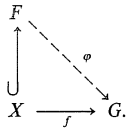
CHAPTER 11

Free Groups and Free Products

Generators and Relations

The notion of generators and relations can be extended from abelian groups to arbitrary groups once we have a nonabelian analogue of free abelian groups. We use the property appearing in Theorem 10.11 as our starting point.

Definition. If X is a subset of a group F, then F is a ***free group*** with ***basis*** X if, for every group G and every function $f: X \to G$, there exists a unique homomorphism $\varphi: F \to G$ extending f



We shall see later that X must generate F.

Observe that a basis in a free group behaves precisely as does a basis $B = \{v_1, \ldots, v_m\}$ of a finite-dimensional vector space V. The theorem of linear algebra showing that matrices correspond to linear transformations rests on the fact that if W is any vector space and $w_1, \ldots, w_m \in W$, then there exists a unique linear transformation $T: V \to W$ with $T(v_i) = w_i$ for all i.

The following construction will be used in proving that free groups exist. Let X be a set and let X^{-1} be a set, disjoint from X, for which there is a bijection $X \to X^{-1}$, which we denote by $x \mapsto x^{-1}$. Let X' be a singleton set disjoint from $X \cup X^{-1}$ whose only element is denoted by 1. If $x \in X$, then x^1 may denote x and x^0 may denote 1.

Definition. A ***word*** on X is a sequence $w = (a_1, a_2, \ldots)$, where $a_i \in X \cup X^{-1} \cup \{1\}$ for all i, such that all $a_i = 1$ from some point on; that is, there is an integer $n \geq 0$ with $a_i = 1$ for all $i > n$. In particular, the constant sequence

$$(1, 1, 1, \ldots)$$

is a word, called the ***empty word***, and it is also denoted by 1.

Since words contain only a finite number of letters before they become constant, we use the more suggestive notation for nonempty words:

$$w = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \ldots x_n^{\varepsilon_n},$$

where $x_i \in X$, $\varepsilon_i = +1, -1$, or 0, and $\varepsilon_n = \pm 1$. Observe that this spelling of a word is unique: two sequences (a_i) and (b_i) are equal if and only if $a_i = b_i$ for all i. The ***length*** of the empty word is defined to be 0; the ***length*** of $w = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \ldots x_n^{\varepsilon_n}$ is defined to be n.

Definition. If $w = x_1^{\varepsilon_1} \ldots x_n^{\varepsilon_n}$ is a word, then its ***inverse*** is the word $w^{-1} = x_n^{-\varepsilon_n} \ldots x_1^{-\varepsilon_1}$.

Definition. A word w on X is ***reduced*** if either w is empty or $w = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \ldots x_n^{\varepsilon_n}$, where all $x_i \in X$, all $\varepsilon_i = \pm 1$, and x and x^{-1} are never adjacent.

The empty word is reduced, and the inverse of a reduced word is reduced.

Definition. A ***subword*** of $w = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \ldots x_n^{\varepsilon_n}$ is either the empty word or a word of the form $v = x_i^{\varepsilon_i} \ldots x_j^{\varepsilon_j}$, where $1 \leq i \leq j \leq n$.

Thus, v is a subword of w if there are (possibly empty) subwords w' and w'' with $w = w'vw''$. A nonempty word w is reduced if and only if it contains no subwords of the form $x^{\varepsilon}x^{-\varepsilon}$ or x^0.

There is a multiplication of words: if $w = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \ldots x_n^{\varepsilon_n}$ and $u = y_1^{\delta_1} y_2^{\delta_2} \ldots y_m^{\delta_m}$, then $wu = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \ldots x_n^{\varepsilon_n} y_1^{\delta_1} y_2^{\delta_2} \ldots y_m^{\delta_m}$. This multiplication does not define a product on the set of all *reduced* words on X because wu need not be reduced (even when both w and u are). One can define a new multiplication of reduced words w and u as the reduced word obtained from wu after cancellations. More precisely, there is a (possibly empty) subword v of w with $w = w'v$ such that v^{-1} is a subword of u with $u = v^{-1}u''$ and such that $w'u''$ is reduced. Define a product of reduced words, called ***juxtaposition***, by

$$wu = w'u''.$$

Theorem 11.1. *Given a set X, there exists a free group F with basis X.*

Proof. Let F be the set of all the reduced words on X. One can show that F is a group under juxtaposition, but verifying associativity involves tedious case analyses. Instead, we use the ***van der Waerden trick*** (1945).

For each $x \in X$, consider the functions $|x|\colon F \to F$ and $|x^{-1}|\colon F \to F$, defined as follows: for $\varepsilon = \pm 1$,

$$|x^{\varepsilon}|(x_1^{\varepsilon_1}x_2^{\varepsilon_2}\dots x_n^{\varepsilon_n}) = \begin{cases} x^{\varepsilon}x_1^{\varepsilon_1}x_2^{\varepsilon_2}\dots x_n^{\varepsilon_n} & \text{if } x^{\varepsilon} \neq x_1^{-\varepsilon_1}, \\ x_2^{\varepsilon_2}\dots x_n^{\varepsilon_n} & \text{if } x^{\varepsilon} = x_1^{-\varepsilon_1}. \end{cases}$$

Since $|x^{\varepsilon}| \circ |x^{-\varepsilon}|$ and $|x^{-\varepsilon}| \circ |x^{\varepsilon}|$ are both equal to the identity $1_F\colon F \to F$, it follows that $|x^{\varepsilon}|$ is a permutation of F with inverse $|x^{-\varepsilon}|$. Let S_F be the symmetric group on F, and let $\mathscr{F}$ be the subgroup of S_F generated by $[X] = \{|x|\colon x \in X\}$. We claim that $\mathscr{F}$ is a free group with basis $[X]$. Note that there is a bijection $\zeta\colon [X] \to X$, namely, $|x| \mapsto x$.

