(ii) Generalize Corollary 2.128 by proving that if the prime factorization of an integer m is $m = p_1^{e_1} \cdots p_n^{e_n}$, then

$$U(\mathbb{I}_m) \cong U(\mathbb{I}_{p_1^{e_1}}) \times \cdots \times U(\mathbb{I}_{p_n^{e_n}}).$$

2.99 Let p be an odd prime, and assume that $a_i \equiv i \bmod p$ for $1 \leq i \leq p-1$. Prove that there exist $i \neq j$ with $ia_i \equiv ja_j \bmod p$.

2.100 **(i)** If p is a prime, prove that $\phi(p^k) = p^k(1 - \frac{1}{p})$.

(ii) If the distinct prime divisors of a positive integer h are $p_1, p_2, \ldots, p_n$, prove that

$$\phi(h) = h(1 - \tfrac{1}{p_1})(1 - \tfrac{1}{p_2}) \cdots (1 - \tfrac{1}{p_n}).$$

2.101 If G is a group and $x, y \in G$, define their ***commutator*** to be $xyx^{-1}y^{-1}$, and define the ***commutator subgroup*** G' to be the subgroup generated by all the commutators (the product of two commutators need not be a commutator).

(i) Prove that $G' \lhd G$.

(ii) Prove that G/G' is abelian.

(iii) If $\varphi\colon G \to A$ is a homomorphism, where A is an abelian group, prove that $G' \leq \ker\varphi$. Conversely, if $G' \leq \ker\varphi$, prove that $\operatorname{im}\varphi$ is abelian.

(iv) If $G' \leq H \leq G$, prove that $H \lhd G$.

2.7 GROUP ACTIONS

Groups of permutations led us to abstract groups; the next result, due to A. Cayley (1821–1895), shows that abstract groups are not so far removed from permutations.

Theorem 2.130 (Cayley). *Every group G is (isomorphic to) a subgroup of the symmetric group S_G. In particular, if $|G| = n$, then G is isomorphic to a subgroup of S_n.*

Proof. For each $a \in G$, define "translation" $\tau_a\colon G \to G$ by $\tau_a(x) = ax$ for every $x \in G$ (if $a \neq 1$, then τ_a is not a homomorphism). For $a, b \in G$, $(\tau_a \circ \tau_b)(x) = \tau_a(\tau_b(x)) = \tau_a(bx) = a(bx) = (ab)x = \tau_{ab}(x)$, by associativity, so that

$$\tau_a\tau_b = \tau_{ab}.$$

It follows that each τ_a is a bijection, for its inverse is $\tau_{a^{-1}}$:

$$\tau_a\tau_{a^{-1}} = \tau_{aa^{-1}} = \tau_1 = 1_G,$$

and so $\tau_a \in S_G$.

Define $\varphi\colon G \to S_G$ by $\varphi(a) = \tau_a$. Rewriting,

$$\varphi(a)\varphi(b) = \tau_a\tau_b = \tau_{ab} = \varphi(ab),$$

so that φ is a homomorphism. Finally, φ is an injection. If $\varphi(a) = \varphi(b)$, then $\tau_a = \tau_b$, and hence $\tau_a(x) = \tau_b(x)$ for all $x \in G$; in particular, when $x = 1$, this gives $a = b$, as desired.

The last statement follows from Exercise 2.56 on page 165, which says that if X is a set with $|X| = n$, then $S_X \cong S_n$. •

The reader may note, in the proof of Cayley's theorem, that the permutation τ_a is just the ath row of the multiplication table of G.

To tell the truth, Cayley's theorem itself is only mildly interesting. However, the identical proof works in a larger setting that is more useful.

Theorem 2.131 (Representation on Cosets). *Let G be a group, and let H be a subgroup of G having finite index n. Then there exists a homomorphism $\varphi\colon G \to S_n$ with $\ker\varphi \leq H$.*

Proof. Even though H may not be a normal subgroup, we still denote the family of all the cosets of H in G by G/H.

For each $a \in G$, define "translation" $\tau_a\colon G/H \to G/H$ by $\tau_a(xH) = axH$ for every $x \in G$. For $a, b \in G$,

$$(\tau_a \circ \tau_b)(xH) = \tau_a(\tau_b(xH)) = \tau_a(bxH) = a(bxH) = (ab)xH = \tau_{ab}(aH),$$

by associativity, so that

$$\tau_a\tau_b = \tau_{ab}.$$

It follows that each τ_a is a bijection, for its inverse is $\tau_{a^{-1}}$:

$$\tau_a\tau_{a^{-1}} = \tau_{aa^{-1}} = \tau_1 = 1_G,$$

and so $\tau_a \in S_{G/H}$. Define $\varphi\colon G \to S_{G/H}$ by $\varphi(a) = \tau_a$. Rewriting,

$$\varphi(a)\varphi(b) = \tau_a\tau_b = \tau_{ab} = \varphi(ab),$$

so that φ is a homomorphism. Finally, if $a \in \ker\varphi$, then $\varphi(a) = 1_{G/H}$, so that $\tau_a(xH) = xH$ for all $x \in G$; in particular, when $x = 1$, this gives $aH = H$, and $a \in H$, by Lemma 2.80(i). The result follows from Exercise 2.56 on page 165, for $|G/H| = n$, and so $S_{G/H} \cong S_n$. •

When $H = \{1\}$, this is the Cayley theorem.

We are now going to classify all groups of order up to 7. By Example 2.88, every group of prime order p is isomorphic to $\mathbb{I}_p$, and so, up to isomorphism, there is just one group of order p. Of the possible orders through 7, four of them, 2, 3, 5, and 7, are primes, and so we need look only at orders 4 and 6.

Proposition 2.132. *Every group G of order 4 is isomorphic to either $\mathbb{I}_4$ or the four-group $\mathbf{V}$. Moreover, $\mathbb{I}_4$ and $\mathbf{V}$ are not isomorphic.*

Proof. By Lagrange's theorem, every element in G, other than 1, has order either 2 or 4. If there is an element of order 4, then G is cyclic. Otherwise, $x^2 = 1$ for all $x \in G$, so that Exercise 2.38 on page 143 shows that G is abelian.

If distinct elements x and y in G are chosen, neither being 1, then one quickly checks that $xy \notin \{1, x, y\}$; hence,

$$G = \{1, x, y, xy\}.$$

It is easy to see that the bijection $f: G \to \mathbf{V}$, defined by $f(1) = 1$, $f(x) = (1\ 2)(3\ 4)$, $f(y) = (1\ 3)(2\ 4)$, and $f(xy) = (1\ 4)(2\ 3)$, is an isomorphism, for the product of any two elements of order 2 here is the other element of order 2.

We have already seen, in Example 2.89, that $\mathbb{I}_4 \ncong \mathbf{V}$. •

Proposition 2.133. *If G is a group of order 6, then G is isomorphic to either $\mathbb{I}_6$ or S_3.*[20] *Moreover, $\mathbb{I}_6$ and S_3 are not isomorphic.*

Proof. By Lagrange's theorem, the only possible orders of nonidentity elements are 2, 3, and 6. Of course, $G \cong \mathbb{I}_6$ if G has an element of order 6. Now Exercise 2.40 on page 144 shows that G must contain an element of order 2, say, t. Let $T = \langle t \rangle$.

Since $[G : T] = 3$, the representation on the cosets of T is a homomorphism $\rho: G \to S_{G/T} \cong S_3$ with $\ker \rho \leq T$. Thus, $\ker \rho = \{1\}$ or $\ker \rho = T$. In the first case, ρ is an injection, and hence it is an isomorphism, for $|G| = 6 = |S_3|$. In the second case, $\ker \rho = T$, so that $T \lhd G$ and the quotient group G/T is defined. Now G/T is cyclic, for $|G/T| = 3$, so there is $a \in G$ with $G/T = \{T, aT, a^2T\}$. Moreover, ρ_t is the permutation

$$\rho_t = \begin{pmatrix} T & aT & a^2T \\ tT & taT & ta^2T \end{pmatrix}.$$

[20] Cayley states this proposition in an article he wrote in 1854. However, in 1878, in the *American Journal of Mathematics*, he wrote, "The general problem is to find all groups of a given order n; ... if $n = 6$, there are three groups; a group

$$1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5 \quad (\alpha^6 = 1),$$

and two more groups

$$1, \beta, \beta^2, \alpha, \alpha\beta, \alpha\beta^2 \qquad (\alpha^2 = 1, \beta^3 = 1),$$

viz., in the first of these $\alpha\beta = \beta\alpha$ while in the other of them, we have $\alpha\beta = \beta^2\alpha, \alpha\beta^2 = \beta\alpha$." Cayley's list is $\mathbb{I}_6$, $\mathbb{I}_2 \times \mathbb{I}_3$, and S_3. Of course, $\mathbb{I}_2 \times \mathbb{I}_3 \cong \mathbb{I}_6$. Even Homer nods.

