1.14 Free Groups

Roughly speaking, a free group over a set X is the largest possible group generated by X. The only relations are the ones required by the group axioms.

1.14.1 Definition. A group F is ***free*** over a set $X \subseteq F$ if, for any group G and any map $\xi : X \to G$, there is a unique group homomorphism $\varphi : F \to G$ such that $\varphi(x) = \xi(x)$ for all $x \in X$.

This definition mimics the construction of a linear map from a vector space with basis to another vector space. Specifically, if $\{v_1, v_2, \dots, v_n\}$ is a basis of a vector space V and W is a vector space with $w_1, w_2, \dots, w_n \in W$, then there is a unique linear map $T : V \to W$ such that $T(v_i) = w_i$ for all $1 \leqslant i \leqslant n$.

1.14.2 Proposition. *Free groups over the sets X and X' are isomorphic if and only if we have $|X| = |X'|$.*

Proof. Suppose that F and F' are free groups over X and X'. Let $i : X \to F$ and $i' : X' \to F'$ be the canonical inclusion maps. Since $|X| = |X'|$, there is a bijection $\tau : X \to X'$. Applying the definition of a free group to the maps $i' \circ \tau : X \to F'$ and $i \circ \tau^{-1} : X' \to F$, we obtain group homomorphisms $\varphi : F \to F'$ and $\theta : F' \to F$ that restrict to $i \circ \tau$ and $i \circ \tau^{-1}$ respectively. Hence, the map $\theta \circ \varphi : F \to F$ restricts to the identity on X and the map $\varphi \circ \theta : F' \to F'$ restricts to the identity on X'. Therefore, the uniqueness part of the definition implies that $\theta \circ \varphi = \mathrm{id}_F$ and $\varphi \circ \theta = \mathrm{id}_{F'}$, so the group homomorphisms φ and θ are mutually inverse and $F \cong F'$. □

Proposition 1.14.2 proves that any two free groups over the same set are isomorphic.

1.14.3 Definition. The ***rank*** of the free group over a set is just the cardinality of the set.

Nothing in their definition ensures that free groups actually exist.

1.14.4 Proposition. *There exists a free group over any nonempty set.*

Proof. Let X be a nonempty set. Choose a set disjoint from X with the same cardinality. Denote this second set by $X^{-1} := \{x^{-1} \mid x \in X\}$. A ***word*** in $X \cup X^{-1}$ is a finite sequence of symbols $w = x_1^{\epsilon_1} x_2^{\epsilon_2} \cdots x_r^{\epsilon_r}$ where $x_i \in X$, $\epsilon_i = \pm 1$, and r is a nonnegative integer. The sequence is empty when $r = 0$ and the ***empty word*** is denoted by 1. The ***product*** of the words $w = x_1^{\epsilon_1} x_2^{\epsilon_2} \cdots x_r^{\epsilon_r}$ and $v = y_1^{\delta_1} y_2^{\delta_2} \cdots y_s^{\delta_s}$ is given by juxtaposition $wv = x_1^{\epsilon_1} x_2^{\epsilon_2} \cdots x_r^{\epsilon_r} y_1^{\delta_1} y_2^{\delta_2} \cdots y_s^{\delta_s}$. By definition, the ***inverse*** of the word w is $w^{-1} := x_r^{-\epsilon_r} \cdots x_2^{-\epsilon_2} x_1^{-\epsilon_1}$.

The number r is the ***length*** of the word and we set $|w| := r$.

By definition, we have $w1 = w = 1w$.

Let W be the set of all words in $X \cup X^{-1}$. We define an equivalence relation on W as follows. Two words w and v are equivalent, $w \sim v$, if it is possible to pass from one word to the other by means of a finite sequence of the following basic operations:

- insertion of an xx^{-1} or $x^{-1}x$ as consecutive elements;
- deletion of consecutive elements of the form xx^{-1} or $x^{-1}x$.

It follows that this relation is transitive, symmetric and reflexive. The equivalence class to which w belongs is denoted $[w]$.

Let $F := W/\sim$ be the set of all equivalence classes. Given $w \sim w'$ and $v \sim v'$, we see that $wv \sim w'v'$, so the product $[w][v] = [wv]$

is well-defined. Since we have $(wv)u = wvu = w(vu)$, it follows that $([w][v])[u] = [(wv)u] = [w(vu)] = [w]([v][u])$. We also have $[w][1] = [w] = [1][w]$ and $[w][w^{-1}] = [ww^{-1}] = [1]$. Therefore, F is a group and we have an inclusion $X \to F$ given by $x \mapsto [x]$.

