Notes in Group Theory

Juan Alonso

1 Introduction to Groups

1.1 Definitions and first properties

A *binary operation* on a set A is a function $\cdot : A \times A \to A$. We will usually denote $\cdot(a, b)$ by $a \cdot b$, or ab when the operation is clear from the context.

Definition A *group* is a pair $(G, \cdot)$, where G is a nonempty set and $\cdot : G \times G \to G$ is a binary operation satisfying the following axioms:

1. (Associative law) For any $a, b, c \in G$, $a \cdot (b \cdot c) = (a \cdot b) \cdot c$
2. (Existence of an identity element) There exists $e \in G$ so that for all $a \in G$, $a \cdot e = e \cdot a = a$
3. (Existence of inverses) For each $a \in G$ there exists some $b \in G$ such that $a \cdot b = b \cdot a = e$

Observe that under these assumptions the identity element e in condition 2 is unique. Indeed, if e_1, e_2 both satisfy this condition, then $e_1 = e_1 \cdot e_2 = e_2$. In most of the cases, we will write 1 to denote the identity element of a group. The element b in condition 3 is called the inverse of a, and written a^{-1}. This terminology is justified by the fact that each $a \in G$ has a unique inverse. The proof is also easy. It is standard to refer to the group $(G, \cdot)$ only as G, and to the operation $\cdot$ as *product*.

In general, the commutative law needs not be satisfied. It's said that the elements $a, b \in G$ *commute* when $ab = ba$. A group G is *abelian* every pair of elements of G commute.

Facts Let G be a group.

1. For $a \in G$, $(a^{-1})^{-1} = a$
2. For $a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$
3. (Generalized associativity) For $a_1, \dots, a_n \in G$, all the different ways of bracketing the expression $a_1 a_2 \cdots a_n$ (and then computing the corresponding iterated product) yield the same result.

Here are a few examples.

1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ with the sum as operation. The identity is 0. The inverse of a is $-a$.
2. The integers modulo n.

   Let $n > 0$ be an integer. We say that $a, b \in \mathbb{Z}$ are *congruent modulo* n, and write $a \equiv b \pmod{n}$, if n divides $b - a$.

   This is an equivalence relation, and so it partitions $\mathbb{Z}$ into disjoint classes. The class of $a \in \mathbb{Z}$, denoted by $\bar{a}$, is defined as
   $$\bar{a} = \{b \in \mathbb{Z} : b \equiv a \pmod{n}\}$$
   and it consists on the integers of the form $a + kn$ for $k \in \mathbb{Z}$. Thus, there are n different classes, $\bar{0}, \bar{1}, \dots, \overline{n-1}$, corresponding to the possible remainders of division by n.

   Define $\mathbb{Z}_n$ to be the set of all classes modulo n, that is, $\mathbb{Z}_n = \{\bar{a} : a \in \mathbb{Z}\} = \{\bar{0}, \dots, \overline{n-1}\}$. The operation in $\mathbb{Z}_n$ will be denoted by $+$, and defined as
   $$\bar{a} + \bar{b} = \overline{a + b}$$
   There is something to check for this to make sense. Namely, $\bar{a} + \bar{b}$ should depend only on the classes $\bar{a}$ and $\bar{b}$. That is, if we choose other representatives, a_1, b_1 of these classes ($\bar{a}_1 = \bar{a}$ and $\bar{b}_1 = \bar{b}$), we

need to show that $\overline{a_1+b_1} = \overline{a+b}$. That is easy to check from the definition of congruence mod n. We say that the operation is *well defined* by the formula in the right hand side.

This operation (that we call sum of classes, or just sum) makes $\mathbb{Z}_n$ into a group, with identity $\bar{0}$. The inverse of $\bar{a}$ is given by $\overline{-a}$.

3. Let X be a set, and let
$$S(X) = \{f : X \to X : f \text{ is bijective}\}$$
This is a group with composition of functions as product. That is, given $f, g \in S(X)$, their product is $f \circ g$, defined by $(f \circ g)(x) = f(g(x))$ for all $x \in X$. In fact, the axioms for a group are chosen to model this example. As a special case, when $X = \{1, \dots, n\}$ this is called the *symmetric group* on n letters, and written S_n. An element of S_n can be seen as an ordering (permutation) of the "letters" $1, \dots, n$. Exept when $n = 2$, this group is not commutative.

4. Let $K = \mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$. Let $GL_n(K)$ be the $n \times n$ matrices with non zero determinant. This is a group with the matrix multiplication.

The *order* of a group G, written $|G|$, is it's cardinality (number of elements, possibly infinite). For example, $|\mathbb{Z}_n| = n$, $|S_n| = n!$, $|\mathbb{Z}| = \infty$ (countable).

1.2 Subgroups, Generators

Let G be a group.

Definition A subset $H \subset G$ is a *subgroup* of G if it is nonempty and satisfies the following:

1. For $x, y \in H$, $xy \in H$.
2. For $x \in H$, $x^{-1} \in H$

That is to say, H is a subset that is closed under the group operations of G. In this case, the product of G can be restricted to a binary operation on H, and this gives a group structure on H. (Condition 2 is necessary for the restriction to be a group, for a counterexample look at $\mathbb{Z}^+ \subset \mathbb{Z}$). We write $H \leq G$.

Examples

1. Trivial subgroups. The group G always has $\{1\}$ and G as subgroups. (We will usually denote $\{1\}$ just by 1)

2. The subgroups of $\mathbb{Z}$ are all of the form
$$n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$$
for some integer $n \geq 0$.

3. Let $\mathrm{Isom}(\mathbb{R}^n)$ be the set of all isometries of $\mathbb{R}^n$, that is, maps from $\mathbb{R}^n$ to itself that preserve the distance. This is a subgroup of $S(\mathbb{R}^n)$.

4. (Dihedral groups) Let P_n be a regular polygon in $\mathbb{R}^2$, centered at the origin 0. Let D_{2n} be the set of all isometries of $\mathbb{R}^2$ that leave P_n invariant. (That is, the image of $x \in P_n$ is again in P_n). This is a subgroup of $\mathrm{Isom}(\mathbb{R}^2)$. It consists of the n rotations around 0 of angles $\frac{2\pi j}{n}$ for $j = 0, \dots, n-1$ (including the identity), and of the n reflections about axes determined by the origin and a vertex or edge middlepoint of P_n. Thus $|D_{2n}| = 2n$.

The following fact provides a criterion to check if some subset of G is a subgroup.

Proposition Let H be a nonempty subset of G. Then

1. H is a subgroup iff for all $x, y \in H$, $xy^{-1} \in H$.
2. If H is finite, then it is a subgroup iff for all $x, y \in H$, $xy \in H$.

Remark The intersection of subgroups is again a subgroup.

Definition Let $A \subseteq G$ be any subset. The *subgroup of G generated by A* is

$$\langle A \rangle = \bigcap \{H : A \subset H, H \leq G\}$$

So, $\langle A \rangle$ is the smallest subgroup containing A. If $H \leq G$, then a subset $A \subseteq H$ such that $H = \langle A \rangle$ is called a *generator* of H.

A group is *finitely generated* if it has a generator which is finite.

Proposition The elements of $\langle A \rangle$ are the $g \in G$ of the form $g = a_1^{\epsilon_1} \cdots a_k^{\epsilon_k}$ for $k \leq 0$, $a_1, \ldots, a_k \in A$ and $\epsilon_i = \pm 1$.

Examples

1. In $\mathbb{Z}$, the subgroup generated by $A \subset \mathbb{Z}$ is $d\mathbb{Z}$ where d is the greatest common divisor of the elements of A.
2. In D_{2n}, let r be the rotation of angle $\frac{2\pi}{n}$, and s be any reflection. Then r and s generate D_n. The elements of D_{2n} are r^j and $r^j s$ for $j = 0, \ldots, n-1$. Note that $sr = r^{-1}s$ and this allows us to compute products in this *normal form*.
3. $\mathbb{R}$ and $\mathbb{C}$ are not finitely generated (they are uncountable). $\mathbb{Q}$ is not finitely generated: Any finite subset $a_1 = p_1/q_1, \ldots a_k = p_k/q_k$ is contained in the subgroup $\frac{1}{m}\mathbb{Z}$ where $m = \text{lcm}(q_1, \ldots, q_k)$.

1.3 Homomorphisms, Isomorphisms

Homomorphisms are the maps between groups that preserve products.

Definition Let G and H be groups. A map $\varphi : G \to H$ is an *homomorphism* if for all $x, y \in G$, $\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$.

It is easy to check that in this case $\varphi(1_G) = 1_H$, and $\varphi(x^{-1}) = \varphi(x)^{-1}$. Also, that composition of homomorphisms is again an homomorphism.

Examples

1. The *trivial* map, $\varphi : G \to H$ s.t. $\varphi(g) = 1$.
2. The map $\varphi : \mathbb{Z} \to \mathbb{Z}_n$ s.t. $\varphi(a) = \bar{a}$.
3. The map $\varphi : \mathbb{Z} \to \mathbb{Z}$ s.t. $\varphi(k) = nk$, for a given $n \in \mathbb{Z}$.
4. The map $\varphi : D_{2n} \to \{1, -1\}$ sending each rotation to 1 and each reflection to -1.

Definition A map $\varphi : G \to H$ between groups is an *isomorphism* if it is an homomorphism and is bijective.

We say that the groups G and H are *isomorphic*, and write $G \cong H$, if there is an isomorphism $\varphi : G \to H$. Since an isomorphism φ is bijective, it has an inverse map φ^{-1}. Note that this map is also an homomorphism, ans thus an isomorphism. This, together with other easy observations, leads to the fact that the isomorphism relation between groups ($\cong$) is an equivalence on the class of all groups.

Isomorphic groups can be regarded as equal from the group theoretic point of wiev. They have the same group structure, but possibly different names for the elements and the operation. An isomorphism can be thought as just a change on these names.

Examples

1. The map $\varphi : \mathbb{R} \to \mathbb{R}^+$ s.t. $\varphi(x) = 2^x$ is an isomorphism between $(\mathbb{R}, +)$ and $(\mathbb{R}^+, \times)$.
2. If $f : X \to Y$ is a bijection, then $\varphi : S(X) \to S(Y)$ s.t. $\varphi(g) = f \circ g \circ f^{-1}$ is an isomorphism.
3. $D_6 \cong S_3$. Label the vertices of the triangle P_3 with the letters $1, 2, 3$. Each isometry in D_6 induces a permutation on the vertices, and hence on the corresponding labels. The same construction gives an isomorphism between D_{2n} and a subgroup of S_n.

Proposition If $\varphi : G \to H$ is an homomorphism, then

1. It's image $\text{Im}\varphi = \varphi(G)$ is a subgroup of H.
2. If $K \leq H$ then the inverse image $\varphi^{-1}(K)$ is a subgroup of G.

One special case is when $K = \{1\}$ above. The *kernel* of φ is

$$\ker\varphi = \varphi^{-1}(\{1\}) = \{g \in G : \varphi(g) = 1\}$$

Proposition An homomorphism φ is injective iff $\ker\varphi = \{1\}$.

1.4 Cyclic groups

Let g be an element of a group G, and n an integer. If $n > 0$, we define g^n to be the n-fold product $g \cdots g$. For $n < 0$, put $g^n = (g^{-1})^{-n}$, and finally, set $g^0 = 1$.

Proposition For G a group, $g \in G$ and $n, m \in \mathbb{Z}$, we have $g^n g^m = g^{n+m}$ and $(g^m)^n = g^{mn}$.

A group is called *cyclic* when it can be generated by a single element.

Proposition Let G be a cyclic group. Then

1. If $|G| = n$ then $G \cong \mathbb{Z}_n$
2. If $|G| = \infty$ then $G \cong \mathbb{Z}$

In order to show this, suppose $G = \langle b \rangle$, for some $b \in G$. Then we know that all the elements of G are of the form b^m, for $m \in \mathbb{Z}$.

If all the powers b^m are different from each other, then the map $\varphi : \mathbb{Z} \to G$ s.t. $\varphi(m) = b^m$ is an isomorphism. (It is an homomorphism by the previous proposition, and bijective by assumption).

On the other hand, suppose that $b^i = b^j$ for some $i \neq j$. Then $b^{i-j} = 1$ with $i - j \neq 0$. Put

$$n = \min\{m > 0 : b^m = 1\}$$

This minimum exists by the assumption of this case. It is then easy to check that $\psi : \mathbb{Z}_n \to G$ s.t. $\psi(\bar{m}) = b^m$ is a well defined map, and an isomorphism.

Now let G be any group, and $g \in G$. Define the *order* of g as $|g| = |\langle g \rangle|$. That is, $|g|$ is the minimum $n > 0$ for which $g^n = 1$, ahd $|g| = \infty$ if there is no such n.

1.5 Cosets, Index

Let G be a group and $H \leq G$ a subgroup of it. For $x \in G$ we denote

$$xH = \{xh : h \in H\}$$

A subset of that form, for some $x \in G$, is called a *right coset* of H. In the same fashion, a *left coset* of H is a subset of the form $Hx = \{hx : h \in H\}$ for $x \in G$.

Note that x belongs to xH and Hx, as $x = x1 = 1x$. Note also that H is both a right and left coset.

Proposition

1. Two right cosets xH and yH are either disjoint or equal.
2. All the right cosets of H have the same cardinality, that is, $|xH| = |H|$.

First we show that if $z \in xH$ then $zH = xH$. Since $z \in xH$, there is $h_0 \in H$ so that $z = xh_0$. Now, an element of zH has the form zh for $h \in H$. But then $zh = xh_0h$, which belongs to xH, since $h_0h \in H$. Thus $zH \subseteq xH$. Write $x = zh_0^{-1}$ and the same argument gives the other inclussion.

This gives us 1, for if x is in the intersection of xH and yH, then $xH = zH = yH$. To show 2, consider the map $f : H \to xH$ s.t. $f(h) = xh$. Check that it is a bijection.

The same is true for left cosets. By this proposition, the left (or right) cosets of H form a partition of G into disjoint subsets.

Proposition The number (cardinality) of left cosets of H is the same as that of right costets of H.

To see this, note that the inversion map $f : G \to G$ s.t. $f(g) = g^{-1}$ is a bijection (in fact $f \circ f = Id$). The image of a left coset under f is a right coset (and the other way around). Explicitely,

$$f(Hx) = \{(hx)^{-1} : h \in H\} = \{x^{-1}h^{-1} : h \in H\} = x^{-1}H$$

This gives a bijection between the set of right cosets of H and that of the left cosets.

The *index* of H in G is defined as the number of left (or right) cosets of H. It is denoted $[G : H]$. The first proposition then gives us the following.

Proposition (Lagrange's Theorem) For G a group and $H \leq G$, $|G| = [G : H]|H|$.

In the case when G is finite, we obtain that the order of a subgroup $H \leq G$ divides the order of G. This allows us to classify all groups without non trivial subgroups.

Theorem Let G be a non trivial group. Then G has no subgroups other than G and $\{1\}$ iff it is cyclic of prime order, that is iff $G \cong \mathbb{Z}_p$, for p prime.

By Lagrange's theorem, if $|G| = p$ prime, then the only subgroups are the trivial ones. For the other direction, let $a \in G$, $a \neq 1$. Then $\langle a \rangle$ is a subgroup of G, that is not $\{1\}$. Then $\langle a \rangle = G$, and G is cyclic. If G is infinite, then $G \cong \mathbb{Z}$, but we have seen that $\mathbb{Z}$ has non trivial subgroups, e.g. $2\mathbb{Z}$. So G is finite, $G \cong \mathbb{Z}_n$. If $n = st$ with $s, t > 1$ we can check that $\bar{s}$ generates a non trivial subgroup of $\mathbb{Z}_n$ (of order t). So the only possibility is $G \cong \mathbb{Z}_p$ with p prime.

A *set of representatives* for the right cosets of H in G is a set $S \subseteq G$ so that:

1. Every right coset of H can be written as xH for $x \in S$.
2. If $x, y \in S$, $x \neq y$ then $xH \neq yH$.

Such an S is formed by picking one element out of every coset of H (and any such choice of elements will give a different set of representatives). Note that $|S| = [G : H]$. The element $x \in S$ is called the *representative* of xH in S. Usually we will take 1 to be the representative of H. Of course, there is an analogous for left cosets.

Note that for any $H \leq G$, $|H| = [H : 1]$. Lagrange's theorem then becomes a particular case of the following

Proposition Let $K \leq H \leq G$. Then $[G : K] = [G : H][H : K]$.

Let S be a set of representatives of the right cosets of H in G, and T a set of representatives of those of K in H. So we have the disjoint unions

$$G = \bigcup\{xH : x \in S\} \qquad H = \bigcup\{yK : y \in T\}$$

Is then easy to see that

$$G = \bigcup\{xyK : (x, y) \in S \times T\}$$

And this union is disjoint: If $xyK = x_1y_1K$, then, since $xyK \subset xH$ and $x_1y_1K \subset x_1H$, we have $xH = x_1H$. So $x = x_1$ because S is a set of representatives. Now $xyK = xy_1K$. But then $yK = y_1K$ and so $y = y_1$. So, the products xy for $x \in S$, $y \in T$ form a set of representatives of the cosets of K in G.

2 Normal subgroups and Quotients

2.1 Conjugation, Normal subgroups

Let G be a group, and $g, h \in G$. We say that the element ghg^{-1} is the *conjugate* of h by g. If $H \leq G$ it's conjugate by g is defined as

$$gHg^{-1} = \{ghg^{-1} : h \in H\}$$

Observe that gHg^{-1} is also a subgroup. Moreover, the map $\alpha_g : G \to G$ s.t. $\alpha_g(x) = gxg^{-1}$ is a group isomorphism.

Definition Let $H \leq G$. We say that H is a *normal subgroup* of G, and write $H \lhd G$, if $gHg^{-1} = H$ for all $g \in G$.

Examples (and non-examples)

1. The subgroups $\{1\}$ and G are always normal.
2. Note that $ghg^{-1} = h$ iff h and g commute. So, in an abelian group every subgroup is normal.
3. In D_{2n} the subgroup $\langle r \rangle$ of all the rotations is normal. However, $\langle s \rangle$ for s a reflection is not normal.
4. Let $H \leq S_n$ be the subgroup of permutations that fix some $j \in \{1, \ldots, n\}$. Then H is not normal. gHg^{-1} is the subgroup that fixes $g(j)$.

Proposition The subgroup $H \leq G$ is normal iff every right coset xH is also a left coset Hy.

The direct is easy, check that $gHg^{-1} = H$ iff $gH = Hg$. For the reciprocal, let $x \in G$. Then there is a $y \in G$ with $xH = Hy$. So $x \in Hy$ and we get $Hx = Hy = xH$.

