Theorem 16. $F(S)$ is a group under the binary operation defined above.

Proof: One easily checks that 1 is an identity and that the inverse of the reduced word $s_1^{\epsilon_1}s_2^{\epsilon_2}\dots s_n^{\epsilon_n}$ is the reduced word $s_n^{-\epsilon_n}s_{n-1}^{-\epsilon_{n-1}}\dots s_1^{-\epsilon_1}$. The difficult part of the proof is the verification of the associative law. This can be done by induction on the "length" of the words involved and considering various cases or one can proceed as follows: For each $s \in S \cup S^{-1} \cup \{1\}$ define $\sigma_s : F(S) \to F(S)$ by

$$\sigma_s(s_1^{\epsilon_1}s_2^{\epsilon_2}\dots s_n^{\epsilon_n}) = \begin{cases} s \cdot s_1^{\epsilon_1}s_2^{\epsilon_2}\dots s_n^{\epsilon_n}, & \text{if } s_1^{\epsilon_1} \neq s^{-1} \\ s_2^{\epsilon_2}s_3^{\epsilon_3}\dots s_n^{\epsilon_n}, & \text{if } s_1^{\epsilon_1} = s^{-1}. \end{cases}$$

Since $\sigma_{s^{-1}} \circ \sigma_s$ is the identity map of $F(S) \to F(S)$, σ_s is a permutation of $F(S)$. Let $A(F)$ be the subgroup of the symmetric group on the set $F(S)$ which is generated by $\{\sigma_s \mid s \in S\}$. It is easy to see that the map

$$s_1^{\epsilon_1}s_2^{\epsilon_2}\dots s_n^{\epsilon_n} \mapsto \sigma_{s_1}^{\epsilon_1} \circ \sigma_{s_2}^{\epsilon_2} \circ \dots \circ \sigma_{s_n}^{\epsilon_n}$$

is a (set) bijection between $F(S)$ and $A(S)$ which respects their binary operations. Since $A(S)$ is a group, hence associative, so is $F(S)$.

The universal property of free groups now follows easily.

Theorem 17. Let G be a group, S a set and $\varphi : S \to G$ a set map. Then there is a unique group homomorphism $\Phi : F(S) \to G$ such that the following diagram commutes:

$$\begin{tikzcd}
S \arrow[r, "\text{inclusion}"] \arrow[dr, "\varphi"'] & F(S) \arrow[d, "\Phi"] \\
& G
\end{tikzcd}$$

Proof: Such a map Φ must satisfy $\Phi(s_1^{\epsilon_1}s_2^{\epsilon_2}\dots s_n^{\epsilon_n}) = \varphi(s_1)^{\epsilon_1}\varphi(s_2)^{\epsilon_2}\dots\varphi(s_n)^{\epsilon_n}$ if it is to be a homomorphism (which proves uniqueness), and it is straightforward to check that this map is in fact a homomorphism (which proves existence).

Corollary 18. $F(S)$ is unique up to a unique isomorphism which is the identity map on the set S.

Proof: This follows from the universal property. Suppose $F(S)$ and $F'(S)$ are two free groups generated by S. Since S is contained in both $F(S)$ and $F'(S)$, we have natural injections $S \hookrightarrow F'(S)$ and $S \hookrightarrow F(S)$. By the universal property in the theorem, it follows that we have unique associated group homomorphisms $\Phi : F(S) \to F'(S)$ and $\Phi' : F'(S) \to F(S)$ which are both the identity on S. The composite $\Phi'\Phi$ is a homomorphism from $F(S)$ to $F(S)$ which is the identity on S, so by the uniqueness statement in the theorem, it must be the identity map. Similarly $\Phi\Phi'$ is the identity, so Φ is an isomorphism (with inverse Φ'), which proves the corollary.

Definition. The group $F(S)$ is called the *free group* on the set S. A group F is a *free group* if there is some set S such that $F = F(S)$ — in this case we call S a set of *free generators* (or a *free basis*) of F. The cardinality of S is called the *rank* of the free group.

One can now simplify expressions in a free group by using exponential notation, so we write a^3b^{-2} instead of the formal reduced word $aaab^{-1}b^{-1}$. Expressions like aba, however, cannot be simplified in the free group on $\{a, b\}$. We mention one important theorem in this area.

Theorem 19. (Schreier) Subgroups of a free group are free.

This is not trivial to prove and we do not include a proof. There is a nice proof of this result using covering spaces (cf. *Trees* by J.-P. Serre, Springer-Verlag, 1980).

