Theorem 2–33. If $(H, *)$ is a normal subgroup of the group $(G, *)$, then the system $(G/H, \otimes)$ forms a group, known as the *quotient group* of G by H.

Proof. First, let us observe that the associativity of the operation $\otimes$ is a direct consequence of the associativity of $*$ in G:

$$\begin{aligned}
[(a * H) \otimes (b * H)] \otimes (c * H) &= \big((a * b) * H\big) \otimes (c * H) \\
&= \big((a * b) * c\big) * H \\
&= \big(a * (b * c)\big) * H \\
&= (a * H) \otimes \big((b * c) * H\big) \\
&= (a * H) \otimes [(b * H) \otimes (c * H)].
\end{aligned}$$

The coset $H = e * H$ is the identity element for the operation $\otimes$, since

$$\begin{aligned}
(a * H) \otimes (e * H) &= (a * e) * H \\
&= a * H \\
&= (e * a) * H \\
&= (e * H) \otimes (a * H).
\end{aligned}$$

It is equally easy to see that the inverse of the coset $a * H$ is $a^{-1} * H$, where a^{-1} denotes the inverse of a in $(G, *)$. This is evident from the computation

$$\begin{aligned}
(a * H) \otimes (a^{-1} * H) &= (a * a^{-1}) * H \\
&= e * H \\
&= (a^{-1} * a) * H \\
&= (a^{-1} * H) \otimes (a * H).
\end{aligned}$$

Hence all the group postulates are fulfilled and the proof is complete.

Example 2–38. Once again we fall back on the group of symmetries of the square for an illustration. Here, the subgroup

$$(S, *) = (\{R_{180}, R_{360}\}, *)$$

is normal, being the center of the group. Its distinct cosets, that is, the elements of G/S, are

$$G/S = \big\{\{R_{180}, R_{360}\}, \{R_{90}, R_{270}\}, \{V, H\}, \{D_1, D_2\}\big\}.$$

A typical coset multiplication proceeds as follows:

$$\begin{aligned}
\{D_1, D_2\} \otimes \{R_{90}, R_{270}\} &= (D_1 * S) \otimes (R_{90} * S) \\
&= (D_1 * R_{90}) * S \\
&= H * S \\
&= \{V, H\}.
\end{aligned}$$

To multiply two cosets under $\otimes$, all we really need to do is select an arbitrary representative from each coset, multiply these elements under the group operation $*$ and determine to which coset the resulting product belongs.

The operation table for the quotient group $(G/S, \otimes)$ is shown in Table 2-4.

Table 2-4

$\otimes$	$\{R_{180}, R_{360}\}$	$\{R_{90}, R_{270}\}$	$\{V, H\}$	$\{D_1, D_2\}$
$\{R_{180}, R_{360}\}$	$\{R_{180}, R_{360}\}$	$\{R_{90}, R_{270}\}$	$\{V, H\}$	$\{D_1, D_2\}$
$\{R_{90}, R_{270}\}$	$\{R_{90}, R_{270}\}$	$\{R_{180}, R_{360}\}$	$\{D_1, D_2\}$	$\{V, H\}$
$\{V, H\}$	$\{V, H\}$	$\{D_1, D_2\}$	$\{R_{180}, R_{360}\}$	$\{R_{90}, R_{270}\}$
$\{D_1, D_2\}$	$\{D_1, D_2\}$	$\{V, H\}$	$\{R_{90}, R_{270}\}$	$\{R_{180}, R_{360}\}$

Example 2-39. A simple, but useful example to keep in mind when working with quotient groups is furnished by the additive group of integers $(Z, +)$. It has been previously established that the (normal) subgroups of $(Z, +)$ are the cyclic subgroups $((n), +)$, n a nonnegative integer. The cosets of (n) in Z take the form

$$a + (n) = \{a + kn \mid k \in Z\} = [a].$$

In other words, the cosets of (n) are merely the congruence classes modulo n. Coset multiplication in $Z/(n)$, moreover, is given by

$$(a + (n)) \otimes (b + (n)) = a + b + (n),$$

or, with a judicious change of notation,

$$[a] \otimes [b] = [a + b].$$

We thus deduce that the quotient group of Z by (n) is none other than the group of integers modulo n,

$$(Z/(n), \otimes) = (Z_n +_n).$$

Among other things, this indicates that had we so desired, the study of the integers modulo n could have been subsumed under the more general theory of quotient groups.