An arbitrary element $g \in \mathscr{F}$ (other than the identity) has a factorization

$$(*) \qquad g = |x_1^{\varepsilon_1}| \circ |x_2^{\varepsilon_2}| \circ \cdots \circ |x_n^{\varepsilon_n}|,$$

where $\varepsilon_i = \pm 1$ and $|x^{\varepsilon}|$ and $|x^{-\varepsilon}|$ are never adjacent (or we can cancel). Such a factorization of g is unique, for $g(1) = x_1^{\varepsilon_1}x_2^{\varepsilon_2}\dots x_n^{\varepsilon_n}$, and we have already noted that the spelling of a (reduced) word is unique.

To see that $\mathscr{F}$ is free with basis $[X]$, assume that G is a group and that $f\colon [X] \to G$ is a function. Since the factorization $(*)$ is unique, the function $\varphi\colon \mathscr{F} \to G$, given by $\varphi(|x_1^{\varepsilon_1}| \circ |x_2^{\varepsilon_2}| \circ \cdots \circ |x_n^{\varepsilon_n}|) = f(|x_1^{\varepsilon_1}|)f(|x_2^{\varepsilon_2}|)\dots f(|x_n^{\varepsilon_n}|)$, is well defined and extends f. Since $[X]$ generates $\mathscr{F}$, it suffices to show that φ is a homomorphism, for uniqueness of φ would then follow from the fact that two homomorphisms agreeing on a generating set must be equal.

Let w and u be reduced words on $[X]$. It is obvious that $\varphi(w \circ u) = \varphi(w)\varphi(u)$ whenever the word wu (obtained from $w \circ u$ by deleting vertical bars) is reduced. Write $w = w' \circ v$ and $u = v^{-1} \circ u''$, as in the definition of juxtaposition. Now $\varphi(w) = \varphi(w')\varphi(v)$ and $\varphi(u) = \varphi(v^{-1})\varphi(u'') = \varphi(v)^{-1}\varphi(u'')$ (because $w' \circ v$ and $v^{-1} \circ u''$ are reduced). Therefore, $\varphi(w)\varphi(u) = \varphi(w')\varphi(v)\varphi(v)^{-1}\varphi(u'') = \varphi(w')\varphi(u'')$. On the other hand, $\varphi(w \circ u) = \varphi(w' \circ u'') = \varphi(w')\varphi(u'')$ (because $w' \circ u''$ is reduced), and so φ is a homomorphism.

We have shown that $\mathscr{F}$ is a free group with basis $[X]$. Since $\tilde{\zeta}\colon \mathscr{F} \to F$, defined by $|x_1^{\varepsilon_1}| \circ |x_2^{\varepsilon_2}| \circ \cdots \circ |x_n^{\varepsilon_n}| \mapsto x_1^{\varepsilon_1}x_2^{\varepsilon_2}\dots x_n^{\varepsilon_n}$, is a bijection with $\tilde{\zeta}([X]) = \zeta([X]) = X$, Exercise 1.44 shows that we may regard F as a group isomorphic to $\mathscr{F}$; thus, F is a free group with basis X (moreover, X generates F because $[X]$ generates $\mathscr{F}$). ∎

Corollary 11.2. *Every group G is a quotient of a free group.*

Proof. Construct a set $X = \{x_g\colon g \in G\}$ so that $f\colon x_g \mapsto g$ is a bijection $X \to G$. If F is free with basis X, then there is a homomorphism $\varphi\colon F \to G$ extending f, and φ is a surjection because f is. Therefore, $G \cong F/\ker \varphi$. ∎

Definition. Let X be a set and let Δ be a family of words on X. A group G has ***generators*** X and ***relations*** Δ if $G \cong F/R$, where F is the free group with basis X and R is the normal subgroup of F generated by Δ. The ordered pair $(X|\Delta)$ is called a ***presentation*** of G.

A relation[1] $r \in \Delta$ is often written as $r = 1$ to convey its significance in the quotient group G being presented.

There are two reasons forcing us to define R as the *normal* subgroup of F generated by Δ: if $r \in \Delta$ and $w \in F$, then $r = 1$ in G implies $wrw^{-1} = 1$ in G; we wish to form a quotient group.

EXAMPLE 11.1. $G = \mathbb{Z}_6$ has generator x and relation $x^6 = 1$.

A free group $F = \langle x \rangle$ on one generator is infinite cyclic, and $\langle x \rangle / \langle x^6 \rangle \cong \mathbb{Z}_6$. A presentation of G is $(x|x^6)$.

