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. $n = -50, m = 8$

4. $n = 50, m = 8$

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. 12

11. 60

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:* Make use of Exercise 44. 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. $\mathbb{Z}_{12}$

In Exercises 17 through 21, 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 $1 + i$

In Exercises 22 through 24, find all subgroups of the given group, and draw the subgroup diagram for the subgroups.

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

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

24. $\mathbb{Z}_8$

In Exercises 25 through 29, find all orders of subgroups of the given group.

25. $\mathbb{Z}_6$

26. $\mathbb{Z}_8$

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

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

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

Concepts

In Exercises 30 and 31, 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.

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

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

32. Mark each of the following 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 33 through 37, either give an example of a group with the property described, or explain why no example exists.

33. A finite group that is not cyclic

34. An infinite group that is not cyclic

35. A cyclic group having only one generator

36. An infinite cyclic group having four generators

37. 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 38 through 41, find the primitive nth roots of unity for the given value of n.

38. $n = 4$

39. $n = 6$

40. $n = 8$

41. $n = 12$

Proof Synopsis

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

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

Theory

44. 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 $x \in G$.

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

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

47. 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.

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

49. 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."

50. 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 $(xax^{-1})^2$.]

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

52. 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.

53. 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.

54. With reference to Exercise 53, what is the situation if $1 < m < n$ and m does not divide n?

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

56. 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 5.17, 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 5.14, 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 The Klein 4-group $V = \{e, a, b, c\}$ of Example 5.9 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. ▲

7.2 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. ▲

We have given an intuitive explanation of the subgroup of a group G generated by a subset of G. What follows is a detailed exposition of the same idea approached in another way, namely via intersections of subgroups. After we get an intuitive grasp of a concept, it is nice to try to write it up as neatly as possible. We give a set-theoretic definition and generalize a theorem that was in Exercise 54 of Section 5.