Exercises sec. 11 HW3 marked in sec. 11

where not all primes p_i need be distinct. Since $(p_1)^{r_1}(p_2)^{r_2}\cdots(p_n)^{r_n}$ is the order of G, then m must be of the form $(p_1)^{s_1}(p_2)^{s_2}\cdots(p_n)^{s_n}$, where $0 \le s_i \le r_i$. By Theorem 6.14, $(p_i)^{r_i-s_i}$ generates a cyclic subgroup of $\mathbb{Z}_{(p_i)^{r_i}}$ of order equal to the quotient of $(p_i)^{r_i}$ by the gcd of $(p_i)^{r_i}$ and $(p_i)^{r_i-s_i}$. But the gcd of $(p_i)^{r_i}$ and $(p_i)^{r_i-s_i}$ is $(p_i)^{r_i-s_i}$. Thus $(p_i)^{r_i-s_i}$ generates a cyclic subgroup $\mathbb{Z}_{(p_i)^{r_i}}$ of order

$$[(p_i)^{r_i}]/[(p_i)^{r_i-s_i}] = (p_i)^{s_i}.$$

Recalling that $\langle a\rangle$ denotes the cyclic subgroup generated by a, we see that

$$\langle (p_1)^{r_1-s_1}\rangle \times \langle (p_2)^{r_2-s_2}\rangle \times \cdots \times \langle (p_n)^{r_n-s_n}\rangle$$

is the required subgroup of order m. ◆

11.17 Theorem If m is a square free integer, that is, m is not divisible by the square of any prime, then every abelian group of order m is cyclic.

Proof Let G be an abelian group of square free order m. Then by Theorem 11.12, G is isomorphic to

$$\mathbb{Z}_{(p_1)^{r_1}} \times \mathbb{Z}_{(p_2)^{r_2}} \times \cdots \times \mathbb{Z}_{(p_n)^{r_n}},$$

where $m = (p_1)^{r_1}(p_2)^{r_2}\cdots(p_n)^{r_n}$. Since m is square free, we must have all $r_i = 1$ and all p_i distinct primes. Corollary 11.6 then shows that G is isomorphic to $\mathbb{Z}_{p_1p_2\cdots p_n}$, so G is cyclic. ◆

EXERCISES 11

Computations

1. List the elements of $\mathbb{Z}_2 \times \mathbb{Z}_4$. Find the order of each of the elements. Is this group cyclic?

2. Repeat Exercise 1 for the group $\mathbb{Z}_3 \times \mathbb{Z}_4$.

In Exercises 3 through 7, find the order of the given element of the direct product.

3. (2, 6) in $\mathbb{Z}_4 \times \mathbb{Z}_{12}$

4. (2, 3) in $\mathbb{Z}_6 \times \mathbb{Z}_{15}$

5. (8, 10) in $\mathbb{Z}_{12} \times \mathbb{Z}_{18}$

6. (3, 10, 9) in $\mathbb{Z}_4 \times \mathbb{Z}_{12} \times \mathbb{Z}_{15}$

7. (3, 6, 12, 16) in $\mathbb{Z}_4 \times \mathbb{Z}_{12} \times \mathbb{Z}_{20} \times \mathbb{Z}_{24}$

8. What is the largest order among the orders of all the cyclic subgroups of $\mathbb{Z}_6 \times \mathbb{Z}_8$? of $\mathbb{Z}_{12} \times \mathbb{Z}_{15}$?

9. Find all proper nontrivial subgroups of $\mathbb{Z}_2 \times \mathbb{Z}_2$.

10. Find all proper nontrivial subgroups of $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

11. Find all subgroups of $\mathbb{Z}_2 \times \mathbb{Z}_4$ of order 4.

12. Find all subgroups of $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4$ that are isomorphic to the Klein 4-group.

13. Disregarding the order of the factors, write direct products of two or more groups of the form $\mathbb{Z}_n$ so that the resulting product is isomorphic to $\mathbb{Z}_{60}$ in as many ways as possible.

14. Fill in the blanks.

a. The cyclic subgroup of $\mathbb{Z}_{24}$ generated by 18 has order___.

b. $\mathbb{Z}_3 \times \mathbb{Z}_4$ is of order___.

c. The element (4, 2) of $\mathbb{Z}_{12} \times \mathbb{Z}_8$ has order___.

d. The Klein 4-group is isomorphic to $\mathbb{Z}$___ $\times$ $\mathbb{Z}$___.

e. $\mathbb{Z}_2 \times \mathbb{Z} \times \mathbb{Z}_4$ has___elements of finite order.

15. Find the maximum possible order for some element of $\mathbb{Z}_4 \times \mathbb{Z}_6$.

16. Are the groups $\mathbb{Z}_2 \times \mathbb{Z}_{12}$ and $\mathbb{Z}_4 \times \mathbb{Z}_6$ isomorphic? Why or why not?

17. Find the maximum possible order for some element of $\mathbb{Z}_8 \times \mathbb{Z}_{10} \times \mathbb{Z}_{24}$.

18. Are the groups $\mathbb{Z}_8 \times \mathbb{Z}_{10} \times \mathbb{Z}_{24}$ and $\mathbb{Z}_4 \times \mathbb{Z}_{12} \times \mathbb{Z}_{40}$ isomorphic? Why or why not?

19. Find the maximum possible order for some element of $\mathbb{Z}_4 \times \mathbb{Z}_{18} \times \mathbb{Z}_{15}$.

20. Are the groups $\mathbb{Z}_4 \times \mathbb{Z}_{18} \times \mathbb{Z}_{15}$ and $\mathbb{Z}_3 \times \mathbb{Z}_{36} \times \mathbb{Z}_{10}$ isomorphic? Why or why not?

In Exercises 21 through 25, proceed as in Example 11.13 to find all abelian groups, up to isomorphism, of the given order.

21. Order 8

22. Order 16

23. Order 32

24. Order 720

25. Order 1089

26. How many abelian groups (up to isomorphism) are there of order 24? of order 25? of order (24)(25)?

27. Following the idea suggested in Exercise 26, let m and n be relatively prime positive integers. Show that if there are (up to isomorphism) r abelian groups of order m and s of order n, then there are (up to isomorphism) rs abelian groups of order mn.

28. Use Exercise 27 to determine the number of abelian groups (up to isomorphism) of order $(10)^5$.

29. **a.** Let p be a prime number. Fill in the second row of the table to give the number of abelian groups of order p^n, up to isomorphism.

n	2	3	4	5	6	7	8
number of groups							

b. Let p, q, and r be distinct prime numbers. Use the table you created to find the number of abelian groups, up to isomorphism, of the given order.

i. $p^3q^4r^7$ **ii.** $(qr)^7$ **iii.** $q^5r^4q^3$

30. Indicate schematically a Cayley digraph for $\mathbb{Z}_m \times \mathbb{Z}_n$ for the generating set $S = \{(1, 0), (0, 1)\}$.

31. Consider Cayley digraphs with two arc types, a solid one with an arrow and a dashed one with no arrow, and consisting of two regular n-gons, for $n \geq 3$, with solid arc sides, one inside the other, with dashed arcs joining the vertices of the outer n-gon to the inner one. Figure 7.9(b) shows such a Cayley digraph with $n = 3$, and Figure 7.11(b) shows one with $n = 4$. The arrows on the outer n-gon may have the same (clockwise or counterclockwise) direction as those on the inner n-gon, or they may have the opposite direction. Let G be a group with such a Cayley digraph.

a. Under what circumstances will G be abelian?

b. If G is abelian, to what familiar group is it isomorphic?

c. If G is abelian, under what circumstances is it cyclic?

d. If G is not abelian, to what group we have discussed is it isomorphic?