Proposition If $[G : H] = 2$ then H is normal.

We use the previous result: Let $x \in G$ not in H. Then G is partitioned as $G = H \cup xH = H \cup Hx$. Thus $xH = Hx$.

Remark The inclussion as normal subgroup is not transitive in general.

For an example let H be all the translations on $\mathbb{R}^2$, $G = \text{Isom}(\mathbb{R}^2)$ and $K = \langle t \rangle$ where t is some non trivial translation. Then $K \lhd H$ and $H \lhd G$ but K is not normal in G.

There is a deep relationship between normal subgroups and homomorphisms. The following results are the first steps in describing it.

Proposition If $\varphi : G \to H$ is an homomorphism then $\ker \varphi$ is a normal subgroup of G. More generally, the inverse image by φ of a normal subgroup of H is normal in G.

Let $K \lhd H$. If $g \in G$ and $k \in \varphi^{-1}(K)$ then we must check that $gkg^{-1} \in \varphi^{-1}(K)$. But $\varphi(gkg^{-1}) = \varphi(g)\varphi(k)\varphi(g)^{-1} \in K$ since K is normal in H.

Proposition Let $\varphi : G \to H$ be an homomorphism and $x, y \in G$. Then $\varphi(x) = \varphi(y)$ iff x and y belong to the same right (left) coset of $\ker \varphi$.

Put $N = \ker \varphi$. Then $\varphi(x) = \varphi(y)$ iff $\varphi(xy^{-1}) = 1$, iff $xy^{-1} \in N$, iff $Ny = Nx$.

2.2 Quotient group

Let G be a group, and $N \lhd G$ a normal subgroup. We define G/N as the set of right cosets of N. That is

$$G/N = \{xN : x \in G\}$$

This can be done (and will be useful) for any subgroup, regardless of if it is normal. But in the case when N is normal, there is a natural product on G/N that makes it a group. We define

$$xN \cdot yN = xyN$$

We need to check this is well defined, as well as the axioms for a group.

To see that it is well defined, pick some other representatives for the cosets xN and yN. They are of the form xh_1 and yh_2 for $h_1, h_2 \in N$. Now we have to show that xh_1yh_2 is in the coset xyN. But since N is normal, $Hy = yH$ and there is some $\hat{h}_1 \in N$ such that $h_1y = y\hat{h}_1$. So $xh_1yh_2 = xy\hat{h}_1h_2$ that belongs to xyH. The axioms for a group are checked easily, and the next result is just an inmediate consequence.

Proposition The map $\pi : G \to G/N$ s.t. $\pi(x) = xN$ is an homomorphism, and it's kernel is N.

The map π is called *canonical projection* onto the quotient. Thus, we have shown that the normal subgroups of G are exactly the kernels of the homomorphisms from G.

Example $\mathbb{Z}_n$ is the quotient of $\mathbb{Z}$ by the normal subgroup $n\mathbb{Z}$.

Note that if $H \leq G$ and $N \leq H$, then N is normal in H and the quotient H/N is naturally included in G/N. In fact $\pi(H) = H/N$ and it consists on those cosets of N on G that are contained in H. On the other hand, if $K \leq G/N$ then $\pi^{-1}(K)$ is a subgroup of G that contains N. This describes the correspondence in the next proposition.

Proposition Let $N \lhd G$. There is a bijection between the subgroups of G that contain N and the subgroups of G/N. Moreover, this bijection preserves normality and index (i.e. $H \lhd G$ iff $H/N \lhd G/N$, and $[G : H] = [G/N : H/N]$).

Example The subgroups of $\mathbb{Z}_n$ are in 1 to 1 correspondence with the divisors of n. If $n = ts$, then $\langle \bar{t} \rangle \leq \mathbb{Z}_n$ is isomorphic to $\mathbb{Z}_s$ and it's index is t.

2.3 Universal property, Isomorphism theorems

Proposition(Universal property for quotients) Let $N \lhd G$ and $\pi : G \to G/N$ the canonical projection. Let $\varphi : G \to H$ be an homomorphism with $N \subseteq \ker\varphi$. Then there is a unique homomorphism $\hat{\varphi} : G/N \to H$ such that $\varphi = \hat{\varphi} \circ \pi$. Moreover $\mathrm{Im}\hat{\varphi} = \mathrm{Im}\varphi$ and $\ker\hat{\varphi} = \ker\varphi/N$.

In that situation, we say that φ *factors* through π. It is clear that if an homomorphism factors through π, then it's kernel must contain N. The proposition gives a reciprocal to that fact.

Uniqueness is easy, if such $\hat{\varphi}$ exists, then it must be $\hat{\varphi}(xN) = \varphi(x)$. For existence, define $\hat{\varphi}$ by the last formula, and check it is well defined and an homomorphism.

The following is the special case when $N = \ker\varphi$.

Proposition(First isomorphism theorem) Let $\varphi : G \to H$ be an homomorphism. Then $\mathrm{Im}\varphi \cong G/\ker\varphi$.

A surjective homomorphism is called an *epimorphism* and an injective one is called a *monomorphism* or an *embedding*. By this theorem, every epimorphism $\varphi : G \to H$ factors as a canonical projection $\pi : G \to G/\ker\varphi$ followed by an isomorphism.

Example The determinant $\det : GL_n(K) \to K^*$ is an homomorphism. So $SL_n(K) = \{A \in GL_n(K) : \det A = 1\}$ is a normal subgroup, and $GL_n(K)/SL_n(K) \cong K^*$.

For $H, K \leq G$ we define $HK = \{hk : h \in H, k \in K\}$. It contains both H and K, and it is contained in $\langle H, K \rangle$, the subgroup generated by both of them. It is a subgroup iff $HK = KH$, and in that case it is equal to $\langle H, K \rangle$.

Lemma If $H \lhd G$ and $K \leq G$, then

1. $HK = KH$ and thus it is a subgroup.
2. $H \cap K \lhd K$

Proposition(Second isomorphism theorem) Let $H \lhd G$ and $K \leq G$. Then $K/H \cap K \cong HK/H$.

Consider the map $\varphi : K \to HK/H$ that consists on the inclussion $K \hookrightarrow HK$ followed by the quotient projection $HK \to HK/H$. It is surjective and it's kernel is $H \cap K$. So we use the first isomorphism theorem.

Proposition(Third isomorphism theorem) Let $N \lhd G$, and $H \lhd G$ with $N \subseteq H$. Then $(G/N)/(H/N) \cong G/H$.

Begin with the projection $\phi : G \to G/H$. Since $N \subseteq H$, the universal property gives a map $\hat{\phi} : G/N \to G/H$ which is also surjective and has kernel H/N. Then use the first isomorphism theorem.

2.4 Direct products and sums

Let G and H be groups. The *direct product* of G and H is $G \times H$ with the operation

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 g_2, h_1 h_2)$$

It is easy to verify the axioms, and to see that $G \times H \cong H \times G$. Also, we can think of G as a subgroup of $G \times H$, as $G \times \{1\}$. The same goes for H.

There are projections of the product onto the factors, as $\pi_1 : G \times H \to G$ s.t. $\pi_1(g, h) = g$. The kernel is $\ker \pi_1 = H$, so $H \lhd G \times H$. The situation with π_2 is symmetric.

Proposition Let G be a group. If there are $H, K \lhd G$ with $G = HK$ and $H \cap K = 1$ then $G \cong H \times K$.

If $h \in H$ and $k \in K$, then $hkh^{-1}k^{-1} = (hkh^{-1})k^{-1}$ is in K, because K is normal. By the same reasoning it belongs to H. So $hkh^{-1}k^{-1} = 1$ and $hk = kh$. Now define the map $\varphi : H \times K \to G$ s.t. $\varphi(h, k) = hk$. It is an homomorphism because of what we just proved. Since $G = HK$, it is surjective. And if $(h, k) \in \ker \varphi$, then $hk = 1$. So $h = k^{-1} \in H \cap K = 1$ and $(h, k) = (1, 1)$. Thus φ is an isomorphism.

We can take products with an arbitrary number of factors. Let G_i be groups, for $i \in I$ an index set. Then put

$$\Pi_{i \in I} G_i = \{f : I \to \cup_i G_i : f(i) \in G_i\}$$

We use to represent an element f of this product as $(g_i)_{i \in I}$ where $g_i = f(i) \in G_i$. The group operation is given by

$$(g_i)_{i \in I} (h_i)_{i \in I} = (g_i h_i)_{i \in I}$$

The *direct sum* of the groups G_i is the subgroup of $\Pi_i G_i$ consisting of all the elements $(g_i)_{i \in I}$ for which $g_i = 1$ for all but finitely many i. It is denoted $\oplus_i G_i$.

Proposition Let G be a group, and $H_i \leq G$ for $i \in I$. If

1. $H_i \lhd G$ for all i
2. $\cup_i H_i$ generates G
3. $H_i \cap \langle \cup_{j \neq i} H_j \rangle = 1$ for all i

Then $G \cong \oplus_i G_i$.

Back to the case with two factors, suppose G is a group, $H \lhd G$ and $K \leq G$ not necessarily normal. Also assume that $G = HK$ and $H \cap K = 1$. We say that G decomposes as a *semidirect product* of H and K. As in the previous situation, we can write the elements of G in a unique normal form hk for $h \in H$ and $k \in K$. This time the operation depends on the particular group. We also have a projection $G \to K$ with kernel H. But this time there is no projection onto the H factor, unless K is normal (and we would have a direct product).

Examples

1. $\mathbb{Z}$ does not decompose into a product. That is because if $H, K \leq \mathbb{Z}$ are non trivial, then $H \cap K \neq 1$.
2. If $n = st$ with $(s, t) = 1$ then $\mathbb{Z}_n \cong \mathbb{Z}_s \times \mathbb{Z}_t$.
3. Let $A \subset \{1, \ldots, n\}$, $|A| = k$. Let $G = \{g \in S_n : g(A) = A\}$. Then $G \cong S_k \times S_{n-k}$.
4. D_{2n} is a semidirect product of $H = \langle r \rangle$ and $K = \langle s \rangle$. It is not a direct product unless $n = 2$.

3 Group Actions

3.1 Actions and related concepts

Let G be a group and X a set.

Definition A *left action* of G on X is a map $\cdot : G \times X \to X$ (denoted by $\cdot(g,x) = g \cdot x$) satisfying

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

There is an analogous definition for right actions. We will just use the term *action*, and it will be clear from the context wether we refer to a left or a right action. We also say that G *acts* on X, and denote an action by $G \curvearrowright X$. As done with the group product, write gx for $g \cdot x$.

Remark If we have a left action $G \curvearrowright X$, then we can define a right action as $x \cdot g = g^{-1}x$ for $g \in G$, $x \in X$. Thus right and left actions are equivalent objects.

Note that an element $g \in G$ defines a map $f_g : X \to X$ given by $f_g(x) = gx$. This map is a bijection, with inverse $f_{g^{-1}}$. The axioms for an action give us $f_g \circ f_h = f_{gh}$ and $f_1 = Id_X$. Thus an action of G on X gives rise to an homomorphism $h : G \to S(X)$ given by $h(g) = f_g$. Conversely, if $h : G \to S(X)$ is an homomorphism, then $g \circ x = (h(g))(x)$ defines an action. So we obtain the following.

Proposition There is a correspondence between the actions of G on X and the homomorphisms $h : G \to S(X)$.

Examples

1. All the groups we have given as subgroups of $S(X)$ clearly act on X. Some important cases are S_n acting on $\{1, \ldots, n\}$, $\mathrm{Isom}(\mathbb{R}^n)$ acting on $\mathbb{R}^n$ and $GL_n(K)$ acting on K^n. Also D_{2n} acting on P_n.
2. Suppose G acts on X and Y is any other set. Then we can define an action of G on Y^X, the set of functions from X to Y, by the formula $(g \cdot f)(x) = f(g^{-1}x)$ for $g \in G$, $f \in Y^X$, $x \in X$. For example, $\mathbb{R}$ acts on the functions $f : \mathbb{R} \to \mathbb{R}$ by translation of the argument.
3. S_n acts on $K[x_1, \ldots, x_n]$, the polynomials on n variables over K. If $P \in K[x_1, \ldots, x_n]$ and $\sigma \in S_n$ then σP is given by
$$(\sigma P)(x_1, \ldots, x_n) = P(x_{\sigma(1)}, \ldots, x_{\sigma(n)})$$
4. $GL_2(\mathbb{C})$ acts on $\mathbb{C} \cup \{\infty\}$ by *Moebius transformations*, that is
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az+b}{cz+d}$$
when $z \in \mathbb{C}$, and the limit extension for ∞ (i.e. $g \cdot \infty = a/c$ and $g \cdot (-d/c) = \infty$).

Let $G \curvearrowright X$ be an action.

Definition For $x \in X$, the *orbit* of x under the action is
$$G \cdot x = O(x) = \{gx : g \in G\}$$

Note that x and y are in the same orbit iff there is $g \in G$ s.t. $gx = y$. It is easy to check that two orbits are either the same or disjoint. So they form a partition of X. An action is called *transitive* if there is only one orbit, i.e. if $O(x) = X$ for some (and all) $x \in X$.

Given an orbit $Y = O(x) \subset X$, we can restrict the action of G on X to an action $G \curvearrowright Y$ which is transitive.

Definition For $x \in X$, the *stabilizer* of x is
$$G_x = \mathrm{Stab}_G(x) = \{g \in G : gx = x\}$$

The stabilizer of a point in X is a subgroup of G. If we think of the action as an homomorphism $h : G \to S(X)$ then we see that

$$\ker h = \bigcap_{x \in X} G_x$$

This is called the *kernel* of the action. An action is *faithful* or *effective* if it's kernel is 1.

Note that any action $h : G \to S(X)$ can be reduced to an effective action of $G/\ker h$ on X. This is given by the universal property of the quotient.

Examples

1. The action of any subgroup of $S(X)$ on X is clearly effective. The full group $S(X)$ acts transitively and the stabilizer of x is isomorphic to $S(X \setminus \{x\})$.

2. $\mathrm{Isom}(\mathbb{R}^n)$ acts transitively on $\mathbb{R}^n$, and the stabilizer of the origin is $O(n)$.

3. $GL_n(\mathbb{R}) \curvearrowright \mathbb{R}^n$ has two orbits: $\{0\}$ and it's complement. The orbits of $O(n)$ are $\{0\}$ and the spheres with center 0.

4. In $D_{2n} \curvearrowright P_n$ we have infinitely many orbits. $\mathrm{Stab}(0) = D_{2n}$. If $x \neq 0$ but is in the axis of a reflection s, then $\mathrm{Stab}(x) = \{1, s\}$. For any other $x \in P_n$, $\mathrm{Stab}(x) = 1$.

5. The action of $GL_2(\mathbb{C})$ on $\mathbb{C} \cup \{\infty\}$ is not effective. It's kernel consists of the matrices of the form λId for $\lambda \in \mathbb{C}^*$. It is transitive and the stabilizer of ∞ is the subgroup of upper triangular matrices.

Proposition Let $g \in G$ and $x \in X$. Then $\mathrm{Stab}_G(gx) = g\mathrm{Stab}_G(x)g^{-1}$.

Indeed, if $h \in G$ then $hgx = gx$ iff $g^{-1}hgx = x$. Hence $h \in G_{gx}$ iff $g^{-1}hg \in G_x$ iff $h \in gG_xg^{-1}$.

For $g \in G$ we denote $X^g = \{x \in X : gx = x\}$. Thus $x \in X^g$ iff $g \in G_x$. The *support* of $g \in G$ is the complement of X^g, that is $\mathrm{supp}(g) = \{x \in X : gx \neq x\}$.

If $A \subseteq G$ we write $X^A = \cap_{g \in A} X^g$, the points fixed by every element in A. Note that $X^A = X^H$ where $H = \langle A \rangle$.

Proposition Let $g, h \in G$. Then $\mathrm{supp}(ghg^{-1}) = g \cdot \mathrm{supp}(h)$, or equivalently $gX^h = X^{ghg^{-1}}$.

This is a consequence of the previous one. We have $x \in X^{ghg^{-1}}$ iff $ghg^{-1} \in G_x$. And if we put $x = gy$, this is equivalent to $h \in G_y$, and hence to $y \in X^h$. Recalling that $x = gy$, that is to say $x \in gX^h$.

In particular, if g commutes with h then the action of g leaves invariant the support of h.

Definition Let $G \curvearrowright X$ and $G \curvearrowright Y$ be two actions of the same group G. A map $f : X \to Y$ is *equivariant* if for all $x \in X$, $g \in G$ it satisfies $f(gx) = gf(x)$.

Two actions of G are *equivalent* if there is an equivariant bijection between them. This is indeed an equivalence relation.

Proposition Let $f : X \to Y$ be equivariant. Then

1. f takes orbits to orbits, i.e. $f(O(x)) = O(f(x))$.

2. G_x fixes $f(x)$, i.e. $G_x \subseteq G_{f(x)}$. If f is an equivalence then $G_x = G_{f(x)}$.

3.2 Regular representation

Let G be a group. For $g \in G$ we define maps $L_g, R_g : G \to G$ by $L_g(h) = gh$ and $R_g(h) = hg$. It is clear that they are bijections. Also $L_gL_h = L_{gh}$ and $R_gR_h = R_{hg}$.

By these properties, the map $L : G \to S(G)$ taking g to L_g is a right action of G on itself. It is called the *left regular representation* or the action by *left translations*. Analogously, the right translations R_g define a right action of G on itself, that is named accordingly.

Observe that $L_gR_h = R_hL_g$ for any $g, h \in G$.

The next result shows that any group defined in the abstract sense is isomorphic to a group of transformations, i.e. a subgroup of $S(X)$ for some set X.

Proposition(Cayley's theorem) Every group G embedds as a subgroup of $S(G)$.

We need to see that the homomorphism $L : G \to S(G)$ is injective. But if g is in the kernel, i.e. $L_g = Id_G$, we get $g = g1 = L_g(1) = 1$.

Given a subgroup $H \leq G$ we can act by left translation on the left cosets of H. Define $G \times G/H \to G/H$ by $g \cdot xH = gxH$. It is easy to check it is an action.

Facts

1. G acts transitively on G/H.
2. The stabilizer of the coset xH is xHx^{-1}.
3. The kernel of the action is $\bigcap\{xHx^{-1} : x \in G\}$, that is the maximal subgroup of H that is normal in G.

Suppose we have a transitive action $G \curvearrowright X$. Pick $x \in X$ and let $H = G_x$ be it's stabilizer. Then we have a surjective map $f : G \to X$ s.t. $f(g) = gx$. If we put the left translation action on G then f is equivariant. Also note that f is constant on the left cosets of H. So the function $\hat{f} : G/H \to X$ s.t. $\hat{f}(gH) = gx$ is well defined. And it is easy to see it is bijective and equivariant. Thus we obtain the following.