Since $t \in T = \ker \rho$, we have ρ_t the identity. In particular, $aT = \rho_t(aT) = taT$, so that $a^{-1}ta \in T = \{1, t\}$, by Lemma 2.80(i). But $a^{-1}ta \neq 1$, so that $a^{-1}ta = t$; that is, $ta = at$. Now a has order 3 or order 6 (for $a \neq 1$ and $a^2 \neq 1$). In either case, G has an element of order 6: if a has order 3, then at has order 6, by Proposition 2.127 (alternatively, just note that $(at)^6 = 1$ and that $(at)^i \neq 1$ for $i < 6$). Therefore, G is cyclic of order 6, and $G \cong \mathbb{I}_6$.

It is clear that $\mathbb{I}_6$ and S_3 are not isomorphic, for one is abelian and the other is not. •

One consequence of this result is another proof that $\mathbb{I}_6 \cong \mathbb{I}_2 \times \mathbb{I}_3$ (see Theorem 2.126).

Classifying groups of order 8 is more difficult, for we have not yet developed enough theory (see my book, *Advanced Modern Algebra*, Theorem 5.83). It turns out that there are only 5 nonisomorphic groups of order 8: three are abelian: $\mathbb{I}_8$; $\mathbb{I}_4 \times \mathbb{I}_2$; $\mathbb{I}_2 \times \mathbb{I}_2 \times \mathbb{I}_2$; two are nonabelian: D_8; $\mathbf{Q}$.

Order of Group	Number of Groups
2	1
4	2
8	5
16	14
32	51
64	267
128	2, 328
256	56, 092
512	10, 494, 213
1024	49, 487, 365, 422

Table 2.4.

One can continue this discussion for larger orders, but things soon get out of hand, as Table 2.4 shows (the calculation of the numbers in the table is very sophisticated). The number of nonisomorphic groups having order ≤ 2000 was found by E. O'Brien, but focusing on the numbers in Table 2.4 is more dramatic. A. McIver and P. M. Neumann proved, for large n, that the number of nonisomorphic groups of order n is about $n^{\mu^2+\mu+2}$, where $\mu(n)$ is the largest exponent occurring in the prime factorization of n. Obviously, making a telephone directory of groups is not the way to study them.

Groups arose by abstracting the fundamental properties enjoyed by permutations. But there is an important feature of permutations that the axioms do not mention: permutations are functions. We shall see that there are interesting consequences when this feature is restored.

Let us agree on some notation before giving the next definition. A function of two variables, $\alpha\colon X \times Y \to Z$, can be regarded as a one-parameter family of functions of one variable: each $x \in X$ gives a function $\alpha_x\colon Y \to Z$, namely, $\alpha_x(y) = \alpha(x, y)$.

Definition. If X is a set and G is a group, then G ***acts*** on X[21] if there exists a function $\alpha\colon G \times X \to X$, called an ***action***, such that

(i) for $g, h \in G$, $\alpha_g \circ \alpha_h = \alpha_{gh}$;

(ii) $\alpha_1 = 1_X$, the identity function.

If G acts on X, we shall usually write gx instead of $\alpha_g(x)$. In this notation, axiom (i) reads $g(hx) = (gh)x$.

Of course, every subgroup $G \leq S_X$ acts on X. More generally, actions of a group G on a set X correspond to homomorphisms $G \to S_X$.

Proposition 2.134. *If $\alpha\colon G \times X \to X$ is an action of a group G on a set X, then $g \mapsto \alpha_g$ defines a homomorphism $G \to S_X$. Conversely, if $B\colon G \to S_X$ is a homomorphism, then $\beta\colon G \times X \to X$, defined by $\beta(g, x) = B(g)(x)$, is an action.*

Proof. If $\alpha\colon G \times X \to X$ is an action, then we claim that each α_g is a permutation of X. Indeed, its inverse is $\alpha_{g^{-1}}$, because $\alpha_g\alpha_{g^{-1}} = \alpha_{gg^{-1}} = \alpha_1 = 1_X$. It follows that $A\colon G \to S_X$, defined by $A(g) = \alpha_g$, is a function with the stated target. That A is a homomorphism follows from axiom (i):

$$A(gh) = \alpha_{gh} = \alpha_g \circ \alpha_h = A(g) \circ A(h).$$

Conversely, the function $\beta\colon G \times X \to X$, defined by a homomorphism $B\colon G \to S_X$ as $\beta(g, x) = B(g)(x)$, is an action. According to our notational agreement, $\beta_g = B(g)$. Thus, axiom (i) merely says that $B(g) \circ B(h) = B(gh)$, which is true because B is a homomorphism, while axiom (ii), $B(1) = 1_X$, holds because every homomorphism takes the identity to the identity. •

Cayley's theorem says that a group G acts on itself by (left) translation, and its generalization, the representation on cosets (Theorem 2.131), shows that G also acts on the family of cosets of a subgroup H by (left) translation.

Example 2.135.
We show that G ***acts on itself by conjugation***; that is, for each $g \in G$, define $\alpha_g\colon G \to G$ by

$$\alpha_g(x) = gxg^{-1}.$$

[21] If G acts on X, then one often calls X a G-***set***.

To verify axiom (i), note that for each $x \in G$,

$$\begin{aligned}(\alpha_g \circ \alpha_h)(x) &= \alpha_g(\alpha_h(x)) \\ &= \alpha_g(hxh^{-1}) \\ &= g(hxh^{-1})g^{-1} \\ &= (gh)x(gh)^{-1} \\ &= \alpha_{gh}(x).\end{aligned}$$

Therefore, $\alpha_g \circ \alpha_h = \alpha_{gh}$.

To prove axiom (ii), note that for each $x \in G$,

$$\alpha_1(x) = 1x1^{-1} = x,$$

and so $\alpha_1 = 1_G$. ◀

The following two definitions are fundamental.

Definition. If G acts on X and $x \in X$, then the ***orbit*** of x, denoted by $\mathcal{O}(x)$, is the subset of X:

$$\mathcal{O}(x) = \{gx : g \in G\} \subseteq X;$$

the ***stabilizer*** of x, denoted by G_x, is the subgroup of G:

$$G_x = \{g \in G : gx = x\} \leq G.$$

It is easy to check that the stabilizer G_x of a point x is a subgroup of G.

Let us find orbits and stabilizers in the examples above.

Example 2.136.

(i) Cayley's theorem says that G acts on itself by translations: $\tau_a : x \mapsto ax$. If $x \in G$, then the orbit $\mathcal{O}(x) = G$, for if $g \in G$, then $g = (gx^{-1})x$. The stabilizer G_x of x is $\{1\}$, for if $x = \tau_a(x) = ax$, then $a = 1$. One says that G acts ***transitively*** on X when there is some $x \in X$ with $\mathcal{O}(x) = X$.

(ii) When G acts on G/H (the family of cosets of a subgroup H) by translations $\tau_a : xH \mapsto axH$, then the orbit $\mathcal{O}(xH) = G/H$, for if $g \in G$ and $a = gx^{-1}$, then $\tau_a : xH \mapsto gH$. Thus, G acts transitively on G/H. The stabilizer G_{xH} of xH is xHx^{-1}, for $axH = xH$ if and only if $x^{-1}ax \in H$ if and only if $a \in xHx^{-1}$. ◀

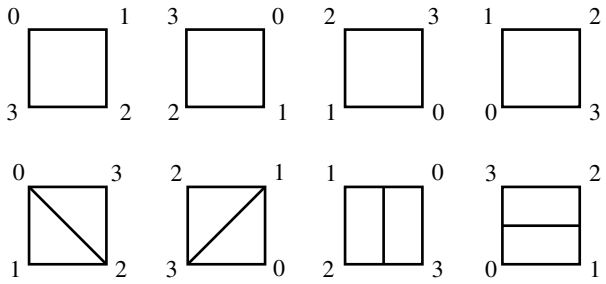

Figure 2.18 Dihedral Group D_8

Example 2.137.
Let $X =$ the vertices $\{v_0,\ v_1,\ v_2,\ v_3\}$ of a square, and let G be the dihedral group D_8 acting on X, as in Figure 2.18 (for clarity, the vertices in the figure are labeled 0, 1, 2, 3 instead of v_0, v_1, v_2, v_3).

$$G = \{\text{rotations} : (1),\ (v_0\ v_1\ v_2\ v_3),\ (v_0\ v_2)(v_1\ v_3),\ (v_0\ v_3\ v_2\ v_1);$$
$$\text{reflections} : (v_1\ v_3),\ (v_0\ v_2),\ (v_0\ v_1)(v_2\ v_3),\ (v_0\ v_3)(v_1\ v_2)\}.$$

For each vertex $v_i \in X$, there is some $g \in G$ with $gv_0 = v_i$; therefore, $\mathcal{O}(v_0) = X$ and D_8 acts transitively.

