.

b) If $g \in G$, denote by Fix_g the set of elements $x \in X$ such that $g \cdot x = x$. Show that $|A| = \sum_{g \in G} |\mathrm{Fix}_g|$.

c) Conclude that $|\Omega| = 1/|G| \sum_{g \in G} |\mathrm{Fix}_g|$.

EXERCISES

Group presentations

Free groups

Exercise 1 [The Ping-pong lemma] We are going to prove a very helpful lemma. It is a powerful tool to prove that some groups are free, another efficient tool being the Bass-Serre theory, that is actions of groups on trees.

Lemma. *Let G be a group acting on a set X. Let S be a generating set of G. Assume that there are non-empty disjoint sets $(X_s)_{s\in S}$ such that*

$$\forall s,t \in S, s \neq t, \forall n \in \mathbb{Z}^*, s^n X_t \subset X_s.$$

Then, the group G is free with free basis S: $G \simeq F(S)$.

To prove this lemma, take $g = s_1^{\alpha_1}...s_n^{\alpha_n} \in G$. Assume that g is reduced. It only has to be shown that $g \neq e$. There are two cases. Either $s_n = s_1$ or $s_n \neq s_1$.

a) Show that each s_i is of infinite order, i.e. $s_i^n = e$ if and only if $n = 0$.

b) Assume that $s_1 = s_n = s$. Denote by $Y_s = \bigcup_{t\neq s} X_t$. Show that if $x_0 \in Y_s$, then $g \cdot x_0 \in X_s$. Deduce that $g \neq e$.

c) Assume that $s_1 = s \neq t = s_n$ Show that there exists $x \in G$ such that $x \neq s_1^{-\alpha_1}$ and $x^{-1} \neq s_n^{-\alpha_n}$ By considering xgx^{-1}, show that $g \neq e$.

Exercise 2 Let $F(a,b)$ a free group of rank 2 and let S_n be the set $\{b, aba^{-1}, ..., a^{n-1}ba^{n-1}\}$. For $k \geqslant 0$, denote by X_k the set of reduced words of F_2 beginning with $a^k b$ or $a^k b^{-1}$.

a) Show that the subgroup of F_2 generated by S_n acts faithfully on F_2.

b) Using the ping-pong lemma, show that the subgroup of F_2 generated by S_n is free of rank n.

c) Show that F_2 is a subgroup of F_n, for every $n \geqslant 2$.

This shows that F_k is a subgroup of F_n for every $k \geqslant 1$ and $n \geqslant 2$. However, the following exercise shows that $F_k \not\simeq F_n$, if $k \neq n$.

Exercise 3 Recall the definition from exercise 15 in the last exercise sheet: the derived subgroup of a group G is the smallest normal subgroup of G such that the quotient is abelian. It is generated by elements of the form $[g,h] := g^{-1}h^{-1}gh$ (those elements are called commutators). The derived subgroup of G is denoted by $D(G)$.

a) Show that $F(S)/D(F(S)) \simeq \mathbb{Z}^S$ (see exercise 5 below). You now understand why the groups $\mathbb{Z}^k$ are called abelian free groups.

b) Show that if $F(S) \simeq F(S')$ then there exists a bijection between S and S'. In particular, if $F_n \simeq F_k$, then $n = k$.

Relations

Exercise 4 Let G be a group and H be a subgroup of G. Recall that $\langle\langle H \rangle\rangle$ is the smallest normal subgroup of G containing H. Show that $\langle\langle H \rangle\rangle$ is the set of elements of G of the form $g_1 h_1 g_1^{-1} ... g_n h_n g_n^{-1}$.

Exercise 5 Prove that $\mathbb{Z}^n \simeq \langle s_1, ..., s_n | s_i s_j = s_j s_i \rangle$.

Exercise 6 Denote by $\mathfrak{S}_n$ the group of permutations of $\{1, ..., n\}$. Show that

$$\mathfrak{S}_n \simeq \langle x_1, ..., x_n | x_i^2, x_i x_j = x_j x_i, (j - i \geqslant 2), x_i x_{i+1} x_i = x_{i+1} x_i x_{i+1} \rangle.$$

A geometric realisation of F_2.

