2

GROUPS

1. DEFINITIONS AND EXAMPLES OF GROUPS

We have seen in Section 4 of Chapter 1 that given any nonempty set, the set $A(S)$ of all 1-1 mappings of S onto itself is not just a set alone, but has a far richer texture. The possibility of combining two elements of $A(S)$ to get yet another element of $A(S)$ endows $A(S)$ with an algebraic structure. We recall how this was done: If $f, g \in A(S)$, then we combine them to form the mapping fg defined by $(fg)(s) = f(g(s))$ for every $s \in S$. We called fg the *product* of f and g, and verified that $fg \in A(S)$, and that this product obeyed certain rules. From the myriad of possibilities we somehow selected four particular rules that govern the behavior of $A(S)$ relative to this product.

These four rules were

1. *Closure*, namely if $f, g \in A(S)$, then $fg \in A(S)$. We say that $A(S)$ is *closed* under this product.
2. *Associativity*, that is, given $f, g, h \in A(S)$, then $f(gh) = (fg)h$.
3. *Existence of a unit element*, namely, there exists a particular element $i \in A(S)$ (the identity mapping) such that $fi = if = f$ for all $f \in A(S)$.
4. *Existence of inverses*, that is, given $f \in A(S)$ there exists an element, denoted by f^{-1}, in $A(S)$ such that $ff^{-1} = f^{-1}f = i$.

To justify or motivate why these four specific attributes of $A(S)$ were singled out, in contradistinction to some other set of properties, is not easy to

do. In fact, in the history of the subject it took quite some time to recognize that these four properties played the key role. We have the advantage of historical hindsight, and with this hindsight we choose them not only to study $A(S)$, but also as the chief guidelines for abstracting to a much wider context.

Although we saw that the four properties above enabled us to calculate concretely in $A(S)$, there were some differences with the kind of calculations we are used to. If S has three or more elements, we saw in Problem 15, Chapter 1, Section 4 that it is possible for $f, g \in A(S)$ to have $fg \neq gf$. However, this did not present us with insurmountable difficulties.

Without any further polemics we go to the

Definition. A nonempty set G is said to be a *group* if in G there is defined an operation $*$ such that:

(a) $a, b \in G$ implies that $a * b \in G$. (We describe this by saying that G is *closed* under $*$.)

(b) Given $a, b, c \in G$, then $a * (b * c) = (a * b) * c$. (This is described by saying that the *associative law* holds in G.)

(c) There exists a special element $e \in G$ such that $a * e = e * a = a$ for all $a \in G$ (e is called the *identity* or *unit element* of G).

(d) For every $a \in G$ there exists an element $b \in G$ such that $a * b = b * a = e$. (We write this element b as a^{-1} and call it the *inverse* of a in G.)

These four defining postulates (called the *group axioms*) for a group were, after all, patterned after those that hold in $A(S)$. So it is not surprising that $A(S)$ is a group relative to the operation "composition of mappings."

The operation $*$ in G is usually called the *product*, but keep in mind that this has nothing to do with product as we know it for the integers, rationals, reals, or complexes. In fact, as we shall see below, in many familiar examples of groups that come from numbers, what we call the product in these groups is actually the addition of numbers. *However, a general group need have no relation whatsoever to a set of numbers.* We reiterate: A group is no more, no less, than a nonempty set with an operation $*$ satisfying the four group axioms.

Before starting to look into the nature of groups, we look at some examples.

Examples of Groups

1. Let $\mathbb{Z}$ be the set of all integers and let $*$ be the ordinary addition, $+$, in $\mathbb{Z}$. That $\mathbb{Z}$ is closed and associative under $*$ are basic properties of the integers. What serves as the unit element, e, of $\mathbb{Z}$ under $*$? Clearly, since $a = a * e =$

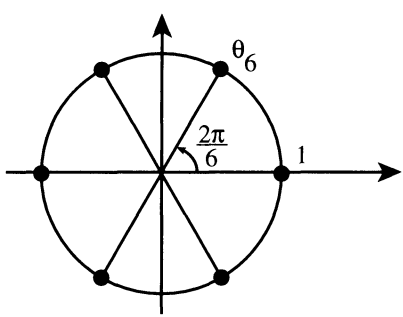
$a + e$, we have $e = 0$, and 0 is the required identity element under addition. What about a^{-1}? Here too, since $e = 0 = a * a^{-1} = a + a^{-1}$, the a^{-1} in this instance is $-a$, and clearly $a * (-a) = a + (-a) = 0$.

2. Let $\mathbb{Q}$ be the set of all rational numbers and let the operation $*$ on $\mathbb{Q}$ be the ordinary addition of rational numbers. As above, $\mathbb{Q}$ is easily shown to be a group under $*$. Note that $\mathbb{Z} \subset \mathbb{Q}$ and both $\mathbb{Z}$ and $\mathbb{Q}$ are groups under the same operation $*$.

3. Let $\mathbb{Q}'$ be the set of all *nonzero* rational numbers and let the operation $*$ on $\mathbb{Q}'$ be the ordinary multiplication of rational numbers. By the familiar properties of the rational numbers we see that $\mathbb{Q}'$ forms a group relative to $*$.

4. Let $\mathbb{R}^+$ be the set of all *positive real* numbers and let the operation $*$ on $\mathbb{R}^+$ be the ordinary product of real numbers. Again it is easy to check that $\mathbb{R}^+$ is a group under $*$.

5. Let E_n be the set of θ_n^i, $i = 0, 1, 2, \ldots, n-1$, where θ_n is the complex number $\theta_n = \cos(2\pi/n) + i \sin(2\pi/n)$. Let $\theta_n^k * \theta_n^j = \theta_n^{k+j}$, the ordinary product of the powers of θ_n as complex numbers. By De Moivre's Theorem we saw that $\theta_n^n = 1$. We leave it to the reader to verify that E_n is a group under $*$. The elements of E_n are called the *n'th roots of unity.* The picture below illustrates the group E_6, whose elements are represented by the dots on the unit circle in the complex plane.



Note one striking difference between the Examples 1 to 4 and Example 5; the first four have an infinite number of elements, whereas E_n has a finite number, n, of elements.

Definition. A group G is said to be a *finite group* if it has a finite number of elements. The number of elements in G is called the *order* of G and is denoted by $|G|$.

Thus E_n above is a finite group, and $|E_n| = n$.

All the examples presented above satisfy the additional property that $a * b = b * a$ for any pair of elements. This need not be true in a group. Just witness the case of $A(S)$, where S has three or more elements; there we saw that we could find $f, g \in A(S)$ such that $fg \neq gf$.

This prompts us to single out as special those groups of G in which $a * b = b * a$ for all $a, b \in G$.

Definition. A group G is said to be *abelian* if $a * b = b * a$ for all $a, b \in G$.

The word abelian derives from the name of the great Norwegian mathematician Niels Henrik Abel (1802–1829), one of the greatest scientists Norway has ever produced.

A group that is not abelian is called *nonabelian*, a not too surprising choice of name.

We now give examples of some nonabelian groups. Of course, the $A(S)$ afford us an infinite family of such. But we present a few other examples in which we can compute quite readily.