What is the stabilizer G_{v_0} of v_0? Aside from the identity, there is only one $g \in D_8$ fixing v_0, namely, $g = (v_1\ v_3)$; therefore G_{v_0} is a subgroup of order 2. (This example can be generalized to the dihedral group D_{2n} acting on a regular n-gon.) ◀

Example 2.138.
Let a group G act on itself by conjugation. If $x \in G$, then

$$\mathcal{O}(x) = \{y \in G : y = axa^{-1} \text{ for some } a \in G\};$$

$\mathcal{O}(x)$ is called the ***conjugacy class*** of x, and it is often denoted by x^G. For example, Proposition 2.33 shows that if $\alpha \in S_n$, then the conjugacy class of α consists of all the permutations in S_n having the same cycle structure as α.

If $x \in G$, then the stabilizer G_x of x is

$$C_G(x) = \{g \in G : gxg^{-1} = x\}.$$

This subgroup of G, consisting of all $g \in G$ that commute with x, is called the ***centralizer*** of x in G. ◀

Example 2.139.
Let $X = \{1, 2, \ldots, n\}$, let $\sigma \in S_n$, and regard the cyclic group $G = \langle \sigma \rangle$ as acting on X. If $i \in X$, then

$$\mathcal{O}(i) = \{\sigma^k(i) : k \in \mathbb{Z}\}.$$

Let $\sigma = \beta_1 \cdots \beta_{t(\sigma)}$ be the complete factorization of σ, and let $i = i_0$ be moved by σ. If the cycle involving i_0 is $\beta_j = (i_0\ i_1\ \ldots\ i_{r-1})$, then the proof of Theorem 2.26 shows that $i_k = \sigma^k(i_0)$ for all $k < r - 1$. Therefore,

$$\mathcal{O}(i) = \{i_0, i_1, \ldots, i_{r-1}\},$$

where $i = i_0$. It follows that $|\mathcal{O}(i)| = r$. The stabilizer G_ℓ of a symbol ℓ is G if σ fixes ℓ, and it is a proper subgroup of G if σ moves ℓ. ◀

A group G acting on a set X gives an equivalence relation on X. Define

$$x \equiv y \text{ if there exists } g \in G \text{ with } y = gx.$$

If $x \in X$, then $1x = x$, where $1 \in G$, and so $x \equiv x$; hence, $\equiv$ is reflexive. If $x \equiv y$, so that $y = gx$, then

$$g^{-1}y = g^{-1}(gx) = (g^{-1}g)x = 1x = x,$$

so that $x = g^{-1}y$ and $y \equiv x$; hence, $\equiv$ is symmetric. If $x \equiv y$ and $y \equiv z$, there are $g, h \in G$ with $y = gx$ and $z = hy$, so that $z = hy = h(gx) = (hg)x$, and $x \equiv z$. Therefore, $\equiv$ is transitive, and hence it is an equivalence relation. Now the equivalence class of $x \in X$ is its orbit, for

$$[x] = \{y \in X : y \equiv x\} = \{gx : g \in G\} = \mathcal{O}(x).$$

Proposition 2.140. *If G acts on a set X, then X is the disjoint union of the orbits. If X is finite, then*

$$|X| = \sum_i |\mathcal{O}(x_i)|,$$

where one x_i is chosen from each orbit.

Proof. This follows from Proposition 2.20, for the orbits form a partition of X.

The count given in the second statement is correct: since the orbits are disjoint, no element in X is counted twice. •

Here is the connection between orbits and stabilizers.

Theorem 2.141. *If G acts on a set X and $x \in X$, then*

$$|\mathcal{O}(x)| = [G : G_x]$$

the index of the stabilizer G_x in G.

Proof. Let G/G_x denote the family of all the cosets of G_x in G. We will exhibit a bijection $\varphi\colon \mathcal{O}(x) \to G/G_x$; this will give the result, since $|G/G_x| = [G : G_x]$, by Corollary 2.82 of Lagrange's theorem. If $y \in \mathcal{O}(x)$, then $y = gx$ for some $g \in G$; define $\varphi(y) = gG_x$. Now φ is well-defined: if $y = hx$ for some $h \in G$, then $h^{-1}gx = x$ and $h^{-1}g \in G_x$; hence $hG_x = gG_x$. To see that φ is injective, suppose that $\varphi(y) = \varphi(z)$; then there are $g, h \in G$ with $y = gx$, $z = hx$, and $gG_x = hG_x$; that is, $h^{-1}g \in G_x$. It follows that $h^{-1}gx = x$, and so $y = gx = hx = z$. Finally, φ is a surjection: if $gG_x \in G/G_x$, then let $y = gx \in \mathcal{O}(x)$, and note that $\varphi(y) = gG_x$. •

In Example 2.137, D_8 acting on the four corners of a square, we saw that $|\mathcal{O}(v_0)| = 4$, $|G_{v_0}| = 2$, and $[G : G_{v_0}] = 8/2 = 4$. In Example 2.139, $G = \langle\sigma\rangle \leq S_n$ acting on $X = \{1, 2, \ldots, n\}$, we saw that if, in the complete factorization of σ into disjoint cycles $\sigma = \beta_1 \cdots \beta_{t(\sigma)}$, the r-cycle β_j moves ℓ, then $r = |\mathcal{O}(\ell)|$ for any ℓ occurring in β_j. Theorem 2.141 says that r is a divisor of the order k of σ. (But Theorem 2.54 tells us more: k is the lcm of the lengths of the cycles occurring in the factorization.)

Corollary 2.142. *If a finite group G acts on a set X, then the number of elements in any orbit is a divisor of $|G|$.*

Proof. This follows at once from Theorem 2.141 and Lagrange's theorem. •

Corollary 2.143. *If x lies in a finite group G, then the number of conjugates of x is the index of its centralizer*:

$$|x^G| = [G : C_G(x)],$$

and hence it is a divisor of $|G|$.

Proof. As in Example 2.138, the orbit of x is its conjugacy class x^G, and the stabilizer G_x is the centralizer $C_G(x)$. •

In Example 2.29, there is a table displaying the number of permutations in S_4 of each cycle structure; these numbers are 1, 6, 8, 6, 3. Note that each of these numbers is a divisor of $|S_4| = 24$. In Example 2.30, we saw that the corresponding numbers in S_5 are 1, 10, 20, 30, 24, 20, and 15, and these are all divisors of $|S_5| = 120$. We now recognize these subsets as being conjugacy classes, and the next corollary explains why these numbers divide the group order.

Corollary 2.144. *If $\alpha \in S_n$, then the number of permutations in S_n having the same cycle structure as α is a divisor of $n!$.*

Proof. This follows at once from Corollary 2.143 once one recalls Proposition 2.33 which says that two permutations in S_n are conjugate in S_n if and only if they have the same cycle structure. •

When we began classifying groups of order 6, it would have been helpful to be able to assert that any such group has an element of order 3 (we were able to use an earlier exercise to assert the existence of an element of order 2). We now prove that every finite group G contains an element of prime order p for every $p \mid |G|$.

If the conjugacy class x^G of an element x in a group G consists of x alone, then x commutes with every $g \in G$, for $gxg^{-1} = x$; that is, $x \in Z(G)$. Conversely, if $x \in Z(G)$, then $x^G = \{x\}$. Thus, the center $Z(G)$ consists of all those elements in G whose conjugacy class has exactly one element.

