Advanced Algebra I

FREE GROUPS AND PRESENTATION OF GROUPS

For any given non-empty set X, we would like to construct a free group $F(X)$ associate to X which is universal w.r.t all functions from X to groups. That is:

Theorem 0.1. *Let X be a non-empty set. There is a group $F(X)$ and a map $\imath : X \to F(X)$ satisfying the following "unerversal property":*

For any function $f : X \to G$ to a group G, there is a unique group homomorphism $\bar{f} : F \to G$ such that $\bar{f} \circ \imath = f$.

One way to prove it is to construct the free group out of X. The idea is to construct a group out of X without any constrain. To do this, we start with X, and then we need the inverse, and identity. And moreover, we need element of the form $x_1 x_2 ...$ etc. After we successfully constructed the group, it's natural that the group $F(X)$ have the universal property.

Proof. Let X be a non-empty set. Let

$$X_0 := (X \times \{1, -1\}) \cup \{1\}.$$

By abuse the notation, we identify X with $X \times \{1\}$ and X^{-1} with $X \times \{-1\}$. And we have the inverse maps $\mu : X \to X^{-1}$ and $\nu : X^{-1} \to X$. We denote the image of inverse maps at $a \in X_0 - \{1\}$ by a^{-1}.

A word on X is a sequence $(a_1, a_2, ...)$ such that $a_i \in X_0$ and there is n_0 such that $a_i = 1$ for all $i > n_0$. (We call it a word of length n_0.)

Given two words $w_1 := (a_1, a_2, ..., a_n, 1, ...), w_2 := (b_1, b_2, ..., b_m, 1...)$ of length n, m respectively, one can compose them to obtain a word

$$w_1 \circ w_2 := (a_1, ..., a_n, b_1, ..., b_m, 1, ...).$$

A word w (of length n) is said to be reduced if

(1) $a_i \neq 1$ for $i \leq n$.
(2) $a_{i+1} \neq a_i^{-1}$ for all $i < n$.

Let W be the set of all words on X and let $F(X)$ be the set of reduced words. It's tedious but elementary to show that there is a well-defined map from $W \to F(X)$. Moreover, the composition on W induces a well-defined composition on $F(X)$.

One can check that $F(X)$ together with composition of words is a group. Moreover, one has $\imath : X \to F(X)$ given by $x \mapsto (x, 1, ...)$.

For simplicity, given a reduced word $(a_1, .., a_n, 1, ...)$, we denote it by $a_1 a_2 ... a_n$.

Lastly, we prove the universal property. Let $f : X \to G$ be a function from X to a group G. One can produce a map $\bar{f} : F(X) \to G$ by $\bar{f}(a_1 ... a_n) := f(a_1) ... f(a_n)$. One checks that this is a group homomorphism and also $\bar{f} \circ \imath = f$.

It remains to prove the uniqueness of the homomorphism $\bar{f}$. Suppose one has a group homomorphism $g : F(X) \to G$ such that $g \circ \imath = f$. Then $g(x) = f(x) = \bar{f}(x)$ for all $x \in X$. One checks that $g(w) = \bar{f}(w)$ by induction on length of reduced word $w \in F(X)$.

□

Proposition 0.2. *Let G be a group, then there is a free group F map onto G. In particular, any group G can be realized as F/N for some free group F and normal subgroup $N \lhd G$.*

Proof. Given a group G. We can take $F = F(G)$. The identity map $i_G : G \to G$ induces a group homomorphism $\bar{f} : F(G) \to G$ by the universal property. It's clear that this homomorphism is surjective. Let N be $ker(\bar{f}$. It follows by the first homomorphism theorem that $G \cong F/N$. □

In general, given a non-empty set X and a set (possibly empty) of reduced words R, one can produced a free group $F(X)$ and a normal subgroup generated by R, denoted N. This give rise to a group $< X|R >:= F(X)/N$. We call it *the group generated by X with relations R.*

Example 0.3. *Let $X = \{x, y\}$ and $R = \{xyx^{-1}y^{-1}\}$, then $< X|R >\cong \mathbb{Z}^2$.*

Example 0.4. *Let $X = \{x, y\}$ and $R = \{x^n, y^2, xyxy\}$, then $< X|R >\cong D_n$.*

Remark 0.5. *If the generators and relations are given explicitly as in the previous examples, we usually write it as $< x, y|x^n = y^2 = 1, (xy)^2 = 1 >$.*

It's in general not easy to determine the structure of the groups of the type $< X|R >$. We present here the *Todd-Coxeter algorithm* if $< X|R >$ is finite. Please note that we don't have good criterion for finiteness of $< X|R >$ yet.

The idea behind the Todd-Coxeter algorithm is the following: if $G :=< X|R >$ is finite, then one has an embedding $G \to S_{|G|}$ by Cayley's theorem. For elements in G and label it by $1, 2, 3..$ and so on. Make tables out of the relation which basically describe the multiplication table of G (or how they correspond to permutations). Once the tables are completed, then we are done.

Please notice that if G is infinite, then the procedure will never end.

For more detail, please see [Ar] p.223- or [Ro] p. 351-.

[Ar] M. Artin, *Algebra, Prentice-Hall International edition.*

[Ro] J. Rotman, *An Introduction to the Theory of Groups, GTM 148.*