Subgroups of Finite Cyclic Groups

We have completed our description of cyclic groups and turn to their subgroups. Corollary 6.7 gives us complete information about subgroups of infinite cyclic groups. Let us give the basic theorem regarding generators of subgroups for the finite cyclic groups.

6.15 Theorem Let G be a cyclic group with n elements and generated by a. Let $b \in G$ and let $b = a^s$. Then b generates a cyclic subgroup H of G containing n/d elements, where d is the greatest common divisor of n and s. Also, $\langle a^s \rangle = \langle a^t \rangle$ if and only if $\gcd(s, n) = \gcd(t, n)$.

Proof That b generates a cyclic subgroup H of G is known from Theorem 5.19. We need show only that H has n/d elements. Following the argument of Case II of Theorem 6.10, we see that H has as many elements as the smallest positive power m of b that gives the identity. Now $b = a^s$, and $b^m = e$ if and only if $(a^s)^m = e$, or if and only if n divides ms. What is the smallest positive integer m such that n divides ms? Let d be the gcd of n and s. Then there exist integers u and v such that

$$d = un + vs.$$

Since d divides both n and s, we may write

$$1 = u(n/d) + v(s/d)$$

where both n/d and s/d are integers. This last equation shows that n/d and s/d are relatively prime, for any integer dividing both of them must also divide 1. We wish to find the smallest positive m such that

$$\frac{ms}{n} = \frac{m(s/d)}{(n/d)} \text{ is an integer.}$$

From the division property (1) following Example 6.9, we conclude that n/d must divide m, so the smallest such m is n/d. Thus the order of H is n/d.

Taking for the moment $\mathbb{Z}_n$ as a model for a cyclic group of order n, we see that if d is a divisor of n, then the cyclic subgroup $\langle d \rangle$ of $\mathbb{Z}_n$ has n/d elements, and contains all the positive integers m less than n such that $\gcd(m, n) = d$. Thus there is only one subgroup of $\mathbb{Z}_n$ of order n/d. Taken with the preceding paragraph, this shows at once that if a is a generator of the cyclic group G, then $\langle a^s \rangle = \langle a^t \rangle$ if and only if $\gcd(s, n) = \gcd(t, n)$. ◆

6.16 Example For an example using additive notation, consider $\mathbb{Z}_{12}$, with the generator $a = 1$. Since the greatest common divisor of 3 and 12 is 3, $3 = 3 \cdot 1$ generates a subgroup of $\frac{12}{3} = 4$ elements, namely

$$\langle 3 \rangle = \{0, 3, 6, 9\}.$$

Since the gcd of 8 and 12 is 4, 8 generates a subgroup of $\frac{12}{4} = 3$ elements, namely,

$$\langle 8 \rangle = \{0, 4, 8\}.$$

Since the gcd of 12 and 5 is 1, 5 generates a subgroup of $\frac{12}{1} = 12$ elements; that is, 5 is a generator of the whole group $\mathbb{Z}_{12}$. ▲

The following corollary follows immediately from Theorem 6.15.

6.17 Corollary If a is a generator of a finite cyclic group G of order n, then the other generators of G are the elements of the form a^r, where r is relatively prime to n.

6.18 Example Let us find all subgroups of $\mathbb{Z}_{18}$ and give their subgroup diagram. All subgroups are cyclic. By Corollary 6.17, the elements 1, 5, 7, 11, 13, and 17 are all generators of $\mathbb{Z}_{18}$. Starting with 2,

$$\langle 2\rangle = \{0, 2, 4, 6, 8, 10, 12, 14, 16\}.$$

is of order 9 and has as generators elements of the form $h2$, where h is relatively prime to 9, namely, $h = 1, 2, 4, 5, 7$, and 8, so $h2 = 2, 4, 8, 10, 14$, and 16. The element 6 of $\langle 2\rangle$ generates {0, 6, 12}, and 12 also is a generator of this subgroup.

