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. Determine whether each of the following is 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 9.12.
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 9.12 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. Find the torsion coefficients for each of the following groups.

a. $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_4$
b. $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_{27}$
c. $\mathbb{Z}_8 \times \mathbb{Z}_2 \times \mathbb{Z}_{49} \times \mathbb{Z}_7$
d. $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_9 \times \mathbb{Z}_5$

Proof Synopsis

45. Give a two-sentence synopsis of the proof of Theorem 9.5.

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 54 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.

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

55. Using the notation of Theorem 9.14, prove that for any finite abelian group G, every cyclic subgroup of G has order no more than d_k, the largest invariant factor for G.

SECTION 10 COSETS AND THE THEOREM OF LAGRANGE

You may have noticed that the order of a subgroup H of a finite group G seems always to be a divisor of the order of G. This is the theorem of Lagrange. We shall prove it by exhibiting a partition of G into cells, all having the same size as H. Thus if there are r such cells, we will have

$$r(\text{order of } H) = (\text{order of } G)$$

from which the theorem follows immediately. The cells in the partition will be called *cosets of* H, and they are important in their own right. In Section 12, we will see that if H satisfies a certain property, then each coset can be regarded as an element of a group in a very natural way. We give some indication of such *coset groups* in this section to help you develop a feel for the topic.

Cosets

Let H be a subgroup of a group G, which may be of finite or infinite order. We exhibit a partition a G by defining an equivalence relation, $\sim_L$ on G.

10.1 Theorem Let H be a subgroup of G. Let the relation $\sim_L$ be defined on G by

$$a \sim_L b \qquad \text{if and only if} \qquad a^{-1}b \in H.$$

Then $\sim_L$ is an equivalence relation on G.

Proof When reading the proof, notice how we must constantly make use of the fact that H is a *subgroup* of G.

Reflexive Let $a \in G$. Then $a^{-1}a = e$ and $e \in H$ since H is a subgroup. Thus $a \sim_L a$.

Symmetric Suppose $a \sim_L b$. Then $a^{-1}b \in H$. Since H is a subgroup, $(a^{-1}b)^{-1}$ is in H and $(a^{-1}b)^{-1} = b^{-1}a$, so $b^{-1}a$ is in H and $b \sim_L a$.

Transitive Let $a \sim_L b$ and $b \sim_L c$. Then $a^{-1}b \in H$ and $b^{-1}c \in H$. Since H is a subgroup, $(a^{-1}b)(b^{-1}c) = a^{-1}c$ is in H, so $a \sim_L c$. ◆

The equivalence relation $\sim_L$ in Theorem 10.1 defines a partition of G, as described in Theorem 0.22. Let's see what the cells in this partition look like. Suppose $a \in G$. The cell containing a consists of all $x \in G$ such that $a \sim_L x$, which means all $x \in G$ such that $a^{-1}x \in H$. Now $a^{-1}x \in H$ if and only if $a^{-1}x = h$ for some $h \in H$, or equivalently, if and only if $x = ah$ for some $h \in H$. Therefore the cell containing a is $\{ah \mid h \in H\}$, which we denote by aH.

10.2 Definition Let H be a subgroup of a group G. The subset $aH = \{ah \mid h \in H\}$ of G is the **left coset** of H containing a. ■

10.3 Example Exhibit the left coset of the subgroup $3\mathbb{Z}$ of $\mathbb{Z}$.

Solution Our notation here is additive, so the left coset of $3\mathbb{Z}$ containing m is $m + 3\mathbb{Z}$. Taking $m = 0$, we see that

$$3\mathbb{Z} = \{\cdots, -9, -6, -3, 0, 3, 6, 9, \cdots\}$$

is itself one of its left cosets, the coset containing 0. To find another left coset, we select an element of $\mathbb{Z}$ not in $3\mathbb{Z}$, say 1, and find the left coset containing it. We have

$$1 + 3\mathbb{Z} = \{\cdots, -8, -5, -2, 1, 4, 7, 10, \cdots\}.$$

These two left cosets, $3\mathbb{Z}$ and $1 + 3\mathbb{Z}$, do not yet exhaust $\mathbb{Z}$. For example, 2 is in neither of them. The left coset containing 2 is

$$2 + 3\mathbb{Z} = \{\cdots, -7, -4, -1, 2, 5, 8, 11, \cdots\}.$$

It is clear that these three left cosets we have found do exhaust $\mathbb{Z}$, so they constitute the partition of $\mathbb{Z}$ into left cosets of $3\mathbb{Z}$. ▲

10.4 Example We find the partition of $\mathbb{Z}_{12}$ into left cosets of $H = \langle 3 \rangle$. One coset is always the subgroup itself, so $0 + H = \{0, 3, 6, 9\}$. We next find $1 + H = \{1, 4, 7, 10\}$. We are still not done since we have not included every element of $\mathbb{Z}_{12}$ in the two cosets we listed so far. Finally, $2 + H = \{2, 5, 8, 11\}$ and we have computed all the left cosets of H in $\mathbb{Z}_{12}$. ▲

10.5 Example We now list the left cosets of the subgroup $H = \langle \mu \rangle = \{\iota, \mu\}$ of the nonabelian group $D_4 = \{\iota, \rho, \rho^2, \rho^3, \mu, \mu\rho, \mu\rho^2, \mu\rho^3\}$.

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

We know this is a complete list of the left cosets since every element of D_4 appears in exactly one of the listed sets. ▲

The Theorem of Lagrange

In Example 10.4 each left coset of $\langle 3 \rangle \leq \mathbb{Z}_{12}$ has four elements. In Example 10.5, each left coset has two elements. From the computation of the left cosets, it is no surprise that all left cosets of a subgroup have the same number of elements. Theorem 10.6 confirms this is what happens in general.

10.6 Theorem Let H be a subgroup of G. Then for any $a \in G$, the coset aH has the same cardinality as H.

Proof Let $f : H \to aH$ be defined by the formula $f(h) = ah$. To show f is one-to-one, we suppose that $b, c \in H$ and $f(b) = f(c)$. Then $ab = ac$ and left cancellation gives $b = c$. So f is one-to-one. Now suppose that $y \in aH$. Then there is an $h \in H$ such that $y = ah$ by definition of the left coset aH. Thus $y = f(h)$ and f is surjective. Since there is a one-to-one function mapping H onto aH, H and aH have the same cardinality. ◆

In the case of a finite subgroup H, Theorem 10.6 says that H and aH have the same number of elements for any a in the group G. This is precisely what we were seeking in order to prove Lagrange's Theorem.

10.7 Theorem **(Theorem of Lagrange)** Let H be a subgroup of a finite group G. Then the order of H is a divisor of the order of G.

Proof Let n be the order of G, and let H have order m. Theorem 10.6 shows that every coset of H also has m elements. Let r be the number of cells in the partition of G into left cosets of H. Then $n = rm$, so m is indeed a divisor of n. ◆

Note that this elegant and important theorem comes from the simple counting of cosets and the number of elements in each coset. We continue to derive consequences of Theorem 10.7, which should be regarded as a counting theorem.

10.8 Corollary Every group of prime order is cyclic.

Proof Let G be of prime order p, and let a be an element of G different from the identity. Then the cyclic subgroup $\langle a \rangle$ of G generated by a has at least two elements, a and e. But by Theorem 10.7, 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* ρ. 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.

10.9 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 Lagrange's Theorem. ◆

10.10 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. We state a basic theorem concerning indices of subgroups, and leave the proof to the exercises (see Exercise 40).