Proposition(Orbit - Stabilizer theorem) Let $G \curvearrowright X$ be an action.

1. If it is transitive, then it is equivalent to the action by left translations on G/G_x for any $x \in X$.
2. For $x \in X$, we have $|O(x)| = [G : G_x]$.

The following is an example of how we can use actions of G to study the structure of G.

Theorem Let G be a finite group. Let p be the smallest prime dividing $|G|$. Then every subgroup of index p in G is normal in G.

Let $H \leq G$, with $[G : H] = p$. Let K be the kernel of the action of G on G/H by left translations. Then G/K acts faithfully on G/H, and since $|G/H| = p$ this implies that G/K embedds as a subgroup of S_p. By Lagrange's theorem then $|G/K| = [G : K]$ must divide $p!$. On the other hand, $[G : K]$ must also divide $|G|$. Now, p is the smallest prime factor of $|G|$ and the largest of $p!$ (and it's exponent is 1). So $[G : K] = p$, and then $p = [G : K] = [G : H][H : K] = p[H : K]$. So $[H : K] = 1$ and $H = K$.

3.3 Action by conjugation

Now we consider another action of a group G on itself. For $g \in G$ consider the map $\alpha_g : G \to G$ s.t. $\alpha_g(h) = ghg^{-1}$. Then α_g is a group isomorphism for each g, and the map $G \to S(G)$ taking g to α_g is a group action. This is called *action by conjugation*. Note that $\alpha_g = L_g R_{g^{-1}}$.

The orbits under this action are called *conjugacy classes*. Note that in this action g is fixed by h iff g and h commute. The stabilizer of $g \in G$ is called the *centralizer* of g in G, and denoted

$$C_G(g) = \{h \in G : hg = gh\}$$

By the orbit-stabilizer theorem, the number of elements conjugate to g is the index $[G : C_G(g)]$.

More generally, the centralizer of $H \leq G$ is

$$C_G(H) = \{g \in G : gh = hg \text{ for all } h \in H\}$$

The *center* of G is the set of fixed points for this action, $Z(G) = C_G(G)$. Note that $Z(G)$ is abelian and normal in G. The center is also the kernel of the action by conjugation.

The orbit-stabilizer theorem gives inmediately the next result for finite groups.

Proposition(Class equation) Let G be a finite group, and $x_1, \ldots, x_k$ be representatives for the conjugacy classes of G not in $Z(G)$. Then

$$|G| = |Z(G)| + \sum_{i=1}^{k} [G : C_G(x_i)]$$

It is now an easy consequence that if $|G| = p^n$ for p prime (G is a p-group) then $Z(G) \neq 1$.

We can also act by conjugation on the set of subgroups of G. That is, if $H \leq G$ define $g \cdot H = gHg^{-1}$. Note that a subgroup is fixed under this action iff it is normal. For any $H \leq G$, it's stabilizer is called *normalizer* of H in G. It is written

$$N_G(H) = \{g \in G : gHg^{-1} = H\}$$

The normalizer $N_G(H)$ clearly contains H, and is the biggest subgroup of G in which H is normal. As above, the number of different conjugates of H is $[G : N_G(H)]$.

It is clear that $C_G(H) \leq N_G(H)$. By its definition, the formula $g \cdot h = ghg^{-1}$ also defines an action of $N_G(H)$ on H. It's kernel is $C_G(H)$. In particular $C_G(H) \lhd N_G(H)$. Also note that $H \cap C_G(H) = Z(H)$.

Examples

1. For D_{2n} there are two cases. When n is even, $n = 2k$ then $Z(D_{2n}) = \{1, r^k\}$. The conjugacy class of r^j for $0 < j < n$, $j \neq k$ is $\{r^j, r^{-j}\}$. For n odd, the former is the case for any $0 < j < n$, and the center is trivial. On the other hand, when n is odd the conjugacy class of a reflection s consists of all reflections of D_{2n}. And when n is even, reflections are divided in those whose axes pass through vertices ($r^j s$ for j even) and those with axes passing through edge middlepoints. These are the conjugacy classes.

2. From the first example, if n is odd or $n = 2k$ and $j \neq k$ then $C_{D_{2n}}(r^j) = \langle r \rangle$. For s a reflection, $C_{D_{2n}}(s)$ is generated by s and $Z(D_{2n})$. It has order either 2 or 4.

3. The center of $GL_n(\mathbb{C})$ is $\{\lambda Id : \lambda \in \mathbb{C}\}$.

4 Automorphisms

4.1 Group of automorphisms

Let G be a group. An isomorphism from G to itself is called an *automorphism* of G. The set of all automorphisms

$$\mathrm{Aut}(G) = \{\varphi : G \to G : \varphi \text{ is an automorphism}\}$$

is a group under composition (thus a subgroup of $S(G)$).

For $g \in G$ we defined $\alpha_g : G \to G$ s.t. $\alpha_g(x) = gxg^{-1}$. We have seen they are automorphisms. They are called *inner automorphisms*. Since the map $G \to \mathrm{Aut}(G)$ sending g to α_g is an homomorphism, the inner automorphisms form a subgroup of $\mathrm{Aut}(G)$. It will be denoted $\mathrm{Inn}(G)$.

Note that $\mathrm{Inn}(G) \cong G/Z(G)$, since $Z(G)$ is the kernel of the conjugation action. We can also see that $\mathrm{Inn}(G)$ is normal in $\mathrm{Aut}(G)$, since if $\varphi \in \mathrm{Aut}(G)$ and $g \in G$ then $\varphi\alpha_g\varphi^{-1} = \alpha_{\varphi(g)}$. The quotient

$$\mathrm{Out}(G) = \mathrm{Aut}(G)/\mathrm{Inn}(G)$$

is called the group of *outer automorphisms* of G.

Examples

1. If G is abelian, then $\mathrm{Inn}(G) = 1$.

2. $\mathrm{Aut}(\mathbb{Z}^n) = GL_n(\mathbb{Z})$ that consists on the $n \times n$ matrices of integer coefficients and determinant ± 1. To see it, notice that an automorphism must take the standard basis of $\mathbb{Z}^n$ to another basis.

3. For p prime, $\mathrm{Aut}((\mathbb{Z}_p)^n) = GL_n(\mathbb{Z}_p)$. Note that $(\mathbb{Z}_p)^n$ is a vector space over $\mathbb{Z}_p$ and that a group automorphism must be linear.

4. $\mathrm{Aut}(D_6) = \mathrm{Inn}(D_6) \cong D_6$. Since $Z(D_6) = 1$, $\mathrm{Inn}(D_6) \cong D_6$. If φ is an automorphism, it must preserve the subgroup $\langle r \rangle = \{1, r, r^{-1}\}$ since $|\varphi(r)| = |r| = 3$. Thus the image of a reflection must also be a reflection. Since $D_6 = \langle r, s \rangle$, the automorphism φ is determined by the images of r and s. Then we can see that $|\mathrm{Aut}D_6| \leq 6$, and since $|\mathrm{Inn}(D_6)| = 6$ they must be equal.

4.2 Semidirect products

If H and K are groups, an action $K \to S(H)$ is an *action by automorphisms* if it's image is contained in $\mathrm{Aut}(H)$. For example if H is a normal subgroup of G, then the action of G on H by conjugation is an action by automorphisms.

If we have an action by automorphisms $\varphi : K \to \mathrm{Aut}(H)$, we can define an operation in $H \times G$ by

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1(h_1 \cdot_\varphi g_2), h_1h_2)$$

This gives a group structure, that we will denote $H \rtimes_\varphi K$.

As in the direct product, the inclussion maps of the factors $H \to H \rtimes_\varphi K$ and $K \to H \rtimes_\varphi K$ are homomorphisms. So H and K can be regarded as subgroups of $H \rtimes_\varphi K$. Also, these subgroups generate $H \rtimes_\varphi K$. The projection onto the second factor (K) is an homomorphism, and so H (it's kernel) is normal.

Notice that for $k \in K$, $h \in H$ we have

$$(1, k)(h, 1)(1, k^{-1}) = (k \cdot_\varphi h, 1)$$

So the action φ of K in H is realized as an action by conjugation in the group $H \rtimes_\varphi K$.

Proposition Let G be a group, and $H, K \leq G$ such that

1. $H \lhd G$

2. $G = \langle H, K \rangle$

3. $H \cap K = 1$

Then $G \cong H \rtimes K$, for the restriction of the action by conjugation.

Unless φ is trivial (i.e. $\text{Im}\varphi = \{Id_H\}$), K is not normal in $H \rtimes_\varphi K$. If it were normal, then $H \rtimes_\varphi K$ would be isomorphic to the direct product $H \times K$, where the conjugation action of K on H is trivial.

Examples

1. $D_{2n} \cong \mathbb{Z}_n \rtimes \mathbb{Z}_2$. If $\mathbb{Z}_2 = \{1, s\}$, it acts on $\mathbb{Z}_n$ by $s \cdot g = g^{-1}$.
2. The action of $\mathbb{Z}_2$ just given works for every abelian group (because $(gh)^{-1} = g^{-1}h^{-1}$). The infinite dihedral group $D_\infty = \mathbb{Z} \rtimes \mathbb{Z}_2$ is a special case of this. It can also be given as the subgroup of Isom($\mathbb{R}$) that leaves $\mathbb{Z}$ invariant.
3. For any G, we can form $G \rtimes \text{Aut}(G)$ by the obvious action. We see that every automorphism of G is a conjugation in a bigger group that contains G as a normal subgroup.
4. $\text{Isom}(\mathbb{R}^n) = \mathbb{R}^n \rtimes O(n)$, where R^n is regarded as the group of translations. The action of $O(n)$ on $\mathbb{R}^n$ is the usual one.

4.3 Characteristic subgroups

Let G be a group and H a subgroup of G. We say that H is a *characteristic* subgroup of G if $\varphi(H) = H$ for all $\varphi \in \text{Aut}(G)$. Note that a characteristic subgroup is also normal.

As opposed to the situation with normal subgroups, the relation of inclussion as characteristic subgroup is transitive.

Proposition Let $K \leq H \leq G$

1. If K is characteristic in H and H is characteristic in G then K is characteristic in G.
2. If $K \lhd H \lhd G$ and K is characteristic in H, then $K \lhd G$.

For (1), note that every automorphism of G restricts to an automorphism of H and hence leaves K invariant. For (2), do the same for a conjugation.

Examples

1. The trivial subgroups, 1 and G.
2. In a cyclic group every subgroup is characteristic.
3. In D_{2n} for $n > 2$, the subgroup of rotations is characteristic. This is because the generators of this subgroup are the only elements of order n.
4. The characteristic subgroups of $\mathbb{Z}^n$ are those of the form $k\mathbb{Z}^n$ for $k \in \mathbb{Z}$.
5. The center $Z(G)$ is always characteristic in G.
6. The *commutator* subgroup of G is
$$G' = \langle [x, y] : x, y \in G \rangle$$
where $[x, y] = xyx^{-1}y^{-1}$. Then G' is characteristic, because $\varphi([x, y]) = [\varphi(x), \varphi(y)]$ for any homomorphism φ.

   So if we take iterated commutator subgroups $G^{(n)} = (G^{(n-1)})'$, we have that $G^{(n)} \lhd G$ for every n.

5 Permutation groups

5.1 Cycle decomposition

We will use the notation $[n] = \{1, \dots, n\}$. An element of S_n is called a *permutation*.

Definition A permutation $\sigma \in S_n$ is a *cycle* of length k if there exist $x_0, \dots, x_{k-1} \in [n]$ such that $\sigma(x_i) = x_{i+1}$ for $i \in \mathbb{Z}_k$, and $\sigma(x) = x$ for every other $x \in [n]$.

In this case we will write $\sigma = (x_1, \dots, x_k)$. It is clear that a cycle of length k has order k. Also

$$(x_1, \dots, x_k)^{-1} = (x_k, \dots, x_1)$$

A cycle of length 2 is called a *transposition*. Note that if σ and τ are two permutations with disjoint support then $\sigma\tau = \tau\sigma$.

Proposition Let σ be a permutation. Then σ can be written as a product of cycles of disjoint support. I.e. $\sigma = \tau_1 \cdots \tau_k$ where each τ_i is a cycle, and $\mathrm{supp}(\tau_i) \cap \mathrm{supp}(\tau_j) = \emptyset$ for $i \neq j$. This decomposition is unique, aside from the order of the factors.

This decomposition corresponds to the orbits of $\langle \sigma \rangle$ acting on $[n]$.

We will abreviate this as *cycle decomposition*. It gives us the order of a permutation, if $\sigma = \tau_1 \cdots \tau_k$ is the cycle decomposition, then $|\sigma| = \mathrm{lcm}(|\tau_1|, \dots, |\tau_k|)$. And $\sigma^{-1} = \tau_1^{-1} \cdots \tau_k^{-1}$ is the cycle decomposition of the inverse.

If we have a cycle $(x_1, \dots, x_k)$ and any permutation σ then

$$\sigma(x_1, \dots, x_k)\sigma^{-1} = (\sigma(x_1), \dots, \sigma(x_k))$$

This can be used to describe the conjugacy classes in S_n.

Proposition Two elements $\sigma, \tau \in S_n$ are conjugate iff their cycle decompositions have the same structure. That is, if they can be written as

$$\sigma = \sigma_1 \cdots \sigma_k \qquad \tau = \tau_1 \cdots \tau_k$$

with $|\sigma_i| = |\tau_i|$ for each i.

5.2 Alternating group

A cycle decomposes as

$$(x_1, \dots, x_k) = (x_1, x_k) \cdots (x_1, x_2)$$

So we obtain the following.

Proposition S_n is generated by the transpositions (i, j), $i < j$.

So every permutation σ is a product of transpositions $\sigma = t_1 \cdots t_m$. This factorization is not unique in general, but we shall show that the parity of the number of factors (i.e. m) is the same for any such decomposition.

Definition The *alternating group* is the set of permutations that are a product of an even number of transpositions. It is denoted by A_n.

It is clear that it is a subgroup. Recall the action of S_n on $\mathbb{Z}[x_1, \dots, x_n]$ by permutation of the variables. Let

$$P = \Pi_{i<j}(x_i - x_j)$$

Observe that for $\sigma \in S_n$, we have that $\sigma \cdot P$ is either P or $-P$. So we can define $\epsilon : S_n \to \{1, -1\}$ by

$$\sigma \cdot P = \epsilon(\sigma)P$$

Proposition $\epsilon : S_n \to \{1, -1\}$ is a surjective homomorphism and it's kernel is A_n.

It is an homomorphism because $(\sigma\tau) \cdot P = \sigma \cdot (\tau \cdot P)$. We see that $\epsilon((1,2)) = -1$ because it flips $(x_1 - x_2)$ but preserves the order in every other factor $(x_i - x_j)$ with $i < j$, $2 < j$. Since every transposition (i,j) is conjugate to $(1,2)$, we see that $\epsilon((i,j)) = -1$. Thus $\epsilon(\sigma) = (-1)^m$ where σ can be written as a product of m transpositions. This gives $\ker \epsilon = A_n$.

So A_n is a normal subgroup of index 2. If σ is any permutation and (i,j) is a transposition, then exactly one of σ, $(i,j)\sigma$ is in A_n.

Thus $\{1, (i,j)\}$ is a set of representatives for the cosets of A_n, and since it forms a subgroup, we get that S_n splits as a semidirect product $S_n = A_n \rtimes \mathbb{Z}_2$.

Definition A group action $G \curvearrowright X$ induces an action of G on the cartesian product X^k by $g \cdot (x_1, \ldots, x_k) = (gx_1, \ldots, gx_k)$. The action $G \curvearrowright X$ is *k-transitive* if the induced action on X^k is transitive.

It is immediate that k-transitivity implies l-transitivity for $l \leq k$. The action of S_n on $[n]$ is n-transitive, but no proper subgroup can act n-transitively.

Proposition A_n, $n \geq 3$, acts $(n-2)$-transitively on $[n]$.

Let $\{x_1, \ldots, x_{n-2}\}$ be an ordered $(n-2)$-subset of $[n]$. Let $\{x_{n-1}, x_n\}$ be it's complement, in some order. Then the formula $\sigma(i) = x_i$ defines a permutation taking $\{1, \ldots, n-2\}$ to the desired ordered subset. But $(x_{n-1}, x_n)\sigma$ also satisfies this property, and one of those must be in A_n.

It doesn't act $(n-1)$-transitively, for that would imply n-transitivity.

5.3 Simplicity of A_n, $n \neq 4$

A group G is *simple* if it has no normal subgroups other than 1 and G.

The first cases, $A_2 = 1$, $A_3 \cong \mathbb{Z}_3$ are simple. But A_4 is not simple, let

$$K = \{Id, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$$

It is contained in A_4, and it can be checked to be a subgroup. It is normal, because it consists on Id and all the products of two disjoint transpositions. So $K \lhd A_4$.

Now we consider the general case, $n \geq 5$.

Proposition A_n, $n \geq 3$, is generated by the cycles of length 3.

Note that since a cycle (a,b,c) has order 3, $\epsilon((a,b,c)) = 1$. So (a,b,c) belongs to A_n. It is clear that A_n is generated by the products of two transpositions, i.e. the elements of the form $(a,b)(c,d)$. When they are overlapping, say $a = d$ we get $(a,b)(a,c) = (a,c,b)$. And when they are disjoint, we reduce it to the previous case: $(a,b)(c,d) = (a,b)(b,c)(b,c)(c,d)$, that is a product of pairs of overlapping transpositions.

Theorem A_n is simple for $n \geq 5$.

The proof puts together all the ideas on this section. First, by the conjugation formula

$$\sigma(a,b,c)\sigma^{-1} = (\sigma(a), \sigma(b), \sigma(c))$$

and since A_n acts $(n-2)$-transitively, $n-2 \geq 3$ we see that the RHS can be any cycle of length 3, while σ can be chosen in A_n. So all cycles of length 3 are conjugate in A_n.

Now let $G \lhd A_n$, $G \neq 1$. If G contains a cycle of length 3, then it contains all its conjugates by elements of A_n. But these are all the length 3 cycles, and they generate A_n. So $G = A_n$.

