Theorem 2–24. Every subgroup of a cyclic group is cyclic.

Proof. Let $((a), *)$ be a cyclic group generated by the element a and let $(H, *)$ be one of its subgroups. If $H = \{e\}$, the theorem is trivially true, for $(\{e\}, *)$ is the cyclic subgroup generated by the identity element. We may thus suppose the set $H \neq \{e\}$. If $a^m \in H$, where $m \neq 0$, then a^{-m} is also an element of H; hence, H must contain positive powers of a. Let n be the smallest positive integer such that $a^n \in H$. We propose to show $H = (a^n)$.

To establish the inclusion $H \subseteq (a^n)$, let a^k be an arbitrary element in the set H. The division algorithm implies there exist integers q and r for which

$$k = qn + r, \qquad 0 \leq r < n.$$

Since both a^n and a^k are elements of H,

$$a^r = a^{k-qn} = a^k * (a^n)^{-q} \in H.$$

If $r > 0$, we have a contradiction to the assumption that a^n is the minimal positive power of a in H. Accordingly, $r = 0$ and $k = qn$. Thus, only powers of a^n lie in H, indicating $H \subseteq (a^n)$.

On the other hand, since the set H is closed under the group operation, any power of a^n must again be a member of H. Consequently, $(a^n) \subseteq H$. The two inclusions demonstrate that $H = (a^n)$.

Corollary. If $(H, *)$ is a subgroup of $((a), *)$ and $H \neq \{e\}$, then $H = (a^n)$ where n is the least positive integer such that $a^n \in H$.

We shall return to a further discussion of cyclic groups at the appropriate place in the sequel. For the moment, though, let us indicate another useful method for manufacturing new subgroups from given ones. For this, some special terminology is required.

Definition 2–22. Let $(G, *)$ be a group and H, K be nonempty subsets of G. The *product* of H and K, in that order, is the set

$$H * K = \{h * k \mid h \in H, k \in K\}.$$

A brief comment on notation that should be made is that the usual custom is to write the product $H * H$ merely as H^2 and, if one of the sets consists of a single element a, simplify $\{a\} * H$ to $a * H$.

At first sight, the reader might reasonably conjecture that whenever $(H, *)$ and $(K, *)$ are both subgroups of $(G, *)$, then $(H * K, *)$ will also be a subgroup. The group of symmetries of the square, however, shows that such a simple outcome is not to be expected. Here, it is enough to consider the subgroups having elements $H = \{R_{360}, D_1\}$ and $K = \{R_{360}, V\}$. A quick check establishes that there is no subgroup whose members comprise the product set

$$H * K = \{R_{360} * R_{360}, R_{360} * V, D_1 * R_{360}, D_1 * V\} = \{R_{360}, V, D_1, R_{270}\}.$$

In fact, the set $H * K$ isn't even closed under the group operation. One need not be dismayed by this state of affairs, for an additional assumption on the subsets H and K readily overcomes the difficulty.

Theorem 2-25. If $(H, *)$ and $(K, *)$ are subgroups of the group $(G, *)$ such that $H * K = K * H$, then the pair $(H * K, *)$ is also a subgroup.

Proof. Innocuous as the equality $H * K = K * H$ appears, it is nonetheless the source of some difficulty. This notation does not mean each element of H commutes with each element of K; all it signifies is that whenever h and k are arbitrary members of H and K, then there exist elements $h' \in H$, $k' \in K$ for which $h * k = k' * h'$. Bearing this in mind, let us proceed with the proof proper.

