Free groups

Contents

1 Free groups

1.1 Definitions and notations

Let G be a group. If H is a subgroup of G then we write $H \leq G$; if H is a normal subgroup of G we write $H \trianglelefteq G$. For a subset $A \subseteq G$ by $\langle A \rangle$ we denote the subgroup of G generated by A (the intersection of all subgroups of G containing A). It is easy to see that

$$\langle A \rangle = \{a_{i_1}^{\varepsilon_1}, \ldots, a_{i_n}^{\varepsilon_n} \mid \ a_{i_j} \in A, \ \varepsilon_j \in \{1, -1\}, \ n \in N\}$$

To treat expressions like $a_{i_1}^{\varepsilon_1}, \ldots, a_{i_n}^{\varepsilon_n}$ a little bit more formally we need some terminology.

Let X be an arbitrary set. A *word* in X is a finite sequence of elements (perhaps, empty) w which we write as $w = y_1 \ldots y_n$ ($y_i \in X$). The number n is called the *length* of the word w, we denote it by $|w|$. We denote the empty word by ϵ and put $|\epsilon| = 0$.

Consider

$$X^{-1} = \{x^{-1} | x \in X\},$$

where x^{-1} is just a formal expression obtained from x and -1. If $x \in X$ then the symbols x and x^{-1} are called *literals* in X. Denote by

$$X^{\pm 1} = X \cup X^{-1}$$

the set of all literals in X. For a literal $y \in X^{\pm 1}$ we define y^{-1} as

$$y^{-1} = \begin{cases} x^{-1}, & \text{if } y = x \in X; \\ x, & \text{if } y = x^{-1} \in X. \end{cases}$$

An expression of the type

$$w = x_{i_1}^{\varepsilon_1} \cdots x_{i_n}^{\varepsilon_n} \quad (x_{i_j} \in X, \varepsilon_j \in \{1, -1\}), \tag{1}$$

is called a *group word* in X. So a group word in X is just a word in the alphabet $X^{\pm 1}$.

A group word

$$w = y_1 \ldots y_n, \quad (y_i \in X^{\pm 1})$$

is *reduced* if for any $i = i, \ldots, n-1$ $y_i \neq y_{i+1}^{-1}$, i.e., w does not contain a subword of the type yy^{-1} for a literal $y \in X^{\pm 1}$. We assume also that the empty word is reduced.

If $X \subseteq G$ then every group word $w = x_{i_1}^{\varepsilon_1} \cdots x_{i_n}^{\varepsilon_n}$ in X determines a unique element from G which is equal to the product $x_{i_1}^{\varepsilon_1} \cdots x_{i_n}^{\varepsilon_n}$ of the elements $x_{i_j}^{\varepsilon_j} \in G$.

In particular, the empty word ϵ determines the identity 1 of G.

Definition 1 *A group G is called a free group if there exists a generating set X of G such that every non-empty reduced group word in X defines a non-trivial element of G.*

In this event X is called a *free basis* of G and G is called *free on X* or *freely generated by X*. It follows from the definition that every element of a free group on X can be defined by a reduced group word on X. Moreover, different reduced words on X define different elements in G. We will say more about this in the next section.

1.2 Construction of a free group with basis X

Let X be an arbitrary set. In this section we construct the canonical free group with basis X. To this end we need to describe a *reduction process* which allows one to obtain a reduced word from an arbitrary word.

An *elementary reduction* of a group word w consists of deleting a subword of the type yy^{-1} $(y \in X^{\pm 1})$ from w.

For example, suppose $w = uyy^{-1}v$ for some words u, v in $X^{\pm 1}$. Then the elementary reduction of w with respect to the given subword yy^{-1} results in the word uv. In this event we write

$$uyy^{-1}v \to uv.$$

A *reduction* of w (or a *reduction process* starting at w) consists of consequent applications of elementary reductions starting at w and ending at a reduced word:

$$w \to w_1 \to \cdots \to w_n, \quad (w_n \textit{ is reduced}).$$

The word w_n is termed a *reduced form* of w.

In general, there may be different possible reductions of w. Nevertheless, it turns out that all possible reductions of w end up with the same reduced form. To see this we need the following lemma.

Lemma 1 *For any two elementary reductions $w \to w_1$ and $w \to w_2$ of a group word w in X there exist elementary reductions $w_1 \to w_0$ and $w_2 \to w_0$, so the following diagram commutes:*

$$\begin{tikzcd}
& w \arrow[dl] \arrow[dr] & \\
w_1 \arrow[dr, dashed] & & w_2 \arrow[dl, dashed] \\
& w_0 &
\end{tikzcd}$$

Proof Let $w \overset{\lambda_1}{\to} w_1$, and $w \overset{\lambda_2}{\to} w_2$ be elementary reductions of a word w. There are two possible ways to carry out the reductions λ_1 and λ_2.