Thus, we must check that if $G \lhd A_n$, $G \neq 1$ then G contains a cycle of length 3. This will be done splitting in cases. Let $g \in G$, $g \neq 1$. Take it's decomposition as product of disjoint cycles $g = g_1 \cdots g_k$. Then:

1. If $g = g_1$ is a length 3 cycle, it is done.

2. Suppose $|g_i| \geq 4$ for some i (we can assume $i = 1$). Let $g_1 = (a_1, \ldots, a_m)$ and let $h = (a_1, a_2, a_3) \in A_n$. We know that $ghg^{-1}h^{-1}$ is in G. Since the support of h is contained in that of g_1, we get

$$ghg^{-1}h^{-1} = g_1 h g_1^{-1} h^{-1} = (a_2, a_4, a_3)$$

3. Now assume $|g_i| \leq 3$ and some $|g_j| = 3$. Let $g_1, \ldots, g_t$ be the length 3 cycles, and hence the rest are transpositions. Then $g^2 = g_1^{-1} \cdots g_t^{-1}$ is in G, and has only length 3 cycles in it's decomposition. If $t = 1$ we are done. Otherwise, let $g_1 = (a_1, a_2, a_3)$ and $g_2 = (b_1, b_2, b_3)$. Put $h = (a_1, a_2, b_3)$. Then

$$ghg^{-1}h^{-1} = g_1 g_2 h g_1^{-1} g_2 h^{-1} = (a_1, a_3, b_2, a_2, b_3)$$

   It is reduced to the previous case.

4. When all the g_i are transpositions and $k \geq 4$. Let $g_1 = (a_1, a_2)$, $g_2 = (b_1, b_2)$, $g_3 = (c_1, c_2)$. Put $h = (a_2, b_1)(b_2, c_1)$. Again

$$ghg^{-1}h^{-1} = g_1 g_2 g_3 h g_1 g_2 g_3 h = (a_1, b_2, c_1)(a_2, c_2, b_1)$$

5. The remaining case is $g = g_1 g_2 = (a, b)(c, d)$. Let $x \neq a, b, c, d$, we use again $n \geq 5$. Put $h = (a, b, x)$. We get $ghg^{-1}h^{-1} = (a, b, x)$.

6 Abelian groups

6.1 Basic facts

A group G is called *abelian* if every two elements of G commute. For abelian groups we will use additive notation. That is, we will denote the group operation by $+$ and call it *sum*. The identity element will be denoted by 0 and the inverse of a by $-a$. For $m \in \mathbb{Z}$, we denote by ma the m-th power of a, as defined in 1.4.

Remarks

1. Direct products of abelian groups are abelian.
2. Subgroups and quotients of abelian groups are abelian.

Lemma Let G be an abelian group, and $a, b \in G$. Then

1. If $m \in \mathbb{Z}$, then $m(a+b) = ma + mb$.
2. If a and b are of finite order, then $|a+b| \leq \operatorname{lcm}(|a|, |b|)$.

A non trivial element of finite order is called a *torsion element*. A group is called *torsion-free* if it has no torsion elements. Let

$$T(G) = \{g \in G : |g| < \infty\}$$

Proposition Let G be an abelian group. Then

1. $T(G)$ is a characteristic subgroup of G.
2. $G/T(G)$ is torsion-free.

6.2 Free abelian groups

We will focus on finitely generated groups, which will be abbreviated as f.g. groups. Suppose that G is a f.g. abelian group and it is generated by $a_1, \ldots, a_n \in G$. By iterated application of the commutative law, we can write any element $a \in G$ in the form

$$a = k_1 a_1 + \cdots + k_n a_n \qquad \text{for } k_1, \ldots, k_n \in \mathbb{Z}$$

Note that the map $\varphi : \mathbb{Z}^n \to G$ s.t. $\varphi(k_1, \ldots, k_n) = k_1 a_1 + \cdots + k_n a_n$ is then a surjective homomorphism.

Definition Let G be a f.g. abelian group.

1. The elements $a_1, \ldots, a_n \in G$ form a *basis* of G if every element $a \in G$ can be written uniquely as $a = k_1 a_1 + \cdots + k_n a_n$ for $k_i \in \mathbb{Z}$.
2. If such a basis exists, G is called a *free abelian* group.

Note that $\mathbb{Z}^n$ is free abelian and the elements $e_1, \ldots, e_n$ form a basis, where e_i has a 1 in coordinate i and zeroes in every other coordinate. This is called the *canonical basis* of $\mathbb{Z}^n$.

On the other hand, suppose that G is free abelian. If $a_1, \ldots, a_n$ is a basis of G, then the corresponding homomorphism $\varphi : \mathbb{Z}^n \to G$ is an isomorphism. So, a f.g. abelian group is free iff $G \cong \mathbb{Z}^n$ for some n. This number is called the *rank* of G. It is well defined, as the next result will imply.

Lemma

1. For any m elements $a_1, \ldots, a_m \in \mathbb{Z}^n$ with $m > n$, there are $k_1, \ldots, k_m \in \mathbb{Z}$, not all equal to 0, such that
$$k_1 a_1 + \cdots + k_m a_m = 0$$
2. $\mathbb{Z}^n$ is not isomorphic to $\mathbb{Z}^m$ if $n \neq m$.

Since $\mathbb{Q}^n$ is a vector space of dimension n, there are $q_1, \ldots, q_m \in \mathbb{Q}$ s.t. $q_1 a_1 + \cdots + q_m a_m = 0$, where not all q_i are equal to 0. Take m a multiple of all the denominators of the q_i, and let $k_i = mq_i$. These coefficients satisfy statement 1. Statement 2 is a consequence, since property 1 is preserved by isomorphism.

The following result is a rephrasing of facts we already obtained.

Proposition(Universal property for free abelian groups) Let G be a f.g. abelian group, with a generating set $a_1, \ldots, a_n$. Then there exists a unique homomorphism $\varphi : \mathbb{Z}^n \to G$ such that $\varphi(e_i) = a_i$ for $i = 1, \ldots, n$.

6.3 Subgroups of a free abelian group

Now we will study the subgroups of $\mathbb{Z}^n$. Together with the universal property, this will allow us to classify the f.g. abelian groups.

Proposition A subgroup $H \leq \mathbb{Z}^n$ is also free abelian, and it's rank is at most n.

We prove it by induction on n. When $n = 1$ this is true, since a subgroup of $\mathbb{Z}$ is of the form $a\mathbb{Z}$. For the inductive step, let $\pi_n : \mathbb{Z}^n \to \mathbb{Z}$ be the projection in the last coordinate. Then $\pi_n(H) = a\mathbb{Z}$ for some $a \in \mathbb{Z}$, since it is a subgroup. If $a = 0$ then $H \leq \ker \pi_n = \mathbb{Z}^{n-1}$ and we use the induction hypothesis. So, suppose $a \neq 0$. Take $x \in H$ so that $\pi_n(x) = a$, and put $K = H \cap \ker \pi_n = H \cap \mathbb{Z}^{n-1}$. Now, if $h \in H$, then there is $m \in \mathbb{Z}$ such that $\pi_n(h) = am$. Applying π_n, we can check that $h - mx \in K$. So $H = \langle x \rangle + K$. And we can also check that $\langle x \rangle \cap K = 0$ by the same method. So $H \cong K \times \mathbb{Z}$ with $K \leq \mathbb{Z}^{n-1}$, and we can apply the induction hypothesis to K.

Lemma Let A be a $n \times k$ matrix with $\mathbb{Z}$ coefficients. Then there exist $P \in GL_n(\mathbb{Z})$ and $Q \in GL_k(\mathbb{Z})$ such that PAQ has the diagonal form

$$PAQ = \begin{pmatrix} d_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & d_k \\ \vdots & & \vdots \\ 0 & \cdots & 0 \end{pmatrix}$$

where d_i divides d_{i+1} for all i. (With the convention that $1|a$ and $a|0$ for every $a \in \mathbb{Z}$).

First we define the elementary matrices, that are the square matrices of the following forms.

1. For $i \neq j$, $T_{ij} = (t_{kl})$ where $t_{ij} = t_{ji} = t_{kk} = 1$ for $k \neq i, j$ and all other entries are zero.

2. For $i \neq j$, $a \in \mathbb{Z}$, $S_{ij}(a) = (s_{kl})$ where $s_{kk} = 1$, $s_{ij} = a$ and all other entries are zero.

These matrices correspond to the standard row and column operations. Let A be an $n \times k$ matrix.

1. $T_{ij}A$ is the result of interchanging row i and row j in A. And AT_{ij} is the same for columns.

2. $S_{ij}(a)A$ is the result of summing a times the j-th row to row i in A. Doing $AS_{ij}(a)$ is to sum a times the i-th column to column j.

The elementary matrices of size $m \times m$ are in $GL_m(\mathbb{Z})$, for $T_{ij}^{-1} = T_{ij}$ and $S_{ij}(a)^{-1} = S_{ij}(-a)$.
Using the row and column operations on $A = (a_{ij})$ we can:

- Move any entry a_{ij} to the $(1, 1)$ position.

- Preform the Euclidean Algorithm to any pair of rows or columns, until it terminates for some entry.

Iterating the above procedures, it is possible to reduce A to the form

$$P_1AQ_1 = \begin{pmatrix} d_1 & 0 \\ 0 & A_1 \end{pmatrix}$$

where d is the gcd of all the entries in A, and divides every entry of A_1. The matrices P_1 and Q_1 are the products of the elementary matrices we used in the process.
So, by induction in k, we prove the lemma.

Now we can characterize every subgroup of $\mathbb{Z}^n$.

Theorem Let $H \leq \mathbb{Z}^n$ be a subgroup of rank k. Then there exist

1. A basis $x_1, \ldots, x_n$ of $\mathbb{Z}^n$.
2. A basis $y_1, \ldots, y_k$ of H.
3. Integers $d_1 | \cdots | d_k$, $d_i > 0$.

Such that $y_i = d_i x_i$ for $i = 1, \ldots, k$.

Take some basis $u_1, \ldots, u_k$ of H. Write these elements in the canonical basis of $\mathbb{Z}^n$.

$$\begin{cases} u_1 &= a_{11}e_1 + \cdots + a_{n1}e_n \\ &\vdots \\ u_k &= a_{1k}e_1 + \cdots + a_{nk}e_n \end{cases}$$

Put $A = (a_{ij})$. Now let $PAQ = D$ as in the previous lemma. Take $y_i = Q^{-1}u_i$, $x_j = Pe_j$. The d_i are non zero. If not, the rank of H would be less than k. And by switching signs in the generators, they can be taken positive.

Note We could have started just with a generator of H. The algorithm produces a basis. In this case some of the d_i could be 0.

Uniqueness of the d_i is true, it is going to follow from the next section.

6.4 Structure of the finitely generated abelian groups

The goal of this section is to prove the following theorem, classifying the f.g. abelian groups.

Theorem Let G be a f.g. abelian group. Then G decomposes as a direct product

$$G \cong \mathbb{Z}_{p_1^{m_1}} \times \cdots \times \mathbb{Z}_{p_s^{m_s}} \times \mathbb{Z}^r$$

For $p_1, \ldots, p_s$ primes (not necessarily different), and $r, m_1, \ldots, m_s > 0$. This decomposition is unique (aside from the order of the factors).

We need a preliminary result about cyclic groups.

Proposition Let $n = st$ with $s, t > 0$ and $(s,t) = 1$. Then $\mathbb{Z}_n \cong \mathbb{Z}_s \times \mathbb{Z}_t$.

Consider the subgroups generated by the classes $\bar{t}$ and $\bar{s}$. Then $\langle \bar{t} \rangle \cong \mathbb{Z}_s$ and $\langle \bar{s} \rangle \cong \mathbb{Z}_t$. Their intersection is trivial by Lagrange's theorem, since $(s,t) = 1$. And they are clearly normal, so they generate a subgroup isomorphic to $\mathbb{Z}_s \times \mathbb{Z}_t$. But that has order n, so it must be all $\mathbb{Z}_n$.

As a consequence, if $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ is the prime factorization of n, then

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{\alpha_1}} \times \cdots \times \mathbb{Z}_{p_k^{\alpha_k}}$$

Existence

If G is a f.g. abelian group, take some generator $a_1, \ldots, a_n$. This defines a surjective homomorphism $\varphi : \mathbb{Z}^n \to G$ s.t. $\varphi(e_i) = a_i$. So $G \cong \mathbb{Z}^n / \ker \varphi$.

We apply the theorem on last section to $\ker \varphi$. Let $x_1, \ldots, x_n$, $y_1, \ldots, y_k$ and $d_1, \ldots, d_k$ be as in that theorem. Now it is easy to check that

$$G \cong \mathbb{Z}_{d_j} \times \cdots \times \mathbb{Z}_{d_k} \times \mathbb{Z}^{n-k}$$

where the factors are the subgroups generated by the $\varphi(x_i)$, and d_j is the first of the d_i that is not equal to 1.

Applying the above result to the $\mathbb{Z}_{d_i}$ factors gives the desired decomposition.

Uniqueness

Regroup the product in the theorem as

$$G = S(p_1) \times \cdots \times S(p_t) \times \mathbb{Z}^r$$

where $p_1, \ldots, p_t$ are different primes, and the $S(p_i)$ are of the form

$$S(p) = \mathbb{Z}_{p^{m_1}} \times \cdots \times \mathbb{Z}_{p^{m_k}}$$

both the number of factors and their orders depending on i.

Now, it is clear that

$$T(G) = S(p_1) \times \cdots \times S(p_t) \qquad \text{and} \qquad G/T(G) \cong \mathbb{Z}^r$$

So, $G/T(G)$ is free abelian, and r is it's rank. So r depends only on the isomorphism class of G.

On the other hand, note that for each prime p, $S(p) \setminus \{0\}$ is the set of all the elements of order p^m for some m. Thus the $S(p_i)$ are characteristic subgroups, and they are determined by the structure of G.

We are reduced to the case when $G = S(p) = \mathbb{Z}_{p^{m_1}} \times \cdots \times \mathbb{Z}_{p^{m_k}}$.

Let m be the maximum of the m_i, and for $j = 1, \ldots, m$ let r_j be the number of $m_i \geq j$. Thus $r_1 = k$ and $r_j - r_{j+1}$ is the number of factors of the form $\mathbb{Z}_{p^j}$ in the given decomposition. So, it is enough to show that m and the r_j are determined by the isomorphism class of G.

For this, condider the nested subgroups $G \geq pG \geq \cdots \geq p^m G = \{0\}$. Note that m is the minimum exponent such that $p^m G = \{0\}$. And for each $j = 1, \ldots, m$ we have

$$p^{j-1}G/p^jG \cong (\mathbb{Z}_p)^{r_j}$$

So $r_j = \dim p^{j-1}G/p^jG$ as a $\mathbb{Z}_p$-vector space. This concludes the proof.

7 Free groups

7.1 Definition of free group

Let $X = \{x_i : i \in I\}$ be a set. Consider a disjoint copy of X, that will be denoted as $X^{-1} = \{x_i^{-1} : i \in I\}$. The elements of $X \cup X^{-1}$ will be called *letters*. Sometimes we refer to X as an *alphabeth*.

A *word* on the alphabeth X is a finite sequence

$$w = x_{i_1}^{\epsilon_1} \cdots x_{i_n}^{\epsilon_n}$$

where $n \geq 0$, $\epsilon_i = \pm 1$. When $n = 0$, it is called the *empty word*, and written $w = 1$. The number n is called the *length* of w, and will be written $l(w)$.

The *concatenation product* of the words v and w is defined as the word vw consisting on the letters of v followed by those of w.

We say that the words $w = w_1 x_i^{\epsilon} x_i^{-\epsilon} w_2$ and $v = w_1 w_2$ are *elementarily equivalent*. We also say that v is an *elementary reduction* of w. The words w and v are *equivalent* if there are words $w = w_1, \ldots, w_k = v$ where w_i and w_{i+1} are elementarily equivalent for all i. This is the smallest equivalence relation containing the elementary reductions.

The equivalence class of w will be denoted $[w]$. Define the product of classes as $[v][w] = [vw]$. It is easy to check it is well defined. This product makes the set of these equivalence classes into a group. The identity element is $[1]$, and the inverse of

$$[w] = [x_{i_1}^{\epsilon_1} \cdots x_{i_n}^{\epsilon_n}] \quad \text{is} \quad [w]^{-1} = [x_{i_n}^{-\epsilon_n} \cdots x_{i_1}^{-\epsilon_1}]$$

The group just defined is denoted by $F(X)$, and is called the *free group* on the free generators $\{x_i\}_{i \in I}$. The *rank* of $F(X)$ is $|X|$. Soon we shall show that free groups of different rank are not isomorphic.

Reduced words

The word $w = x_{i_1}^{\epsilon_1} \cdots x_{i_n}^{\epsilon_n}$ is *reduced* if it admits no elementary reductions. That is , if there is no j such that $x_{i_j}^{\epsilon_j} = x_{i_{j+1}}^{-\epsilon_{j+1}}$. The reduced words are a set of representatives for the classes $[w] \in F(X)$.

Proposition Let w be a word on the alphabeth X. There is a unique reduced word v that is equivalent to w.

Such word will be obtained by the following *reduction process*. Let $w = x_{i_1}^{\epsilon_1} \cdots x_{i_n}^{\epsilon_n}$. Then, for $k = 1, \ldots, n$ we define $R_k(w) = r_k$ inductively,

$$r_1 = x_{i_1}^{\epsilon_1}$$

And if $r_{k-1} = x_{i_1}^{\epsilon_1} \cdots x_j^{\epsilon}$

$$r_k = \begin{cases} r_{k-2} & \text{if} \quad x_{i_k}^{\epsilon_k} = x_j^{-\epsilon} \\ r_{k-1} x_{i_k}^{\epsilon_k} & \text{otherwise} \end{cases}$$

Put $R(w) = R_n(w)$.

The result $R(w)$ of the reduction process is a reduced word equivalent to w. And if w is reduced then $w = R(w)$. It is also easy to check that if we have a reduction $w = w_1 x_i^{\epsilon} x_i^{-\epsilon} w_2$, $v = w_1 w_2$ then $R(w) = R(v)$. So if w and v are equivalent words, then $R(w) = R(v)$. This shows the uniqueness.

This shows that we could have defined $F(X)$ as the set of reduced words, with the product $v \cdot w = R(vw)$. (Proving associativity would have been harder). We will use these two definitions without distinction.

Let v and w be reduced words. When the concatenation vw is reduced, we say that the product $v \cdot w$ in $F(X)$ is *reduced as written*. Under the second definition, this is the case when the concatenation and the group product agree. In the contrary case, we say that there is *cancellation* in the product $v \cdot w$.

7.2 Basic properties

It is clear that the group structure of $F(X)$ only depends on it's rank. If $|X| = n$, we shall write $F_n = F(X)$ and call it the free group on n generators.

Now we will characterize conjugation for elements of a free group. A reduced word $w = x_{i_1}^{\epsilon_1} \cdots x_{i_n}^{\epsilon_n}$ is *cyclically reduced* if $x_{i_1}^{\epsilon_1} \neq x_{i_n}^{-\epsilon_n}$. Every reduced word $w \neq 1$ is of the form $w = uvu^{-1}$ for v a non trivial, cyclically reduced word. If w is a cyclically reduced word, then a *cyclic permutation* of w is a word of the form $v = ba$ where $w = ab$. Note that such v is also cyclically reduced.