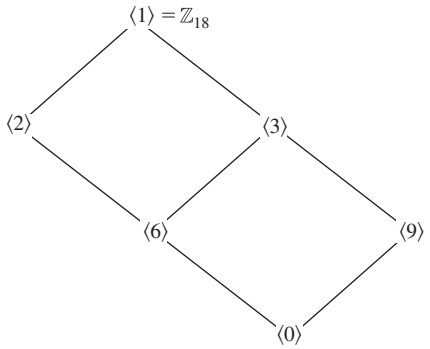
We have thus far found all subgroups generated by 0, 1, 2, 4, 5, 6, 7, 8, 10, 11, 12, 13, 14, 16, and 17. This leaves just 3, 9, and 15 to consider.

$$\langle 3\rangle = \{0, 3, 6, 9, 12, 15\},$$

and 15 also generates this group of order 6, since $15 = 5 \cdot 3$, and the gcd of 5 and 6 is 1. Finally,

$$\langle 9\rangle = \{0, 9\}.$$

The subgroup diagram for these subgroups of $\mathbb{Z}_{18}$ is given in Fig. 6.19.



6.19 Figure Subgroup diagram for $\mathbb{Z}_{18}$.

This example is straightforward; we are afraid we wrote it out in such detail that it may look complicated. The exercises give some practice along these lines. ▲

6.20 Corollary Let G be a finite cyclic group and $H \leq G$. Then $|H|$ divides $|G|$. That is, $|G|$ is a multiple of $|H|$.

Proof Let g be a generator for G and let $n = |G|$. By Theorem 6.6, H is cyclic, so there is an element in $h \in H$ such that h generates H. Since $h \in H \leq G$, $h = g^s$ for some s. Theorem 6.15 states that

$$|H| = \frac{n}{\gcd(n, s)}$$

which is a divisor of n. ◆

6.21 Example We find all orders of the subgroups of $\mathbb{Z}_{28}$. Factoring gives $28 = 2^2 \cdot 7$, so the possible orders of subgroups of the cyclic group $\mathbb{Z}_{28}$ are 1, 2, 4, 7, 14, and 28. We note that $|\langle 0\rangle| = 1$, $|\langle 14\rangle| = 2$, $|\langle 7\rangle| = 4$, $|\langle 4\rangle| = 7$, $|\langle 2\rangle| = 14$, $|\langle 1\rangle| = |\mathbb{Z}_{28}| = 28$. So there are subgroups of order 1, 2, 4, 7, 14, and 28. ▲

Actually, Corollary 6.20 can be strengthened considerably. The assumption that G is cyclic is completely unnecessary. As we will see in Section 10, Lagrange's Theorem states that for any finite group, the order of a subgroup divides the order of the group.

EXERCISES 6

Computations

In Exercises 1 through 4, find the quotient and remainder, according to the division algorithm, when n is divided by m.

1. $n = 42, m = 9$

2. $n = -42, m = 9$

3. $n = -37, m = 8$

4. $n = 37, m = 8$

In Exercises 5 through 7, find the greatest common divisor of the two integers.

5. 32 and 24

6. 48 and 88

7. 360 and 420

In Exercises 8 through 11, find the number of generators of a cyclic group having the given order.

8. 5

9. 8

10. 24

11. 84

An isomorphism of a group with itself is an **automorphism of the group.** In Exercises 12 through 16, find the number of automorphisms of the given group.
[*Hint:* You may use Exercise 53. What must be the image of a generator under an automorphism?]

12. $\mathbb{Z}_2$

13. $\mathbb{Z}_6$

14. $\mathbb{Z}_8$

15. $\mathbb{Z}$

16. $\mathbb{Z}_{84}$

In Exercises 17 through 23, find the number of elements in the indicated cyclic group.