Exercise 7 This exercise is for those who know a little about hyperbolic geometry. However, someone without knowledge in this domain of mathematics can still do the exercise, but will miss the geometric flavour. It seems that it is the first example of the use of the ping-pong lemma to show that some group is free.

Take the hyperbolic upper-half plane $\mathbb{H}^2$, i.e. $\mathbb{H}^2 := \{z = x + iy \in \mathbb{C}, x \in \mathbb{R}, y > 0\}$. Recall that the group $SL_2(\mathbb{R})$ acts on $\mathbb{H}^2$ by homography, that is

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

This action is continuous on $\overline{\mathbb{H}^2} := \{z = x + iy, x \in \mathbb{R}, y \geqslant 0\} \cup \{\infty\}$ (the closure is taken into the Riemann sphere). By definition, one has

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \infty = \frac{a}{c}.$$

a) Define $\partial\mathbb{H}^2 := \{z = x \in \mathbb{R}\} \cup \{\infty\}$. Show that the action preserves $\partial\mathbb{H}^2$, i.e. if $z \in \partial\mathbb{H}^2$, then its image by any matrix of $SL_2(\mathbb{R})$ is still in $\partial\mathbb{H}^2$.

b) Consider the two matrices

$$A = \begin{pmatrix} 2 & 0 \\ 0 & 1/2 \end{pmatrix} \text{ and } B = \begin{pmatrix} \sqrt{2} & 1 \\ 1 & \sqrt{2} \end{pmatrix}.$$

Show that $A, B \in SL_2(\mathbb{Z})$ and that A and B only have two fixed points on $\partial\mathbb{H}^2$. Denote them by a_1, a_2, b_1, b_2, with $A \cdot a_i = a_i$, $B \cdot b_i = b_i$.

c) Show that for any $z \in \mathbb{H}^2$, $A^n \cdot z$ converges to a_1 if n tends to $+\infty$ and converges to a_2 when n tends to $-\infty$.

d) Show that for any $z \in \mathbb{H}^2$, $B^n \cdot z$ converges to b_1 if n tends to $+\infty$ and converges to b_2 when n tends to $-\infty$.

e) Using the ping-pong lemma, show that for some integers $k, l \geqslant 1$, the subgroup of $SL_2(\mathbb{Z})$ generated by A^k and B^l is free.

This result is really important in hyperbolic geometry. The matrices A and B are called loxodromic (sometimes they are called hyperbolic). Since their fixed points are disjoint, they are called independent loxodromic matrices. Such free groups generated by independent loxodromic matrices are called Schottky groups.

EXERCISES

Cayley graphs

Words and metric structures

Exercise 1 Recall that if G is a group and S a generating set, we define $d(g,h)$ to be the minimum number of generators $s_1, ..., s_n$ of S such that $g^{-1}h = s_1...s_n$. Show that d defines a metric structure on G (it is called the word metric).

Exercise 2 Recall that a quasi-isometry from a metric space (X,d) to a metric space (X',d') is a map $f : X \to X'$ with the property that there exists $\lambda \geqslant 1$ and $c \geqslant 0$ such that for every $x, y \in X$, $\frac{1}{\lambda}d(x,y) - c \leqslant d'(f(x), f(y)) \leqslant \lambda d(x,y) + c$.

Recall that a map $f : (X,d) \to (X',d')$ is quasi-onto if there exists $\alpha \geqslant 0$ such that for every $x' \in X'$ there exists $x \in X$ such that $d(f(x), x') \leqslant \alpha$.

a) Show that if there exists a quasi-onto quasi-isometry $f : X \to X'$, then there exists quasi-onto quasi-isometry $g : X' \to X$.

b) Say that two metric spaces (X,d), (X',d') are quasi-isometric if there exists a quasi-onto quasi-isometry $f : X \to X'$. Show that this is an equivalence relation. Show that you cannot remove the quasi-onto hypothesis.

