Chapter 6

More Group Theory

The more to do or to prove, the easier the doing or the proof.

James Joseph Sylvester

1. THE OPERATIONS OF A GROUP ON ITSELF

By an operation of a group G on itself, we mean that in the definition of the operation, G plays the role both of the group and of the set on which it operates. Any group operates on itself in several ways, two of which we single out here. The first is *left multiplication:*

(1.1) $$G \times G \longrightarrow G$$
$$g, x \rightsquigarrow gx.$$

This is obviously a transitive operation of G on G, that is, G forms a single orbit, and the stabilizer of any element is the identity subgroup $\{1\}$. So the action is faithful, and the homomorphism

(1.2) $$G \longrightarrow \mathrm{Perm}(G)$$
$$g \rightsquigarrow m_g = \text{ left multiplication by } g$$

defined in Chapter 5, Section 8 is injective.

(1.3) **Theorem.** *Cayley's Theorem:* Every finite group G is isomorphic to a subgroup of a permutation group. If G has order n, then it is isomorphic to a subgroup of the symmetric group S_n.

Proof. Since the operation by left multiplication is faithful, G is isomorphic to its image in $\mathrm{Perm}(G)$. If G has order n, then $\mathrm{Perm}(G)$ is isomorphic to S_n. □

Though Cayley's Theorem is intrinsically interesting, it is not especially useful for computation because S_n, having order $n!$, is too large in comparison with n.

The second operation we will consider is more subtle. It is *conjugation*, the map $G \times G \longrightarrow G$, defined by

$$(g, x) \rightsquigarrow gxg^{-1}. \tag{1.4}$$

For obvious reasons, we will not use multiplicative notation for this operation. You should verify the axioms (5.1) in Chapter 5, introducing a temporary notation such as $g*x$ to denote the conjugate gxg^{-1}.

The stabilizer of an element $x \in G$ for the operation of conjugation has a special name. It is called the *centralizer* of x and is denoted by $Z(x)$:

$$Z(x) = \{g \in G \mid gxg^{-1} = x\} = \{g \in G \mid gx = xg\}. \tag{1.5}$$

The centralizer is the set of group elements which commute with x. Note that $x \in Z(x)$, because x commutes with itself.

The orbit of x for the operation of conjugation is called the *conjugacy class* of x. It consists of all conjugate elements gxg^{-1}. We often write the conjugacy class as

$$C_x = \{x' \in G \mid x' = gxg^{-1} \text{ for some } g \in G\}. \tag{1.6}$$

By the Counting Formula [Chapter 5 (7.2)], $|G| = |C_x|\,|Z(x)|$.

Since the conjugacy classes are orbits for a group operation, they partition G. This gives us what is called the *Class Equation* for a finite group [see Chapter 5(7.3)]:

$$|G| = \sum_{\substack{\text{conjugacy} \\ \text{classes } C}} |C|. \tag{1.7}$$

If we number the conjugacy classes, say as C_i, $i = 1, \ldots, k$, then this formula reads

$$|G| = |C_1| + \cdots + |C_k|.$$

However there is some danger of confusion, because the subscript i in C_i is an index, while the notation C_x as used above stands for the conjugacy class containing the element x of G. In particular, C_1 has two meanings. Perhaps it will be best to list the conjugacy class of the identity element 1 of G first. Then the two interpretations of C_1 will agree.

Notice that the identity element is left fixed by all $g \in G$. Thus C_1 consists of the element 1 alone. Note also that each term on the right side of (1.7), being the order of an orbit, divides the left side. This is a strong restriction on the combinations of integers which may occur in such an equation.

(1.8) *The numbers on the right side of the Class Equation divide the order of the group, and at least one of them is equal to* 1.

For example, the conjugacy classes in the dihedral group D_3, presented as in Chapter 5 (3.6), are the following three subsets:

$$\{1\},\ \{x, x^2\},\ \{y, xy, x^2y\}.$$

The two rotations x, x^2 are conjugate, as are the three reflections. The Class Equation for D_3 is

$$6 = 1 + 2 + 3. \tag{1.9}$$

Recall from Chapter 2 (4.10) that the center of a group G is the set Z of elements which commute with all elements of the group:

$$Z = \{g \in G \mid gx = xg \text{ for all } x \in G\}.$$

Now the conjugacy class of an element x consists of that element alone if and only if $x = gxg^{-1}$ for all $g \in G$. This means that x is in the center. Thus the elements of the center are represented by 1 on the right side of the Class Equation.

The next proposition follows directly from the definitions.

(1.10) **Proposition.** An element x is in the center of a group G if and only if its centralizer $Z(x)$ is the whole group. □

One case in which the Class Equation (1.7) can be used effectively is when the order of G is a positive power of a prime p. Such a group is called a *p-group*. Here are a few applications of the Class Equation to p-groups.

(1.11) **Proposition.** The center of a p-group G has order > 1.

Proof. The left side of (1.7) is a power of p, say p^e. Also, every term on the right side is a power of p too, because it divides p^e. We want to show that some term on the right side of (1.7) is equal to 1. Now the terms other than 1, being positive powers of p, are divisible by p. Suppose that the class C_1 made the only contribution of 1 to the right side. Then the equation would read

$$p^e = 1 + \sum(\textit{multiples of } p),$$

which is impossible unless $e = 0$. □

The argument used in this proof can be turned around and abstracted to give the following important *Fixed Point Theorem* for actions of p-groups:

(1.12) **Proposition.** Let G be a p-group, and let S be a finite set on which G operates. Assume that the order of S is not divisible by p. Then there is a fixed point for the action of G on S, that is, an element $s \in S$ whose stabilizer is the whole group. □

(1.13) **Proposition.** Every group of order p^2 is abelian.

Proof. Let G be a group of order p^2. We will show that for every $x \in G$, the centralizer $Z(x)$ is the whole group. Proposition (1.10) will then finish the proof. So let $x \in G$. If x is in the center Z, then $Z(x) = G$ as claimed. If $x \notin Z$, then $Z(x)$ is strictly larger than Z, because it contains Z and also contains the element x. Now the orders of Z and $Z(x)$ divide $|G| = p^2$, and Proposition (1.11) tells us that $|Z|$ is at

least p. The only possibility is that $|Z(x)| = p^2$. Hence $Z(x) = G$, and x was in the center after all. □

There are nonabelian groups of order p^3. The dihedral group D_4, for example, has order 8.

Let us use (1.13) to classify groups of order p^2.

(1.14) **Corollary.** Every group of order p^2 is of one of the following types:

(i) a cyclic group of order p^2;

(ii) a product of two cyclic groups of order p.

Proof. Since the order of an element divides p^2, there are two cases to consider:

Case 1: G contains an element of order p^2 and is therefore a cyclic group.

Case 2: Every element x of G except the identity has order p. Let x, y be two elements different from 1, and let H_1, H_2 be the cyclic groups of order p generated by x and y respectively. We may choose y so that it is not a power of x. Then since $y \notin H_1$, $H_1 \cap H_2$ is smaller than H_2, which has order p. So $H_1 \cap H_2 = \{1\}$. Also, the subgroups H_i are normal because G is abelian. Since $y \notin H_1$, the group H_1H_2 is strictly larger than H_1, and its order divides p^2. Thus $H_1H_2 = G$. By Chapter 2 (8.6), $G \approx H_1 \times H_2$. □

The number of possibilities for groups of order p^n increases rapidly with n. There are five isomorphism classes of groups of order 8, and 14 classes of groups of order 16.

2. THE CLASS EQUATION OF THE ICOSAHEDRAL GROUP

In this section we determine the conjugacy classes in the icosahedral group I of rotational symmetries of a dodecahedron, and use them to study this very interesting group. As we have seen, the order of the icosahedral group is 60. It contains rotations by multiples of $2\pi/5$ about the centers of the faces of the dodecahedron, by multiples of $2\pi/3$ about the vertices, and by π about the centers of the edges. Each of the 20 vertices has a stabilizer of order 3, and opposite vertices have the same stabilizer. Thus there are 10 subgroups of order 3—the stabilizers of the vertices. Each subgroup of order 3 contains two elements of order 3, and the intersection of any two of these subgroups consists of the identity element alone. So I contains $10 \times 2 = 20$ elements of order 3. Similarly, the faces have stabilizers of order 5, and there are six such stabilizers, giving us $6 \times 4 = 24$ elements of order 5. There are 15 stabilizers of edges, and these stabilizers have order 2. So there are 15 elements of order 2. Finally, there is one element of order 1. Since

$$60 = 1 + 15 + 20 + 24, \tag{2.1}$$

we have listed all elements of the group.

Equation (2.1) is obtained by partitioning the group according to the orders of the elements. It is closely related to the Class Equation, but we can see that (2.1) is not the Class Equation itself, because 24, which appears on the right side, does not divide 60. On the other hand, we do know that conjugate elements have the same order. So the Class Equation is obtained by subdividing this partition of G still further. Also, note that the *subgroups* of order 3 are all conjugate. This is a general property of group operations, because they are the stabilizers of the vertices, which form a single orbit [Chapter 5 (6.5)]. The same is true for the subgroups of order 5 and for those of order 2.

Clearly the 15 elements of order 2, being the nontrivial elements in conjugate subgroups of order 2, form one conjugacy class. What about the elements of order 3? Let x denote a counterclockwise rotation by $2\pi/3$ about a vertex v. Though x will be conjugate to rotation with the same angle about any other vertex [Chapter 5 (6.5)], it is not so clear whether or not x is conjugate to x^2. Perhaps the first guess would be that x and x^2 are not conjugate.

Let v' denote the vertex opposite to v, and let x' be the counterclockwise rotation by $2\pi/3$ about v'. So x and x' are conjugate elements of the group. Notice that the counterclockwise rotation x about v is the same motion as the clockwise rotation by $2\pi/3$ about the opposite vertex v'. Thus $x^2 = x'$, and this shows that x and x^2 are conjugate after all. It follows that all the elements of order 3 are conjugate. Similarly, the 12 rotations by $2\pi/5$ and $-2\pi/5$ are conjugate. They are not conjugate to the remaining 12 rotations by $4\pi/5$, $-4\pi/5$ of order 5. (One reason, as we have already remarked, is that the order of a conjugacy class divides the order of the group, and 24 does not divide 60.) Thus there are two conjugacy classes of elements of order 5, and the Class Equation is

$$60 = 1 + 15 + 20 + 12 + 12. \tag{2.2}$$

We will now use this Class Equation to prove the following theorem.

(2.3) **Theorem.** The icosahedral group I has no proper normal subgroup.

A group $G \neq \{1\}$ is called a *simple group* if it is not the trivial group and if it contains no proper normal subgroup (no normal subgroup other than $\{1\}$ and G). Thus the theorem can be restated as follows:

(2.4) *The icosahedral group is a simple group.*

Cyclic groups of prime order contain no proper subgroup at all and are therefore simple groups. All other groups, except for the trivial group, contain proper subgroups, though not necessarily normal ones. We should emphasize that this use of the word *simple* does not imply "uncomplicated." Its meaning here is roughly "not compound."

Proof of Theorem (2.3). The proof of the following lemma is straightforward:

(2.5) **Lemma.**

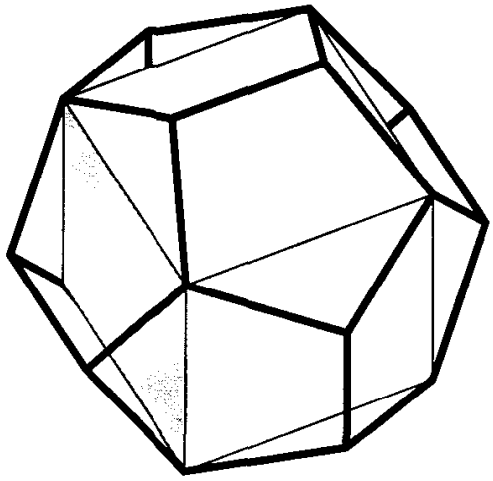
(a) If a normal subgroup N of a group G contains an element x, then it contains the conjugacy class C_x of x in G. In other words, a normal subgroup is a union of conjugacy classes.

(b) The order of a normal subgroup N of G is the sum of the orders of the conjugacy classes which it contains. □

We now apply this lemma. The order of a proper normal subgroup of the icosahedral group is a proper divisor of 60 and is also the sum of some of the terms on the right side of the Class Equation (2.2), including the term 1. It happens that there is no such integer. This proves the theorem. □

(2.6) **Theorem.** The icosahedral group is isomorphic to the alternating group A_5.

Proof. To describe this isomorphism, we need to find a set S of five elements on which I operates. One such set consists of the five cubes which can be inscribed into a dodecahedron, one of which is illustrated below:



(2.7) **Figure.** One of the cubes inscribed in a dodecahedron.

The group I operates on this set of cubes S, and this operation defines a homomorphism $\varphi: I \longrightarrow S_5$, the associated permutation representation. The map φ is our isomorphism from I to its image A_5. To show that it is an isomorphism, we will use the fact that I is a simple group, but we need very little information about the operation itself.

Since the kernel of φ is a normal subgroup of I and since I is a simple group, $\ker \varphi$ is either $\{1\}$ or I. To say $\ker \varphi = I$ would mean that the operation of I on the set of five cubes was the trivial operation, which it is not. Therefore $\ker \varphi = \{1\}$, and φ is injective, defining an isomorphism of I onto its image in S_5.

Let us denote the image in S_5 by I too. We restrict the sign homomorphism $S_5 \longrightarrow \{\pm 1\}$ to I, obtaining a homomorphism $I \longrightarrow \{\pm 1\}$. If this homomorphism were surjective, its kernel would be a normal subgroup of I of order 30 [Chapter 2 (6.15)]. This is impossible because I is simple. Therefore the restriction is the trivial

homomorphism, which just means that I is contained in the kernel A_5 of the sign homomorphism. Since both groups have order 60, $I = A_5$. □

3. OPERATIONS ON SUBSETS

Whenever a group G operates on a set S, there is also an operation on subsets. If $U \subset S$ is a subset, then

$$gU = \{gu \mid u \in U\} \tag{3.1}$$

is another subset of S. The axioms for an operation are clearly verified. So G operates on the set of subsets of S. We can consider the operation on subsets of a given order if we want to do so. Since multiplication by g is a permutation of S, the subsets U and gU have the same order.