EXAMPLE 11.2. Another presentation of $G = \mathbb{Z}_6$ is

$$\mathbb{Z}_6 = (x, y|x^3 = 1, y^2 = 1, xyx^{-1}y^{-1} = 1).$$

When we described a presentation of $\mathbb{Z}_6$ as an abelian group in Example 10.2 (i.e., when we viewed $\mathbb{Z}_6$ as a quotient of a free abelian group), the only relations were x^3 and y^2. Now we must also have the commutator as a relation to force the images of x and y to commute in F/R.

EXAMPLE 11.3. The dihedral group D_{2n} has a presentation

$$D_{2n} = (x, y|x^n = 1, y^2 = 1, yxy = x^{-1}).$$

It is acceptable to write a relation as $yxy = x^{-1}$ instead of $xyxy = 1$. In particular, compare the presentation of D_6 with that of $\mathbb{Z}_6$ in Example 11.2.

We have passed over a point needing more discussion. By definition, D_{2n} is a group *of order* $2n$ having generators S and T satisfying the given relations. If $G = F/R$, where F is the free group with basis $\{x, y\}$ and R is the normal subgroup generated by $\{x^n, y^n, xyxy\}$, does G have order $2n$? We have seen various concrete versions of D_{2n}; for example, Theorem 3.31 displays it as the symmetry group of a regular n-gon. The definition of free group gives a surjective homomorphism $\varphi\colon F \to D_{2n}$ with $\varphi(x) = S$ and $\varphi(y) = T$. Moreover, $R \leq \ker \varphi$, because S and T satisfy the relations, so that the third isomorphism theorem gives a surjection $F/R \to F/\ker \varphi$; that is, there is a surjection[2] $G = F/R \to D_{2n}$. Hence, $|G| \geq 2n$. The reverse inequality also

[1] Many authors use the words "relation" and "relator" interchangeably.

[2] W. von Dyck (1882) invented free groups and used them to give the first precise definition of presentations. The version of the third isomorphism theorem used here is often called ***von Dyck's Theorem***: Let G have a presentation

$$G = (x_1, \dots, x_n | r_j(x_1, \dots, x_n), j \in J)$$

so that $G = F/R$, where F is the free group with basis $\{x_1, \dots, x_n\}$ and R is the normal subgroup generated by the r_j. If H is a group with $H = \langle y_1, \dots, y_n \rangle$ and if $r_j(y_1, \dots, y_n) = 1$ for all j, then there is a surjective homomorphism $G \to H$ with $x_i \mapsto y_i$ for all i.

holds, for each element in G has a factorization $x^i y^j R$ with $0 \le i < n$ and $0 \le j < 2$. Thus, $|G| = 2n$, and we are now entitled to write $G \cong D_{2n}$.

A description of a group by generators and relations is flawed in that the order of the presented group is difficult to determine. This is not a minor difficulty, for we shall see in the next chapter that it is even an unsolvable problem (in the logicians' precise sense) to determine, from an arbitrary presentation, the order of the presented group. Indeed, it is an unsolvable problem to determine whether a presentation defines a group of order 1. The reader should also see the next section on coset enumeration.

Let us continue the list of examples.

EXAMPLE 11.4. The group of quaternions has presentations

$$\mathbf{Q} = (a, b | a^4 = 1, b^2 = a^2, bab^{-1} = a^{-1})$$

and

$$\mathbf{Q} = (x, y | xyx = y, x^2 = y^2).$$

In each case, an argument is needed to show that the presented group has order 8.

EXAMPLE 11.5. Given positive integers l, m, and n, define

$$P(l, m, n) = (s, t | s^l = t^m = (st)^n = 1).$$

Example 11.3 shows that $P(n, 2, 2) = D_{2n}$ and, using Exercise 3.52, one can show that $P(2, 3, 3) \cong A_4$, $P(2, 3, 4) \cong S_4$, and $P(2, 3, 5) \cong A_5$. These groups are called *polyhedral groups*, and they are finite only in the cases just listed (see Coxeter–Moser).

EXAMPLE 11.6. The ***braid group*** B_m has the presentation

$$(\sigma_1, \ldots, \sigma_m | [\sigma_i, \sigma_j] = 1 \text{ if } j \ne i \pm 1,\ \sigma_i \sigma_{i+1} \sigma_i = \sigma_{i+1} \sigma_i \sigma_{i+1}).$$

Braid groups were introduced by E. Artin (1925) and are related to knot theory.

EXAMPLE 11.7. A free abelian group G with basis X has presentation

$$G = (X | xyx^{-1}y^{-1} = 1 \text{ for all } x, y \in X);$$

a free group F with basis X has presentation

$$F = (X | \varnothing).$$

Having proved that free groups exist, let us now consider their uniqueness; that is, when are two free groups isomorphic.

Lemma 11.3. *If F is a free group with basis X, then F/F' is a free abelian group with basis $X_{\#} = \{xF' : x \in X\}$.*

Proof. Assume that A is an abelian group and that $f: X_{\#} \to A$ is a function. Define $f_{\#}: X \to A$ by $x \mapsto f(xF')$. Since F is free with basis X, there is a homomorphism $\varphi: F \to A$ extending $f_{\#}$. But $F' \le \ker \varphi$, because A is abelian, so that there is a homomorphism $\tilde{\varphi}: F/F' \to A$, defined by $wF' \mapsto \varphi(w)$, extending f.