Drawing Cayley graphs

Exercise 3 Define the dihedral group D_n to be the group of symmetries of the regular n-gon, that is reflections and rotations of the complex-plane that preserves the regular n-gon. Fix the vertices of the regular n-gon to be the set $\{z \in \mathbb{C}, |z|^n = 1\}$. Define σ to be the reflection of axis the real line, that is $\sigma(z) = \overline{z}$. Define ρ_n to be the rotation of angle $2\pi/n$.

a) Show that $\sigma\rho_n\sigma^{-1} = \rho_n^{-1}$.

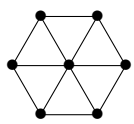
b) Show that D_n is generated by σ and ρ_n and that D_n is of order $2n$.

c) Choose your favorite n and draw the Cayley graph of D_n with respect to the generating set $\{\rho_n, \sigma\}$.

Exercise 4 Draw the Cayley graph of $\mathbb{Z}/5\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ with respect to the generating set $\{(1,0),(0,1)\}$. What is the difference between this graph and the Cayley graph of D_5 with respect to $\{\rho_5, \sigma\}$?

Exercise 5 Recall that there is an embedding of F_3 into F_2: if F_2 is generated by $\{a,b\}$, then the subgroup of F_2 generated by $\{b, aba^{-1}, a^2ba^{-2}\}$ is isomorphic to F_3. Try to draw this embedding, that is try to find the Cayley graph of F_3 inside the Cayley graph of F_2.

Exercise 6 If Γ is a graph and $e \in \Gamma$ an edge and if G is a group acting on Γ, there are two natural ways of defining the stabiliser of e. Define $\mathrm{Stab}_e = \{g \in G, g \cdot e = e\}$ and $\mathrm{Stab}'_e = \{g \in G, g \cdot v_1 = v_1, g \cdot v_2 = v_2\}$, with $e = (v_1, v_2)$. Let Γ be the "wheel graph" drawn below. Let G be the symmetry group of Γ, that is the group of isometries of the plan that preserves Γ. Show that if e is a central edge, then $\mathrm{Stab}_e \simeq \mathrm{Stab}'_e \simeq \mathbb{Z}/2\mathbb{Z}$, but if e is an external edge, then $\mathrm{Stab}_e \simeq \mathbb{Z}/2\mathbb{Z}$, while $\mathrm{Stab}'_e = \{Id\}$.



The Wheel graph

EXERCISES

Elementary theory of groups

To get warmed up

Exercise 1 Let G be a group.
a) Show that the neutral element e is unique.
b) Show that if $a \in G$, then its inverse a^{-1} is unique.

Exercise 2 Show that if G is a group and H is a subgroup of G, then H is itself a group.

Exercise 3 Let G, G' be two groups and $f : G \to G'$ a group morphism.
a) Show that $f(e) = e'$
b) Show that for every $a \in G$, $f(a^{-1}) = f(a)^{-1}$.

Exercise 4 Let G, G' be two groups and $f : G \to G'$ a group morphism. Show that the map f is one-to-one if and only if $\mathrm{Ker}(f) = \{e\}$.

Exercise 5 Let G be a group. Denote by $Z(G)$ the set of elements $g \in G$ that commute with every element h of G, i.e. $g \in Z(G)$ if $\forall h \in G, gh = hg$. Show that $Z(G)$ is a subgroup of G. It is called the center of G.

Exercise 6 Let G be a group and let $g, h \in G$.
a) Show that $(gh)^{-1} = h^{-1}g^{-1}$.
b) Show that $(ghg^{-1})^{-1} = gh^{-1}g^{-1}$.
c) Show that for all $n \in \mathbb{Z}$, $(ghg^{-1})^n = gh^ng^{-1}$.

Normal subgroups and quotient groups

Exercise 7 Show that if G is abelian, then all its subgroups are normal.