To show that the group F is free over X, let G be an arbitrary group and let $\xi : X \to G$ be any map. Consider the map $\widetilde{\varphi} : W \to G$ defined by $\widetilde{\varphi}(x_1^{\epsilon_1} \cdots x_r^{\epsilon_r}) := \xi(x_1)^{\epsilon_1} \cdots \xi(x_r)^{\epsilon_r}$. When $w \sim w'$, we see that $\widetilde{\varphi}(w) = \widetilde{\varphi}(w')$ because products like gg^{-1} and $g^{-1}g$ equal e_G in the group G. Hence, we obtain a well-defined map $\varphi : F \to G$. Moreover, we have

$$\begin{aligned}\varphi([w][v]) &= \varphi([wv]) = [\widetilde{\varphi}(wv)] \\ &= [\widetilde{\varphi}(w)\widetilde{\varphi}(v)] = [\widetilde{\varphi}(w)][\widetilde{\varphi}(v)] = \varphi([w])\varphi([v])\end{aligned}$$

so φ is a group homomorphism extending ξ. It is clearly unique.

To see that the map $x \mapsto [x]$ defines a bijection from X to $[X]$, let G be any group with $|G| \geqslant |X|$ and let $\xi : X \to G$ be an injection. Since $\varphi([x]) = \xi(x)$ for all $x \in X$, we deduce that $x \mapsto [x]$ must define a bijection. □

The equivalence classes used to construct $F := W/\sim$ have preferred representatives.

1.14.5 Definition. A word is ***reduced*** if it contains neither xx^{-1} nor $x^{-1}x$ as a substring.

1.14.6 Proposition. *Each equivalence class of words in X contains a unique reduced word.* □

Sketch of Proof. We have $x^{\varepsilon}x^{-\varepsilon} \sim 1$ for all $x \in X \cup X^{-1}$. Since deleting such a pair reduces the length, each equivalence class contains a reduced word.

Suppose that an equivalence class contains two distinct reduced words w and w'. There is a sequence $w = w_0, w_1, \dots, w_\ell = w'$ of words such that w_{i-1} and w_i are related by a basic operation. Choose this sequence to minimize the sum of the lengths $|w_i|$. Two words related by a basic operation differ in length by 2 and cannot both be reduced, so $\ell > 1$. Choose i such that $|w_i|$ is maximal. It follows that $0 < i < r$ and $|w_{i-1}| = |w_{i+1}| = |w_i| - 2$. If these two deleted substrings of w_i are disjoint, then we can reverse the order of the substititions and obtain another sequence with $|w_i| = |w_{i-1}| - 2$ which contradicts the minimality of the sequence. On the other hand, if these two substrings are not disjoint, then either they are equal or they are the substrings of $x^{\varepsilon}x^{-\varepsilon}$, $x^{-\varepsilon}x^{\varepsilon}$ of a substring $x^{\varepsilon}x^{-\varepsilon}x^{\varepsilon}$ of w_i. In both cases, we have $w_{i-1} = w_{i+1}$ so we can shorten the sequence contradicting minimality. □

1.15 Generators and Relations

Free groups allow one to describe any group in terms of generators and relations. Before formalizing this idea, we collect a few easy consequences of our construction of free groups.

1.15.1 Corollary. *When $|X| \geqslant 2$, the free group over X is nonabelian.*

Proof. For any two distinct elements $x, y \in X$, the word $x^{-1}y^{-1}xy$ is reduced which means $x^{-1}y^{-1}xy \neq 1$ so $xy \neq yx$. □

1.15.2 Corollary. *Every element, except for the identity, in a free group has infinite order.*

The free group over the one-element set $\{x\}$ is an infinite cyclic group and hence isomorphic to $\mathbb{Z}$.

Proof. Consider a free group over a set X. Given an element $x \in X$, the word $\underbrace{x\,x \cdots x}_{n\text{-times}}$ is reduced, so $\underbrace{x\,x \cdots x}_{n\text{-times}} \neq 1$. Hence, element x does not have finite order. □

1.15.3 Corollary. *Let F be the free group over the two-element set $\{x, y\}$. The three elements $u := x^2$, $v := y^2$ and $w := xy$ generate a subgroup isomorphic to the free group over the three-element set $\{u, v, w\}$.*

Proof. Let F' be the free group on $\{u, v, w\}$. The map defined by $u \mapsto x^2$, $v \mapsto y^2$, and $w \mapsto xy$ determines a group homomorphism $\varphi : F' \to F$. Since the images of uv, vu, uw, wu, vw and wv are all reduced words in $\{x, y, z\}$, a reduced word in $\{u, v, w\} \cup \{u^{-1}, v^{-1}, w^{-1}\}$ maps to a reduced word in $\{x^2, y^2, xy\} \cup \{x^{-1}, y^{-1}, (xy)^{-1}\}$. Hence, the kernel of the map φ is trivial and the map φ is injective. □