It is a simple matter to see that any quotient group of a commutative group is necessarily commutative. A natural question is whether a noncommutative group can possess commutative quotient groups and, more pointedly, what conditions (if any at all) would insure their existence. As a concluding topic in this section, we investigate this particular situation. Our analysis begins with a basic definition.

Definition 2-26. Given a group $(G, *)$ and elements $a, b \in G$, the *commutator* of a and b is defined to be the product $a * b * a^{-1} * b^{-1}$.

To simplify matters, the symbol $[a, b]$ will be used to represent the commutator of two elements a and b; any other symbol would do as well, but this notation is standard. Inasmuch as $[a, b]$ satisfies the identity

$$a * b = [a, b] * b * a,$$

one may view the commutator of a and b as a measure of the extent to which $a * b$ differs from $b * a$. Indeed, the elements a and b commute if and only if $[a, b] = e$.

In general, the commutators do not by themselves form the elements of a subgroup, since they fail to be closed under multiplication. The usual procedure for bypassing this difficulty is to work instead with the subgroup generated by all the commutators $[a, b]$, $a, b \in G$. The resulting subgroup is known either as the *derived subgroup* or *commutator subgroup* of $(G, *)$ and may be denoted simply by $([G, G], *)$.

Now, the inverse of a commutator is again a commutator: $[a, b]^{-1} = [b, a]$. There is no necessity then of explicitly considering inverses in the definition of the set $[G, G]$; its elements consist merely of products of finitely many commutators of G. That is,

$$[G, G] = \{\prod[a_i, b_i] \mid a_i, b_i \in G\},$$

where the symbol $\prod$ should be construed as representing a finite product with one or more factors.

With these preparatory remarks out of the way, we proceed to establish some of the special properties of the commutator subgroup.

Theorem 2-34. The group $([G, G], *)$ is a normal subgroup of $(G, *)$.

Proof. The proof proceeds along the usual line. Namely, it must be shown that for $c \in [G, G]$ and a in G, $a * c * a^{-1}$ lies in $[G, G]$. But,

$$a * c * a^{-1} = (a * c * a^{-1} * c^{-1}) * c = [a, c] * c.$$

The element $[a, c] * c$ is a finite product of commutators and accordingly belongs to $[G, G]$.

The quotient group $(G/[G, G], \otimes)$, which exists by virtue of Theorem 2-34, is called the *commutator quotient group* or *abelianized group*. The motivation for this latter choice of terminology will only become apparent after the next result.

Theorem 2-35. Let $(H, *)$ be a normal subgroup of the group $(G, *)$. The quotient group $(G/H, \otimes)$ is commutative if and only if $[G, G] \subseteq H$.

Proof. Suppose $a * H$ and $b * H$ are two arbitrary elements in G/H. Since the coset $H = e * H$ is the identity element of $(G/H, \otimes)$, the group operation

$\otimes$ will be commutative if and only if

$$H = [a * H, b * H] = (a * H) \otimes (b * H) \otimes (a * H)^{-1} \otimes (b * H)^{-1},$$

or, what amounts to the same thing,

$$H = (a * b * a^{-1} * b^{-1}) * H.$$

But, Theorem 2-26 tells us a necessary and sufficient condition for the last equality to hold is that

$$[a, b] = a * b * a^{-1} * b^{-1} \in H.$$

In other words, commutativity of the quotient group $(G/H, \otimes)$ is equivalent to requiring that the subgroup $(H, *)$ contain all the commutators of G. As $([G, G], *)$ is by definition the smallest subgroup with this property, the latter condition may be replaced by $[G, G] \subseteq H$.

A special case, but itself of interest, occurs on taking $H = [G, G]$:

Corollary. For any group $(G, *)$, the commutator quotient group $(G/[G, G], \otimes)$ is commutative.