We claim that the extension $\tilde{\varphi}$ is unique. Suppose that $\theta: F/F' \to A$ and $\theta(xF') = f(xF')$. If $\nu: F \to F/F'$ is the natural map, then $\theta\nu: F \to A$ is a homomorphism with $\theta\nu(x) = \theta(xF') = f(xF') = \varphi(x)$ for all $x \in X$. Since X is a basis of F, $\theta\nu = \varphi = \tilde{\varphi}\nu$; since ν is surjective, $\theta = \tilde{\varphi}$. Therefore, F/F' is free abelian with basis $X_{\#}$. ∎

Theorem 11.4. *Let F and G be free groups with bases X and Y, respectively. Then $F \cong G$ if and only if $|X| = |Y|$.*

Proof. If $\varphi: F \to G$ is an isomorphism, then $F/F' \cong G/G'$. By the lemma, F/F' is free abelian with basis $X_{\#} = \{xF' : x \in X\}$. As $|X_{\#}| = |X|$, it follows that $|X| = \text{rank}(F/F')$. Similarly, $|Y| = \text{rank}(G/G')$, and so $|X| = |Y|$, by Theorem 10.14.

If $|X| = |Y|$, there is a bijection $f: X \to Y$ which, upon composing with the inclusion $Y \hookrightarrow G$, may be regarded as a function $X \to G$. Since F is free with basis X, there is a unique homomorphism $\varphi: F \to G$ extending f. Similarly, there is a unique homomorphism $\psi: G \to F$ extending $f^{-1}: Y \to X$. The composite $\psi\varphi: F \to F$ is a homomorphism which fixes X pointwise; that is, $\psi\varphi$ extends the inclusion function $\iota: X \hookrightarrow F$. But the identity 1_F also extends ι, and so uniqueness of extension gives $\psi\varphi = 1_F$. Similarly, $\varphi\psi = 1_G$, so that $\varphi: F \to G$ is an isomorphism. ∎

Definition. The *rank* of a free group F is the number of elements in a basis of F.

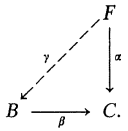
Theorem 11.4 says that $\text{rank}(F)$ does not depend on the choice of basis of F.

Corollary 11.5. *If F is free with basis X, then F is generated by X.*

Proof. Choose a set Y with $|Y| = |X|$ and a bijection $f: Y \to X$. The free group G with basis Y constructed in Theorem 11.1 (as the set of all reduced words on Y) is generated by Y. As in the proof of Theorem 11.4, the homomorphism $\psi: G \to F$ extending f is an isomorphism, so that $G = \langle Y \rangle$ implies $F = \langle \psi(Y) \rangle = \langle f(Y) \rangle = \langle X \rangle$. ∎

Theorem 11.6 (Projective Property). *Let $\beta: B \to C$ be a surjective homomorphism. If F is free and if $\alpha: F \to C$ is a homomorphism, then there exists a*

homomorphism γ: $F \to B$ making the diagram below commute (i.e., $\beta\gamma = \alpha$):



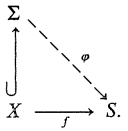
Proof. The proof is identical to that given for free abelian groups in Theorem 10.15. ∎

We shall see in Exercise 11.46 below that the converse of Theorem 11.6 is also true: a group G is free if and only if it has the projective property.

Semigroup Interlude

We are now going to construct free semigroups; the formal definition is no surprise.

Definition. If X is a subset of a semigroup Σ, then Σ is a ***free semigroup*** with ***basis*** X if, for every semigroup S and every function $f: X \to S$, there exists a unique homomorphism $\varphi: \Sigma \to S$ extending f.



Definition. A word w on X is ***positive*** if either $w = 1$ or $w = x_1^{\varepsilon_1}x_2^{\varepsilon_2}\dots x_n^{\varepsilon_n}$, where all exponents $\varepsilon_i > 0$.

The set Σ of all positive words on X is a free semigroup with basis X (the product of positive words is positive and, with no cancellation possible, it is easy to prove that multiplication is associative). It follows that every semigroup is a homomorphic image of a free semigroup. Before defining presentations of semigroups, however, we first define quotients.

Definition. A ***congruence*** on a semigroup S is an equivalence relation $\equiv$ on S such that

$$a \equiv a' \quad \text{and} \quad b \equiv b' \quad \text{imply} \quad ab \equiv a'b'.$$

If $\equiv$ is a congruence on a semigroup S, then the ***quotient semigroup*** is the set of all equivalence classes, denoted by $S/\equiv$, with the operation

$$[a][b] = [ab],$$

where $[a]$ denotes the equivalence class of $a \in S$ (this operation is well defined because $\equiv$ is a congruence).