6. Let $\mathbb{R}$ be the set of all real numbers, and let G be the set of all mappings $T_{a,b}: \mathbb{R} \to \mathbb{R}$ defined by $T_{a,b}(r) = ar + b$ for any real number r, where a, b are real numbers and $a \neq 0$. Thus, for instance, $T_{5,-6}$ is such that $T_{5,-6}(r) = 5r - 6$; $T_{5,-6}(14) = 5 \cdot 14 - 6 = 64$, $T_{5,-6}(\pi) = 5\pi - 6$. The $T_{a,b}$ are 1-1 mappings of $\mathbb{R}$ onto itself, and we let $T_{a,b} * T_{c,d}$ be the product of two of these mappings. So

$$(T_{a,b} * T_{c,d})(r) = T_{a,b}(T_{c,d}(r)) = aT_{c,d}(r) + b = a(cr + d) + b$$
$$= (ac)r + (ad + b) = T_{ac,\,ad+b}(r).$$

So we have the formula

$$T_{a,b} * T_{c,d} = T_{ac,\,ad+b}. \tag{1}$$

This result shows us that $T_{a,b} * T_{c,d}$ is in G—for it satisfies the membership requirement for belonging to G—so G is closed under $*$. Since we are talking about the product of mappings (i.e., the composition of mappings), $*$ is associative. The element $T_{1,0} = i$ is the identity mapping of $\mathbb{R}$ onto itself. Finally, what is $T_{a,b}^{-1}$? Can we find real numbers $x \neq 0$ and y, such that

$$T_{a,b} * T_{x,y} = T_{x,y} * T_{a,b} = T_{1,0}?$$

Go back to (1) above; we thus want $T_{ax,\,ay+b} = T_{1,0}$, that is, $ax = 1$, $ay + b = 0$. Remember now that $a \neq 0$, so if we put $x = a^{-1}$ and $y = -a^{-1}b$, the required relations are satisfied. One verifies immediately that

$$T_{a,b} * T_{a^{-1},-a^{-1}b} = T_{a^{-1},-a^{-1}b} * T_{a,b} = T_{1,0}.$$

So G is indeed a group.

What is $T_{c,d} * T_{a,b}$? According to the formula given in (1), where we replace a by c, c by a, b by d, d by b, we get

$$T_{c,d} * T_{a,b} = T_{ca,\,cb+d}. \tag{2}$$

Thus $T_{c,d} * T_{a,b} =$ if $T_{a,b} * T_{c,d}$ and only if $bc + d = ad + b$. This fails to be true, for instance, if $a = 1$, $b = 1$, $c = 2$, $d = 3$. So G is nonabelian.

7. Let $H \subset G$, where G is the group in Example 6, and H is defined by $H = \{T_{a,b} \in G \mid a \text{ is rational, } b \text{ any real}\}$. We leave it to the reader to verify that H is a group under the operation $*$ defined on G. H is nonabelian.

8. Let $K \subset H \subset G$, where H, G are as above and $K = \{T_{1,b} \in G \mid b \text{ any real}\}$. The reader should check that K is a group relative to the operation $*$ of G, and *that K is, however, abelian.*

9. Let S be the plane, that is, $S = \{(x, y) \mid x, y \text{ real}\}$ and consider $f, g \in A(S)$ defined by $f(x, y) = (-x, y)$ and $g(x, y) = (-y, x)$; f is the reflection about the y-axis and g is the rotation through 90° in a counterclockwise direction about the origin. We then define $G = \{f^i g^j \mid i = 0, 1; j = 0, 1, 2, 3\}$, and let $*$ in G be the product of elements in $A(S)$. Clearly, $f^2 = g^4 =$ identity mapping;

$$(f * g)(x, y) = (fg)(x, y) = f(g(x, y)) = f(-y, x) = (y, x)$$

and

$$(g * f)(x, y) = g(f(x, y)) = g(-x, y) = (-y, -x).$$

So $g * f \neq f * g$. We leave it to the reader to verify that $g * f = f * g^{-1}$ and G is a nonabelian group of order 8. This group is called the *dihedral group* of order 8. [Try to find a formula for $(f^i g^j) * (f^s g^t) = f^a g^b$ that expresses a, b in terms of i, j, s, and t.]

10. Let S be as in Example 9 and f the mapping in Example 9. Let $n > 2$ and let h be the rotation of the plane about the origin through an angle of $2\pi/n$ in the counterclockwise direction. We then define $G = \{f^k h^j \mid k = 0, 1; j = 0, 1, 2, \ldots, n - 1\}$ and define the product $*$ in G via the usual product of mappings. One can verify that $f^2 = h^n =$ identity mapping, and $fh = h^{-1}f$.

These relations allow us to show (with some effort) that G is a nonabelian group of order $2n$. G is called the *dihedral group* of order $2n$.

11. Let $G = \{ f \in A(S) \mid f(s) \neq s$ for only a finite number of $s \in S\}$, where we suppose that S is an *infinite* set. We claim that G is a group under the product $*$ in $A(S)$. The associativity holds automatically in G, since it already holds in $A(S)$. Also, $i \in G$, since $i(s) = s$ for *all* $s \in S$. So we must show that G is closed under the product and if $f \in G$, then $f^{-1} \in G$.

We first dispose of the closure. Suppose that $f, g \in G$; then $f(s) = s$ except, say, for $s_1, s_2, \ldots, s_n$ and $g(s) = s$ except for $s_1', s_2', \ldots, s_m'$. Then $(fg)(s) = f(g(s)) = s$ for all s other than $s_1, s_2, \ldots, s_n, s_1', \ldots, s_m'$ (and possibly even for some of these). So fg moves only a finite number of elements of S, so $fg \in G$.

Finally, if $f(s) = s$ for all s other than $s_1, s_2, \ldots, s_n$, then $f^{-1}(f(s)) = f^{-1}(s)$, but $f^{-1}(s) = f^{-1}(f(s)) = (f^{-1}f)(s) = i(s) = s$. So we obtain that $f^{-1}(s) = s$ for all s except $s_1, \ldots, s_n$. Thus $f^{-1} \in G$ and G satisfies all the group axioms, hence G is a group.

12. Let G be the set of all mappings T_θ, where T_θ is the rotation of a given circle about its center through an angle θ in the clockwise direction. In G define $*$ by the composition of mappings. Since, as is readily verified, $T_\theta * T_\psi = T_{\theta+\psi}$, G is closed under $*$. The other group axioms check out easily. Note that $T_{2\pi} = T_0 =$ the identity mapping, and $T_\theta^{-1} = T_{-\theta} = T_{2\pi-\theta}$. G is an abelian group.

As we did for $A(S)$ we introduce the shorthand notation a^n for

$$\underbrace{a * a * a \cdots * a}_{n \text{ times}}$$

and define $a^{-n} = (a^{-1})^n$, for n a positive integer, and $a^0 = e$. The usual rules of exponents then hold, that is, $(a^m)^n = a^{mn}$ and $a^m * a^n = a^{m+n}$ for *any* integers m and n.

Note that with this notation, if G is the group of integers under $+$, then a^n is really na.

Having seen the 12 examples of groups above, the reader might get the impression that all, or almost all, sets with some operation $*$ form groups. This is far from true. We now give some examples of nongroups. In each case we check the four group axioms and see which of these fail to hold.

Nonexamples

1. Let G be the set of all integers, and let $*$ be the ordinary product of integers in G. Since $a * b = ab$, for $a, b \in G$ we clearly have that G is closed and associative relative to $*$. Furthermore, the number 1 serves as the unit ele-

ment, since $a * 1 = a1 = a = 1a = 1 * a$ for every $a \in G$. So we are three-fourths of the way to proving that G is a group. All we need is inverses for the elements of G, relative to $*$, to lie in G. But this just isn't so. Clearly, we cannot find an integer b such that $0 * b = 0b = 1$, since $0b = 0$ for all b. But even other integers fail to have inverses in G. For instance, we *cannot find an integer* b such that $3 * b = 1$ (for this would require that $b = \frac{1}{3}$, and $\frac{1}{3}$ is not an integer).

2. Let G be the set of all nonzero real numbers and define, for $a, b \in G$, $a * b = a^2b$; thus $4 * 5 = 4^2(5) = 80$. Which of the group axioms hold in G under this operation $*$ and which fail to hold? Certainly, G is closed under $*$. Is $*$ associative? If so, $(a * b) * c = a * (b * c)$, that is, $(a * b)^2c = a^2(b * c)$, and so $(a^2b)^2c = a^2(b^2c)$, which boils down to $a^2 = 1$, which holds only for $a = \pm 1$. So, in general, the associative law does *not* hold in G relative to $*$. We similarly can verify that G does not have a unit element. Thus even to discuss inverses relative to $*$ would not make sense.