Exercise 8 Denote by $GL_n(\mathbb{K})$ the set of invertible matrices of size n and by $SL_n(\mathbb{K})$ the set of those matrices with determinant 1.
a) Show that $SL_n(\mathbb{K})$ is a normal subgroup of $GL_n(\mathbb{K})$.
b) Show that the quotient group $GL_n(\mathbb{K})/SL_n(\mathbb{K})$ is isomorphic to $\mathbb{K}^*$.

Exercise 9 Let G, G' be two groups and $f : G \to G'$ a group morphism. Show that $\mathrm{Ker}(f)$ is a normal subgroup of G.

Exercise 10 Let G be a group and H a subgroup of G of index 2. Show that H is a normal subgroup of G.

Exercise 11 Let G, G' be two groups and $f : G \to G'$ a group morphism. Assume that G is finite. Show that $|G| = |\mathrm{Ker}(f)| \times |\mathrm{Im}(f)|$.

Cyclic groups

Exercise 12

a) If $n \in \mathbb{Z}$, denote by $n\mathbb{Z}$ the set of integers of the form nk. Show that $n\mathbb{Z}$ is a normal subgroup of $\mathbb{Z}$.

b) Determine all the subgroups of $\mathbb{Z}$.

Hint : Use euclidean division.

Exercise 13 Let G be a **cyclic** group.

a) Show that there exists a group morphism $f : \mathbb{Z} \to G$ that is onto.

b) Show that either G is isomorphic to $\mathbb{Z}$ or there exists $n \in \mathbb{Z}$ such that G is isomorphic to $\mathbb{Z}/n\mathbb{Z}$.

Exercise 14 Find all the automorphisms of $\mathbb{Z}$.

The derived subgroup

Exercise 15 Let G be a group. If $g, h \in G$, define their commutator by $[g, h] := g^{-1}h^{-1}gh$. The derived subgroup (sometimes called commutator subgroup) of G is the subgroup $D(G)$ generated by all the commutators $[g, h]$, for $g, h \in G$.

a) Show that the derived subgroup of G is normal.

Hint : Use exercise 6.

b) Show that $G/D(G)$ is abelian.

c) Show that $D(G)$ is the smallest normal subgroup of G such that the quotient is abelian.

Group actions

Exercise 16 Let G be a group of order p^k, acting on a finite set X. Denote by X^G the set of (globally) fixed elements, i.e. $x \in X^G$ if $\forall g \in G$, $g \cdot x = x$. Show that $|X| = |X^G|$ modulo p.

Hint : Use the class formula.

Exercise 17 [A theorem of Cauchy] Let G be a finite group and let p be a prime number such that p divides $|G|$. We are going to prove that there exists in G some element g of order exactly $p : g^p = e$ and $g^k \neq e$, if $k \leqslant p - 1$.

a) Denote by X the set $\{(g_1, ..., g_p) \in G^p, g_1...g_p = e\}$. Show that $|X| = |G|^{p-1}$. Thus, p divides $|X|$.

b) Show that $j \cdot (g_1, ..., g_p) := (g_{1+j}, ..., g_{p+j})$ defines a group action of $\mathbb{Z}/p\mathbb{Z}$ on X.

c) Show that $X^{\mathbb{Z}/p\mathbb{Z}} = \{(x, ..., x) \in G^p, x = e \text{ or } x \text{ is of order } p\}$ and conclude, using exercise 16.

Exercise 18

a) Let G be a group of order p. Show that G is isomorphic to $\mathbb{Z}/p\mathbb{Z}$.

b) Let G be a group of order p^k. Using exercise 16, show that $Z(G)$ is not trivial.

c) Let G be a group of order p^2. Show that G is abelian.

Exercise 19 [A Burnside formula] Let G be a finite group acting on a finite set X. Denote by Ω the set of all orbits. Denote by A the set $\{(g, x) \in G \times X, g \cdot x = x\}$.

a) Show that $|A| = \sum_{\omega \in \Omega} \sum_{x \in \omega} |\mathrm{Stab}_x| = |\Omega||G|$.

b) If $g \in G$, denote by Fix_g the set of elements $x \in X$ such that $g \cdot x = x$. Show that $|A| = \sum_{g \in G} |\mathrm{Fix}_g|$.

c) Conclude that $|\Omega| = 1/|G| \sum_{g \in G} |\mathrm{Fix}_g|$.

