18. Generators and Relations

Definition-Lemma 18.1. *Let A be a set. A **word** in A is any string of elements of A and their inverses. We say that the word w' is obtained from w by a **reduction**, if we can get from w to w' by repeatedly applying the following rule,*

- *replace either aa^{-1} or $a^{-1}a$ by the empty string.*

*Given any word w, the **reduced word** w' associated to w is any word obtained from w by reduction, such that w' cannot be reduced any further.*

*Given two words w_1 and w_2 of A, the **concatenation** of w_1 and w_2 is the word $w = w_1w_2$. The empty word is denoted e.*

*The set of all reduced words is denoted F_A. With product defined as the reduced concatenation, this set becomes a group, called the **free group with generators** A.*

It is interesting to look at examples. Suppose that A contains one element a. Then any element of $F_A = F_a$, is equal to a string $w = aaaa^{-1}a^{-1}aaa$ etc. Given any such word, we pass to the reduction w' of w. This means cancelling as much as we can, and replacing strings of a's by the corresponding power. Thus

$$\begin{aligned} w &= aaa^{-1}aaa \\ &= aaaa \\ &= a^4 = w', \end{aligned}$$

where equality means up to reduction. Thus the free group on one generator is isomorphic to $\mathbb{Z}$.

The free group on two generators is much more complicated and it is not abelian. A typical reduced word might be

$$a^3b^{-2}a^5b^{13}.$$

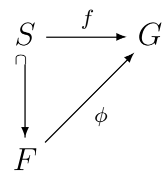
Clearly $F_{a,b}$ has quite a few elements. Free groups have a very useful universal property.

Lemma 18.2. *Let $F = F_S$ be a free group with generators S. Let G be any group. Suppose that we are given a function $f\colon S \longrightarrow G$.*

Then there is a unique homomorphism

$$\phi\colon F \longrightarrow G$$

that extends f. In other words, the following diagram commutes



Proof. Given a reduced word w in F, send this to the element given by replacing every letter by its image in G. It is easy to see that this is a homomorphism, as there are no relations between the elements of F. □

In other words if $S = \{a, b\}$ and you send a to g and b to h then you have no choice but to send $w = a^2b^{-3}a$ to $g^2h^{-3}g$, whatever that element is in G.

This gives us a convenient way to present a group G. Pick generators S of G. Then we get a homomorphism

$$\phi\colon F_S \longrightarrow G.$$

As S generates G, ϕ is surjective. Let the kernel be H. By the First Isomorphism Theorem, G is isomorphic to F_S/H. To describe H, we need to write down generators R for H. These generators are called relations, since they describe relations amongs the generators, such that if we mod out by these relations, then we get G.

Definition 18.3. *A* ***presentation*** *of a group G is a choice of generators S of G and a description of the* ***relations*** *R amongst these generators.*

It is probably easiest to give some examples.

Let G be a cyclic group of order n. Pick a generator a. Then we get a homomorphism

$$\phi\colon F_a \longrightarrow G.$$

The kernel of ϕ is equal to H, which contains all elements of the form a^m, where m is a multiple of n, $H = \langle a^n \rangle$. Thus a presentation for G is given by the single generator a with the single relation $a^n = e$.

Take the group D_4, the symmetries of the square. This has two natural generators g and f, where g is rotation through $2\pi/4 = \pi/2$ and f is reflection about a diagonal.

Thus we get a map

$$F_{a,b} \longrightarrow D_4$$

given by sending a to g and b to f. What are the relations, that is, what is the kernel? Well $f^2 = e$ and $g^4 = e$, so two obvious relations are f^2 and g^4. On the other hand

$$fgf^{-1} = g^{-1}.$$

Using this relation, any word w can be manipulated into the form

$$f^i g^j,$$

where $i \in \{0, 1\}$ and $j \in \{0, 1, 2, 3\}$. Since this gives eight elements of the quotient and there are eight elements of G, it follows that the kernel is generated by

$$f^2, g^4, fgf^{-1}g.$$

There are many ways to present the symmetric group S_n. One way is to take the transpositions

$$\tau_i = (i, i+1) \qquad \text{where} \qquad 1 \leq i \leq n-1.$$

The relations are then

$$\tau_i^2 = e, \qquad (\tau_i \tau_{i+1})^3 = e \qquad \text{and} \qquad (\tau_i \tau_j)^2 = e,$$

where $|i - j| > 1$.

