10.11 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 $(G : K) = (G : H)(H : K)$.

Lagrange's Theorem says that for any subgroup H of a finite group G, the order of H divides the order of G. But if d is a divisor of the order of G, does G necessarily have a subgroup with exactly d elements? We will show in Section 13 that the answer is no for some groups. This suggests a new question: Under what conditions does G have a subgroup of every order d that is a divisor of G? We saw in Section 9 that for every divisor of the order of an abelian group, there is a subgroup of that order. The complete answer to this question is beyond the scope of this book, but we will come back to the question later.

Cosets Left and Right!

It is possible to do everything we have done in this section using right cosets instead of left cosets. All it takes is some minor and straightforward modifications to the definitions and proofs. We briefly give the corresponding definitions that lead to right cosets and point out some of their properties.

Let H be a subgroup of G. To start with, instead of $\sim_L$ we could have used $\sim_R$ defined by

$$a \sim_R b \quad \text{if and only if} \quad ab^{-1} \in H.$$

With this definition, $\sim_R$ is an equivalence relation and the equivalence classes are the **right cosets**. The right coset of H containing the element $a \in G$ is

$$Ha = \{ha \mid h \in H\}.$$

Just like left cosets, each right coset of a subgroup H has the same cardinality as H. So left cosets and right cosets have the same cardinality. In abelian groups, the right and left cosets are the same, but there is no reason to think they would be the same in general for nonabelian groups. If the right and left cosets are the same, we can drop left or right and just refer to cosets.

10.12 Example In Example 10.5 we computed the left cosets of the subgroup $H = \langle \mu \rangle = \{\iota, \mu\}$ of the group $D_4 = \{\iota, \rho, \rho^2, \rho^3, \mu, \mu\rho, \mu\rho^2, \mu\rho^3\}$. We now compute the right cosets.

$$\begin{aligned} \{\iota, \mu\}\iota &= \{\iota, \mu\} \\ \{\iota, \mu\}\rho &= \{\rho, \mu\rho\} \\ \{\iota, \mu\}\rho^2 &= \{\rho^2, \mu\rho^2\} \\ \{\iota, \mu\}\rho^3 &= \{\rho^3, \mu\rho^3\} \end{aligned}$$

The right cosets and the left cosets are not the same. For example, $\rho H = \{\rho, \mu\rho^3\}$ while $H\rho = \{\rho, \mu\rho\}$. ▲

If this were the whole story of left and right cosets, there would be no reason to even mention right cosets. We could just use left coset, prove Lagrange's Theorem, and call it a day. However, as we shall see in Part III, a curious thing happens when the left and right cosets are the same. We illustrate with an example.

10.13 Example The group $\mathbb{Z}_6$ is abelian. Find the partition of $\mathbb{Z}_6$ into cosets of the subgroup $H = \{0, 3\}$.

Solution One coset is {0, 3} itself. The coset containing 1 is $1 + \{0, 3\} = \{1, 4\}$. The coset containing 2 is $2 + \{0, 3\} = \{2, 5\}$. Since {0, 3}, {1, 4}, and {2, 5} exhaust all of $\mathbb{Z}_6$, these are all the cosets. ▲

We point out a fascinating thing that we will develop in detail in Section 12. Referring back to Example 10.13, Table 10.14 gives the binary operation for $\mathbb{Z}_6$ but with elements listed in the order they appear in the cosets {0, 3}, {1, 4}, {2, 5}. We shaded the table according to these cosets.

10.14 Table

$+_6$	0	3	1	4	2	5
0	0	3	1	4	2	5
3	3	0	4	1	5	2
1	1	4	2	5	3	0
4	4	1	5	2	0	3
2	2	5	3	0	4	1
5	5	2	0	3	1	4

10.15 Table

	LT	MD	DK
LT	LT	MD	DK
MD	MD	DK	LT
DK	DK	LT	MD

Suppose we denote these cosets by LT(light), MD(medium), and DK(dark) according to their shading. Table 10.14 then defines a binary operation on these shadings, as shown in Table 10.15. Note that if we replace LT by 0, MD by 1, and DK by 2 in Table 10.15, we obtain the table for $\mathbb{Z}_3$. Thus the table of shadings forms a group!

We will see in Section 12 that when left cosets and right cosets are the same, then the cosets form a group as in Example 10.13. If right and left cosets are different, the construction fails.

10.16 Example Let $H = \{\iota, \mu\} \leq D_3$. The group table for D_3 is given below with the elements arranged so that left cosets are together. The double lines divide the cosets.