Presentations

Let G be any group. Then G is a homomorphic image of a free group: take $S = G$ and φ as the identity map from G to G; then Theorem 16 produces a (surjective) homomorphism from $F(G)$ onto G. More generally, if S is any subset of G such that $G = \langle S \rangle$, then again there is a unique surjective homomorphism from $F(S)$ onto G which is the identity on S. (Note that we can now independently formulate the notion that a subset *generates* a group by noting that $G = \langle S \rangle$ if and only if the map $\pi : F(S) \to G$ which extends the identity map of S to G is surjective.)

Definition. Let S be a subset of a group G such that $G = \langle S \rangle$.

(1) A *presentation* for G is a pair (S, R), where R is a set of words in $F(S)$ such that the normal closure of $\langle R \rangle$ in $F(S)$ (the smallest normal subgroup containing $\langle R \rangle$) equals the kernel of the homomorphism $\pi : F(S) \to G$ (where π extends the identity map from S to S). The elements of S are called *generators* and those of R are called *relations* of G.

(2) We say G is *finitely generated* if there is a presentation (S, R) such that S is a finite set and we say G is *finitely presented* if there is a presentation (S, R) with both S and R finite sets.

Note that if (S, R) is a presentation, the kernel of the map $F(S) \to G$ is not $\langle R \rangle$ itself but rather the (much larger) group generated by R and *all conjugates* of elements in R. Note that even for a fixed set S a group will have many different presentations (we can always throw redundant relations into R, for example). If G is finitely presented with $S = \{s_1, s_2, \ldots, s_n\}$ and $R = \{w_1, w_2, \ldots, w_k\}$, we write (as we have in preceding chapters):

$$G = \langle s_1, s_2, \ldots, s_n \mid w_1 = w_2 = \cdots = w_k = 1 \rangle$$

and if w is the word $w_1w_2^{-1}$, we shall write $w_1 = w_2$ instead of $w = 1$.

Examples

(1) Every finite group is finitely presented. To see this let $G = \{g_1, \dots, g_n\}$ be a finite group. Let $S = G$ and let $\pi : F(S) \to G$ be the homomorphism extending the identity map of S. Let R_0 be the set of words $g_i g_j g_k^{-1}$, where $i, j = 1, \dots, n$ and $g_i g_j = g_k$ in G. Clearly $R_0 \le \ker \pi$. If N is the normal closure of R_0 in $F(S)$ and $\widetilde{G} = F(S)/N$, then G is a homomorphic image of $\widetilde{G}$ (i.e., π factors through N). Moreover, the set of elements $\{\widetilde{g}_i \mid i = 1, \dots, n\}$ is closed under multiplication. Since this set generates $\widetilde{G}$, it must equal $\widetilde{G}$. Thus $|\widetilde{G}| = |G|$ and so $N = \ker \pi$ and (S, R_0) is a presentation of G.

This illustrates a sufficient condition for (S, R) to be a presentation for a given finite group G:

(i) S must be a generating set for G, and

(ii) any group generated by S satisfying the relations in R must have order $\le |G|$.

(2) Abelian groups can be presented easily. For instance

$$\begin{aligned}\mathbb{Z} &\cong F(\{a\}) = \langle\, a \,\rangle,\\ \mathbb{Z} \times \mathbb{Z} &\cong \langle\, a, b \mid [a, b] = 1 \,\rangle,\\ Z_n \times Z_m &\cong \langle\, a, b \mid a^n = b^m = [a, b] = 1 \,\rangle.\end{aligned}$$

(Recall $[a, b] = a^{-1}b^{-1}ab$).

(3) Some familiar non-abelian groups introduced in earlier chapters have simple presentations:

$$\begin{aligned}D_{2n} &= \langle\, r, s \mid r^n = s^2 = 1,\ s^{-1}rs = r^{-1} \,\rangle\\ Q_8 &= \langle\, i, j \mid i^4 = 1,\ j^2 = i^2,\ j^{-1}ij = i^{-1} \,\rangle.\end{aligned}$$

To check, for example, the presentation for D_{2n} note that the relations in the presentation $\langle\, r, s \mid r^n = s^2 = 1,\ s^{-1}rs = r^{-1} \,\rangle$ imply that this group has a normal subgroup (generated by r) of order $\le n$ whose quotient is generated by s (which has order ≤ 2). Thus any group with these generators and relations has order at most $2n$. Since we already know of the existence of the group D_{2n} of order $2n$ satisfying these conditions, the abstract presentation must equal D_{2n}.