Proposition The reduced words v and w are conjugate in $F(X)$ iff they are of the form

$$v = v_0 ab v_0^{-1} \qquad w = w_0 ba w_0^{-1}$$

where ab and ba are cyclically reduced.

By the observations above, $v = v_0 \hat{v} v_0^{-1}$ and $w = w_0 \hat{w} w_0^{-1}$ for $\hat{v}$, $\hat{w}$ cyclically reduced. This reduces us to the case when v and w are cyclically reduced. It is clear that ab is conjugate to ba. Now suppose that $w = g \cdot v \cdot g^{-1}$ for $g \in F(X)$. Since v is cyclically reduced, there can not be cancellation in both products. Suppose there is no cancellation in $g \cdot v$, the other case being analogous. Now, since w is cyclically reduced, g^{-1} must be cancelled completely in $gv \cdot g^{-1}$. That is, $gv = v_1 g$ for some word v_1. We can assume that $l(g) < l(v)$, since otherwise we must have $g = g_1 v$, and so $g \cdot v \cdot g^{-1} = g_1 \cdot v \cdot g_1^{-1}$ with $l(g_1) < l(g)$. But under this assumption, we must have $v = ab$ with $g = b$. And so $w = ba$.

This shows that the conjugacy classes in $F(X)$ correspond to the *cyclic words* on the alphabeth X. That is, the cyclically reduced words modulo cyclic permutation.

Proposition(Universal property for free groups) Let G be a group and $S = \{s_i : i \in I\} \subseteq G$ a generating set. Let $X = \{x_i : i \in I\}$. Then there exists a unique homomorphism $\varphi : F(X) \to G$ such that $\varphi(x_i) = s_i$ for all $i \in I$.

This is easier using the first definition. For a word $w = x_{i_1}^{\epsilon_1} \cdots x_{i_n}^{\epsilon_n}$, it must be $\varphi([w]) = s_{i_1}^{\epsilon_1} \cdots s_{i_n}^{\epsilon_n}$. To show that it is well defined, note that it is enough to check it for elementary reductions. It clearly takes concatenation of words to products in G, so it is an homomorphism.

This implies that every group is a quotient of a free group. Intuitively, this says that the free groups $F(X)$ are the groups with the least possible relations.

For any group G, we defined it's commutator subgroup as

$$G' = \langle xyx^{-1}y^{-1} : x, x \in G \rangle$$

It is normal, and the quotient G/G' is called the *abelianization* of G. It is the maximal abelian quotient in the following sense. If $N \lhd G$ has G/N abelian, then $G' \leq N$. Equivalently, if $\varphi : G \to A$ is a homomorphism and A is abelian, then φ factors through the quotient map $G \to G/G'$.

Proposition The abelianization of $F(X)$ is isomorphic to

$$\bigoplus_{i \in I} \mathbb{Z}$$

In particular $F_n/F_n' \cong \mathbb{Z}^n$.

By the universal property of the free group, there exists an homomorphism $\pi : F(X) \to \oplus_{i \in I} \mathbb{Z}$ taking x_i to a generator of the i-th coordinate, that we will also call x_i.

In the last section we have seen a universal property for free finitely generated abelian groups. The same statement is true for $\oplus_{i \in I} \mathbb{Z}$. Consider an homomorphism $\varphi : F(X) \to A$ where A is abelian. By the mentioned universal property, there exists $\psi : \oplus_{i \in I} \mathbb{Z} \to A$ s.t. $\psi(x_i) = \varphi(x_i)$. It is then clear that $\varphi = \psi \circ \pi$. Apply this when A is the abelianizaton, and φ it's canonical projection. On the other hand, by the observation made above, π must also factor through φ. Say that $\pi = \hat{\psi} \circ \varphi$. By the uniqueness part of the universal property, ψ and $\hat{\psi}$ must be inverses of each other.

As a consequence, we obtain

Proposition $F(X)$ and $F(Y)$ are isomorphic iff $|X| = |Y|$.

A group G is *free* if it is isomorphic to $F(X)$ for some X, and in this case we say that $|X|$ is the *rank* of G.

7.3 Graphs

Graphs are geometric objects deeply related to free groups. First we give the basic definitions.

Definition A *(directed) graph* Γ consist on a set V of *vertices*, a set E of *edges* and two functions $s, t : E \to V$. The sets V and E are at most countable.

We usually denote $\Gamma = (V, E)$. For $\sigma \in E$, $s(\sigma)$ is called it's *source* and $t(\sigma)$ it's *target.* We say that σ is *oriented* or *directed* from $s(\sigma)$ towards $t(\sigma)$.

Intuitively, elements of V corresponds to points, and an element $\sigma \in E$ corresponds to an oriented line segment connecting the vertices $s(\sigma)$ and $t(\sigma)$. Note that we allow loops (edges with $s(\sigma) = t(\sigma)$) and multiple edges (there may be any number of edges with the same source and target).

As done with the alphabeth X before, we introduce a set $E^{-1} = \{\sigma^{-1} : \sigma \in E\}$ and assign $s(\sigma^{-1}) = t(\sigma)$, $t(\sigma^{-1}) = s(\sigma)$. We also refer to elements of $E \cup E^{-1}$ as *edges*, with the convention that $(\sigma^{-1})^{-1} = \sigma$ for any of these edges. The pairs $\{\sigma, \sigma^{-1}\}$ are called *geometric* or *unoriented* edges.

Definition A *path* w in a graph Γ is a sequence of edges

$$w = \sigma_1 \cdots \sigma_n$$

such that $t(\sigma_i) = s(\sigma_{i+1})$ for all $i = 1, \ldots, n-1$.

The path w is *closed* if $t(\sigma_n) = s(\sigma_1)$. It is *reduced* if no $\sigma\sigma^{-1}$ appears in the sequence. The paths of the form $\sigma\sigma^{-1}$ are called *spurs.*

Definition Let $\Gamma = (V, E)$ be a graph.

1. Γ is *finite* if V and E are finite.
2. Γ is *connected* if for every $x, y \in V$ there is a path $w = \sigma_1 \cdots \sigma_n$ s.t. $s(\sigma_1) = x$ and $t(\sigma_n) = y$. In this case we say that w goes from x to y.
3. The *degree* or *valence* of a vertex $x \in V$ is the number of edges starting at x. I.e. $\deg_\Gamma(x) = |\{\sigma \in E \cup E^{-1} : s(\sigma) = x\}|$.

A graph is called a *tree* if it is connected and contains no reduced closed paths. Given any two vertices x and y in a tree T, there is a unique reduced path in T going from x to y.

Definition A *subgraph* Δ of the graph $\Gamma = (V, E)$ consists on subsets $V_1 \subseteq V$, $E_1 \subseteq E$ such that for $\sigma \in E_1$ we have $s(\sigma), t(\sigma) \in V_1$.

Thus a subgraph $\Delta = (V_1, E_1)$ of Γ is a graph whose source and target maps are the restrictions of those of Γ. A *spanning tree* for a graph Γ is a subgraph T, which is a tree and contains all the vertices of Γ.

Lemma Every graph contains a spanning tree.

The key idea is to define subgraphs T_k by recursion. T_0 is just a vertex $x \in V$, and no edges. T_k is obtained by adding to T_{k-1} all the edges $\sigma \in E \cup E^{-1}$ with $s(\sigma) \in T_{k-1}$ but $t(\sigma) \notin T_{k_1}$, as well as the corresponding vertices $t(\sigma)$ and their inverse edges σ^{-1}. Check that $T = \cup_{k=0}^{\infty} T_k$ is a spanning tree.

The *connectivity number* of a graph Γ is the number of geometric edges in the complement of a spanning tree. When Γ is finite, $|V| = v$ and $|E| = e$, this number is $e - v + 1$.

7.4 Fundamental group

Let Γ be a connected graph, and x_0 a vertex of Γ. Given a path w in Γ we can reduce it by deleting spurs, yielding a unique reduced path. This is analogous as what we did for words. We can also define an equivalence relation between paths, which is the minimal one containing reductions of spurs. Let $[w]$ be the class of w.

When the ending vertex of w_1 is equal to the starting vertex of w_2, we can concatenate them forming a new path $w_1 w_2$. Note that equivalent paths have the same starting and ending vertices. When w is closed, we say that it is *based* at it's starting (ending) vertex.

Put

$$\pi_1(\Gamma, x_0) = \{[w] : w \text{ based at } x_0\}$$

with the product $[w_1][w_2] = [w_1 w_2]$. This is well defined and a group operation, by the same proof we used for free groups. The identity element is the path with no edges, which can be seen as the constant x_0. The inverse of w is the path obtained by travelling w backwards, and it has the same formula as the case with words.

With this product, $\pi_1(\Gamma, x_0)$ is called the *fundamental group* of Γ with basepoint in x_0.

Proposition With the above notations, $\pi_1(\Gamma, x_0)$ is a free group, and it's rank is the connectivity number of Γ.

Let T be a spanning tree for Γ. Let $S = \{s_i\}_{i\in I}$ be the set of edges in E that are not in T. For a path $w = \sigma_1 \cdots \sigma_n$ in Γ let $\varphi(w)$ be the word obtained from w by reading only the σ_j that are in $S \cup S^{-1}$, and ignoring the edges in T.

This gives a well defined map $\varphi : \pi_1(\Gamma, x_0) \to F(S)$. It is easy to see that it is surjective and an homomorphism.

Suppose w is a path in Γ with $\varphi(w) = v_1 s_i^\epsilon s_i^{-\epsilon} v_2$. Then w has the form $w_1 s_i^\epsilon u s_i^{-\epsilon} w_2$ where u is a closed path in T, based at the target of s_i^ϵ. Since T is a tree, u can be reduced to the constant $t(s_i^\epsilon)$. Thus w reduces to $w_1 s_i^\epsilon s_i^{-\epsilon} w_2$, which in turn reduces to $w_1 w_2$. This is mapped to $v_1 v_2$ under φ.

By iterating this argument, we see that a reduction of $\varphi(w)$ comes from a reduction of w. This proves that $\ker \varphi = 1$.

In particular, $\pi_1(\Gamma, x_0) \cong \pi_1(\Gamma, x_1)$ for any other vertex x_1 of Γ. So we usually speak of $\pi_1(\Gamma)$, without reference to the basepoint.

Remark The proof provides free generators for $\pi_1(\Gamma, x_0)$ as follows. For a spanning tree T and an edge σ not in T, let $s = s(\sigma)$, $t = t(\sigma)$. Let v_σ, w_σ be the unique paths in T from x_0 to s and t respectively. Then $\bar\sigma = v_\sigma \sigma w_\sigma^{-1}$ is a closed path based at x_0. Then the elements $\bar\sigma$ for $\sigma \in E$ not in T form a free generator of $\pi_1(\Gamma, x_0)$.

7.5 Coverings

Let Γ be a graph. If v is a vertex of Γ, the *star* of v is the set of edges starting at x. That is

$$\mathrm{St}(x) = \{\sigma \in E \cup E^{-1} : s(\sigma) = x\}$$

Definition A map $f : \hat\Gamma \to \Gamma$ between graphs is a *covering* if

1. it maps the vertices (edges) of $\hat\Gamma$ to the vertices (edges) of Γ surjectively.
2. it preserves endpoints and orientation of edges. I.e. if σ is an edge of $\hat\Gamma$, then $s(f(\sigma)) = f(s(\sigma))$ and $t(f(\sigma)) = f(t(\sigma))$. Also $f(\sigma)^{-1} = f(\sigma^{-1})$.
3. If x is a vertex of $\hat\Gamma$, then f maps $\mathrm{St}(x)$ to $\mathrm{St}(f(x))$ bijectively.

By condition 2, the image of a path under f is again a path. Condition 3 says that a covering is locally bijective (bijective in some neighborhood of every vertex or edge).

Observe that the image of a spur under f is a spur. Thus, if the paths w_1 and w_2 in $\hat\Gamma$ are equivalent, we have that $f(w_1)$ is equivalent to $f(w_2)$. So we can define

$$f_* : \pi_1(\hat\Gamma, x) \to \pi_1(\Gamma, f(x)) \quad \text{as} \quad f_*([w]) = [f(w)]$$

It is easy to check that it is an homomorphism.

Applying condition 3, we can show that if w is a reduced path, then $f(w)$ is also reduced. In particular $\ker f_* = 1$. For if $[w] \in \ker f_*$ with w reduced, then $f(w)$ has to be the constant $f(x)$. And the length of a path (number of edges in it) is clearly preserved by f, so w must be the constant x.

Thus, if we have a covering $f : \hat\Gamma \to \Gamma$, a vertex x_0 of Γ and a vertex x of $\hat\Gamma$ with $f(x) = x_0$, then the induced homomorphism $f_* : \pi_1(\hat\Gamma, x) \to \pi_1(\Gamma, x_0)$ is an embedding. We can see $\pi_1(\hat\Gamma, x)$ as a subgroup of $\pi_1(\Gamma, x_0)$.

Coverings have the following important property

Proposition(Path lifting property) Let $f : \hat{\Gamma} \to \Gamma$ be a covering, w a path in Γ starting at x, and $\hat{x}$ a vertex of $\hat{\Gamma}$ with $f(\hat{x}) = x$. Then there exists a unique path $\hat{w}$ which starts at $\hat{x}$ and satisfies $f(\hat{w}) = w$.

This is proved by induction on the length of w, using the condition 3 for a covering on each step.

The path $\hat{w}$ is called the *lift* of w at $\hat{x}$. Note that $\pi_1(\hat{\Gamma}, \hat{x}_0)$ can be identified with the $[w] \in \pi_1(\Gamma, x_0)$ whose lifts at $\hat{x}_0$ are closed.

Let $f^{-1}(x_0) \subset \hat{\Gamma}$ be the inverse image of x_0, i.e. the vertices mapped to x_0 under f. Then $\pi_1(\Gamma, x_0)$ acts in $f^{-1}(x_0)$ as follows. If $[w] \in \pi_1(\Gamma, x_0)$, and $x \in f^{-1}(x_0)$ take $\hat{w}$ the lift of w at x, and define $x \cdot [w]$ to be the ending vertex of $\hat{w}$. This is a right action, and the stabilizer of $x \in f^{-1}(x_0)$ is $\pi_1(\hat{\Gamma}, x)$.

Hence, changing the basepoint x among the preimages of x_0 yields the conjugates of $\pi_1(\hat{\Gamma}, \hat{x}_0)$.

Now we will see that any subgroup of $\pi_1(\Gamma, x_0)$ can be obtained as the fundamental group of a covering.

Theorem Given any subgroup $H \leq \pi_1(\Gamma, x_0)$, there is a covering $f : \hat{\Gamma} \to \Gamma$ and $\hat{x}_0 \in \hat{\Gamma}$ such that $f(\hat{x}_0) = x_0$ and $H = \pi_1(\hat{\Gamma}, \hat{x}_0)$.

Let $S = \{g_i\}_{i_I}$ be a set of representatives for the right cosets of H, with $g_1 = 1$. Take T a spanning tree for Γ, and a copy T_i for each coset Hg_i. For each edge σ not in T let $s = s(\sigma)$, $t = t(\sigma)$. And let s_i, t_i their corresponding vertices in T_i.

To make $\hat{\Gamma}$, start with $\cup_i T_i$. And for each σ as above, add edges σ_i with $s(\sigma_i) = s_i$ and $t(\sigma_i) = t_j$ where j is such that $Hg_i\bar{\sigma} = Hg_j$ for $\bar{\sigma}$ being the generator associated to σ.

The map $f : \hat{\Gamma} \to \Gamma$ takes each T_i to T by their standard identifications, and each σ_i to the corresponding σ.

It is easy to check it is a covering. Let $\{\hat{x}_i\}$ be the vertices projecting to x_0 under f, with $\hat{x}_i \in T_i$. Then the action of $\pi_1(\Gamma, x_0)$ is given by $\hat{x}_i \cdot \bar{\sigma} = \hat{x}_j$ iff $Hg_i\bar{\sigma} = Hg_j$. Thus $\hat{x}_1 \cdot [w] = \hat{x}_1$ iff $[w] \in H$, i.e. the stabilizer of $\hat{x}_1$ is H. We have already seen that in that case $\pi_1(\hat{\Gamma}, \hat{x}_1) = H$.

7.6 The Nielsen - Schreier theorem

Every free group $F(X)$ can be written as the fundamental group of a graph. Let Γ consist on a single vertex x_0, and one edge for each element of X ($V = \{x_0\}$, $E = X$, $s(\sigma) = t(\sigma) = x_0$). Then $F(X) = \pi_1(\Gamma, x_0)$. When $|X| = n$, this graph is called the *rose* of n petals, R_n.

Theorem Let G be a free group and $H \leq G$. Then H is free. Moreover, if $[G : H] < \infty$ then

$$\text{rank}(H) = (\text{rank}(G) - 1)[G : H] + 1$$

Consider Γ with $G = \pi_1(\Gamma)$ as above. By the result of the last section, there is a covering $f : \hat{\Gamma} \to \Gamma$ with $H = \pi_1(\hat{\Gamma})$. So H is free, since it is the fundamental group of a graph.

For the second statement, let $i = [G : H]$. By the construction of $\hat{\Gamma}$, we know it has i vertices, and $\text{rank}(G) \cdot i$ edges (the spanning tree in Γ is just x_0). A spanning tree for $\hat{\Gamma}$ takes up $i - 1$ edges, so it's connectivity number is

$$\text{rank}(G) \cdot i - i + 1$$

And this is the rank of H.

This theorem was first proved by Nielsen, for H finitely generated. The proof by Schreier gives a set of generators for H in terms of it's cosets. These generators can also be obtained from the geometric method, as we shall discuss now.

Let $H \leq F(X)$ and consider a set of representatives $S = \{w_j\}_{j \in J}$ for the right cosets of H. We say that S satisfy the *Schreier condition* if every initial subword of a $w_j \in S$ is also in S. In this case S is called a *Schreier system* for H. We will see that such systems exist and have a geometric interpretation in terms of graphs.

Let $f : \hat{\Gamma} \to \Gamma$ be the covering corresponding to H that was constructed in the proof of the theorem. Then the vertices of $\hat{\Gamma}$ are exactly the elements of $f^{-1}(x_0)$, that are in correspondence with the right cosets of H. And each edge of $\hat{\Gamma}$ projects under f to a generator $x_i \in X$. Let x_1 be the basepoint of $\hat{\Gamma}$, corresponding to the coset H.

If T is a spanning tree for the graph $\hat{\Gamma}$, then the elements of the form $[f(\hat{w})]$ where $\hat{w}$ is a path in T starting at x_1 form a set of representatives of the right cosets of H. Note that they satisfiy the Schreier condition.