Theorem 2.145 (*Cauchy*). *If G is a finite group whose order is divisible by a prime p, then G contains an element of order p.*

Proof. We prove the theorem by induction on $|G|$; the base step $|G| = 1$ is vacuously true, for there are no prime divisors of 1. If $x \in G$, then the number of conjugates of x is $|x^G| = [G : C_G(x)]$, where $C_G(x)$ is the centralizer of x in G. As noted above, if $x \notin Z(G)$, then x^G has more than one element, and so $|C_G(x)| < |G|$. If $p \mid |C_G(x)|$ for some noncentral x, then the inductive hypothesis says there is an element of order p in $C_G(x) \leq G$, and we are done. Therefore, we may assume that $p \nmid |C_G(x)|$ for all noncentral $x \in G$. Better, since $|G| = [G : C_G(x)]|C_G(x)|$, Euclid's lemma gives

$$p \mid [G : C_G(x)].$$

After recalling that $Z(G)$ consists of all those elements $x \in G$ with $|x^G| = 1$, we may use Proposition 2.140 to see

$$|G| = |Z(G)| + \sum_i [G : C_G(x_i)],$$

where one x_i is selected from each conjugacy class having more than one element. Since $|G|$ and all $[G : C_G(x_i)]$ are divisible by p, it follows that $|Z(G)|$ is divisible by p. But $Z(G)$ is abelian, and so Proposition 2.122 says that $Z(G)$, and hence G, contains an element of order p. •

Definition. The ***class equation*** of a finite group G is

$$|G| = |Z(G)| + \sum_i [G : C_G(x_i)],$$

where one x_i is selected from each conjugacy class having more than one element.

Definition. If p is a prime, then a ***p-group*** is a group of order p^n for some $n \geq 0$.

There are groups whose center is trivial; for example, $Z(S_3) = \{1\}$. For p-groups with more than one element, however, this is never true.

Theorem 2.146. *If p is a prime and G is a p-group with more than one element, then $Z(G) \neq \{1\}$.*

Proof. Consider the class equation

$$|G| = |Z(G)| + \sum_i [G : C_G(x_i)].$$

Each $C_G(x_i)$ is a proper subgroup of G, for $x_i \notin Z(G)$. Since G is a p-group, $[G : C_G(x_i)]$ is a divisor of $|G|$, hence is itself a power of p. Thus, p divides each of the terms in the class equation other than $|Z(G)|$, and so $p \mid |Z(G)|$ as well. Therefore, $Z(G) \neq \{1\}$. •

Corollary 2.147. *If p is a prime, then every group G of order p^2 is abelian.*

Proof. If G is not abelian, then its center $Z(G)$ is a proper subgroup, so that $|Z(G)| = 1$ or p, by Lagrange's theorem. But Theorem 2.146 says that $Z(G) \neq \{1\}$, and so $|Z(G)| = p$. The center is always a normal subgroup, so that the quotient $G/Z(G)$ is defined; it has order p, and hence $G/Z(G)$ is cyclic. This contradicts Exercise 2.87 on page 187. •

Example 2.148.
For every prime p, there exist nonabelian groups of order p^3. Define $\mathrm{UT}(3, p)$ to be the subgroup of $\mathrm{GL}(3, \mathbb{I}_p)$ consisting of all upper triangular matrices having 1's on the diagonal; that is,

$$\mathrm{UT}(3, p) = \left\{ A = \begin{bmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{bmatrix} : a, b, c \in \mathbb{I}_p \right\}.$$

It is easy to see that $\mathrm{UT}(3, p)$ is a subgroup of $\mathrm{GL}(3, \mathbb{I}_p)$, and it has order p^3 because there are p choices for each of a, b, c. The reader will have no difficulty finding two matrices in $\mathrm{UT}(3, p)$ that do not commute. (Exercise 2.111 on page 204 says that $\mathrm{UT}(3, 2) \cong D_8$) ◀

Example 2.149.
Who would have guessed that Cauchy's theorem and Fermat's theorem are special cases of some common theorem?[22] The elementary yet ingenious proof of this is due to J. H. McKay (as A. Mann has shown me). If G is a finite group and p is a prime, denote the cartesian product of p copies of G by G^p, and define

$$X = \{(a_1, a_2, \ldots, a_p) \in G^p : a_1 a_2 \ldots a_p = 1\}.$$

Note that $|X| = |G|^{p-1}$, for having chosen the first $p-1$ entries arbitrarily, the pth entry must equal $(a_1 a_2 \cdots a_{p-1})^{-1}$. Now make X into an $\mathbb{I}_p$-set by defining, for $0 \le i \le p-1$,

$$[i](a_1, a_2, \ldots, a_p) = (a_{i+1}, a_{i+2}, \ldots, a_p, a_1, a_2, \ldots, a_i).$$

The product of the entries in the new p-tuple is a conjugate of $a_1 a_2 \cdots a_p$:

$$a_{i+1} a_{i+2} \cdots a_p a_1 a_2 \cdots a_i = (a_1 a_2 \cdots a_i)^{-1} (a_1 a_2 \cdots a_p)(a_1 a_2 \cdots a_i).$$

This conjugate is 1 (for $g^{-1} 1 g = 1$), and so $[i](a_1, a_2, \ldots, a_p) \in X$. By Corollary 2.142, the size of every orbit of X is a divisor of $|\mathbb{I}_p| = p$; since p is prime, these sizes are either 1 or p. Now orbits with just one element consist of a p-tuple all of whose entries a_i are equal, for all cyclic permutations of the p-tuple are the same. In other words, such an orbit corresponds to an element $a \in G$ with $a^p = 1$. Clearly, $(1, 1, \ldots, 1)$ is such an orbit; if it were the only such, then we would have

$$|G|^{p-1} = |X| = 1 + kp$$

for some $k \ge 0$; that is, $|G|^{p-1} \equiv 1 \bmod p$. If p is a divisor of $|G|$, then we have a contradiction, for $|G|^{p-1} \equiv 0 \bmod p$. We have thus proved Cauchy's theorem: if a prime p is a divisor of $|G|$, then G has an element of order p.

Suppose now that G is a group of order n and that p is not a divisor of n; for example, let $G = \mathbb{I}_n$. By Lagrange's theorem, G has no elements of order p, so that if $a \in G$ and $a^p = 1$, then $a = 1$. Therefore, the only orbit in G^p of size 1 is $(1, 1, \ldots, 1)$, and so

$$n^{p-1} = |G|^{p-1} = |X| = 1 + kp;$$

that is, if p is not a divisor of n, then $n^{p-1} \equiv 1 \bmod p$. Multiplying both sides by n, we have $n^p \equiv n \bmod p$. This congruence also holds when p is a divisor of n, and this is Fermat's theorem. ◀

We have seen, in Proposition 2.97, that A_4 is a group of order 12 having no subgroup of order 6. Thus, the assertion that if d is a divisor of $|G|$, then G must have a subgroup of order d, is false. However, this assertion is true when G is a p-group. Indeed, more is true; G must have a normal subgroup of order d.

[22] If G is a group of order n and p is a prime, then the number of solutions $x \in G$ of the equation $x^p = 1$ is congruent to $n^{p-1} \bmod p$.

Proposition 2.150. *If G is a group of order $|G| = p^e$, then G has a normal subgroup of order p^k for every $k \leq e$.*

Proof. We prove the result by induction on $e \geq 0$. The base step is obviously true, and so we proceed to the inductive step. By Theorem 2.146, the center of G is nontrivial: $Z(G) \neq \{1\}$. If $Z(G) = G$, then G is abelian, and we have already proved the result in Proposition 2.122. Therefore, we may assume that $Z(G)$ is a proper subgroup of G. Since $Z(G) \lhd G$, we have $G/Z(G)$ a p-group of order strictly smaller than $|G|$. Assume that $|Z(G)| = p^c$. If $k \leq c$, then $Z(G)$ and, hence G, contains a normal subgroup of order p^k, because $Z(G)$ is abelian. If $k > c$, then $G/Z(G)$ contains a normal subgroup S^* of order p^{k-c}, by induction. The correspondence theorem gives a normal subgroup S of G with

$$Z(G) \leq S \leq G$$

such that $S/Z(G) \cong S^*$. By Corollary 2.82 to Lagrange's theorem,

$$|S| = |S^*||Z(G)| = p^{k-c} \cdot p^c = p^k. \quad \bullet$$

Abelian groups (and the quaternions) have the property that every subgroup is normal. At the opposite pole are groups having no normal subgroups other than the two obvious ones: $\{1\}$ and G.

Definition. A group G is called ***simple*** if $G \neq \{1\}$ and G has no normal subgroups other than $\{1\}$ and G itself.

Proposition 2.151. *An abelian group G is simple if and only if it is finite and of prime order.*

Proof. If G is finite of prime order p, then G has no subgroups H other than $\{1\}$ and G, otherwise Lagrange's theorem would show that $|H|$ is a divisor of p. Therefore, G is simple.