There are two general constructions of congruences. The first arises from a homomorphism $\varphi: S \to T$ of semigroups; define $a \equiv b$ if $\varphi(a) = \varphi(b)$. This congruence is called ***ker φ***, and it is straightforward to prove the first isomorphism theorem:

$$S/\ker \varphi \cong \operatorname{im} \varphi$$

(if S and T are groups and $K = \{s \in S: \varphi(s) = 1\}$, then $\ker \varphi$ is the equivalence relation on S whose equivalence classes are the cosets of K). Here is a second construction. As any relation on S, a congruence is a subset of $S \times S$. It is easy to see that any intersection of congruences is itself a congruence. Since $S \times S$ is a congruence, one may thus define the congruence *generated* by any subset E of $S \times S$ as the intersection of all the congruences containing E. If Σ is the free semigroup with basis X and if $\{w_i = u_i: i \in I\}$ is a family of equations, where $w_i, u_i \in \Sigma$, then define $\equiv$ to be the congruence generated by $\{(w_i, u_i): i \in I\} \subset \Sigma \times \Sigma$. The quotient semigroup $\Sigma/\equiv$ is said to have the ***presentation***

$$(X | w_i = u_i \text{ for all } i \in I).$$

Exercises

11.1. Use presentations to prove the existence of the nonabelian groups of order p^3, where p is prime. (See Exercise 4.32.)

11.2. Prove that a free group of rank ≥ 2 is a centerless torsion-free group.

11.3. Prove that the group $G = (x, y | x^m, y^n)$ is infinite when $m, n \geq 2$.

11.4 **(Baer).** Prove that a group E has the injective property if and only if $E = 1$. (*Hint.* ***D.L. Johnson***). Let A be free with basis $\{x, y\}$ and let B be the semidirect product $B = A \rtimes \langle z \rangle$, where z is an involution acting by $zxz = y$ and $zyz = x$.)

11.5. Let X be the disjoint union $X = Y \cup Z$. If F is free with basis X and N is the normal subgroup generated by Y, then F/N is free with basis $\{zN: z \in Z\}$.

11.6. Show that a free group F of rank ≥ 2 has an automorphism φ with $\varphi(\varphi(w)) = w$ for all $w \in F$ and with no fixed points ($\varphi(w) = w$ implies $w = 1$). (Compare Exercise 1.50.)

11.7. If $H \lhd G$ and G/H is free, then G is a semidirect product of H by G/H. (*Hint.* Corollary 10.16 and Lemma 7.20.)

11.8. Let G be a group, let $\{t_i: i \in I\} \subset G$, and let $S = \langle t_i: i \in I \rangle \leq G$. If there is a homomorphism $\varphi: G \to F$ (where F is the free group with basis $X = \{x_i: i \in I\}$) with $\varphi(t_i) = x_i$ for all i, then S is a free group with basis $\{t_i: i \in I\}$.

11.9. The ***binary tetrahedral group*** B is the group having the presentation

$$B = (r, s, t | r^2 = s^3 = t^3 = rst).$$

(i) Prove that $rst \in Z(B)$ and that $B/\langle rst \rangle \cong A_4$ (the tetrahedral group).
(ii) Prove that B has order 24.
(iii) Prove that B has no subgroup of order 12.

11.10. The ***dicyclic group*** DC_n is the group having the presentation

$$DC_n = (r, s, t | r^2 = s^2 = t^n = rst).$$

(i) If $n = 2^{m-2}$, then $DC_n \cong Q_m$, the generalized quaternion group (see Exercise 4.40).

(ii) Show that DC_n has order $4n$.

11.11. Show that $(\sigma_1\sigma_2 \dots \sigma_m)^{m+1} \in Z(B_m)$, where B_m is the braid group (see Example 11.6). It is known that $Z(B_m)$ is the infinite cyclic group generated by this element.

11.12. (i) Show that a free semigroup with a basis having at least two elements is not commutative.

(ii) Show that a subsemigroup of a free semigroup need not be free. (*Hint.* Find an appropriate subsemigroup of the multiplicative semigroup of positive integers.)

Coset Enumeration

The method of coset enumeration, distilled by Todd and Coxeter (1936) from earlier particular cases, is a mechanical way to find the order of a given group from a presentation. It does not always work (nor can any such algorithm always work, as we shall see in the next chapter), but it does work whenever the presented group is finite. The method rests on the following elementary lemma.

Lemma 11.7. *Let G be a finite group, X a set of generators of G, $H \leq G$ a subgroup, and $Hw_1, \dots, Hw_n$ some distinct cosets of H. If $\bigcup_{i=1}^{n} Hw_i$ is closed under right multiplication by every $a \in X \cup X^{-1}$, then $G = \bigcup_{i=1}^{n} Hw_i$, $[G : H] = n$, and $|G| = n|H|$.*

Proof. If Y is any nonempty subset of G with $Ya \subset Y$ for all $a \in X \cup X^{-1}$, then $Y = G$ (because X generates G and $w \in Y$ for every word w on X). In particular, $G = \bigcup_{i=1}^{n} Hw_i$, so that every coset of H must appear as Hw_i for some i; that is, $[G : H] = n$. ∎

We illustrate the method in a specific case before describing it in general. Let G be the group having the presentation

$$G = (s, t | s^3 = t^2 = 1, tst = s^2).$$

Write each of the relations as a word with all exponents ± 1:

$$sss; \qquad tt; \qquad tsts^{-1}s^{-1}.$$

For each of these relation words, begin making a ***relation table*** by putting a vertical line under each of its letters.

s	s	s

t	t

t	s	t	s^{-1}	s^{-1}

If a word has l letters, there are thus l vertical lines. We regard these lines as being the dividing lines forming $l + 1$ columns, and we now proceed to create rows. In each of the three tables, put 1 at the beginning and at the end of the first row. Draw row 2 (in each table), beginning and ending with 2, and put 2 next to 1 in the first table.

s	s	s	
1	2		1
2			2

t	t	
1		1
2		2

t	s	t	s^{-1}	s^{-1}	
1					1
2					2

Build an ***auxiliary table*** containing entries

s	s^{-1}
1 | 2	2 | 1.