For example, let O be the octahedral group of 24 rotations of a cube, and let S be the set of vertices of the cube. Consider the operation of O on subsets of order 2 of S, that is, on unordered pairs of vertices. There are 28 such pairs, and they form three orbits for the group:

(i) {pairs of vertices on an edge};

(ii) {pairs which are opposite on a face of the cube};

(iii) {pairs which are opposite on the cube}.

These orbits have orders 12, 12, and 4 respectively: $28 = 12 + 12 + 4$.

The stabilizer of a subset U is the set of group elements g such that $gU = U$. Thus the stabilizer of a pair of opposite vertices on a face contains two elements—the identity and the rotation by π about the face. This agrees with the counting formula: $24 = 2 \cdot 12$.

Note this important point once more: The equality $gU = U$ does not mean that g leaves the elements in U fixed, but rather that g permutes the elements within U, that is, that $gu \in U$ whenever $u \in U$.

(3.2) **Proposition.** Let H be a group which operates on a set S, and let U be a subset of S. Then H stabilizes U if and only if U is a union of H-orbits. □

This proposition just restates the fact that the H-orbit of an element $u \in U$ is the set of all elements hu. If H stabilizes U, then U contains the H-orbit of any of its elements. □

Let's consider the case that G operates by left multiplication on the subsets of G. Any subgroup H of G is a subset, and its orbit consists of the left cosets. This operation of G on cosets was defined in Chapter 5 (6.1). But any subset of G has an orbit.

(3.3) **Example.** Let $G = D_3$ be the dihedral group of symmetries of an equilateral triangle, presented as usual:

$$G = \{x^i y^j \mid 0 \le i \le 2,\ 0 \le j \le 1,\ x^3 = 1,\ y^2 = 1,\ yx = x^2 y\}.$$

This group contains 15 subsets of order 2, and we can decompose this set of 15 into orbits for left multiplication. There are three subgroups of order 2:

$$H_1 = \{1, y\}, \quad H_2 = \{1, xy\}, \quad H_3 = \{1, x^2y\}. \tag{3.4}$$

Their cosets form three orbits of order 3. The other six subsets of order 2 form a single orbit: $15 = 3 + 3 + 3 + 6$. The orbit of six is

$$\{1, x\}, \{x, x^2\}, \{x^2, 1\}, \{y, x^2y\}, \{xy, y\}, \{x^2y, xy\}. \quad \square \tag{3.5}$$

(3.6) **Proposition.** Let U be a subset of a group G. The order of the stabilizer $\mathrm{Stab}(U)$ of U for the operation of left multiplication divides the order of U.

Proof. Let H denote the stabilizer of U. Proposition (3.2) tells us that U is a union of orbits for the operation of H on G. These H-orbits are right cosets Hg. So U is a union of right cosets. Hence the order of U is a multiple of $|H|$. $\square$

Of course since the stabilizer is a subgroup of G, its order also divides $|G|$. So if $|U|$ and $|G|$ have no common factor, then $\mathrm{Stab}(U)$ is the trivial subgroup $\{1\}$.

The operation by conjugation on subsets of G is also interesting. For example, we can partition the 15 subsets of D_3 of order 2 into orbits for conjugation. The set $\{H_1, H_2, H_3\}$ of conjugate subgroups is one orbit, and the set $\{x, x^2\}$ forms an orbit by itself. The other orbits have orders 2, 3, and 6: $15 = 1 + 2 + 3 + 3 + 6$.

For our purposes, the important thing is the orbit under conjugation of a subgroup $H \subset G$. This orbit is the set of *conjugate subgroups*

$$\{gHg^{-1} \mid g \in G\}.$$

The subgroup H is normal if and only if its orbit consists of H alone, that is, $gHg^{-1} = H$ for all $g \in G$.

The stabilizer of a subgroup H for the operation of conjugation is called the *normalizer* of H and is denoted by

$$N(H) = \{g \in G \mid gHg^{-1} = H\}. \tag{3.7}$$

The Counting Formula reads

$$|G| = |N(H)| \cdot |\{\text{conjugate subgroups}\}|. \tag{3.8}$$

Hence the number of conjugate subgroups is equal to the index $[G : N(H)]$.

Note that the normalizer always contains the subgroup

$$N(H) \supset H, \tag{3.9}$$

because $hHh^{-1} = H$ when $h \in H$. So by Lagrange's Theorem, $|H|$ divides $|N(H)|$, and $|N(H)|$ divides $|G|$.

In example (3.3), the subgroups H_1, H_2, H_3 are all conjugate, and so $|N(H_i)| = 2$; hence $N(H_i) = H_i$.

The definition of the normalizer $N(H)$ shows that H is a normal subgroup of $N(H)$, and in fact $N(H)$ is the largest group containing H as a normal subgroup. In particular, $N(H) = G$ if and only if H is a normal subgroup of G.

4. THE SYLOW THEOREMS

The Sylow Theorems, which we will prove in this section, describe the subgroups of prime power order of an arbitrary finite group.

Let G be a group of order $n = |G|$, and let p be a prime number which divides n. We will use the following notation: p^e will denote the largest power of p dividing n, so that

$$n = p^e m \tag{4.1}$$

for some integer m, and p does not divide m.

(4.2) **Theorem.** *First Sylow Theorem:* There is a subgroup of G whose order is p^e.

The proofs of the Sylow Theorems are at the end of the section.

(4.3) **Corollary.** If a prime p divides the order of a finite group G, then G contains an element of order p.

For, let H be a subgroup of order p^e, and let x be an element of H different from 1. The order of x divides p^e, so it is p^r for some r in the range $0 < r \leq e$. Then $x^{p^{r-1}}$ has order p. □

Without the Sylow Theorem, this corollary is not obvious. We already know that the order of any element divides $|G|$, but we might imagine a group of order 6, for example, made up of the identity 1 and five elements of order 2. No such group exists. According to (4.3), a group of order 6 must contain an element of order 3 and an element of order 2.

(4.4) **Corollary.** There are exactly two isomorphism classes of groups of order 6. They are the classes of the cyclic group C_6 and of the dihedral group D_3.

Proof. Let x be an element of order 3 and y an element of order 2 in G. It is easily seen that the six products $x^i y^j$, $0 \leq i \leq 2$, $0 \leq j \leq 1$ are distinct elements of the group. For we can rewrite an equation $x^i y^j = x^r y^s$ in the form $x^{i-r} = y^{s-j}$. Every power of x except the identity has order 3, and every power of y except the identity has order 2. Thus $x^{i-r} = y^{s-j} = 1$, which shows that $r = i$ and $s = j$. Since G has order 6, the six elements $1, x, x^2, y, xy, x^2y$ run through the whole group. In particular, yx must be one of them. It is not possible that $yx = y$ because this would imply $x = 1$. Similarly, $yx \neq 1, x, x^2$. Therefore one of the two relations

$$yx = xy \quad \text{or} \quad yx = x^2y$$

holds in G. Either of these relations, together with $x^3 = 1$ and $y^2 = 1$, allows us to determine the multiplication table for the group. Therefore there are at most two isomorphism classes of groups of order 6. We know two already, namely the classes of the cyclic group C_6 and of the dihedral group D_3. So they are the only ones. □

(4.5) **Definition.** Let G be a group of order $n = p^e m$, where p is a prime not dividing m and $e \geq 1$. The subgroups H of G of order p^e are called *Sylow p-subgroups* of G, or often just *Sylow subgroups*.

Thus a Sylow p-subgroup is a p-subgroup whose index in the group is not divisible by p. By Theorem (4.2), a finite group G always has a Sylow p-subgroup if p divides the order of G. The remaining Sylow Theorems (4.6) and (4.8) give more information about them.

(4.6) **Theorem.** *Second Sylow Theorem:* Let K be a subgroup of G whose order is divisible by p, and let H be a Sylow p-subgroup of G. There is a conjugate subgroup $H' = gHg^{-1}$ such that $K \cap H'$ is a Sylow subgroup of K.

(4.7) **Corollary.**

(a) If K is any subgroup of G which is a p-group, then K is contained in a Sylow p-subgroup of G.

(b) The Sylow p-subgroups of G are all conjugate.

It is clear that a conjugate of a Sylow subgroup is also a Sylow subgroup. So to obtain the first part of the corollary, we only need to note that the Sylow subgroup of a p-group K is the group K itself. So if H is a Sylow subgroup and K is a p-group, there is a conjugate H' such that $K \cap H' = K$, which is to say that H' contains K. For part (b), let K and H be Sylow subgroups. Then there is a conjugate H' of H which contains K. Since their orders are equal, $K = H'$. Thus K and H are conjugate. □

(4.8) **Theorem.** *Third Sylow Theorem:* Let $|G| = n$, and $n = p^e m$ as in (4.1). Let s be the number of Sylow p-subgroups. Then s divides m and is congruent 1 (modulo p): $s|m$, and $s = ap + 1$ for some integer $a \geq 0$.

Before proving these theorems, we will use them to determine the groups of orders 15 and 21. These examples show how powerful the Sylow Theorems are, but do not be misled. The classification of groups of order n is not easy when n has many factors. There are just too many possibilities.

(4.9) **Proposition.**

(a) Every group of order 15 is cyclic.

(b) There are two isomorphism classes of groups of order 21: the class of the cyclic group C_{21} and the class of the group G having two generators x, y which satisfy the relations $x^7 = 1$, $y^3 = 1$, $yx = x^2y$.

Proof.

(a) Let G be a group of order 15. By (4.8) the number of its Sylow 3-subgroups divides 5 and is congruent 1 (modulo 3). The only such integer is 1. Therefore there is

one Sylow 3-subgroup H, and so it is a normal subgroup. There is one Sylow 5-subgroup K, and it is normal too, for similar reasons. Clearly, $K \cap H = \{1\}$, because the order of $K \cap H$ divides both 5 and 3. Also, KH is a subgroup of order >5, and hence $KH = G$. By (8.6) in Chapter 2, G is isomorphic to the product group $H \times K$. Thus every group of order 15 is isomorphic to a direct product of cyclic groups of orders 3 and 5. All groups of order 15 are isomorphic. Since the cyclic group C_{15} is one of them, every group of order 15 is cyclic.

(b) Let G be a group of order 21. Then Theorem (4.8) shows that the Sylow 7-subgroup K must be normal. But the possibility that there are seven conjugate Sylow 3-subgroups H is not ruled out by the theorem, and in fact this case does arise. Let x denote a generator for K, and y a generator for one of the Sylow 3-subgroups H. Then $x^7 = 1$, $y^3 = 1$, and, since K is normal, $yxy^{-1} = x^i$ for some $i < 7$.

We can restrict the possible exponents i by using the relation $y^3 = 1$. It implies that

$$x = y^3xy^{-3} = y^2x^iy^{-2} = yx^{i^2}y^{-1} = x^{i^3}.$$

Hence $i^3 \equiv 1 \pmod 7$. This means that i can take the values 1, 2, 4.

Case 1: $yxy^{-1} = x$. The group is abelian, and by (8.6) in Chapter 2 it is isomorphic to a direct product of cyclic groups of orders 3 and 7. Such a group is cyclic [Chapter 2 (8.4)].

Case 2: $yxy^{-1} = x^2$. The multiplication in G can be carried out using the rules $x^7 = 1$, $y^3 = 1$, $yx = x^2y$, to reduce every product of the elements x,y to one of the forms x^iy^j with $0 \leq i < 7$ and $0 \leq j < 3$. We leave the proof that this group actually exists as an exercise.

Case 3: $yxy^{-1} = x^4$. In this case, we replace y by y^2, which is also a generator for H, to reduce to the previous case: $y^2xy^{-2} = yx^4y^{-1} = x^{16} = x^2$. Thus there are two isomorphism classes of groups of order 21, as claimed. □

We will now prove the Sylow Theorems.

Proof of the First Sylow Theorem. We let $\mathcal{S}$ be the set of all subsets of G of order p^e. One of these subsets is the subgroup we are looking for, but instead of finding it directly we will show that one of these subsets has a stabilizer of order p^e. The stabilizer will be the required subgroup.

(4.10) **Lemma.** The number of subsets of order p^e in a set of $n = p^em$ elements (p not dividing m) is the binomial coefficient

$$N = \binom{n}{p^e} = \frac{n\ (n-1)\cdots(n-k)\cdots(n-p^e+1)}{p^e(p^e-1)\cdots(p^e-k)\cdots\qquad 1}$$

Moreover N is not divisible by p.

Proof. It is a standard fact that the number of subsets of order p^e is this binomial coefficient. To see that N is not divisible by p, note that every time p divides a term $(n - k)$ in the numerator of N, it also divides the term $(p^e - k)$ of the denominator exactly the same number of times: If we write k in the form $k = p^i l$, where p does not divide l, then $i < e$. Therefore $(n - k)$ and $(p^e - k)$ are both divisible by p^i but not divisible by p^{i+1}. □

We decompose $\mathcal{S}$ into orbits for the operation of left multiplication, obtaining the formula

$$N = |\mathcal{S}| = \sum_{\text{orbits } O} |O|.$$

Since p does not divide N, some orbit has an order which is not divisible by p, say the orbit of the subset U. We now apply Proposition (3.6) to conclude that $|\operatorname{Stab}(U)|$ is a power of p. Since

$$|\operatorname{Stab}(U)| \cdot |O_U| = |G| = p^e m \tag{4.11}$$

by the Counting Formula, and since $|O_U|$ is not divisible by p, it follows that $|\operatorname{Stab}(U)| = p^e$. This stabilizer is the required subgroup. □

Proof of the Second Sylow Theorem. We are given a subgroup K and a Sylow subgroup H of G, and we are to show that for some conjugate subgroup H' of H, the intersection $K \cap H'$ is a Sylow subgroup of K.