Plainly, the product set $H * K$ is nonempty, for $e = e * e \in H * K$. Now, let a and b be any pair of elements in $H * K$. Then $a = h * k$ and $b = h_1 * k_1$ for suitable choice of h, $h_1 \in H$ and k, $k_1 \in K$. As usual, our aim in what follows is to show that the product $a * b^{-1}$ lies in $H * K$. This is achieved through first noting

$$a * b^{-1} = (h * k) * (h_1 * k_1)^{-1} = h * ((k * k_1^{-1}) * h_1^{-1}).$$

Since K is closed under $*$, the element $k * k_1^{-1}$ belongs to K and consequently

$$(k * k_1^{-1}) * h_1^{-1} \in K * H.$$

By virtue of the condition $K * H = H * K$, there exist elements $h_2 \in H$ and $k_2 \in K$ satisfying

$$(k * k_1^{-1}) * h_1^{-1} = h_2 * k_2.$$

We may thus conclude that

$$a * b^{-1} = h * (h_2 * k_2) = (h * h_2) * k_2 \in H * K,$$

for the closure of the set H insures $h * h_2$ also is a member of it. To complete the proof, it suffices to invoke Theorem 2-17.

Corollary. If $(H, *)$ and $(K, *)$ are subgroups of the commutative group $(G, *)$ then $(H * K, *)$ is again a subgroup.

The utility of Theorem 2-25 lies in the fact that it permits another characterization of the subgroup generated by a union of sets. What happens is this: if the pair $(H * K, *)$ forms a subgroup of $(G, *)$, it must in fact be the subgroup generated by $H \cup K$; in symbols,

$$(H * K, *) = ((H \cup K), *).$$

Let us briefly outline the argument involved. To start with, the two inclusions

$$H = H * e \subseteq H * K \qquad \text{and} \qquad K = e * K \subseteq H * K$$

indicate $H \cup K \subseteq H * K$. We have already observed that the subgroup generated by $H \cup K$ is the smallest subgroup to contain this union. Thus, whenever $(H * K, *)$ is a subgroup, it follows that $(H \cup K) \subseteq H * K$. On the other hand, the set $(H \cup K)$ by definition must contain all products of the form $h * k$ with $h \in H$, $k \in K$. This results in the reverse inclusion $H * K \subseteq (H \cup K)$ and the subsequent equality $H * K = (H \cup K)$.

The significant point in this discussion is that we have gained a great deal of insight into the structure of the group generated by the union $H \cup K$, where $(H, *)$ and $(K, *)$ are both subgroups of the group $(G, *)$. To be specific, in the event the condition $H * K = K * H$ holds, each member of $((H \cup K), *)$ is expressible as the product of an element of H with an element of K. This statement obviously applies in the case where the parent group $(G, *)$ is commutative.

Example 2–34. For purposes of illustrating the above remarks, let us return again to the commutative group $(Z_{12}, +_{12})$ and the two subgroups $(\{0, 6\}, +_{12})$ and $(\{0, 4, 8\}, +_{12})$. To obtain the smallest subgroup which contains $\{0, 6\}$ and $\{0, 4, 8\}$, it suffices merely to compute the product of these subsets:

$$\begin{aligned}\{0, 6\} +_{12} \{0, 4, 8\} &= \{0 +_{12} 0, 0 +_{12} 4, 0 +_{12} 8, 6 +_{12} 0, 6 +_{12} 4, 6 +_{12} 8\}\\ &= \{0, 4, 8, 6, 10, 2\}.\end{aligned}$$

Hence, the subgroup of $(Z_{12}, +_{12})$ generated by the union $\{0, 6\} \cup \{0, 4, 8\}$ is just $(\{0, 2, 4, 6, 8, 10\}, +_{12})$.

•

PROBLEMS

1. In each of the following cases, establish that $(H, \cdot)$ is a subgroup of the group $(G, \cdot)$:

   a) $H = \{1, -1\}$, $\quad G = \{1, -1, i, -i\}$, $\quad$ where $i^2 = -1$;
   b) $H = \{2^n \mid n \in Z\}$, $\quad G = Q - \{0\}$;
   c) $H = Q - \{0\}$, $\quad G = R^{\#} - \{0\}$;
   d) $H = \{(1 + 2n)/(1 + 2m) \mid n, m \in Z\}$, $\quad G = Q - \{0\}$.

2. Prove that $(\{0, 4, 8, 12\}, +_{16})$ is a subgroup of $(Z_{16}, +_{16})$, the group of integers modulo 16.

3. In the symmetric group $(S_n, \circ)$, let H denote the set of permutations leaving the integer n fixed:
$$H = \{f \in S_n \mid f(n) = n\}.$$
Show that the pair $(H, \circ)$ is a subgroup of $(S_n, \circ)$.

