14. Write the group table for D_3. Compare the group tables for D_3 and S_3. Are the groups isomorphic?

Let A be a set and let $\sigma \in S_A$. For a fixed $a \in A$, the set

$$\mathcal{O}_{a,\sigma} = \{\sigma^n(a) \mid n \in \mathbb{Z}\}$$

is the **orbit** of a **under** σ. In Exercises 15 through 17, find the orbit of 1 under the permutation defined prior to Exercise 1.

15. σ **16.** τ **17.** μ

18. Verify that $H = \{\iota, \mu, \rho^2, \mu\rho^2\} \subseteq D_4$ is a group using the operation function composition.

19. **a.** Verify that the six matrices

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

form a group under matrix multiplication. [*Hint*: Don't try to compute all products of these matrices. Instead, think how the column vector $\begin{bmatrix} 0 \\ 1 \\ 2 \end{bmatrix}$ is transformed by multiplying it on the left by each of the matrices.]

b. What group discussed in this section is isomorphic to this group of six matrices?

20. After working Exercise 18, write down eight matrices that form a group under matrix multiplication that is isomorphic to D_4.

Concepts

In Exercises 21 through 23, 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.

21. The *dihedral group* D_n is the set of all functions $\phi : \mathbb{Z}_n \to \mathbb{Z}_n$ such that the line segment between vertex i and vertex j of U_n is an edge of P_n if and only if the line segment between vertices $\phi(i)$ and $\phi(j)$ in U_n is an edge of P_n.

22. A *permutation* of a set S is a one-to-one map from S to S.

23. The *order* of a group is the number of elements in the group.

In Exercises 24 through 28, determine whether the given function is a permutation of $\mathbb{R}$.

24. $f_1 : \mathbb{R} \to \mathbb{R}$ defined by $f_1(x) = x + 1$

25. $f_2 : \mathbb{R} \to \mathbb{R}$ defined by $f_2(x) = x^2$

26. $f_3 : \mathbb{R} \to \mathbb{R}$ defined by $f_3(x) = -x^3$

27. $f_4 : \mathbb{R} \to \mathbb{R}$ defined by $f_4(x) = e^x$

28. $f_5 : \mathbb{R} \to \mathbb{R}$ defined by $f_5(x) = x^3 - x^2 - 2x$

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

a. Every permutation is a one-to-one function.

b. Every function is a permutation if and only if it is one-to-one.

c. Every function from a finite set onto itself must be one-to-one.

d. Every subset of an abelian group G that is also a group using the same operation as G is abelian.

e. The symmetric group S_{10} has 10 elements.

f. If $\phi \in D_n$, then ϕ is a permutation on the set $\mathbb{Z}_n$.

g. The group D_n has exactly n elements.

h. D_3 is a subset of D_4.

Theory

30. Let $n \geq 3$ and $k \in \mathbb{Z}_n$. Prove that in D_n, $\rho^k\mu = \mu\rho^{n-k}$.

31. Show that S_n is a nonabelian group for $n \geq 3$.

32. Strengthening Exercise 31, show that if $n \geq 3$, then the only element of σ of S_n satisfying $\sigma\gamma = \gamma\sigma$ for all $\gamma \in S_n$ is $\sigma = \iota$, the identity permutation.

33. Orbits were defined before Exercise 15. Let $a, b \in A$ and $\sigma \in S_A$. Show that if $\mathcal{O}_{a,\sigma}$ and $\mathcal{O}_{b,\sigma}$ have an element in common, then $\mathcal{O}_{a,\sigma} = \mathcal{O}_{b,\sigma}$.

34. (See the warning following Theorem 4.8.) Let G be a group with binary operation $*$. Let G' be the same set as G, and define a binary operation $*'$ on G' by $x *' y = y * x$ for all $x, y \in G'$.

a. (Intuitive argument that G' under $*'$ is a group.) Suppose the front wall of your classroom were made of transparent glass, and that all possible products $a * b = c$ and all possible instances $a * (b * c) = (a * b) * c$ of the associative property for G under $*$ were written on the wall with a magic marker. What would a person see when looking at the other side of the wall from the next room in front of yours?

b. Show from the mathematical definition of $*'$ that G' is a group under $*'$.

35. Give a careful proof using the definition of isomorphism that if G and G' are both groups with G abelian and G' not abelian, then G and G' are not isomorphic.

36. Prove that for any integer $n \geq 2$, there are at least two nonisomorphic groups with exactly $2n$ elements.

37. Let $n \geq 3$ and $0 \leq k \leq n - 1$. Prove that the map $\mu\rho^k \in D_n$ is reflection about the line through the origin that makes an angle of $-\frac{\pi k}{n}$ with the $x-$axis.

38. Let $n \geq 3$ and $k, r \in \mathbb{Z}_n$. Based on Exercise 37, determine the element of D_n that corresponds to first reflecting across the line through the origin at an angle of $-\frac{2\pi k}{n}$ and then reflection across the line through the origin making an angle of $-\frac{2\pi r}{n}$. Prove your answer.

SECTION 5 SUBGROUPS

Subsets and Subgroups

You may have noticed that we sometimes have had groups contained within larger groups. For example, the group $\mathbb{Z}$ under addition is contained within the group $\mathbb{Q}$ under addition, which in turn is contained in the group $\mathbb{R}$ under addition. When we view the group $\langle \mathbb{Z}, + \rangle$ as contained in the group $\langle \mathbb{R}, + \rangle$, it is very important to notice that the operation $+$ on integers n and m as elements of $\langle \mathbb{Z}, + \rangle$ produces the same element $n + m$ as would result if you were to think of n and m as elements in $\langle \mathbb{R}, + \rangle$. Thus we should *not* regard the group $\langle \mathbb{Q}^+, \cdot \rangle$ as contained in $\langle \mathbb{R}, + \rangle$, even though $\mathbb{Q}^+$ is contained in $\mathbb{R}$ as a set. In this instance, $2 \cdot 3 = 6$ in $\langle \mathbb{Q}^+, \cdot \rangle$, while $2 + 3 = 5$ in $\langle \mathbb{R}, + \rangle$. We are requiring not only that the set of one group be a subset of the set of the other, but also that the group operation on the subset be the *induced operation* that assigns the same element to each ordered pair from this subset as is assigned by the group operation on the whole set.

5.1 Definition If a subset H of a group G is closed under the binary operation of G and if H with the induced operation from G is itself a group, then H is a **subgroup of** G. We shall let $H \leq G$ or $G \geq H$ denote that H is a subgroup of G, and $H < G$ or $G > H$ shall mean $H \leq G$ but $H \neq G$. ■

Thus $\langle \mathbb{Z}, + \rangle < \langle \mathbb{R}, + \rangle$ but $\langle \mathbb{Q}^+, \cdot \rangle$ is *not* a subgroup of $\langle \mathbb{R}, + \rangle$, even though as sets, $\mathbb{Q}^+ \subset \mathbb{R}$. Every group G has as subgroups G itself and $\{e\}$, where e is the identity element of G.

5.2 Definition If G is a group, then the subgroup consisting of G itself is the **improper subgroup** of G. All other subgroups are **proper subgroups**. The subgroup $\{e\}$ is the **trivial subgroup** of G. All other subgroups are **nontrivial**. ■

We turn to some illustrations.

5.3 Example Let $\mathbb{R}^n$ be the additive group of all n-component row vectors with real number entries. The subset consisting of all of these vectors having 0 as entry in the first component is a subgroup of $\mathbb{R}^n$. ▲

5.4 Example $\mathbb{Q}^+$ under multiplication is a proper subgroup of $\mathbb{R}^+$ under multiplication. ▲

5.5 Example The n^{th} roots of unity in $\mathbb{C}$, U_n, form a subgroup of U, the complex numbers whose absolute value is 1, which in turn is a subgroup of $\mathbb{C}^*$, the nonzero complex numbers under multiplication. ▲

5.6 Example Recall that $S_{\mathbb{Z}_n}$ is the set of all one-to-one functions mapping $\mathbb{Z}_n$ onto $\mathbb{Z}_n$ and D_n is the set of all one-to-one functions ϕ mapping $\mathbb{Z}_n$ onto $\mathbb{Z}_n$ with the further property that the line segment between i and j is an edge of the regular n-gon P_n if and only if the line segment between $\phi(i)$ and $\phi(j)$ is an edge. $D_n \subseteq S_{\mathbb{Z}_n}$. Since both D_n and $S_{\mathbb{Z}_n}$ are groups under composition of functions, $D_n \leq S_{\mathbb{Z}_n}$. ▲

5.7 Example There are two different types of group structures of order 4 (see Exercise 20 of Section 2). We describe them by their group tables (Tables 5.8 and 5.9). The group V is the Klein 4-group.

The only nontrivial proper subgroup of $\mathbb{Z}_4$ is $\{0, 2\}$. Note that $\{0, 3\}$ is *not* a subgroup of $\mathbb{Z}_4$, since $\{0, 3\}$ is *not closed* under $+$. For example, $3 + 3 = 2$, and $2 \notin \{0, 3\}$. However, the group V has three nontrivial proper subgroups, $\{e, a\}, \{e, b\}$, and $\{e, c\}$. Here $\{e, a, b\}$ is *not* a subgroup, since $\{e, a, b\}$ is not closed under the operation of V because $ab = c$, and $c \notin \{e, a, b\}$. ▲

5.8 Table

$\mathbb{Z}_4$:

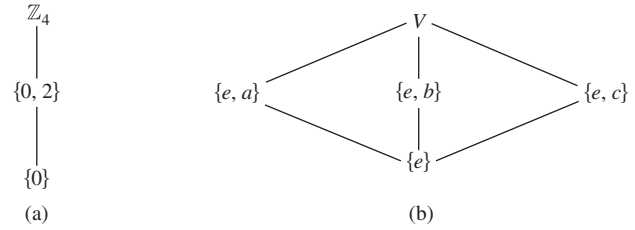
$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

5.9 Table

V:

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

It is often useful to draw a *subgroup diagram* of the subgroups of a group. In such a diagram, a line running downward from a group G to a group H means that H is a subgroup of G. Thus the larger group is placed nearer the top of the diagram. Figure 5.10 contains the subgroup diagrams for the groups $\mathbb{Z}_4$ and V of Example 5.7.



5.10 Figure (a) Subgroup diagram for $\mathbb{Z}_4$. (b) Subgroup diagram for V.

Note that if $H \leq G$ and $a \in H$, then by Theorem 2.17, the equation $ax = a$ must have a unique solution, namely the identity element of H. But this equation can also

be viewed as one in G, and we see that this unique solution must also be the identity element e of G. A similar argument then applied to the equation $ax = e$, viewed in both H and G, shows that the inverse a^{-1} of a in G is also the inverse of a in the subgroup H.

5.11 Example Let F be the group of all real-valued functions with domain $\mathbb{R}$ under addition. The subset of F consisting of those functions that are continuous is a subgroup of F, for the sum of continuous functions is continuous, the function f where $f(x) = 0$ for all x is continuous and is the additive identity element, and if f is continuous, then $-f$ is continuous. ▲

It is convenient to have routine steps for determining whether a subset of a group G is a subgroup of G. Example 5.11 indicates such a routine, and in the next theorem, we demonstrate carefully its validity.

5.12 Theorem A subset H of a group G is a subgroup of G if and only if

1. H is closed under the binary operation of G,
2. the identity element e of G is in H, and
3. for all $a \in H$, $a^{-1} \in H$ also.

Proof The fact that if $H \leq G$ then Conditions 1, 2, and 3 must hold follows at once from the definition of a subgroup and from the remarks preceding Example 5.11.

Conversely, suppose H is a subset of a group G such that Conditions 1, 2, and 3 hold. By 2 we have at once that $\mathscr{G}_2$ is satisfied. Also $\mathscr{G}_3$ is satisfied by 3. It remains to check the associative axiom, $\mathscr{G}_1$. But surely for all $a, b, c \in H$ it is true that $(ab)c = a(bc)$ in H, for we may actually view this as an equation in G, where the associative law holds. Hence $H \leq G$. ◆

5.13 Example Let F be as in Example 5.11. The subset of F consisting of those functions that are differentiable is a subgroup of F, for the sum of differentiable functions is differentiable, the constant function 0 is differentiable, and if f is differentiable, then $-f$ is differentiable. ▲

5.14 Example Recall from linear algebra that every square matrix A has associated with it a number $\det(A)$ called its determinant, and that A is invertible if and only if $\det(A) \neq 0$. If A and B are square matrices of the same size, then it can be shown that $\det(AB) = \det(A) \cdot \det(B)$. Let G be the multiplicative group of all invertible $n \times n$ matrices with entries in $\mathbb{C}$ and let T be the subset of G consisting of those matrices with determinant 1. The equation $\det(AB) = \det(A) \cdot \det(B)$ shows that T is closed under matrix multiplication. Recall that the identity matrix I_n has determinant 1. From the equation $\det(A) \cdot \det(A^{-1}) = \det(AA^{-1}) = \det(I_n) = 1$, we see that if $\det(A) = 1$, then $\det(A^{-1}) = 1$. Theorem 5.12 then shows that T is a subgroup of G. ▲

Theorem 5.15 provides an alternate way of checking that a subset of a group is a subgroup.

5.15 Theorem A nonempty subset H of the group G is a subgroup of G if and only if for all $a, b \in G$, $ab^{-1} \in G$.

Proof We leave the proof as Exercise 51. ◆

On the surface Theorem 5.15 may seem simpler than Theorem 5.12 since we only need to show that H is not empty and one other condition. In practice, it is usually just as efficient to use Theorem 5.12. On the other hand, Theorem 5.16 can often be used efficiently.

5.16 Theorem Let H be a finite nonempty subset of the group G. Then H is a subgroup of G if and only if H is closed under the operation of G.

Proof We leave the proof as Exercise 57. ◆

5.17 Example Recall that $U_n = \{z \in \mathbb{C} \mid z^n = 1\}$. We could use Theorem 5.16 to verify that U_n is a subgroup of C^* by noting that U_n has exactly n elements, so U_n is a finite nonempty subset of $\mathbb{C}^*$ and if $z_1, z_2 \in U_n$, then $(z_1 z_2)^n = 1$, which implies that U_n is closed under multiplication. ▲

5.18 Example We verify that the subset $H = \{\iota = \rho^0, \rho, \rho^2, \ldots, \rho^{n-1}\} \subset D_n$ is a subgroup of D_n. By Theorem 5.16, we only need to check that H is closed under the operation of D_n. Let $k, r \in \mathbb{Z}_n$. Then $\rho^k \rho^r = \rho^{k +_n r} \in H$. Therefore $H \leq D_n$. ▲

Cyclic Subgroups

Let us see how large a subgroup H of $\mathbb{Z}_{12}$ would have to be if it contains 3. It would have to contain the identity element 0 and $3 + 3$, which is 6. Then it has to contain $6 + 3$, which is 9. Note that the inverse of 3 is 9 and the inverse of 6 is 6. It is easily checked that $H = \{0, 3, 6, 9\}$ is a subgroup of $\mathbb{Z}_{12}$, and it is the smallest subgroup containing 3.

Let us imitate this reasoning in a general situation. As we remarked before, for a general argument we always use multiplicative notation. Let G be a group and let $a \in G$. A subgroup of G containing a must, by Theorem 5.12, contain a^n, the result of computing products of a and itself for n factors for every positive integer n. These positive integral powers of a do give a set closed under multiplication. It is possible, however, that the inverse of a is not in this set. Of course, a subgroup containing a must also contain a^{-1}, and, in general, it must contain a^{-m} for all $m \in \mathbb{Z}^+$. It must contain the identity element $e = a^0$. Summarizing, *a subgroup of G containing the element a must contain all elements* a^n (*or na for additive groups*) *for all* $n \in \mathbb{Z}$. That is, a subgroup containing a must contain $\{a^n | n \in \mathbb{Z}\}$. Observe that these powers a^n of a need not be distinct. For example, in the group V of Example 5.7,

$$a^2 = e, \quad a^3 = a, \quad a^4 = e, \quad a^{-1} = a, \qquad \text{and so on.}$$

We have almost proved the next theorem.

5.19 Theorem Let G be a group and let $a \in G$. Then

$$H = \{a^n \mid n \in \mathbb{Z}\}$$

is a subgroup of G and is the smallest[†] subgroup of G that contains a, that is, every subgroup containing a contains H.

Proof We check the three conditions given in Theorem 5.12 for a subset of a group to give a subgroup. Since $a^r a^s = a^{r+s}$ for $r, s \in \mathbb{Z}$, we see that the product in G of two elements of H is again in H. Thus H is closed under the group operation of G. Also $a^0 = e$, so $e \in H$, and for $a^r \in H, a^{-r} \in H$ and $a^{-r} a^r = e$. Hence all the conditions are satisfied, and $H \leq G$.

[†] We may find occasion to distinguish between the terms *minimal* and *smallest* as applied to subsets of a set S that have some property. A subset H of S is minimal with respect to the property if H has the property, and no subset $K \subset H, K \neq H$, has the property. If H has the property and $H \subseteq K$ for every subset K with the property, then H is the smallest subset with the property. There may be many minimal subsets, but there can be only one smallest subset. To illustrate, $\{e, a\}, \{e, b\}$, and $\{e, c\}$ are all minimal nontrivial subgroups of the group V. (See Fig. 5.10.) However, V contains no smallest nontrivial subgroup.

Our arguments prior to the statement of the theorem showed that any subgroup of G containing a must contain H, so H is the smallest subgroup of G containing a. ◆

5.20 Definition Let G be a group and let $a \in G$. Then the subgroup $\{a^n \mid n \in \mathbb{Z}\}$ of G, characterized in Theorem 5.19, is called the **cyclic subgroup of G generated by a**, and denoted by $\langle a \rangle$. ■

5.21 Example Let us find two of the cyclic subgroups to D_{10}. We first consider $\langle \mu\rho^k \rangle$ for $k \in \mathbb{Z}_{10}$. Since $(\mu\rho^k)^2 = \iota$ and $(\mu\rho^k)^{-1} = \mu\rho^k$, for any integer r, $(\mu\rho^k)^r$ is either $\mu\rho^k$ or ι. Thus

$$\langle \mu\rho^k \rangle = \{\iota, \mu\rho^k\}.$$

Since $\rho^{-1} = \rho^9$, every negative power of ρ is also a positive power of ρ and $\rho^{10} = \iota$,

$$\langle \rho \rangle = \{\iota, \rho, \rho^2, \ldots, \rho^9\}.$$

▲

5.22 Definition An element a of a group G **generates** G and is a **generator for** G if $\langle a \rangle = G$. A group G is **cyclic** if there is some element a in G that generates G. ■

5.23 Example Let $\mathbb{Z}_4$ and V be the groups of Example 5.7. Then $\mathbb{Z}_4$ is cyclic and both 1 and 3 are generators, that is,

$$\langle 1 \rangle = \langle 3 \rangle = \mathbb{Z}_4.$$

However, V is *not* cyclic, for $\langle a \rangle$, $\langle b \rangle$, and $\langle c \rangle$ are proper subgroups of two elements. Of course, $\langle e \rangle$ is the trivial subgroup of one element. ▲

5.24 Example The group $\mathbb{Z}$ under addition is a cyclic group. Both 1 and -1 are generators for this group, and they are the only generators. Also, for $n \in \mathbb{Z}^+$, the group $\mathbb{Z}_n$ under addition modulo n is cyclic. If $n > 1$, then both 1 and $n - 1$ are generators, but there may be others. ▲

5.25 Example Consider the group $\mathbb{Z}$ under addition. Let us find $\langle 3 \rangle$. Here the notation is additive, and $\langle 3 \rangle$ must contain

$$\begin{array}{cccccc} & & 3, & 3+3=6, & 3+3+3=9, & \text{and so on,} \\ 0, & -3, & -3+-3=-6, & -3+-3+-3=-9, & & \text{and so on.} \end{array}$$

In other words, the cyclic subgroup generated by 3 consists of all multiples of 3, positive, negative, and zero. We denote this subgroup by $3\mathbb{Z}$ as well as $\langle 3 \rangle$. In a similar way, we shall let $n\mathbb{Z}$ be the cyclic subgroup $\langle n \rangle$ of $\mathbb{Z}$. Note that $6\mathbb{Z} < 3\mathbb{Z}$. ▲

5.26 Example For each positive integer n, U_n is the multiplicative group of the nth roots of unity in $\mathbb{C}$. These elements of U_n can be represented geometrically by equally spaced points on a circle about the origin, as illustrated in Fig. 5.27. The point labeled represents the number

$$\zeta = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}.$$

The geometric interpretation of multiplication of complex numbers, explained in Section 3, shows at once that as ζ is raised to powers, it works its way counterclockwise around the circle, landing on each of the elements of U_n in turn. Thus U_n under multiplication is a cyclic group, and ζ is a generator. The group U_n is the cyclic subgroup $\langle \zeta \rangle$ of the group U of all complex numbers z, where $|z| = 1$, under multiplication. ▲