Concepts

32. Mark each of the following true or false.

_____ **a.** If G_1 and G_2 are any groups, then $G_1 \times G_2$ is always isomorphic to $G_2 \times G_1$.

_____ **b.** Computation in an external direct product of groups is easy if you know how to compute in each component group.

_____ **c.** Groups of finite order must be used to form an external direct product.

_____ **d.** A group of prime order could not be the internal direct product of two proper nontrivial subgroups.

_____ **e.** $\mathbb{Z}_2 \times \mathbb{Z}_4$ is isomorphic to $\mathbb{Z}_8$.

_____ **f.** $\mathbb{Z}_2 \times \mathbb{Z}_4$ is isomorphic to S_8.

_____ **g.** $\mathbb{Z}_3 \times \mathbb{Z}_8$ is isomorphic to S_4.

_____ **h.** Every element in $\mathbb{Z}_4 \times \mathbb{Z}_8$ has order 8.

_____ **i.** The order of $\mathbb{Z}_{12} \times \mathbb{Z}_{15}$ is 60.

_____ **j.** $\mathbb{Z}_m \times \mathbb{Z}_n$ has mn elements whether m and n are relatively prime or not.

33. Give an example illustrating that not every nontrivial abelian group is the internal direct product of two proper nontrivial subgroups.

34. a. How many subgroups of $\mathbb{Z}_5 \times \mathbb{Z}_6$ are isomorphic to $\mathbb{Z}_5 \times \mathbb{Z}_6$?

b. How many subgroups of $\mathbb{Z} \times \mathbb{Z}$ are isomorphic to $\mathbb{Z} \times \mathbb{Z}$?

35. Give an example of a nontrivial group that is not of prime order and is not the internal direct product of two nontrivial subgroups.

36. Mark each of the following true or false.

_____ **a.** Every abelian group of prime order is cyclic.

_____ **b.** Every abelian group of prime power order is cyclic.

_____ **c.** $\mathbb{Z}_8$ is generated by $\{4, 6\}$.

_____ **d.** $\mathbb{Z}_8$ is generated by $\{4, 5, 6\}$.

_____ **e.** All finite abelian groups are classified up to isomorphism by Theorem 11.12.

_____ **f.** Any two finitely generated abelian groups with the same Betti number are isomorphic.

_____ **g.** Every abelian group of order divisible by 5 contains a cyclic subgroup of order 5.

_____ **h.** Every abelian group of order divisible by 4 contains a cyclic subgroup of order 4.

_____ **i.** Every abelian group of order divisible by 6 contains a cyclic subgroup of order 6.

_____ **j.** Every finite abelian group has a Betti number of 0.

37. Let p and q be distinct prime numbers. How does the number (up to isomorphism) of abelian groups of order p^r compare with the number (up to isomorphism) of abelian groups of order q^r?

38. Let G be an abelian group of order 72.

a. Can you say how many subgroups of order 8 G has? Why, or why not?

b. Can you say how many subgroups of order 4 G has? Why, or why not?

39. Let G be an abelian group. Show that the elements of finite order in G form a subgroup. This subgroup is called the **torsion subgroup** of G.

Exercises 40 through 43 deal with the concept of the torsion subgroup just defined.

40. Find the order of the torsion subgroup of $\mathbb{Z}_4 \times \mathbb{Z} \times \mathbb{Z}_3$; of $\mathbb{Z}_{12} \times \mathbb{Z} \times \mathbb{Z}_{12}$.

41. Find the torsion subgroup of the multiplicative group $\mathbb{R}^*$ of nonzero real numbers.

42. Find the torsion subgroup T of the multiplicative group $\mathbb{C}^*$ of nonzero complex numbers.

43. An abelian group is **torsion free** if e is the only element of finite order. Use Theorem 11.12 to show that every finitely generated abelian group is the internal direct product of its torsion subgroup and of a torsion-free subgroup. (Note that $\{e\}$ may be the torsion subgroup, and is also torsion free.)

44. The part of the decomposition of G in Theorem 11.12 corresponding to the subgroups of prime-power order can also be written in the form $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_r}$, where m_i divides m_{i+1} for $i = 1, 2, \cdots, r-1$. The numbers m_i can be shown to be unique, and are the **torsion coefficients** of G.

a. Find the torsion coefficients of $\mathbb{Z}_4 \times \mathbb{Z}_9$.

b. Find the torsion coefficients of $\mathbb{Z}_6 \times \mathbb{Z}_{12} \times \mathbb{Z}_{20}$.

c. Describe an algorithm to find the torsion coefficients of a direct product of cyclic groups.

Proof Synopsis

45. Give a two-sentence synopsis of the proof of Theorem 11.5.

Theory

46. Prove that a direct product of abelian groups is abelian.

47. Let G be an abelian group. Let H be the subset of G consisting of the identity e together with all elements of G of order 2. Show that H is a subgroup of G.

48. Following up the idea of Exercise 47 determine whether H will always be a subgroup for every abelian group G if H consists of the identity e together with all elements of G of order 3; of order 4. For what positive integers n will H always be a subgroup for every abelian group G, if H consists of the identity e together with all elements of G of order n? Compare with Exercise 48 of Section 5.

49. Find a counterexample of Exercise 47 with the hypothesis that G is abelian omitted.

Let H and K be subgroups of a group G. Exercises 50 and 51 ask you to establish necessary and sufficient criteria for G to appear as the internal direct product of H and K.

50. Let H and K be groups and let $G = H \times K$. Recall that both H and K appear as subgroups of G in a natural way. Show that these subgroups H (actually $H \times \{e\}$) and K (actually $\{e\} \times K$) have the following properties.

a. Every element of G is of the form hk for some $h \in H$ and $k \in K$.

b. $hk = kh$ for all $h \in H$ and $k \in K$.

c. $H \cap K = \{e\}$.

51. Let H and K be subgroups of a group G satisfying the three properties listed in the preceding exercise. Show that for each $g \in G$, the expression $g = hk$ for $h \in H$ and $k \in K$ is unique. Then let each g be renamed (h, k). Show that, under this renaming, G becomes structurally identical (isomorphic) to $H \times K$.

52. Show that a finite abelian group is not cyclic if and only if it contains a subgroup isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$ for some prime p.

53. Prove that if a finite abelian group has order a power of a prime p, then the order of every element in the group is a power of p. Can the hypothesis of commutativity be dropped? Why, or why not?

54. Let G, H, and K be finitely generated abelian groups. Show that if $G \times K$ is isomorphic to $H \times K$, then $G \simeq H$.

Exercises sec. 13

Ker(ϕ). Section 14 will indicate the importance of the image $\phi[G]$. Exercise 44 asks us to show that if $|G|$ is finite, then $|\phi[G]|$ is finite and is a divisor of $|G|$.

EXERCISES 13

Computations

In Exercises 1 through 15, determine whether the given map ϕ is a homomorphism. [*Hint:* The straightforward way to proceed is to check whether $\phi(ab) = \phi(a)\phi(b)$ for all a and b in the domain of ϕ. However, if we should happen to notice that $\phi^{-1}[\{e'\}]$ is not a subgroup whose left and right cosets coincide, or that ϕ does not satisfy the properties given in Exercise 44 or 45 for finite groups, then we can say at once that ϕ is not a homomorphism.]