On the other hand, given a Schreier system $S = \{w_j\}_{j\in J}$, the union of the lifts $\hat{w}_j$ at x_1 is a spanning tree for $\hat{\Gamma}$.

This clearly establishes a bijection between the spanning trees of $\hat{\Gamma}$ and the Schreier systems for H.

Schreier systems can be used to write generators for the subgroup. Let $S = \{w_j\}_{j\in J}$ be a Schreier system for H. For $w_j \in S$ and $x_i \in X$ define

$$\overline{w_j x_i} = w_k \quad \text{where} \quad Hw_k = Hw_j x_i$$

That is, $\overline{w_j x_i}$ is the representative in S of the coset of $w_j x_i$.

Note that $w_j x_i \overline{w_j x_i}^{-1}$ is always in H. And it equals to 1 iff $w_j x_i$ is an element of S.

Theorem Let $H \leq F(X)$, and $S = \{w_j\}_{j\in J}$ a Schreier system for H. Then the elements of the form $w_j x_i (\overline{w_j x_i})^{-1}$ that are different from 1 form a free generator for H

Consider the spanning tree T in $\hat{\Gamma}$ given by S. Let $\hat{w}_j$ be the lift of w_j at x_1. So $\hat{w}_j$ is a path in T. This gives a bijection between S and the vertices of $\hat{\Gamma}$, for $\hat{w}_j$ is the unique reduced path in T going from x_1 to it's ending point.

We have seen that $\pi_1(\hat{\Gamma}, x_1)$ is freely generated by the elements of the form $\bar{\sigma} = v_\sigma \sigma w_\sigma^{-1}$ for σ an edge (in $E(\hat{\Gamma})$) not in T, and v_σ, w_σ the unique paths in T from x_1 to $s(\sigma)$, $t(\sigma)$ respectively. Thus H is freely generated by the corresponding projections $[f(\bar{\sigma})]$.

From the above discussion, we get that $v_\sigma = \hat{w}_j$, $w_\sigma = \hat{w}_k$ for some $w_j, w_k \in S$. And by the construction of the covering $f : \hat{\Gamma} \to \Gamma$, we have that $f(\sigma) = x_i$ for some i. Thus $[f(\bar{\sigma})] = w_j x_i w_k^{-1}$, and since $[f(\bar{\sigma})] \in H$ we see that $w_k = \overline{w_j x_i}$.

On the other hand, the lift of an element $w_j x_i (\overline{w_j x_i})^{-1}$ must be of the form $\hat{w}_j \tau \hat{w}_k^{-1}$ for some edge τ projecting to x_i and $w_k = \overline{w_j x_i}$. This is because elements in H lift to closed paths based at x_1. If τ is not in T we are in the above case, that is $w_j x_i (\overline{w_j x_i})^{-1} = [f(\bar{\tau})]$. Otherwise, we see that $\hat{w}_k = \hat{w}_i \tau$ (possibly after reduction), and thus $w_j x_i \in S$.

So, the elements $w_j x_i (\overline{w_j x_i})^{-1}$ that are different from 1 are exactly the projections $[f(\bar{\sigma})]$ for σ not in T, and thus are free generators for H.

Examples

1. In $F(a, b)$, let $H = \langle a^2, ab, b^2\rangle$. It has index 2 (note that $ba = b^2(ab)^{-1}a^2 \in H$). So it has rank 3. $S = \{1, a\}$ is a Schreier system, and the generators obtained from it are ba^{-1}, a^2, ab.

2. In $F(a, b)$, let $H = \langle a^2, b\rangle$. It clearly has rank 2. It has infinite index, since $H \neq F(a, b)$ (e.g. $a \notin H$) but 1 is the only integer i satisfying $\text{rank}(H) = (\text{rank}(F(a, b)) - 1)i + 1$. A Schreier system is formed by 1 and all the reduced words of the form aw, i.e. with first letter a. It gives the original generator.

8 Group presentations

8.1 Normal closure and presentations

Let $A \subseteq G$, where G is a group. The *normal closure* of A is

$$\langle\langle A\rangle\rangle = \bigcap\{N \lhd G : A \subseteq N\}$$

It is easy to see that $\langle\langle A\rangle\rangle \lhd G$, and it is the smallest normal subgroup of G containing A. The following is analogous to the result for subgroup generators.

Proposition The elements of $\langle\langle A\rangle\rangle$ are exactly those of the form $g_1 a_1^{\epsilon_1} g_1^{-1} \cdots g_n a_n^{\epsilon_n} g_n^{-1}$ for $n \geq 0$, $a_i \in A$, $g_i \in G$ and $\epsilon_i = \pm 1$.

Now let $X = \{x_i\}_{i\in I}$ and consider the free group $F(X)$. Let $R \subseteq F(X)$ be any subset. Define

$$\langle X|R\rangle = F(X)/\langle\langle R\rangle\rangle$$

Definition Let G be a group. A *presentation* for G is a pair X, R, where X is a set and R a subset of $F(X)$ satisfying

$$G \cong \langle X|R\rangle$$

We refer to X as the set of *generators* of the presentation $\langle X|R\rangle$. The elements of $\langle\langle R\rangle\rangle$ are called the *relations* of this presentation, and those of R are called *defining relations*.

This notation is justified by the following facts. Let s_i be the image of x_i under the isomorphism $G \cong \langle X|R\rangle$. Then it is clear that $S = \{s_i\}_{i\in I}$ is a generating set for G. And if $w \in F(X)$ is a reduced word, let $w(S)$ be the result of substituting each x_i in w for s_i (that is also the image of w under the isomorphism in consideration). Then $w(S) = 1$ iff $w \in \langle\langle R\rangle\rangle$.

Of course, we will usually abuse notation and call s_i and x_i by the same name.

Proposition Every group has a presentation.

If G is a group, take X a generator (that may be G itself). By the universal property for free groups, there is an homomorphism $\varphi : F(X) \to G$, commuting with the inclussions $X \hookrightarrow F(X)$ and $X \hookrightarrow G$. Let N be it's kernel. Then $G \cong F(X)/N$. If R is any subset whose normal closure is N, then we have that $\langle X|R\rangle$ is a presentation for G.

We can see that there is a lot of freedom in the above construction, so a group will have many different presentations. Also, $\langle X|R\rangle$ is the maximal group generated by X and satisfying the relations in R, in the sense of the following universal property.

Proposition Let $G = \langle X|R\rangle$. And let H be a group generated by $S = \{s_i\}_{i\in I}$ which verifies $r(S) = 1$ for each $r \in R$. Then there exists a unique homomorphism $\varphi : G \to H$, such that $\varphi(x_i) = s_i$.

This is obtained using the universal properties for free groups and for quotients.

Notice that any group G with generators in X that satisfies this universal property is isomorphic to $\langle X|R\rangle$. We say that the relations in $\langle\langle R\rangle\rangle$ are *consequence* of those in R. Also, we often express the relations $w \in \langle\langle R\rangle\rangle$ in the form of equations $w(X) = 1$.

Examples

1. $\mathbb{Z}_n \cong \langle a|a^n\rangle$. From the classification of cyclic groups.
2. $\mathbb{Z}^2 \cong \langle a, b|ab = ba\rangle$. The key point is to see that this presentation is an abelian quotient of F_2, for if the generators commute, every word on them will also do so.
3. $D_{2n} \cong \langle r, s|r^n, s^2, (sr)^2\rangle$. We have seen that choosing suitable generators for D_{2n} these relations are satisfied. So D_{2n} is a quotient of this presentation. But from the relations $sr = r^{-1}s$, every element in the RHS group can be put in the normal form $r^j s^k$, for $j = 0, \ldots, n-1$, $k = 0, 1$. This allows us to prove that that the quotient map is an isomorphism.

A group is called *finitely presented* if it has a presentation $\langle X|R\rangle$ with both X and R finite.

Proposition Let G be finitely presented. Then in any presentation with finitely many generators

$$G \cong \langle x_1, \dots, x_n | R\rangle$$

there are $r_1, \dots, r_m \in R$ such that $\langle\langle r_1, \dots, r_m\rangle\rangle = \langle\langle R\rangle\rangle$. So $G \cong \langle x_1, \dots, x_n | r_1, \dots, r_m\rangle$.

Let $G = \langle A|B\rangle$ with A and B finite. Applying the universal property for quotients, we can see that the isomorphism between $\langle A|B\rangle$ and $\langle X|R\rangle$ induces an isomorphism $F(A) \to F(X)$ where $X = \{x_1, \dots, x_n\}$. Let N be the image of $\langle\langle B\rangle\rangle$ under this isomorphism, and let $N_k = \langle\langle r_1, \dots, r_k\rangle\rangle$ where $R = \{r_i\}_{i=1}^{\infty}$. We have $N = \bigcup_{k=1}^{\infty} N_k$. But since B is finite, it must be contained in some N_m. So $N = N_m$, and $G \cong F(X)/N_m$.

8.2 Tietze transformations

Consider a presentation $\langle X|R\rangle$. We can apply the following transformations to it.

T_1: Add a new relation that is consequence of those in R. So we get $\langle X|R, s\rangle$ where $s \in \langle\langle R\rangle\rangle$.

T_2: Add a new generator y together with a relation of the form $y = w(X)$, for w any word on the letters of X. The new presentation is then $\langle X, y|R, w(X)y^{-1}\rangle$.

Such transformations yield a presentation that is equivalent to $\langle X|R\rangle$. That is, the groups defined by them are isomorphic. We also consider the inverse moves T_1^{-1}, T_2^{-1} when it is possible to apply them.

The transformations of type T_1, T_2 or their inverses are called *Tietze transformations.*

Theorem Let $\langle X|R\rangle$ and $\langle X'|R'\rangle$ be two finite presentations of the same group G. Then there is a sequence of Tietze transformations that takes $\langle X|R\rangle$ to $\langle X'|R'\rangle$.

Write the generarors in X as words on the letters of X'. That is $x_i = w_i(X')$ for all $x_i \in X$. And for $r_j \in R$ put $r_j(X') = r_j(w_1(X'), \dots, w_n(X'))$. Define $x'_k = v_k(X)$ and $r'_l(X)$ in the same manner.

Transform $\langle X|R\rangle = \langle x_i|r_j\rangle$ to

$$\langle x_i|r_j, r'_l(X)\rangle$$

by T_1 moves. Next, apply T_2 moves to get

$$\langle x_i, x'_k|r_j, r'_l(X), x'_k = v_k(X)\rangle$$

Now the r'_l are consequence of that set of relations. So we apply T_1 moves, and get

$$\langle x_i, x'_k|r_j, r'_l, r'_l(X), x'_k = v_k(X)\rangle$$

By their definition, the $r'_l(X)$ are consequence of the other relations. So they can be removed by T_1^{-1}, yielding

$$\langle x_i, x'_k|r_j, r'_l, x'_k = v_k(X)\rangle$$

This is still a presentation for G, so the relations $x_i = w_i(X')$ must be satisfied. Using T_1, we get

$$\langle x_i, x'_k|r_j, r'_l, x_i = w_i(X'), x'_k = v_k(X)\rangle$$

and this expression is symmetric, so we can bring $\langle X'|R'\rangle$ to this form with transformations of the same type.

Example $\langle a, b|abab^{-1}\rangle \cong \langle c, d|c^2d^2\rangle$. Use T_2 with $c = ab$, $d = b^{-1}$.

8.3 Cayley graphs

Let G be a group and $S = \{s_i\}$ a generating set. The *Cayley graph* associated to the pair (G, S) is a graph with edges labelled by the elements of S, that we construct as follows. It has G as set of vertices. And for $g, h \in G$, there is an edge labelled s_i from g to h iff $gs_i = h$.

This graph is denoted by $\mathcal{C}(G, S)$. Observe that each vertex has exactly one incoming and one outgoing edge for each element of S. In other words, the labelling is a bijection $\mathrm{St}(x) \to S \cup S^{-1}$ for each vertex $x \in G$.

In general, the graph $\mathcal{C}(G, S)$ depends on the generating set S. That is, for different generating sets of G, the associated Cayley graphs need not be isomorphic. This may happen even if the generating sets are minimal, as happens in the example from last section.

However, for free groups the situation is simpler.

Proposition The Cayley graph $\mathcal{C} = \mathcal{C}(F(X), X)$ of a free group $F(X)$ is a tree.

Let $\mathcal{C}_k$ be the subgraph whose vertices are all the reduced words of length at most k, and contains all the edges between them.

$\mathcal{C}_0$ consists only on the vertex 1. $\mathcal{C}_1$ consists on the vertices 1 and x_i^ϵ for $x_i \in X$, $\epsilon = \pm 1$. It is clear that $\mathcal{C}_1$ is a tree, in which 1 has it's full star from $\mathcal{C}$. And each x_i^ϵ is connected to exactly one edge, with label x_i.

Check that in $\mathcal{C}_k$ the vertices w with length $l(w) < k$ have their full stars form $\mathcal{C}$, and those with $l(w) = k$ are connected to just one edge.

All $\mathcal{C}_k$ are trees, by induction on k. Base cases are clear. If there is a reduced closed path γ in $\mathcal{C}_{k+1}$, it must pass through some vertex w with $l(w) = k + 1$, otherwise γ would be contained in $\mathcal{C}_k$ and we use the induction hypothesis. But the vertex w has degree 1 in $\mathcal{C}_{k+1}$, so γ contains a spur. Absurd, for γ was reduced.

Since $\mathcal{C} = \bigcup_k \mathcal{C}_k$ is a nested union, $\mathcal{C}$ is also a tree.

This proposition, together with the fact that $\mathrm{St}(x) \cong X \cup X^{-1}$ for $x \in F(X)$ defines the graph structure of $\mathcal{C}(F(X), S)$ for S any free generator.

Back to the general setting, let $\mathcal{C} = \mathcal{C}(G, S)$.

Let $\gamma = \sigma_1 \cdots \sigma_n$ be a path in $\mathcal{C}$ starting at 1 and ending at some $g \in G$. Consider the word $w = s_{i_1}^{\epsilon_1} \cdots s_{i_n}^{\epsilon_n}$ obtained by taking the labels of the edges in γ, where $\epsilon_j = \pm 1$ according to the orientation in which σ_j is traveled. More precisely, $\epsilon_j = -1$ iff $\sigma_j \in E^{-1}(\mathcal{C})$.

Then $g = s_{i_1}^{\epsilon_1} \cdots s_{i_n}^{\epsilon_n}$ as a product in G. In particular, if $g = 1$ then w is a relation in the presentation of G given by S. This relationship can be seen in terms of covering spaces as follows.

Let Γ_S be the graph with a single vertex x_0 and an edge for each $s_i \in S$. Then we can define $f : \mathcal{C} \to \Gamma_S$ by taking the edges $\sigma \in E(\mathcal{C})$ of label s_i to the edge s_i of Γ_S. Recall that $\pi_1(\Gamma_S, x_0) = F(S)$.

Proposition Let $f : \mathcal{C}(G, S) \to \Gamma_S$ defined as above. Then

1. f is a covering.
2. The projection f induces a bijection between paths from 1 to g in $\mathcal{C}$ and words w on S representing g in G.
3. If N is the kernel of the homomorphism $F(S) \to G$, we have $N = \pi_1(\mathcal{C}, 1)$ under the standard identifications.

Part 1 is true because of the form of $\mathrm{St}(x)$ for $x \in \mathcal{C}$.

With γ and w as in the above discussion, we can see that $f(\gamma) = w$. And for any word w representing g in G, the lift through f at 1 is a path ending at g. It is clear that this is inverse to the projection, proving 2.

In the case of closed paths based at 1, the correspondence in 2 is the standard identification of $\pi_1(\mathcal{C}, 1)$ as a subgroup of $\pi_1(\Gamma_S, x_0) = F(S)$. We see that if $G = F(S)/N$ is the presentation of G given by S, then $N = \pi_1(\mathcal{C}, 1)$.

As a corollary, we obtain the reciprocal of the proposition before. That is, if $\mathcal{C}(G, S)$ is a tree, then G is a free group.

8.4 Free actions on graphs

Let G be a group and S a generating set. There is a natural action of G on $\mathcal{C} = \mathcal{C}(G, S)$. In the vertex set, it is $G \curvearrowright G$ by left translations, i.e. $g \cdot x = gx$. And since $(g \cdot x)s_i = g \cdot xs_i$ (for $g, x \in G$, $s_i \in S$), it is possible to extend it as an action of G on $\mathcal{C}$ by graph isomorphisms that preserve labels.

Note The graphs isomorphisms we consider preserve the edge orientations. It is also common to say that G acts *without edge inversions* in this case.

Facts

1. The action $G \curvearrowright \mathcal{C}$ is *free*, that is, $\mathrm{Stab}_G(x) = 1$ for every $x \in \mathcal{C}$.
2. It is transitive in the set of vertices, and on that of the edges of a given label.
3. The orbit space $\mathcal{C}/G$ can be identified with the graph Γ_S defined in last section.

Note then that the quotient map $\mathcal{C} \to \Gamma_S = \mathcal{C}/G$ is exactly the covering we discussed in the last section. So $G \cong \pi_1(\Gamma_S)/\pi_1(\mathcal{C})$. The situation is similar for general free actions on graphs, as stated in the next result.

Proposition Let G be a group and Γ a graph. Let $G \curvearrowright \Gamma$ be a free action by graph isomorphisms. Then

1. Γ/G has a natural graph structure, and the quotient $\Gamma \to \Gamma/G$ is a covering.
2. Let $x \in \Gamma$ be a vertex, and $\bar{x} \in \Gamma/G$ be it's projection. Then $\pi_1(\Gamma, x) \lhd \pi_1(\Gamma/G, \bar{x})$.
3. If Γ is connected, then $G \cong \pi_1(\Gamma/G, \bar{x})/\pi_1(\Gamma, x)$.
4. If in addition, G acts transitively on the vertices of Γ, then Γ is a Cayley graph for G (with a suitable labelling of the edges).

Let $[x]$ denote the projection of x into the quotient Γ/G, for x a vertex or edge of Γ. Formally, $[x]$ is the orbit of x under G. Since G acts by graph isomorphisms, the maps $s([\sigma]) = [s(\sigma)]$ and $t([\sigma]) = [t(\sigma)]$ for $\sigma \in E(\Gamma)$ are well defined. This makes Γ/G into a graph. The projection clearly satisfies the first two conditions for a covering. For condition 3, observe that if $g \in G$, $x \in V(\Gamma)$ then

$$g\mathrm{St}(x) = \mathrm{St}(gx)$$

So, if $\sigma_1, \sigma_2 \in \mathrm{St}(x)$ then any $g \in G$ with $\sigma_1 = g\sigma_2$ has to verify $gx = x$. So $g = 1$, since the action is free. We obtain that two different edges in $\mathrm{St}(x)$ are in different orbits, proving condition 3.