4. Prove that if $(H, *)$ is a subgroup of the group $(G, *)$ and $(K, *)$ is a subgroup of $(H, *)$, then $(K, *)$ is also a subgroup of $(G, *)$.

5. Let $(H, *)$ be a subgroup of the group $(G, *)$. We say that two elements a and b of G are *congruent modulo H*, written $a \equiv b \pmod{H}$, if and only if $a * b^{-1} \in H$. Establish that congruence modulo H is an equivalence relation in G.

Observe that in the additive group of integers $(Z, +)$, where the subgroups are of the form $((n), +)$, n a nonnegative integer, this relation reduces to congruence modulo n.

6. Suppose that $(G, *)$ is a group and $a \in G$. Let $C(a)$ denote the set of all elements of G which commute with a:

$$C(a) = \{x \in G \mid a * x = x * a\}.$$

Prove that the pair $(C(a), *)$ is a subgroup of $(G, *)$, known as the *centralizer* of a in G. Also verify the equality, cent $G = \bigcap_{a \in G} C(a)$.

7. Given $(G, *)$ is a finite group, prove that

a) there exists a positive integer n such that $a^n = e$ for all $a \in G$,

b) if H is a nonempty subset of G which is closed under the operation $*$, then $(H, *)$ is a subgroup of $(G, *)$.

8. In the commutative group $(G, *)$, define the set H by

$$H = \{a \in G \mid a^k = e \text{ for some } k \in Z\}.$$

Determine whether the pair $(H, *)$ is a subgroup of $(G, *)$.

9. Let $(G, *)$ be a group and $a, b \in G$. Establish the following facts regarding the order of an element.

a) The elements a, a^{-1} and $b * a * b^{-1}$ all have the same order.

b) Both the products $a * b$ and $b * a$ have the same order. [*Hint:* Write $a * b = a * (b * a) * a^{-1}$ and use (a).]

c) If a is of order n, then $a^i = a^j$ if and only if $i \equiv j \pmod{n}$.

10. Determine the cyclic subgroup of $(S_5, \circ)$, the symmetric group on five symbols, generated by the cycle $(1\ 3\ 5\ 2\ 4)$.

11. Prove that a group of even order contains an element $a \neq e$ such that $a^2 = e$. [*Hint:* If $a \neq a^{-1}$ for all a, the group contains an odd number of elements.]

12. Let $(H, *)$ be a subgroup of the group $(G, *)$ such that $H \neq G$. Prove that the subgroup generated by the complement $G - H$ is the group $(G, *)$ itself.

13. Suppose $(G, *)$ is a group and S is a nonempty subset of G. If the elements of S all commute, show that the subgroup generated by S, $((S), *)$ is a commutative group.

14. Given a group $(G, *)$ and $\emptyset \neq H \subseteq G$, verify that the following statements are equivalent:

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

b) $H * H \subseteq H$ and $H^{-1} \subseteq H$.

c) $H * H^{-1} \subseteq H$.

15. If $(H, *)$ is a subgroup of the group $(G, *)$ and $\emptyset \neq K \subseteq G$, prove $H * K \subseteq H$ implies $K \subseteq H$.

16. Let $(H, *)$ and $(K, *)$ be subgroups of the commutative group $(G, *)$ with orders n and m, respectively. Assuming $H \cap K = \{e\}$, verify that the order of the group $(H * K, *)$ is nm.

17. Consider the group of symmetries of the square. Use Theorem 2-25 to obtain the subgroup generated by $H \cup K$, where $H = \{R_{180}, R_{360}\}$, $K = \{R_{360}, D_1\}$.
18. Let $(G, *)$ be a group of order n, where n is odd. Prove that each element of G is a square (i.e., if $x \in G$, then $x = y^2$ for some y in G).

2-5 NORMAL SUBGROUPS AND QUOTIENT GROUPS

Although we have derived some interesting results concerning subgroups, this concept, if unrestricted, is too general for many purposes. To obtain certain highly desirable conclusions, additional assumptions that go beyond Definition 2-19 must be imposed.