1. Let $\phi : \mathbb{Z} \to \mathbb{R}$ under addition be given by $\phi(n) = n$.
2. Let $\phi : \mathbb{R} \to \mathbb{Z}$ under addition be given by $\phi(x) =$ the greatest integer $\leq x$.
3. Let $\phi : \mathbb{R}^* \to \mathbb{R}^*$ under multiplication be given by $\phi(x) = |x|$.
4. Let $\phi : \mathbb{Z}_6 \to \mathbb{Z}_2$ be given by $\phi(x) =$ the remainder of x when divided by 2, as in the division algorithm.
5. Let $\phi : \mathbb{Z}_9 \to \mathbb{Z}_2$ be given by $\phi(x) =$ the remainder of x when divided by 2, as in the division algorithm.
6. Let $\phi : \mathbb{R} \to \mathbb{R}^*$, where $\mathbb{R}$ is additive and $\mathbb{R}^*$ is multiplicative, be given by $\phi(x) = 2^x$.
7. Let $\phi_i : G_i \to G_1 \times G_2 \times \cdots \times G_i \times \cdots \times G_r$ be given by $\phi_i(g_i) = (e_1, e_2, \ldots, g_i, \ldots, e_r)$, where $g_i \in G_i$ and e_j is the identity element of G_j. This is an **injection map**. Compare with Example 13.8.
8. Let G be any group and let $\phi : G \to G$ be given by $\phi(g) = g^{-1}$ for $g \in G$.
9. Let F be the additive group of functions mapping $\mathbb{R}$ into $\mathbb{R}$ having derivatives of all orders. Let $\phi : F \to F$ be given by $\phi(f) = f''$, the second derivative of f.
10. Let F be the additive group of all continuous functions mapping $\mathbb{R}$ into $\mathbb{R}$. Let $\mathbb{R}$ be the additive group of real numbers, and let $\phi : F \to \mathbb{R}$ be given by

$$\phi(f) = \int_0^4 f(x)dx.$$

11. Let F be the additive group of all functions mapping $\mathbb{R}$ into $\mathbb{R}$, and let $\phi : F \to F$ be given by $\phi(f) = 3f$.
12. Let M_n be the additive group of all $n \times n$ matrices with real entries, and let $\mathbb{R}$ be the additive group of real numbers. Let $\phi(A) = \det(A)$, the determinant of A, for $A \in M_n$.
13. Let M_n and $\mathbb{R}$ be as in Exercise 12. Let $\phi(A) = \text{tr}(A)$ for $A \in M_n$, where the **trace** tr(A) is the sum of the elements on the main diagonal of A, from the upper-left to the lower-right corner.
14. Let $GL(n, \mathbb{R})$ be the multiplicative group of invertible $n \times n$ matrices, and let $\mathbb{R}$ be the additive group of real numbers. Let $\phi : GL(n, \mathbb{R}) \to \mathbb{R}$ be given by $\phi(A) = \text{tr}(A)$, where tr(A) is defined in Exercise 13.
15. Let F be the multiplicative group of all continuous functions mapping $\mathbb{R}$ into $\mathbb{R}$ that are nonzero at every $x \in \mathbb{R}$. Let $\mathbb{R}^*$ be the multiplicative group of nonzero real numbers. Let $\phi : F \to \mathbb{R}^*$ be given by $\phi(f) = \int_0^1 f(x)dx$.

In Exercises 16 through 24, compute the indicated quantities for the given homomorphism ϕ. (See Exercise 46.)

16. Ker(ϕ) for $\phi : S_3 \to \mathbb{Z}_2$ in Example 13.3
17. Ker(ϕ) and $\phi(25)$ for $\phi : \mathbb{Z} \to \mathbb{Z}_7$ such that $\phi(1) = 4$
18. Ker(ϕ) and $\phi(18)$ for $\phi : \mathbb{Z} \to \mathbb{Z}_{10}$ such that $\phi(1) = 6$

19. Ker(ϕ) and $\phi(20)$ for $\phi : \mathbb{Z} \to S_8$ such that $\phi(1) = (1, 4, 2, 6)(2, 5, 7)$

20. Ker(ϕ) and $\phi(3)$ for $\phi : \mathbb{Z}_{10} \to \mathbb{Z}_{20}$ such that $\phi(1) = 8$

21. Ker(ϕ) and $\phi(14)$ for $\phi : \mathbb{Z}_{24} \to S_8$ where $\phi(1) = (2, 5)(1, 4, 6, 7)$

22. Ker(ϕ) and $\phi(-3, 2)$ for $\phi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ where $\phi(1, 0) = 3$ and $\phi(0, 1) = -5$

23. Ker(ϕ) and $\phi(4, 6)$ for $\phi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ where $\phi(1, 0) = (2, -3)$ and $\phi(0, 1) = (-1, 5)$

24. Ker(ϕ) and $\phi(3, 10)$ for $\phi : \mathbb{Z} \times \mathbb{Z} \to S_{10}$ where $\phi(1, 0) = (3, 5)(2, 4)$ and $\phi(0, 1) = (1, 7)(6, 10, 8, 9)$

25. How many homomorphisms are there of $\mathbb{Z}$ onto $\mathbb{Z}$?

26. How many homomorphisms are there of $\mathbb{Z}$ into $\mathbb{Z}$?

27. How many homomorphisms are there of $\mathbb{Z}$ into $\mathbb{Z}_2$?

28. Let G be a group, and let $g \in G$. Let $\phi_g : G \to G$ be defined by $\phi_g(x) = gx$ for $x \in G$. For which $g \in G$ is ϕ_g a homomorphism?

29. Let G be a group, and let $g \in G$. Let $\phi_g : G \to G$ be defined by $\phi_g(x) = gxg^{-1}$ for $x \in G$. For which $g \in G$ is ϕ_g a homomorphism?

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. A *homomorphism* is a map such that $\phi(xy) = \phi(x)\phi(y)$.

31. Let $\phi : G \to G'$ be a homomorphism of groups. The *kernel of* ϕ is $\{x \in G \mid \phi(x) = e'\}$ where e' is the identity in G'.

32. Mark each of the following true or false.

_____ **a.** A_n is a normal subgroup of S_n.

_____ **b.** For any two groups G and G', there exists a homomorphism of G into G'.

_____ **c.** Every homomorphism is a one-to-one map.

_____ **d.** A homomorphism is one to one if and only if the kernel consists of the identity element alone.

_____ **e.** The image of a group of 6 elements under some homomorphism may have 4 elements. (See Exercise 44.)

_____ **f.** The image of a group of 6 elements under a homomorphism may have 12 elements.

_____ **g.** There is a homomorphism of some group of 6 elements into some group of 12 elements.

_____ **h.** There is a homomorphism of some groups of 6 elements into some group of 10 elements.

_____ **i.** A homomorphism may have an empty kernel.

_____ **j.** It is not possible to have a nontrivial homomorphism of some finite group into some infinite group.

In Exercises 33 through 43, give an example of a nontrivial homomorphism ϕ for the given groups, if an example exists. If no such homomorphism exists, explain why that is so. You may use Exercises 44 and 45.

33. $\phi : \mathbb{Z}_{12} \to \mathbb{Z}_5$

34. $\phi : \mathbb{Z}_{12} \to \mathbb{Z}_4$

35. $\phi : \mathbb{Z}_2 \times \mathbb{Z}_4 \to \mathbb{Z}_2 \times \mathbb{Z}_5$

36. $\phi : \mathbb{Z}_3 \to \mathbb{Z}$

37. $\phi : \mathbb{Z}_3 \to S_3$

38. $\phi : \mathbb{Z} \to S_3$

39. $\phi : \mathbb{Z} \times \mathbb{Z} \to 2\mathbb{Z}$

40. $\phi : 2\mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$

41. $\phi : D_4 \to S_3$

42. $\phi : S_3 \to S_4$

43. $\phi : S_4 \to S_3$

Several examples from 33-42 for discussion

Theory

44. Let $\phi : G \to G'$ be a group homomorphism. Show that if $|G|$ is finite, then $|\phi[G]|$ is finite and is a divisor of $|G|$.