Let $f : \Gamma \to \Gamma/G$ be the projection. Let $N = \pi_1(\Gamma, x) \leq \pi_1(\Gamma/G, \bar{x})$. Recall that if $[w] \in \pi_1(\Gamma/G, \bar{x})$ then the conjugate of N by $[w]$ is $[w]^{-1}N[w] = \pi_1(\Gamma, x_1)$, where x_1 is the ending point of the lift of w at x. On the other hand, since $f(x_1) = f(x) = \bar{x}$, there is $g \in G$ with $x_1 = gx$. Note that a closed path w in Γ is based at x iff $g \cdot w$ is based at $gx = x_1$. Thus $f_*\pi_1(\Gamma, x) = f_*\pi_1(\Gamma, x_1)$. We get that $N = [w]^{-1}N[w]$. This is for a general conjugate, so $N \lhd \pi_1(\Gamma/G, \bar{x})$. So we have proved points 1 and 2 so far.

Take $x \in V(\Gamma)$, and $\bar{x} = f(x)$. Let $Y = f^{-1}(\bar{x}) = O(x)$, that is, the orbit of x under G. Recall that $\pi_1(\Gamma/G)$ acts on Y, being $y \cdot [w]$ the ending point of $\hat{w}$, the lift of w at y.

On the other hand, we have that G acts freely and transitively on Y. So for any $y \in Y$ there is a unique $g \in G$ s.t. $y = gx$. Define

$$H : \pi_1(\Gamma/G) \to G \qquad \text{by} \qquad H([w]) = g \quad \text{iff} \quad x \cdot [w] = gx$$

Assume that $H([w]) = g$ and $H([v]) = h$. We have seen that $x \cdot [wv]$ is the ending point of $\hat{w}\hat{v}$ where $\hat{w}$ lifts w at x and $\hat{v}$ lifts v at $x \cdot [w]$. Since $g^{-1}(x \cdot [w]) = x$, the lift of v at x is $g^{-1} \cdot \hat{v}$. This gives $g^{-1}(x \cdot [wv]) = x \cdot [v] = hx$. So $x \cdot [wv] = (gh)x$. Thus $H([wv]) = gh = H([w])H([v])$, and H is an homomorphism.

It is clear that $x \cdot [w] = x$ iff $[w] \in N = \pi_1(\Gamma)$. So $\ker H = N$. And it is surjective if Γ is connected. For $g \in G$, there is a path v from x to gx. Then $[f(v)] \in \pi_1(\Gamma/G)$ maps to g under H. So we have $\pi_1(\Gamma/G)/N \cong G$, proving statement 3.

If the action is transitive on $V(\Gamma)$ then Γ/G has a single vertex. Let $\{\sigma_i\}$ be the edges of Γ/G, and let $s_i = H(\sigma_i) \in G$. Then $S = \{s_i\}$ is a generator for G. Labelling $\sigma \in E(\Gamma)$ with $H(f(\sigma))$ (the s_i corresponding to the projection of σ), we have that Γ is isomorphic to $\mathcal{C}(G, S)$.

From now on, when we say that a group acts on a graph, we will assume it acts by graph isomorphisms.

Corollary Let G be a group, and suppose it acts freely on a tree. Then G is a free group.

Let $G \curvearrowright T$ be a free action on a tree. Since T is connected, the last proposition says that $G \cong \pi_1(T/G)/\pi_1(T)$. But $\pi_1(T) = 1$ because T is a tree. So $G \cong \pi_1(T/G)$ and so it is free.

9 Splittings of groups

9.1 Free products

Let G and H be two groups. Recall that a word on the set $G \cup H$, is a sequence $w = x_1 \cdots x_n$ where $x_i \in G \cup H$. We consider the minimal equivalence relation on the set of these words that contains the following *elementary reductions*

1. $w = w_1 x w_2$ reduces to $v = w_1 w_2$ if x is either 1_G or 1_H.
2. $w = w_1 x y w_2$ reduces to $v = w_1 z w_2$ if either $x, y \in G$ or $x, y \in H$, and $z = xy$ in the corresponding group.

The word $w = x_1 \cdots x_n$ is *reduced* if it admits none of the above reductions. It is clear that w is reduced iff no x_i equals 1 and no two consecutive letters x_i, x_{i+1} belong to the same group (G or H).

We define $G * H$ as the set of equivalence classes of words on $G \cup H$. Let $[w]$ be the class of w. Then we define the product of classes as usual, $[w][v] = [vw]$.

Lemma

1. The product above is well defined, and makes $G * H$ into a group.
2. Each equivalence class in $G * H$ contains a unique reduced representative.

The proof is analogous as the case for free groups.

Notice that we have embeddings $G \hookrightarrow G * H$, $H \hookrightarrow G * H$ as one-letter words. We will identify their images with G and H as usual. Then $G * H$ is generated by G and H. They are not normal, unless one of them is trivial.

Remarks

1. The free product between groups satisfies $(G * H) * K \cong G * (H * K)$ and $G * H \cong H * G$, via natural isomorphisms.
2. $F_n = \mathbb{Z} * \cdots * \mathbb{Z}$, n times.
3. If G and H are non trivial, then $G * H$ is infinite.

The following is the analogous to the universal property for free groups.

Proposition(Universal property) Let $\varphi : G \to K$, $\psi : H \to K$ be homomorphisms. Then there exists a unique homomorphism $\chi : G * H \to K$ that restricts to the factors as $\chi|_G = \varphi$ and $\chi|_H = \psi$.

The map χ is often called $\varphi * \psi$. Free products can also be defined as those which satisfy such universal property. They also can be defined through presentations, as follows.

Proposition Let $G = \langle X | R \rangle$ and $H = \langle Y | S \rangle$. Then the free product has the presentation

$$G * H \cong \langle X, Y | R, S \rangle$$

Another consequence of the universal property is that when we have a group G, and $H_1, H_2 \leq G$ two subgroups, then $\langle H_1, H_2 \rangle \leq G$ is a quotient of $H_1 * H_2$.

9.2 Ping-Pong Lemma

The ping-pong lemma provides a way of recognizing free products. There are a few different versions, some specialized to free groups. The following is the most general for two factors.

Proposition(Ping-Pong lemma) Let G be a group, and H_1 and H_2 subgroups of G that are not $\{1\}$ and that generate G (i.e. $G = \langle H_1, H_2 \rangle$). Also assume that $|H_1| > 2$. Suppose there exists an action $G \curvearrowright X$, with two non-empty subsets $X_1, X_2 \subseteq X$, X_2 not included in X_1 such that

$$g(X_2) \subseteq X_1 \qquad \text{for } g \in H_1,\ g \neq 1$$

$$g(X_1) \subseteq X_2 \qquad \text{for } g \in H_2,\ g \neq 1$$

Then $G \cong H_1 * H_2$.

Let w be a reduced word on the letters $H_1 \cup H_2$, that is, an element of $H_1 * H_2$. We want to show that the element of G defined by w (i.e. the product in G of the letters of w) is different from 1. We denote this element also by w.

First assume that $w = a_1 b_1 \cdots a_{k-1} b_{k-1} a_k$ where $a_i \in H_1$, $b_i \in H_2$ (none equals 1). Then we have

$$w(X_2) = a_1 b_1 \cdots a_{k-1} b_{k-1} a_k(X_2) \subseteq a_1 b_1 \cdots a_{k-1} b_{k-1}(X_1) \subseteq a_1 b_1 \cdots a_{k-1}(X_2) \subseteq \cdots$$

$$\cdots \subseteq a_1(X_2) \subseteq X_1$$

So $w(X_2) \subseteq X_1$. Since $X_2 \nsubseteq X_1$, we get $w \neq 1$ in G.

We can reduce the general case to the one just discussed, by taking awa^{-1} for a suitable $a \in H_1$. Explicitely,

1. If $w = b_1 a_2 b_2 \cdots a_k b_k$, take any $a \in H_1$, $a \neq 1$.
2. If $w = a_1 b_1 \cdots a_k b_k$, take $a \in H_1$, $a \neq 1, a_1^{-1}$. (Recall $|H_1| > 2$).
3. If $w = b_1 a_2 b_2 \cdots a_k$ take $a \in H_1$, $a \neq 1, a_k$.

Then awa^{-1} is in the previous case, and so $awa^{-1} \neq 1$. We get $w \neq 1$.

Example Consider the matrices $A, B \in SL_2(\mathbb{Z})$ given by

$$A = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \qquad B = \begin{pmatrix} 1 & 0 \\ k & 1 \end{pmatrix}$$

where $k \geq 2$. Then A and B generate a free subgroup of rank 2 in $SL_2(\mathbb{Z})$.

To see this, consider the standard action of $SL_2(\mathbb{Z})$ in $\mathbb{Z}^2$, and let $X_1 = \{(x, y) \in \mathbb{Z}^2 : |x| < |y|\}$ and $X_2 = \{(x, y) \in \mathbb{Z}^2 : |y| < |x|\}$. Check they satisfy the ping-pong lemma.

9.3 Amalgamated products and HNN extensions

Let A, B and C be groups, and $\alpha : C \to A$, $\beta : C \to B$ be injective homomorphisms. Let

$$A = \langle X | R \rangle \qquad B = \langle Y | S \rangle$$

be presentations for A and B.

Definition

1. The *amalgamated product* of A and B over α and β is

   $$A *_C B = \langle X, Y | R, S, \alpha(c)\beta(c)^{-1} : c \in C \rangle$$

   we usually abuse notation and speak about the amalgamated product of A and B over C.

2. Now let $A = B$. The *HNN extension* of A over α and β is

   $$A *_C = \langle X, t | R, t\alpha(c)t^{-1}\beta(c)^{-1} : c \in C \rangle$$

   we call t the *stable letter*.

Note that $A *_C B = A * B / \langle\langle \alpha(c)\beta(c)^{-1} : c \in C \rangle\rangle$, so the amalgamated product depends only on A, B and the embeddings of C. Similarly, an HNN extension is a quotient of $A * \mathbb{Z}$, with the same property.

The groups A and B embed naturally into $A *_C B$. And C also embeds in $A *_C B$ through α or β, that give the same embedding. And the intersection of the embedded copies of A and B inside of $A *_C B$ is the mentioned copy of C. We will abuse notation and think of C as a subgroup of both A and B.

Respectively A embeds into $A *_C$, and with it C embedds in two ways, as $\alpha(C)$ and $\beta(C)$. In this case they are not identified, but note they are conjugate by t.

Lemma With the notations above, changing the maps α or β by an inner automorphism of C gives an isomorphic amalgamated product or HNN extension.

Suppose $\beta'(g) = \beta(cgc^{-1})$ for all $g \in C$. Then the isomorphisms are given as follows:
For the amalgamated products: conjugate the generators and relations of B by $\beta(c)^{-1}$.
For the HNN extensions: change the stable letter t to $s = \beta(c)^{-1}t$.

Examples

1. When $C = 1$, the amalgamted product reduces to the free product, i.e. $A *_C B = A * B$. For HNN extensions we have $A*_C = A * \mathbb{Z}$.
2. $\mathbb{Z}^{n+1} = \mathbb{Z}^n *_{\mathbb{Z}^n}$, where $\alpha = \beta = Id$.
3. The genus 2 orientable surface group is given by
$$G = \langle a_1, b_1, a_2, b_2 | \, [a_1, b_1][a_2, b_2] = 1\rangle$$
It can be written as an amalgamated product $G = F_2 *_{\mathbb{Z}} F_2$. Explicitely, the factors are $A = \langle a_1, b_1\rangle$ and $B = \langle a_2, b_2\rangle$. If $C = \langle c\rangle$ then $\alpha(c) = [a_1, b_1]$ and $\beta(c) = [a_2, b_2]^{-1}$.
4. That group also decomposes as an HNN extension $G = F_3 *_{\mathbb{Z}}$.
Here, $A = \langle a_1, b_1, a_2\rangle$ and $\alpha(c) = [a_1, b_1]a_2$, $\beta(c) = a_2$. The stable letter gives b_2^{-1}.

Amalgamated products and HNN extensions also have normal forms for their elements. First we deal with amalgamated products.

Definiton A *reduced word* in the amalgamated product $A *_C B$ is a word
$$w = a_1 b_1 \cdots a_n b_n$$
where $a_i \in A$, $b_i \in B$ and $a_i \notin C$ for $i > 1$, $b_i \notin C$ for $i < n$.

Proposition Every element $g \in A *_C B$ can be written as a reduced word $g = a_1 b_1 \cdots a_n b_n$. If $g = a'_1 b'_1 \cdots a'_k b'_k$ is another reduced word, then $n = k$ and $a'_i = c_i a_i$, $b'_i = d_i b_i$ for $c_i, d_i \in C$.

Choose sets of representatives S, T for the right cosets of C in A, B respectively. We assume that 1 is the representative of C in both cases. Then an element $g \in A *_C B$ has a unique normal form $g = cs_1 t_1 \cdots s_n t_n$, where $s_i \in S$, $t_i \in T$, $c \in C$ and $s_i \neq 1$ for $i > 1$, $t_i \neq 1$ for $i < n$. This statement implies the proposition, and can be proven by similar arguments to those we used in the case of free groups.

We can do almost the same with HNN extensions. We state the corresponding reduced form.

Definition A *reduced word* in the HNN-extension $A*_C$ is a word
$$a_1 t^{\epsilon_1} a_2 \cdots a_{n-1} t^{\epsilon_{n-1}} a_n$$
where $a_i \in A$, $\epsilon_i = \pm 1$ and if $\epsilon_i = -\epsilon_{i+1}$:
- If $\epsilon_i = 1$, then $a_{i+1} \notin \alpha(C)$.
- If $\epsilon_i = -1$, then $a_{i+1} \notin \beta(C)$.

There is a similat result that holds for the case of HNN extensions.

9.4 Graphs of groups

The amalgamated products and HNN extensions are often called *elementary splittings* of the resulting group G. Graphs of groups will encode the data for iteration of these constructions.

Definition A *graph of groups* consists on the following:

1. A connected finite graph Γ.
2. A group G_v for each vertex v of Γ.
3. A group G_e for each edge e of Γ, and two injective homomorphisms

$$\partial_e^+ : G_e \to G_{t(e)}$$

$$\partial_e^- : G_e \to G_{s(e)}$$

This is denoted by $(\Gamma, G, \partial^+, \partial^-)$, or simply by Γ

Note that one-edge graphs provide the data for an amalgamation (when the endpoints are different), or an HNN extension (when they agree).

Let Γ be a graph of groups. In what follows, we will define the *fundamental group* of Γ. First define $G(\Gamma)$ by the following presentation:

- Generators: the elements of G_v for the vertices $v \in V(\Gamma)$, and the edges $e \in E(\Gamma)$.
- Relations: the relations in G_v for each vertex v, and

$$e\partial_e^+(g)e^{-1} = \partial_e^-(g)$$

for $e \in E(\Gamma)$ and $g \in G_e$.

If $c = \sigma_1 \cdots \sigma_n$ is a path in Γ, then a *word of type* c is an element $w \in G(\Gamma)$ of the form

$$w = g_0 e_1^{\epsilon_1} g_1 \cdots g_{n-1} e_n^{\epsilon_n} g_n$$

where $\sigma_i = e_i^{\epsilon_i}$, $g_0 \in G_{s(\sigma_1)}$ and $g_i \in G_{t(\sigma_i)}$ for $i > 0$.

For v_0 a vertex of Γ, let $\pi_1(\Gamma, v_0)$ be the set of the $w \in G(\Gamma)$ s.t. w is a word of type c, for some c closed path based at v_0. Note that $\pi_1(\Gamma, v_0)$ is a subgroup of $G(\Gamma)$.

Remarks

1. Different choices of the basepoint v_0 give conjugate subgroups of $G(\Gamma)$.
2. Suppose Γ has only one edge e. If $s(e) \neq t(e)$ then $\pi_1(\Gamma) \cong G_{s(e)} *_{G_e} G_{t(e)}$. And if $s(e) = t(e)$, then $\pi_1(\Gamma) \cong G_{s(e)} *_{G_e}$.

Now we give a presentation for this fundamental group. If T is a spanning tree for Γ, let $\pi_1(\Gamma, T)$ be defined by the following presentation,

- Generators: the elements of G_v for the vertices $v \in V(\Gamma)$, and the edges $e \in E(\Gamma)$, $e \notin T$.
- Relations: the relations in G_v for each vertex v, and

$$\partial_e^+(g) = \partial_e^-(g) \qquad \text{for } e \in T,\ g \in G_e$$

$$e\partial_e^+(g)e^{-1} = \partial_e^-(g) \qquad \text{for } e \in E(\Gamma),\ e \notin T,\ g \in G_e$$

Proposition Let Γ be a graph of groups, v_0 a vertex in Γ and T a spanning tree. Then $\pi_1(\Gamma, v_0) \cong \pi_1(\Gamma, T)$.

Consider the homomorphism $G(\Gamma) \to \pi_1(\Gamma, T)$ that sends the edges $e \in T$ to 1, and all other generators to themselves. The restriction of this map to $\pi_1(\Gamma, v_0)$ is an isomorphism.

The fundamental group of a graph of groups corresponds to an iteration of amalgamated products and HNN extensions on it's vertex groups. This is implied by the following result.

Proposition Let Γ be a graph of groups, Γ' a connected subgraph, and Δ the graph obtained by collapsing Γ' to a vertex v, and setting $G_v = \pi_1(\Gamma')$. Then

$$\pi_1(\Gamma) \cong \pi_1(\Delta)$$

Let T' a spanning tree for Γ', and T a spanning tree for Γ containing T'. Let Λ be the tree obtained from T by contracting T' to v. Then it is a spanning tree for Δ. Define a map

$$\pi_1(\Gamma, T) \to \pi_1(\Delta, \Lambda)$$

by sending the generators in the above presentation as follows:
- Elements not in Γ' (be them vertex group elements, or edges not in T) map bijectively to $\Delta - \{v\}$.
- Elements of Γ' map to their image in $\pi_1(\Gamma', T') = G_v$.

It is clear that this map is an isomorphism.

Lastly, there is also a concept of reduced word for the case of a general graph of groups.

A word of type c in $G(\Gamma)$

$$w = g_0 e_1^{\epsilon_1} g_1 \cdots g_{n-1} e_n^{\epsilon_n} g_n$$

is *reduced* if the following holds:

-If $n = 0$, then $g_0 \neq 1$.

-If $n > 0$, whenever $e_i = e_{i+1}$ and $\epsilon_i = -\epsilon_{i+1}$, we have $g_i \notin \partial_{e_i}^{\epsilon_i}(G_{e_i})$

Proposition If w is a reduced word in $\pi_1(\Gamma)$, then w is not the identity.