Now scan each of the tables to see whether there are any empty squares of either of the two forms

s	
1	

or

	s^{-1}
	1

;

in either case, fill the empty square with 2, obtaining

s	s	s	
1	2		1
2			2

t	t	
1		1
2		2

t	s	t	s^{-1}	s^{-1}	
1				2	1
2					2

Having filled all such squares, now draw row 3 (in each table), beginning and ending with 3, and put 3 in the first available square in the first table (next to 2).

s	s	s	
1	2	3	1
2			2
3			3

t	t	
1		1
2		2
3		3

t	s	t	s^{-1}	s^{-1}	
1				2	1
2					2
3					3

The auxiliary table receives new entries

s	s^{-1}
2 | 3	3 | 2

and, because the first row of table one has been completed, there are bonus entries: the auxiliary table also receives

s	s^{-1}
3 | 1	1 | 3.

Now fill more squares using the (enlarged) auxiliary table to obtain

s	s	s	
1	2	3	1
2	3	1	2
3	1	2	3

t	t	
1		1
2		2
3		3

t	s	t	s^{-1}	s^{-1}
1			3	2	1
2			1	3	2
3			2	1	3

The first table is complete, but we will continue until all the relation tables are complete (if possible). The next step draws row 4 (in all three tables) with 4 in the first row of the second table, yielding auxiliary table entries

$$\begin{matrix} t \\ 1 \mid 4 \end{matrix} \quad \text{and} \quad \begin{matrix} t^{-1} \\ 4 \mid 1 \end{matrix}$$

as well as bonus entries

$$\begin{matrix} t \\ 4 \mid 1 \end{matrix} \quad \text{and} \quad \begin{matrix} t^{-1} \\ 1 \mid 4. \end{matrix}$$

Fill in more square using the auxiliary table and obtain

s	s	s	
1	2	3	1
2	3	1	2
3	1	2	3
4			4

t	t	
1	4	1
2		2
3		3
4	1	4

t	s	t	s^{-1}	s^{-1}
1	4		3	2	1
2		4	1	3	2
3			2	1	3
4	1	2			4

Continue adding rows 5 and 6, filling in squares using all the entries in the auxiliary table.

s	s	s	
1	2	3	1
2	3	1	2
3	1	2	3
4	5		4
5		4	5
6			6

t	t	
1	4	1
2	6	2
3	5	3
4	1	4
5	3	5
6	2	6

t	s	t	s^{-1}	s^{-1}
1	4	5	3	2	1
2	6	4	1	3	2
3	5	6	2	1	3
4	1	2	6	5	4
5	3	1	4		5
6	2	3	5	4	6

When we try to add row 7, a new feature appears. In row 4 of the first table, the new 7 after 5 gives the auxiliary table entry

$$\begin{matrix} s \\ 5 \mid 7; \end{matrix}$$

but the auxiliary table already contains

$$\begin{matrix} s \\ 5 \mid 6. \end{matrix}$$

This is an instance of ***coset collapse***; delete row 7 and replace all other occurrences of 7 by the smaller number 6, including the entries in the auxiliary table. Continuing this procedure ultimately leads to the completed tables

s	s	s	
1	2	3	1
2	3	1	2
3	1	2	3
4	5	6	4
5	6	4	5
6	4	5	6

t	t	
1	4	1
2	6	2
3	5	3
4	1	4
5	3	5
6	2	6

t	s	t	s^{-1}	s^{-1}
1	4	5	3	2	1
2	6	4	1	3	2
3	5	6	2	1	3
4	1	2	6	5	4
5	3	1	4	6	5
6	2	3	1	3	6

The procedure now stops because *all* the relation tables are complete. According to the next theorem, the conclusion is that the presented group G has order 6 (of course, $G \cong S_3$).

Theorem 11.8 (Coset Enumeration). *Let G have a presentation with a finite number of generators and relations. Set up one table for each relation as above, add new integer entries and enlarge the auxiliary table as above whenever possible, and delete any larger numbers involved in coset collapse. If the procedure ends with all relation tables complete and having n rows, then the presented group G has order n.*

Proof. Let 1 denote the identity element of G, and assume that the other integers i in the tables, where $1 < i \leq n$, denote other elements of G. The entry

$$\begin{matrix} a \\ i \mid j \end{matrix}$$

in any relation table is interpreted as the equation $ia = j$ in G. This explains the twin entries in the auxiliary table: if $ia = j$, then $ja^{-1} = i$. The construction of the relation tables is a naming of elements of G. If there is a blank square to the right of i, with line labeled a between, then j is the element ia; if the blank square is to the left, then j is the element ia^{-1}. Coset collapse occurs when $ia = j$ and $ia = k$, in which case $j = k$.

