Proof We let

$$X = \{(g_0, g_1, g_2, \ldots, g_{p-1}) \mid g_0, g_1, \ldots, g_{p-1} \in G \text{ and } g_0 g_1 g_2 \ldots g_{p-1} = e\}.$$

That is, X is the set of all p-tuples with entries in G so that when the entries are multiplied together (in order) their product is the identity e. Since the product is e, $g_0 = (g_1 g_2 \ldots g_{p-1})^{-1}$ and given any $g_1, g_2, \ldots, g_{p-1} \in G$, by picking $g_0 = (g_1 g_2 \ldots g_{p-1})^{-1}$ we have an element in X. Thus $|X| = |G|^{p-1}$ and in particular, p divides the order of X since p divides the order of G.

Suppose that $(g_0, g_1, g_2, \ldots, g_{p-1}) \in X$. Since $g_0 = (g_1 g_2 \ldots g_{p-1})^{-1}$, it follows that $(g_1, g_2, \ldots g_{p-1}, g_0)$ is in X. Repeating this process, noting that $g_1 = (g_2 g_3 \ldots g_{p-1} g_0)^{-1}$ we conclude that $(g_2, g_3, g_4, \cdots, g_{p-1}, g_0, g_1) \in X$. Continuing in this manner we have that for any $k \in \mathbb{Z}_p$,

$$(g_k, g_{k+_p 1}, g_{k+_p 2}, \ldots, g_{k+_p(p-1)}) \in X.$$

We check that this gives a group action of $\mathbb{Z}_p$ on X. Let $k \in \mathbb{Z}_p$ and $(g_0, g_1, g_2, \ldots, g_{p-1}) \in X$. Then

$$k(g_0, g_1, g_2, \ldots, g_{p-1}) = (g_k, g_{k+_p 1}, g_{k+_p 2}, \ldots, g_{k+_p(p-1)}) \in X.$$

Since

$$0(g_0, g_1, g_2, \ldots, g_{p-1}) = (g_0, g_1, g_2, \ldots, g_{p-1}) \text{ and}$$

$$\begin{aligned} k(l(g_0, g_1, g_2, \ldots, g_{p-1})) &= k(g_l, g_{l+_p 1}, g_{l+_p 2}, \ldots, g_{l+_p(p-1)}) \\ &= (g_{k+_p l}, g_{k+_p l+_p 1}, \ldots, g_{k+_p l+_p(p-1)}) \\ &= (k +_p l)(g_0, g_1, g_2, \ldots, g_{p-1}) \end{aligned}$$

this is indeed a group action.

By Theorem 14.19, $0 \equiv |X| \equiv |X_{\mathbb{Z}_p}| \mod p$. The p-tuple $(e, e, e, \ldots, e)$ is in $X_{\mathbb{Z}_p}$ because rearranging the entries does not change the p-tuple. Since $X_{\mathbb{Z}_p}$ contains at least one element and p divides $|X_{\mathbb{Z}_p}|$, $X_{\mathbb{Z}_p}$ must contain at least one element other than $(e, e, e, \ldots, e)$. That element must have the form $(a, a, a, \ldots, a)$ with $a \neq e$ and $a^p = e$. So a has order p and the subgroup it generates is a subgroup of G with order p. ◆

14.21 Definition A p-group is a group such that each element in the group has order a power of p. A p-subgroup of a group is a subgroup that is a p-group. ■

14.22 Example The group D_{16} is a 2-group since the order of any element of D_{16} divides $|D_{16}| = 32$. ▲

14.23 Example Using the Fundamental Theorem of Finitely Generated Abelian Groups, a finite abelian group is a p-group if and only if it is isomorphic to

$$\mathbb{Z}_{p^{r_1}} \times \mathbb{Z}_{p^{r_2}} \times \mathbb{Z}_{p^{r_3}} \times \cdots \times \mathbb{Z}_{p^{r_n}}.$$

This is because if there were a factor of the form $\mathbb{Z}_{q^s}$ where $q \neq p$ is a prime number and $s \geq 1$, then there would be an element in G with order q^s which is not a power of p.