Let S denote the set of left cosets G/H. The facts that we need about this set are that G operates transitively, that is, the set forms a single orbit, and that H is the stabilizer of one of its elements, namely of $s = 1H$. So the stabilizer of as is the conjugate subgroup aHa^{-1} [see Chapter 5(6.5b)].

We restrict the operation of G to K and decompose S into K-orbits. Since H is a Sylow subgroup, the order of S is prime to p. So there is some K-orbit O whose order is prime to p. Say that O is the K-orbit of the element as. Let H' denote the stabilizer aHa^{-1} of as for the operation of G. Then the stabilizer of as for the restricted operation of K is obviously $H' \cap K$, and the index $[K:H' \cap K]$ is $|O|$, which is prime to p. Also, since it is a conjugate of H, H' is a p-group. Therefore $H' \cap K$ is a p-group. It follows that $H' \cap K$ is a Sylow subgroup of K. □

Proof of the Third Sylow Theorem. By Corollary (4.7), the Sylow subgroups of G are all conjugate to a given one, say to H. So the number of Sylow subgroups is $s = [G:N]$, where N is the normalizer of H. Since $H \subset N$, $[G:N]$ divides $[G:H] = m$. To show $s \equiv 1$ (modulo p), we decompose the set $\{H_1, \ldots, H_s\}$ of Sylow subgroups into orbits for the operation of conjugation by $H = H_1$. An orbit consists of a single group H_i if and only if H is contained in the normalizer N_i of H_i. If so, then H and H_i are both Sylow subgroups of N_i, and H_i is normal in N_i. Corollary (4.7b) shows that $H = H_i$. Therefore there is only one H-orbit of order 1, namely $\{H\}$. The other orbits have orders divisible by p because their orders divide $|H|$, by the Counting Formula. This shows that $s \equiv 1$ (modulo p). □

5. THE GROUPS OF ORDER 12

In this section, we use the Sylow Theorems to classify the groups of order 12:

(5.1) **Theorem.** There are five isomorphism classes of groups of order 12. They are represented by:

(i) the product of cyclic groups $C_3 \times C_4$;
(ii) the product of cyclic groups $C_2 \times C_2 \times C_3$;
(iii) the alternating group A_4,
(iv) the dihedral group D_6,
(v) the group generated by x, y, with relations $x^4 = 1$, $y^3 = 1$, $xy = y^2x$.

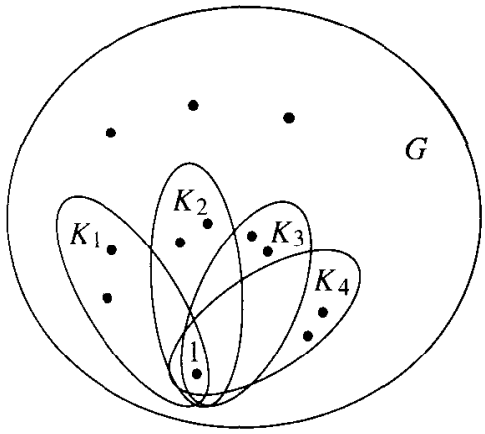
Note that $C_3 \times C_4$ is isomorphic to C_{12} and that $C_2 \times C_2 \times C_3$ is isomorphic to $C_2 \times C_6$ (see [Chapter 2 (8.4)]).

Proof. Let G be a group of order 12. Denote by H a Sylow 2-subgroup of G, which has order 4, and by K a Sylow 3-subgroup, of order 3. It follows from Theorem (4.8) that the number of Sylow 2-subgroups is either 1 or 3, and that the number of Sylow 3-subgroups is 1 or 4. Also, H is a group of order 4 and is therefore either a cyclic group or the Klein four group V, a product of two cyclic groups of order 2:

$$H \approx C_4 \quad \text{or} \quad H \approx V. \tag{5.2}$$

(5.3) **Lemma.** At least one of the two subgroups H, K is normal.

Proof. Suppose that K is not normal. Then K has four conjugate subgroups $K = K_1, \ldots, K_4$. Since $|K_i| = 3$, the intersection of any two of these groups must be the identity. Counting elements shows that there are only three elements of G which are not in any of the groups K_i.



Any Sylow 2-subgroup H has order 4, and $H \cap K_i = \{1\}$. Therefore it consists of these three elements and 1. This describes H for us and shows that there is only one Sylow 2-subgroup. Thus H is normal. □

Since $H \cap K = \{1\}$, every element of HK has a unique expression as a product hk [Chapter 2 (8.6)], and since $|G| = 12$, $HK = G$. If H is normal, then K operates on H by conjugation, and we will show that this operation, together with the structure of H and K, determines the structure of G. Similarly, if K is normal then H operates on K, and this operation determines G.

Case 1: H and K are both normal. Then by (8.6) in Chapter 2, G is isomorphic to the product group $H \times K$. By (5.2) there are two possibilities:

$$G \approx C_4 \times C_3 \quad \text{or} \quad G \approx V \times C_3. \tag{5.4}$$

These are the abelian groups of order 12.

Case 2: H is normal but K is not. So there are four conjugate Sylow 3-subgroups $\{K_1, \ldots, K_4\}$, and G operates by conjugation on this set S of four subgroups. This operation determines a permutation representation

$$G \xrightarrow{\varphi} S_4. \tag{5.5}$$

Let us show that φ maps G isomorphically to the alternating group A_4 in this case.

The stabilizer of K_i for the operation of conjugation is the normalizer $N(K_i)$, which contains K_i. The Counting Formula shows that $|N(K_i)| = 3$, and hence that $N(K_i) = K_i$. Since the only element common to the subgroups K_i is the identity element, only the identity stabilizes all of these subgroups. Thus φ is injective and G is isomorphic to its image in S_4.

Since G has four subgroups of order 3, it contains eight elements of order 3, and these elements certainly generate the group. If x has order 3, then $\varphi(x)$ is a permutation of order 3 in S_4. The permutations of order 3 are even. Therefore $\operatorname{im}\varphi \subset A_4$. Since $|G| = |A_4|$, the two groups are equal.

As a corollary, we note that if H is normal and K is not, then H is the Klein four group V, because the Sylow 2-subgroup of A_4 is V.

Case 3: K is normal, but H is not. In this case H operates on K by conjugation, and conjugation by an element of H is an automorphism of K. We let y be a generator for the cyclic group K: $y^3 = 1$. There are only two automorphisms of K—the identity and the automorphism which interchanges y and y^2.

Suppose that H is cyclic of order 4, and let x generate H: $x^4 = 1$. Then since G is not abelian, $xy \neq yx$, and so conjugation by x is not the trivial automorphism of K. Hence $xyx^{-1} = y^2$. The Todd–Coxeter Algorithm (see Section 9) is one way to show that these relations define a group of order 12:

$$x^4 = 1\,,\ y^3 = 1\,,\ xyx^{-1} = y^2. \tag{5.6}$$

The last possibility is that H is isomorphic to the Klein four group. Since there are only two automorphisms of K, there is an element $w \in H$ besides the identity which operates trivially: $wyw^{-1} = y$. Since G is not abelian, there is also an element v which operates nontrivially: $vyv^{-1} = y^2$. Then the elements of H are $\{1,v,w,vw\}$, and the relations $v^2 = w^2 = 1$, and $vw = wv$ hold in H. The element $x = wy$ has

order 6, and $vxv^{-1} = vwyv^{-1} = wy^2 = y^2w = x^{-1}$. The relations $x^6 = 1$, $v^2 = 1$, $vxv^{-1} = x^{-1}$ define the group D_6, so G is dihedral in this case. □

6. COMPUTATION IN THE SYMMETRIC GROUP

We want to bring up two points about calculation with permutations. The first concerns the order of multiplication. To have a uniform convention, we have used the functional notation $p(x)$ for all our maps p, including permutations. This has the consequence that a product pq must be interpreted as the composed operation $p \circ q$, that is, "first apply q, then p." When multiplying permutations, it is more usual to read pq as "first apply p, then q." We will use this second convention here. A compatible notation for the operation of a permutation p on an index $\mathbf{i}$ requires writing the permutation on the right side of the index:

$$(\mathbf{i})p.$$

Applying first p and then q to an index $\mathbf{i}$, we get $((\mathbf{i})p)q = (\mathbf{i})pq$, as desired. Actually, this notation looks funny to me. We will usually drop the parentheses:

$$(\mathbf{i})p = \mathbf{i}p.$$

What is important is that p must appear on the right.

To make our convention for multiplication compatible with matrix multiplication, we must replace the matrix P associated to a permutation p in Chapter 1 (4.6) by its transpose P^t, and use it to multiply on the right on a row vector.

The second point is that it is not convenient to compute with permutation matrices, because the matrices are large in relation to the amount of information they contain. A better notation is needed. One way to describe a permutation is by means of a table. We can consider the configuration

$$p = \begin{bmatrix} \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{4} & \mathbf{5} & \mathbf{6} & \mathbf{7} & \mathbf{8} \\ \mathbf{4} & \mathbf{6} & \mathbf{8} & \mathbf{3} & \mathbf{5} & \mathbf{2} & \mathbf{1} & \mathbf{7} \end{bmatrix} \tag{6.1}$$

as a notation for the permutation defined by

$$\mathbf{1}p = \mathbf{4},\ \mathbf{2}p = \mathbf{6},\ldots\ .$$

It is easy to compute products using this notation. If for example

$$q = \begin{bmatrix} \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{4} & \mathbf{5} & \mathbf{6} & \mathbf{7} & \mathbf{8} \\ \mathbf{2} & \mathbf{4} & \mathbf{6} & \mathbf{8} & \mathbf{1} & \mathbf{3} & \mathbf{5} & \mathbf{7} \end{bmatrix},$$

then we can evaluate pq (first p, then q) by reading the two tables in succession:

$$pq = \begin{bmatrix} \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{4} & \mathbf{5} & \mathbf{6} & \mathbf{7} & \mathbf{8} \\ \mathbf{8} & \mathbf{3} & \mathbf{7} & \mathbf{6} & \mathbf{1} & \mathbf{4} & \mathbf{2} & \mathbf{5} \end{bmatrix}.$$

Table (6.1) still requires a lot of writing, and of course the top row is always the same. It could, in principle, be left off, to reduce the amount of writing by half,

but this would make it hard to find our place in the bottom row if we were permuting, say, 18 digits.

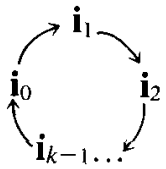
Another notation, called *cycle notation,* is commonly used. It describes a permutation of n elements by at most n symbols and is based on the partition of the indices into orbits for the operation of a permutation. Let p be a permutation, and let H be the cyclic subgroup generated by p. We decompose the set $\{\mathbf{1},\ldots,\mathbf{n}\}$ into H-orbits and refer to these orbits as the *p-orbits.* The p-orbits form a partition of the set of indices, called the *cycle decomposition* associated to the permutation p.

If an index $\mathbf{i}$ is in an orbit of k elements, the elements of the orbit will be

$$O = \{\mathbf{i}, \mathbf{i}p, \mathbf{i}p^2, \ldots, \mathbf{i}p^{k-1}\}.$$

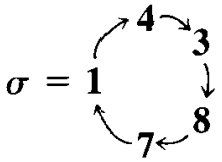
Let us denote $\mathbf{i}p^r$ by $\mathbf{i}_r$, so that $O = \{\mathbf{i}_0, \mathbf{i}_1, \ldots, \mathbf{i}_{k-1}\}$. Then p operates on this orbit as

(6.2)



A permutation which operates in this way on a subset $\{\mathbf{i}_0, \mathbf{i}_1, \ldots, \mathbf{i}_{k-1}\}$ of the indices and leaves the remaining indices fixed is called a *cyclic permutation.* Thus

(6.3)



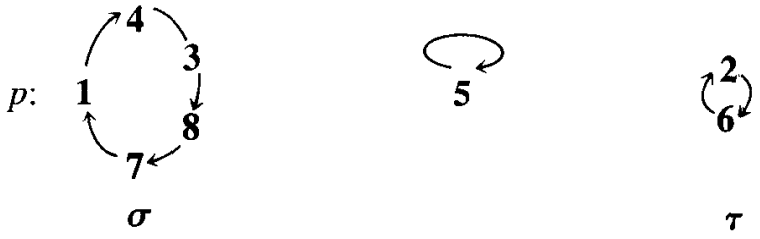
defines a cyclic permutation of order 5 of $\{\mathbf{1},\ldots,\mathbf{8}\}$, it being understood that the indices $\mathbf{2}, \mathbf{5}, \mathbf{6}$ which are not mentioned are left fixed—each forms a σ-orbit of one element. When we speak of *the indices on which a permutation operates,* we will mean the ones which are not fixed: $\mathbf{1}, \mathbf{3}, \mathbf{4}, \mathbf{7}, \mathbf{8}$ in this case.

Another cyclic permutation of $\{\mathbf{1},\ldots,\mathbf{8}\}$ is

(6.4)

Such a cyclic permutation of order 2 is called a *transposition.* A transposition is a permutation which operates on two indices.

Our permutation p (6.1) is not cyclic because there are three p-orbits:



σ τ

It is clear that

$$p = \sigma\tau = \tau\sigma,$$

where $\sigma\tau$ denotes the product permutation.

(6.5) **Proposition.** Let σ, τ be permutations which operate on disjoint sets of indices. Then $\sigma\tau = \tau\sigma$.

Proof. If neither σ nor τ operates on an index $\mathbf{i}$, then $\mathbf{i}\sigma\tau = \mathbf{i}\tau\sigma = \mathbf{i}$. If σ sends $\mathbf{i}$ to $\mathbf{j} \neq \mathbf{i}$, then τ fixes both $\mathbf{i}$ and $\mathbf{j}$. In that case, $\mathbf{i}\sigma\tau = \mathbf{j}\tau = \mathbf{j}$ and $\mathbf{i}\tau\sigma = \mathbf{i}\sigma = \mathbf{j}$ too. The case that τ operates on $\mathbf{i}$ is the same. □

Note, however, that when we multiply permutations which operate on overlapping sets of indices, the operations need not commute. The symmetric group S_n is not a commutative group if $n > 2$. For example, if τ' is the transposition which interchanges 3 and 6 and if σ is as above, then $\sigma\tau' \neq \tau'\sigma$.