Let Y be the set of elements in G that have been denoted by some i with $1 \leq i \leq n$. That all the tables are complete says that right multiplication by any $a \in X \cup X^{-1}$ produces only elements of Y. Therefore, Lemma 11.7 applies to Y (with H taken to be the trivial subgroup), and so $|G| = n$. ∎

Notice the hypothesis "If the procedure ends"; one does not know in advance whether the procedure will end.

There is a generalization of the algorithm from which the name "coset enumeration" arises. Consider the binary tetrahedral group (of order 24) given in Exercise 11.9:

$$B = (r, s, t | r^2 = s^3 = t^3 = rst).$$

First rewrite the presentation to display relations equal to 1:

$$B = (r, s, t | r^{-1}st = r^{-2}s^3 = r^{-1}s^{-1}t^2 = 1).$$

One could use Theorem 11.8 to show that B has order 24, but tables with 24 rows are tedious to do. Instead, let us choose a subgroup $H \leq G$ for which generators are known. For example, we might choose $H = \langle s \rangle$ in this example (cyclic subgroups are simplest). The idea is to use a slight variant of Theorem 11.8 to enumerate the cosets of H in G (instead of the elements of G). This is done as follows. In addition to relation tables, draw ***subgroup generator tables***, one for each generator of H. For example, there are two such tables if we choose $H = \langle rst, s \rangle$; there is just one such table if we choose $H = \langle s \rangle$. New tables consist of one row, and they are called complete once all their squares are filled *without drawing any new rows under them.* In our example, there is just one subgroup generator table, and it is already complete.

s	
1	1

In the general case, the rows of the subgroup generator tables are completed first, giving pairs of entries to the auxiliary table (in our example, the entries in the auxiliary table arising from the subgroup generator table are

s		s^{-1}
1	and	1).

After completing these one-rowed tables, the relation tables are completed as before. The numbers i now denote right cosets of H in G, with 1 denoting H. The entry

a
j

in a table means that if $i = Hw$, then $j = Hwa$. When all the tables are completed, Lemma 11.7 applies to calculate $[G : H]$, and hence $|G|$ is known if $|H|$ is. This version actually does enumerate the cosets of H.

In Exercise 11.13 below, the reader is asked to use coset enumeration to show that the order of the binary tetrahedral group B is 24. One must compute $|H|$; that is, one must compute the order of s (it is 6) and then see that the relation tables are complete with 4 rows.

There are two unexpected consequences of coset enumeration. When $H = 1$, the completed relation tables can be used to construct the regular representation of G. For example, we saw above that the presentation of $G = S_3$,

$$G = (s, t | s^3 = t^2 = 1, tst = s^2),$$

has relation tables:

	s	s	s	
1	2	3	1	1
2	3	1	2	2
3	1	2	3	3
4	5	6	4	4
5	6	4	5	5
6	4	5	6	6

	t	t	
1	4	1	1
2	6	2	2
3	5	3	3
4	1	4	4
5	3	5	5
6	2	6	6

	t	s	t	s^{-1}	s^{-1}	
1	4	5	3	2	1	1
2	6	4	1	3	2	2
3	5	6	2	1	3	3
4	1	2	6	5	4	4
5	3	1	4	6	5	5
6	2	3	1	3	6	6

The first column of the first table displays the values of right multiplication by s (as a permutation of $\{1, \ldots, 6\}$), and the first column of the second table does this for t. Right multiplication by s and t are:

$$s \mapsto (1\ 2\ 3)(4\ 5\ 6) \qquad \text{and} \qquad t \mapsto (1\ 4)(2\ 6)(3\ 5),$$

so that the right regular representation has $R_s = (1\ 3\ 2)(4\ 6\ 5)$ (because R_s: $i \mapsto is^{-1}$) and $R_t = (1\ 4)(2\ 6)(3\ 5)$. More generally, when one enumerates the cosets of a subgroup H of G, then one obtains the representation of G on the cosets of H (the construction above differs from that of Theorem 3.14 only in giving the representation on the right cosets of H instead of on the left cosets as in that theorem).

The information contained in completed relation tables can also be used to draw a directed graph.

Definition. A ***directed graph*** Γ is a set V, called *vertices*, together with a subset $E \subset V \times V$; ordered pairs $(u, v) \in E$ are called ***directed edges.*** A directed graph yields an ***associated graph*** Γ': both Γ and Γ' have the same vertices, and u and v are called adjacent in Γ' if $u \neq v$ and either (u, v) or (v, u) is a directed edge in Γ.

One can picture a finite directed graph Γ by drawing V as points and drawing an arrow from u to v if $(u, v) \in E$. In contrast to graphs, which have at most one edge between any pair of vertices, a directed graph may have two edges between a pair of vertices, one in each direction (given $u, v \in V$, it may happen that both (u, v) and $(v, u) \in E$). However, even if both (u, v) and (v, u) are directed edges in Γ, there is only edge between them in the associated graph Γ'. (There is a notion of *multigraph*, directed or nondirected, which allows many edges between a given pair of vertices, but we do not need them here.)