Conversely, assume that G is simple. Since G is abelian, every subgroup is normal, and so G has no subgroups other than $\{1\}$ and G. Choose $x \in G$ with $x \neq 1$. Since $\langle x \rangle$ is a subgroup, we have $\langle x \rangle = G$. If x has infinite order, then all the powers of x are distinct, and so $\langle x^2 \rangle < \langle x \rangle$ is a forbidden subgroup of $\langle x \rangle$, a contradiction. Therefore, every $x \in G$ has finite order, say, m. If m is composite, then $m = k\ell$ and $\langle x^k \rangle$ is a proper nontrivial subgroup of $\langle x \rangle$, a contradiction. Therefore, $G = \langle x \rangle$ has prime order. $\bullet$

We are now going to show that A_5 is a nonabelian simple group (indeed, it is the smallest such; there is no nonabelian simple group of order less than 60).

Suppose that an element $x \in G$ has k conjugates; that is

$$|x^G| = |\{gxg^{-1} : g \in G\}| = k.$$

If there is a subgroup $H \leq G$ with $x \in H \leq G$, how many conjugates does x have in H? Since

$$x^H = \{hxh^{-1} : h \in H\} \subseteq \{gxg^{-1} : g \in G\} = x^G,$$

we have $|x^H| \leq |x^G|$. It is possible that there is strict inequality $|x^H| < |x^G|$. For example, take $G = S_3$, $x = (1\ 2)$, and $H = \langle x \rangle$. We know that $|x^G| = 3$ (because all transpositions are conjugate), whereas $|x^H| = 1$ (because H is abelian).

Now let us consider this question, in particular, for $G = S_5$, $x = (1\ 2\ 3)$, and $H = A_5$.

Lemma 2.152. *All* 3*-cycles are conjugate in* A_5.

Proof. Let $G = S_5$, $\alpha = (1\ 2\ 3)$, and $H = A_5$. We know that $|\alpha^{S_5}| = 20$, for there are 20 3-cycles in S_5 (as we saw in Example 2.30). Therefore, $20 = |S_5|/|C_{S_5}(\alpha)| = 120/|C_{S_5}(\alpha)|$, by Corollary 2.143, so that $|C_{S_5}(\alpha)| = 6$; that is, there are exactly six permutations in S_5 that commute with α. Here they are:

$$(1),\ (1\ 2\ 3),\ (1\ 3\ 2),\ (4\ 5),\ (4\ 5)(1\ 2\ 3),\ (4\ 5)(1\ 3\ 2).$$

The last three of these are odd permutations, so that $|C_{A_5}(\alpha)| = 3$. We conclude that

$$|\alpha^{A_5}| = |A_5|/|C_{A_5}(\alpha)| = 60/3 = 20;$$

that is, all 3-cycles are conjugate to $\alpha = (1\ 2\ 3)$ in A_5. •

This lemma, which says that A_5 is generated by the 3-cycles, can be generalized from A_5 to A_n for all $n \geq 5$; see Exercise 2.116 on page 205.

Lemma 2.153. *Every element in* A_5 *is a* 3*-cycle or a product of* 3*-cycles.*

Proof. If $\alpha \in A_5$, then α is a product of an even number of transpositions: $\alpha = \tau_1\tau_2 \cdots \tau_{2n-1}\tau_{2n}$. As the transpositions may be grouped in pairs $\tau_{2i-1}\tau_{2i}$, it suffices to consider products $\tau\tau'$, where τ and τ' are transpositions. If τ and τ' are not disjoint, then $\tau = (i\ j)$, $\tau' = (i\ k)$, and $\tau\tau' = (i\ k\ j)$; if τ and τ' are disjoint, then $\tau\tau' = (i\ j)(k\ \ell) = (i\ j)(j\ k)(j\ k)(k\ \ell) = (i\ j\ k)(j\ k\ \ell)$. •

Theorem 2.154. A_5 *is a simple group.*

Proof. We shall show that if H is a normal subgroup of A_5 and $H \neq \{(1)\}$, then $H = A_5$. Now if H contains a 3-cycle, then normality forces H to contain all its conjugates. By Lemma 2.152, H contains every 3-cycle, and by Lemma 2.153, $H = A_5$. Therefore, it suffices to prove that H contains a 3-cycle.

As $H \neq \{(1)\}$, it contains some $\sigma \neq (1)$. We may assume, after a harmless relabeling, that either $\sigma = (1\ 2\ 3)$, $\sigma = (1\ 2)(3\ 4)$, or $\sigma = (1\ 2\ 3\ 4\ 5)$. As we have just remarked, we are done if σ is a 3-cycle.

If $\sigma = (1\ 2)(3\ 4) \in H$, use Proposition 2.32: conjugate σ by $\beta = (3\ 4\ 5)$ to have $\beta\sigma\beta^{-1} = \sigma' = (1\ 2)(4\ 5) \in H$ (because $\beta \in A_5$ and $H \lhd S_5$). Hence, $\sigma\sigma' = (3\ 4\ 5) \in H$.

If $\sigma = (1\ 2\ 3\ 4\ 5) \in H$, use Proposition 2.32: conjugate σ by $\gamma = (1\ 2\ 3)$ to have $\gamma\sigma\gamma^{-1} = \sigma'' = (2\ 3\ 1\ 4\ 5) \in H$ (because $\gamma \in A_5$ and $H \lhd S_5$). Hence, $\sigma''\sigma^{-1} = (2\ 3\ 1\ 4\ 5)(5\ 4\ 3\ 2\ 1) = (1\ 2\ 4) \in H$. We should say how this last equation arose. If $\sigma \in H$ and γ is a 3-cycle, then $\gamma\sigma\gamma^{-1} \in H$, and so $(\gamma\sigma\gamma^{-1})\sigma^{-1} \in H$. Reassociating, $\gamma(\sigma\gamma^{-1}\sigma^{-1}) \in H$. But $\sigma\gamma^{-1}\sigma^{-1}$ is a 3-cycle, so that H contains a product of two 3-cycles. We have chosen γ more carefully to force this product of two 3-cycles to be a 3-cycle.

We have shown, in all cases, that H contains a 3-cycle. Therefore, the only normal subgroups in A_5 are $\{(1)\}$ and A_5 itself, and so A_5 is simple. •

As we shall see in Chapter 5, Theorem 2.154 turns out to be the basic reason why the quadratic formula has no generalization giving the roots of polynomials of degree 5 or higher.

Without much more effort, we can prove that the alternating groups A_n are simple for all $n \geq 5$. Observe that A_4 is not simple, for the four-group $\mathbf{V}$ is a normal subgroup of A_4.

Lemma 2.155. *A_6 is a simple group.*

Proof. Let $H \neq \{(1)\}$ be a normal subgroup of A_6; we must show that $H = A_6$. Assume that there is some $\alpha \in H$ with $\alpha \neq (1)$ which fixes some i, where $1 \leq i \leq 6$. Define

$$F = \{\sigma \in A_6 : \sigma(i) = i\}.$$

Now $\alpha \in H \cap F$, so that $H \cap F \neq \{(1)\}$. The second isomorphism theorem gives $H \cap F \lhd F$. But F is simple, for $F \cong A_5$, by Exercise 2.118 on page 205, and so the only normal subgroups in F are $\{(1)\}$ and F. Since $H \cap F \neq \{(1)\}$, we have $H \cap F = F$; that is, $F \leq H$. It follows that H contains a 3-cycle, and so $H = A_6$, by Exercise 2.116 on page 205.