(4) As mentioned in Section 1.2, in general it is extremely difficult even to determine if a given set of generators and relations is or is not the identity group (let alone determine whether it is some other nontrivial finite group). For example, in the following two presentations the first group is an *infinite* group and the second is the *identity* group (cf. *Trees*, Chapter 1):

$$\begin{gathered}\langle\, x_1, x_2, x_3, x_4 \mid x_2x_1x_2^{-1} = x_1^2,\ x_3x_2x_3^{-1} = x_2^2,\ x_4x_3x_4^{-1} = x_3^2,\ x_1x_4x_1^{-1} = x_4^2 \,\rangle\\ \langle\, x_1, x_2, x_3, \mid x_2x_1x_2^{-1} = x_1^2,\ x_3x_2x_3^{-1} = x_2^2,\ x_1x_3x_1^{-1} = x_3^2 \,\rangle.\end{gathered}$$

(5) It is easy to see that S_n is generated by the transpositions $(1\,2), (2\,3), \dots, (n-1\,n)$, and that these satisfy the relations

$$((i\;i+1)(i+1\;i+2))^3 = 1 \quad \text{and} \quad [(i\;i+1), (j\;j+1)] = 1, \text{ whenever } |i - j| \ge 2$$

(here $|i-j|$ denotes the absolute value of the integer $i-j$). One can prove by induction on n that these form a presentation of S_n:

$$\begin{aligned}S_n \cong \langle\, t_1, \dots, t_{n-1} \mid t_i^2 = 1,\ (t_it_{i+1})^3 = 1,\ &\text{and } [t_i, t_j] = 1\\ &\text{whenever } |i - j| \ge 2,\ 1 \le i, j \le n-1 \,\rangle.\end{aligned}$$

As mentioned in Section 1.6 we can use presentations of a group to find homomorphisms between groups or to find automorphisms of a group. We did this in classifying groups of order 6, for example, when we proved that any non-abelian group of order 6 was generated by an element of order 3 and an element of order 2 inverting it; thus there is a homomorphism from S_3 onto any non-abelian group of order 6 (hence an isomorphism, by computing orders). More generally, suppose G is presented by, say, generators a, b with relations $r_1, \ldots, r_k$. If a', b' are any elements of a group H satisfying these relations, there is a homomorphism from G into H. Namely, if $\pi : F(\{a, b\}) \to G$ is the presentation homomorphism, we can define $\pi' : F(\{a, b\}) \to H$ by $\pi'(a) = a'$ and $\pi'(b) = b'$. Then $\ker \pi \leq \ker \pi'$ so π' factors through $\ker \pi$ and we obtain

$$G \cong F(\{a, b\}) / \ker \pi \longrightarrow H.$$

In, particular, if $\langle a', b' \rangle = H = G$, this homomorphism is an automorphism of G. Conversely, any automorphism must send a set of generators to another set of generators satisfying the same relations. For example, $D_8 = \langle a, b \mid a^2 = b^4 = 1,\ aba = b^{-1} \rangle$ and any pair a', b' of elements, where a' is a noncentral element of order 2 and b' is of order 4, satisfies the same relations. Since there are four noncentral elements of order 2 and two elements of order 4, D_8 has 8 automorphisms.

Similarly, any pair of elements of order 4 in Q_8 which are not equal or inverses of each other necessarily generate Q_8 and satisfy the relations given in Example 3 above. It is easy to check that there are 24 such pairs, so

$$|\mathrm{Aut}(Q_8)| = 24.$$

Free objects can be constructed in (many, but not all) other categories. For instance, a *monoid* is a set together with a binary operation satisfying all of the group axioms except the axiom specifying the existence of inverses. Free objects in the category of monoids play a fundamental role in theoretical computer science where they model the behavior of machines (Turing machines, etc.). We shall encounter free algebras (i.e., polynomial algebras) and free modules in later chapters.

EXERCISES

1. Let F_1 and F_2 be free groups of finite rank. Prove that $F_1 \cong F_2$ if and only if they have the same rank. What facts do you need in order to extend your proof to infinite ranks (where the result is also true)?

2. Prove that if $|S| > 1$ then $F(S)$ is non-abelian.

3. Prove that the commutator subgroup of the free group on 2 generators is not finitely generated (in particular, subgroups of finitely generated groups need not be finitely generated).

4. Prove that every nonidentity element of a free group is of infinite order.

5. Establish a finite presentation for A_4 using 2 generators.

6. Establish a finite presentation for S_4 using 2 generators.

7. Prove that the following is a presentation for the quaternion group of order 8:

$$Q_8 = \langle a, b \mid a^2 = b^2,\ a^{-1}ba = b^{-1} \rangle.$$

8. Use presentations to find the orders of the automorphism groups of the groups $Z_2 \times Z_4$ and $Z_4 \times Z_4$.