	ι	μ	ρ	$\mu\rho^2$	ρ^2	$\mu\rho$
ι	ι	μ	ρ	$\mu\rho^2$	ρ^2	$\mu\rho$
μ	μ	ι	$\mu\rho$	ρ^2	$\mu\rho^2$	ρ
ρ	ρ	$\mu\rho^2$	ρ^2	$\mu\rho$	ι	μ
$\mu\rho^2$	$\mu\rho^2$	ρ	μ	ι	$\mu\rho$	ρ^2
ρ^2	ρ^2	$\mu\rho$	ι	μ	ρ	$\mu\rho^2$
$\mu\rho$	$\mu\rho$	ρ^2	$\mu\rho^2$	ρ	μ	ι

The situation here is much different from the situation in Example 10.13. In Table 10.14 the two-by-two blocks in the table each contain only elements of a left coset. In the present example, most blocks do not contain elements from only one left coset. Furthermore, even if we tried to use the two-by-two blocks of elements to form a three-by-three group table, the second row of blocks contains two blocks, both having the same elements, $\{\rho^2, \mu\rho, \mu, \iota\}$. So the table of blocks would have a row with the same element listed twice. In this case, there is no natural way of making the left cosets a group. ▲

If G is an abelian group, then the left and right cosets are the same. Theorem 10.17 gives another condition when left and right cosets are the same. Recall that if $\phi : G \to G'$ is a group homomorphism, then $\mathrm{Ker}(\phi) = \phi^{-1}[\{e\}] \leq G$ is the kernel of ϕ.

10.17 Theorem Let $\phi : G \to G'$ be a group homomorphism. Then the left and right cosets of $\mathrm{Ker}(\phi)$ are identical. Furthermore, $a, b \in G$ are in the same coset of $\mathrm{Ker}(\phi)$ if and only if $\phi(a) = \phi(b)$.

Proof We first assume that a and b are in the same left cosets of $\text{Ker}(\phi)$ and show they are also in the same right cosets. Then $a^{-1}b \in \text{Ker}(\phi)$. So $\phi(a^{-1}b) = e$, the identity element. Because ϕ is a homomorphism, $\phi(a)^{-1}\phi(b) = e$, which implies that $\phi(a) = \phi(b)$. Therefore, $\phi(ab^{-1}) = \phi(a)\phi(b)^{-1} = \phi(a)\phi(a)^{-1} = e$. Thus $ab^{-1} \in \text{Ker}(\phi)$, which says that a and b are in the same right coset. Note that in the process we showed that if a and b are in the same left coset of $\text{Ker}(\phi)$, then $\phi(a) = \phi(b)$.

Now suppose that $\phi(a) = \phi(b)$. Then $\phi(b^{-1}a) = \phi(b)^{-1}\phi(a) = e$. Thus $b^{-1}a \in \text{Ker}(\phi)$, which implies that a and b are in the same left coset.

To complete the proof, we need to show that if a and b are in the same right coset, then they are also in the same left coset. The proof is essentially the same as above, so we leave this detail to the reader. ◆

10.18 Example Consider the determinant map $\det : GL(2, \mathbb{R}) \to \mathbb{R}^*$. In linear algebra you learn that $\det(AB) = \det(A)\det(B)$, so the determinant is a group homomorphism. The kernel of det is the set of all 2×2 matrices with determinant 1. Two matrices $A, B \in GL(2, \mathbb{R})$ are in the same left coset of Ker(det) if and only if they are in the same right coset of Ker(det) if and only if $\det(A) = \det(B)$. In particular, the two matrices

$$\begin{bmatrix} 2 & 0 \\ 0 & 1 \end{bmatrix} \text{ and } \begin{bmatrix} 3 & 2 \\ 2 & 2 \end{bmatrix}$$

each have determinant 2, so they are in the same left (and right) cosets of Ker(det). ▲

10.19 Corollary A homomorphism $\phi : G \to G'$ is one-to-one if and only if $\text{Ker}(\phi)$ is the trivial subgroup of G.

Proof We first assume that $\text{Ker}(\phi) = \{e\}$. Every coset of $\text{Ker}(\phi)$ has only one element. Suppose that $\phi(a) = \phi(b)$. Then a and b are in the same coset of $\text{Ker}(\phi)$ by Theorem 10.17. Thus $a = b$.

Now suppose that ϕ is one-to-one. Then only the identity e is mapped to the identity in G'. So $\text{Ker}(\phi) = \{e\}$. ◆

Corollary 10.19 says that to check if a homomorphism $\phi : G \to G'$ is one-to-one one merely needs to check that $\text{Ker}(\phi)$ is the trivial subgroup. In other words, show that the only solution to $\phi(x) = e'$ is e, where e and e' are the identities in G and G', respectively.

10.20 Example Let $\phi : \mathbb{R} \to \mathbb{R}^+$ be defined by $\phi(x) = 2^x$. Since ϕ is a homomorphism, we can check that ϕ is one-to-one by solving $\phi(x) = 1$. The equation $2^x = \phi(x) = 1$ has only the solution 0 since for $x > 0$, $2^x > 1$ and for $x < 0$, $2^x < 1$. Thus ϕ is one-to-one. ▲

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 $\langle 3 \rangle$ in $\mathbb{Z}_{18}$.

4. Find all cosets of the subgroup $\langle 6 \rangle$ in $\mathbb{Z}_{18}$.

5. Find all cosets of the subgroup $\langle 18 \rangle$ of $\mathbb{Z}_{36}$.

6. Find all left cosets of $\langle \mu\rho \rangle$ in D_4.

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

8. Are the left and right cosets the same for the subgroup $\{\iota, \rho^4, \mu, \mu\rho^4\}$ of D_8? If so, display the cosets. If not, find a left coset that is not the same as any right coset.