We may now assume that there is no $\alpha \in H$ with $\alpha \neq (1)$ which fixes some i with $1 \leq i \leq 6$. If one considers the cycle structures of permutations in A_6, however, any such α must have cycle structure $(1\ 2)(3\ 4\ 5\ 6)$ or $(1\ 2\ 3)(4\ 5\ 6)$. In the first case, $\alpha^2 \in H$ is a nontrivial permutation which fixes 1 (and also 2), a contradiction. In the second case, H contains $\alpha(\beta\alpha^{-1}\beta^{-1})$, where $\beta = (2\ 3\ 4)$, and it is easily checked that this is a nontrivial element in H which fixes 6, another contradiction. Therefore, no such normal subgroup H can exist, and so A_6 is a simple group. •

Theorem 2.156. *A_n is a simple group for all $n \geq 5$.*

Proof. If H is a nontrivial normal subgroup of A_n [that is, $H \neq (1)$], then we must show that $H = A_n$; by Exercise 2.116 on page 205, it suffices to prove that H contains a 3-cycle. If $\beta \in H$ is nontrivial, then there exists some i that β moves; say, $\beta(i) = j \neq i$. Choose a 3-cycle α which fixes i and moves j. The permutations α and β do not commute: $\beta\alpha(i) = \beta(i) = j$, while $\alpha\beta(i) = \alpha(j) \neq j$. It follows that $\gamma = (\alpha\beta\alpha^{-1})\beta^{-1}$ is a nontrivial element of H. But $\beta\alpha^{-1}\beta^{-1}$ is a 3-cycle, by Proposition 2.32, and so $\gamma = \alpha(\beta\alpha^{-1}\beta^{-1})$ is a product of two 3-cycles. Hence, γ moves at most 6 symbols, say, $i_1, \ldots, i_6$ (if γ moves fewer than 6 symbols, just adjoin others so we have a list of 6). Define

$$F = \{\sigma \in A_n : \sigma \text{ fixes all } i \neq i_1, \ldots, i_6\}.$$

Now $F \cong A_6$, by Exercise 2.118 on page 205, and $\gamma \in H \cap F$. Hence, $H \cap F$ is a nontrivial normal subgroup of F. But F is simple, being isomorphic to A_6, and so $H \cap F = F$; that is, $F \leq H$. Therefore, H contains a 3-cycle, and so $H = A_n$; the proof is complete. •

EXERCISES

2.102 If a and b are elements in a group G, prove that ab and ba have the same order.

2.103 Prove that every translation $\tau_a \in S_G$, where $\tau_a : g \mapsto ag$, is a regular permutation (see Exercise 2.26 on page 121). The homomorphism $\varphi : G \to S_G$, defined by $\varphi(a) = \tau_a$, is often called the ***regular representation*** of G.

2.104 Prove that no pair of the following groups of order 8,

$$\mathbb{I}_8; \quad \mathbb{I}_4 \times \mathbb{I}_2; \quad \mathbb{I}_2 \times \mathbb{I}_2 \times \mathbb{I}_2; \quad D_8; \quad \mathbf{Q},$$

are isomorphic.

***2.105** If p is a prime and G is a finite group in which every element has order a power of p, prove that G is a p-group.

***2.106** Prove that a finite p-group G is simple if and only if $|G| = p$.

***2.107** Show that S_4 has a subgroup isomorphic to D_8.

***2.108** Prove that $S_4/\mathbf{V} \cong S_3$.

2.109 **(i)** Prove that $A_4 \ncong D_{12}$.

(ii) Prove that $D_{12} \cong S_3 \times \mathbb{I}_2$.

***2.110** **(i)** If H is a subgroup of G and if $x \in H$, prove that

$$C_H(x) = H \cap C_G(x).$$

(ii) If H is a subgroup of index 2 in a finite group G and if $x \in H$, prove that either $|x^H| = |x^G|$ or $|x^H| = \frac{1}{2}|x^G|$, where x^H is the conjugacy class of x in H.

***2.111** Prove that the group UT(3, 2) in Example 2.148 is isomorphic to D_8.

2.112 **(i)** How many permutations in S_5 commute with (1 2)(3 4), and how many *even* permutations in S_5 commute with (1 2)(3 4).

(ii) How many permutations in S_7 commute with (1 2)(3 4 5)?

(iii) Exhibit all the permutations in S_7 commuting with (1 2)(3 4 5).

***2.113** **(i)** Show that there are two conjugacy classes of 5-cycles in A_5, each of which has 12 elements.

(ii) Prove that the conjugacy classes in A_5 have sizes 1, 12, 12, 15, and 20.

2.114 **(i)** Prove that every normal subgroup H of a group G is a union of conjugacy classes of G, one of which is $\{1\}$.

(ii) Use part (i) and Exercise 2.113 to give a second proof of the simplicity of A_5.

***2.115** If $\sigma, \tau \in S_5$, where σ is a 5-cycle and τ is a transposition, prove that $\langle \sigma, \tau \rangle = S_5$.

***2.116** **(i)** For all $n \geq 3$, prove that every $\alpha \in A_n$ is a product of 3- cycles.

(ii) Prove that if a normal subgroup $H \lhd A_n$ contains a 3-cycle, where $n \geq 5$, then $H = A_n$. (*Remark.* See Lemmas 2.153 and 2.153.)

2.117 Prove that the only normal subgroups of S_4 are $\{(1)\}$, $\mathbf{V}$, A_4, and S_4.

***2.118** Let $\{i_1, \ldots, i_r\} \subseteq \{1, 2, \ldots n\}$, and let

$$F = \{\sigma \in A_n : \sigma \text{ fixes all } i \text{ with } i \neq i_1, \ldots, i_r\}.$$

Prove that $F \cong A_r$.

2.119 Prove that A_5 is a group of order 60 that has no subgroup of order 30.

2.120 Let $X = \{1, 2, 3, \ldots\}$ be the set of all positive integers, and let S_X be the symmetric group on X.

(i) Prove that $F_\infty = \{\sigma \in S_X : \sigma \text{ moves only finitely many } n \in X\}$ is a subgroup of S_X.

(ii) Define A_∞ to be the subgroup of F_∞ generated by the 3-cycles. Prove that A_∞ is an infinite simple group.

2.121 **(i)** Prove that if a simple group G has a subgroup of index n, then G is isomorphic to a subgroup of S_n.

(ii) Prove that an infinite simple group has no subgroups of finite index $n > 1$.

***2.122** Let G be a group with $|G| = mp$, where p is a prime and $1 < m < p$. Prove that G is not simple.

Remark. . Of all the numbers smaller than 60, we can now show that all but 11 are not orders of nonabelian simple groups (namely, 12, 18, 24, 30, 36, 40, 45, 48, 50, 54, 56). Theorem 2.146 eliminates all prime powers (for the center is always a normal subgroup), and Exercise 2.122 eliminates all numbers of the form mp, where p is a prime and $m < p$. (We will complete the proof that there are no nonabelian simple groups of order less than 60 in Theorem 6.25.) ◀

***2.123** If $n \geq 3$, prove that A_n is the only subgroup of S_n of order $\frac{1}{2}n!$.

***2.124** Prove that A_6 has no subgroups of prime index.

2.8 COUNTING WITH GROUPS

We are now going to use group theory to do some fancy counting.

Lemma 2.157.

(i) *Let a group G act on a set X. If $x \in X$ and $\sigma \in G$, then $G_{\sigma x} = \sigma G_x \sigma^{-1}$.*

(ii) *If a finite group G acts on a finite set X and if x and y lie in the same orbit, then $|G_y| = |G_x|$.*

Proof.
(i) If $\tau \in G_x$, then $\tau x = x$. If $\sigma x = y$, we have

$$\sigma\tau\sigma^{-1}y = \sigma\tau\sigma^{-1}\sigma x = \sigma\tau x = \sigma x = y.$$

Therefore, $\sigma\tau\sigma^{-1}$ fixes y, and so $\sigma G_x \sigma^{-1} \leq G_y$. The reverse inclusion is proved in the same way, for $x = \sigma^{-1}y$.
(ii) If x and y are in the same orbit, then there is $\sigma \in G$ with $y = \sigma x$, and so $|G_y| = |G_{\sigma x}| = |\sigma G_x \sigma^{-1}| = |G_x|$. •

Theorem 2.158 (Burnside's Lemma).[23] *Let G act on a finite set X. If N is the number of orbits, then*

$$N = \frac{1}{|G|}\sum_{\tau\in G} F(\tau),$$

where $F(\tau)$ is the number of $x \in X$ fixed by τ.