3. Let G be the set of all *positive* integers, under $*$ where $a * b = ab$, the ordinary product of integers. Then one can easily verify that G fails to be a group *only because it fails* to have inverses for some (in fact, most) of its elements relative to $*$.

We shall find some other nonexamples of groups in the exercises.

PROBLEMS

Easier Problems

1. Determine if the following sets G with the operation indicated form a group. If not, point out which of the group axioms fail.
- **(a)** G = set of all integers, $a * b = a - b$.
- **(b)** G = set of all integers, $a * b = a + b + ab$.
- **(c)** G = set of nonnegative integers, $a * b = a + b$.
- **(d)** G = set of all rational numbers $\neq -1$, $a * b = a + b + ab$.
- **(e)** G = set of all rational numbers with denominator divisible by 5 (written so that numerator and denominator are relatively prime), $a * b = a + b$.
- **(f)** G a set having more than one element, $a * b = a$ for all $a, b \in G$.

2. In the group G defined in Example 6, show that the set $H = \{T_{a,b} \mid a = \pm 1, b \text{ any real}\}$ forms a group under the $*$ of G.

3. Verify that Example 7 is indeed an example of a group.

4. Prove that K defined in Example 8 is an abelian group.
5. In Example 9, prove that $g * f = f * g^{-1}$, and that G is a group, is nonabelian, and is of order 8.
6. Let G and H be as in Examples 6 and 7, respectively. Show that if $T_{a,b} \in G$, then $T_{a,b} * V * T_{a,b}^{-1} \in H$ if $V \in H$.
7. Do Problem 6 with H replaced by the group K of Example 8.
8. If G is an abelian group, prove that $(a * b)^n = a^n * b^n$ for all integers n.
9. If G is a group in which $a^2 = e$ for all $a \in G$, show that G is abelian.
10. If G is the group in Example 6, find all $T_{a,b} \in G$ such that $T_{a,b} * T_{1,x} = T_{1,x} * T_{a,b}$ for *all* real x.
11. In Example 10, for $n = 3$ find a formula that expresses $(f^i h^j) * (f^s h^t)$ as $f^a h^b$. Show that G is a nonabelian group of order 6.
12. Do Problem 11 for $n = 4$.
13. Show that any group of order 4 or less is abelian.
14. If G is any group and $a, b, c \in G$, show that if $a * b = a * c$, then $b = c$, and if $b * a = c * a$, then $b = c$.
15. Express $(a * b)^{-1}$ in terms of a^{-1} and b^{-1}.
16. Using the result of Problem 15, prove that a group G in which $a = a^{-1}$ for every $a \in G$ must be abelian.
17. In any group G, prove that $(a^{-1})^{-1} = a$ for all $a \in G$.
18. If G is a finite group of *even* order, show that there must be an element $a \neq e$ such that $a = a^{-1}$. (**Hint:** Try to use the result of Problem 17.)
19. In S_3, show that there are four elements x satisfying $x^2 = e$ and three elements y satisfying $y^3 = e$.
20. Find all the elements in S_4 such that $x^4 = e$.

Middle-Level Problems

21. Show that a group of order 5 must be abelian.
22. Show that the set defined in Example 10 is a group, is nonabelian, and has order $2n$. Do this by finding the formula for $(f^i h^j) * (f^s h^t)$ in the form $f^a h^b$.
23. In the group G of Example 6, find all elements $U \in G$ such that $U * T_{a,b} = T_{a,b} * U$ for every $T_{a,b} \in G$.
24. If G is the dihedral group of order $2n$ as defined in Example 10, prove that:
    (a) If n is odd and $a \in G$ is such that $a * b = b * a$ for all $b \in G$, then $a = e$.
    (b) If n is even, show that there is an $a \in G$, $a \neq e$, such that $a * b = b * a$ for all $b \in G$.

(c) If n is even, find all the elements $a \in G$ such that $a * b = b * a$ for all $b \in G$.

25. If G is any group, show that:

(a) e is unique (i.e., if $f \in G$ also acts as a unit element for G, then $f = e$).

(b) Given $a \in G$, then $a^{-1} \in G$ is unique.

***26.** If G is a finite group, prove that, given $a \in G$, there is a positive integer n, depending on a, such that $a^n = e$.

***27.** In Problem 26, show that there is an integer $m > 0$ such that $a^m = e$ for *all* $a \in G$.

Harder Problems

28. Let G be a set with an operation $*$ such that:

1. G is closed under $*$.
2. $*$ is associative.
3. There exists an element $e \in G$ such that $e * x = x$ for all $x \in G$.
4. Given $x \in G$, there exists a $y \in G$ such that $y * x = e$.

Prove that G is a group. (Thus you must show that $x * e = x$ and $x * y = e$ for e, y as above.)

29. Let G be a *finite* nonempty set with an operation $*$ such that:

1. G is closed under $*$.
2. $*$ is associative.
3. Given $a, b, c \in G$ with $a * b = a * c$, then $b = c$.
4. Given $a, b, c, \in G$ with $b * a = c * a$, then $b = c$.

Prove that G must be a group under $*$.

30. Give an example to show that the result of Problem 29 can be false if G is an infinite set.

31. Let G be the group of all nonzero real numbers under the operation $*$ which is the ordinary multiplication of real numbers, and let H be the group of all real numbers under the operation #, which is the addition of real numbers.

(a) Show that there is a mapping $F: G \to H$ of G onto H which satisfies $F(a * b) = F(a) \# F(b)$ for all $a, b \in G$ [i.e., $F(ab) = F(a) + F(b)$].

(b) Show that no such mapping F can be 1-1.

2. SOME SIMPLE REMARKS

In this short section we show that certain formal properties which follow from the group axioms hold in any group. As a matter of fact, most of these results have already occurred as problems at the end of the preceding section.

It is a little clumsy to keep writing the $*$ for the product in G, and *from now on we shall write the product $a * b$ simply as ab* for all $a, b \in G$.

The first such formal results we prove are contained in

Lemma 2.2.1. If G is a group, then:

(a) Its identity element is *unique*.
(b) Every $a \in G$ has a *unique* inverse $a^{-1} \in G$.
(c) If $a \in G$, $(a^{-1})^{-1} = a$.
(d) For $a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$.

Proof. We start with Part (a). What is expected of us to carry out the proof? We must show that if $e, f \in G$ and $af = fa = a$ for all $a \in G$ and $ae = ea = a$ for all $a \in G$, then $e = f$. This is very easy, for then $e = ef$ and $f = ef$; hence $e = ef = f$, as required.

Instead of proving Part (b), we shall prove a stronger result (listed below as Lemma 2.2.2), which will have Part (b) as an immediate consequence. We claim that in a group G if $ab = ac$, then $b = c$; that is, we can *cancel a given element from the same side of an equation*. To see this, we have, for $a \in G$, an element $u \in G$ such that $ua = e$. Thus from $ab = ac$ we have

$$u(ab) = u(ac),$$

so, by the associative law, $(ua)b = (ua)c$, that is, $eb = ec$. Hence $b = eb = ec = c$, and our result is established. A similar argument shows that if $ba = ca$, then $b = c$. However, we *cannot conclude* from $ab = ca$ that $b = c$; in any abelian group, yes, but in general, no.

Now to get Part (b) as an implication of the cancellation result. Suppose that $b, c \in G$ act as inverses for a; then $ab = e = ac$, so by cancellation $b = c$ and we see that the inverse of a is unique. We shall always write it as a^{-1}.

To see Part (c), note that by definition $a^{-1}(a^{-1})^{-1} = e$; but $a^{-1}a = e$, so by cancellation in $a^{-1}(a^{-1})^{-1} = e = a^{-1}a$ we get that $(a^{-1})^{-1} = a$.