Case a) (disjoint reductions). In this case

$$w = u_1 y_1 y_1^{-1} u_2 y_2 y_2^{-1} u_3, \quad (y_i \in X^{\pm 1})$$

and λ_i deletes the subword $y_i y_i^{-1}, i = 1, 2$. Then

$$w \overset{\lambda_1}{\to} u_1 u_2 y_2 y_2^{-1} u_3 \overset{\lambda_2}{\to} u_1 u_2 u_3$$

$$w \overset{\lambda_2}{\to} u_1 y_1 y_1^{-1} u_2 u_3 \overset{\lambda_1}{\to} u_1 u_2 u_3.$$

Hence the lemma holds.

Case b) (overlapping reductions). In this case $y_1 = y_2$ and w takes on the following form

$$w = u_1 y y^{-1} y u_2.$$

Then

$$w = u_1 y(y^{-1}y)u_2 \xrightarrow{\lambda_2} u_1 y u_2,$$

$$w = u_1(yy^{-1})yu_2 \xrightarrow{\lambda_1} u_1 y u_2;$$

and the lemma holds.

□

Proposition 1 *Let w be a group word in X. Then any two reductions of w:*

$$w \to w'_1 \to \cdots \to w'_n$$

$$w \to w''_1 \to \cdots \to w''_m$$

result in the same reduced form, i. e. , $w'_n = w''_m$.

Proof. Induction on $|w|$. If $|w| = 0$ then w is reduced and there is nothing to prove. Let now $|w| \geq 1$ and

$$w \to w'_1 \to \cdots \to w'_n$$

$$w \to w''_1 \to \cdots w''_m$$

be two reductions of w. Then by Lemma 1 there are elementary reductions $w'_1 \to w_0$ and $w''_1 \to w_0$. Consider a reduction process for w_0 :

$$w_0 \to w_1 \to \cdots \to w_k.$$

This corresponds to the following diagram:

$$\begin{tikzcd}
 & & w \arrow[dl] \arrow[dr] & & \\
 & w_1' \arrow[dl, dashed] \arrow[dr, dashed] & & w_2'' \arrow[dl, dashed] \arrow[dr, dashed] & \\
w_n' & & w_0 \arrow[d, dashed] & & w_m'' \\
 & & w_k & &
\end{tikzcd}$$

By induction all reduced forms of the word w_1' are equal to each other, as well as all reduced forms of w_1''. Since w_k is a reduced form of both w_1' and w_1'', then $w_n' = w_k = w_m''$ as desired. This proves the proposition.

□

For a group word w by $\overline{w}$ we denote the unique reduced form of w.

Let $F(X)$ be the set of all reduced words in $X^{\pm 1}$. For $u, v \in F(X)$ we define multiplication $u \cdot v$ as follows:

$$u \cdot v = \overline{uv}.$$

Theorem 1 *The set $F(x)$ forms a group with respect to the multiplication $\cdot$. This group is free on X.*

Proof. The multiplication defined above is associative:

$$(u \cdot v) \cdot w = u \cdot (v \cdot w)$$

for any $u, v, w \in F(X)$. To see this it suffices to prove that

$$\overline{\overline{(uv)}w} = \overline{u(\overline{vw})}$$

for given u, v, w. Observe, that each of the reduced words $\overline{\overline{(uv)}w}, \overline{u(\overline{vw})}$ can be obtained form the word uvw by a sequence of elementary reductions, hence by Proposition 1

$$\overline{\overline{uv}w} = \overline{uvw} = \overline{u\overline{vw}}.$$

Clearly, the empty word ϵ is the identity in $F(X)$ with respect to the multiplication above, i.e.,

$$\epsilon \cdot w = w \cdot \epsilon$$

for every $w \in F(X)$. For this reason we usually denote ϵ by 1.

Let $w = y_1 \cdots y_n$, $y_i \in X^{\pm 1}$. Then the word

$$w^{-1} = y_n^{-1} \cdots y_1^{-1}$$

is also reduced and

$$w \cdot w^{-1} = \overline{y_1 \cdots y_n y_n^{-1} \cdots y_1^{-1}} = 1.$$

Hence w^{-1} is the inverse of w. This shows that $F(X)$ satisfies all the axioms of a group.

Notice that X is a generating set of $F(X)$ and every non-empty reduced word

$$w = x_{i_1}^{\varepsilon_1} \cdots x_{i_n}^{\varepsilon_n}$$

in $X^{\pm 1}$ defines a non-trivial element in $F(X)$ (the word w itself). Hence X is a free basis of $F(X)$, so that $F(X)$ is free on X.