17. The cyclic subgroup of $\mathbb{Z}_{30}$ generated by 25

18. The cyclic subgroup of $\mathbb{Z}_{42}$ generated by 30

19. The cyclic subgroup $\langle i \rangle$ of the group $\mathbb{C}^*$ of nonzero complex numbers under multiplication

20. The cyclic subgroup of the group $\mathbb{C}^*$ of Exercise 19 generated by $(1 + i)/\sqrt{2}$

21. The cyclic subgroup of the group $\mathbb{C}^*$ of Exercise 19 generated by $1 + i$

22. The cyclic subgroup $\langle \rho^{10} \rangle$ of D_{24}

23. The cyclic subgoup $\langle \rho^{35} \rangle$ of D_{375}

24. Consider the group S_{10}

- **a.** What is the order of the cycle $(2, 4, 6, 7)$?
- **b.** What is the order of $(1, 4)(2, 3, 5)$? Of $(1, 3)(2, 4, 6, 7, 8)$?
- **c.** What is the order of $(1, 5, 9)(2, 6, 7)$? Of $(1, 3)(2, 5, 6, 8)$?
- **d.** What is the order of $(1, 2)(3, 4, 5, 6, 7, 8)$? Of $(1, 2, 3)(4, 5, 6, 7, 8, 9)$?
- **e.** State a theorem suggested by parts (c) and (d). [Hint: The important words you are looking for are *least common multiple*.]

In Exercises 25 through 30, find the maximum possibe order for an element of S_n for a given value of n.

25. $n = 5$

26. $n = 6$

27. $n = 7$

28. $n = 8$

29. $n = 10$

30. $n = 15$

In Exercises 31 through 33, find all subgroups of the given group, and draw the subgroup diagram for the subgroups.

31. $\mathbb{Z}_{12}$

32. $\mathbb{Z}_{36}$

33. $\mathbb{Z}_8$

In Exercises 34 through 38, find all orders of subgroups of the given group.

34. $\mathbb{Z}_6$

35. $\mathbb{Z}_8$

36. $\mathbb{Z}_{12}$

37. $\mathbb{Z}_{20}$

38. $\mathbb{Z}_{17}$

Concepts

In Exercises 39 and 40, 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.

39. An element a of a group G has *order* $n \in \mathbb{Z}^+$ if and only if $a^n = e$.

40. The *greatest common divisor* of two positive integers is the largest positive integer that divides both of them.

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

a. Every cyclic group is abelian.
b. Every abelian group is cyclic.
c. $\mathbb{Q}$ under addition is a cyclic group.
d. Every element of every cyclic group generates the group.
e. There is at least one abelian group of every finite order >0.
f. Every group of order ≤ 4 is cyclic.
g. All generators of $\mathbb{Z}_{20}$ are prime numbers.
h. If G and G' are groups, then $G \cap G'$ is a group.
i. If H and K are subgroups of a group G, then $H \cap K$ is a group.
j. Every cyclic group of order >2 has at least two distinct generators.

In Exercises 42 through 46, either give an example of a group with the property described, or explain why no example exists.

42. A finite abelian group that is not cyclic

43. An infinite group that is not cyclic

44. A cyclic group having only one generator

45. An infinite cyclic group having four generators

46. A finite cyclic group having four generators

The generators of the cyclic multiplicative group U_n of all nth roots of unity in $\mathbb{C}$ are the **primitive** nth **roots of unity**. In Exercises 47 through 50, find the primitive nth roots of unity for the given value of n.

47. $n = 4$

48. $n = 6$

49. $n = 8$

50. $n = 12$

Proof Synopsis

51. Give a one-sentence synopsis of the proof of Theorem 6.1.

52. Give at most a three-sentence synopsis of the proof of Theorem 6.6.

Theory

53. Let G be a cyclic group with generator a, and let G' be a group isomorphic to G. If $\phi : G \to G'$ is an isomorphism, show that, for every $x \in G, \phi(x)$ is completely determined by the value $\phi(a)$. That is, if $\phi : G \to G'$ and $\psi : G \to G'$ are two isomophisms such that $\phi(a) = \psi(a)$, then $\phi(x) = \psi(x)$ for all $x \in G$.

54. Let r and s be integers. Show that $\{nr + ms \mid n, m \in \mathbb{Z}\}$ is a subgroup of $\mathbb{Z}$.

55. Prove that if G is a finite cyclic group, H and K are subgroups of G, and $H \neq K$, then $|H| \neq |K|$.

56. Let a and b be elements of a group G. Show that if ab has finite order n, then ba also has order n.

57. Let r and s be positive integers.

a. Define the **least common multiple** of r and s as a generator of a certain cyclic group.
b. Under what condition is the least common multiple of r and s their product, rs?
c. Generalizing part (b), show that the product of the greatest common divisor and of the least common multiple of r and s is rs.

