Theorem 10.10, the order $m \geq 2$ of $\langle a \rangle$ must divide the prime p. Thus we must have $m = p$ and $\langle a \rangle = G$, so G is cyclic. ◆

Since every cyclic group of order p is isomorphic to $\mathbb{Z}_p$, we see that *there is only one group structure, up to isomorphism, of a given prime order* p. Now doesn't this elegant result follow easily from the theorem of Lagrange, a *counting* theorem? *Never underestimate a theorem that counts something.* Proving the preceding corollary is a favorite examination question.

10.12 Theorem The order of an element of a finite group divides the order of the group.

Proof Remembering that the order of an element is the same as the order of the cyclic subgroup generated by the element, we see that this theorem follows directly from Theorem 10.10. ◆

10.13 Definition Let H be a subgroup of a group G. The number of left cosets of H in G is the **index** $(G : H)$ **of** H **in** G. ■

The index $(G : H)$ just defined may be finite or infinite. If G is finite, then obviously $(G : H)$ is finite and $(G : H) = |G|/|H|$, since every coset of H contains $|H|$ elements. Exercise 35 shows the index $(G : H)$ could be equally well defined as the number of right cosets of H in G. We state a basic theorem concerning indices of subgroups, and leave the proof to the exercises (see Exercise 38).

10.14 Theorem Suppose H and K are subgroups of a group G such that $K \leq H \leq G$, and suppose $(H : K)$ and $(G : H)$ are both finite. Then $(G : K)$ is finite, and $(G : K) = (G : H)(H : K)$.

Theorem 10.10 shows that if there is a subgroup H of a finite group G, then the order of H divides the order of G. Is the converse true? That is, if G is a group of order n, and m divides n, is there always a subgroup of order m? We will see in the next section that this is true for abelian groups. However, A_4 can be shown to have no subgroup of order 6, which gives a counterexample for nonabelian groups.

EXERCISES 10

Computations

1. Find all cosets of the subgroup $4\mathbb{Z}$ of $\mathbb{Z}$.
2. Find all cosets of the subgroup $4\mathbb{Z}$ of $2\mathbb{Z}$.
3. Find all cosets of the subgroup $\langle 2 \rangle$ of $\mathbb{Z}_{12}$.
4. Find all cosets of the subgroup $\langle 4 \rangle$ of $\mathbb{Z}_{12}$.
5. Find all cosets of the subgroup $\langle 18 \rangle$ of $\mathbb{Z}_{36}$.
6. Find all left cosets of the subgroup $\{\rho_0, \mu_2\}$ of the group D_4 given by Table 8.12.
7. Repeat the preceding exercise, but find the right cosets this time. Are they the same as the left cosets?

8. Rewrite Table 8.12 in the order exhibited by the left cosets in Exercise 6. Do you seem to get a coset group of order 4? If so, is it isomorphic to $\mathbb{Z}_4$ or to the Klein 4-group V?

9. Repeat Exercise 6 for the subgroup $\{\rho_0, \rho_2\}$ of D_4.

10. Repeat the preceding exercise, but find the right cosets this time. Are they the same as the left coset?

11. Rewrite Table 8.12 in the order exhibited by the left cosets in Exercise 9. Do you seem to get a coset group of order 4? If so, is it isomorphic to $\mathbb{Z}_4$ or to the Klein 4-group V?

12. Find the index of $\langle 3 \rangle$ in the group $\mathbb{Z}_{24}$.

13. Find the index of $\langle \mu_1 \rangle$ in the group S_3, using the notation of Example 10.7

14. Find the index of $\langle \mu_2 \rangle$ in the group D_4 given in Table 8.12

15. Let $\sigma = (1, 2, 5, 4)(2, 3)$ in S_5. Find the index of $\langle \sigma \rangle$ in S_5.

16. Let $\mu = (1, 2, 4, 5)(3, 6)$ in S_6. Find the index of $\langle \mu \rangle$ in S_6.

Concepts

In Exercises 17 and 18, 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.

