38. Let $\phi : G \to G'$ be a group homomorphism, and let N' be a normal subgroup of G'. Show that $\phi^{-1}[N']$ is a normal subgroup of G.

39. Show that if G is nonabelian, then the factor group $G/Z(G)$ is not cyclic. [*Hint:* Show the equivalent contrapositive, namely, that if $G/Z(G)$ is cyclic then G is abelian (and hence $Z(G) = G$).]

40. Using Exercise 39, show that a nonabelian group G of order pq where p and q are primes has a trivial center.

41. Prove that A_n is simple for $n \geq 5$, following the steps and hints given.

a. Show A_n contains every 3-cycle if $n \geq 3$.

b. Show A_n is generated by the 3-cycles for $n \geq 3$. [*Hint:* Note that $(a, b)(c, d) = (a, c, b)(a, c, d)$ and $(a, c)(a, b) = (a, b, c)$.]

c. Let r and s be fixed elements of $\{1, 2, \cdots, n\}$ for $n \geq 3$. Show that A_n is generated by the n "special" 3-cycles of the form (r, s, i) for $1 \leq i \leq n$ [*Hint:* Show every 3-cycle is the product of "special" 3-cycles by computing

$$(r, s, i)^2, \quad (r, s, j)(r, s, i)^2, \quad (r, s, j)^2(r, s, i),$$

and

$$(r, s, i)^2(r, s, k)(r, s, j)^2(r, s, i).$$

Observe that these products give all possible types of 3-cycles.]

d. Let N be a normal subgroup of A_n for $n \geq 3$. Show that if N contains a 3-cycle, then $N = A_n$. [*Hint:* Show that $(r, s, i) \in N$ implies that $(r, s, j) \in N$ for $j = 1, 2, \cdots, n$ by computing

$$((r, s)(i, j))(r, s, i)^2((r, s)(i, j))^{-1}.]$$

e. Let N be a nontrivial normal subgroup of A_n for $n \geq 5$. Show that one of the following cases must hold, and conclude in each case that $N = A_n$.

Case I N contains a 3-cycle.

Case II N contains a product of disjoint cycles, at least one of which has length greater than 3. [*Hint:* Suppose N contains the disjoint product $\sigma = \mu(a_1, a_2, \cdots, a_r)$. Show $\sigma^{-1}(a_1, a_2, a_3)\sigma(a_1, a_2, a_3)^{-1}$ is in N, and compute it.]

Case III N contains a disjoint product of the form $\sigma = \mu(a_4, a_5, a_6)(a_1, a_2, a_3)$. [*Hint:* Show $\sigma^{-1}(a_1, a_2, a_4)\sigma(a_1, a_2, a_4)^{-1}$ is in N, and compute it.]

Case IV N contains a disjoint product of the form $\sigma = \mu(a_1, a_2, a_3)$ where μ is a product of disjoint 2-cycles. [*Hint:* Show $\sigma^2 \in N$ and compute it.]

Case V N contains a disjoint product σ of the form $\sigma = \mu(a_3, a_4)(a_1, a_2)$, where μ is a product of an even number of disjoint 2-cycles. [*Hint:* Show that $\sigma^{-1}(a_1, a_2, a_3)\sigma(a_1, a_2, a_3)^{-1}$ is in N, and compute it to deduce that $\alpha = (a_2, a_4)(a_1, a_3)$ is in N. Using $n \geq 5$ for the first time, find $i \neq a_1, a_2, a_3, a_4$ in $\{1, 2, \cdots, n\}$. Let $\beta = (a_1, a_3, i)$. Show that $\beta^{-1}\alpha\beta\alpha \in N$, and compute it.]

42. Let N be a normal subgroup of G and let H be any subgroup of G. Let $HN = \{hn \mid h \in H, n \in N\}$. Show that HN is a subgroup of G, and is the smallest subgroup containing both N and H.

43. With reference to the preceding exercise, let M also be a normal subgroup of G. Show that NM is again a normal subgroup of G.

44. Show that if H and K are normal subgroups of a group G such that $H \cap K = \{e\}$, then $hk = kh$ for all $h \in H$ and $k \in K$. [*Hint:* Consider the commutator $hkh^{-1}k^{-1} = (hkh^{-1})k^{-1} = h(kh^{-1}k^{-1})$.]