The foregoing theorem says, in effect, that the commutator group is the smallest (again, in the sense of inclusion) normal subgroup whose associated quotient group is commutative. The transition from a group to its commutator quotient group is referred to as the *abelization* of the group and provides a convenient means of manufacturing commutative groups from noncommutative ones.

PROBLEMS

1. If $H = \{0, 6, 12, 18\}$, show that $(H, +_{24})$ is a cyclic subgroup of $(Z_{24}, +_{24})$. Also, list the elements of each coset of H in Z_{24}.
2. In the symmetric group $(S_4, \circ)$, let the set H consist of the four permutations

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}.$$

   List the elements of each coset of H in S_4.
3. Assume $(H, *)$ is a subgroup of $(G, *)$.
   a) Show that every left coset of H has the same number of elements as every right coset.
   b) Prove that $(c * a) * H = (c * b) * H$ implies $a * H = b * H$.
   c) Show that there exists a one-to-one correspondence between the left cosets of H in G and the right cosets of H in G. [*Hint:* $a * H \to H * a^{-1}$.]

4. Determine the left coset decomposition of the group of symmetries of the square with respect to the subgroup $(\{R_{360}, D_1\}, *)$.

5. In the group of symmetries of the equilateral triangle, find:

   a) all subgroups,
   b) all normal subgroups,
   c) the center of the group.

6. Show that if the cyclic group $((a), *)$ is infinite, then a and a^{-1} are its only generators, and all subgroups except $(\{e\}, *)$ are infinite.

7. Let $(H, *)$ be a subgroup of index 2 in the group $(G, *)$. Prove that $(H, *)$ is a normal subgroup. [*Hint:* $H \cup (a * H) = G = H \cup (H * a)$ for any $a \in G - H$.]

8. Given that $(H_1, *)$ and $(H_2, *)$ are both normal subgroups of the group $(G, *)$, prove that the subgroup $(H_1 \cap H_2, *)$ is also normal.

9. Let $(H, *)$ be a subgroup of the group $(G, *)$ and the set $N(H)$ be defined by

$$N(H) = \{a \in G \mid a * H * a^{-1} = H\}.$$

   a) Prove that the pair $(N(H), *)$ is a subgroup of $(G, *)$, called the ***normalizer*** of H in G.
   b) Prove that $(H, *)$ is normal if and only if $N(H) = G$.

10. Suppose that $(H, *)$ and $(K, *)$ are normal subgroups of the group $(G, *)$, with $H \cap K = \{e\}$. By considering elements of the form $h * k * h^{-1} * k^{-1}$, show that $h * k = k * h$ for all $h \in H$, $k \in K$.

11. Given $(H, *)$ and $(K, *)$ are subgroups of the group $(G, *)$ and one of these subgroups is normal, prove that the pair $(H * K, *)$ is a subgroup of $(G, *)$; when both are normal subgroups, show the group $(H * K, *)$ is also normal.

12. Find an example of a group $(G, *)$ having a subgroup $(H, *)$ for which the product of two left cosets of H in G need not be a left coset of H.

13. Describe the quotient group of

    a) $(Z_e, +)$ in $(Z, +)$, b) $(\{0, 2, 4, 6, 8\}, +_{10})$ in $(Z_{10}, +_{10})$,
    c) $(Z, +)$ in $(Q, +)$, d) $(\{1, -1\}, \cdot)$ in $(\{1, -1, i, -i\}, \cdot)$.

14. Let $(G, *)$ be a cyclic group with generator a and $(H, *)$ be any subgroup of $(G, *)$. Prove that the quotient group $(G/H, \otimes)$ is also cyclic with the coset $a * H$ as a generator.

15. Given $(H, *)$ is a normal subgroup of the group $(G, *)$, prove that the quotient group $(G/H, \otimes)$ is commutative whenever $(G, *)$ is commutative.

16. For any group $(G, *)$, describe the quotient groups of the trivial normal subgroups $(\{e\}, *)$ and $(G, *)$.

17. Consider the cyclic group $((a), *)$ of order 15 and the subgroup $((a^3), *)$. List the elements of each coset of (a^3) and construct the multiplication table for the quotient group $((a)/(a^3), \otimes)$.