Thus, in the present section, we narrow the field and focus attention on a restricted class of subgroups which we shall refer to as normal subgroups. From a conceptual point of view, such groups are "normal" in the sense that they make the resulting theory so much richer than would otherwise be the case. While not every subgroup need be of this type, normal subgroups occur nonetheless with considerable frequency. It will soon become apparent that for the major part of our work, the significant aspect of this class of subgroups resides in the fact that they permit the construction of algebraic structures known as quotient groups.

Having already divulged some of the content of this section, let us now proceed to develop these ideas in detail. As a starting point, we prove a sequence of theorems leading to the conclusion that each subgroup induces a decomposition of the elements of the parent group into disjoint subsets known as *cosets.*

Definition 2-23. Let $(H, *)$ be a subgroup of the group $(G, *)$ and let $a \in G$. The set

$$a * H = \{a * h \mid h \in H\}$$

is called a *left coset* of H in G. The element a is a *representative* of $a * H$.

In a similar fashion, we can define the right cosets $H * a$ of H. The right cosets of the same subgroup are in general different from the left cosets. If the group operation $*$ of $(G, *)$ is commutative, then clearly $a * H = H * a$ for all $a \in G$. In the subsequent discussions, we will generally consider only left cosets of a subgroup. It is obvious that a parallel theory for right cosets may be developed.

Before proceeding to an example, we shall make several simple observations. First, if e is the identity element of $(G, *)$, then

$$e * H = \{e * h \mid h \in H\} = \{h \mid h \in H\} = H,$$

so that H itself is a left coset of H. Moreover, since $e \in H$, we have

$$a = a * e \in a * H,$$

that is, every element a of G belongs to some left coset of H, and more specifically, to the coset $a * H$. We shall make use of this fact in a little while.

We note further that there is a one-to-one correspondence between the elements of H and those of any coset of H. Indeed, if $a * H$ is a left coset of H, we may define a mapping $f: H \to a * H$ by $f(h) = a * h$. This function maps onto $a * H$, since every element of $a * H$ is of the form $a * h$ for some choice of $h \in H$. In addition f is a one-to-one function, for if $a * h_1 = a * h_2$, where $h_1, h_2 \in H$, the cancellation law for groups yields $h_1 = h_2$. That is, $f(h_1) = f(h_2)$ implies $h_1 = h_2$. If the group $(G, *)$ has a finite number of elements, we may therefore conclude that any two left cosets of H have the same number of elements, namely, the number of elements in H.

Example 2-35. Returning once again to the group of symmetries of the square, let us select the subgroup $(S, *)$, where $S = \{R_{360}, V\}$. The task of computing the left cosets of S is straightforward, since we have the operation table for this group at our disposal (see Example 2-24).

$$\begin{aligned}
R_{90} * S &= \{R_{90} * R_{360}, R_{90} * V\} = \{R_{90}, D_2\},\\
R_{180} * S &= \{R_{180} * R_{360}, R_{180} * V\} = \{R_{180}, H\},\\
R_{270} * S &= \{R_{270} * R_{360}, R_{270} * V\} = \{R_{270}, D_1\},\\
R_{360} * S &= \{R_{360} * R_{360}, R_{360} * V\} = \{R_{360}, V\},\\
H * S &= \{H * R_{360}, H * V\} = \{H, R_{180}\},\\
V * S &= \{V * R_{360}, V * V\} = \{V, R_{360}\},\\
D_1 * S &= \{D_1 * R_{360}, D_1 * V\} = \{D_1, R_{270}\},\\
D_2 * S &= \{D_2 * R_{360}, D_2 * V\} = \{D_2, R_{90}\}.
\end{aligned}$$

From a quick inspection, the reader will observe that there are only four distinct cosets,

$$\{R_{90}, D_2\}, \quad \{R_{180}, H\}, \quad \{R_{270}, D_1\}, \quad \text{and} \quad \{R_{360}, V\} = S.$$

These cosets are disjoint and their union is the underlying set of elements of the whole group. As we shall see, this is always the case. Also, for this subgroup the notions of left and right cosets do not agree, since

$$D_1 * S = \{D_1, R_{270}\} \neq \{D_1, R_{90}\} = S * D_1.$$

Theorem 2-26. If $(H, *)$ is a subgroup of the group $(G, *)$, then $a * H = H$ if and only if $a \in H$.