EXERCISES

Elementary theory of groups

To get warmed up

Exercise 1 Let G be a group.
a) Show that the neutral element e is unique.
b) Show that if $a \in G$, then its inverse a^{-1} is unique.

Exercise 2 Show that if G is a group and H is a subgroup of G, then H is itself a group.

Exercise 3 Let G, G' be two groups and $f : G \to G'$ a group morphism.
a) Show that $f(e) = e'$
b) Show that for every $a \in G$, $f(a^{-1}) = f(a)^{-1}$.

Exercise 4 Let G, G' be two groups and $f : G \to G'$ a group morphism. Show that the map f is one-to-one if and only if $\mathrm{Ker}(f) = \{e\}$.

Exercise 5 Let G be a group. Denote by $Z(G)$ the set of elements $g \in G$ that commute with every element h of G, i.e. $g \in Z(G)$ if $\forall h \in G, gh = hg$. Show that $Z(G)$ is a subgroup of G. It is called the center of G.

Exercise 6 Let G be a group and let $g, h \in G$.
a) Show that $(gh)^{-1} = h^{-1}g^{-1}$.
b) Show that $(ghg^{-1})^{-1} = gh^{-1}g^{-1}$.
c) Show that for all $n \in \mathbb{Z}$, $(ghg^{-1})^n = gh^ng^{-1}$.

Normal subgroups and quotient groups

Exercise 7 Show that if G is abelian, then all its subgroups are normal.

Exercise 8 Denote by $GL_n(\mathbb{K})$ the set of invertible matrices of size n and by $SL_n(\mathbb{K})$ the set of those matrices with determinant 1.
a) Show that $SL_n(\mathbb{K})$ is a normal subgroup of $GL_n(\mathbb{K})$.
b) Show that the quotient group $GL_n(\mathbb{K})/SL_n(\mathbb{K})$ is isomorphic to $\mathbb{K}^*$.

Exercise 9 Let G, G' be two groups and $f : G \to G'$ a group morphism. Show that $\mathrm{Ker}(f)$ is a normal subgroup of G.

Exercise 10 Let G be a group and H a subgroup of G of index 2. Show that H is a normal subgroup of G.

Exercise 11 Let G, G' be two groups and $f : G \to G'$ a group morphism. Assume that G is finite. Show that $|G| = |\mathrm{Ker}(f)| \times |\mathrm{Im}(f)|$.

Cyclic groups

Exercise 12

a) If $n \in \mathbb{Z}$, denote by $n\mathbb{Z}$ the set of integers of the form nk. Show that $n\mathbb{Z}$ is a normal subgroup of $\mathbb{Z}$.

b) Determine all the subgroups of $\mathbb{Z}$.

Hint : Use euclidean division.

Exercise 13 Let G be a **cyclic** group.

a) Show that there exists a group morphism $f : \mathbb{Z} \to G$ that is onto.

b) Show that either G is isomorphic to $\mathbb{Z}$ or there exists $n \in \mathbb{Z}$ such that G is isomorphic to $\mathbb{Z}/n\mathbb{Z}$.

Exercise 14 Find all the automorphisms of $\mathbb{Z}$.

The derived subgroup

Exercise 15 Let G be a group. If $g, h \in G$, define their commutator by $[g, h] := g^{-1}h^{-1}gh$. The derived subgroup (sometimes called commutator subgroup) of G is the subgroup $D(G)$ generated by all the commutators $[g, h]$, for $g, h \in G$.

a) Show that the derived subgroup of G is normal.

Hint : Use exercise 6.

b) Show that $G/D(G)$ is abelian.

c) Show that $D(G)$ is the smallest normal subgroup of G such that the quotient is abelian.