1.15.4 Proposition. *Every group is a quotient of a free group.*

Proof. Let X be a set for which there exists a bijection $\xi : X \to G$ and let F be the free group on X. Hence, there exists a surjective group homomorphism $\varphi : F \to G$, so $G \cong F/\operatorname{Ker}(\varphi)$. □

1.15.5 Definition. A ***presentation*** of a group G is given by surjective homomorphism ψ from a free group F over a set X to G. We call the set X the ***generators*** of G and a set R such that $\langle R \rangle = \operatorname{Ker}(\psi)$ ***relations***. One often writes $G = \langle X \mid R \rangle$.

Informally, $\langle X \mid R \rangle$ is the 'largest' group that is generated by X in which all of the strings $w \in R$ represent the identity element.

1.15.6 Example. The cyclic group of order 6 can be presented as either $\langle x \mid x^6 \rangle$ or $\langle a, b \mid a^3, b^2, a^{-1}b^{-1}ab \rangle$. ◇

1.15.7 Example. The free group has a presentation $\langle X \mid \varnothing \rangle$. ◇

1.15.8 Theorem (Von Dyck). *Let $G := \langle x_1, \dots, x_n \mid r_j, j \in J \rangle$. Given a group $H := \langle h_1, \dots, h_n \rangle$ such that $r_j(h_1, \dots, h_n) = e_H$ for all $j \in J$, there exists a surjective group homomorphism $\varphi : G \to H$ such that $\varphi(x_i) = y_i$ for all $1 \leqslant i \leqslant n$.*

Walther von Dyck (1882) provided the first systematic study of presentations of groups by generators and relations.

Proof. Let F be the free group over the set $\{x_1, \dots, x_n\}$. There is a group homomorphism $\varphi : F \to H$ with $\varphi(x_i) = h_i$. Since we have $r_j(h_1, \dots, h_n) = e_H$ for all $j \in j$, it follows that $r_j \in \operatorname{Ker}(\varphi)$. By the First Isomorphism Theorem, the map φ induces a surjective group homomorphism $G = F/\operatorname{Ker}(\varphi) \to H$. □

1.15.9 Problem. For all integers n greater than 1, show that the dihedral group D_n has a presentation $\langle x, y \mid x^n, y^2, yxyx \rangle$.

Proof. Let G be the group defined by the given presentation. Theorem 1.15.8 produces a surjective group homomorphism $\varphi : G \to D_n$, which sends x to a rotation by $2\pi/n$ and y to a reflection. We see that $|G| \geqslant 2n$. The cyclic subgroup $\langle x \rangle$ in G has order at most n, because $x^n = e_G$. The relation $yxy^{-1} = x^{-1}$ implies that $\langle x \rangle$ is a normal subgroup of G. It follows that $G/\langle x \rangle s$ is generated by the image of y. Finally, the equation $y^2 = e_G$ shows that $|G/\langle x \rangle| \leqslant 2$. We conclude that $|G| = |\langle x \rangle|\,|G/\langle x \rangle| \leqslant 2n$. □

1.15.10 Remark. Given integer ℓ, m, and n such that $1 < \ell \leqslant m \leqslant n$, the group $G := \langle x, y, z \mid x^\ell, y^m, z^n, xyz \rangle$ is finite if and only if

$$\frac{1}{|G|} = \frac{1}{\ell} + \frac{1}{m} + \frac{1}{n} - 1 > 0\,.$$

This condition is satisfied only when
- $\ell = m = 2$ and $n \geqslant 2$, or
- $\ell = 2$, $m = 3$, and $3 \leqslant n \leqslant 5$.

We are at the beginning of combinatorial group theory which explores how much can be said about a group given a presentation.
- A group G has a solvable word problem if it has a presentation $G = \langle X \mid R \rangle$ for which there exists an algorithm to determine whether an arbitrary word is equal to the identity. Novikov (1955) showed that there exists there exists a finitely presented group such that the word problem is undecidable.
- Presentations play an important role in algebraic topology. Van Kampen's theorem yields presentations for fundamental groups. Moreover, topological techniques provide a "natural" prove of the Nielsen-Schreier theorem: every subgroup of a free group is free.
- One can study the growth rates of a group (with respect to a symmetric generating set). Gromov characterizes finitely generated groups having a polynomial growth rate as those groups which have nilpotent subgroups of finite index.
- One can introduce a metric: the word metric measures the length of the shortest path in the Cayley graph.