Proof. Suppose first that $a * H = H$. As we have just remarked, the fact that the identity e is a member of H implies that the element a belongs to $a * H$, and thus by hypothesis to H also. On the other hand, if $a \in H$, then $a * H \subseteq H$, since the set H, being the set of elements of a subgroup, is closed under the group operation $*$. The opposite inclusion is obtained by noting that each element $h \in H$ may be written as

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

Here, $a^{-1} * h \in H$, since both $a, h \in H$ and $(H, *)$ is a subgroup of $(G, *)$. This implies that $h \in a * H$ and consequently $H \subseteq a * H$.

Our next theorem provides a simple criterion for the equality of two left cosets, when a representative of each is known.

Theorem 2-27. If $(H, *)$ is a subgroup of the group $(G, *)$, then

$$a * H = b * H,$$

if and only if $a^{-1} * b \in H$.

Proof. Assume that $a * H = b * H$. Then, if $a * h_1$ is an arbitrary element of $a * H$, there must exist an $h_2 \in H$ such that $a * h_1 = b * h_2$. From this we conclude that

$$a^{-1} * b = h_1 * h_2^{-1},$$

and, since the product $h_1 * h_2^{-1}$ belongs to H, that $a^{-1} * b \in H$.

Conversely, if $a^{-1} * b \in H$, then by Theorem 2-26 we have

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

This implies that any element $h_1 \in H$ can be expressed as

$$h_1 = (a^{-1} * b) * h_2$$

for some $h_2 \in H$, from which we infer that $a * h_1 = b * h_2$. Thus each product $a * h_1$ in the coset $a * H$ is equal to an element of the form $b * h_2$, and consequently lies in the coset $b * H$. Since this statement also holds, with a and b interchanged,

$$a * H = b * H.$$

Remark. When working with right cosets, the requirement $a^{-1} * b \in H$ must be replaced by $a * b^{-1} \in H$; that is, $H * a = H * b$ if and only if $a * b^{-1} \in H$.

As an immediate consequence of the last theorem, we see that any element a_1 of the left coset $a * H$ determines this coset. For if $a_1 \in a * H$, then $a_1 = a * h_1$ for suitable $h_1 \in H$. Thus $a^{-1} * a_1 \in H$, so that by the theorem, $a * H = a_1 * H$. This means that each element of a coset can be thought of as a representative of that coset. In a certain sense we are being prejudiced whenever we denote a coset by $a * H$, for someone else might choose to call it $b * H$ where $b \neq a$, but $a^{-1} * b \in H$.

We are now in a position to prove a fundamental result concerning cosets to the effect that if two left cosets have an element in common, then they are precisely the same set.

Theorem 2-28. If $(H, *)$ is a subgroup of the group $(G, *)$ then either the cosets $a * H$ and $b * H$ are disjoint or else $a * H = b * H$.

Proof. Suppose that $a * H$ and $b * H$ contain some element c in common. Since c is in $a * H$, there exists an $h_1 \in H$ such that $c = a * h_1$. Similarly, we have $c = b * h_2$ for some element $h_2 \in H$. It follows then that

$$a * h_1 = b * h_2, \qquad \text{or} \qquad a^{-1} * b = h_1 * h_2^{-1}.$$

Since $(H, *)$ is a subgroup, the product $h_1 * h_2^{-1}$, and thus $a^{-1} * b$, must lie in the set H. One need only apply Theorem 2-27 to conclude

$$a * H = b * H.$$

We saw earlier that each element $a \in G$ is a member of some left coset of H in G, namely, the coset $a * H$; that is, G is exhausted by its left cosets. Theorem 2-28 indicates that an element can belong to one and only one left coset of H. Thus the set G is partitioned by H into disjoint sets, each of which has exactly as many elements as H. For ease of future reference let us summarize these remarks in the following theorem.