Group actions

Exercise 16 Let G be a group of order p^k, acting on a finite set X. Denote by X^G the set of (globally) fixed elements, i.e. $x \in X^G$ if $\forall g \in G$, $g \cdot x = x$. Show that $|X| = |X^G|$ modulo p.

Hint : Use the class formula.

Exercise 17 [A theorem of Cauchy] Let G be a finite group and let p be a prime number such that p divides $|G|$. We are going to prove that there exists in G some element g of order exactly $p : g^p = e$ and $g^k \neq e$, if $k \leqslant p - 1$.

a) Denote by X the set $\{(g_1, ..., g_p) \in G^p, g_1...g_p = e\}$. Show that $|X| = |G|^{p-1}$. Thus, p divides $|X|$.

b) Show that $j \cdot (g_1, ..., g_p) := (g_{1+j}, ..., g_{p+j})$ defines a group action of $\mathbb{Z}/p\mathbb{Z}$ on X.

c) Show that $X^{\mathbb{Z}/p\mathbb{Z}} = \{(x, ..., x) \in G^p, x = e \text{ or } x \text{ is of order } p\}$ and conclude, using exercise 16.

Exercise 18

a) Let G be a group of order p. Show that G is isomorphic to $\mathbb{Z}/p\mathbb{Z}$.

b) Let G be a group of order p^k. Using exercise 16, show that $Z(G)$ is not trivial.

c) Let G be a group of order p^2. Show that G is abelian.

Exercise 19 [A Burnside formula] Let G be a finite group acting on a finite set X. Denote by Ω the set of all orbits. Denote by A the set $\{(g, x) \in G \times X, g \cdot x = x\}$.

a) Show that $|A| = \sum_{\omega \in \Omega} \sum_{x \in \omega} |\mathrm{Stab}_x| = |\Omega||G|$.

b) If $g \in G$, denote by Fix_g the set of elements $x \in X$ such that $g \cdot x = x$. Show that $|A| = \sum_{g \in G} |\mathrm{Fix}_g|$.

c) Conclude that $|\Omega| = 1/|G| \sum_{g \in G} |\mathrm{Fix}_g|$.

EXERCISES

Elementary theory of groups

To get warmed up

Exercise 1 Let G be a group.
a) Show that the neutral element e is unique.
b) Show that if $a \in G$, then its inverse a^{-1} is unique.

Exercise 2 Show that if G is a group and H is a subgroup of G, then H is itself a group.

Exercise 3 Let G, G' be two groups and $f : G \to G'$ a group morphism.
a) Show that $f(e) = e'$
b) Show that for every $a \in G$, $f(a^{-1}) = f(a)^{-1}$.

Exercise 4 Let G, G' be two groups and $f : G \to G'$ a group morphism. Show that the map f is one-to-one if and only if $\mathrm{Ker}(f) = \{e\}$.

Exercise 5 Let G be a group. Denote by $Z(G)$ the set of elements $g \in G$ that commute with every element h of G, i.e. $g \in Z(G)$ if $\forall h \in G, gh = hg$. Show that $Z(G)$ is a subgroup of G. It is called the center of G.

Exercise 6 Let G be a group and let $g, h \in G$.
a) Show that $(gh)^{-1} = h^{-1}g^{-1}$.
b) Show that $(ghg^{-1})^{-1} = gh^{-1}g^{-1}$.
c) Show that for all $n \in \mathbb{Z}$, $(ghg^{-1})^n = gh^ng^{-1}$.

Normal subgroups and quotient groups

Exercise 7 Show that if G is abelian, then all its subgroups are normal.

Exercise 8 Denote by $GL_n(\mathbb{K})$ the set of invertible matrices of size n and by $SL_n(\mathbb{K})$ the set of those matrices with determinant 1.
a) Show that $SL_n(\mathbb{K})$ is a normal subgroup of $GL_n(\mathbb{K})$.
b) Show that the quotient group $GL_n(\mathbb{K})/SL_n(\mathbb{K})$ is isomorphic to $\mathbb{K}^*$.