If Γ' is a connected subgraph and Δ is the contraction of Γ to a vertex, then the inclusion

$$\pi_1(\Gamma') \to \pi_1(\Gamma)$$

and the map

$$\pi_1(\Gamma) \to \pi_1(\Delta)$$

take reduced words to reduced words. We know the theorem is true for graphs with one edge. So we use induction, using the last result.

10 Actions on trees

10.1 Introduction

For a group G, we consider actions $G \curvearrowright T$ where T is a tree, and G acts by graph isomorphisms. For any tree T, there is a metric on $V(T)$ given by

$$d(x, y) = \min\{l(w) : w \text{ path from } x \text{ to } y\}$$

where $l(w)$ is the length of w. This is the same as setting edges to have length 1. It is clear that this metric is preserved by the action. Recall that given two vertices x and y in a tree, there is a unique reduced path between them. This path realizes the distance $d(x, y)$. We denote it $[x, y]$.

We usually call *points* to the vertices of T.

Example Let T be the real line, with $\mathbb{Z}$ as the vertex set. For $a \in \mathbb{Z}$, define the action $\mathbb{Z} \curvearrowright T$ by $n \cdot x = x + na$. The tree T is called a *line*, and the action is called an *action by translations* on T.

In general, for $G \curvearrowright T$, T a tree, and $g \in G$ we define

$$l(g) = \min\{d(x, gx) : x \in T\}$$

this is called the *translation length* of g. It is clear that $l(g) = 0$ iff g has a fixed point. In this case g is called *elliptic*.

Proposition Let $G \curvearrowright T$, T a tree. Let $g \in G$ with $l(g) > 0$. Then there exists a unique subgraph $A \subset T$ such that

1. A is invariant under g.
2. A is isomorphic to a line.
3. The action of g on A is by translations of length $l(g)$. I.e. $\langle g \rangle \cong \mathbb{Z}$ and the action $\langle g \rangle \curvearrowright A$ is equivalent to the one in the previous example, with $a = l(g)$.

Let $x \in T$, and consider the paths $[x, gx]$ and $[x, g^{-1}x]$. Their intersection is of the form $[x, y]$ for some y (possibly $y = x$). Now gy belongs to $[x, gx]$, and $d(x, y) = d(gy, gx)$. If this distance were more than $d(x, y)/2$, then $[y, gy]$ is invariant under g, and so g would have a fixed point in $[y, gy]$. We are assuming this is not the case, so we have $[x, gx] = [x, y][y, gy][gy, gx]$. So $[g^{-1}y, y]$ and $[y, gy]$ meet only at y. Put

$$A = \bigcup_{j \in \mathbb{Z}} [g^j y, g^{j+1} y]$$

Properties 1 and 2 are clear. And if we start from x such that $l(g) = d(x, gx)$ we can see that we obtain $y = x$.

For uniqueness, let A be a line, invariant under g. Note that for any $x \in T$ there is a unique $y \in A$ such that $d(x, y) = \min\{d(x, z) : z \in A\}$. In this case $[x, y]$ and A meet only at y. So $[x, y][y, gy][gy, gx]$ is a reduced path, and thus A is obtained from the previous construction.

In the case of the proposition, g is called *hyperbolic* and $A = A_g$ is it's *translation axis*. Note that

$$A_g = \{x \in T : d(x, gx) = l(g)\}$$

If we define $d(x, A) = \min\{d(x, z) : z \in A\}$, then we have

$$d(x, gx) = 2d(x, A_g) + l(g)$$

for any $x \in T$.

These formulas are also true for g elliptic, and for $\mathrm{Fix}(g)$ instead of A_g.

Observe that $l(g^n) = |n|l(g)$ for $n \in \mathbb{Z}$. If g is elliptic this is clear. If it is hyperbolic, and $n \neq 0$, note that A_g is also a translation axis for g^n.

Proposition Let $G \curvearrowright T$, T a tree. Let $g, h \in G$. Then

1. $l(g) = l(hgh^{-1})$.
2. If they are hyperbolic $A_{hgh^{-1}} = hA_g$.

This is easy from the definition of $l(g)$, and the formulas above.

It is clear that a common fixed point of g and h is also a fixed point of gh. The following result is the reciprocal of this.

Lemma Let $g, h \in G$ be elliptic elements. Then gh is elliptic iff $\mathrm{Fix}(g) \cap \mathrm{Fix}(h) \neq \emptyset$.

Note that $\mathrm{Fix}(g)$ is a subtree, for if g fixes x and x', it also fixes every point in $[x, x']$. So there are $x \in \mathrm{Fix}(g)$ and $y \in \mathrm{Fix}(h)$ that minimize the distance. Then $[x, y]$ meets $\mathrm{Fix}(g)$ only at x and $\mathrm{Fix}(h)$ only at y. Because of that, $[y, x][x, gy]$ is reduced (so $[y, gy] = [y, x][x, gy]$), and meets $[(gh)^{-1}y, (gh)^{-1}gy]$ only at y. So the union of the translates of $[y, gy]$ under gh form a translation axis for gh.

Remark If $g \in G$ is elliptic and $x \in T$, then $[x, gx]$ has a middle point y (i.e. $d(x, y) = d(y, gx)$) and y is fixed by g.

Proposition(Serre's theorem) Let G be a f.g. group. If $G \curvearrowright T$, T a tree, such that every element is elliptic. Then T has a global fixed point.

Induction on the rank of G. Let $g_1, \ldots, g_n$ be a generator for G. If $n = 1$ it is trivial. For $n > 1$, let $H = \langle g_1, \ldots, g_{n-1} \rangle$. By induction, $H \curvearrowright T$ has a fixed point x. If x is fixed by g_n we are done. If not, let y be the middle point of $[x, g_n x]$. We have $g_n y = y$. If $h \in H$, then $[x, g_n hx] = [x, g_n x]$ and by the previous remark, y is fixed by $g_n h$, since it is elliptic. So y is fixed by all $h \in H$, as well as by g_n. Thus y is a global fixed point.

The action $G \curvearrowright T$ is called *minimal* if there are no proper invariant subtrees. We have just seen that if all elements are elliptic, then T is minimal iff it is reduced to a single point. We say that $G \curvearrowright T$ is *non-trivial* if there is some hyperbolic element.

Lemma Let $G \curvearrowright T$ non-trivial. There is a unique invariant subtree T' such that $G \curvearrowright T'$ is minimal.

Note that the intersection of invariant subtrees is also an invariant subtree, and use Zorn's lemma. Such T' has to contain the translation axes of the hyperbolic elements. In fact it can be shown to be equal to the union of these axes. To see it, check that if A_g and A_h are disjoint, then gh is hyperbolic and A_{gh} meets both A_g and A_h.

An action $G \curvearrowright T$ is *cocompact* if T/G is a finite graph.

Lemma Let G be a f.g. group, and $G \curvearrowright T$ be minimal. Then it is cocompact.

Let $g_1, \ldots, g_n$ be a generator for G. Take $x \in T$. Let D be the convex hull in T of $x, g_1 x, \ldots, g_n x$, that is, the minimal tree containing such points. D is clearly finite. So

$$T = \bigcup_{g \in G} gD$$

because the RHS is an invariant subtree, and T is minimal. So $T/G = D/G$ and it is finite.

10.2 Action induced by a graph of groups

For a graph of groups Γ, we will define an action of the fundamental group $\pi_1(\Gamma)$ on a tree. Let $G = \pi_1(\Gamma, T)$ for T a spanning tree of Γ.

Now we will construct an action of G on a tree $\tilde{X}$, such that

$$\Gamma = \tilde{X}/G$$

Define the set of vertices (resp. edges) of $\tilde{X}$ to be the set of left cosets in G of the vertex groups G_v of Γ (resp. the edge groups G_e), i.e.:

$$V(\tilde{X}) = \bigsqcup_{v \in V(\Gamma)} G/G_v$$

$$E(\tilde{X}) = \bigsqcup_{e \in E(\Gamma)} G/G_e$$

(because of the defining relations of G, there is a standard inclusion of each G_e into G).
The graph structure is defined by:

$$s(gG_e) = gG_{s(e)}$$

$$t(gG_e) = geG_{t(e)}$$

where it's assumed that $e = 1$ if $e \in T$.

Note that G acts on $\tilde{X}$ by left multiplication on the cosets, and it acts by graph isomorphisms. Note also that $\Gamma = \tilde{X}/G$.

Proposition $\tilde{X}$ is a tree.

First we prove that $\tilde{X}$ is connected.

For each edge $e \in T$, the edge G_e of $\tilde{X}$ connects $G_{s(e)}$ to $G_{t(e)}$. Hence all vertices of the form G_v for $v \in V(\Gamma)$ can be joined to each other. In fact they form a tree that projects isomorphically onto T. The same is true for the vertices of the form gG_v, $v \in V(\Gamma)$ for a fixed $g \in G$ (because G acts on $\tilde{X}$).

We will show that any vertex of $\tilde{X}$ can be joined to one of the form G_v. In the case of a vertex gG_v where $g \in G_u$, we've seen that gG_v can be joined with $gG_u = G_u$. In the case of eG_v where e is an edge, we can join this vertex with $eG_{t(e)}$ and this is connected with $G_{s(e)}$ by the edge G_e. Since G is generated by the G_v and the edges of Γ, we can proceed by induction.

Next we show that $\tilde{X}$ is simply connected.

Suppose we have a reduced closed path γ in $\tilde{X}$ based at G_{v_0}. Note that if there is an edge between gG_u and hG_v, then u and v are the endpoints of an edge e in Γ, and we can take h to be gg_0e^{ϵ}, where $g_0 \in G_u$ and $\epsilon = \pm 1$. Applying this we can write the i-th vertex of γ as $h_iG_{v_i}$ where

$$h_i = g_0 e_1^{\epsilon_1} g_1 \cdots g_{i-1} e_i^{\epsilon_i}$$

Then h_n is a word of type c, where n is the length of γ and c the projection of γ in Γ.

Since γ is closed, we have $h_nG_{v_n} = G_{v_0}$ and so $h_n \in G_{v_0}$. Put $g_n = h_n^{-1}$. Then

$$g = g_0 e_1^{\epsilon_1} g_1 \cdots e_n^{\epsilon_n} g_n = 1$$

is a word of type c, equal to the identity in $G = \pi_1(\Gamma, T)$.

On the other hand, γ admits a reduction iff there is some i with $v_i = v_{i+2}$ and $h_iG_{v_i} = h_{i+2}G_{v_i}$, i.e. iff $e_{i+1} = e_{i+2}$, $\epsilon_{i+1} = -\epsilon_{i+2}$ and $g_{i+1} \in \partial_{e_{i+1}}^{\epsilon_{i+1}}(G_{e_{i+1}})$. So γ is reduced iff g is a reduced word.

So we have a reduced word equal to the identity in G, a contradiction.

10.3 Bass-Serre theory

We are going to see that any cocompact action of a group G on a tree arise as the one just defined, for a decomposition $G \cong \pi_1(\Gamma)$ where Γ is some graph of groups.

Let $G \curvearrowright X$ be cocompact, X a graph. We associate a graph of groups to this action. Let

$$\Gamma = X/G$$

note it is a finite graph.

For each vertex v (edge e) of Γ, choose a lift $\tilde{v}$ (resp. $\tilde{e}$) in X, and define

$$G_v = \mathrm{Stab}_G(\tilde{v})$$

$$G_e = \mathrm{Stab}_G(\tilde{e})$$

If e is an edge of Γ and $v = t(e)$, let's define the map $\partial_e^+ : G_e \to G_v$. By construction, there is an element $g \in G$ such that $g \cdot \tilde{e}$ has $\tilde{v}$ as target. Then we have

$$gG_eg^{-1} = \mathrm{Stab}_G(g \cdot \tilde{e}) \subset \mathrm{Stab}_G(\tilde{v}) = G_v$$

Let ∂_e^+ be the conjugation by g followed by this inclussion.

The maps ∂^- are defined in the analogous way.

Different choices of the lifts $\tilde{v}$, $\tilde{e}$ give equivalent graphs in the following sense. Let $(\Gamma, \bar{G}, \bar{\partial}^+, \bar{\partial}^-)$ be obtained from another such choice of lifts. Then,

- For any vertex v (edge e) of Γ, there are isomorphisms $f_v : G_v \to \bar{G}_v$ (resp. f_e), that are given by conjugations by elements of G.
- If $v = t(e)$, then $f_v \circ \partial_e^+ = \bar{\partial}_e^+ \circ f_e$, possibly up to an inner automorphism of G_e. The same holds for $v = s(e)$ and the maps ∂^-, $\bar{\partial}^-$.

Remark Suppose that Γ is a graph of groups, $G = \pi_1(\Gamma)$ and $\tilde{X}$ is the tree defined in the previous section. Note that the above construction applied to $\tilde{X}$ gives a graph of groups that is equivalent to Γ.

Theorem Let G be a group, and $G \curvearrowright X$ a cocompact action on a tree. Let $\Gamma = X/G$ be the associated graph of groups. Then $G \cong \pi_1(\Gamma)$.

Let T be a spanning tree for $\Gamma = X/G$, and let

$$j : T \to X$$

be a lifting. So $j(T)$ is a tree that projects isomorphically to T. Extend j for the edges $e \in E(\Gamma)$, $e \notin T$, setting $j(e)$ to be an edge of X projecting to e and starting at $j(s(e))$ (i.e. $s(j(e)) = j(s(e))$). Since $j(e)$ projects to e, there is $\gamma_e \in G$ such that

$$t(j(e)) = \gamma_e j(t(e))$$

Set $\gamma_e = 1$ for $e \in T$.

Recall that Γ can be constructed with

$$G_v = \mathrm{Stab}_G(j(v))$$

$$G_e = \mathrm{Stab}_G(j(e))$$

even when X is not a tree.

Let

$$\phi : \pi_1(\Gamma, T) \to G$$

be the homomorphism that restricts to the generators as $G_v \hookrightarrow G$ (standard inclussion) and $\phi(e) = \gamma_e$. It exists, since the relations on the generators of $\pi_1(\Gamma, T)$ hold for their images in G.

Let $\tilde{X}$ be the tree associated to Γ as in the previous section, and

$$\psi : \tilde{X} \to X$$

be defined by $\psi(gG_v) = \phi(g)j(v)$ for $g \in \pi_1(\Gamma, T)$ and v a vertex of Γ (same for the edges). Then ψ is a graph map.

- ψ is onto: It is easy to check that $\psi(\tilde{X})$ is closed in X (with the topology coming from the metric d). It is also open: if $w = \psi(gG_v) = \phi(g)j(v)$ and f is an edge of X adjacent to w, let e be the projection of f to Γ and take $h \in G$ so that $f = h\phi(g)j(e)$. Then

$$h \in \mathrm{Stab}_G(w) = \phi(g)G_v\phi(g)^{-1}$$

and so $h = \phi(h_0)$ and $f = \phi(h_0 g)j(e)$ is in $\psi(\tilde{X})$. So, for every vertex in $\psi(\tilde{X})$ we have a neighborhood of it inside $\psi(\tilde{X})$. Since X is connected, ψ is onto.

- ϕ is onto: Let $g \in G$, and take v a vertex of Γ. Since ψ is onto, we have

$$gj(v) = \psi(hG_v) = \phi(h)j(v)$$

for some $h \in \pi_1(\Gamma, T)$. Then $g\phi(h)^{-1} \in G_v \subset \mathrm{Im}\phi$ and so $g \in \mathrm{Im}\phi$.

Now, for $v \in V(\Gamma)$ we have $\ker\phi \cap G_v = 1$ (and the same for edges $e \in E(\Gamma)$). So the restricted action $\ker\phi \curvearrowright \tilde{X}$ is free.

On the other hand, if $\psi(gG_v) = \psi(hG_v)$ then $\phi(g^{-1}h) \in G_v$ and so $g^{-1}h \in \ker\phi \cdot G_v$, by the previous observation. So $hG_v = gkG_v$ for some $k \in \ker\phi$. Since $\ker\phi$ is normal, the inverse image under ψ of $\psi(gG_v)$ can also be written as $\{kgG_v : k \in \ker\phi\}$. But this is the orbit of gG_v under the action of $\ker\phi$. The same is true for an edge e in place of v.

Thus X can be identified with $\tilde{X}/\ker\phi$, and $\psi : \tilde{X} \to X$ with the quotient map, that is a covering.

Now we finally use that X is a tree. Since a tree is simply connected, every connected covering of it is an isomorphism. So $\ker\phi = 1$, and $\phi : \pi_1(\Gamma, T) \to G$ is an isomorphism.

These results establish a correspondence between cocompact actions of G on trees, and decompositions of G as a fundamental group of a graph of groups. In this context, the action $G \curvearrowright T$, and the graph Γ with $G = \pi_1(\Gamma)$ are associated iff

- $\Gamma = T/G$
- G_x is the stabilizer of some point projecting to x, for x vertex or edge of Γ.

This is called the Bass-Serre correspondence.

10.4 Applications on free products

Here we prove Kurosh's classification of the subgroups of a free product, using Bass-Serre theory. We restrict to the case of f.g. subgroups, the general case involves the theory with infinite graphs of groups.

Theorem(Kurosh) Let $G = A * B$, and $H \leq G$ finitely generated. Then there exist $A_1, \ldots, A_n \leq A$, $g_1, \ldots, g_n \in G$, $B_1, \ldots, B_m \leq B$, $h_1, \ldots, h_m \in G$ and $X \subset G$ finite, such that

$$H \cong (*_i g_i A_i g_i^{-1}) * (*_j h_j B_j h_j^{-1}) * F(X)$$

Let Γ be the one-edge graph with two vertices, whose groups are A and B, and the edge group is 1. Then $G = \pi_1(\Gamma)$. Let T be it's Bass-Serre tree. Then H also acts on T by restricting the action of G. Let T' be the minimal subtree for H, that is cocompact because H is f.g., and let $\Gamma' = T'/H$ be the associated graph of groups. Let $x \in \Gamma'$, vertex or edge, and H_x it's group in Γ'. So $H_x = \mathrm{Stab}_H(\tilde{x})$ for $\tilde{x} \in T'$ projecting to x. Note that $\mathrm{Stab}_H(\tilde{x}) \leq \mathrm{Stab}_G(\tilde{x})$. So, if x is an edge then $H_x = 1$. And if x is a vertex, then H_x is a subgroup of a conjugate of A or B. Let $g_i A_i g_i^{-1}$, $h_j B_j h_j^{-1}$ be the vertex groups of Γ'. Since all edge groups are trivial, it is easy to show that $H \cong \pi_1(\Gamma')$ has the form given in the statement.