Theorem 2-29. If $(H, *)$ is a subgroup of the group $(G, *)$, the left (right) cosets of H in G form a partition of the set G.

Example 2-36. Consider $(Z_{12}, +_{12})$, the group of integers modulo 12. If we take $\{0, 4, 8\}$ for the set H, then $(\{0, 4, 8\}, +_{12})$ is evidently a subgroup of $(Z_{12}, +_{12})$. The left cosets of H in Z_{12} are

$$\begin{aligned} 0 +_{12} H &= \{0, 4, 8\} = 4 +_{12} H = 8 +_{12} H, \\ 1 +_{12} H &= \{1, 5, 9\} = 5 +_{12} H = 9 +_{12} H, \\ 2 +_{12} H &= \{2, 6, 10\} = 6 +_{12} H = 10 +_{12} H, \\ 3 +_{12} H &= \{3, 7, 11\} = 7 +_{12} H = 11 +_{12} H. \end{aligned}$$

In this case, the coset decomposition of Z_{12} relative to the subset H is just

$$Z_{12} = \{0, 4, 8\} \cup \{1, 5, 9\} \cup \{2, 6, 10\} \cup \{3, 7, 11\}.$$

Suppose now that $(G, *)$ is a finite group, say of order n, and $(H, *)$ is a subgroup of $(G, *)$ of order k. We can then decompose the set G into a union of a finite number of disjoint left cosets of H:

$$G = (a_1 * H) \cup (a_2 * H) \cup \cdots \cup (a_r * H).$$

The number r of distinct left cosets appearing in this decomposition is called the *index* of H in G. Since each coset in the above decomposition has k elements, the set G itself must have $r \cdot k$ elements; hence $n = r \cdot k$ or

$$\text{order } G = (\text{index } H) \cdot (\text{order } H).$$

This establishes the following classical result due to Lagrange.

Theorem 2–30. (*Lagrange*). The order and index of any subgroup of a finite group divides the order of the group.

There is a corollary to Theorem 2–30 which is of some intrinsic interest.

Corollary. If $(G, *)$ is a group of order n, then the order of any element $a \in G$ is a factor of n; in addition, $a^n = e$.

Proof. Let the element a have order k. By definition, the cyclic subgroup $((a), *)$ generated by a must also be of order k. According to the conclusion of Lagrange's Theorem, k is a divisor of n; that is, $n = rk$ for some $r \in Z_+$. Hence,

$$a^n = a^{rk} = (a^k)^r = e^r = e,$$

completing the proof of both assertions.

From Lagrange's Theorem, we are able to conclude that any finite group of prime order has no nontrivial subgroups. Actually a stronger statement can be made:

Theorem 2–31. If $(G, *)$ is a finite group of composite order, then $(G, *)$ has nontrivial subgroups.

Proof. If the group $(G, *)$ is not cyclic, any element $a \in G$ with $a \neq e$ generates a nontrivial cyclic subgroup $((a), *)$. Thus, it suffices to consider cyclic groups of composite order. To this end, suppose $G = (a)$ where the generator a has order nm $(n, m \neq 1)$. Then $(a^n)^m = e$, while $(a^n)^{m'} \neq e$ for $0 < m' < m$. From this, it is obvious that $((a^n), *)$ is a nontrivial cyclic subgroup of $(G, *)$ with order m.

Corollary. Every group $(G, *)$ of prime order is cyclic.

Proof. Consider the cyclic subgroup $((a), *)$ generated by any $a \in G$, with $a \neq e$. Now, the order of $((a), *)$ must divide the order of $(G, *)$, a prime; since (a) contains more than one element, order $(a) =$ order G, whence $(a) = G$.

As a further application of Lagrange's Theorem, we can now give a simplified proof of Theorem 2–7:

Theorem 2–7. (*Revisited*). Any noncommutative group has at least six elements.