Exercise 9 Let G, G' be two groups and $f : G \to G'$ a group morphism. Show that $\mathrm{Ker}(f)$ is a normal subgroup of G.

Exercise 10 Let G be a group and H a subgroup of G of index 2. Show that H is a normal subgroup of G.

Exercise 11 Let G, G' be two groups and $f : G \to G'$ a group morphism. Assume that G is finite. Show that $|G| = |\mathrm{Ker}(f)| \times |\mathrm{Im}(f)|$.

Cyclic groups

Exercise 12

a) If $n \in \mathbb{Z}$, denote by $n\mathbb{Z}$ the set of integers of the form nk. Show that $n\mathbb{Z}$ is a normal subgroup of $\mathbb{Z}$.

b) Determine all the subgroups of $\mathbb{Z}$.

Hint : Use euclidean division.

Exercise 13 Let G be a **cyclic** group.

a) Show that there exists a group morphism $f : \mathbb{Z} \to G$ that is onto.

b) Show that either G is isomorphic to $\mathbb{Z}$ or there exists $n \in \mathbb{Z}$ such that G is isomorphic to $\mathbb{Z}/n\mathbb{Z}$.

Exercise 14 Find all the automorphisms of $\mathbb{Z}$.

The derived subgroup

Exercise 15 Let G be a group. If $g, h \in G$, define their commutator by $[g, h] := g^{-1}h^{-1}gh$. The derived subgroup (sometimes called commutator subgroup) of G is the subgroup $D(G)$ generated by all the commutators $[g, h]$, for $g, h \in G$.

a) Show that the derived subgroup of G is normal.

Hint : Use exercise 6.

b) Show that $G/D(G)$ is abelian.

c) Show that $D(G)$ is the smallest normal subgroup of G such that the quotient is abelian.

Group actions

Exercise 16 Let G be a group of order p^k, acting on a finite set X. Denote by X^G the set of (globally) fixed elements, i.e. $x \in X^G$ if $\forall g \in G$, $g \cdot x = x$. Show that $|X| = |X^G|$ modulo p.

Hint : Use the class formula.

Exercise 17 [A theorem of Cauchy] Let G be a finite group and let p be a prime number such that p divides $|G|$. We are going to prove that there exists in G some element g of order exactly $p : g^p = e$ and $g^k \neq e$, if $k \leqslant p - 1$.

a) Denote by X the set $\{(g_1, ..., g_p) \in G^p, g_1...g_p = e\}$. Show that $|X| = |G|^{p-1}$. Thus, p divides $|X|$.

b) Show that $j \cdot (g_1, ..., g_p) := (g_{1+j}, ..., g_{p+j})$ defines a group action of $\mathbb{Z}/p\mathbb{Z}$ on X.

c) Show that $X^{\mathbb{Z}/p\mathbb{Z}} = \{(x, ..., x) \in G^p, x = e \text{ or } x \text{ is of order } p\}$ and conclude, using exercise 16.

Exercise 18

a) Let G be a group of order p. Show that G is isomorphic to $\mathbb{Z}/p\mathbb{Z}$.

b) Let G be a group of order p^k. Using exercise 16, show that $Z(G)$ is not trivial.

c) Let G be a group of order p^2. Show that G is abelian.

Exercise 19 [A Burnside formula] Let G be a finite group acting on a finite set X. Denote by Ω the set of all orbits. Denote by A the set $\{(g, x) \in G \times X, g \cdot x = x\}$.

a) Show that $|A| = \sum_{\omega \in \Omega} \sum_{x \in \omega} |\mathrm{Stab}_x| = |\Omega||G|$.

b) If $g \in G$, denote by Fix_g the set of elements $x \in X$ such that $g \cdot x = x$. Show that $|A| = \sum_{g \in G} |\mathrm{Fix}_g|$.

c) Conclude that $|\Omega| = 1/|G| \sum_{g \in G} |\mathrm{Fix}_g|$.