Finally, for Part (d) we calculate

$$\begin{aligned}(ab)(b^{-1}a^{-1}) &= ((ab)b^{-1})a^{-1} \qquad \text{(associative law)} \\ &= (a(bb^{-1})a^{-1} \qquad \text{(again the associative law)} \\ &= (ae)a^{-1} = aa^{-1} = e.\end{aligned}$$

Similarly, $(b^{-1}a^{-1})(ab) = e$. Hence, by definition, $(ab)^{-1} = b^{-1}a^{-1}$. □

We promised to list a piece of the argument given above as a separate lemma. We keep this promise and write

Lemma 2.2.2. In any group G and $a, b, c \in G$, we have:

(a) If $ab = ac$, then $b = c$.

(b) If $ba = ca$, then $b = c$.

Before leaving these results, note that if G is the group of real numbers under $+$, then Part (c) of Lemma 2.2.1 translates into the familiar $-(-a) = a$.

There is only a scant bit of mathematics in this section; accordingly, we give only a few problems. No indication is given as to the difficulty of these.

PROBLEMS

1. Suppose that G is a set closed under an associative operation such that
1. given $a, y \in G$, there is an $x \in G$ such that $ax = y$, and
2. given $a, w \in G$, there is a $u \in G$ such that $ua = w$.

Show that G is a group.

***2.** If G is a *finite* set closed under an associative operation such that $ax = ay$ forces $x = y$ and $ua = wa$ forces $u = w$, for every $a, x, y, u, w \in G$, prove that G is a group. (This is a repeat of a problem given earlier. It will be used in the body of the text later.)

3. If G is a group in which $(ab)^i = a^i b^i$ for three consecutive integers i, prove that G is abelian.

4. Show that the result of Problem 3 would not always be true if the word "three" were replaced by "two." In other words, show that there is a group G and consecutive numbers $i, i + 1$ such that G is not abelian but does have the property that $(ab)^i = a^i b^i$ and $(ab)^{i+1} = a^{i+1} b^{i+1}$ for all a, b in G.

5. Let G be a group in which $(ab)^3 = a^3 b^3$ and $(ab)^5 = a^5 b^5$ for all $a, b \in G$. Show that G is abelian.

6. Let G be a group in which $(ab)^n = a^n b^n$ for some fixed integer $n > 1$ for all $a, b \in G$. For all $a, b \in G$, prove that:

(a) $(ab)^{n-1} = b^{n-1} a^{n-1}$.

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

(c) $(aba^{-1}b^{-1})^{n(n-1)} = e$.

[Hint for Part (c): Note that $(aba^{-1})^r = ab^r a^{-1}$ for all integers r.]

3. SUBGROUPS

In order for us to find out more about the makeup of a given group G, it may be too much of a task to tackle all of G head-on. It might be desirable to focus our attention on appropriate pieces of G, which are smaller, over which we have some control, and are such that the information gathered about them can be used to get relevant information and insight about G itself. The question then becomes: What should serve as suitable pieces for this kind of dissection of G? Clearly, whatever we choose as such pieces, we want them to reflect the fact that G is a group, not merely any old set.

A group is distinguished from an ordinary set by the fact that it is endowed with a well-behaved operation. It is thus natural to demand that such pieces above behave reasonably with respect to the operation of G. Once this is granted, we are led almost immediately to the concept of a subgroup of a group.

Definition. A nonempty subset, H, of a group G is called a *subgroup* of G if, relative to the product in G, H itself forms a group.

We stress the phrase "relative to the product in G." Take, for instance, the subset $A = \{1, -1\}$ in $\mathbb{Z}$, the set of integers. Under the multiplication of integers, A is a group. But A is *not* a subgroup of $\mathbb{Z}$ viewed as a group with respect to $+$.

Every group G automatically has two obvious subgroups, namely G itself and the subgroup consisting of the identity element, e, alone. These two subgroups we call *trivial subgroups*. Our interest will be in the remaining ones, the *proper subgroups* of G.

Before proceeding to a closer look at the general character of subgroups, we want to look at some specific subgroups of some particular, explicit groups. Some of the groups we consider are those we introduced as examples in Section 1; we maintain the numbering given there for them. In some of these examples we shall verify that certain specified subsets are indeed subgroups. We would strongly recommend that the reader carry out such a verification in lots of the others and try to find other examples for themselves.

In trying to verify whether or not a given subset of a group is a subgroup, we are spared checking one of the axioms defining a group, namely the associative law. Since the associative law holds universally in a group G, given any subset A of G and any three elements of A, then the associative law certainly holds for them. So we must check, for a given subset A of G, whether A is closed under the operation of G, whether e is in A, and finally, given $a \in A$, whether a^{-1} is also in A.

Note that we can save one more calculation. Suppose that $A \subset G$ is nonempty and that given $a, b \in A$, then $ab \in A$. Suppose further that given $a \in A$, then $a^{-1} \in A$. Then we assert that $e \in A$. For pick $a \in A$; then $a^{-1} \in A$ by supposition, hence $aa^{-1} \in A$, again by supposition. Since $aa^{-1} = e$, we have that $e \in A$. Thus a is a subgroup of G. In other words,

Lemma 2.3.1. A nonempty subset $A \subset G$ is a subgroup of G if and only if A is closed with respect to the operation of G and, given $a \in A$, then $a^{-1} \in A$.

We now consider some examples.

Examples

1. Let G be the group $\mathbb{Z}$ of integers under $+$ and let H be the set of even integers. We claim that H is a subgroup of $\mathbb{Z}$. Why? Is H closed, that is, given $a, b \in H$, is $a + b \in H$? In other words, if a, b are even integers, is $a + b$ an even integer? The answer is yes, so H is certainly closed under $+$. Now to the inverse. Since the operation in $\mathbb{Z}$ is $+$, the inverse of $a \in \mathbb{Z}$ relative to this operation is $-a$. If $a \in H$, that is, if a is even, then $-a$ is also even, hence $-a \in H$. In short, H is a subgroup of $\mathbb{Z}$ under $+$.

2. Let G once again be the group $\mathbb{Z}$ of integers under $+$. In Example 1, H, the set of even integers, can be described in another way: namely H consists of all multiples of 2. There is nothing particular in Example 1 that makes use of 2 itself. Let $m > 1$ be any integer and let H_m consist of all multiples of m in $\mathbb{Z}$. We leave it to the reader to verify that H_m is a subgroup of $\mathbb{Z}$ under $+$.

3. Let S be any nonempty set and let $G = A(S)$. If $a \in S$, let $H(a) = \{f \in A(S) \mid f(a) = a\}$. We claim that $H(a)$ is a subgroup of G. For if $f, g \in H(a)$, then $(fg)(a) = f(g(a)) = f(a) = a$, since $f(a) = g(a) = a$. Thus $fg \in H(a)$. Also, if $f \in H(a)$, then $f(a) = a$, so that $f^{-1}(f(a)) = f^{-1}(a)$. But $f^{-1}(f(a)) = f^{-1}(a) = i(a) = a$. Thus, since $a = f^{-1}(f(a)) = f^{-1}(a)$, we have that $f^{-1} \in H(a)$. Moreover, H is nonempty. (Why?) Consequently, $H(a)$ is a subgroup of G.

4. Let G be as in Example 6 of Section 1, and H as in Example 7. Then H is a subgroup of G (see Problem 3 in Section 1).

5. Let G be as in Example 6, H as in Example 7, and K as in Example 8 in Section 1. Then $K \subset H \subset G$ and K is a subgroup of both H and of G.

6. Let $\mathbb{C}'$ be the nonzero complex numbers as a group under the multiplication of complex numbers. Let $V = \{a \in \mathbb{C}' \mid |a| \text{ is rational}\}$. Then V is a subgroup of $\mathbb{C}'$. For if $|a|$ and $|b|$ are rational, then $|ab| = |a|\,|b|$ is rational, so

$ab \in V$; also, $|a^{-1}| = 1/|a|$ is rational, hence $a^{-1} \in V$. Therefore, V is a subgroup of $\mathbb{C}'$.