(6.6) **Proposition.** Every permutation p not the identity is a product of cyclic permutations which operate on disjoint sets of indices: $p = \sigma_1\sigma_2 \cdots \sigma_k$, and these cyclic permutations σ_r are uniquely determined by p.

Proof. We know that p operates as a cyclic permutation when restricted to a single orbit. For each p-orbit, we may define a cyclic permutation σ_r which permutes that orbit in the same way that p does and which fixes the other indices. Clearly, p is the product of these cyclic permutations. Conversely, let p be written as a product $\sigma_1\sigma_2 \cdots \sigma_k$ of cyclic permutations operating on distinct sets $O_1, \ldots, O_k$ of indices. According to Proposition (6.5), the order does not matter. Note that $\sigma_2, \ldots, \sigma_k$ fix the elements of O_1; hence p and σ_1 act in the same way on O_1. Therefore O_1 is a p-orbit. The same is true for the other cyclic permutations. Thus $O_1, \ldots, O_k$ are the p-orbits which contain more than one element, and the permutations σ_i are those constructed at the start of the proof. □

A *cycle notation* for the cyclic permutation (6.2) is

$$(\mathbf{i}_0\mathbf{i}_1 \cdots \mathbf{i}_{k-1}). \tag{6.7}$$

Thus our particular permutation σ has the cycle notation $(\mathbf{14387})$. The notation is not completely determined by the permutation, because we can start the list with any of the indices $\mathbf{i}_0, \ldots, \mathbf{i}_{k-1}$. There are five equivalent notations for σ:

$$\sigma = (\mathbf{43871}) = (\mathbf{38714}) = \cdots.$$

Any one of these notations may be used.

A *cycle notation* for an arbitrary permutation p is obtained by writing the permutation as a product of cyclic permutations which operate on disjoint indices, and then writing the cycle notations for each of these permutations in succession. The order is irrelevant. Thus two of the possible cycle notations for the permutation p described above are

$$(\mathbf{14387})(\mathbf{26}) \quad \text{and} \quad (\mathbf{62})(\mathbf{87143}).$$

If we wish, we can include the "one-cycle" $(\mathbf{5})$, to represent the fixed element $\mathbf{5}$, thereby presenting all the indices in the list. But this is not customary.

With this notation, every permutation can be denoted by a string of at most n integers, suitably bracketed. Products can still be described by juxtaposition. A cycle notation for the permutation q considered above is $q = (\mathbf{12487\,5})(\mathbf{36})$. Thus

$$\overset{\sigma}{} \quad \overset{\tau}{} \quad \overset{\sigma'}{} \quad \overset{\tau'}{}$$

$$pq = (\mathbf{14387})(\mathbf{26})(\mathbf{12487\,5})(\mathbf{36}) = \sigma\tau\sigma'\tau'. \tag{6.8}$$

This string of cycles represents the permutation pq. To evaluate the product on an index, the index is followed through the four factors:

$$\mathbf{1} \overset{\sigma}{\rightsquigarrow} \mathbf{4} \overset{\tau}{\rightsquigarrow} \mathbf{4} \overset{\sigma'}{\rightsquigarrow} \mathbf{8} \overset{\tau'}{\rightsquigarrow} \mathbf{8}, \text{ and so on.}$$

However, (6.8) does not exhibit the decomposition of pq into disjoint cycles, because indices appear more than once. Computation of the permutation as above leads to the cycle decomposition

$$pq = (\mathbf{185})(\mathbf{237})(\mathbf{46}) = \begin{array}{ccc} \overset{8}{\curvearrowright} & \overset{3}{\curvearrowright} & \overset{4}{\circlearrowleft} \\ \mathbf{1}\ \ \mathbf{5} & \mathbf{2}\ \ \mathbf{7} & \mathbf{6} \end{array}.$$

When the computation is finished, every index occurs at most once.

For another sample, let $\rho = (\mathbf{548})$. Then

$$\begin{aligned} \sigma\rho &= (\mathbf{14387})(\mathbf{548}) = (\mathbf{187})(\mathbf{354}) \\ \rho\sigma &= (\mathbf{548})(\mathbf{14387}) = (\mathbf{147})(\mathbf{385}). \end{aligned} \tag{6.9}$$

Now let us compute the conjugate of a permutation p. Since p is a product of disjoint cycles, it will be enough to describe the conjugate $q^{-1}\sigma q$ of a cyclic permutation σ, say the permutation $(\mathbf{i}_1 \cdots \mathbf{i}_k)$. (The fact that we have switched the order of multiplication makes the expression for conjugation by q^{-1} a little nicer than that for conjugation by q.)

(6.10) **Proposition.**

(a) Let σ denote the cyclic permutation $(\mathbf{i}_1\mathbf{i}_2 \cdots \mathbf{i}_k)$, and let q be any permutation. Denote the index $\mathbf{i}_r q$ by $\mathbf{j}_r$. Then the conjugate permutation $q^{-1}\sigma q$ is the cyclic permutation $(\mathbf{j}_1\mathbf{j}_2 \cdots \mathbf{j}_k)$.

(b) If an arbitrary permutation p is written as a product of disjoint cycles σ, then $q^{-1}pq$ is the product of the disjoint cycles $q^{-1}\sigma q$.

(c) Two permutations p, p' are conjugate elements of the symmetric group if and only if their cycle decompositions have the same orders.

Proof. The proof of (a) is the following computation:

$$\mathbf{j}_r q^{-1}\sigma q = \mathbf{i}_r \sigma q = \mathbf{i}_{r+1} q = \mathbf{j}_{r+1},$$

in which the indices are to be read modulo k. Part (b) follows easily. Also, the fact that conjugate permutations have cycle decompositions with the same orders follows from (b). Conversely, suppose that p and p' have cycle decompositions of the same

orders. Say that $p = (\mathbf{i}_1 \cdots \mathbf{i}_r)(\mathbf{i}_1' \cdots \mathbf{i}_s') \cdots$ and $p' = (\mathbf{j}_1 \cdots \mathbf{j}_r)(\mathbf{j}_1' \cdots \mathbf{j}_s') \cdots$. Define q to be the permutation sending $\mathbf{i}_\nu \rightsquigarrow \mathbf{j}_\nu$, $\mathbf{i}_\nu' \rightsquigarrow \mathbf{j}_\nu'$, and so on. Then $p' = q^{-1}pq$. □

Let us determine the Class Equation for the symmetric group S_4 as an example. This group contains six transpositions

$$(\mathbf{12}), \quad (\mathbf{13}), \quad (\mathbf{14}), \quad (\mathbf{23}), \quad (\mathbf{24}), \quad (\mathbf{34}),$$

three products of disjoint transpositions

$$(\mathbf{12})(\mathbf{34}), \quad (\mathbf{13})(\mathbf{24}), \quad (\mathbf{14})(\mathbf{23}),$$

eight 3-cycles, and six 4-cycles. By Proposition (6.10), each of these sets forms one conjugacy class. So the Class Equation of S_4 is

$$24 = 1 + 3 + 6 + 6 + 8.$$

We will now describe the subgroups G of the symmetric group S_p whose order is divisible by p and whose Sylow p-subgroup is normal. We assume that p is a prime integer. Since p divides $p! = |S_p|$ only once, it also divides $|G|$ once, and so the Sylow p-subgroup of G is a cyclic group.

It turns out that such subgroups have a very nice description in terms of the finite field $\mathbb{F}_p$. To obtain it, we use the elements $\{\mathbf{0}, \mathbf{1}, \cdots, \mathbf{p-1}\}$ of the finite field as the indices. Certain permutations of this set are given by the field operations themselves. Namely, we have the operations (*add a*) and (*multiply by c*) for any given $a, c \in \mathbb{F}_p$, $c \neq 0$. They are invertible operations and hence permutations of $\mathbb{F}_p$, so they represent elements of the symmetric group. For example, (*add* 1) is the p-cycle

$$(\textit{add } 1) = (\mathbf{0}\,\mathbf{1}\,\mathbf{2} \cdots (\mathbf{p-1})). \tag{6.11}$$

The operator (*multiply by c*) always fixes the index **0**, but its cycle decomposition depends on the order of the element c in $\mathbb{F}_p^\times$. For example,

$$\begin{aligned} (\textit{multiply by } 2) &= (\mathbf{1243}) \qquad \text{if } p = 5 \\ &= (\mathbf{124})(\mathbf{365}) \quad \text{if } p = 7. \end{aligned} \tag{6.12}$$

Combining the operations of addition and multiplication gives us all operators on $\mathbb{F}_p$ of the form

$$x \rightsquigarrow cx + a. \tag{6.13}$$

The set of these operators forms a subgroup G of order $p(p-1)$ of the symmetric group.

The group of operators (6.13) has a nice matrix representation, as the set of 2×2 matrices with entries in the field $\mathbb{F}_p$, of the form

$$\begin{bmatrix} 1 & a \\ & c \end{bmatrix}. \tag{6.14}$$

This matrix operates by right multiplication on the vector $(1, x)$, sending it to $(1, cx + a)$. So we can recover the operation of G on $\mathbb{F}_p$ from right multiplication by the corresponding matrix. (We use right multiplication because of our chosen order of operations.) The operations (add a) and (multiply by c) are represented by the elementary matrices

$$\begin{bmatrix} 1 & a \\ & 1 \end{bmatrix}, \begin{bmatrix} 1 & \\ & c \end{bmatrix}.$$

(6.15) **Theorem.** Let p be a prime, and let H be a subgroup of the symmetric group S_p whose order is divisible by p. If the Sylow p-subgroup of H is normal, then, with suitable labeling of the indices, H is contained in the group of operators of the form (6.13).

For example, the dihedral group D_p operates faithfully on the vertices of a regular p-gon, and so it is realized as a subgroup of the symmetric group S_p. It is the subgroup of (6.14) consisting of the matrices in which $c = \pm 1$.

Proof of the theorem. The only elements of order p of S_p are the p-cycles. So H contains a p-cycle, say σ. We may relabel indices so that σ becomes the standard p-cycle $(add\ 1) = (\mathbf{0}\,\mathbf{1}\cdots(\mathbf{p-1}))$. Then this permutation generates the Sylow p-subgroup of H.

Let τ_1 be another element of H. We have to show that τ_1 corresponds to an operator of the form (6.13). Say that τ_1 sends the index $\mathbf{0}$ to $\mathbf{i}$. Since σ^i also sends $\mathbf{0}$ to $\mathbf{i}$, the product $\tau = \sigma^{-i}\tau_1$ fixes $\mathbf{0}$. It suffices to show that τ has the form (6.13), and to do so, we will show that τ is one of the operators $(multiply\ by\ c)$.

By hypothesis, $K = \{1, \sigma, \ldots, \sigma^{p-1}\}$ is a normal subgroup of H. Therefore

$$\tau^{-1}\sigma\tau = \sigma^k \tag{6.16}$$

for some k between 1 and $p-1$. We now determine τ by computing both sides of this equation. By Proposition (6.10), the left side is the p-cycle $\tau^{-1}\sigma\tau = (\mathbf{0}\tau\ \mathbf{1}\tau \ldots (\mathbf{p-1})\tau)$, while direct computation of the right side gives $\sigma^k = (\mathbf{0k}\ \mathbf{2k} \ldots (\mathbf{p-1})\mathbf{k})$:

$$(\mathbf{0}\tau\ \mathbf{1}\tau \ldots (\mathbf{p-1})\tau) = (\mathbf{0}\ \mathbf{k}\ \mathbf{2k} \ldots (\mathbf{p-1})\mathbf{k}).$$

We must be careful in interpreting the equality of these two cycles, because the cycle notation is not unique. We need to know that the first index on the left is the same as the first index on the right. Otherwise we will have to identify equal indices in the two cycles and begin with them. That is why we normalized at the start, to have $\mathbf{0}\tau = \mathbf{0}$. Knowing that fact, the two lists are the same, and we conclude that

$$\mathbf{1}\tau = \mathbf{k}, \quad \mathbf{2}\tau = \mathbf{2k}, \quad \ldots .$$

This is the operator $(multiply\ by\ k)$, as claimed. □

We now return for a moment to the question of order of operations. If we wish to use the notation $p(\mathbf{i})$ for permutations in this section, as we do for functions else-

where, we must modify our way of computing with cycles in order to take this into account. The most systematic way to proceed is to read *everything*, including cycles, from right to left. In other words, we should read the cycle (**14387**) as

$$\mathbf{1} \leftsquigarrow \mathbf{4} \leftsquigarrow \mathbf{3} \leftsquigarrow \mathbf{8} \leftsquigarrow \mathbf{7} \leftsquigarrow \mathbf{1}.$$

This is the inverse of the permutation (6.3). We can then interpret the product (**14387**)(**548**) as composition: "First apply (**548**), then (**14387**)." Computation of this product gives

$$\mathbf{1} \leftsquigarrow \mathbf{8} \leftsquigarrow \mathbf{7} \leftsquigarrow \mathbf{1}, \quad \mathbf{3} \leftsquigarrow \mathbf{5} \leftsquigarrow \mathbf{4} \leftsquigarrow \mathbf{3},$$

which we would write as (**187**)(**354**). Notice that this is the same string of symbols as we obtained in (6.9). Miraculously, reading everything backward gives the same answer when we multiply permutations. But of course, the notation (**187**)(**354**) now stands for the inverse of the permutation (6.9). The fact that the notations multiply consistently in our two ways of reading permutations mitigates the crime we have committed in switching from left to right.

7. THE FREE GROUP

We have seen a few groups, such as the symmetric group S_3, the dihedral groups D_n, and the group M of rigid motions of the plane, in which one can compute easily using a list of generators and a list of relations for manipulating them. The rest of this chapter is devoted to the formal background for such methods. In this section, we consider groups which have a set of generators satisfying *no* relations other than ones [such as $x(yz) = (xy)z$] which are implied by the group axioms. A set S of elements of a group which satisfy no relations except those implied by the axioms is called *free*, and a group which has a free set of generators is called a *free group*. We will now describe the free groups.