45. Let $\phi : G \to G'$ be a group homomorphism. Show that if $|G'|$ is finite, then, $|\phi[G]|$ is finite and is a divisor of $|G'|$.

46. Let a group G be generated by $\{a_i \mid i \in I\}$, where I is some indexing set and $a_i \in G$ for all $i \in I$. Let $\phi : G \to G'$ and $\mu : G \to G'$ be two homomorphisms from G into a group G', such that $\phi(a_i) = \mu(a_i)$ for every $i \in I$. Prove that $\phi = \mu$. [Thus, for example, a homomorphism of a cyclic group is completely determined by its value on a generator of the group.] [*Hint*: Use Theorem 7.6 and, of course, Definition 13.1.]

47. Show that any group homomorphism $\phi : G \to G'$ where $|G|$ is a prime must either be the trivial homomorphism or a one-to-one map.

48. The **sign of an even permutation** is $+1$ and the **sign of an odd permutation** is -1. Observe that the map $\text{sgn}_n : S_n \to \{1, -1\}$ defined by

$$\text{sgn}_n(\sigma) = \text{sign of } \sigma$$

is a homomorphism of S_n onto the multiplicative group $\{1, -1\}$. What is the kernel? Compare with Example 13.3.

49. Show that if G, G', and G'' are groups and if $\phi : G \to G'$ and $\gamma : G' \to G''$ are homomorphisms, then the composite map $\gamma\phi : G \to G''$ is a homomorphism.

50. Let $\phi : G \to H$ be a group homomorphism. Show that $\phi[G]$ is abelian if and only if for all $x, y \in G$, we have $xyx^{-1}y^{-1} \in \text{Ker}(\phi)$.

51. Let G be any group and let a be any element of G. Let $\phi : \mathbb{Z} \to G$ be defined by $\phi(n) = a^n$. Show that ϕ is a homomorphism. Describe the image and the possibilities for the kernel of ϕ.

52. Let $\phi : G \to G'$ be a homomorphism with kernel H and let $a \in G$. Prove the set equality $\{x \in G \mid \phi(x) = \phi(a)\} = Ha$.

53. Let G be a group, Let $h, k \in G$ and let $\phi : \mathbb{Z} \times \mathbb{Z} \to G$ be defined by $\phi(m, n) = h^m k^n$. Give a necessary and sufficient condition, involving h and k, for ϕ to be a homomorphism. Prove your condition.

54. Find a necessary and sufficient condition on G such that the map ϕ described in the preceding exercise is a homomorphism for *all* choices of $h, k \in G$.

55. Let G be a group, h an element of G, and n a positive integer. Let $\phi : \mathbb{Z}_n \to G$ be defined by $\phi(i) = h^i$ for $0 \leq i \leq n$. Give a necessary and sufficient condition (in terms of h and n) for ϕ to be a homomorphism. Prove your assertion.

SECTION 14 Factor Groups

Let H be a subgroup of a finite group G. Suppose we write a table for the group operation of G, listing element heads at the top and at the left as they occur in the left cosets of H. We illustrated this in Section 10. The body of the table may break up into blocks corresponding to the cosets (Table 10.5), giving a group operation on the cosets, or they may not break up that way (Table 10.9). We start this section by showing that if H is the kernel of a group homomorphism $\phi : G \to G'$, then the cosets of H (remember that left and right cosets then coincide) are indeed elements of a group whose binary operation is derived from the group operation of G.

Exercises sec. 14

EXERCISES 14

Computations

In Exercises 1 through 8, find the order of the given factor group.

Problems 1-8

1. $\mathbb{Z}_6/\langle 3\rangle$

2. $(\mathbb{Z}_4 \times \mathbb{Z}_{12})/(\langle 2\rangle \times \langle 2\rangle)$

3. $(\mathbb{Z}_4 \times \mathbb{Z}_2)/\langle (2, 1)\rangle$

4. $(\mathbb{Z}_3 \times \mathbb{Z}_5)/(\{0\} \times \mathbb{Z}_5)$

5. $(\mathbb{Z}_2 \times \mathbb{Z}_4)/\langle (1, 1)\rangle$

6. $(\mathbb{Z}_{12} \times \mathbb{Z}_{18})/\langle (4, 3)\rangle$

7. $(\mathbb{Z}_2 \times S_3)/\langle (1, \rho_1)\rangle$

8. $(\mathbb{Z}_{11} \times \mathbb{Z}_{15})/\langle (1, 1)\rangle$

In Exercises 9 through 15, give the order of the element in the factor group.

Problems 9-16

9. $5 + \langle 4\rangle$ in $\mathbb{Z}_{12}/\langle 4\rangle$

10. $26 + \langle 12\rangle$ in $\mathbb{Z}_{60}/\langle 12\rangle$

11. $(2, 1) + \langle (1, 1)\rangle$ in $(\mathbb{Z}_3 \times \mathbb{Z}_6)/\langle (1, 1)\rangle$

12. $(3, 1) + \langle (1, 1)\rangle$ in $(\mathbb{Z}_4 \times \mathbb{Z}_4)/\langle (1, 1)\rangle$

13. $(3, 1) + \langle (0, 2)\rangle$ in $(\mathbb{Z}_4 \times \mathbb{Z}_8)/\langle (0, 2)\rangle$

14. $(3, 3) + \langle (1, 2)\rangle$ in $(\mathbb{Z}_4 \times \mathbb{Z}_8)/\langle (1, 2)\rangle$

15. $(2, 0) + \langle (4, 4)\rangle$ in $(\mathbb{Z}_6 \times \mathbb{Z}_8)/\langle (4, 4)\rangle$

16. Compute $i_{\rho_1}[H]$ for the subgroup $H = \{\rho_0, \mu_1\}$ of the group S_3 of Example 8.7.

Concepts

In Exercises 17 through 19, 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. A *normal subgroup* H of G is one satisfying $hG = Gh$ for all $h \in H$.

18. A *normal subgroup* H of G is one satisfying $g^{-1}hg \in H$ for all $h \in H$ and all $g \in G$.

19. An *automorphism* of a group G is a homomorphism mapping G into G.

20. What is the importance of a *normal* subgroup of a group G?

Students often write nonsense when first proving theorems about factor groups. The next two exercises are designed to call attention to one basic type of error.

21. A student is asked to show that if H is a normal subgroup of an abelian group G, then G/H is abelian. The student's proof starts as follows:

We must show that G/H is abelian. Let a and b be two elements of G/H.

a. Why does the instructor reading this proof expect to find nonsense from here on in the student's paper?

b. What should the student have written?

c. Complete the proof.

22. A **torsion group** is a group all of whose elements have finite order. A group is **torsion free** if the identity is the only element of finite order. A student is asked to prove that if G is a torsion group, then so is G/H for every normal subgroup H of G. The student writes

We must show that each element of G/H is of finite order. Let $x \in G/H$.

Answer the same questions as in Exercise 21.