In Exercise 30, you are asked to show that for G a finite group, G is a p-group if and only if the order of G is a power of p.

The next theorem assures us that any finite p-group has a nontrivial normal subgroup, namely the center of the group. ▲

14.24 Theorem Let G be a finite p-group. Then the center of G, $Z(G)$, is not the trivial group.

Proof We let $X = G$ and we make X into a G-set using conjugation. That is, $*(g, a) = gag^{-1}$. Equation 2 states that $0 \equiv |X| \equiv |X_G| \mod p$. For all $g \in G$, $geg^{-1} = e$. So X_G has at least one element, namely e. Since the number of elements in X_G must be at least p, there is an element $a \in X$ such that $a \neq e$ and $gag^{-1} = a$ for all $g \in G$. Thus $ga = ag$ for all $g \in G$, which says that $a \in Z(G)$. So $Z(G)$ is not the trivial subgroup. ◆

When studying p-groups, the fact that the center is nontrivial is often very helpful. We conclude this section with a theorem that illustrates the utility of Theorem 14.24.

14.25 Theorem Every group of order p^2 is abelian.

Proof Let G be a group of order p^2 with center $Z(G)$. By Theorem 14.24, $Z(G)$ is not the trivial group so it is either all of G or else it has order p. We wish to show that $Z(G) = G$ using proof by contradiction. So we assume that $Z(G)$ has p elements. Since $Z(G)$ is a normal subgroup of G, we can form $G/Z(G)$. The group $G/Z(G)$ also has p elements and so both $Z(G)$ and $G/Z(G)$ are cyclic. Let $\langle a \rangle = Z(G)$ and $\langle bZ(G) \rangle = G/Z(G)$. Let $x, y \in G$. Then $x = b^i a^j$ and $y = b^r a^s$ for some integers i, j, r, s since the cosets of $Z(G)$ partition G. Then

$$xy = b^i a^j b^r a^s = b^i b^r a^j a^s$$

since $\langle a \rangle$ is the center of G. So

$$xy = b^{i+r} a^{j+s} = b^r b^i a^s a^j = b^r a^s b^i a^j = yx.$$

Since every element in G commutes with every other element, $Z(G) = G$, which contradicts our assumption that the center has only p elements. So the center of G must be G, which means that G is abelian. ◆

14.26 Example Since every group of order p^2 is abelian, the Fundamental Homomorphism Theorem says that every group with p^2 elements is isomorphic to either $\mathbb{Z}_{p^2}$ or $\mathbb{Z}_p \times \mathbb{Z}_p$. The two groups of order 4 are $\mathbb{Z}_4$ and the Klein 4-group. The two groups of order 9 are $\mathbb{Z}_9$ and $\mathbb{Z}_3 \times \mathbb{Z}_3$. ▲

■ EXERCISES 14

Computations

In Exercises 1 through 3, let

$$X = \{0, 1, 2, 3, s_0, s_1, s_2, s_3, m_1, m_2, d_1, d_2, C, P_0, P_1, P_2, P_3\}$$

be the D_4-set of Example 14.9. Find the following, where $G = D_4$.

1. The fixed sets X_σ for each $\sigma \in D_4$.

2. The isotropy subgroups G_x for each $x \in X$, that is, $G_0, G_1, \cdots, G_{P_2}, G_{P_3}$.

3. The orbits in X under D_4.

4. Theorem 14.24 states that every p-group has nontrivial center. Find the center of D_8.

5. Find the center of D_7.

6. Let $G = X = S_3$ and make X a G-set using conjugation. That is, $*(\sigma, \tau) = \sigma\tau\sigma^{-1}$. Find all the orbits of X using this action. (Write permutations in disjoint cycle notation.)

7. Let $G = D_4$ and X be the set of all subgroups of D_4 with order two. The set X is a G-set using conjugation, $*(\sigma, H) = \sigma H \sigma^{-1}$. Find all the orbits of this group action.

8. Let $G = U = \{z \in \mathbb{C} \mid |z| = 1\}$ be the circle group. Then $X = \mathbb{C}$, the set of complex numbers, is a G-set with group action given by complex number multiplication. That is, if $z \in U$ and $w \in \mathbb{C}$, $*(z, w) = zw$. Find all the orbits of this action. Also, find X_G.