We start with an arbitrary set S of symbols, say $S = \{a, b, c, \ldots\}$, which may be finite or infinite, and define a *word* to be a finite string of symbols from S, in which repetition is allowed. For instance a, aa, ba, and $aaba$ are words. Two words can be composed by juxtaposition:

$$aa, ba \rightsquigarrow aaba;$$

in this way the set W of all words has an associative law of composition. Moreover, the "empty word" can be introduced as an identity element for this law. We will need a symbol to denote the empty word; let us use 1. The set W is called the *free semigroup* on the set of symbols S. Unfortunately it is not a group because inverses are lacking, and the introduction of inverses complicates things.

Let S' be the set consisting of the symbols in S and also of symbols a^{-1} for every $a \in S$:

$$S' = \{a, a^{-1}, b, b^{-1}, c, c^{-1}, \ldots\}. \tag{7.1}$$

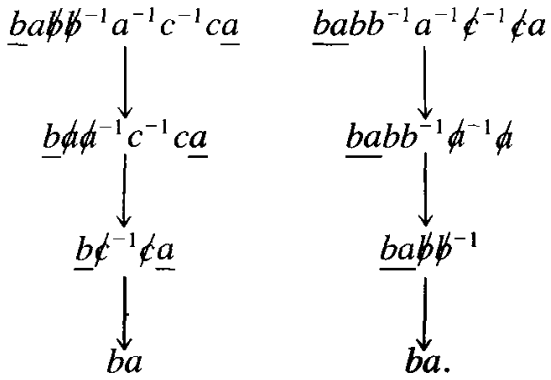
Let W' be the set of words made using the symbols S'. If a word $w \in W'$ looks

like

$$\cdots xx^{-1}\cdots \quad \text{or} \quad \cdots x^{-1}x\cdots$$

for some $x \in S$, then we can agree to *cancel* the two symbols x, x^{-1} and reduce the length of the word. The word will be called *reduced* if no such cancellation can be made. Starting with any word w, we can perform a finite sequence of cancellations and must eventually get a reduced word w_0, possibly the empty word 1. We call this word w_0 a *reduced form* of w.

Now there is often more than one way to proceed with cancellation. For instance, starting with $w = babb^{-1}a^{-1}c^{-1}ca$, we can proceed in several ways, such as



The same reduced word is obtained at the end, though the letters come from different places in the original word. (The letters which remain at the end have been underlined.) This is the general situation.

(7.2) **Proposition.** There is only one reduced form of a given word w.

Proof. We use induction on the length of w. If w is reduced, there is nothing to show. If not, there must be some pair of letters which can be cancelled, say the underlined pair

$$w = \cdots \underline{xx^{-1}} \cdots .$$

(Let us allow x to denote any element of S', with the obvious convention that if $x = a^{-1}$ then $x^{-1} = a$.) If we show that we can obtain every reduced form w_0 of w by cancelling the pair $\underline{xx^{-1}}$ first, then the proposition will follow by induction on the shorter word $\cdots \not{x}\not{x}^{-1}\cdots$ thus obtained.

Let w_0 be a reduced form of w. We know that w_0 is obtained from w by some sequence of cancellations. The first case is that our pair $\underline{xx^{-1}}$ is cancelled at some step in this sequence. Then we might as well rearrange the operations and cancel $\underline{xx^{-1}}$ first. So this case is settled. On the other hand, the pair $\underline{xx^{-1}}$ can not remain in w_0, since w_0 is reduced. Therefore at least one of the two symbols must be cancelled at some time. If the pair itself is not cancelled, then the first cancellation involving the pair must look like

$$\cdots \not{x}^{-1}\underline{\not{x}x^{-1}}\cdots \quad \text{or} \quad \cdots \underline{x\not{x}^{-1}}\not{x}\cdots .$$

Notice that the word obtained by this cancellation is the same as that obtained by

cancelling the original pair $\underline{xx}^{-1}$. So we may cancel the original pair at this stage instead. Then we are back in the first case, and the proposition is proved. □

Now we call two words w, w' in W' *equivalent*, and we write $w \sim w'$, if they have the same reduced form. This is an equivalence relation.

(7.3) **Proposition.** The product of equivalent words is equivalent: If $w \sim w'$ and $v \sim v'$, then $wv \sim w'v'$.

Proof. To obtain the reduced word equivalent to the product wv, we can first cancel as much as possible in w and in v, to reduce w to w_0 and v to v_0. Then wv is reduced to w_0v_0. Now we continue cancelling in w_0v_0 if possible. Since $w' \sim w$ and $v' \sim v$, the same process, applied to $w'v'$, passes through w_0v_0 too, and hence it leads to the same reduced word. □

It follows from this proposition that equivalence classes of words may be multiplied, that is, that there is a well-defined law of composition on the set of equivalence classes of words.

(7.4) **Proposition.** Let F denote the set of equivalence classes of words in W'. Then F is a group with the law of composition induced from W'.

Proof. The facts that multiplication is associative and that the class of the empty word 1 is an identity follow from the corresponding facts in W'. It remains to check that all elements of F are invertible. But clearly, if $w = xy \cdots z$ then the class of $z^{-1} \cdots y^{-1}x^{-1}$ is the inverse of the class of w. □

(7.5) **Definition.** The group F of equivalence classes of words is called the *free group* on the set S.

So an element of the free group F corresponds to exactly one reduced word in W', by Proposition (7.2). To multiply reduced words, combine and cancel:

$$(abc^{-1})(cb) \rightsquigarrow abc^{-1}cb = abb.$$

One can also introduce power notation for reduced words: $aaab^{-1}b^{-1} = a^3b^{-2}$.

The free group on the set $S = \{a\}$ consisting of one element is the same as the set of all powers of a: $F = \{a^n\}$. It is an infinite cyclic group. In contrast, the free group on a set $S = \{a, b\}$ of two elements is very complicated.

8. GENERATORS AND RELATIONS

Having described free groups, we now consider the more likely case that a set of generators of a group is not free—that there are some nontrivial relations among them. Our discussion is based on the mapping properties of the free group and of quotient groups.

(8.1) **Proposition.** *Mapping property of the free group:* Let F be the free group on a set $S = \{a, b, \ldots\}$, and let G be a group. Every map of sets f: $S \longrightarrow G$ extends in a unique way to a group homomorphism φ: $F \longrightarrow G$. If we denote the image $f(x)$ of an element $x \in S$ by $\tilde{x}$, then φ sends a word in $S' = \{a, a^{-1}, b, b^{-1}, \ldots\}$ to the corresponding product of the elements $\{\tilde{a}, \tilde{a}^{-1}, \tilde{b}, \tilde{b}^{-1}, \ldots\}$ in G.

Proof. This rule does define a map on the set of words in S'. We must show that equivalent words are sent to the same product in G. But since cancellation in a word will not change the corresponding product in G, this is clear. Also, since multiplication in F is defined by juxtaposition, the map φ thus defined is a homomorphism. It is the only way to extend f to a homomorphism. □

If S is any subset of a group G, the mapping property defines a homomorphism φ: $F \longrightarrow G$ from the free group on S to G. This reflects the fact that the elements of S satisfy no relations in F except those implied by the group axioms, and explains the reason for the adjective *free*.

A family S of elements is said to *generate* a group G if the map φ from the free group on S to G is surjective. This is the same as saying that every element of G is a product of some string of elements of S', so it agrees with the terminology introduced in Section 2 of Chapter 2. In any case, whether or not S generates G, the image of the homomorphism φ of Proposition (8.1) is a subgroup called the *subgroup generated by* S. This subgroup consists precisely of all products of elements of S'.

Assume that S generates G. The elements of S are then called *generators*. Since φ is a surjective homomorphism, the First Isomorphism Theorem [Chapter 2 (10.9)] tells us that G is isomorphic to the quotient group F/N, where $N = \ker \varphi$. The elements of N are called *relations* among the generators. They are equivalence classes of words w with the property that the corresponding product in G is 1:

$$\varphi(w) = 1 \quad \text{or} \quad w = 1 \text{ in } G.$$

In the special case that $N = \{1\}$, φ is an isomorphism. In this case G is called a free group too.

If we know a set of generators and also all the relations, then we can compute in the isomorphic group F/N and hence in our group G. But the subgroup N will be infinite unless G is free, so we can't list all its elements. Rather, a set of words

$$R = \{r_1, r_2, \ldots\}$$

is called a set of *defining relations* for G if $R \subset N$ and if N is the *smallest normal subgroup containing* R. This means that N is generated by the subset consisting of all the words in R and also all their conjugates.

It might seem more systematic to require the defining relations to be generators for the group N. But remember that the kernel of the homomorphism $F \longrightarrow G$ defined by a set of generators is always a normal subgroup, so there is no need to make the list of defining relations longer. If we know that some relation $r = 1$ holds in G, then we can conclude that $grg^{-1} = 1$ holds in G too, simply by multiplying both sides of the equation on the left and right by g and g^{-1}.

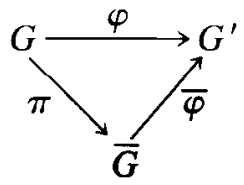
We already know a few examples of generators and relations, such as the dihedral group D_n [Chapter 5 (3.6), (3.7)]. It is generated by the two elements x, y, with relations

$$x^n = 1, \quad y^2 = 1, \quad xyxy = 1. \tag{8.2}$$

(8.3) **Proposition.** The elements $x^n, y^2, xyxy$ form a set of defining relations for the dihedral group.

This proposition is essentially what was checked in Chapter 5 (3.6). But to prove it formally, and to work freely with the concept of generators and relations, we will need what is called the mapping property of quotient groups. It is a generalization of the First Isomorphism Theorem:

(8.4) **Proposition.** *Mapping property of quotient groups:* Let N be a normal subgroup of G, let $\overline{G} = G/N$, and let π be the canonical map $G \longrightarrow \overline{G}$ defined by $\pi(a) = \overline{a} = aN$. Let $\varphi\colon G \longrightarrow G'$ be a homomorphism whose kernel contains N. There is a unique homomorphism $\overline{\varphi}\colon \overline{G} \longrightarrow G'$ such that $\overline{\varphi}\pi = \varphi$:



This map is defined by the rule $\overline{\varphi}(\overline{a}) = \varphi(a)$.

Proof. To define a map $\overline{\varphi}\colon \overline{G} \longrightarrow G'$, we must define $\overline{\varphi}(\alpha)$ for every element α of $\overline{G}$. To do this, we represent α by an element $a \in G$, choosing a so that $\alpha = \pi(a)$. In the bar notation, this means that $\alpha = \overline{a}$. Now since we want our map $\overline{\varphi}$ to satisfy the relation $\overline{\varphi}(\pi(a)) = \varphi(a)$, there is no choice but to define $\overline{\varphi}$ by the rule $\overline{\varphi}(\alpha) = \varphi(a)$, as asserted in the proposition. To show that this is permissible, we must show that the value we obtained for $\overline{\varphi}(\alpha)$, namely $\varphi(a)$, depends only on α and not on our choice of the representative a. This is often referred to as showing that our map is "well-defined."

Let a and a' be two elements of G such that $\overline{a} = \overline{a}' = \alpha$. The equality $\overline{a} = \overline{a}'$ means that $aN = a'N$, or [Chapter 2 (5.13)] that $a' \in aN$. So $a' = an$ for some $n \in N$. Since $N \subset \ker \varphi$ by hypothesis, $\varphi(n) = 1$. Thus $\varphi(a') = \varphi(a)\varphi(n) = \varphi(a)$, as required.

Finally, the map $\overline{\varphi}$ is a homomorphism because $\overline{\varphi}(\overline{a})\overline{\varphi}(\overline{b}) = \varphi(a)\varphi(b) = \varphi(ab) = \overline{\varphi}(\overline{ab})$. □

Proof of Proposition (8.3). We showed in Chapter 5 (3.6) that D_n is generated by elements x, y which satisfy (8.2). Therefore there is a surjective map $\varphi\colon F \longrightarrow D_n$ from the free group on x, y to D_n, and $R = \{x^n, y^2, xyxy\}$ is contained in $\ker \varphi$. Let N be the smallest normal subgroup of F containing R. Then since $\ker \varphi$ is a normal subgroup which contains R, $N \subset \ker \varphi$. The mapping property of quo-

tients gives us a homomorphism $\overline{\varphi}$: $F/N \longrightarrow D_n$. If we show that $\overline{\varphi}$ is bijective, the proposition will be proved.

Note that since φ is surjective, $\overline{\varphi}$ is too. Also, in F/N the relations $\overline{x}^n = 1$, $\overline{y}^2 = 1$, and $\overline{x}\overline{y}\overline{x}\overline{y} = 1$ hold. Using them, we can put any word in $\overline{x}, \overline{y}$ into the form $\overline{x}^i\overline{y}^j$, with $0 \leq i \leq n-1$ and $0 \leq j \leq 1$. This shows that F/N has at most $2n$ elements. Since $|D_n| = 2n$, it follows that $\overline{\varphi}$ is bijective, as required. □

We will use the notation

$$\langle x_1, \ldots, x_m; r_1, \ldots, r_k \rangle \tag{8.5}$$

to denote the group generated by elements $x_1, \ldots, x_m$, with defining relations $r_1, \ldots, r_k$. Thus

$$D_n = \langle x, y; x^n, y^2, xyxy \rangle. \tag{8.6}$$

As a new example, let us consider the group generated by x, y, with the single relation $xyx^{-1}y^{-1} = 1$. If x, y are elements of a group, then

$$xyx^{-1}y^{-1} \tag{8.7}$$

is called their *commutator*. This commutator is important because it is equal to 1 if and only if x and y commute. This is seen by multiplying both sides of the equation $xyx^{-1}y^{-1} = 1$ on the right by yx. So if we impose the relation $xyx^{-1}y^{-1} = 1$ on the free group, we will obtain a group in which x and y commute. Thus if N is the smallest normal subgroup containing the commutator $xyx^{-1}y^{-1}$ and if $G = F/N$, then the residues of x and y are commuting elements of G. This forces any two elements of G to commute.