Proof. A group of prime order, being a cyclic group, is necessarily commutative. Accordingly, any group having order 2, 3, or 5 will be commutative. Suppose next that $(G, *)$ is a group of order 4. By Lagrange's Theorem, each element of G distinct from the identity has order 2 or 4. If one of them has order 4, then $(G, *)$ is a cyclic group of order 4 and therefore commutative. On the other hand, a group each of whose elements other than the identity has order 2 must be commutative by Problem 6, Section 2-2. This argument establishes that all groups of order less than 6 are commutative groups.

Incidentally, the implication of Lagrange's Theorem cannot be reversed; that is to say, a group of order n need not have a subgroup of order k, where k is a divisor of n. To be more specific, a group of order 12 exists which has no subgroups of order 6. The particular group we are referring to happens to be a subgroup of the symmetric group $(S_4, \circ)$ and has as its elements:

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

This permutation group does, however, have subgroups of orders 2, 3, and 4.

We shall introduce next a particularly important class of subgroups which we shall refer to as normal subgroups.

Definition 2-24. A subgroup $(H, *)$ of the group $(G, *)$ is said to be *normal* (or invariant) in $(G, *)$ if and only if every left coset of H in G is also a right coset of H in G.

Thus, if $(H, *)$ is normal and $a * H$ is any left coset of H in G, there exists some element $b \in G$ such that

$$a * H = H * b.$$

Since a is in the left coset $a * H$, this means that a is also a member of the right coset $H * b$. The cosets $H * b$ and $H * a$ have the element a in common; so the analog of Theorem 2-28 for right cosets implies that

$$H * b = H * a.$$

In other words, if $a * H$ happens to be a right coset of H, then it must be the right coset $H * a$. This observation allows us to reformulate Definition 2-24 as follows.

Definition 2-25. A subgroup $(H, *)$ is normal in the group $(G, *)$ if and only if $a * H = H * a$ for every $a \in G$.

For a normal subgroup $(H, *)$, we may thus speak simply of the cosets of H in G without specifying right or left. The trivial subgroups are obviously normal. More generally, every subgroup of a commutative group is a normal subgroup.

We will sometimes speak of a *simple* group (in the technical sense), meaning thereby that it has no normal subgroups other than the two trivial ones. For instance, the finite cyclic groups of prime order are simple groups.

Definition 2-25 indicates that normality of a subgroup $(H, *)$ guarantees a weak form of commutativity relative to H. For, if $h \in H$, while it cannot in general be concluded that $a * h = h * a$ for any $a \in G$, we do know that there exists an element $h' \in H$ such that

$$a * h = h' * a.$$

It would be gratifying to have a less cumbersome procedure than to compute cosets for determining whether a given subgroup is in fact a normal subgroup. Just such a criterion is given in the next theorem, and we shall have frequent occasion to make use of it.

Theorem 2-32. The subgroup $(H, *)$ is a normal subgroup of the group $(G, *)$ if and only if for each element $a \in G$,

$$a * H * a^{-1} \subseteq H.$$

Proof. First, assume that $a * H * a^{-1} \subseteq H$ for every $a \in G$. We must prove that in this case $a * H = H * a$. Let $a * h$ be an arbitrary element of $a * H$. Since $a * H * a^{-1} \subseteq H$, $a * h * a^{-1} = h_1$ for some $h_1 \in H$. Thus

$$a * h = (a * h * a^{-1}) * a = h_1 * a.$$

The product $h_1 * a$ lies in the right coset $H * a$, so we conclude that

$$a * H \subseteq H * a.$$

We obtain the opposite inclusion, $H * a \subseteq a * H$, by a similar argument upon observing that our hypothesis also implies

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

Conversely, suppose $a * H = H * a$ for each $a \in G$. Let $a * h_1 * a^{-1}$ be any element in $a * H * a^{-1}$. Then, since $a * H = H * a$, there exists an element

$h_2 \in H$ such that

$$a * h_1 = h_2 * a.$$

Consequently,

$$a * h_1 * a^{-1} = (h_2 * a) * a^{-1} = h_2,$$

which implies $a * H * a^{-1} \subseteq H$.

