16. Free groups I

Recall the following elementary fact from Lecture 2: If G is a group and X is a generating set of G, then any $g \in G$ can be written as

$$g = x_1^{\varepsilon_1} \dots x_k^{\varepsilon_k} \text{ where } x_i \in X, \varepsilon_i = \pm 1, \text{ and if }$$
$$x_{i+1} = x_i \text{ for some } i, \text{ then } \varepsilon_{i+1} \neq \varepsilon_i \text{ (we allow } k = 0).$$

In this lecture we will construct a free group on X – this will be a group generated by X such that any element has unique factorization of the above form. Equivalently, there will be no non-trivial relations between the elements of X in this group, so the group will be "free of relations".

16.1. **Explicit construction of free groups.** Let X be a set, and let $X^{-1} = \{x^{-1} : x \in X\}$ be the set of formal inverses of elements of X. At this point the symbol x^{-1} does not have any special meaning; all we really require is that X^{-1} is another set such that $|X^{-1}| = |X|$ and $X \cap X^{-1} = \emptyset$.

Let $\Omega(X)$ be the set of all (finite) words in the alphabet $X \cup X^{-1}$, that is, the set of all sequences $x_1 \dots x_k$ with $x_i \in X \cup X^{-1}$. We assume that $\Omega(X)$ contains the empty sequence denoted by e. Define the multiplication on $\Omega(X)$ in the natural way

$$w \cdot v = \text{ concatenation of } w \text{ and } v.$$

Clealrly, this multiplication is associative and the empty word e is an identity element, so $\Omega(X)$ is a monoid. Note that $\Omega(X)$ is not a group; in fact, e is the only invertible element of $\Omega(X)$.

Next we define an equivalence relation on $\Omega(X)$: given $w, v \in \Omega(X)$, we set $w \sim v$ if w can be obtained from v by a finite sequence of operations of the form

(i) insert a subword of the form xx^{-1} or $x^{-1}x$ with $x \in X$
(ii) delete a subword of the form xx^{-1} or $x^{-1}x$ with $x \in X$

Note: by a subword of a word w we mean a subsequence consisting of several *consecutive* letters of w.

Now let $F(X) = \Omega(X)/\sim$ be the set of equivalence classes with respect to the equivalence relation $\sim$. As usual by $[w]$ we denote the equivalence class of $w \in \Omega(X)$.

Define multiplication on $F(X)$ by setting

$$[w] \cdot [v] = [wv].$$

This multiplication is

- well defined – this is almost obvious from definition
- associative since multiplication on $\Omega(X)$ is associative and
- $[e]$ is clearly an identity element

Finally, observe that any element of $F(X)$ is invertible: if $w = x_1^{\varepsilon_1} \dots x_k^{\varepsilon_k}$ with $x_i \in X$ and $\varepsilon_i = \pm 1$, we put $v = x_k^{-\varepsilon_k} \dots x_1^{-\varepsilon_1}$. Then clearly $[w][v] = [v][w] = [e]$.

Thus, we proved that $F(X)$ is a group. In fact it is a free group on X we were looking for, but to prove the latter we need a more transparent description of $F(X)$.

Definition. A word $w \in \Omega(X)$ is called reduced if f does not contain subwords xx^{-1} or $x^{-1}x$ with $x \in X$. We shall denote the set of reduced words by $\Omega_{\text{red}}(X)$.

Proposition 16.1. *For any $w \in \Omega(X)$ there exists a unique reduced word v such that $w \sim v$.*

Proof. The existence is clear: if w is not reduced, we delete a subword xx^{-1} or $x^{-1}x$, and repeat the procedure until we get a reduced word.

Suppose now that uniqueness does not hold, so there exist distinct reduced words u and v with $u \sim v$. By definition there exists a sequence

$$u = w_0, w_1, \dots, w_k = v \qquad (***)$$

where each w_{i+1} is obtained from w_i by inserting or removing a subword of the form xx^{-1} or $x^{-1}x$.

For each $w \in \Omega(X)$ let $|w|$ be the length of w, that is, the number of symbols in w. Among all sequences of the form (***) choose one for which $|w_0| + |w_1| + \ldots + |w_k|$ is smallest possible.

Note: $|w_0| < |w_1|$ and $|w_{k-1}| > |w_k|$ since w_0 and w_k are reduced, and $|w_{i+1}| \neq |w_i|$ for each i.

Hence there exists i such that $|w_{i-1}| < |w_i| > |w_{i+1}|$, so

w_{i-1} is obtained from w_i by deleting some subword aa^{-1}, with $a \in X \cup X^{-1}$

w_{i+1} is obtained from w_i by deleting some subword bb^{-1}, with $b \in X \cup X^{-1}$.

Case 1: aa^{-1} and bb^{-1} do not intersect (as subwords of w_i).

Without loss of generality we can assume that aa^{-1} is located to the left of bb^{-1}. Then there exist subwords P, Q and R of w_i such that

$$w_i = Paa^{-1}Qbb^{-1}R, \quad w_{i-1} = PQbb^{-1}R \quad \text{and } w_{i+1} = Paa^{-1}QR$$

Set $w_i' = PQR$. Then $w_0, w_1, \dots, w_{i-1}, w_i', w_{i+1}, \dots, w_k$ is still an admissible sequence connecting u and v, but its length is smaller than that of the original sequence since $|w_i'| = |w_i| - 4$, which contradicts our assumption.

Case 2: Subwords aa^{-1} and bb^{-1} intersect.
We can still write $w_{i-1} = PQ$ and $w_i = Paa^{-1}Q$. There are 3 subcases:
Subcase 1: the subwords aa^{-1} and bb^{-1} are located in the same place. Then $b = a$, and by construction $w_{i+1} = PQ = w_{i-1}$. Thus, we can get an admissible sequence of smaller length by removing w_i and w_{i+1}.
Subcase 2: the subword bb^{-1} is located one position to the right of aa^{-1}. Thus $a^{-1} = b$ and $Q = aQ'$ for some Q', so that $w_{i-1} = PaQ'$ and $w_{i+1} = Paa^{-1}(aQ') = Pa(bb^{-1})Q'$. Again by construction $w_{i+1} = PaQ' = w_{i-1}$, and we reach a contradiction as in Case 1.
Subcase 3: the subword bb^{-1} is located one position to the left of aa^{-1}. This is analogous to subcase 2. □

Having proved Proposition 16.1, we can state a more explicit definition of the free group $F(X)$.

Corollary 16.2. *The free group $F(X)$ can be identified with the set $\Omega_{\text{red}}(X)$ of reduced words in $X \cup X^{-1}$, with multiplication defined by*

$$v \cdot w = \text{ unique reduced word equivalent to } v \circ w,$$

where $v \circ w$ is the concatenation of v and w.

From now on we will usually think of $F(X)$ as the set of reduced words in $\Omega(X)$, and we will refer to $F(X)$ as the standard free group on X. While we are yet to give an abstract definition of a free group, Proposition 16.1 shows that $F(X)$ has the desired property we formulated at the beginning of the lecture:

Corollary 16.3. *Let X be a set. Every element of the standard free group $F(X)$ can be uniquely written as $f = x_1^{\varepsilon_1} \dots x_k^{\varepsilon_k}$ where $x_i \in X, \varepsilon_i = \pm 1,$ and if $x_{i+1} = x_i$ for some $i,$ then $\varepsilon_{i+1} \neq \varepsilon_i$.*