(8.8) **Proposition.** Let F be the free group on x, y and let N be the smallest normal subgroup generated by the commutator $xyx^{-1}y^{-1}$. The quotient group $G = F/N$ is abelian.

Proof. Let us denote the residues of the generators x, y in G by the same letters. Since the commutator is in N, the elements x,y commute in G. Then x commutes with y^{-1} too. For xy^{-1} and $y^{-1}x$ both become equal to x when multiplied on the left by y. So by the Cancellation Law, they are equal. Also, x obviously commutes with x and with x^{-1}. So x commutes with any word in $S' = \{x, x^{-1}, y, y^{-1}\}$. So does y. It follows by induction that any two words in S' commute. Since x,y generate the group, G is commutative. □

Note this consequence: The commutator $uvu^{-1}v^{-1}$ of any two words in S' is in the normal subgroup generated by the single commutator $xyx^{-1}y^{-1}$, because, since u, v commute in G, the commutator represents the identity element in G.

The group G constructed above is called the *free abelian group* on the set $\{x, y\}$, because the elements x,y satisfy no relations except those implied by the group axioms and the commutative law.

In the examples we have seen, knowledge of the relations allows us to compute

easily in the group. This is somewhat misleading, because computation with a given set of relations is often not easy at all. For example, suppose that we change the defining relations (8.6) for the dihedral group slightly, substituting y^3 for y^2:

$$G = \langle x, y; x^n, y^3, xyxy \rangle. \tag{8.9}$$

This group is much more complicated. When $n > 5$, it is an infinite group.

Things become very difficult when the relations are complicated enough. Suppose that we are given a set R of words, and let N be the smallest normal subgroup containing R. Let w, w' be any other words. Then we can pose the problem of deciding whether or not w and w' represent the same element of F/N. This is called the *word problem for groups*, and it is known that there is no general procedure for deciding it in a predictable length of time. Nevertheless, generators and relations allow efficient computation in many cases, and so they are a useful tool. We will discuss an important method for computation, the Todd–Coxeter Algorithm, in the next section.

Recapitulating, when we speak of a group defined by generators S and relations R, we mean the quotient group F/N, where F is the free group on S and N is the smallest normal subgroup of F containing R. Note that *any* set R of relations will define a group, because F/N is always defined. The larger R is, the larger N becomes and the more collapsing takes place in the homomorphism $\pi: F \longrightarrow F/N$. If R gets "too big," the worst that can happen is that $N = F$, hence that F/N is the trivial group. Thus there is no such thing as a contradictory set of relations. The only problems which may arise occur when F/N becomes too small, which happens when the relations cause more collapsing than was expected.

9. THE TODD–COXETER ALGORITHM

Let H be a subgroup of a finite group G. The Todd–Coxeter Algorithm which is described in this section is an amazing direct method of counting the cosets of H in G and of determining the operation of G on the set of cosets. Since we know that any operation on an orbit looks like an operation on cosets [Chapter 5 (6.3)], the algorithm is really a method of describing any group operation.

In order to compute explicitly, both the group G and the subgroup H must be given to us in an explicit way. So we consider a group

$$G = \langle x_1, \ldots, x_m; r_1, \ldots, r_k \rangle \tag{9.1}$$

presented by generators $x_1, \ldots, x_m$ and explicitly given relations $r_1, \ldots, r_k$, as in the previous section. Thus G is realized as the quotient group F/N, where F is the free group on the set $\{x_1, \ldots, x_m\}$ and N is the smallest normal subgroup containing $\{r_1, \ldots, r_k\}$. We also assume that the subgroup H of G is given to us explicitly by a set of words

$$\{h_1, \ldots, h_s\} \tag{9.2}$$

in the free group F, whose images in G generate H.

Let us work out a specific example to begin with. We take for G the group generated by three elements x, y, z, with relations x^3, y^2, z^2, xyz, and for H the cyclic subgroup generated by z:

$$G = \langle x, y, z; x^3, y^2, z^2, xyz \rangle, \quad H = \{z\}. \tag{9.3}$$

Since we will be determining the operation on cosets, which is a permutation representation [Chapter 5 (8.1)], we must decide how to write permutations. We will use the cycle notation of Section 6. This forces us to work with *right cosets Hg* rather than with left cosets, because we want G to operate on the right. Let us denote the set of right cosets of H in G by $\mathscr{C}$. We must also decide how to describe the operation of our group explicitly, and the easiest way is to go back to the free group again, that is, to describe the permutations associated to the given generators x, y, z.

The operations of the generators on the set of cosets will satisfy these rules:

(9.4) **Rules.**

1. The operation of each generator (x,y,z in our example) is a permutation.
2. The relations (x^3, y^2, z^2, xyz in our example) operate trivially.
3. The generators of H (z in our example) fix the coset $H1$.
4. The operation on cosets is transitive.

The first rule is a general property of group operations. It follows from the fact that group elements are invertible. We list it instead of mentioning inverses of the generators explicitly. The second rule holds because the relations represent 1 in G, and it is the group G which operates. Rules 3 and 4 are special properties of the operation on cosets.

We now determine the coset representation by applying only these rules. Let us use indices $\mathbf{1}, \mathbf{2}, \mathbf{3}, \ldots$ to denote the cosets, with $\mathbf{1}$ standing for the coset $H1$. Since we don't know how many cosets there are, we don't know how many indices we need. We will add new ones as necessary.

First, Rule 3 tells us that z sends $\mathbf{1}$ to itself: $\mathbf{1}z = \mathbf{1}$. This exhausts the information in Rule 3, so Rules 1 and 2 take over. Rule 4 will appear only implicitly.

We don't know what x does to the index $\mathbf{1}$. Let's guess that $\mathbf{1}x \neq \mathbf{1}$ and assign a new index, say $\mathbf{1}x = \mathbf{2}$. Continuing with the generator x, we don't know $\mathbf{2}x$, so we assign a third index: $\mathbf{1}x^2 = \mathbf{2}x = \mathbf{3}$. Rule 2 now comes into play. It tells us that x^3 fixes every index. Therefore $\mathbf{1}x^3 = \mathbf{3}x = \mathbf{1}$. It is customary to sum up this information in a table

x	x	x	
1	**2**	**3**	**1**

which exhibits the operation of x on the three indices. The relation xxx appears on the top, and Rule 2 is reflected in the fact that the same index $\mathbf{1}$ appears at both ends.

At this point, we have determined the operation of x on the three indices $\mathbf{1}, \mathbf{2}, \mathbf{3}$, except for one thing: We don't yet know that these indices represent distinct cosets.

We now ask for the operation for y on the index $\mathbf{1}$. Again, we don't know it, so we assign a new index, say $\mathbf{1}y = \mathbf{4}$. Rule 2 applies again. Since y^2 operates trivially, we know that $\mathbf{1}y^2 = \mathbf{4}y = \mathbf{1}$:

	y	y	
1	**4**	**1**.	

The remaining relation is xyz. We know that $\mathbf{1}x = \mathbf{2}$, but we don't yet know $\mathbf{2}y$. So we set $\mathbf{1}xy = \mathbf{2}y = \mathbf{5}$. Rule 2 then tells us that $\mathbf{1}xyz = \mathbf{5}z = \mathbf{1}$:

	x	y	z	
1	**2**	**5**	**1**.	

We now apply Rule 1: The operation of each group element is a permutation of the indices. We have determined that $\mathbf{1}z = \mathbf{1}$ and also that $\mathbf{5}z = \mathbf{1}$. It follows that $\mathbf{5} = \mathbf{1}$. We eliminate the index $\mathbf{5}$, replacing it by $\mathbf{1}$. This in turn tells us that $\mathbf{2}y = \mathbf{1}$. On the other hand, we have already determined that $\mathbf{4}y = \mathbf{1}$. So $\mathbf{4} = \mathbf{2}$ by Rule 1, and we eliminate $\mathbf{4}$.

The entries in the table below have now been determined:

x	x	x	y	y	z	z	x	y	z	
1	**2**	**3**	**1**	**2**	**1**	**1**	**1**	**2**	**1**	**1**
2	**3**	**1**	**2**	**1**	**2**		**2**	**3**		**2**
3	**1**	**2**	**3**		**3**		**3**	**1**	**2**	**3**.

The bottom right corner shows that $\mathbf{2}z = \mathbf{3}$. This determines the rest of the table. There are three indices, and the operation is

$$x = (\mathbf{123}),\ y = (\mathbf{12}),\ z = (\mathbf{23}).$$

Since there are three indices, we conclude that there are three cosets and that the index of H in G is 3. We also conclude that the order of H is 2, and hence that G has order 6. For $z^2 = 1$ is one of our relations; therefore z has order 1 or 2, and since z does not operate trivially on the indices, $z \neq 1$. The three permutations listed above generate the symmetric group, so the permutation representation is an isomorphism from G onto S_3.

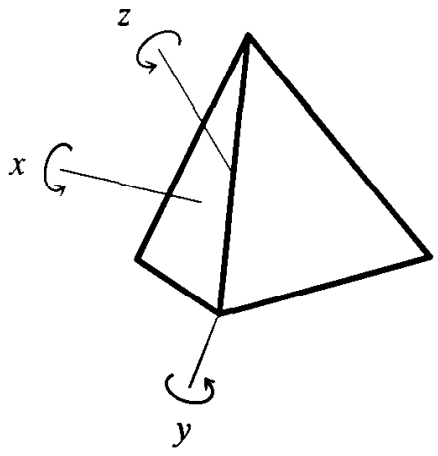
Of course, these conclusions depend on our knowing that the permutation representation we have constructed is the right one. We will show this at the end of the section. Let's compute a few more examples first.

(9.5) **Example.** Consider the tetrahedral group T of the 12 rotational symmetries of a regular tetrahedron (see Section 9 of Chapter 5). If we let y and x denote counterclockwise rotations by $2\pi/3$ about a vertex and the center of a face as shown below,

then $yx = z$ is the rotation by π about an edge. Thus the relations

$$x^3 = 1,\ y^3 = 1,\ yxyx = 1 \tag{9.6}$$

hold in T.



Let us show that (9.6) is a complete set of relations for T. To do so, we consider the group $G = \langle y, x;\ y^3, x^3, yxyx \rangle$ defined by these relations. Since the relations (9.6) hold in T, the mapping property of quotient groups provides a homomorphism φ: $G \longrightarrow T$. This map is surjective because, as is easily seen, y and x generate T. We need only show that φ is injective. We will do this by showing that the order of the group G is 12.

It is possible to analyze the relations directly, but they aren't particularly easy to work with. We could also compute the order of G by enumerating the cosets of the trivial subgroup $H = \{1\}$. This is not efficient either. It is better to use a nontrivial subgroup H of G, such as the one generated by y. This subgroup has order at most 3 because $y^3 = 1$. If we show that its order is 3 and that its index in G is 4, it will follow that G has order 12, and we will be done.

Here is the resulting table. To fill it in, work from both ends of the relations.

x	x	x	y	y	y	y	x	y	x	
1	**2**	**3**	**1**	**1**	**1**	**1**	**1**	**2**	**3**	**1**
2	**3**	**1**	**2**	**3**	**4**	**2**	**3**	**1**	**1**	**2**
3	**1**	**2**	**3**	**4**	**2**	**3**	**4**	**4**	**2**	**3**
4	**4**	**4**	**4**	**2**	**3**	**4**	**2**	**3**	**4**	**4**

Thus the permutation representation is

$$x = (\mathbf{123}),\ y = (\mathbf{234}). \tag{9.7}$$

Since there are four indices, the index of H is 4. Also, notice that y does have order precisely 3. For since $y^3 = 1$, the order is at most 3, and since the permutation $(\mathbf{234})$ associated to y has order 3, it is at least 3. So the order of the group is 12, as predicted. Incidentally, we can derive the fact that T is isomorphic to the alternating group A_4 by verifying that the permutations (9.7) generate that group. □

(9.8) **Example.** We modify the relations (9.6) slightly. Let G be generated by x, y, with relations

$$x^3 = 1, y^3 = 1, yxy^2x = 1,$$

and let H be the subgroup generated by y. Here is a start for a table. Since $y^3 = 1$, we have shortened the last relation, substituting y^{-1} for y^2. Clearly, y^{-1} acts as the inverse of the permutation associated to y. The entries in the bottom row have been determined by working from the right side.

x	x	x	y	y	y	y	x	y^{-1}	x
1	**2**	**3**	**1**	**1**	**1**	**1**	**1**	**2**	**3**	**1**
2			**2**			**2**	**3**	**1**	**1**	**2**

We rewrite the relation $\mathbf{2}y^{-1} = \mathbf{3}$ as $\mathbf{3}y = \mathbf{2}$. Since $\mathbf{2}y = \mathbf{3}$ as well, it follows that $\mathbf{3}y^2 = \mathbf{3}$ and that $\mathbf{3}y^3 = \mathbf{2}$. But $y^3 = 1$, so $\mathbf{3} = \mathbf{2}$, which in turn implies $\mathbf{1} = \mathbf{2} = \mathbf{3}$. Since the generators x, y fix $\mathbf{1}$, there is one coset, and $H = G$. Therefore x is a power of y. The third relation shows that $x^2 = 1$. Combining this fact with the first relation, we find $x = 1$. Thus G is a cyclic group of order 3. This example illustrates how relations may collapse the group. □

In our examples, we have taken for H the subgroup generated by one of the chosen generators of G, but we could also make the computation with a subgroup H generated by an arbitrary set of words. They must be entered into the computation using Rule 3.

This method can also be used when G is infinite, provided that the index $[G:H]$ is finite. The procedure can not be expected to terminate if there are infinitely many cosets.