18. In the commutative group $(G, *)$, let the set H consist of all elements of G with finite order. Prove that

    a) $(H, *)$ is a normal subgroup of $(G, *)$, called the ***torsion subgroup***,
    b) the quotient group $(G/H, \otimes)$ is ***torsion-free;*** that is, none of its elements other than the identity are of finite order.

19. Show that a group $(G, *)$ is commutative if and only if $[G, G] = \{e\}$.

20. For any group $(G, *)$, let $(H, *)$ be the subgroup generated by the set of squares of elements of G. Establish the following:

    a) $(H, *)$ is a normal subgroup of $(G, *)$.

    b) The quotient group $(G/H, \otimes)$ is commutative. [*Hint:* $[G, G] \subseteq H$, since $[a, b] = (a * b)^2 * (b^{-1} * a^{-1} * b)^2 * b^{-2}$.]

21. Let $(H_i, *)$ be a collection of nontrivial normal subgroups of the group $(G, *)$ such that $G = \cup H_i$. Assume further that $H_i \cap H_j = \{e\}$ for $i \neq j$. Prove that the parent group $(G, *)$ is necessarily commutative. [*Hint:* Let $a \in H_i$ and $b \in H_j$. For $i \neq j$, use Problem 10. In case $i = j$, choose any element $c \in G - H_i$. Then c and $c * a$ commute with every element of H_i; in particular, $e = [c * a, b * a] = [a, b]$.]

22. Prove that if the quotient group $(G/\text{cent } G, \otimes)$ is cyclic, then $(G, *)$ is a commutative group.

2–6 HOMOMORPHISMS

Up to this point in the text, we have not considered mappings from one group to another; indeed, any knowledge of functions was irrelevant to most of the topics considered. They now enter in an essential way, for we wish to introduce a concept the idea of algebraically indistinguishable systems—which will be of fundamental importance throughout the remainder of the book and which is, in fact, one of the most important notions in mathematics.

This section begins, however, with an analysis of a class of functions which preserve algebraic structure.

Definition 2–27. Let $(G, *)$ and $(G', \circ)$ be two groups and f a function from G into G', $f\colon G \to G'$. Then f is said to be a *homomorphism* (or operation-preserving function) from $(G, *)$ into $(G', \circ)$ if and only if

$$f(a * b) = f(a) \circ f(b)$$

for every pair of elements $a, b \in G$.

A few remarks are in order before considering any examples. First, notice that on the left-hand side of the above equation, the product $a * b$ is computed in G, while on the right side the product $f(a) \circ f(b)$ is that of elements of G'. The functions indicated in this definition have the characteristic property of carrying products into products. A common way of expressing the situation is to say that the image of a product under f is equal to the product of the images.

$$\begin{tikzcd}
(a, b) \arrow[r, "*"] \arrow[d, "f"'] & a * b \arrow[d, "f"'] \\
(f(a), f(b)) \arrow[r, "\circ"] & f(a) \circ f(b) = f(a * b)
\end{tikzcd}$$

Another viewpoint is perhaps beneficial. The requirement that $f(a * b) = f(a) \circ f(b)$ for every pair of elements $a, b \in G$ is sometimes described by saying that the diagram of mappings on page 89 is commutative. For this condition asserts that if we start with elements a, b of G and move them to G' by either of the two routes indicated by the arrows—by first forming the product $a * b$ and then applying f to it or by first obtaining the images $f(a)$ and $f(b)$ and then taking their product—the result will be the same.

It may also strike the reader that the language in which Definition 2–27 is couched is open to criticism. To speak of a homomorphism from a group $(G, *)$ into a group $(G', \circ)$ is somewhat imprecise, since the mapping concerned is actually between their underlying sets of elements. This linguistic convention has the decided advantage, however, of indicating the operations preserved as well as the domain and range of the function.