23. Mark each of the following true or false.

_____ **a.** It makes sense to speak of the factor group G/N if and only if N is a normal subgroup of the group G.

_____ **b.** Every subgroup of an abelian group G is a normal subgroup of G.

_____ **c.** An inner automorphism of an abelian group must be just the identity map.

_____ **d.** Every factor group of a finite group is again of finite order.

_____ **e.** Every factor group of a torsion group is a torsion group. (See Exercise 22.)

_____ **f.** Every factor group of a torsion-free group is torsion free. (See Exercise 22.)

_____ **g.** Every factor group of an abelian group is abelian.

_____ **h.** Every factor group of a nonabelian group is nonabelian.

_____ **i.** $\mathbb{Z}/n\mathbb{Z}$ is cyclic of order n.

_____ **j.** $\mathbb{R}/n\mathbb{R}$ is cyclic of order n, where $n\mathbb{R} = \{nr \mid r \in \mathbb{R}\}$ and $\mathbb{R}$ is under addition.

Theory

24. Show that A_n is a normal subgroup of S_n and compute S_n/A_n; that is, find a known group to which S_n/A_n is isomorphic.

25. Complete the proof of Theorem 14.4 by showing that if H is a subgroup of a group G and if left coset multiplication $(aH)(bH) = (ab)H$ is well defined, then $Ha \subseteq aH$.

26. Prove that the torsion subgroup T of an abelian group G is a normal subgroup of G, and that G/T is torsion free. (See Exercise 22.)

27. A subgroup H is **conjugate to a subgroup** K of a group G if there exists an inner automorphism i_g of G such that $i_g[H] = K$. Show that conjugacy is an equivalence relation on the collection of subgroups of G.

28. Characterize the normal subgroups of a group G in terms of the cells where they appear in the partition given by the conjugacy relation in the preceding exercise.

29. Referring to Exercise 27, find all subgroups of S_3 (Example 8.7) that are conjugate to $\{\rho_0, \mu_2\}$.

30. Let H be a normal subgroup of a group G, and let $m = (G : H)$. Show that $a^m \in H$ for every $a \in G$.

31. Show that an intersection of normal subgroups of a group G is again a normal subgroup of G.

32. Given any subset S of a group G, show that it makes sense to speak of the smallest normal subgroup that contains S. [*Hint:* Use Exercise 31.]

33. Let G be a group. An element of G that can be expressed in the form $aba^{-1}b^{-1}$ for some $a, b \in G$ is a **commutator** in G. The preceding exercise shows that there is a smallest normal subgroup C of a group G containing all commutators in G; the subgroup C is the **commutator subgroup** of G. Show that G/C is an abelian group.

34. Show that if a finite group G has exactly one subgroup H of a given order, then H is a normal subgroup of G.

35. Show that if H and N are subgroups of a group G, and N is normal in G, then $H \cap N$ is normal in H. Show by an example that $H \cap N$ need not be normal in G.

36. Let G be a group containing at least one subgroup of a fixed finite order s. Show that the intersection of all subgroups of G of order s is a normal subgroup of G. [*Hint:* Use the fact that if H has order s, then so does $x^{-1}Hx$ for all $x \in G$.]

37. a. Show that all automorphisms of a group G form a group under function composition.

b. Show that the inner automorphisms of a group G form a normal subgroup of the group of all automorphisms of G under function composition. [*Warning:* Be sure to show that the inner automorphisms do form a subgroup.]

38. Show that the set of all $g \in G$ such that $i_g : G \to G$ is the identity inner automorphism i_e is a normal subgroup of a group G.

39. Let G and G' be groups, and let H and H' be normal subgroups of G and G', respectively. Let ϕ be a homomorphism of G into G'. Show that ϕ induces a natural homomorphism $\phi_* : (G/H) \to (G'/H')$ if $\phi[H] \subseteq H'$. (This fact is used constantly in algebraic topology.)

40. Use the properties $\det(AB) = \det(A) \cdot \det(B)$ and $\det(I_n) = 1$ for $n \times n$ matrices to show the following:

a. The $n \times n$ matrices with determinant 1 form a normal subgroup of $GL(n, \mathbb{R})$.

b. The $n \times n$ matrices with determinant ± 1 form a normal subgroup of $GL(n, \mathbb{R})$.

41. Let G be a group, and let $\mathscr{P}(G)$ be the set of all *subsets* of G. For any $A, B \in \mathscr{P}(G)$, let us define the product subset $AB = \{ab \mid a \in A, b \in B\}$.

a. Show that this multiplication of subsets is associative and has an identity element, but that $\mathscr{P}(G)$ is not a group under this operation.

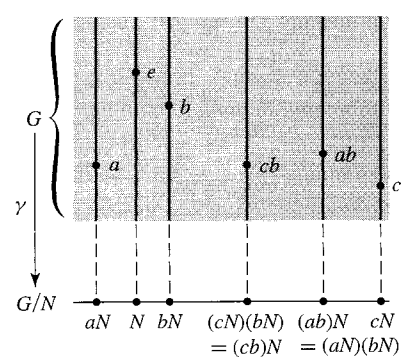
b. Show that if N is a normal subgroup of G, then the set of cosets of N is closed under the above operation on $\mathscr{P}(G)$, and that this operation agrees with the multiplication given by the formula in Corollary 14.5.

c. Show (without using Corollary 14.5) that the cosets of N in G form a group under the above operation. Is its identity element the same as the identity element of $\mathscr{P}(G)$?

SECTION 15 Factor-Group Computations and Simple Groups

Factor groups can be a tough topic for students to grasp. There is nothing like a bit of computation to strengthen understanding in mathematics. We start by attempting to improve our intuition concerning factor groups. Since we will be dealing with normal subgroups throughout this section, we often denote a subgroup of a group G by N rather than by H.

Let N be a normal subgroup of G. In the factor group G/N, the subgroup N acts as identity element. We may regard N as being *collapsed* to a single element, either to 0 in additive notation or to e in multiplicative notation. This collapsing of N together with the algebraic structure of G require that other subsets of G, namely, the cosets of N, also collapse into a single element in the factor group. A visualization of this collapsing is provided by Fig. 15.1. Recall from Theorem 14.9 that $\gamma : G \to G/N$ defined by $\gamma(a) = aN$ for $a \in G$ is a homomorphism of G onto G/N. Figure 15.1 is very similar to Fig. 13.14, but in Fig. 15.1 the image group under the homomorphism is actually formed from G. We can view the "line" G/N at the bottom of the figure as obtained by collapsing to a point each coset of N in another copy of G. Each point of G/N thus corresponds to a whole vertical line segment in the shaded portion, representing a coset of N in G. It is crucial to remember that multiplication of cosets in G/N can be computed by multiplying in G, using any representative elements of the cosets as shown in the figure.



15.1 Figure

Proof The commutators certainly generate a subgroup C; we must show that it is normal in G. Note that the inverse $(aba^{-1}b^{-1})^{-1}$ of a commutator is again a commutator, namely, $bab^{-1}a^{-1}$. Also $e = eee^{-1}e^{-1}$ is a commutator. Theorem 7.6 then shows that C consists precisely of all finite products of commutators. For $x \in C$, we must show that $g^{-1}xg \in C$ for all $g \in G$, or that if x is a product of commutators, so is $g^{-1}xg$ for all $g \in G$. By inserting $e = gg^{-1}$ between each product of commutators occurring in x, we see that it is sufficient to show for each commutator $cdc^{-1}d^{-1}$ that $g^{-1}(cdc^{-1}d^{-1})g$ is in C. But

$$\begin{aligned} g^{-1}(cdc^{-1}d^{-1})g &= (g^{-1}cdc^{-1})(e)(d^{-1}g) \\ &= (g^{-1}cdc^{-1})(gd^{-1}dg^{-1})(d^{-1}g) \\ &= [(g^{-1}c)d(g^{-1}c)^{-1}d^{-1}][dg^{-1}d^{-1}g], \end{aligned}$$

which is in C. Thus C is normal in G.