7. Let $\mathbb{C}'$ and V be as above and let

$$U = \{a \in \mathbb{C}' \mid a = \cos\theta + i\sin\theta, \theta \text{ any real}\}.$$

If $a = \cos\theta + i\sin\theta$ and $b = \cos\psi + i\sin\psi$, we saw in Chapter 1 that $ab = \cos(\theta + \psi) + i\sin(\theta + \psi)$, so that $ab \in U$, and that $a^{-1} = \cos\theta - i\sin\theta = \cos(-\theta) + i\sin(-\theta) \in U$. Also, $|a| = 1$, since $|a| = \sqrt{\cos^2\theta + \sin^2\theta} = 1$. Therefore, $U \subset V \subset \mathbb{C}'$ and U is a subgroup both of V and of $\mathbb{C}'$.

8. Let $\mathbb{C}'$, U, V be as above, and let $n > 1$ be an integer. Let $\theta_n = \cos(2\pi/n) + i\sin(2\pi/n)$, and let $B = \{1, \theta_n, \theta_n^2, \ldots, \theta_n^{n-1}\}$. Since $\theta_n^n = 1$ (as we saw by De Moivre's Theorem), it is easily checked that B is a subgroup of U, V, and $\mathbb{C}'$, and is of order n.

9. Let G be any group and let $a \in G$. The set $A = \{a^i \mid i \text{ any integer}\}$ is a subgroup of G. For, by the rules of exponents, if $a^i \in A$ and $a^j \in A$, then $a^i a^j = a^{i+j}$, so is in A. Also, $(a^i)^{-1} = a^{-i}$, so $(a^i)^{-1} \in A$. This makes A into a subgroup of G.

A is the cyclic subgroup of G generated by a in the following sense.

Definition. The *cyclic subgroup of* G generated by a is a set $\{a^i \mid i \text{ any integer}\}$. It is denoted (a).

Note that if e is the identity element of G, then $(e) = \{e\}$. In Example 8, the group B is the cyclic group (θ_n) of $\mathbb{C}$ generated by θ_n.

10. Let G be any group; for $a \in G$ let $C(a) = \{g \in G \mid ga = ag\}$. We claim that $C(a)$ is a subgroup of G. First, the closure of $C(a)$. If $g, h \in C(a)$, then $ga = ag$ and $ha = ah$, thus $(gh)a = g(ha) = g(ah) = (ga)h = (ag)h = a(gh)$ (by the repeated use of the associative law), hence $gh \in C(a)$. Also, if $g \in C(a)$, then from $ga = ag$ we have $g^{-1}(ga)g^{-1} = g^{-1}(ag)g^{-1}$, which simplifies to $ag^{-1} = g^{-1}a$; whence $g^{-1} \in C(a)$. So, $C(a)$ is thereby a subgroup of G.

These particular subgroups $C(a)$ will come up later for us and they are given a special name. We call $C(a)$ the *centralizer* of a in G. If in a group $ab = ba$, we say that a and b *commute*. Thus $C(a)$ is the set of all elements in G that commute with a.

11. Let G be any group and let $Z(G) = \{z \in G \mid zx = xz \text{ for all } x \in G\}$. We leave it to the reader to verify that $Z(G)$ is a subgroup of G. It is called the *center* of G.

12. Let G be any group and H a subgroup of G. For $a \in G$, let $a^{-1}Ha = \{a^{-1}ha \mid h \in H\}$. We assert that $a^{-1}Ha$ is a subgroup of G. If $x = a^{-1}h_1a$ and $y = a^{-1}h_2a$ where $h_1, h_2 \in H$, then $xy = (a^{-1}h_1a)(a^{-1}h_2a) = a^{-1}(h_1h_2)a$ (associative law), and since H is a subgroup of G, $h_1h_2 \in H$. Therefore, $a^{-1}(h_1h_2)a \in a^{-1}Ha$, which says that $xy \in a^{-1}Ha$. Thus $a^{-1}Ha$ is closed. Also, if $x = a^{-1}ha \in a^{-1}Ha$, then, as is easily verified, $x^{-1} = (a^{-1}ha)^{-1} = a^{-1}h^{-1}a \in a^{-1}Ha$. Therefore, $a^{-1}Ha$ is a subgroup of G.

An even dozen seems to be about the right number of examples, so we go on to other things. Lemma 2.3.1 points out for us what we need in order that a given subset of a group be a subgroup. In an important special case we can make a considerable saving in checking whether a given subset H is a subgroup of G. This is the case in which H is *finite*.

Lemma 2.3.2. Suppose that G is a group and H a nonempty *finite* subset of G closed under the product in G. Then H is a subgroup of G.

Proof. By Lemma 2.3.1 we must show that $a \in H$ implies $a^{-1} \in H$. If $a = e$, then $a^{-1} = e$ and we are done. Suppose then that $a \neq e$; consider the elements $a, a^2, \ldots, a^{n+1}$, where $n = |H|$, the order of H. *Here we have written down $n + 1$ elements, all of them in H since H is closed, and H has only n distinct elements.* How can this be? Only if some two of the elements listed are equal; put another way, only if $a^i = a^j$ for some $1 \leq i < j \leq n + 1$. But then, by the cancellation property in groups, $a^{j-i} = e$. Since $j - i \geq 1$, $a^{j-i} \in H$, hence $e \in H$. However, $j - i - 1 \geq 0$, so $a^{j-i-1} \in H$ and $aa^{j-i-1} = a^{j-i} = e$, whence $a^{-1} = a^{j-i-1} \in H$. This proves the lemma. □

An immediate, but nevertheless important, corollary to Lemma 2.3.2 is the

Corollary. If G is a finite group and H a nonempty subset of G closed under multiplication, then H is a subgroup of G.

PROBLEMS

Easier Problems

1. If A, B are subgroups of G, show that $A \cap B$ is a subgroup of G.
2. What is the cyclic subgroup of $\mathbb{Z}$ generated by -1 under $+$?
3. Let S_3 be the symmetric group of degree 3. Find all the subgroups of S_3.
4. Verify that $Z(G)$, the center of G, is a subgroup of G. (See Example 11.)

5. If $C(a)$ is the centralizer of a in G (Example 10), prove that $Z(G) = \cap_{a \in G} C(a)$.
6. Show that $a \in Z(G)$ if and only if $C(a) = G$.
7. In S_3, find $C(a)$ for each $a \in S_3$.
8. If G is an abelian group and if $H = \{a \in G \mid a^2 = e\}$, show that H is a subgroup of G.
9. Give an example of a nonabelian group for which the H in Problem 8 is *not* a subgroup.
10. If G is an abelian group and $n > 1$ an integer, let $A_n = \{a^n \mid a \in G\}$. Prove that A_n is a subgroup of G.
*11. If G is an abelian group and $H = \{a \in G \mid a^{n(a)} = e$ for some $n(a) > 1$ depending on $a\}$, prove that H is a subgroup of G.

We say that a group G is *cyclic* if there exists an $a \in G$ such that every $x \in G$ is a power of a, that is, $x = a^j$ for some j. In other words, G is cyclic if $G = (a)$ for some $a \in G$, in which case we say that a is a *generator* for G.

*12. Prove that a cyclic group is abelian.
13. If G is cyclic, show that every subgroup of G is cyclic.
14. If G has no proper subgroups, prove that G is cyclic.
15. If G is a group and H a nonempty subset of G such that, given $a, b \in H$, then $ab^{-1} \in H$, prove that H is a subgroup of G.