9. Let G be a group of order 3 and suppose that $|X| = 6$. For each possible action of G on X, give a list of the orbit sizes. List the orbit sizes from largest to smallest. (Recall that the orbits partition the set X.)

10. Let G be a group of order 9 and suppose that $|X| = 10$. For each possible action of G on X, give a list of the orbit sizes. List the orbit sizes from largest to smallest.

11. Let G be a group of order 8 and suppose that $|X| = 10$. For each possible way to make X a G-set the orbits partition X. For each possible action of G on X, give a list of the orbit sizes. List the orbit sizes from largest to smallest.

Concepts

In Exercises 12 and 13, correct the definition of the italicized term without reference to the text, if correction is needed, so that it is in a form acceptable for publication.

12. A group G *acts faithfully* on X if and only if $gx = x$ implies that $g = e$.

13. A group G is *transitive* on a G-set X if and only if, for some $g \in G$, gx can be every other x.

14. Let X be a G-set and let $S \subseteq X$. If $Gs \subseteq S$ for all $s \in S$, then S is a **sub-G-set.** Characterize a sub-G-set of a G-set X in terms of orbits in X under G.

15. Characterize a transitive G-set in terms of its orbits.

16. Determine whether each of the following is true or false.

a. Every G-set is also a group.

b. Each element of a G-set is fixed by the identity of G.

c. If every element of a G-set is fixed by the same element g of G, then g must be the identity e.

d. Let X be a G-set with $x_1, x_2 \in X$ and $g \in G$. If $gx_1 = gx_2$, then $x_1 = x_2$.

e. Let X be a G-set with $x \in X$ and $g_1, g_2 \in G$. If $g_1x = g_2x$, then $g_1 = g_2$.

f. Each orbit of a G-set X is a transitive sub-G-set. (See Exercise 14.)

g. Let X be a G-set and let $H \leq G$. Then X can be regarded in a natural way as an H-set.

h. With reference to (g), the orbits in X under H are the same as the orbits in X under G.

i. If X is a G-set, then each element of G acts as a permutation of X.

j. Let X be a G-set and let $x \in X$. If G is finite, then $|G| = |Gx| \cdot |G_x|$.

17. Let X and Y be G-sets with the *same* group G. An **isomorphism** between G-sets X and Y is a map $\phi : X \to Y$ that is one-to-one, onto Y, and satisfies $g\phi(x) = \phi(gx)$ for all $x \in X$ and $g \in G$. Two G-sets are **isomorphic** if such an isomorphism between them exists. Let X be the D_4-set of Example 14.9.

a. Find two distinct orbits of X that are isomorphic sub-D_4-sets. (See Exercise 14.)

b. Show that the orbits {0, 1, 2, 3} and $\{s_0, s_1, s_2, s_3\}$ are not isomorphic sub-D_4-sets. [*Hint:* Find an element of G that acts in an essentially different fashion on the two orbits.]

c. Are the orbits you gave for your answer to part (a) the only two different isomorphic sub-D_4-sets of X?

18. Let X be the D_4-set in Example 14.9.

a. Does D_4 act faithfully on X?

b. Find all orbits in X on which D_4 acts faithfully as a sub-D_4-set. (See Exercise 14.)

Theory

19. Let X be a G-set. Show that G acts faithfully on X if and only if no two distinct elements of G have the same action on each element of X.

20. Let X be a G-set and let $Y \subseteq X$. Let $G_Y = \{g \in G \mid gy = y \text{ for all } y \in Y\}$. Show G_Y is a subgroup of G, generalizing Theorem 14.13.

21. Let G be the additive group of real numbers. Let the action of $\theta \in G$ on the real plane $\mathbb{R}^2$ be given by rotating the plane counterclockwise about the origin through θ radians. Let P be a point other than the origin in the plane.

a. Show $\mathbb{R}^2$ is a G-set.

b. Describe geometrically the orbit containing P.

c. Find the group G_P.

Exercises 22 through 25 show how all possible G-sets, up to isomorphism (see Exercise 17), can be formed from the group G.