We now address the question of why the procedure we have described does give the operation on cosets. A formal proof of this fact is not possible without first defining the algorithm formally, and we have not done this. So we will discuss the question informally. We describe the procedure this way: At a given stage of the computation, we will have some set $\mathbf{I}$ of indices, and the operation of some generators of the group on some indices will have been determined. Let us call this a *partial operation* on $\mathbf{I}$. A partial operation need not be consistent with Rules 1, 2, and 3, but it should be transitive; that is, all indices should be in the "partial orbit" of $\mathbf{1}$. This is where Rule 4 comes in. It tells us not to introduce any indices we don't need.

The starting position is $\mathbf{I} = \{\mathbf{1}\}$, with no operations assigned. At any stage there are two possible steps:

(9.9)

(i) We may equate two indices $\mathbf{i}, \mathbf{j} \in \mathbf{I}$ as a consequence of one of the first three rules, or

(ii) we may choose a generator x and an index $\mathbf{i}$ such that $\mathbf{i}x$ has not yet been determined and define $\mathbf{i}x = \mathbf{j}$, where $\mathbf{j}$ is a new index.

We stop the process when an operation has been determined which is consistent with the rules, that is, when we have a complete, consistent table and the rules hold.

There are two questions to ask: First, will this procedure terminate? Second, if it terminates, is the operation the right one? The answer to both questions is yes. It can be shown that the process always terminates, provided that the group is finite and that preference is given to Step (i). We will not prove this. The more important fact for applications is that if the process terminates, the resulting permutation representation is the right one.

(9.10) **Theorem.** Suppose that a finite number of repetitions of Steps (i) and (ii) yields a consistent table. Then the table defines a permutation representation which is isomorphic, by suitable numbering, to the representation on cosets.

Sketch of proof. Let $\mathbf{I}^*$ denote the final set of indices, with its operation. We will prove the proposition by defining a bijective map φ^*: $\mathbf{I}^* \longrightarrow \mathcal{C}$ from this set to the set of cosets which is compatible with the two operations. We define φ^* inductively, by defining at each stage a map φ: $\mathbf{I} \longrightarrow \mathcal{C}$ from the set of indices determined at that stage to $\mathcal{C}$, such that φ is compatible with the partial operation on $\mathbf{I}$. To start, $\{\mathbf{1}\} \longrightarrow \mathcal{C}$ sends $\mathbf{1} \rightsquigarrow H1$. Now suppose that φ: $\mathbf{I} \longrightarrow \mathcal{C}$ has been defined, and let $\mathbf{I}'$ be the result of applying one of Steps (9.9) to $\mathbf{I}$. In case of Step (ii), there is no difficulty in extending φ to a map φ': $\mathbf{I} \longrightarrow \mathcal{C}$. We simply define $\varphi'(\mathbf{k}) = \varphi(\mathbf{k})$ if $\mathbf{k} \neq \mathbf{j}$, and $\varphi'(\mathbf{j}) = \varphi(\mathbf{i})x$. Next, suppose that we use Step (ii) to equate two indices, say $\mathbf{i}, \mathbf{j}$, so that $\mathbf{I}$ is collapsed to form the new index set $\mathbf{I}'$. Then the next lemma allows us to define the map φ': $\mathbf{I}' \longrightarrow \mathcal{C}$:

(9.11) **Lemma.** Suppose that a map φ: $\mathbf{I} \longrightarrow \mathcal{C}$ is given, compatible with a partial operation on $\mathbf{I}$. Let $\mathbf{i}, \mathbf{j} \in \mathbf{I}$, and suppose that one of the Rules 1, 2, or 3 forces $\mathbf{i} = \mathbf{j}$. Then $\varphi(\mathbf{i}) = \varphi(\mathbf{j})$.

Proof. This is true because, as we have already remarked, the operation on cosets does satisfy all of the Rules (9.4). So if the rules force $\mathbf{i} = \mathbf{j}$, they also force $\varphi(\mathbf{i}) = \varphi(\mathbf{j})$. □

It remains to prove that the map φ^*: $\mathbf{I}^* \longrightarrow \mathcal{C}$ is bijective. To do this, we construct the inverse map ψ^*: $\mathcal{C} \longrightarrow \mathbf{I}^*$, using the following lemma:

(9.12) **Lemma.** Let S be a set on which G operates, and let $s \in S$ be an element stabilized by H. There is a unique map ψ: $\mathcal{C} \longrightarrow S$ which is compatible with the operations on the two sets and which sends $H1 \rightsquigarrow s$.

Proof. This proof repeats that of (6.4) in Chapter 5, except that we have changed to right operations. Since g sends $H \rightsquigarrow Hg$ and since we want $\psi(Hg) = \psi(H)g$, we must try to set $\psi(Hg) = sg$. This proves uniqueness of the map ψ. To prove existence, we first check that the rule $\psi(Hg) = sg$ is well-defined: If $Ha = Hb$, then $ba^{-1} \in H$. By hypothesis, ba^{-1} stabilizes s, so $sa = sb$. Finally, ψ is compatible with the operations of G because $\psi(Hga) = sga = (sg)a = \psi(Hg)a$. □

Now, to prove the bijectivity of ψ^*, we use the lemma to construct a map $\psi^*: \mathscr{C} \longrightarrow \mathbf{I}^*$. Consider the composed map $\varphi^*\psi^*: \mathscr{C} \longrightarrow \mathscr{C}$. It sends $H1 \rightsquigarrow H1$. We apply the lemma again, substituting $\mathscr{C}$ for S. The uniqueness assertion of the lemma tells us that $\varphi^*\psi^*$ is the identity map. On the other hand, since the operation on $\mathbf{I}^*$ is transitive and since ψ^* is compatible with the operations, ψ^* must be surjective. It follows that φ^* and ψ^* are bijective. □

The axiomatic method has many advantages over honest work.

Bertrand Russell

EXERCISES

1. The Operations of a Group on Itself

1. Does the rule $g, x \rightsquigarrow xg^{-1}$ define an operation of G on itself?
2. Let H be a subgroup of a group G. Then H operates on G by left multiplication. Describe the orbits for this operation.
3. Prove the formula $|G| = |Z| + \Sigma|C|$, where the sum is over the conjugacy classes containing more than one element and where Z is the center of G.
4. Prove the Fixed Point Theorem (1.12).
5. Determine the conjugacy classes in the group M of motions of the plane.
6. Rule out as many of the following as possible as Class Equations for a group of order 10: $1+1+1+2+5$, $1+2+2+5$, $1+2+3+4$, $1+1+2+2+2+2$.
7. Let $F = \mathbb{F}_5$. Determine the order of the conjugacy class of $\begin{bmatrix} 1 & \\ & 2 \end{bmatrix}$ in $GL_2(\mathbb{F}_5)$.
8. Determine the Class Equation for each of the following groups.
   (a) the quaternion group, (b) the Klein four group, (c) the dihedral group D_5, (d) D_6, (e) D_n, (f) the group of upper triangular matrices in $GL_2(\mathbb{F}_3)$, (g) $SL_2(\mathbb{F}_3)$.
9. Let G be a group of order n, and let F be any field. Prove that G is isomorphic to a subgroup of $GL_n(F)$.
10. Determine the centralizer in $GL_3(\mathbb{R})$ of each matrix.

(a) $\begin{bmatrix} 1 & & \\ & 2 & \\ & & 3 \end{bmatrix}$ (b) $\begin{bmatrix} 1 & & \\ & 1 & \\ & & 2 \end{bmatrix}$ (c) $\begin{bmatrix} 1 & 1 & \\ & 1 & \\ & & 1 \end{bmatrix}$ (d) $\begin{bmatrix} 1 & 1 & \\ & 1 & 1 \\ & & 1 \end{bmatrix}$

(e) $\begin{bmatrix} 1 & & \\ & & 1 \\ & 1 & \end{bmatrix}$ (f) $\begin{bmatrix} & 1 & \\ & & 1 \\ 1 & & \end{bmatrix}$

*11. Determine all finite groups which contain at most three conjugacy classes.
12. Let N be a normal subgroup of a group G. Suppose that $|N| = 5$ and that $|G|$ is odd. Prove that N is contained in the center of G.

*13. (a) Determine the possible Class Equations for groups of order 8.
(b) Classify groups of order 8.

14. Let Z be the center of a group G. Prove that if G/Z is a cyclic group, then G is abelian and hence $G = Z$.

*15. Let G be a group of order 35.
(a) Suppose that G operates nontrivially on a set of five elements. Prove that G has a normal subgroup of order 7.
(b) Prove that every group of order 35 is cyclic.

2. The Class Equation of the Icosahedral Group

1. Identify the intersection $I \cap O$ when the dodecahedron and cube are as in Figure (2.7).
2. Two tetrahedra can be inscribed into a cube C, each one using half the vertices. Relate this to the inclusion $A_4 \subset S_4$.
3. Does I contain a subgroup T? D_6? D_3?
4. Prove that the icosahedral group has no subgroup of order 30.
5. Prove or disprove: A_5 is the only proper normal subgroup of S_5.
6. Prove that no group of order p^e, where p is prime and $e > 1$, is simple.
7. Prove or disprove: An abelian group is simple if and only if it has prime order.
8. (a) Determine the Class Equation for the group T of rotations of a tetrahedron.
(b) What is the center of T?
(c) Prove that T has exactly one subgroup of order 4.
(d) Prove that T has no subgroup of order 6.
9. (a) Determine the Class Equation for the octahedral group O.
(b) There are exactly two proper normal subgroups of O. Find them, show that they are normal, and show that there are no others.
10. Prove that the tetrahedral group T is isomorphic to the alternating group A_4, and that the octahedral group O is isomorphic to the symmetric group S_4. Begin by finding sets of four elements on which these groups operate.
11. Prove or disprove: The icosahedral group is not a subgroup of the group of real upper triangular 2×2 matrices.
*12. Prove or disprove: A nonabelian simple group can not operate nontrivially on a set containing fewer than five elements.

3. Operations on Subsets

1. Let S be the set of subsets of order 2 of the dihedral group D_3. Determine the orbits for the action of D_3 on S by conjugation.
2. Determine the orbits for left multiplication and for conjugation on the set of subsets of order 3 of D_3.
3. List all subgroups of the dihedral group D_4, and divide them into conjugacy classes.
4. Let H be a subgroup of a group G. Prove that the orbit of the left coset gH for the operation of conjugation contains the right coset Hg.
5. Let U be a subset of a finite group G, and suppose that $|U|$ and $|G|$ have no common factor. Is the stabilizer of $|U|$ trivial for the operation of conjugation?
6. Consider the operation of left multiplication by G on the set of its subsets. Let U be a

subset whose orbit $\{gU\}$ partitions G. Let H be the unique subset in this orbit which contains 1. Prove that H is a subgroup of G and that the sets gU are its left cosets.

7. Let H be a subgroup of a group G. Prove or disprove: The normalizer $N(H)$ is a normal subgroup of the group G.
8. Let $H \subset K \subset G$ be groups. Prove that H is normal in K if and only if $K \subset N(H)$.
9. Prove that the subgroup B of upper triangular matrices in $GL_n(\mathbb{R})$ is conjugate to the group L of lower triangular matrices.
10. Let B be the subgroup of $G = GL_n(\mathbb{C})$ of upper triangular matrices, and let $U \subset B$ be the set of upper triangular matrices with diagonal entries 1. Prove that $B = N(U)$ and that $B = N(B)$.
*11. Let S_n denote the subgroup of $GL_n(\mathbb{R})$ of permutation matrices. Determine the normalizer of S_n in $GL_n(\mathbb{R})$.
12. Let S be a finite set on which a group G operates transitively, and let U be a subset of S. Prove that the subsets gU cover S evenly, that is, that every element of S is in the same number of sets gU.
13. **(a)** Let H be a normal subgroup of G of order 2. Prove that H is in the center of G.
(b) Let H be a normal subgroup of prime order p in a finite group G. Suppose that p is the smallest prime dividing $|G|$. Prove that H is in the center $Z(G)$.
*14. Let H be a proper subgroup of a finite group G. Prove that the union of the conjugates of H is not the whole group G.
15. Let K be a normal subgroup of order 2 of a group G, and let $\overline{G} = G/K$. Let $\overline{C}$ be a conjugacy class in $\overline{G}$. Let S be the inverse image of $\overline{C}$ in G. Prove that one of the following two cases occurs.
(a) $S = C$ is a single conjugacy class and $|C| = 2|\overline{C}|$.
(b) $S = C_1 \cup C_2$ is made up of two conjugacy classes and $|C_1| = |C_2| = |\overline{C}|$.
16. Calculate the double cosets HgH of the subgroup $H = \{1, y\}$ in the dihedral group D_n. Show that each double coset has either two or four elements.
17. Let H, K be subgroups of G, and let H' be a conjugate subgroup of H. Relate the double cosets $H'gK$ and HgK.
18. What can you say about the order of a double coset HgK?

4. The Sylow Theorems

1. How many elements of order 5 are contained in a group of order 20?
2. Prove that no group of order pq, where p and q are prime, is simple.
3. Prove that no group of order p^2q, where p and q are prime, is simple.
4. Prove that the set of matrices $\begin{bmatrix} 1 & a \\ & c \end{bmatrix}$ where $a, c \in \mathbb{F}_7$ and $c = 1, 2, 4$ forms a group of the type presented in (4.9b) (and that therefore such a group exists).
5. Find Sylow 2-subgroups in the following cases:
(a) D_{10} **(b)** T **(c)** O **(d)** I.
6. Find a Sylow p-subgroup of $GL_2(\mathbb{F}_p)$.
*7. **(a)** Let H be a subgroup of G of prime index p. What are the possible numbers of conjugate subgroups of H?
(b) Suppose that p is the smallest prime integer which divides $|G|$. Prove that H is a normal subgroup.

*8. Let H be a Sylow p-su group of G, and let $K = N(H)$. Prove or disprove: $K = N(K)$.

9. Let G be a group of order $p^e m$. Prove that G contains a subgroup of order p^r for every integer $r \leq e$.

10. Let $n = pm$ be an integer which is divisible exactly once by p, and let G be a group of order n. Let H be a Sylow p-subgroup of G, and let S be the set of all Sylow p-subgroups. How does S decompose into H-orbits?