Middle-Level Problems

*16. If G has no proper subgroups, prove that G is cyclic of order p, where p is a prime number. (This sharpens the result of Problem 14.)
17. If G is a group and $a, x \in G$, prove that $C(x^{-1}ax) = x^{-1}C(a)x$. [See Examples 10 and 12 for the definitions of $C(b)$ and of $x^{-1}C(a)x$.]
18. If S is a nonempty set and $X \subset S$, show that $T(X) = \{f \in A(S) \mid f(X) \subset X\}$ is a subgroup of $A(S)$ *if X is finite.*
19. If A, B are subgroups of an abelian group G, let $AB = \{ab \mid a \in A, b \in B\}$. Prove that AB is a subgroup of G.
20. Give an example of a group G and two subgroups A, B of G such that AB is *not* a subgroup of G.
21. If A, B are subgroups of G such that $b^{-1}Ab \subset A$ for all $b \in B$, show that AB is a subgroup of G.
*22. If A and B are finite subgroups, of orders m and n, respectively, of the abelian group G, prove that AB is a subgroup of order mn *if m and n are relatively prime.*

23. What is the order of AB in Problem 22 if m and n are not relatively prime?

24. If H is a subgroup of G, let $N = \cap_{x \in G} x^{-1}Hx$. Prove that N is a subgroup of G such that $y^{-1}Ny = N$ for every $y \in G$.

Harder Problems

25. Let S, X, $T(X)$ be as in Problem 18 (but X no longer finite). Give an example of a set S and an infinite subset X such that $T(X)$ is *not* a subgroup of $A(S)$.

***26.** Let G be a group, H a subgroup of G. Let $Hx = \{hx \mid h \in H\}$. Show that, given $a, b \in G$, then $Ha = Hb$ or $Ha \cap Hb = \emptyset$.

***27.** If in Problem 26 H is a finite subgroup of G, prove that Ha and Hb have the same number of elements. What is this number?

28. Let M, N be subgroups of G such that $x^{-1}Mx \subset M$ and $x^{-1}Nx \subset N$ for all $x \in G$. Prove that MN is a subgroup of G and that $x^{-1}(MN)x \subset MN$ for all $x \in G$.

***29.** If M is a subgroup of G such that $x^{-1}Mx \subset M$ for all $x \in G$, prove that actually $x^{-1}Mx = M$.

30. If M, N are such that $x^{-1}Mx = M$ and $x^{-1}Nx = N$ for all $x \in G$, and if $M \cap N = (e)$, prove that $mn = nm$ for any $m \in M$, $n \in N$. (**Hint:** Consider the element $m^{-1}n^{-1}mn$.)

4. LAGRANGE'S THEOREM

We are about to derive the first real group-theoretic result of importance. Although its proof is relatively easy, this theorem is like the A-B-C's for finite groups and has interesting implications in number theory.

As a matter of fact, those of you who solved Problems 26 and 27 of Section 3 have all the necessary ingredients to effect a proof of the result. The theorem simply states that in a finite group the order of a subgroup divides the order of the group.

To smooth the argument of this theorem—which is due to Lagrange—and for use many times later, we make a short detour into the realm of set theory.

Just as the concept of "function" runs throughout most phases of mathematics, so also does the concept of "relation." A *relation* is a statement aRb about the elements $a, b \in S$. If S is the set of integers, $a = b$ is a relation on S. Similarly, $a < b$ is a relation on S, as is $a \leq b$.

Definition. A relation $\sim$ on a set S is called an *equivalence relation* if, for all $a, b, c \in S$, it satisfies:

(a) $a \sim a$ (*reflexivity*).
(b) $a \sim b$ implies that $b \sim a$ (*symmetry*).
(c) $a \sim b$, $b \sim c$ implies that $a \sim c$ (*transitivity*).

Of course, equality, $=$, is an equivalence relation, so the general notion of equivalence relation is a generalization of that of equality. In a sense, an equivalence relation measures equality with regard to some attribute. This vague remark may become clearer after we see some examples.

Examples

1. Let S be all the items for sale in a grocery store; we declare $a \sim b$, for $a, b \in S$, if the price of a equals that of b. Clearly, the defining rules of an equivalence relation hold for this $\sim$. Note that in measuring this "generalized equality" on S we ignore all properties of the elements of S other than their price. So $a \sim b$ if they are equal as far as the attribute of price is concerned.

2. Let S be the integers and $n > 1$ a fixed integer. We define $a \sim b$ for $a, b \in S$ if $n \mid (a - b)$. We verify that this is an equivalence relation. Since $n \mid 0$ and $0 = a - a$, we have $a \sim a$. Because $n \mid (a - b)$ implies that $n \mid (b - a)$, we have that $a \sim b$ implies that $b \sim a$. Finally, if $a \sim b$ and $b \sim c$, then $n \mid (a - b)$ and $n \mid (b - c)$; hence $n \mid ((a - b) + (b - c))$, that is, $n \mid (a - c)$. Therefore, $a \sim c$.

This relation on the integers is of great importance in number theory and is called *congruence modulo* n; when $a \sim b$, we write this as $a \equiv b \bmod n$ [or, sometimes, as $a \equiv b(n)$], which is read "a congruent to b mod n." We'll be running into it very often from now on. As we shall see, this is a special case of a much wider phenomenon in groups.

3. We generalize Example 2. Let G be a group and H a subgroup of G. For $a, b \in G$, define $a \sim b$ if $ab^{-1} \in H$. Since $e \in H$ and $e = aa^{-1}$, we have that $a \sim a$. Also, if $ab^{-1} \in H$, then since H is a subgroup of G, $(ab^{-1})^{-1} \in H$. But $(ab^{-1})^{-1} = (b^{-1})^{-1}a^{-1} = ba^{-1}$, so $ba^{-1} \in H$, hence $b \sim a$. This tells us that $a \sim b$ implies that $b \sim a$. Finally, if $a \sim b$ and $b \sim c$, then $ab^{-1} \in H$ and $bc^{-1} \in H$. But $(ab^{-1})(bc^{-1}) = ac^{-1}$, whence $ac^{-1} \in H$ and therefore $a \sim c$. We have shown the transitivity of $\sim$, thus $\sim$ is an equivalence relation on G.

Note that if $G = \mathbb{Z}$, the group of integers under $+$, and H is the subgroup consisting of all multiples of n, for $n > 1$ a fixed integer, then $ab^{-1} \in H$

translates into $a \equiv b(n)$. So congruence mod n is a very special case of the equivalence we have defined in Example 3.

It is this equivalence relation that we shall use in proving Lagrange's theorem.

4. Let G be any group. For $a, b \in G$ we declare that $a \sim b$ if there exists an $x \in G$ such that $b = x^{-1}ax$. We claim that this defines an equivalence relation on G. First, $a \sim a$ for $a = e^{-1}ae$. Second, if $a \sim b$, then $b = x^{-1}ax$, hence $a = (x^{-1})^{-1}b(x^{-1})$, so that $b \sim a$. Finally, if $a \sim b$, $b \sim c$, then $b = x^{-1}ax$, $c = y^{-1}by$ for some $x, y \in G$. Thus $c = y^{-1}(x^{-1}ax)y = (xy)^{-1}a(xy)$, and so $a \sim c$. We have established that this defines an equivalence relation on G.

This relation, too, plays an important role in group theory and is given the special name *conjugacy*. When $a \sim b$ we say that "*a and b are conjugate in G.*" Note that if G is abelian, then $a \sim b$ if and only if $a = b$.

We could go on and on to give numerous interesting examples of equivalence relations, but this would sidetrack us from our main goal in this section. There will be no lack of examples in the problems at the end of this section.

We go on with our discussion and make the

Definition. If $\sim$ is an equivalence relation on S, then $[a]$, the *class* of a, is defined by $[a] = \{b \in S \mid b \sim a\}$.

Let us see what the class of a is in the two examples, Examples 3 and 4, just given.