The rest of the theorem is obvious if we have acquired the proper feeling for factor groups. One doesn't visualize in this way, but writing out that G/C is abelian follows from

$$\begin{aligned} (aC)(bC) &= abC = ab(b^{-1}a^{-1}ba)C \\ &= (abb^{-1}a^{-1})baC = baC = (bC)(aC). \end{aligned}$$

Furthermore, if N is a normal subgroup of G and G/N is abelian, then $(a^{-1}N)(b^{-1}N) = (b^{-1}N)(a^{-1}N)$; that is, $aba^{-1}b^{-1}N = N$, so $aba^{-1}b^{-1} \in N$, and $C \leq N$. Finally, if $C \leq N$, then

$$\begin{aligned} (aN)(bN) &= abN = ab(b^{-1}a^{-1}ba)N \\ &= (abb^{-1}a^{-1})baN = baN = (bN)(aN). \end{aligned}$$

◆

15.21 Example For the group S_3 in Table 8.8, we find that one commutator is $\rho_1\mu_1\rho_1^{-1}\mu_1^{-1} = \rho_1\mu_1\rho_2\mu_1 = \mu_3\mu_2 = \rho_2$. We similarly find that $\rho_2\mu_1\rho_2^{-1}\mu_1^{-1} = \rho_2\mu_1\rho_1\mu_1 = \mu_2\mu_3 = \rho_1$. Thus the commutator subgroup C of S_3 contains A_3. Since A_3 is a normal subgroup of S_3 and S_3/A_3 is abelian, Theorem 15.20 shows that $C = A_3$. ▲

EXERCISES 15

Computations

In Exercises 1 through 12, classify the given group according to the fundamental theorem of finitely generated abelian groups.

1. $(\mathbb{Z}_2 \times \mathbb{Z}_4)/\langle(0, 1)\rangle$

2. $(\mathbb{Z}_2 \times \mathbb{Z}_4)/\langle(0, 2)\rangle$

3. $(\mathbb{Z}_2 \times \mathbb{Z}_4)/\langle(1, 2)\rangle$

4. $(\mathbb{Z}_4 \times \mathbb{Z}_8)/\langle(1, 2)\rangle$

5. $(\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_8)/\langle(1, 2, 4)\rangle$

6. $(\mathbb{Z} \times \mathbb{Z})/\langle(0, 1)\rangle$

7. $(\mathbb{Z} \times \mathbb{Z})/\langle(1, 2)\rangle$

8. $(\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z})/\langle(1, 1, 1)\rangle$

9. $(\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}_4)/\langle(3, 0, 0)\rangle$

10. $(\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}_8)/\langle(0, 4, 0)\rangle$

11. $(\mathbb{Z} \times \mathbb{Z})/\langle(2, 2)\rangle$

12. $(\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z})/\langle(3, 3, 3)\rangle$

13. Find both the center $Z(D_4)$ and the commutator subgroup C of the group D_4 of symmetries of the square in Table 8.12.

14. Find both the center and the commutator subgroup of $\mathbb{Z}_3 \times S_3$.

15. Find both the center and the commutator subgroup of $S_3 \times D_4$.

16. Describe all subgroups of order ≤ 4 of $\mathbb{Z}_4 \times \mathbb{Z}_4$, and in each case classify the factor group of $\mathbb{Z}_4 \times \mathbb{Z}_4$ modulo the subgroup by Theorem 11.12. That is, describe the subgroup and say that the factor group of $\mathbb{Z}_4 \times \mathbb{Z}_4$ modulo the subgroup is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_4$, or whatever the case may be. [*Hint:* $\mathbb{Z}_4 \times \mathbb{Z}_4$ has six different cyclic subgroups of order 4. Describe them by giving a generator, such as the subgroup $\langle (1, 0) \rangle$. There is one subgroup of order 4 that is isomorphic to the Klein 4-group. There are three subgroups of order 2.]

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. The *center* of a group G contains all elements of G that commute with every element of G.

18. The *commutator subgroup* of a group G is $\{a^{-1}b^{-1}ab \mid a, b \in G\}$.

19. Mark each of the following true or false.

_____ **a.** Every factor group of a cyclic group is cyclic.
_____ **b.** A factor group of a noncyclic group is again noncyclic.
_____ **c.** $\mathbb{R}/\mathbb{Z}$ under addition has no element of order 2.
_____ **d.** $\mathbb{R}/\mathbb{Z}$ under addition has elements of order n for all $n \in \mathbb{Z}^+$.
_____ **e.** $\mathbb{R}/\mathbb{Z}$ under addition has an infinite number of elements of order 4.
_____ **f.** If the commutator subgroup C of a group G is $\{e\}$, then G is abelian.
_____ **g.** If G/H is abelian, then the commutator subgroup of C of G contains H.
_____ **h.** The commutator subgroup of a simple group G must be G itself.
_____ **i.** The commutator subgroup of a nonabelian simple group G must be G itself.
_____ **j.** All nontrivial finite simple groups have prime order.

In Exercises 20 through 23, let F be the additive group of all functions mapping $\mathbb{R}$ into $\mathbb{R}$, and let F^* be the multiplicative group of all elements of F that do not assume the value 0 at any point of $\mathbb{R}$.

20. Let K be the subgroup of F consisting of the constant functions. Find a subgroup of F to which F/K is isomorphic.

21. Let K^* be the subgroup of F^* consisting of the nonzero constant functions. Find a subgroup of F^* to which F^*/K^* is isomorphic.

22. Let K be the subgroup of continuous functions in F. Can you find an element of F/K having order 2? Why or why not?

23. Let K^* be the subgroup of F^* consisting of the continuous functions in F^*. Can you find an element of F^*/K^* having order 2? Why or why not?

In Exercises 24 through 26, let U be the multiplicative group $\{z \in \mathbb{C} \mid |z| = 1\}$.

24. Let $z_0 \in U$. Show that $z_0U = \{z_0 z \mid z \in U\}$ is a subgroup of U, and compute U/z_0U.

25. To what group we have mentioned in the text is $U/\langle -1 \rangle$ isomorphic?

26. Let $\zeta_n = \cos(2\pi/n) + i \sin(2\pi/n)$ where $n \in \mathbb{Z}^+$. To what group we have mentioned is $U/\langle \zeta_n \rangle$ isomorphic?

27. To what group mentioned in the text is the additive group $\mathbb{R}/\mathbb{Z}$ isomorphic?

28. Give an example of a group G having no elements of finite order > 1 but having a factor group G/H, all of whose elements are of finite order.

29. Let H and K be normal subgroups of a group G. Give an example showing that we may have $H \simeq K$ while G/H is not isomorphic to G/K.

30. Describe the center of every simple

a. abelian group

b. nonabelian group.

31. Describe the commutator subgroup of every simple

a. abelian group

b. nonabelian group.

Proof Synopsis

32. Give a one-sentence synopsis of the proof of Theorem 15.9.

33. Give at most a two-sentence synopsis of the proof of Theorem 15.18.

Theory

34. Show that if a finite group G contains a nontrivial subgroup of index 2 in G, then G is not simple.

35. Let $\phi : G \to G'$ be a group homomorphism, and let N be a normal subgroup of G. Show that $\phi[N]$ is normal subgroup of $\phi[G]$.

36. Let $\phi : G \to G'$ be a group homomorphism, and let N' be a normal subgroup of G'. Show that $\phi^{-1}[N']$ is a normal subgroup of G.

37. Show that if G is nonabelian, then the factor group $G/Z(G)$ is not cyclic. [*Hint:* Show the equivalent contrapositive, namely, that if $G/Z(G)$ is cyclic then G is abelian (and hence $Z(G) = G$).]