Definition. Let G be a group and let X be a set of generators of G. The ***Cayley graph*** $\Gamma = \Gamma(G, X)$ is the directed graph with vertices the elements of G and with a directed edge from g to h if $h = gx$ for some $x \in X$.

If coset enumeration of a presentation $(X|\Delta)$ of a group G yields complete relation tables, then one can record the information in these tables as the Cayley graph $\Gamma(G, X)$. For example, here is the Cayley graph of S_3 obtained from the presentation above.

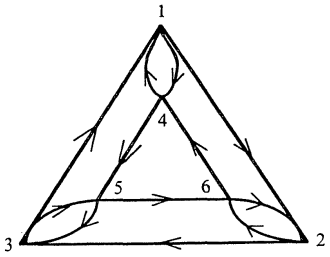


Figure 11.1

The Cayley graph of a group and a generating set is always defined, whether or not coset enumeration can be completed. Notice that the Cayley graph does depend on the choice of generating set. For example, a ***loop*** is an edge of the form (v, v). If we take G itself as a generating set, then $\Gamma(G, G)$ contains the loop $(1, 1)$, while $\Gamma(G, X)$ has no loops if $1 \notin X$. The Cayley graph is the beginning of a rich and fruitful geometric way of viewing presentations (see Burnside (1911), Dicks and Dunwoody (1989), Gersten (1987), Lyndon and Schupp (1977), and Serre (1980)).

EXERCISES

11.13. (i) In the presentation of the binary tetrahedral group B given above, show that s has order 6 in B.
(ii) Use coset enumeration relative to the subgroup $H = \langle s \rangle$ to compute the order of B.
(iii) Find the representation of B on the (right) cosets of H.

11.14. Describe the group G to isomorphism if G has the presentation

$$(q, r, s, t | rqr^{-1} = q^2, rtr^{-1} = t^2, s^{-1}rs = r^2, tst^{-1} = s^2, rt = tr).$$

11.15. Let $(X|\Delta)$ be a presentation of a group G. Show that the Cayley graph $\Gamma(G, X)$ has no loops if and only if $1 \notin X$.

Definition. The ***degree*** of a vertex v in a graph Γ is the number of vertices adjacent to it; the ***degree*** of a vertex v in a directed graph Γ is its degree in the associated graph Γ'. A graph or directed graph is ***regular*** of degree k if every vertex has the same degree, namely, k.

11.16. If X is a finite generating set of a group G with $1 \notin X$, then the Cayley graph $\Gamma(G, X)$ is regular of degree $2|X|$. (*Hint.* If $g \in G$ and $x \in X$, then (gx^{-1}, g) and (g, gx) are directed edges.)

11.17. Draw the Cayley graph $\Gamma(G, X)$ if G is a free abelian group of rank 2 and X is a basis.

11.18. Draw the Cayley graph $\Gamma(G, X)$ if G is a free group of rank 2 and X is a basis.

Presentations and the Schur Multiplier

The Schur multiplier $M(Q)$ of a group Q is discussed in Chapter 7 (the reader is advised to reread the appropriate section); it is related to presentations of Q because of the following isomorphism.

Hopf's Formula. *If $Q \cong F/R$ is a finite*[3] *group, where F is free, then*

$$M(Q) \cong (R \cap F')/[F, R].$$

Remark. An "aspherical" topological space X has the property that its homology groups are completely determined by its fundamental group $\pi_1(X)$. Hopf (1942) proved that $H_2(X) \cong (R \cap F')/[F, R]$, where F is free and $F/R \cong \pi_1(X)$. Schur (1907) proved that $M(Q) \cong (R \cap F')/[F, R]$ when Q is finite (i.e., Schur proved Hopf's formula in this case!). Comparison of Hopf's formula to Schur's theorem led Eilenberg and Mac Lane to their creation of Cohomology of Groups; the homology group $H_2(X)$ of the aspherical space X is the homology group $H_2(\pi_1(X), \mathbb{Z})$ of the fundamental group $\pi_1(X)$. When $\pi_1(X)$ is finite, $H_2(\pi_1(X), \mathbb{Z})$ is isomorphic to the second cohomology group $H^2(\pi_1(X), \mathbb{C}^\times) = M(\pi_1(X))$.

We will prove Hopf's formula for all finite groups Q, but we first consider a special class of groups.

Definition. A group Q is ***perfect*** if $Q = Q'$.

Every simple group is perfect. The proofs of Theorems 8.13 and 8.23 show that the groups $\mathrm{SL}(n, q)$ are perfect unless $(n, q) = (2, 2)$ or $(2, 3)$.

[3] Let us explain the finiteness hypothesis in Hopf's formula. In Chapter 7, we defined $M(Q)$ as the cohomology group $H^2(Q, \mathbb{C}^\times)$. Nowadays, after defining homology groups of Q, one defines $M(Q)$ as the second homology group $H_2(Q, \mathbb{Z})$. There is always an isomorphism $H_2(Q, \mathbb{Z}) \cong (H^2(Q, \mathbb{C}^\times))^*$, where * denotes character group. When Q is finite, the abelian group H^2 is also finite, and hence it is isomorphic to its own character group, by Theorem 10.54.