In Example 3, $a \sim b$ if $ab^{-1} \in H$, that is, if $ab^{-1} = h$, for some $h \in H$. Thus $a \sim b$ implies that $a = hb$. On the other hand, if $a = kb$ where $k \in H$, then $ab^{-1} = (kb)b^{-1} = k \in H$, so $a \sim b$ if and only if $a \in Hb = \{hb \mid h \in H\}$. Therefore, $[b] = Hb$.

The set Hb is called a *right coset of H* in G. We ran into such in Problem 26 of Section 3. Note that $b \in Hb$, since $b = eb$ and $e \in H$ (also because $b \in [b] = Hb$). Right cosets, and left handed counterparts of them called *left cosets*, play important roles in what follows.

In Example 4, we defined $a \sim b$ if $b = x^{-1}ax$ for some $x \in G$. Thus $[a] = \{x^{-1}ax \mid x \in G\}$. We shall denote $[a]$ in this case as $\mathrm{cl}(a)$ and call it the *conjugacy class* of a in G. If G is abelian, then $\mathrm{cl}(a)$ consists of a alone. In fact, if $a \in Z(G)$, the center of G, then $\mathrm{cl}(a)$ consists merely of a.

The notion of conjugacy and its properties will crop up again often, especially in Section 11.

We shall examine the class of an element a in Example 2 later in this chapter.

The important influence that an equivalence relation has on a set is to break it up and *partition* it into nice disjoint pieces.

Theorem 2.4.1. If $\sim$ is an equivalence relation on S, then $S = \cup[a]$, where this union runs over one element from each class, and where $[a] \neq [b]$ implies that $[a] \cap [b] = \emptyset$. That is, $\sim$ partitions S into equivalence classes.

Proof. Since $a \in [a]$, we have $\cup_{a \in S}[a] = S$. The proof of the second assertion is also quite easy. We show that if $[a] \neq [b]$, then $[a] \cap [b] = \emptyset$, or, what is equivalent to this, if $[a] \cap [b] \neq \emptyset$, then $[a] = [b]$.

Suppose, then, that $[a] \cap [b] \neq \emptyset$; let $c \in [a] \cap [b]$. By definition of class, $c \sim a$ since $c \in [a]$ and $c \sim b$ since $c \in [b]$. Therefore, $a \sim c$ by symmetry of $\sim$, and so, since $a \sim c$ and $c \sim b$, we have $a \sim b$. Thus $a \in [b]$; if $x \in [a]$, then $x \sim a$, $a \sim b$ gives us that $x \sim b$, hence $x \in [b]$. Thus $[a] \subset [b]$. The argument is obviously symmetric in a and b, so we have $[b] \subset [a]$, whence $[a] = [b]$, and our assertion above is proved.

The theorem is now completely proved. □

We now can prove a famous result of Lagrange.

Theorem 2.4.2 (Lagrange's Theorem). If G is a finite group and H is a subgroup of G, then the order of H divides the order of G.

Proof. Let us look back at Example 3, where we established that the relation $a \sim b$ if $ab^{-1} \in H$ is an equivalence relation and that

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

Let k be the number of distinct classes—call them $Ha_1, \ldots, Ha_k$. By Theorem 2.4.1, $G = Ha_1 \cup Ha_2 \cup \cdots \cup Ha_k$ and we know that $Ha_j \cap Ha_i = \emptyset$ if $i \neq j$.

We assert that any Ha_i has $|H|$ = order of H number of elements. Map $H \to Ha_i$ by sending $h \to ha_i$. We claim that this map is 1-1, for if $ha_i = h'a_i$, then by cancellation in G we would have $h = h'$; thus the map is 1-1. It is definitely onto by the very definition of Ha_i. So H and Ha_i have the same number, $|H|$, of elements.

Since $G = Ha_1 \cup \cdots \cup Ha_k$ and the Ha_i are disjoint and each Ha_i has $|H|$ elements, we have that $|G| = k|H|$. Thus $|H|$ divides $|G|$ and Lagrange's Theorem is proved. □

Although Lagrange sounds like a French name, J. L. Lagrange (1736–1813) was actually Italian, having been born and brought up in Turin. He spent most of his life, however, in France. Lagrange was a great mathematician who made fundamental contributions to all the areas of mathematics of his day.

If G is finite, the number of right cosets of H in G, namely $|G|/|H|$, is called the *index* of H in G and is written as $i_G(H)$.

Recall that a group G is said to be *cyclic* if there is an element $a \in G$ such that every element in G is a power of a.

Theorem 2.4.3. A group G of prime order is cyclic.

Proof. If H is a subgroup of G then, by invoking Lagrange's Theorem, $|H|$ divides $|G| = p$, p a prime, so $|H| = 1$ or p. So if $H \neq (e)$, then $H = G$. If $a \in G$, $a \neq e$, then the powers of a form a subgroup (a) of G different from (e). So this subgroup is all of G. This says that any $x \in G$ is of the form $x = a^i$. Hence, G is cyclic by the definition of cyclic group. □

If G is finite and $a \in G$, we saw earlier in the proof of Lemma 2.3.2 that $a^{n(a)} = e$ for some $n(a) \geq 1$, depending on a. We make the

Definition. If G is finite, then the *order* of a, written $o(a)$, is the *least positive integer* m such that $a^m = e$.

Suppose that $a \in G$ has order m. Consider the set $A = \{e, a, a^2, \ldots, a^{m-1}\}$; we claim that A is a subgroup of G (since $a^m = e$) and that the m elements listed in A are distinct. We leave the verification of these claims to the reader. Thus $|A| = m = o(a)$. Since $|A| \mid |G|$, we have

Theorem 2.4.4. If G is finite and $a \in G$, then $o(a) \mid |G|$.

If $a \in G$, where G is finite, we have, by Theorem 2.4.4, $|G| = k \cdot o(a)$. Thus

$$a^{|G|} = a^{k \cdot o(a)} = (a^{o(a)})^k = e^k = e.$$

We have proved the

Theorem 2.4.5. If G is a finite group of order n, then $a^n = e$ for all $a \in G$.

When we apply this last result to certain special groups arising in number theory, we shall obtain some classical number-theoretic results due to Fermat and Euler.

Let $\mathbb{Z}$ be the integers and let $n > 1$ be a fixed integer. We go back to Example 2 of equivalence relations, where we defined $a \equiv b \bmod n$ (a congruent to $b \bmod n$) if $n \mid (a - b)$. The class of a, $[a]$, consists of all $a + nk$, where k runs through all the integers. We call it the *congruence class* of a.

By Euclid's Algorithm, given any integer b, $b = qn + r$, where $0 \leq r < n$, thus $[b] = [r]$. So the n classes $[0], [1], \ldots, [n-1]$ give us all the congruence classes. We leave it to the reader to verify that they are distinct.

Let $\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}$. We shall introduce two operations, $+$ and $\cdot$ in $\mathbb{Z}_n$. Under $+$ $\mathbb{Z}_n$ will form an abelian group; under $\cdot$ $\mathbb{Z}_n$ will not form a group, but a certain piece of it will become a group.

How to define $[a] + [b]$? What is more natural than to define

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

But there is a fly in the ointment. Is this operation $+$ in $\mathbb{Z}_n$ well-defined? What does that mean? We can represent $[a]$ by many a's—for instance, if $n = 3$, $[1] = [4] = [-2] = \cdots$, yet we are using a *particular* a to define the addition. What we must show is that if $[a] = [a']$ and $[b] = [b']$, then $[a + b] = [a' + b']$, for then we will have $[a] + [b] = [a + b] = [a' + b'] = [a'] + [b']$.

Suppose that $[a] = [a']$; then $n \mid (a - a')$. Also from $[b] = [b']$, $n \mid (b - b')$, hence $n \mid ((a - a') + (b - b')) = ((a + b) - (a' + b'))$. Therefore, $a + b \equiv (a' + b') \bmod n$, and so $[a + b] = [a' + b']$.