To demonstrate the convenience of this result, we now prove the following assertion:

(cent G, $*$) is a normal subgroup of each group (G, $*$).

In terms of elements, it must be shown that if $c \in$ cent G and a is arbitrary in G, then $a * c * a^{-1} \in$ cent G. But this is fairly obvious, since from the definition of the center of a group, $a * c = c * a$. It follows at once that

$$a * c * a^{-1} = c * a * a^{-1} = c * e = c \in \text{cent } G.$$

Example 2-37. Let us return to the noncommutative group (G, $\circ$) of order 6 presented in Example 2-22. The reader may recall that the elements of G are functions $f_1, f_2, \ldots, f_6$, while the group operation is functional composition. For convenience, the operation table is reproduced below:

$\circ$	f_1	f_2	f_3	f_4	f_5	f_6
f_1	f_1	f_2	f_3	f_4	f_5	f_6
f_2	f_2	f_1	f_6	f_5	f_4	f_3
f_3	f_3	f_4	f_1	f_2	f_6	f_5
f_4	f_4	f_3	f_5	f_6	f_2	f_1
f_5	f_5	f_6	f_4	f_3	f_1	f_2
f_6	f_6	f_5	f_2	f_1	f_3	f_4

If we take as H the subset $\{f_1, f_4, f_6\}$, then it is easily verified that the pair (H, $\circ$) is a normal subgroup of (G, $\circ$). The coset breakdown for the subgroup in question is

$$f_k \circ H = \{f_1, f_4, f_6\} = H \circ f_k \qquad \text{for} \quad k = 1, 4, 6,$$

$$f_k \circ H = \{f_2, f_3, f_5\} = H \circ f_k \qquad \text{for} \quad k = 2, 3, 5.$$

On the other hand, the subgroup ($\{f_1, f_2\}$, $\circ$) is not normal; a short computation indicates why the criterion of Theorem 2-32 fails to be satisfied:

$$f_4 \circ f_2 \circ f_4^{-1} = f_4 \circ f_2 \circ f_6 = f_5 \notin \{f_1, f_2\}.$$

The significance of normal subgroups—indeed, our main purpose for introducing them—is that they enable us to define new groups which are associated in a natural way with the original group. More specifically, we shall show that the set of cosets of a normal subgroup is itself the set of elements of a group.

If $(H, *)$ is a normal subgroup of the group $(G, *)$, then we shall denote the collection of distinct cosets of H in G by G/H:

$$G/H = \{a * H \mid a \in G\}.$$

These are also right cosets, since the definition of a normal subgroup guarantees that $a * H = H * a$ for every $a \in G$.

A rule of composition $\otimes$ may be defined on G/H by the formula

$$(a * H) \otimes (b * H) = (a * b) * H.$$

Since this definition is stated in terms of coset representatives, we must first show that the multiplication of cosets under $\otimes$ is unambiguously defined, independent of the arbitrary choice of representatives from these sets. That is, it must be shown that if

$$a * H = a_1 * H \qquad \text{and} \qquad b * H = b_1 * H,$$

then also

$$(a * b) * H = (a_1 * b_1) * H.$$

According to Theorem 2–27, it is enough merely to prove that the product

$$(a * b)^{-1} * (a_1 * b_1)$$

is a member of H. Now, $a * H = a_1 * H$ and $b * H = b_1 * H$ imply both $a^{-1} * a_1, b^{-1} * b_1 \in H$. Since $(H, *)$ is normal in $(G, *)$, we know that

$$x * H * x^{-1} \subseteq H$$

for every $x \in G$. In particular,

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

From this we conclude $b^{-1} * (a^{-1} * a_1) * b \in H$ and, since H is closed, that

$$(a * b)^{-1} * (a_1 * b_1) = \big(b^{-1} * (a^{-1} * a_1) * b\big) * (b^{-1} * b_1) \in H.$$

The above argument shows $\otimes$ to be a *well-defined* binary operation on G/H in the sense that the product of two cosets depends only on the cosets involved and in no way on the representative elements chosen from them; any other choice would have yielded the same product.

Having thus prepared the way, we now state and prove the principal result of this section.