Definition 18.4. *Let S be a set. The* ***free abelian group*** *A_S* ***generated by*** *S is the quotient of F_S, the free group generated by S, and the relations R given by the commutators of the elements of S.*

Let $S = \{a, b\}$. Then $A_{a,b}$ is isomorphic to $\mathbb{Z} \times \mathbb{Z}$. Similarly for any finite set:

Lemma 18.5. *The free abelian group on n generators is isomorphic to the product of n copies of $\mathbb{Z}$.*

Proof. We do the case $n = 2$. There are two maps $f_i \colon \{a, b\} \longrightarrow \mathbb{Z}$. The first sends a to 1 and b to 0 and the second sends a to 0 and b to 1. By the universal property of the free group $F_{a,b}$ there are two group homomorphisms $\phi_i \colon F_{a,b} \longrightarrow \mathbb{Z}$.

Since $\mathbb{Z}$ is abelian we get two group homomorphism $\psi_i \colon A_{a,b} \longrightarrow \mathbb{Z}$, by the universal property of the commutator subgroup.

Finally by the universal property of the product there is a group homomorphism $\psi \colon A_{a,b} \longrightarrow \mathbb{Z} \times \mathbb{Z}$. We have $\psi(a) = (1, 0)$ and $\psi(b) = (0, 1)$. The image of ψ is the whole of $\mathbb{Z} \times \mathbb{Z}$ as $(1, 0)$ and $(0, 1)$ are generators of $\mathbb{Z} \times \mathbb{Z}$.

The elements of $A_{a,b}$ are of the form $a^m b^n$. It is clear that the kernel is trivial so that ψ is an isomorphism. □

Lemma 18.6. *Let S be any set and let G be any abelian group. Given any map $f \colon S \longrightarrow G$ there is a unique homomorphism*

$$A_S \longrightarrow G.$$

Proof. As F_S is a free group, there is a unique homomorphism

$$\phi\colon F_S \longrightarrow G.$$

As G is abelian the kernel of ϕ contains the commutator subgroup. But then, as A_S is by definition the quotient of F_S by the commutator subgroup, there is a unique map $A_S \longrightarrow G$ extending f. □

In the proof of (18.5) we could have deduced the existence of the group homomorphisms ψ_i directly from f_i using the universal property of $A_{a,b}$.

Lemma 18.7. *Let G be any finitely generated abelian group.*
Then G is a quotient of $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$.

Proof. Pick a finite set of generators S of G. By (18.6) there is a unique homomorphism

$$A_S \longrightarrow G.$$

As S generates G this map is surjective. On the other hand A_S is isomorphic to a product of copies of $\mathbb{Z}$. □

Theorem 18.8. *Let G be a finitely generated abelian group.*
Then G is isomorphic to $\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z} \times T$, where T may be presented uniquely as either,

(1) $\mathbb{Z}_{q_1} \times \mathbb{Z}_{q_2} \times \cdots \times \mathbb{Z}_{q_r}$, where each q_i is a power of a prime, or
(2) $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_r}$, where $m_i | m_{i+1}$.

Given this, we can classify all abelian groups of a fixed finite order. For example, take $n = 60 = 2^2 \cdot 3 \cdot 5$. Then we have

$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \qquad \text{or} \qquad \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_5,$$

using the first representation, or

$$\mathbb{Z}_2 \times \mathbb{Z}_{30} \qquad \text{or} \qquad \mathbb{Z}_{60}$$

using the second representation.

Finally let me mention that in general if one is given generators and relations, it can be very hard to describe the resulting quotient.

Theorem 18.9. *There is no effective algorithm to solve any of the following problems,*
Given relations R, decide if

(1) two words w_1 and w_2 are equivalent, modulo the relations.
(2) a word w is equivalent, modulo the relations, to the identity.

Succintly, the method of representing groups by generators and relations is an art not a science.