22. Let $\{X_i \mid i \in I\}$ be a disjoint collection of sets, so $X_i \cap X_j = \varnothing$ for $i \neq j$. Let each X_i be a G-set for the same group G.

a. Show that $\bigcup_{i \in I} X_i$ can be viewed in a natural way as a G-set, the **union** of the G-sets X_i.

b. Show that every G-set X is the union of its orbits.

23. Let X be a transitive G-set, and let $x_0 \in X$. Show that X is isomorphic (see Exercise 17) to the G-set L of all left cosets of G_{x_0}, described in Example 14.8. [*Hint:* For $x \in X$, suppose $x = gx_0$, and define $\phi : X \to L$ by $\phi(x) = gG_{x_0}$. Be sure to show ϕ is well defined!]

24. Let X_i for $i \in I$ be G-sets for the same group G, and suppose the sets X_i are not necessarily disjoint. Let $X_i' = \{(x, i) \mid x \in X_i\}$ for each $i \in I$. Then the sets X_i' are disjoint, and each can still be regarded as a G-set in an obvious way. (The elements of X_i have simply been tagged by i to distinguish them from the elements of X_j for $i \neq j$.) The G-set $\bigcup_{i \in I} X_i'$ is the **disjoint union** of the G-sets X_i. Using Exercises 22 and 23, show that every G-set is isomorphic to a disjoint union of left coset G-sets, as described in Example 14.12.

25. The preceding exercises show that every G-set X is isomorphic to a disjoint union of left coset G-sets. The question then arises whether left coset G-sets of distinct subgroups H and K of G can themselves be isomorphic. Note that the map defined in the hint of Exercise 23 depends on the choice of x_0 as "base point." If x_0 is replaced by g_0x_0 and if $G_{x_0} \neq G_{g_0x_0}$, then the collections L_H of left cosets of $H = G_{x_0}$ and L_K of left cosets of $K = G_{g_0x_0}$ form distinct G-sets that must be isomorphic, since both L_H and L_K are isomorphic to X.

a. Let X be a transitive G-set and let $x_0 \in X$ and $g_0 \in G$. If $H = G_{x_0}$, describe $K = G_{g_0x_0}$ in terms of H and g_0.

b. Based on part (a), conjecture conditions on subgroups H and K of G such that the left coset G-sets of H and K are isomorphic.

c. Prove your conjecture in part (b).

26. Up to isomorphism, how many transitive $\mathbb{Z}_4$-sets X are there? (Use the preceding exercises.) Give an example of each isomorphism type, listing an action table of each as in Table 14.11. Take lowercase names a, b, c, and so on for the elements in the set X.

27. Repeat Exercise 26 for the group $\mathbb{Z}_6$.

28. Repeat Exercise 26 for the group S_3. List the elements of S_3 in the order ι, (1, 2, 3), (1, 3, 2), (2, 3), (1, 3), (1, 2).

29. Prove that if G is a group of order p^3, where p is a prime number, then $|Z(G)|$ is either p or p^3. Give an example where $|Z(G)| = p$ and an example where $|Z(G)| = p^3$.

30. Let p be a prime number. Prove that a finite group G is a p-group if and only if $|G| = p^n$ for some integer $n \geq 0$.

31. Let G be a group that acts on $X = \{H \mid H \leq G\}$ by conjugation. That is, $g * H = gHg^{-1}$. State and prove an equivalent condition for a subgroup $H \leq G$ to be a normal subgroup of G in terms of

a. G_H, the isotropy subgroup of H.

b. GH, the orbit of H.

SECTION 15 †APPLICATIONS OF *G*-SETS TO COUNTING

This section presents an application of our work with G-sets to counting. Suppose, for example, we wish to count how many distinguishable ways the six faces of a cube can be marked with from one to six dots to form a die. The standard die is marked so that when placed on a table with the 1 on the bottom and the 2 toward the front, the 6 is on top, the 3 on the left, the 4 on the right, and the 5 on the back. Of course, other ways of marking the cube to give a distinguishably different die are possible.

† This section is not used in the remainder of the text.