□

Digression. The reduction process above is a particular instance of a rewriting system in action. Now we pause for a while to discuss *rewriting systems* in general.

the discussion follows

1.3 The universal property of free groups.

Theorem 2 *Let G be a group with a generating set $X \subseteq G$. Then G is free on X if and only if the following universal property holds: every map $\varphi : X \to H$ from X into a group H can be extended to a unique homomorphism $\varphi^* : G \to H$, so that the diagram below commutes*

$$\begin{tikzcd}
X \arrow[r, "i"] \arrow[dr, "\phi"'] & G \arrow[d, dotted, "\phi^*"] \\
& H
\end{tikzcd}$$

(here $X \xrightarrow{i} G$ is the inclusion of X into G).

Proof. Let G be a free group freely generated by X and $\varphi : X \to H$ a map from X into a group H. Since G is free on X then every element $g \in G$ is defined by a unique reduced word in $X^{\pm 1}$,

$$g = x_{i_1}^{\varepsilon_1} \cdots x_{i_n}^{\varepsilon_n}, \quad (x_{i_j} \in X, \varepsilon_i \in \{1, -1\}).$$

Put

$$g^{\varphi^*} = (x_{i_1}^{\varphi})^{\varepsilon_1} \ldots (x_{i_n}^{\varphi})_{i_n}^{\varepsilon_n}. \tag{2}$$

We claim that φ^* is a homomorphism. Indeed, let $g, h \in G$ and

$$g = y_1 \cdots y_n z_1 \cdots z_m,$$

$$h = z_m^{-1} \cdots z_1^{-1} y_{n+1} \cdots y_k,$$

are the corresponding reduced words in $X^{\pm 1}$, where $y_i, z_j \in X^{\pm 1}$ and $y_n \neq y_{n+1}^{-1}$ (we allow the subwords $y_1 \cdots y_n$, $z_1 \cdots z_m$, and $y_{n+1} \cdots y_k$ to be empty). Then

$$gh = y_1 \cdots y_n y_{n+1} \cdots y_k$$

is a reduced word in $X^{\pm 1}$ presenting gh. Now

$$(gh)^{\varphi^*} = y_1^{\varphi^*} \ldots y_n^{\varphi^*} y_{n+1}^{\varphi^*} \ldots y_n^{\varphi^*} =$$

$$= y_1^{\varphi^*} \ldots y_n^{\varphi^*} z_1^{\varphi^*} \ldots z_m^{\varphi^*} (z_m^{\varphi^*})^{-1} \ldots (z_1^{\varphi^*})^{-1} \ldots y_{n+1}^{\varphi^*} \ldots y_k^{\varphi^*} = g^{\varphi^*} h^{\varphi^*}.$$

Hence φ^* is a homomorphism.

Clearly, φ^* extends φ and the corresponding diagram commutes. Observe that any homomorphism $\varphi^* : G \to H$, that makes the diagram commutative, must satisfy the equalities 2, so φ^* is unique. This shows that G satisfies the required universal property.

Suppose now that a group G with a generating set X satisfies the universal property. Take $H = F(X)$ and define a map $\varphi : X \to H$ by $x^{\varphi} = x$, $(x \in X)$. Then by the universal property φ extends to a unique homomorphism $\varphi^* : G \to F(X)$.

Let w be a non-empty reduced group word on X. Then w defines an element g in G for which $g^{\varphi^*} = w \in F(X)$. Hence $g^{\varphi^*} \neq 1$ and consequently $g \neq 1$ in G. This shows that G is a free group on X. This proves the theorem. □

Observe, that the argument above implies the following result, which we state as a corollary.

Corollary 1 *Let G be a free group on X. Then the identical map $X \to X$ extends to an isomorphism $G \to F(X)$.*

This corollary allows us to identify a free group freely generated by X with the group $F(X)$. In what follows we usually refer to the group $F(X)$ as to a free group on X.

Digression. Defining various free objects (groups, rings, etc.) via their universal properties is a standard way to define universal objects in category theory.

the discussion follows

References: see any book on category theory, for example:
S. MacLane *Categories for the Working Mathematician*, 1972,
S. MacLane *Homology*, Springer, 1967.

1.4 Presentations of groups

The universal property of free groups allows one to describe arbitrary groups in terms of *generators* and *relators*.