38. Using Exercise 37, show that a nonabelian group G of order pq where p and q are primes has a trivial center.

39. Prove that A_n is simple for $n \geq 5$, following the steps and hints given.

a. Show A_n contains every 3-cycle if $n \geq 3$.

b. Show A_n is generated by the 3-cycles for $n \geq 3$. [*Hint:* Note that $(a, b)(c, d) = (a, c, b)(a, c, d)$ and $(a, c)(a, b) = (a, b, c)$.]

c. Let r and s be fixed elements of $\{1, 2, \cdots, n\}$ for $n \geq 3$. Show that A_n is generated by the n "special" 3-cycles of the form (r, s, i) for $1 \leq i \leq n$ [*Hint:* Show every 3-cycle is the product of "special" 3-cycles by computing

$$(r, s, i)^2, \quad (r, s, j)(r, s, i)^2, \quad (r, s, j)^2(r, s, i),$$

and

$$(r, s, i)^2(r, s, k)(r, s, j)^2(r, s, i).$$

Observe that these products give all possible types of 3-cycles.]

d. Let N be a normal subgroup of A_n for $n \geq 3$. Show that if N contains a 3-cycle, then $N = A_n$. [*Hint:* Show that $(r, s, i) \in N$ implies that $(r, s, j) \in N$ for $j = 1, 2, \cdots, n$ by computing

$$((r, s)(i, j))(r, s, i)^2((r, s)(i, j))^{-1}.]$$

e. Let N be a nontrivial normal subgroup of A_n for $n \geq 5$. Show that one of the following cases must hold, and conclude in each case that $N = A_n$.

Case I N contains a 3-cycle.

Case II N contains a product of disjoint cycles, at least one of which has length greater than 3. [*Hint:* Suppose N contains the disjoint product $\sigma = \mu(a_1, a_2, \cdots, a_r)$. Show $\sigma^{-1}(a_1, a_2, a_3)\sigma(a_1, a_2, a_3)^{-1}$ is in N, and compute it.]

Case III N contains a disjoint product of the form $\sigma = \mu(a_4, a_5, a_6)(a_1, a_2, a_3)$. [*Hint:* Show $\sigma^{-1}(a_1, a_2, a_4)\sigma(a_1, a_2, a_4)^{-1}$ is in N, and compute it.]

Case IV N contains a disjoint product of the form $\sigma = \mu(a_1, a_2, a_3)$ where μ is a product of disjoint 2-cycles. [*Hint:* Show $\sigma^2 \in N$ and compute it.]

Case V N contains a disjoint product σ of the form $\sigma = \mu(a_3, a_4)(a_1, a_2)$, where μ is a product of an even number of disjoint 2-cycles. [*Hint:* Show that $\sigma^{-1}(a_1, a_2, a_3)\sigma(a_1, a_2, a_3)^{-1}$ is in N, and compute it to deduce that $\alpha = (a_2, a_4)(a_1, a_3)$ is in N. Using $n \geq 5$ for the first time, find $i \neq a_1, a_2, a_3, a_4$ in $\{1, 2, \cdots, n\}$. Let $\beta = (a_1, a_3, i)$. Show that $\beta^{-1}\alpha\beta\alpha \in N$, and compute it.]

40. Let N be a normal subgroup of G and let H be any subgroup of G. Let $HN = \{hn \mid h \in H, n \in N\}$. Show that HN is a subgroup of G, and is the smallest subgroup containing both N and H.

41. With reference to the preceding exercise, let M also be a normal subgroup of G. Show that NM is again a normal subgroup of G.

42. Show that if H and K are normal subgroups of a group G such that $H \cap K = \{e\}$, then $hk = kh$ for all $h \in H$ and $k \in K$. [*Hint:* Consider the commutator $hkh^{-1}k^{-1} = (hkh^{-1})k^{-1} = h(kh^{-1}k^{-1})$.]

SECTION 16 †GROUP ACTION ON A SET

We have seen examples of how groups may *act on things*, like the group of symmetries of a triangle or of a square, the group of rotations of a cube, the general linear group acting on $\mathbb{R}^n$, and so on. In this section, we give the general notion of group action on a set. The next section will give an application to counting.

The Notion of a Group Action

Definition 2.1 defines a binary operation $*$ on a set S to be a function mapping $S \times S$ into S. The function $*$ gives us a rule for "multiplying" an element s_1 in S and an element s_2 in S to yield an element $s_1 * s_2$ in S.

More generally, for any sets A, B, and C, we can view a map $* : A \times B \to C$ as defining a "multiplication," where any element a of A times any element b of B has as value some element c of C. Of course, we write $a * b = c$, or simply $ab = c$. In this section, we will be concerned with the case where X is a set, G is a group, and we have a map $* : G \times X \to X$. We shall write $*(g, x)$ as $g * x$ or gx.

16.1 Definition Let X be a set and G a group. An **action of G on X** is a map $* : G \times X \to X$ such that ■

1. $ex = x$ for all $x \in X$,
2. $(g_1g_2)(x) = g_1(g_2x)$ for all $x \in X$ and all $g_1, g_2 \in G$.

Under these conditions, X is a **G-set.**

† This section is a prerequisite only for Sections 17 and 36.

16.17 Example Let X be the D_4-set in Example 16.8, with action table given by Table 16.10. With $G = D_4$, we have $G1 = \{1, 2, 3, 4\}$ and $G_1 = \{\rho_0, \delta_2\}$. Since $|G| = 8$, we have $|G1| = (G : G_1) = 4$. ▲

We should remember not only the cardinality equation in Theorem 16.16 but also that the *elements of G carrying x into g_1x are precisely the elements of the left coset g_1Gx*. Namely, if $g \in G_x$, then $(g_1g)x = g_1(gx) = g_1x$. On the other hand, if $g_2x = g_1x$, then $g_1^{-1}(g_2x) = x$ so $(g_1^{-1}g_2)x = x$. Thus $g_1^{-1}g_2 \in G_x$ so $g_2 \in g_1G_x$.

EXERCISES 16

Computations

In Exercises 1 through 3, let

$$X = \{1, 2, 3, 4, s_1, s_2, s_3, s_4, m_1, m_2, d_1, d_2, C, P_1, P_2, P_3, P_4\}$$

be the D_4-set of Example 16.8 with action table in Table 16.10. Find the following, where $G = D_4$.

1. The fixed sets X_σ for each $\sigma \in D_4$, that is, $X_{\rho_0}, X_{\rho_1}, \cdots, X_{\delta_2}$
2. The isotropy subgroups G_x for each $x \in X$, that is, $G_1, G_2, \cdots, G_{P_3}, G_{P_4}$
3. The orbits in X under D_4

Concepts

In Exercises 4 and 5, 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.

4. A group G *acts faithfully* on X if and only if $gx = x$ implies that $g = e$.
5. A group G is *transitive* on a G-set X if and only if, for some $g \in G$, gx can be every other x.
6. Let X be a G-set and let $S \subseteq X$. If $Gs \subseteq S$ for all $s \in S$, then S is a **sub-G-set.** Characterize a sub-G-set of a G-set X in terms of orbits in X and G.
7. Characterize a transitive G-set in terms of its orbits.
8. Mark each of the following true or false.