Proof. List the elements of X as follows: choose $x_1 \in X$, and then list all the elements in the orbit $\mathcal{O}(x_1)$; say, $\mathcal{O}(x_1) = \{x_1, x_2, \ldots, x_r\}$; then choose $x_{r+1} \notin \mathcal{O}(x_1)$, and list the elements of $\mathcal{O}(x_{r+1})$ as $x_{r+1}, x_{r+2}, \ldots$; continue this procedure until all the elements of X are listed. Now list the elements $\tau_1, \tau_2, \ldots, \tau_n$ of G, and form the following array of 0's and 1's, where

$$f_{i,j} = \begin{cases} 1 & \text{if } \tau_i \text{ fixes } x_j \\ 0 & \text{if } \tau_i \text{ moves } x_j. \end{cases}$$

Now $F(\tau_i)$, the number of x fixed by τ_i, is the number of 1's in the ith row of the array; therefore, $\sum_{\tau\in G} F(\tau)$ is the total number of 1's in the array. Let us now look at the columns. The number of 1's in the first column is the number of τ_i that fix x_1; by definition, these τ_i comprise G_{x_1}. Thus, the number of

[23] Burnside's influential book, *The Theory of Groups of Finite Order*, had two editions. In the first edition, he attributed this theorem to G. Frobenius; in the second edition, he gave no attribution at all. However, the commonly accepted name of this theorem is *Burnside's lemma*. To avoid the confusion that would be caused by changing a popular name, P. M. Neumann suggested that it be called "not-Burnside's lemma." Burnside was a fine mathematician, and there do exist theorems properly attributed to him. For example, Burnside proved that if p and q are primes, then there are no simple groups of order $p^m q^n$.

	x_1	$\cdots$	x_r	x_{r+1}	$\cdots$	x_j	$\cdots$
τ_1	$f_{1,1}$	$\cdots$	$f_{1,r}$	$f_{1,r+1}$	$\cdots$	$f_{1,j}$	$\cdots$
τ_2	$f_{2,1}$	$\cdots$	$f_{2,r}$	$f_{2,r+1}$	$\cdots$	$f_{2,j}$	$\cdots$
τ_i	$f_{i,1}$	$\cdots$	$f_{i,r}$	$f_{i,r+1}$	$\cdots$	$f_{i,j}$	$\cdots$
τ_n	$f_{n,1}$	$\cdots$	$f_{n,r}$	$f_{n,r+1}$	$\cdots$	$f_{n,j}$	$\cdots$

1's in column 1 is $|G_{x_1}|$. Similarly, the number of 1's in column 2 is $|G_{x_2}|$. By Lemma 2.157(ii), $|G_{x_1}| = |G_{x_2}|$. By Theorem 2.141, the number of 1's in the r columns labeled by the $x_i \in \mathcal{O}(x_1)$ is thus

$$r|G_{x_1}| = |\mathcal{O}(x_1)| \cdot |G_{x_1}| = \big(|G|/|G_{x_1}|\big)\,|G_{x_1}| = |G|.$$

The same is true for any other orbit: its columns contain exactly $|G|$ 1's. Therefore, if there are N orbits, there are $N|G|$ 1's in the array. We conclude that

$$\sum_{\tau \in G} F(\tau) = N|G|. \quad \bullet$$

We are going to use Burnside's lemma to solve problems of the following sort. How many striped flags are there having six stripes (of equal width) each of which can be colored red, white, or blue? Clearly, the two flags in Figure 2.19 are the same: the bottom flag is just the reverse of the top one (the flag may be viewed by standing in front of it or by standing in back of it).

r	*w*	*b*	*r*	*w*	*b*

b	*w*	*r*	*b*	*w*	*r*

Figure 2.19 A Flag

Let X be the set of all 6-tuples of colors; if $x \in X$, then

$$x = (c_1, c_2, c_3, c_4, c_5, c_6),$$

where each c_i denotes either red, white, or blue. Let τ be the permutation that reverses all the indices:

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix} = (1\ 6)(2\ 5)(3\ 4)$$

(thus, τ "turns over" each 6-tuple x of colored stripes). The cyclic group $G = \langle \tau \rangle$ acts on X; since $|G| = 2$, the orbit of any 6-tuple x consists of either 1 or 2 elements: either τ fixes x or it does not. Since a flag is unchanged by turning it over, it is reasonable to identify a flag with an orbit of a 6-tuple. For example, the orbit consisting of the 6-tuples

$$(r, w, b, r, w, b) \quad \text{and} \quad (b, w, r, b, w, r)$$

describes the flag in Figure 2.19. The number of flags is thus the number N of orbits; by Burnside's lemma, $N = \frac{1}{2}[F((1)) + F(\tau)]$. The identity permutation (1) fixes every $x \in X$, and so $F((1)) = 3^6$ (there are 3 colors). Now τ fixes a 6-tuple x if and only if x is a "palindrome," that is, if the colors in x read the same forward as backward. For example,

$$x = (r, r, w, w, r, r)$$

is fixed by τ. Conversely, if

$$x = (c_1, c_2, c_3, c_4, c_5, c_6)$$

is fixed by $\tau = (1\ 6)(2\ 5)(3\ 4)$, then $c_1 = c_6$, $c_2 = c_5$, and $c_3 = c_4$; that is, x is a palindrome. It follows that $F(\tau) = 3^3$, for there are 3 choices for each of c_1, c_2, and c_3. The number of flags is thus

$$N = \tfrac{1}{2}(3^6 + 3^3) = 378.$$

Let us make the notion of coloring more precise.

Definition. Given an action of a group G on $X = \{1, \ldots, n\}$ and a set $\mathcal{C}$ of q *colors*, then G acts on the set $\mathcal{C}^n$ of all n-tuples of colors by

$$\tau(c_1, \ldots, c_n) = (c_{\tau 1}, \ldots, c_{\tau n}) \quad \text{for all } \tau \in G.$$

An orbit of $(c_1, \ldots, c_n) \in \mathcal{C}^n$ is called a ***(q, G)-coloring*** of X.

Example 2.159.
Color each square in a 4×4 grid red or black (adjacent squares may have the same color; indeed, one possibility is that all the squares have the same color).

If X consists of the 16 squares in the grid and if $\mathcal{C}$ consists of the two colors red and black, then the cyclic group $G = \langle R \rangle$ of order 4 acts on X, where R is clockwise rotation by 90°; Figure 2.20 shows how R acts: the right square is R's action on the left square. In cycle notation,

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	16

13	9	5	1
14	10	6	2
15	11	7	3
16	12	8	4

Figure 2.20 Chessboard

$$R = (1,\ 4,\ 16,\ 13)(2,\ 8,\ 15,\ 9)(3,\ 12,\ 14,\ 5)(6,\ 7,\ 11,\ 10),$$
$$R^2 = (1,\ 16)(4,\ 13)(2,\ 15)(8,\ 9)(3,\ 14)(12,\ 5)(6,\ 11)(7,\ 10),$$
$$R^3 = (1,\ 13,\ 16,\ 4)(2,\ 9,\ 15,\ 8)(3,\ 5,\ 14,\ 12)(6,\ 10,\ 11,\ 7).$$

A red-and-black chessboard does not change when it is rotated; it is merely viewed from a different position. Thus, we may regard a chessboard as a $(2, G)$-coloring of X; the orbit of a 16-tuple corresponds to the four ways of viewing the board.

By Burnside's lemma, the number of chessboards is

$$\tfrac{1}{4}\Big[F((1)) + F(R) + F(R^2) + F(R^3)\Big].$$

Now $F((1)) = 2^{16}$, for every 16-tuple is fixed by the identity. To compute $F(R)$, note that squares 1, 4, 16, 13 must all have the same color in a 16-tuple fixed by R. Similarly, squares 2, 8, 15, 9 must have the same color, squares 3, 12, 14, 5 must have the same color, and squares 6, 7, 11, 10 must have the same color. We conclude that $F(R) = 2^4$; note that the exponent 4 is the number of cycles in the complete factorization of R. A similar analysis shows that $F(R^2) = 2^8$, for the complete factorization of R^2 has 8 cycles, and $F(R^3) = 2^4$, because the cycle structure of R^3 is the same as that of R. Therefore, the number N of chessboards is

$$N = \tfrac{1}{4}\Big[2^{16} + 2^4 + 2^8 + 2^4\Big] = 16{,}456.$$

Doing this count without group theory is more difficult because of the danger of counting the same chessboard more than once. ◀

We now show that the cycle structure of a permutation τ allows one to calculate $F(\tau)$.

Theorem 2.160. *Let $\mathcal{C}$ be a set of q colors, and let $\tau \in S_n$.*

(i) *If $F(\tau)$ is the number of $x \in \mathcal{C}^n$ fixed by τ, and if $t(\tau)$ is the number of cycles in the complete factorization of τ, then*

$$F(\tau) = q^{t(\tau)}.$$

(ii) *If a finite group G acts on $X = \{1, \ldots, n\}$, then the number N of (q, G)-colorings of X is*

$$N = \frac{1}{|G|} \sum_{\tau \in G} q^{t(\tau)},$$

where $t(\tau)$ is the number of cycles in the complete factorization of τ.