45. With reference to the three preceding exercises, let H and K be normal subgroups of a group G such that $HK = G$ and $H \cap K = \{e\}$. Prove that G is isomorphic with $H \times G$.

SECTION 14 †Group Action on a Set

We have seen examples of how groups may *act on things*, like the group of symmetries of a triangle or of a square, the group of rotations of a cube, the general linear group acting on $\mathbb{R}^n$, and so on. In this section we give the general notion of group action and apply it to learn more about finite groups. The next section will give applications to counting.

The Notion of a Group Action

Definition 1.1 defines a binary operation $*$ on a set S to be a function mapping $S \times S$ into S. The function $*$ gives us a rule for "multiplying" an element s_1 in S and an element s_2 in S to yield an element $s_1 * s_2$ in S.

More generally, for any sets A, B, and C, we can view a map $* : A \times B \to C$ as defining a "multiplication," where any element a of A times any element b of B has as value some element c of C. Of course, we write $a * b = c$, or simply $ab = c$. In this section, we will be concerned with the case where X is a set, G is a group, and we have a map $* : G \times X \to X$. We shall write $*(g, x)$ as $g * x$ or gx.

14.1 Example Let $G = \mathrm{GL}(n, \mathbb{R})$ and X the set of all column vectors in $\mathbb{R}^n$. Then for any matrix $A \in G$ and vector $v \in X$, Av is a vector in X. So multiplying is an operation $* : G \times X \to X$. From linear algebra, we know that if B is also a matrix in G, then $(AB)v = A(Bv)$. Furthermore, for the identity matrix I, $Iv = v$. ▲

14.2 Example Let G be the dihedral group D_n. Then elements of D_n permute the set $\mathbb{Z}_n = \{0, 1, 2, 3, \ldots, n-1\}$. For example, $\rho(k) = k +_n 1$. Thus we have an operation $* : D_n \times \mathbb{Z}_n \to \mathbb{Z}_n$. Furthermore, if $\alpha, \gamma \in D_n$ and $k \in \mathbb{Z}_n$, then $(\alpha\gamma)(k) = \alpha(\gamma(k))$ and $\iota(k) = k$. ▲

The two previous examples share the same properties, which we formalize in Definition 14.3.

14.3 Definition Let X be a set and G a group. An **action of G on X** is a map $* : G \times X \to X$ such that

1. $ex = x$ for all $x \in X$,
2. $(g_1 g_2)(x) = g_1(g_2 x)$ for all $x \in X$ and all $g_1, g_2 \in G$.

Under these conditions, X is a **G-set.** ■

14.4 Example Let X be any set, and let H be a subgroup of the group S_X of all permutations of X. Then X is an H-set, where the action of $\sigma \in H$ on X is its action as an element of S_X, so that $\sigma x = \sigma(x)$ for all $x \in X$. Condition 2 is a consequence of the definition of permutation multiplication as function composition, and Condition 1 is immediate from the definition of the identity permutation as the identity function. Note that, in particular, $\{1, 2, 3, \cdots, n\}$ is an S_n-set. ▲

Our next theorem will show that for every G-set X and each $g \in G$, the map $\sigma_g : X \to X$ defined by $\sigma_g(x) = gx$ is a permutation of X, and that there is a homomorphism $\phi : G \to S_X$ such that the action of G on X is essentially the Example 14.4 action of the image subgroup $H = \phi[G]$ of S_X on X. So actions of subgroups of S_X on X describe all possible group actions on X. When studying the set X, actions using subgroups of S_X suffice. However, sometimes a set X is used to study G via a group action of G on X. Thus we need the more general concept given by Definition 14.3.

† This section is a prerequisite only for Sections 15 and 17.

14.5 Theorem Let X be a G-set. For each $g \in G$, the function $\sigma_g : X \to X$ defined by $\sigma_g(x) = gx$ for $x \in X$ is a permutation of X. Also, the map $\phi : G \to S_X$ defined by $\phi(g) = \sigma_g$ is a homomorphism with the property that $\phi(g)(x) = gx$.