   _____ **a.** Every G-set is also a group.
   _____ **b.** Each element of a G-set is left fixed by the identity of G.
   _____ **c.** If every element of a G-set is left fixed by the same element g of G, then g must be the identity e.
   _____ **d.** Let X be a G-set with $x_1, x_2 \in X$ and $g \in G$. If $gx_1 = gx_2$, then $x_1 = x_2$.
   _____ **e.** Let X be a G-set with $x \in X$ and $g_1, g_2 \in G$. If $g_1x = g_2x$, then $g_1 = g_2$.
   _____ **f.** Each orbit of a G-set X is a transitive sub-G-set.
   _____ **g.** Let X be a G-set and let $H \leq G$. Then X can be regarded in a natural way as an H-set.
   _____ **h.** With reference to (g), the orbits in X under H are the same as the orbits in X under G.
   _____ **i.** If X is a G-set, then each element of G acts as a permutation of X.
   _____ **j.** Let X be a G-set and let $x \in X$. If G is finite, then $|G| = |Gx| \cdot |G_x|$.

9. Let X and Y be G-sets with the *same* group G. An **isomorphism** between G-sets X and Y is a map $\phi : X \to Y$ that is one to one, onto Y, and satisfies $g\phi(x) = \phi(gx)$ for all $x \in X$ and $g \in G$. Two G-sets are **isomorphic** if such an isomorphism between them exists. Let X be the D_4-set of Example 16.8.

a. Find two distinct orbits of X that are isomorphic sub-D_4-sets.

b. Show that the orbits $\{1, 2, 3, 4\}$ and $\{s_1, s_2, s_3, s_4\}$ are not isomorphic sub-D_4-sets. [*Hint:* Find an element of G that acts in an essentially different fashion on the two orbits.]

c. Are the orbits you gave for your answer to part (a) the only two different isomorphic sub-D_4-sets of X?

10. Let X be the D_4-set in Example 16.8.

a. Does D_4 act faithfully on X?

b. Find all orbits in X on which D_4 acts faithfully as a sub-D_4-set.

Theory

11. Let X be a G-set. Show that G acts faithfully on X if and only if no two distinct elements of G have the same action on each element of X.

12. Let X be a G-set and let $Y \subseteq X$. Let $G_Y = \{g \in G \mid gy = y \text{ for all } y \in Y\}$. Show G_Y is a subgroup of G, generalizing Theorem 16.12.

13. Let G be the additive group of real numbers. Let the action of $\theta \in G$ on the real plane $\mathbb{R}^2$ be given by rotating the plane counterclockwise about the origin through θ radians. Let P be a point other than the origin in the plane.

a. Show $\mathbb{R}^2$ is a G-set.

b. Describe geometrically the orbit containing P.

c. Find the group G_P.

Exercises 14 through 17 show how all possible G-sets, up to isomorphism (see Exercise 9), can be formed from the group G.

14. Let $\{X_i \mid i \in I\}$ be a disjoint collection of sets, so $X_i \cap X_j = \varnothing$ for $i \neq j$. Let each X_i be a G-set for the same group G.

a. Show that $\bigcup_{i \in I} X_i$ can be viewed in a natural way as a G-set, the **union** of the G-sets X_i.

b. Show that every G-set X is the union of its orbits.

15. Let X be a transitive G-set, and let $x_0 \in X$. Show that X is isomorphic (see Exercise 9) to the G-set L of all left cosets of G_{x_0}, described in Example 16.7. [*Hint:* For $x \in X$, suppose $x = gx_0$, and define $\phi : X \to L$ by $\phi(x) = gG_{x_0}$. Be sure to show ϕ is well defined!]

16. Let X_i for $i \in I$ be G-sets for the same group G, and suppose the sets X_i are not necessarily disjoint. Let $X_i' = \{(x, i) \mid x \in X_i\}$ for each $i \in I$. Then the sets X_i' are disjoint, and each can still be regarded as a G-set in an obvious way. (The elements of X_i have simply been tagged by i to distinguish them from the elements of X_j for $i \neq j$.) The G-set $\bigcup_{i \in I} X_i'$ is the **disjoint union** of the G-sets X_i. Using Exercises 14 and 15, show that every G-set is isomorphic to a disjoint union of left coset G-sets, as described in Example 16.7.

17. The preceding exercises show that every G-set X is isomorphic to a disjoint union of left coset G-sets. The question then arises whether left coset G-sets of distinct subgroups H and K of G can themselves be isomorphic. Note that the map defined in the hint of Exercise 15 depends on the choice of x_0 as "base point." If x_0 is replaced by g_0x_0 and if $G_{x_0} \neq G_{g_0x_0}$, then the collections L_H of left cosets of $H = G_{x_0}$ and L_K of left cosets of $K = G_{g_0x_0}$ form distinct G-sets that must be isomorphic, since both L_H and L_K are isomorphic to X.

a. Let X be a transitive G-set and let $x_0 \in X$ and $g_0 \in G$. If $H = G_{x_0}$ describe $K = G_{g_0x_0}$ in terms of H and g_0.

b. Based on part (a), conjecture conditions on subgroups H and K of G such that the left coset G-sets of H and K are isomorphic.

c. Prove your conjecture in part (b).

18. Up to isomorphism, how many transitive $\mathbb{Z}_4$ sets X are there? (Use the preceding exercises.) Give an example of each isomorphism type, listing an action table of each as in Table 16.10. Take lowercase names a, b, c, and so on for the elements in the set X.

19. Repeat Exercise 18 for the group $\mathbb{Z}_6$.

20. Repeat Exercise 18 for the group S_3. List the elements of S_3 in the order ι, (1, 2, 3), (1, 3, 2), (2, 3), (1, 3), (1, 2).

SECTION 17 †Applications of G-Sets to Counting

This section presents an application of our work with G-sets to counting. Suppose, for example, we wish to count how many distinguishable ways the six faces of a cube can be marked with from one to six dots to form a die. The standard die is marked so that when placed on a table with the 1 on the bottom and the 2 toward the front, the 6 is on top, the 3 on the left, the 4 on the right, and the 5 on the back. Of course, other ways of marking the cube to give a distinguishably different die are possible.

Let us distinguish between the faces of the cube for the moment and call them the bottom, top, left, right, front, and back. Then the bottom can have any one of six marks from one dot to six dots, the top any one of the five remaining marks, and so on. There are $6! = 720$ ways the cube faces can be marked in all. Some markings yield the same die as others, in the sense that one marking can be carried into another by a rotation of the marked cube. For example, if the standard die described above is rotated 90° counterclockwise as we look down on it, then 3 will be on the front face rather than 2, but it is the same die.

There are 24 possible positions of a cube on a table, for any one of six faces can be placed down, and then any one of four to the front, giving $6 \cdot 4 = 24$ possible positions. Any position can be achieved from any other by a rotation of the die. These rotations form a group G, which is isomorphic to a subgroup of S_8 (see Exercise 45 of Section 8). We let X be the 720 possible ways of marking the cube and let G act on X by rotation of the cube. We consider two markings to give the same die if one can be carried into the other under action by an element of G, that is, by rotating the cube. In other words, we consider each *orbit* in X under G to correspond to a single die, and different orbits to give different dice. The determination of the number of distinguishable dice thus leads to the question of determining the number of orbits under G in a G-set X.

The following theorem gives a tool for determining the number of orbits in a G-set X under G. Recall that for each $g \in G$ we let X_g be the set of elements of X left fixed by g, so that $X_g = \{x \in X \mid gx = x\}$. Recall also that for each $x \in X$, we let $G_x = \{g \in G \mid gx = x\}$, and Gx is the orbit of x under G.

17.1 Theorem **(Burnside's Formula)** Let G be a finite group and X a finite G-set. If r is the number of orbits in X under G, then

$$r \cdot |G| = \sum_{g \in G} |X_g|. \tag{1}$$

† This section is not used in the remainder of the text.