17. Let G be a group and let $H \subseteq G$. The *left coset of H containing a* is $aH = \{ah \mid h \in H\}$.

18. Let G be a group and let $H \leq G$. The *index of H in G* is the number of right cosets of H in G.

19. Mark each of the following true or false.

_______ **a.** Every subgroup of every group has left cosets.

_______ **b.** The number of left cosets of a subgroup of a finite group divides the order of the group.

_______ **c.** Every group of prime order is abelian.

_______ **d.** One cannot have left cosets of a finite subgroup of an infinite group.

_______ **e.** A subgroup of a group is a left coset of itself.

_______ **f.** Only subgroups of finite groups can have left cosets.

_______ **g.** A_n is of index 2 in S_n for $n > 1$.

_______ **h.** The theorem of Lagrange is a nice result.

_______ **i.** Every finite group contains an element of every order that divides the order of the group.

_______ **j.** Every finite cyclic group contains an element of every order that divides the order of the group.

In Exercises 20 through 24, give an example of the desired subgroup and group if possible. If impossible, say why it is impossible.

20. A subgroup of an abelian group G whose left cosets and right cosets give different partitions of G

21. A subgroup of a group G whose left cosets give a partition of G into just one cell

22. A subgroup of a group of order 6 whose left cosets give a partition of the group into 6 cells

23. A subgroup of a group of order 6 whose left cosets give a partition of the group into 12 cells

24. A subgroup of a group of order 6 whose left cosets give a partition of the group into 4 cells

Proof Synopsis

25. Give a one-sentence synopsis of the proof of Theorem 10.10.

Theory

26. Prove that the relation $\sim_R$ of Theorem 10.1 is an equivalence relation.

27. Let H be a subgroup of a group G and let $g \in G$. Define a one-to-one map of H onto Hg. Prove that your map is one to one and is onto Hg.

28. Let H be a subgroup of a group G such that $g^{-1}hg \in H$ for all $g \in G$ and all $h \in H$. Show that every left coset gH is the same as the right coset Hg.

29. Let H be a subgroup of a group G. Prove that if the partition of G into left cosets of H is the same as the partition into right cosets of H, then $g^{-1}hg \in H$ for all $g \in G$ and all $h \in H$. (Note that this is the converse of Exercise 28.)

Let H be a subgroup of a group G and let $a, b \in G$. In Exercises 30 through 33 prove the statement or give a counterexample.

30. If $aH = bH$, then $Ha = Hb$.

31. If $Ha = Hb$, then $b \in Ha$.

32. If $aH = bH$, then $Ha^{-1} = Hb^{-1}$.

33. If $aH = bH$, then $a^2H = b^2H$.

34. Let G be a group of order pq, where p and q are prime numbers. Show that every proper subgroup of G is cyclic.

35. Show that there are the same number of left as right cosets of a subgroup H of a group G; that is, exhibit a one-to-one map of the collection of left cosets onto the collection of right cosets. (Note that this result is obvious by counting for finite groups. Your proof must hold for any group.)

36. Exercise 29 of Section 4 showed that every finite group of even order $2n$ contains an element of order 2. Using the theorem of Lagrange, show that if n is odd, then an abelian group of order $2n$ contains precisely one element of order 2.

37. Show that a group with at least two elements but with no proper nontrivial subgroups must be finite and of prime order.

38. Prove Theorem 10.14 [*Hint:* Let $\{a_iH \mid i = 1, \cdots, r\}$ be the collection of distinct left cosets of H in G and $\{b_jK \mid j = 1, \cdots, s\}$ be the collection of distinct left cosets of K in H. Show that

$$\{(a_ib_j)K \mid i = 1, \cdots, r; j = 1, \cdots, s\}$$

is the collection of distinct left cosets of K in G.]

39. Show that if H is a subgroup of index 2 in a finite group G, then every left coset of H is also a right coset of H.

40. Show that if a group G with identity e has finite order n, then $a^n = e$ for all $a \in G$.

41. Show that every left coset of the subgroup $\mathbb{Z}$ of the additive group of real numbers contains exactly one element x such that $0 \leq x < 1$.