Proof To show that σ_g is a permutation of X, we must show that σ_g is a one-to-one map of X onto itself. Suppose that $\sigma_g(x_1) = \sigma_g(x_2)$ for $x_1, x_2 \in X$. Then $gx_1 = gx_2$. Consequently, $g^{-1}(gx_1) = g^{-1}(gx_2)$. Using Condition 2 in Definition 14.3, we see that $(g^{-1}g)x_1 = (g^{-1}g)x_2$, so $ex_1 = ex_2$. Condition 1 of the definition then yields $x_1 = x_2$, so σ_g is one-to-one. The two conditions of the definition show that for $x \in X$, we have $\sigma_g(g^{-1}x) = g(g^{-1})x = (gg^{-1})x = ex = x$, so σ_g maps X onto X. Thus σ_g is indeed a permutation.

To show that $\phi : G \to S_X$ defined by $\phi(g) = \sigma_g$ is a homomorphism, we must show that $\phi(g_1g_2) = \phi(g_1)\phi(g_2)$ for all $g_1, g_2 \in G$. We show the equality of these two permutations in S_X by showing they both carry an $x \in X$ into the same element. Using the two conditions in Definition 14.3 and the rule for function composition, we obtain

$$\begin{aligned}\phi(g_1g_2)(x) &= \sigma_{g_1g_2}(x) = (g_1g_2)x = g_1(g_2x) = g_1\sigma_{g_2}(x) = \sigma_{g_1}(\sigma_{g_2}(x))\\ &= (\sigma_{g_1} \circ \sigma_{g_2})(x) = (\sigma_{g_1}\sigma_{g_2})(x) = (\phi(g_1)\phi(g_2))(x).\end{aligned}$$

Thus ϕ is a homomorphism. The stated property of ϕ follows at once since by our definitions, we have $\phi(g)(x) = \sigma_g(x) = gx$. ◆

It follows from the preceding theorem and Theorem 12.17 that if X is a G-set, then the subset of G leaving every element of X fixed is a normal subgroup N of G, and we can regard X as a G/N-set where the action of a coset gN on X is given by $(gN)x = gx$ for each $x \in X$. If $N = \{e\}$, then the identity element of G is the only element that leaves every $x \in X$ fixed; we then say that G **acts faithfully** on X. A group G is **transitive** on a G-set X if for each $x_1, x_2 \in X$, there exists $g \in G$ such that $gx_1 = x_2$.

We continue with more examples of G-sets.

14.6 Example Every group G is itself a G-set, where the action on $g_2 \in G$ by $g_1 \in G$ is given by left multiplication. That is, $*(g_1, g_2) = g_1g_2$. If H is a subgroup of G, we can also regard G as an H-set, where $*(h, g) = hg$. ▲

14.7 Example Let H be a subgroup of G. Then G is an H-set under conjugation where $*(h, g) = hgh^{-1}$ for $g \in G$ and $h \in H$. Condition 1 is obvious, and for Condition 2 note that

$$*(h_1h_2, g) = (h_1h_2)g(h_1h_2)^{-1} = h_1(h_2gh_2^{-1})h_1^{-1} = *(h_1, *(h_2, g)).$$

We always write this action of H on G by conjugation as hgh^{-1}. The abbreviation hg described before the definition would cause terrible confusion with the group operation of G. ▲

14.8 Example Let H be a subgroup of G, and let L_H be the set of all left cosets of H. Then L_H is a G-set, where the action of $g \in G$ on the left coset xH is given by $g(xH) = (gx)H$. Observe that this action is well defined: if $yH = xH$, then $y = xh$ for some $h \in H$, and $g(yH) = (gy)H = (gxh)H = (gx)(hH) = (gx)H = g(xH)$. A series of exercises shows that every G-set is isomorphic to one that may be formed using these left coset G-sets as building blocks. (See Exercises 22 through 25.) ▲

14.9 Example Let us look closer at the the dihedral group D_4, which permutes the vertices of the square as labeled in Figure 14.10. As indicated in the figure, we label the vertices $0, 1, 2, 3$ as usual; the sides s_0, s_1, s_2, s_3; the midpoints of the sides P_0, P_1, P_2, P_3; the diagonals d_1, d_2; the lines joining opposite side midpoints m_1, m_2; and we label the intersection of the lines d_1, d_2, m_1, m_2 with C.