58. Show that a group that has only a finite number of subgroups must be a finite group.

59. Show by a counterexample that the following "converse" of Theorem 6.6 is not a theorem: "If a group G is such that every proper subgroup is cyclic, then G is cyclic."

60. Let G be a group and suppose $a \in G$ generates a cyclic subgroup of order 2 and is the *unique* such element. Show that $ax = xa$ for all $x \in G$. [*Hint:* Consider $(xax^{-1})^2$.]

61. Prove that if G is a cyclic group with an odd number of generators, then G has two elements.

62. Let p and q be distinct prime numbers. Find the number of generators of the cyclic group $\mathbb{Z}_{pq}$.

63. Let p be a prime number. Find the number of generators of the cyclic group $\mathbb{Z}_{p^r}$, where r is an integer ≥ 1.

64. Show that in a finite cyclic group G of order n, written multiplicatively, the equation $x^m = e$ has exactly m solutions x in G for each positive integer m that divides n.

65. With reference to Exercise 64, what is the situation if $1 < m < n$ and m does not divide n?

66. Show that $\mathbb{Z}_p$ has no proper nontrivial subgroups if p is a prime number.

67. Let G be an abelian group and let H and K be finite cyclic subgroups with $|H| = r$ and $|K| = s$.

a. Show that if r and s are relatively prime, then G contains a cyclic subgroup of order rs.

b. Generalizing part (a), show that G contains a cyclic subgroup of order the least common multiple of r and s.

SECTION 7 GENERATING SETS AND CAYLEY DIGRAPHS

Let G be a group, and let $a \in G$. We have described the cyclic subgroup $\langle a \rangle$ of G, which is the smallest subgroup of G that contains the element a. Suppose we want to find as small a subgroup as possible that contains both a and b for another element b in G. By Theorem 5.19, we see that any subgroup containing a and b must contain a^n and b^m for all $m, n \in \mathbb{Z}$, and consequently must contain all finite products of such powers of a and b. For example, such an expression might be $a^2b^4a^{-3}b^2a^5$. Note that we cannot "simplify" this expression by writing first all powers of a followed by the powers of b, since G may not be abelian. However, products of such expressions are again expressions of the same type. Furthermore, $e = a^0$ and the inverse of such an expression is again of the same type. For example, the inverse of $a^2b^4a^{-3}b^2a^5$ is $a^{-5}b^{-2}a^3b^{-4}a^{-2}$. By Theorem 5.12, this shows that all such products of integral powers of a and b form a subgroup of G, which surely must be the smallest subgroup containing both a and b. We call a and b **generators** of this subgroup. If this subgroup should be all of G, then we say that $\{a, b\}$ **generates** G. Of course, there is nothing sacred about taking just two elements $a, b \in G$. We could have made similar arguments for three, four, or any number of elements of G, as long as we take only finite products of their integral powers.

7.1 Example As we have seen, the dihedral group is generated by $\{\mu, \rho\}$ since every element in D_n can be written in the form ρ^k or $\mu\rho^k$ for $0 \leq k < n$. Also, $\{\mu, \mu\rho\}$ generates D_n since $\rho = \mu(\mu\rho)$, so any element in the dihedral group can also be written as a product of copies of μ and $\mu\rho$. It is interesting to note that both μ and $\mu\rho$ have order 2, while in the generating set $\{\mu, \rho\}$ one element has order 2, but the other has order n. ▲

7.2 Example The Klein 4-group $V = \{e, a, b, c\}$ of Example 5.7 is generated by $\{a, b\}$ since $ab = c$. It is also generated by $\{a, c\}$, $\{b, c\}$, and $\{a, b, c\}$. If a group G is generated by a subset S, then every subset of G containing S generates G. ▲

7.3 Example The group $\mathbb{Z}_6$ is generated by $\{1\}$ and $\{5\}$. It is also generated by $\{2, 3\}$ since $2 + 3 = 5$, so that any subgroup containing 2 and 3 must contain 5 and must therefore be $\mathbb{Z}_6$. It is also generated by $\{3, 4\}$, $\{2, 3, 4\}$, $\{1, 3\}$, and $\{3, 5\}$, but it is not generated by $\{2, 4\}$ since $\langle 2 \rangle = \{0, 2, 4\}$ contains 2 and 4. ▲