Proof.
(i) Let $\tau \in S_n$ and let $\tau = \beta_1 \cdots \beta_t$ be a complete factorization, where each β_j is an r_j-cycle. If $i_1, \ldots, i_{r_j}$ are the symbols moved by β_j, then $i_{k+1} = \tau^k i_1$ for $k < r_j$. Since $\tau(c_1, \ldots, c_n) = (c_{\tau 1}, \ldots, c_{\tau n}) = (c_1, \ldots, c_n)$, we see that $c_{\tau i_1} = c_{i_1}$ have the same color. But $\tau^2 i_1$ also has the same color as i_1; if fact, $\tau^k i_1$ has the same color as i_1 for all k. Now there is another way to view these points. By Example 2.139, the points $\tau^k i_1$ are precisely the symbols moved by β_j; that is, $\beta_j = (i_1, i_2, \ldots, i_{r_j})$. Thus, $(c_1, \ldots, c_n)$ is fixed by τ if, for each j, all the symbols c_k for k moved by β_j must have the same color. As there are q colors and $t(\tau)$ β_j's, there are $q^{t(\tau)} n$-tuples fixed by τ.
(ii) Substitute $q^{t(\tau)}$ for $F(\tau)$ into the formula in Burnside's lemma. •

Example 2.161.
We can now simplify the computations in Example 2.159. The group G acting on the set X of all 4×4 grids consists of the 4 elements 1, R, R^2, R^3. The complete factorizations of these elements were given in the example, from which we see that

$$\tau(1) = 16, \quad \tau(R) = 4 = \tau(R^3), \quad \tau(R^2) = 8.$$

It follows from Theorem 2.160 that

$$N = \tfrac{1}{4}\big[2^{16} + 2 \cdot 2^4 + 2^8\big]. \quad \blacktriangleleft$$

We introduce a polynomial in several variables to allow us to state a more delicate counting result due to P´olya.

Definition. If the complete factorization of $\tau \in S_n$ has $e_r(\tau) \geq 0$ r-cycles, then the ***index*** of τ is the monomial

$$\operatorname{ind}(\tau) = x_1^{e_1(\tau)} x_2^{e_2(\tau)} \cdots x_n^{e_n(\tau)}.$$

If G is a subgroup of S_n, then the ***cycle index*** of G is the polynomial in n variables with coefficients in $\mathbb{Q}$:

$$P_G(x_1, \ldots, x_n) = \frac{1}{|G|} \sum_{\tau \in G} \text{ind}(\tau).$$

In our earlier discussion of the striped flags, the group G was a cyclic group of order 2 with generator $\tau = (1\ 6)(2\ 5)(3\ 4)$. Thus, $\text{ind}((1)) = x_1^6$, $\text{ind}(\tau) = x_2^3$, and

$$P_G(x_1, \ldots, x_6) = \tfrac{1}{2}(x_1^6 + x_2^3).$$

As a second example, consider all possible blue-and-white flags having 9 stripes. Here $|X| = 9$ and $G = \langle \tau \rangle \leq S_9$, where

$$\tau = (1\ 9)(2\ 8)(3\ 7)(4\ 6)(5).$$

Now, $\text{ind}((1)) = x_1^9$, $\text{ind}(\tau) = x_1 x_2^4$, and the cycle index of $G = \langle \tau \rangle$ is thus

$$P_G(x_1, \ldots, x_9) = \tfrac{1}{2}(x_1^9 + x_1 x_2^4).$$

In Example 2.159, we saw that the cyclic group $G = \langle R \rangle$ of order 4 acts on a grid with 16 squares, and:

$$\text{ind}((1)) = x_1^{16}; \ \ \text{ind}(R) = x_4^4; \ \ \text{ind}(R^2) = x_2^8; \ \ \text{ind}(R^3) = x_4^4.$$

The cycle index is thus

$$P_G(x_1, \ldots, x_{16}) = \tfrac{1}{4}(x_1^{16} + x_2^8 + 2x_4^4).$$

Proposition 2.162. *If $|X| = n$ and G is a subgroup of S_n, then the number of (q, G)-colorings of X is $P_G(q, \ldots, q)$, where $P_G(x_1, \ldots, x_n)$ is the cycle index.*

Proof. By Theorem 2.160, the number of (q, G)-colorings of X is

$$\frac{1}{|G|} \sum_{\tau \in G} q^{t(\tau)},$$

where $t(\tau)$ is the number of cycles in the complete factorization of τ. On the other hand,

$$\begin{aligned} P_G(x_1, \ldots, x_n) &= \frac{1}{|G|} \sum_{\tau \in G} \text{ind}(\tau) \\ &= \frac{1}{|G|} \sum_{\tau \in G} x_1^{e_1(\tau)} x_2^{e_2(\tau)} \cdots x_n^{e_n(\tau)}, \end{aligned}$$

and so

$$P_G(q,\ldots,q) = \frac{1}{|G|}\sum_{\tau\in G} q^{e_1(\tau)+e_2(\tau)+\cdots+e_n(\tau)}$$
$$= \frac{1}{|G|}\sum_{\tau\in G} q^{t(\tau)}. \quad \bullet$$

Let us count again the number of red-and-black chessboards with sixteen squares in Example 2.159. Here,

$$P_G(x_1,\ldots,x_{16}) = \tfrac{1}{4}(x_1^{16} + x_2^8 + 2x_4^4).$$

and so the number of chessboards is

$$P_G(2,\ldots,2) = \tfrac{1}{4}(2^{16} + 2^8 + 2\cdot 2^4).$$

The reason we have introduced the cycle index is that it allows us to state P´olya's generalization of Burnside's lemma which solves the following sort of problem. How many blue-and-white flags with 9 stripes have 4 blue stripes and 5 white stripes? More generally, we want to count the number of orbits in which we prescribe the number of "stripes" of any given color.

Theorem 2.163 (*Pólya*). *Let $G \le S_X$, where $|X| = n$, let $|\mathcal{C}| = q$, and, for each $i \ge 1$, define $\sigma_i = c_1^i + \cdots + c_q^i$. Then the number of (q, G)-colorings of X having f_r elements of color c_r, for every r, is the coefficient of $c_1^{f_1}c_2^{f_2}\cdots c_q^{f_q}$ in $P_G(\sigma_1,\ldots,\sigma_n)$.*

Proofs of P´olya's theorem can be found in combinatorics books (for example, see Biggs, *Discrete Mathematics*). To solve the flag problem posed above, first note that the cycle index for blue-and-white flags having 9 stripes is

$$P_G(x_1,\ldots,x_9) = \tfrac{1}{2}(x_1^9 + x_1x_2^4).$$

and so the number of flags is $P_G(2,\ldots,2) = \frac{1}{2}(2^9 + 2^5) = 272$. Using P´olya's theorem, the number of flags with 4 blue stripes and 5 white ones is the coefficient of b^4w^5 in

$$P_G(\sigma_1,\ldots,\sigma_9) = \tfrac{1}{2}\Big[(b+w)^9 + (b+w)(b^2+w^2)^4\Big].$$

A calculation using the binomial theorem shows that the coefficient of b^4w^5 is 66.

EXERCISES

2.125 How many flags are there with n stripes each of which can be colored any one of q given colors?

2.126 Let X be the squares in an $n \times n$ grid, and let ρ be a rotation by $90°$. Define a ***chessboard*** to be a (q, G)-coloring, where the cyclic group $G = \langle\rho\rangle$ of order 4 is acting. Show that the number of chessboards is

$$\tfrac{1}{4}\left(q^{n^2} + q^{\lfloor (n^2+1)/2 \rfloor} + 2q^{\lfloor (n^2+3)/4 \rfloor}\right),$$

where $\lfloor x \rfloor$ is the greatest integer in the number x.

2.127 Let X be a disk divided into n congruent circular sectors, and let ρ be a rotation by $(360/n)°$. Define a ***roulette wheel*** to be a (q, G)-coloring, where the cyclic group $G = \langle\rho\rangle$ of order n is acting. Prove that if $n = 6$, then there are $\frac{1}{6}(2q + 2q^2 + q^3 + q^6)$ roulette wheels having 6 sectors.

[The formula for the number of roulette wheels with n sectors is

$$\tfrac{1}{n}\sum_{d|n} \phi(n/d)q^d,$$

where ϕ is the Euler ϕ-function.]

2.128 Let X be the vertices of a regular n-gon, and let the dihedral group $G = D_{2n}$ act (as the usual group of symmetries [see Example 2.62]). Define a ***bracelet*** to be a (q, G)-coloring of a regular n-gon, and call each of its vertices a ***bead***. (Not only can one rotate a bracelet; one can also flip it.)

- **(i)** How many bracelets are there having 5 beads, each of which can be colored any one of q available colors?
- **(ii)** How many bracelets are there having 6 beads, each of which can be colored any one of q available colors?
- **(iii)** How many bracelets are there with exactly 6 beads having 1 red bead, 2 white beads, and 3 blue beads?