9. Find all the left cosets of $\langle \rho^2 \rangle \leq D_4$.

10. Repeat the previous exercise, but find the right cosets. Are the left and right cosets the same? If so, make the group table for D_4, ordering the elements so that the cosets are in blocks, see if the blocks form a group with four elements, and determine what group of order 4 the blocks form.

11. Find the index of $\langle \rho^2 \rangle$ in the group D_6.

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

13. Find the index of $12\mathbb{Z}$ in $\mathbb{Z}$.

14. Find the index of $12\mathbb{Z}$ in $3\mathbb{Z}$.

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 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. 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. Let $\phi : G \to G'$. Then the *kernel* of ϕ is $\text{Ker}(\phi) = \{g \in G \mid \phi(g) = e\}$.

20. Determine whether each of the following is 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.

k. The kernel of a homomorphism is a subgroup of the range of the homomorphism.

l. Left cosets and right cosets of the kernel of a homomorphism are the same.

In Exercises 21 through 26, give an example of the desired subgroup and group if possible. If impossible, say why it is impossible.

21. A subgroup $H \leq G$ with G infinite and H having only a finite number of left cosets in G

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

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

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

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

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

Proof Synopsis

27. Give a one-sentence synopsis of the proof of the Theorem of Lagrange.

Theory

28. Prove that the relation $\sim_R$ that is used to define right cosets is an equivalence relation.

29. 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.

30. 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.

31. 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 30.)

Let H be a subgroup of a group G and let $a, b \in G$. In Exercises 32 through 35 prove the statement or give a counterexample.

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

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

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

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

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

37. 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.)

38. Exercise 29 of Section 2 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.

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

40. Prove Theorem 10.11 [*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.]

41. 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.

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

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

44. 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 $\sin x$.)

45. 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.**)

46. 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).

47. 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.

48. 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 47 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 6.17.]

49. 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 10.9 and Exercise 48 to show that G must contain an element of order $n = |G|$.]

50. Show that a finite group cannot be written as the union of two of its proper subgroups. Does the statement remain true if "two" is replaced by "three"? (This was problem B-2 on the 1969 Putnam Exam.)

SECTION 11 [†]Plane Isometries

Consider the Euclidean plane $\mathbb{R}^2$. An **isometry of** $\mathbb{R}^2$ is a permutation $\phi : \mathbb{R}^2 \to \mathbb{R}^2$ that preserves distance, so that the distance between points P and Q is the same as the distance between the points $\phi(P)$ and $\phi(Q)$ for all points P and Q in $\mathbb{R}^2$. If ψ is also an isometry of $\mathbb{R}^2$, then the distance between $\psi(\phi(P))$ and $\psi(\phi(Q))$ must be the same as the distance between $\phi(P)$ and $\phi(Q)$, which in turn is the distance between P and Q, showing that the composition of two isometries is again an isometry. Since the identity map is an isometry and the inverse of an isometry is an isometry, we see that the isometries of $\mathbb{R}^2$ form a subgroup of the group of all permutations of $\mathbb{R}^2$.

Given any subset S of $\mathbb{R}^2$, the isometries of $\mathbb{R}^2$ that carry S onto itself form a subgroup of the group of isometries. This subgroup is the **group of symmetries of** S **in** $\mathbb{R}^2$. Although we defined the dihedral group D_n as one-to-one maps from the vertices of a regular n-gon onto itself that preserves edges, we can extend each map in D_n to an isometry of the whole plane; μ is reflection across the x-axis and ρ is rotation about the origin by $\frac{2\pi}{n}$. So we can think of D_n as the group of isometries of a regular n-gon in $\mathbb{R}^2$.

Everything we have defined in the two preceding paragraphs could equally well have been done for n-dimensional Euclidean space $\mathbb{R}^n$, but we will concern ourselves chiefly with plane isometries here.

It can be proved that every isometry of the plane is one of just four types (see Artin [5]). We will list the types and show, for each type, a labeled figure that can be carried into itself by an isometry of that type. In each of Figs. 11.1, 11.3, and 11.4, consider the line with spikes shown to be extended infinitely to the left and to the right. We also give an example of each type in terms of coordinates.

translation τ: Slide every point the same distance in the same direction. See Fig. 11.1. (*Example:* $\tau(x, y) = (x, y) + (2, -3) = (x + 2, y - 3)$.)

rotation ρ: Rotate the plane about a point P through an angle θ. See Fig. 11.2. (*Example:* $\rho(x, y) = (-y, x)$ is a rotation through 90° counterclockwise about the origin (0, 0).)

reflection μ: Map each point into its mirror image (μ for mirror) across a line L, each point of which is left fixed by μ. See Fig. 11.3. The line L is the *axis of reflection*. (*Example:* $\mu(x, y) = (y, x)$ is a reflection across the line $y = x$.)

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