Let G be a group with a generating set X. By the universal property of free groups there exists a homomorphism $\psi : F(X) \to G$ such that $\psi(x) = x$ for $x \in X$. It follows that ψ is onto, so by the first isomorphism theorem

$$G \simeq F(X)/\ker(\psi).$$

In this event $\ker(\psi)$ is viewed as the set of relators of G, and a group word $w \in \ker(\psi)$ is called a *relator* of G in generators X. If a subset $R \subseteq \ker(\psi)$ generates $\ker(\psi)$ as a normal subgroup of $F(X)$ then it is termed a set of *defining relations* of G relative to X. The pair $\langle X \mid R\rangle$ is called a *presentation* of G, it determines G uniquely up to isomorphism. The presentation $\langle X \mid R\rangle$ is finite if both sets X and R are finite. A group is *finitely presented* if it has at least one finite presentation. Presentations provide a universal method to describe groups. In particular, finitely presented groups admit finite descriptions. How easy is to work with groups given by finite presentations - is another matter. The whole spectrum of algorithmic problems in combinatorial group theory arose as an attempt to answer this question. We will discuss this in due course.

Digression. Presentations of groups lie in the heart of combinatorial group theory. They are the source of many great achievements and big disappointments. We are not going to mention relevant results here. Instead, we refer to few books on the subject.

References:

Magnus W., Karrass A., Solitar D. *Combinatorial group theory*, New York, Wiley, 1966.

Johnson , *Presentations of groups*,

More advanced:

Lyndon R., Schupp P. *Combinatorial Group Theory*, Springer, 1977.

Epstein D. and all *Word Processing in Groups*, Jones and Bartlett Publishers, Boston, 1992.

1.5 Rank of free groups

Theorem 3 *If G is free on X and also on Y, then $|X| = |Y|$.*

Proof. By the universal property of free groups any map $X \to \mathbf{Z}_2$ gives rise to a homomorphism of G into the cyclic group $\mathbf{Z}_2$ of order 2. Moreover, every homomorphism $G \to \mathbf{Z}_2$ can be obtained in this way (every homomorphism is completely defined by its values on a given generating set). Hence there are exactly $2^{|X|}$ different homomorphism form G into $\mathbf{Z}_2$. This implies that

$$2^{|X|} = 2^{|Y|}$$

and, assuming Generalized Continuum Hypothesis from set theory, $|X| = |Y|$. In fact, one may avoid using the Generalized Continuum Hypothesis here, indeed, when one of the sets X or Y is finite the result follows as above. If both of them are infinite then the result follows from an observation that cardinality of a group generated by an infinite set A is equal to $|A|$. This proves the theorem.

Corollary 2 *Let X and Y be sets. Then*

$$F(X) \simeq F(Y) \Leftrightarrow |X| = |Y|.$$

Theorem 3 shows that the cardinality of a basis of a free group G is an invariant of G which characterizes G uniquely up to an isomorphism.

Definition 2 *Let G be a free group on X. Then the cardinality of X is called the rank of G.*

Sometimes we refer to a free group of rank n as to F_n.

Notice that if $X \subseteq Y$ then the subgroup $\langle X \rangle$ generated by X in $F(Y)$ is itself a free group with basis X. This implies that if m and n are cardinals and $n \leq m$, then F_n is embeddable into F_m.

We will show now that in some sense the reverse is also true for finite or countable ranks.

Proposition 2 *Any countable free group G is embeddable into a free group of rank 2.*

Proof. To prove the result it suffices to find a free subgroup of countable rank in a free group of rank 2.

Let F_2 be a free group with a basis $\{a, b\}$. Denote

$$x_n = b^{-n}ab^n \quad (n = 0, 1, 2, \dots)$$

and put

$$X = \{x_0, x_1, \dots\}.$$

We claim that X freely generates the subgroup $\langle X \rangle$ in F_2. Indeed, let

$$w = x_{i_1}^{\varepsilon_1} \dots x_{i_n}^{\varepsilon_n}$$

be a reduced non-empty word in $X^{\pm 1}$. Then w can also be viewed as a word in $\{a, b\}$:

$$w = b^{-i_1}a^{\varepsilon_1}b^{i_1}b^{-i_2}a^{\varepsilon_2}b^{i_2} \dots b^{-i_n}a^{\varepsilon_n}b^{i_n}.$$

Since w is reduced on X, then for each $j = 1, \dots, n-1$ either $i_j \neq i_{j+1}$ or $i_j = i_{j+1}$ and $\varepsilon_j + \varepsilon_{j+1} \neq 0$. In either case any reduction of w (as a word on $\{a, b\}$) does not affect a^{ε_j} and $a^{\varepsilon_{j+1}}$ in the subword

$$b^{-i_j}a^{\varepsilon_j}b^{i_j}b^{-i_{j+1}}a^{\varepsilon_{j+1}}b^{i_{j+1}};$$

i.e., the literals a^{ε_j} and $a^{\varepsilon_{j+1}}$ are present in the reduced form of w as a word in $\{a, b\}^{\pm 1}$. Hence the reduced form of w is non-empty, so $w \neq 1$ in F_2. Clearly, $\langle X \rangle$ is a free group of countable rank.

□

Digression

Similar results are true for many other relatively free groups.

the discussion follows

References: