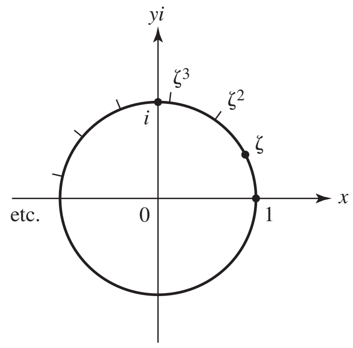


5.27 Figure

EXERCISES 5

Computations

In Exercises 1 through 6, determine whether the given subset of the complex numbers is a subgroup of the group $\mathbb{C}$ of complex numbers under addition.

1. $\mathbb{R}$ **2.** $\mathbb{Q}^+$ **3.** $7\mathbb{Z}$

4. The set $i\mathbb{R}$ of pure imaginary numbers including 0

5. The set $\pi\mathbb{Q}$ of rational multiples of π **6.** The set $\{\pi^n \mid n \in \mathbb{Z}\}$

7. Which of the sets in Exercises 1 through 6 are subgroups of the group $\mathbb{C}^*$ of nonzero complex numbers under multiplication?

In Exercises 8 through 13, determine whether the given set of invertible $n \times n$ matrices with real number entries is a subgroup of $GL(n, \mathbb{R})$.

8. The $n \times n$ matrices with determinant greater than or equal to 1

9. The diagonal $n \times n$ matrices with no zeros on the diagonal

10. The $n \times n$ matrices with determinant 2^k for some integer k

11. The $n \times n$ matrices with determinant -1

12. The $n \times n$ matrices with determinant -1 or 1

13. The set of all $n \times n$ matrices A such that $(A^T)A = I_n$. [These matrices are called **orthogonal.** Recall that A^T, the *transpose* of A, is the matrix whose jth column is the jth row of A for $1 \leq j \leq n$, and that the transpose operation has the property $(AB)^T = (B^T)(A^T)$.]

Let F be the set of all real-valued functions with domain $\mathbb{R}$ and let $\tilde{F}$ be the subset of F consisting of those functions that have a nonzero value at every point in $\mathbb{R}$. In Exercises 14 through 19, determine whether the given subset of F with the induced operation is (a) a subgroup of the group F under addition, (b) a subgroup of the group $\tilde{F}$ under multiplication.

14. The subset $\tilde{F}$

15. The subset of all $f \in F$ such that $f(1) = 0$

16. The subset of all $f \in \tilde{F}$ such that $f(1) = 1$

17. The subset of all $f \in \tilde{F}$ such that $f(0) = 1$

18. The subset of all $f \in \tilde{F}$ such that $f(0) = -1$

19. The subset of all constant functions in F.

20. Nine groups are given below. Give a *complete* list of all subgroup relations, of the form $G_i \leq G_j$, that exist between these given groups $G_1, G_2, \cdots, G_9$.
$G_1 = \mathbb{Z}$ under addition
$G_2 = 12\mathbb{Z}$ under addition
$G_3 = \mathbb{Q}^+$ under multiplication
$G_4 = \mathbb{R}$ under addition
$G_5 = \mathbb{R}^+$ under multiplication
$G_6 = \{\pi^n \mid n \in \mathbb{Z}\}$ under multiplication
$G_7 = 3\mathbb{Z}$ under addition
$G_8 =$ the set of all integral multiples of 6 under addition
$G_9 = \{6^n \mid n \in \mathbb{Z}\}$ under multiplication

21. Write at least 5 elements of each of the following cyclic groups.

a. $25\mathbb{Z}$ under addition
b. $\{(\frac{1}{2})^n \mid n \in \mathbb{Z}\}$ under multiplication
c. $\{\pi^n \mid n \in \mathbb{Z}\}$ under multiplication
d. $\langle \rho^3 \rangle$ in the group D_{18}
e. $\langle (1,2,3)(5,6) \rangle$ in the group S_6

In Exercises 22 through 25, describe all the elements in the cyclic subgroup of $GL(2,\mathbb{R})$ generated by the given 2×2 matrix.

22. $\begin{bmatrix} 0 & -1 \\ -1 & 0 \end{bmatrix}$ **23.** $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ **24.** $\begin{bmatrix} 3 & 0 \\ 0 & 2 \end{bmatrix}$ **25.** $\begin{bmatrix} 0 & -2 \\ -2 & 0 \end{bmatrix}$

26. Which of the following groups are cyclic? For each cyclic group, list all the generators of the group.

$$G_1 = \langle \mathbb{Z}, + \rangle \quad G_2 = \langle \mathbb{Q}, + \rangle \quad G_3 = \langle \mathbb{Q}^+, \cdot \rangle \quad G_4 = \langle 6\mathbb{Z}, + \rangle$$
$$G_5 = \{6^n \mid n \in \mathbb{Z}\} \text{ under multiplication}$$
$$G_6 = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\} \text{ under addition}$$

In Exercises 27 through 35, find the order of the cyclic subgroup of the given group generated by the indicated element.

27. The subgroup of $\mathbb{Z}_4$ generated by 3

28. The subgroup of V generated by c (see Table 5.9)

29. The subgroup of U_6 generated by $\cos \frac{2\pi}{3} + i \sin \frac{2\pi}{3}$

30. The subgroup of $\mathbb{Z}_{10}$ generated by 8

31. The subgroup of $\mathbb{Z}_{16}$ generated by 12

32. The subgroup of the symmetric group S_8 generated by $(2,4,6,9)(3,5,7)$

33. The subgroup of the symmetric group S_{10} generated by $(1,10)(2,9)(3,8)(4,7)(5,6)$

34. The subgroup of the multiplicative group G of invertible 4×4 matrices generated by

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

35. The subgroup of the multiplicative group G of invertible 4×4 matrices generated by

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

36. **a.** Complete Table 5.28 to give the group $\mathbb{Z}_6$ of 6 elements.
b. Compute the subgroups $\langle 0 \rangle$, $\langle 1 \rangle$, $\langle 2 \rangle$, $\langle 3 \rangle$, $\langle 4 \rangle$, and $\langle 5 \rangle$ of the group $\mathbb{Z}_6$ given in part (a).

c. Which elements are generators for the group $\mathbb{Z}_6$ of part (a)?

d. Give the subgroup diagram for the part (b) subgroups of $\mathbb{Z}_6$. (We will see later that these are all the subgroups of $\mathbb{Z}_6$.)

5.28 Table

$\mathbb{Z}_6$:

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2					
3	3					
4	4					
5	5					

Concepts

In Exercises 37 and 38, 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.

37. A *subgroup* of a group G is a subset H of G that contains the identity element e of G and also contains the inverse of each of its elements.

38. A group G is *cyclic* if and only if there exists $a \in G$ such that $G = \{a^n \mid n \in \mathbb{Z}\}$.

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

a. The associative law holds in every group.
b. There may be a group in which the cancellation law fails.
c. Every group is a subgroup of itself.
d. Every group has exactly two improper subgroups.
e. In every cyclic group, every element is a generator.
f. A cyclic group has a unique generator.
g. Every set of numbers that is a group under addition is also a group under multiplication.
h. A subgroup may be defined as a subset of a group.
i. $\mathbb{Z}_4$ is a cyclic group.
j. Every subset of every group is a subgroup under the induced operation.
k. For any $n \geq 3$, the dihedral group D_n has at least $n + 2$ cyclic subgroups.

40. Show by means of an example that it is possible for the quadratic equation $x^2 = e$ to have more than two solutions in some group G with identity e.

In Exercises 41 through 44 let B be a subset of A, and let b be a particular element of B. Determine whether the given set is a subgroup of the symmetric group S_A under the induced operation. Here $\sigma[B] = \{\sigma(x) \mid x \in B\}$.

41. $\{\sigma \in S_A \mid \sigma(b) = b\}$

42. $\{\sigma \in S_A \mid \sigma(b) \in B\}$

43. $\{\sigma \in S_A \mid \sigma[B] \subseteq B\}$

44. $\{\sigma \in S_A \mid \sigma[B] = B\}$

Theory

In Exercises 45 and 46, let $\phi : G \to G'$ be an isomorphism of a group $\langle G, * \rangle$ with a group $\langle G', *' \rangle$. Write out a proof to convince a skeptic of the intuitively clear statement.

45. If H is a subgroup of G, then $\phi[H] = \{\phi(h) \mid h \in H\}$ is a subgroup of G'. That is, an isomorphism carries subgroups into subgroups.

46. If there is an $a \in G$ such that $\langle a \rangle = G$, then G' is cyclic.

47. Show that if H and K are subgroups of an abelian group G, then

$$\{hk \mid h \in H \text{ and } k \in K\}$$

is a subgroup of G.

48. Find an example of a group G and two subgroups H and K such that the set in Exercise 47 is not a subgroup of G.

49. Prove that for any integer $n \geq 3$, S_n has a subgroup isomorphic with D_n.

50. Find the flaw in the following argument: "Condition 2 of Theorem 5.12 is redundant, since it can be derived from 1 and 3, for let $a \in H$. Then $a^{-1} \in H$ by 3, and by 1, $aa^{-1} = e$ is an element of H, proving 2."

51. Prove Theorem 5.15.

52. Prove that if G is a cyclic group and $|G| \geq 3$, then G has at least 2 generators.

53. Prove that if G is an abelian group, written multiplicatively, with identity element e, then all elements x of G satisfying the equation $x^2 = e$ form a subgroup H of G.

54. Repeat Exercise 53 for the general situation of the set H of all solutions x of the equation $x^n = e$ for a fixed integer $n \geq 1$ in an abelian group G with identity e.

55. Find a counterexample to Exercise 53 if the assumption of abelian is dropped.

56. Show that if $a \in G$, where G is a finite group with identity e, then there exists $n \in \mathbb{Z}^+$ such that $a^n = e$.

57. Prove Theorem 5.16.

58. Let G be a group and let a be one fixed element of G. Show that

$$H_a = \{x \in G \mid xa = ax\}$$

is a subgroup of G.

59. Generalizing Exercise 58, let S be any subset of a group G.
a. Show that $H_S = \{x \in G \mid xs = sx \text{ for all } s \in S\}$ is a subgroup of G.
b. In reference to part (a), the subgroup H_G is the **center of** G. Show that H_G is an abelian group.

60. Let H be a subgroup of a group G. For $a, b \in G$, let $a \sim b$ if and only if $ab^{-1} \in H$. Show that $\sim$ is an equivalence relation on G.

61. For sets H and K, we define the **intersection** $H \cap K$ by

$$H \cap K = \{x \mid x \in H \text{ and } x \in K\}.$$

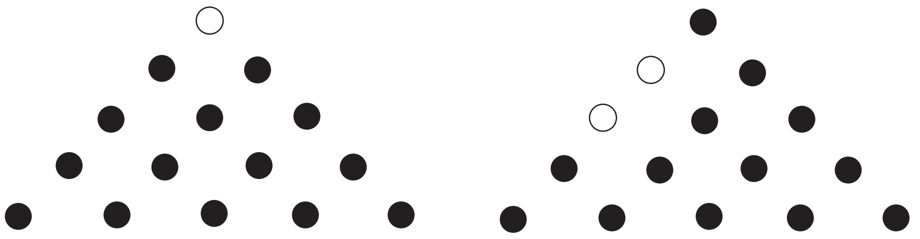
Show that if $H \leq G$ and $K \leq G$, then $H \cap K \leq G$. (Remember: $\leq$ denotes "is a subgroup of," not "is a subset of.")

62. Prove that every cyclic group is abelian.

63. Let G be a group and let $G_n = \{g^n \mid g \in G\}$. Under what hypothesis about G can we show that G_n is a subgroup of G?

64. Show that a group with no proper nontrivial subgroups is cyclic.

65. Cracker Barrel Restaurants place a puzzle called "Jump All But One Game" at each table. The puzzle starts with golf tees arranged in a triangle as in Figure 5.29a where the presence of a tee is noted with a solid dot and the absence is noted with a hollow dot. A move can be made if a tee can jump over one adjacent tee and land on an empty space. When a move is made, the tee that is jumped over is removed. A possible first move is shown in Figure 5.29b. The goal is to have just one remaining tee. Use the Klein 4-group to show that no matter what sequence of (legal) moves you make, the last remaining tee cannot be in a bottom corner position.



(a) (b)

5.29 Figure

SECTION 6 CYCLIC GROUPS

Recall the following facts and notations from Section 5. If G is a group and $a \in G$, then

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

is a subgroup of G (Theorem 5.19). This group is the **cyclic subgroup** $\langle a \rangle$ **of** G **generated by** a. Also, given a group G and an element a in G, if

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

then a is a **generator of** G and the group $G = \langle a \rangle$ is **cyclic.** We introduce one new bit of terminology. Let a be an element of a group G. If the cyclic subgroup $\langle a \rangle$ of G is finite, then the **order of** a is the order $|\langle a \rangle|$ of this cyclic subgroup. Otherwise, we say that a is of **infinite order.** We will see in this section that if $a \in G$ is of finite order m, then m is the smallest positive integer such that $a^m = e$.

The first goal of this section is to describe all cyclic groups and all subgroups of cyclic groups. This is not an idle exercise. We will see later that cyclic groups serve as building blocks for a significant class of abelian groups, in particular, for all finite abelian groups. Cyclic groups are fundamental to the understanding of groups.

Elementary Properties of Cyclic Groups

We start with a demonstration that cyclic groups are abelian.

6.1 Theorem Every cyclic group is abelian.

Proof Let G be a cyclic group and let a be a generator of G so that

$$G = \langle a \rangle = \{a^n \mid n \in \mathbb{Z}\}.$$

If g_1 and g_2 are any two elements of G, there exist integers r and s such that $g_1 = a^r$ and $g_2 = a^s$. Then

$$g_1 g_2 = a^r a^s = a^{r+s} = a^{s+r} = a^s a^r = g_2 g_1,$$

so G is abelian. ◆

We shall continue to use multiplicative notation for our general work on cyclic groups, even though they are abelian.

The *division algorithm* that follows is well known and seems pretty simple. In fact, this algorithm is taught in elementary school. If you divide an integer n by a positive integer m, you get an integer quotient q with a remainder r where $0 \leq r < m$. You might write this as $n \div m = q \text{ R } r$, which of course means $\frac{n}{m} = q + \frac{r}{m}$. Multiplying both sides by m gives the form of the division algorithm that is a fundamental tool for the study of cyclic groups.