Example 2–40. For an arbitrary group $(G, *)$, define the function $f\colon G \to G$ by taking $f = i_G$, the identity map on G. It is a triviality to check that f is a homomorphism from the group $(G, *)$ into itself, as

$$f(a * b) = a * b = f(a) * f(b).$$

Example 2–41. Suppose that $(G, *)$ and $(G', \circ)$ are two groups with identity elements e and e', respectively. The function $f\colon G \to G'$ given by $f(a) = e'$ for each $a \in G$ is a homomorphism:

$$f(a * b) = e' = e' \circ e' = f(a) \circ f(b).$$

This particular mapping (the so-called *trivial homomorphism*) is the only constant function which satisfies Definition 2–27.

Example 2–42. Consider the two groups $(R^f, +)$ and $(R^f - \{0\}, \cdot)$, where as usual, $+$ and $\cdot$ denote ordinary addition and multiplication. For $a \in R^f$, define the function f by $f(a) = 2^a$. To show that the mapping f is operation-preserving, we must establish whether $f(a + b) = f(a) \cdot f(b)$. This is readily verified, since

$$f(a + b) = 2^{a+b} = 2^a \cdot 2^b = f(a) \cdot f(b).$$

Example 2–43. Let $(Z, +)$ be the group of integers under addition and $(Z_n, +_n)$ be the group of integers modulo n. Define $f\colon Z \to Z_n$ by $f(a) = [a]$; that is, map each integer into the congruence class containing it. That f is a homomorphism follows directly from the definition of modular addition:

$$f(a + b) = [a + b] = [a] +_n [b] = f(a) +_n f(b).$$

For future use, we shall label the set of all homomorphisms from the group $(G, *)$ into itself (the so-called *endomorphisms*) by the symbol hom G; a frequently used alternative notation is to write end G. Both notations have a certain suggestive power, and it reduces to a matter of personal preference.

Interestingly enough, the set hom G can be endowed with an algebraic structure:

Theorem 2-36. The pair (hom G, $\circ$), where $\circ$ denotes functional composition, forms a semigroup with identity.

Proof. For the proof, which is quite elementary, it must first be shown that the composition $f \circ g$ of two functions f, $g \in$ hom G again preserves the group operation. This is easily accomplished by noting that whenever a, $b \in G$,

$$\begin{aligned}(f \circ g)(a * b) &= f(g(a * b)) \\ &= f(g(a) * g(b)) \\ &= f(g(a)) * f(g(b)) = (f \circ g)(a) * (f \circ g)(b).\end{aligned}$$

As we have seen in an earlier section, composition of functions is associative. Finally, Example 2-40 indicates that the identity mapping i_G (the identity element for composition) is itself operation-preserving.

A reasonable subject of curiosity would be the question of whether or not there exists a subset $S \subseteq$ hom G such that $(S, \circ)$ is a group. For inverses to exist, one must plainly single out the one-to-one functions. Moreover, in order that the domain of f^{-1} be the set G, consideration should be further restricted to those functions which map onto G. Thus a natural undertaking is to investigate the collection of all one-to-one homomorphisms from the group $(G, *)$ onto itself; as a matter of notation, we shall designate this set of mappings by the symbol $A(G)$, for *automorphism.*

The elements of $A(G)$ are now restricted to the extent that $(A(G), \circ)$ does indeed have the agreeable property of being a group. Let us give some details.

Theorem 2-37. The system $(A(G), \circ)$ is a subgroup of the symmetric group (sym G, $\circ$).

Proof. For functions f, $g \in A(G)$, we already know the composition of $f \circ g$ is in sym G. In conjunction with the last result, this shows $f \circ g$ belongs to $A(G)$, as does the identity map i_G. It remains only to verify here that whenever a function $f \in A(G)$, its inverse f^{-1} (which clearly is a member of sym G) is a homomorphism. If $\bar{a}$, $\bar{b} \in G$, the onto character of f implies $\bar{a} = f(a)$, $\bar{b} = f(b)$ for some choice of a, b in G. Therefore,

$$\begin{aligned}f^{-1}(\bar{a} * \bar{b}) &= f^{-1}(f(a) * f(b)) \\ &= f^{-1}(f(a * b)) \\ &= a * b = f^{-1}(\bar{a}) * f^{-1}(\bar{b}),\end{aligned}$$

and the proof is complete.

There are many important and interesting facts concerning homomorphic mappings. In the succeeding theorems, we shall examine some of these results in detail.