*11. (a) Compute the order of $GL_n(\mathbb{F}_p)$.
(b) Find a Sylow p-subgroup of $GL_n(\mathbb{F}_p)$.
(c) Compute the number of Sylow p-subgroups.
(d) Use the Second Sylow Theorem to give another proof of the First Sylow Theorem.

*12. Prove that no group of order 224 is simple.

13. Prove that if G has order $n = p^e a$ where $1 \leq a < p$ and $e \geq 1$, then G has a proper normal subgroup.

14. Prove that the only simple groups of order < 60 are groups of prime order.

15. Classify groups of order 33.

16. Classify groups of order 18.

17. Prove that there are at most five isomorphism classes of groups of order 20.

*18. Let G be a simple group of order 60.
(a) Prove that G contains six Sylow 5-subgroups, ten Sylow 3-subgroups, and five Sylow 2-subgroups.
(b) Prove that G is isomorphic to the alternating group A_5.

5. The Groups of Order 12

1. Determine the Class Equations of the groups of order 12.

2. Prove that a group of order $n = 2p$, where p is prime, is either cyclic or dihedral.

*3. Let G be a group of order 30.
(a) Prove that either the Sylow 5-subgroup K or the Sylow 3-subgroup H is normal.
(b) Prove that HK is a cyclic subgroup of G.
(c) Classify groups of order 30.

4. Let G be a group of order 55.
(a) Prove that G is generated by two elements x,y, with the relations $x^{11} = 1$, $y^5 = 1$, $yxy^{-1} = x^r$, for some r, $1 \leq r < 11$.
(b) Prove that the following values of r are not possible: 2, 6, 7, 8, 10.
(c) Prove that the remaining values are possible, and that there are two isomorphism classes of groups of order 55.

6. Computation in the Symmetric Group

1. Verify the products (6.9).

2. Prove explicitly that the permutation $(\mathbf{1}\,\mathbf{2}\,\mathbf{3})(\mathbf{4}\,\mathbf{5})$ is conjugate to $(\mathbf{2}\,\mathbf{4}\,\mathbf{1})(\mathbf{3}\,\mathbf{5})$.

3. Let p, q be permutations. Prove that the products pq and qp have cycles of equal sizes.

4. (a) Does the symmetric group S_7 contain an element of order 5? of order 10? of order 15?
(b) What is the largest possible order of an element of S_7?

5. Show how to determine whether a permutation is odd or even when it is written as a product of cycles.
6. Prove or disprove: The order of a permutation is the least common multiple of the orders of the cycles which make it up.
7. Is the cyclic subgroup H of S_n generated by the cycle $(\mathbf{1\,2\,3\,4\,5})$ a normal subgroup?

*8. Compute the number of permutations in S_n which do not leave any index fixed.

9. Determine the cycle decomposition of the permutation $\mathbf{i} \rightsquigarrow \mathbf{n-i}$.
10. (a) Prove that every permutation p is a product of transpositions.
    (b) How many transpositions are required to write the cycle $(\mathbf{1\,2\,3}\cdots\mathbf{n})$?
    (c) Suppose that a permutation is written in two ways as a product of transpositions, say $p = \tau_1\tau_2\cdots\tau_m$ and $p = \tau_1'\tau_2'\cdots\tau_n'$. Prove that m and n are both odd or else they are both even.
11. What is the centralizer of the element $(\mathbf{1\,2})$ of S_4?
12. Find all subgroups of order 4 of the symmetric group S_4. Which are normal?
13. Determine the Class Equation of A_4.
14. (a) Determine the number of conjugacy classes and the Class Equation for S_5.
    (b) List the conjugacy classes in A_5, and reconcile this list with the list of conjugacy classes in the icosahedral group [see (2.2)].
15. Prove that the transpositions $(\mathbf{1\,2}), (\mathbf{2\,3}),\ldots,(\mathbf{n-1,n})$ generate the symmetric group S_n.
16. Prove that the symmetric group S_n is generated by the cycles $(\mathbf{1\,2}\cdots\mathbf{n})$ and $(\mathbf{1\,2})$.
17. (a) Show that the product of two transpositions $(\mathbf{ij})(\mathbf{kl})$ can always be written as a product of 3-cycles. Treat the case that some indices are equal too.
    (b) Prove that the alternating group A_n is generated by 3-cycles, if $n \geq 3$.
18. Prove that if a proper normal subgroup of S_n contains a 3-cycle, it is A_n.

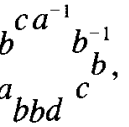
*19. Prove that A_n is simple for all $n \geq 5$.

*20. Prove that A_n is the only subgroup of S_n of index 2.

21. Explain the miraculous coincidence at the end of the section in terms of the opposite group (Chapter 2, Section 1, exercise 12).

7. *The Free Group*

1. Prove or disprove: The free group on two generators is isomorphic to the product of two infinite cyclic groups.
2. (a) Let F be the free group on x,y. Prove that the two elements $u = x^2$ and $v = y^3$ generate a subgroup of F which is isomorphic to the free group on u, v.
    (b) Prove that the three elements $u = x^2$, $v = y^2$, and $z = xy$ generate a subgroup isomorphic to the free group on u, v, z.
3. We may define a *closed word* in S' to be the oriented loop obtained by joining the ends of a word. Thus



represents a closed word, if we read it clockwise. Establish a bijective correspondence between reduced closed words and conjugacy classes in the free group.

4. Let p be a prime integer. Let N be the number of words of length p in a finite set S. Show that N is divisible by p.

8. Generators and Relations

1. Prove that two elements a, b of a group generate the same subgroup as bab^2, bab^3.
2. Prove that the smallest normal subgroup of a group G containing a subset S is generated as a subgroup by the set $\{gsg^{-1} \mid g \in G, s \in S\}$.
3. Prove or disprove: y^2x^2 is in the normal subgroup generated by xy and its conjugates.
4. Prove that the group generated by x, y, z with the single relation $yxyz^{-2} = 1$ is actually a free group.
5. Let S be a set of elements of a group G, and let $\{r_i\}$ be some relations which hold among the elements S in G. Let F be the free group on S. Prove that the map $F \longrightarrow G$ (8.1) factors through F/N, where N is the normal subgroup generated by $\{r_i\}$.
6. Let G be a group with a normal subgroup N. Assume that G and G/N are both cyclic groups. Prove that G can be generated by two elements.
7. A subgroup H of a group G is called *characteristic* if it is carried to itself by all automorphisms of G.
   (a) Prove that every characteristic subgroup is normal.
   (b) Prove that the center Z of a group G is a characteristic subgroup.
   (c) Prove that the subgroup H generated by all elements of G of order n is characteristic.
8. Determine the normal subgroups and the characteristic subgroups of the quaternion group.
9. The *commutator subgroup* C of a group G is the smallest subgroup containing all commutators.
   (a) Prove that the commutator subgroup is a characteristic subgroup.
   (b) Prove that G/C is an abelian group.
10. Determine the commutator subgroup of the group M of motions of the plane.
11. Prove by explicit computation that the commutator $x(yz)x^{-1}(yz)^{-1}$ is in the normal subgroup generated by the two commutators $xyx^{-1}y^{-1}$ and $xzx^{-1}z^{-1}$ and their conjugates.
12. Let G denote the free abelian group $\langle x, y; xyx^{-1}y^{-1}\rangle$ defined in (8.8). Prove the universal property of this group: If u, v are elements of an abelian group A, there is a unique homomorphism φ: $G \longrightarrow A$ such that $\varphi(x) = u$, $\varphi(y) = v$.
13. Prove that the normal subgroup in the free group $\langle x, y\rangle$ which is generated by the single commutator $xyx^{-1}y^{-1}$ is the commutator subgroup.
14. Let N be a normal subgroup of a group G. Prove that G/N is abelian if and only if N contains the commutator subgroup of G.
15. Let φ: $G \longrightarrow G'$ be a surjective group homomorphism. Let S be a subset of G such that $\varphi(S)$ generates G', and let T be a set of generators of $\ker \varphi$. Prove that $S \cup T$ generates G.
16. Prove or disprove: Every finite group G can be presented by a finite set of generators and a finite set of relations.
17. Let G be the group generated by x, y, z, with certain relations $\{r_i\}$. Suppose that one of the relations has the form wx, where w is a word in y, z. Let r_i' be the relation obtained by substituting w^{-1} for x into r_i, and let G' be the group generated by y, z, with relations $\{r_i'\}$. Prove that G and G' are isomorphic.

9. The Todd–Coxeter Algorithm

1. Prove that the elements x, y of (9.5) generate T, and that the permutations (9.7) generate A_4.
2. Use the Todd–Coxeter Algorithm to identify the group generated by two elements x, y, with the following relations.
   (a) $x^2 = y^2 = 1, xyx = yxy$
   (b) $x^2 = y^3 = 1, xyx = yxy$
   (c) $x^3 = y^3 = 1, xyx = yxy$
   (d) $x^4 = y^2 = 1, xyx = yxy$
   (e) $x^4 = y^4 = x^2y^2 = 1$
3. Use the Todd–Coxeter Algorithm to determine the order of the group generated by x, y, with the following relations.
   (a) $x^4 = 1, y^3 = 1, xy = y^2x$ (b) $x^7 = 1, y^3 = 1, yx = x^2y$.
4. Identify the group G generated by elements x, y, z, with relations $x^4 = y^4 = z^3 = x^2z^2 = 1$ and $z = xy$.
5. Analyze the group G generated by x, y, with relations $x^4 = 1$, $y^4 = 1$, $x^2 = y^2$, $xy = y^3x$.

*6. Analyze the group generated by elements x, y, with relations $x^{-1}yx = y^{-1}$, $y^{-1}xy = x^{-1}$.

7. Let G be the group generated by elements x, y, with relations $x^4 = 1, y^3 = 1, x^2 = yxy$. Prove that this group is trivial in these two ways.
   (a) using the Todd–Coxeter Algorithm
   (b) working directly with the relations
8. Identify the group G generated by two elements x, y, with relations $x^3 = y^3 = yxyxy = 1$.
9. Let $p \leq q \leq r$ be integers >1. The *triangle group* G^{pqr} is defined by generators $G^{pqr} = \langle x, y, z; x^p, y^q, z^r, xyz \rangle$. In each case, prove that the triangle group is isomorphic to the group listed.
   (a) the dihedral group D_n, when $p, q, r = 2, 2, n$
   (b) the tetrahedral group, when $p, q, r = 2, 3, 3$
   (c) the octahedral group, when $p, q, r = 2, 3, 4$
   (d) the icosahedral group, when $p, q, r = 2, 3, 5$
10. Let Δ denote an isosceles right triangle, and let a, b, c denote the reflections of the plane about the three sides of Δ. Let $x = ab$, $y = bc$, $z = ca$. Prove that x, y, z generate a triangle group.
11. (a) Prove that the group G generated by elements x, y, z with relations $x^2 = y^3 = z^5 = 1, xyz = 1$ has order 60.
    (b) Let H be the subgroup generated by x and zyz^{-1}. Determine the permutation representation of G on G/H, and identify H.
    (c) Prove that G is isomorphic to the alternating group A_5.
    (d) Let K be the subgroup of G generated by x and yxz. Determine the permutation representation of G on G/K, and identify K.

Miscellaneous Problems

1. (a) Prove that the subgroup T' of O_3 of all symmetries of a regular tetrahedron, including orientation-reversing symmetries, has order 24.

(b) Is T' isomorphic to the symmetric group S_4?
(c) State and prove analogous results for the group of symmetries of a dodecahedron.

2. (a) Let $U = \{1, x\}$ be a subset of order 2 of a group G. Consider the graph having one vertex for each element of G and an edge joining the vertices g to gx for all $g \in G$. Prove that the vertices connected to the vertex 1 are the elements of the cyclic group generated by x.
(b) Do the analogous thing for the set $U = \{1, x, y\}$.

***3.** (a) Suppose that a group G operates transitively on a set S, and that H is the stabilizer of an element $s_0 \in S$. Consider the action of G on $S \times S$ defined by $g(s_1, s_2) = (gs_1, gs_2)$. Establish a bijective correspondence between double cosets of H in G and G-orbits in $S \times S$.
(b) Work out the correspondence explicitly for the case that G is the dihedral group D_5 and S is the set of vertices of a 5-gon.
(c) Work it out for the case that $G = T$ and that S is the set of edges of a tetrahedron.

***4.** Assume that $H \subset K \subset G$ are subgroups, that H is normal in K, and that K is normal in G. Prove or disprove: H is normal in G.

***5.** Prove the *Bruhat decomposition,* which asserts that $GL_n(\mathbb{R})$ is the union of the double cosets BPB, where B is the group of upper triangular matrices and P is a permutation matrix.

6. (a) Prove that the group generated by x, y with relations x^2, y^2 is an infinite group in two ways:
(i) It is clear that every word can be reduced by using these relations to the form $\cdots xyxy \cdots$. Prove that every element of G is represented by exactly one such word.
(ii) Exhibit G as the group generated by reflections r, r' about lines ℓ, ℓ' whose angle of intersection is not a rational multiple of 2π.
(b) Let N be any proper normal subgroup of G. Prove that G/N is a dihedral group.

7. Let H, N be subgroups of a group G, and assume that N is a normal subgroup.
(a) Determine the kernels of the restrictions of the canonical homomorphism $\pi: G \longrightarrow G/N$ to the subgroups H and HN.
(b) Apply the First Isomorphism Theorem to these restrictions to prove the *Second Isomorphism Theorem:* $H/(H \cap N)$ is isomorphic to $(HN)/N$.

8. Let H, N be normal subgroups of a group G such that $H \supset N$, and let $\overline{H} = H/N$, $\overline{G} = G/N$.
(a) Prove that $\overline{H}$ is a normal subgroup of $\overline{G}$.
(b) Use the composed homomorphism $G \longrightarrow \overline{G} \longrightarrow \overline{G}/\overline{H}$ to prove the *Third Isomorphism Theorem:* G/H is isomorphic to $\overline{G}/\overline{H}$.