42. Show that the function *sine* assigns the same value to each element of any fixed left coset of the subgroup $\langle 2\pi \rangle$ of the additive group $\mathbb{R}$ of real numbers. (Thus *sine* induces a well-defined function on the set of cosets; the value of the function on a coset is obtained when we choose an element x of the coset and compute $\sin x$.)

43. Let H and K be subgroups of a group G. Define $\sim$ on G by $a \sim b$ if and only if $a = hbk$ for some $h \in H$ and some $k \in K$.

a. Prove that $\sim$ is an equivalence relation on G.

b. Describe the elements in the equivalence class containing $a \in G$. (These equivalence classes are called **double cosets.**)

44. Let S_A be the group of all permutations of the set A, and let c be one particular element of A.

a. Show that $\{\sigma \in S_A \mid \sigma(c) = c\}$ is a subgroup $S_{c,c}$ of S_A.

b. Let $d \neq c$ be another particular element of A. Is $S_{c,d} = \{\sigma \in S_A \mid \sigma(c) = d\}$ a subgroup of S_A? Why or why not?

c. Characterize the set $S_{c,d}$ of part (b) in terms of the subgroup $S_{c,c}$ of part (a).

45. Show that a finite cyclic group of order n has exactly one subgroup of each order d dividing n, and that these are all the subgroups it has.

46. The **Euler phi-function** is defined for positive integers n by $\varphi(n) = s$, where s is the number of positive integers less than or equal to n that are relatively prime to n. Use Exercise 45 to show that

$$n = \sum_{d \mid n} \varphi(d),$$

the sum being taken over all positive integers d dividing n. [*Hint:* Note that the number of generators of $\mathbb{Z}_d$ is $\varphi(d)$ by Corollary 6.16.]

47. Let G be a finite group. Show that if for each positive integer m the number of solutions x of the equation $x^m = e$ in G is at most m, then G is cyclic. [*Hint:* Use Theorem 10.12 and Exercise 46 to show that G must contain an element of order $n = |G|$.]

SECTION 11 Direct Products and Finitely Generated Abelian Groups

Direct Products

Let us take a moment to review our present stockpile of groups. Starting with finite groups, we have the cyclic group $\mathbb{Z}_n$, the symmetric group S_n, and the alternating group A_n for each positive integer n. We also have the dihedral groups D_n of Section 8, and the Klein 4-group V. Of course we know that subgroups of these groups exist. Turning to infinite groups, we have groups consisting of sets of numbers under the usual addition or multiplication, as, for example, $\mathbb{Z}$, $\mathbb{R}$, and $\mathbb{C}$ under addition, and their nonzero elements under multiplication. We have the group U of complex numbers of magnitude 1 under multiplication, which is isomorphic to each of the groups $\mathbb{R}_c$ under addition modulo c, where $c \in \mathbb{R}^+$. We also have the group S_A of all permutations of an infinite set A, as well as various groups formed from matrices.

One purpose of this section is to show a way to use known groups as building blocks to form more groups. The Klein 4-group will be recovered in this way from the cyclic groups. Employing this procedure with the cyclic groups gives us a large class of abelian groups that can be shown to include all possible structure types for a finite abelian group. We start by generalizing Definition 0.4.

11.1 Definition The **Cartesian product of sets** $S_1, S_2, \cdots, S_n$ is the set of all ordered n-tuples $(a_1, a_2, \cdots, a_n)$, where $a_i \in S_i$ for $i = 1, 2, \cdots, n$. The Cartesian product is denoted by either

$$S_1 \times S_2 \times \cdots \times S_n$$

or by

$$\prod_{i=1}^{n} S_i. \qquad \blacksquare$$

We could also define the Cartesian product of an infinite number of sets, but the definition is considerably more sophisticated and we shall not need it.

Now let $G_1, G_2, \cdots, G_n$ be groups, and let us use multiplicative notation for all the group operations. Regarding the G_i as sets, we can form $\prod_{i=1}^{n} G_i$. Let us show that we can make $\prod_{i=1}^{n} G_i$ into a group by means of a binary operation of *multiplication by*