So we now have a well-defined addition in $\mathbb{Z}_n$. The element $[0]$ acts as the identity element and $[-a]$ acts as $-[a]$, the inverse of $[a]$. We leave it to the reader to check out that $\mathbb{Z}_n$ is a group under $+$. It is a cyclic group of order n generated by $[1]$.

We summarize this all as

Theorem 2.4.6. $\mathbb{Z}_n$ forms a cyclic group under the addition $[a] + [b] = [a + b]$.

Having disposed of the addition in $\mathbb{Z}_n$, we turn to the introduction of a multiplication. Again, what is more natural than defining

$$[a] \cdot [b] = [ab]?$$

So, for instance, if $n = 9$, $[2][7] = [14] = [5]$, and $[3][6] = [18] = [0]$. Under this multiplication—we leave the fact that it is well-defined to the reader—$\mathbb{Z}_n$ *does not form* a group. Since $[0][a] = [0]$ for all a, and the unit element under multiplication is $[1]$, $[0]$ cannot have a multiplicative inverse. Okay, why not try the nonzero elements $[a] \neq [0]$ as a candidate for a group under this product? Here again it is no go *if n is not a prime.* For instance, if $n = 6$, then $[2] \neq [0]$, $[3] \neq [0]$, yet $[2][3] = [6] = [0]$, so the nonzero elements do not, in general, give us a group.

So we ask: Can we find an appropriate piece of $\mathbb{Z}_n$ that will form a

group under multiplication? Yes! Let $U_n = \{[a] \in \mathbb{Z}_n \mid (a, n) = 1\}$, noting that $(a, n) = 1$ if and only if $(b, n) = 1$ for $[a] = [b]$. By the Corollary to Theorem 1.5.5, if $(a, n) = 1$ and $(b, n) = 1$, then $(ab, n) = 1$. So $[a][b] = [ab]$ yields that if $[a], [b] \in U_n$, then $[ab] \in U_n$ and U_n is closed. Associativity is easily checked, following from the associativity of the integers under multiplication. The identity element is easy to find, namely [1]. Multiplication is commutative in U_n.

Note that if $[a][b] = [a][c]$ where $[a] \in U_n$, then we have $[ab] = [ac]$, and so $[ab - ac] = [0]$. This says that $n \mid a(b - c) = ab - ac$; but a is relatively prime to n. By Theorem 1.5.5 one must have that $n \mid (b - c)$, and so $[b] = [c]$. In other words, we have the cancellation property in U_n. By Problem 2 of Section 2, U_n is a group.

What is the order of U_n? By the definition of U_n, $|U_n|$ = number of integers $1 \leq m < n$ such that $(m, n) = 1$. This number comes up often and we give it a name.

Definition. The *Euler φ-function*, $\varphi(n)$, is defined by $\varphi(1) = 1$ and, for $n > 1$, $\varphi(n)$ = the number of positive integers m with $1 \leq m < n$ such that $(m, n) = 1$.

Thus $|U_n| = \varphi(n)$. If $n = p$, a prime, we have $\varphi(p) = p - 1$. We see that $\varphi(8) = 4$ for only 1, 3, 5, 7 are less than 8 and positive and relatively prime to 8. We try another one, $\varphi(15)$. The numbers $1 \leq m < 15$ relatively prime to 15 are 1, 2, 4, 7, 8, 11, 13, 14, so $\varphi(15) = 8$.

Let us look at some examples of U_n.

1. $U_8 = \{[1], [3], [5], [7]\}$. Note that $[3][5] = [15] = [7]$, $[5]^2 = [25] = [1]$. In fact, U_8 is a group of order 4 in which $a^2 = e$ for every $a \in U_8$.

2. $U_{15} = \{[1], [2], [4], [7], [8], [11], [13], [14]\}$. Note that $[11][13] = [143] = [8]$, $[2]^4 = [1]$, and so on.

The reader should verify that $a^4 = e = [1]$ for every $a \in U_{15}$.

3. $U_9 = \{[1], [2], [4], [5], [7], [8]\}$. Note that $[2]^1 = [2]$, $[2]^2 = [4]$, $[2]^3 = [8]$, $[2^4] = [16] = [7]$, $[2]^5 = [32] = [5]$; also $[2]^6 = [2][2]^5 = [2][5] = [10] = [1]$. So the powers of [2] give us every element in U_9. Thus U_9 is a *cyclic* group of order 6. What other elements in U_9 generate U_9?

In parallel to Theorem 2.4.6 we have

Theorem 2.4.7. U_n forms an abelian group, under the product $[a][b] = [ab]$, of order $\varphi(n)$, where $\varphi(n)$ is the Euler φ-function.

An immediate consequence of Theorems 2.4.7 and 2.4.5 is a famous result in number theory.

Theorem 2.4.8 (Euler). If a is an integer relatively prime to n, then $a^{\varphi(n)} \equiv 1 \bmod n$.

Proof. U_n forms a group of order $\varphi(n)$, so by Theorem 2.4.5, $a^{\varphi(n)} = e$ for all $a \in U_n$. This translates into $[a^{\varphi(n)}] = [a]^{\varphi(n)} = [1]$, which in turn translates into $n \mid (a^{\varphi(n)} - 1)$ for every integer a relatively prime to p. In other words, $a^{\varphi(n)} \equiv 1 \bmod n$. □

A special case, where $n = p$ is a prime, is due to Fermat.

Corollary (Fermat). If p is a prime and $p \nmid a$, then

$$a^{p-1} \equiv 1 \bmod p.$$

For any integer b, $b^p \equiv b \bmod p$.

Proof. Since $\varphi(p) = p - 1$, if $(a, p) = 1$, we have, by Theorem 2.4.8, that $a^{p-1} \equiv 1(p)$, hence $a^1 \cdot a^{p-1} \equiv a(p)$, so that $a^p \equiv a(p)$. If $p \mid b$, then $b \equiv 0(p)$ and $b^p \equiv 0(p)$, so that $b^p \equiv b(p)$. □

Leonard Euler (1707–1785) was probably the greatest scientist that Switzerland has produced. He was the most prolific of all mathematicians ever.

Pierre Fermat (1601–1665) was a great number theorist. Fermat's Last Theorem—which was in fact first proved in 1994 by Andrew Wiles—states that the equation $a^n + b^n = c^n$ (a, b, c, n being integers) has only the trivial solution where $a = 0$ or $b = 0$ or $c = 0$ if $n > 2$.

One final cautionary word about Lagrange's Theorem. Its *converse* in general is *not* true. That is, if G is a finite group of order n, then it need not be true that for every divisor m of n there is a subgroup of G of order m. A group with this property is very special indeed, and its structure can be spelled out quite well and precisely.

PROBLEMS

Easier Problems

1. Verify that the relation $\sim$ is an equivalence relation on the set S given.

(a) $S = \mathbb{R}$ reals, $a \sim b$ if $a - b$ is rational.

(b) $S = \mathbb{C}$, the complex numbers, $a \sim b$ if $|a| = |b|$.

(c) $S =$ straight lines in the plane, $a \sim b$ if a, b are parallel.

(d) $S =$ set of all people, $a \sim b$ if they have the same color eyes.

2. The relation $\sim$ on the real numbers $\mathbb{R}$ defined by $a \sim b$ if both $a > b$ and $b > a$ is *not* an equivalence relation. Why not? What properties of an equivalence relation does it satisfy?

3. Let $\sim$ be a relation on a set S that satisfies (1) $a \sim b$ implies that $b \sim a$ and (2) $a \sim b$ and $b \sim c$ implies that $a \sim c$. These seem to imply that $a \sim a$. For if $a \sim b$, then by (1), $b \sim a$, so $a \sim b$, $b \sim a$, so by (2), $a \sim a$. If this argument is correct, then the relation $\sim$ must be an equivalence relation. Problem 2 shows that this is not so. What is wrong with the argument we have given?

4. Let S be a set, $\{S_\alpha\}$ nonempty subsets such that $S = \cup_\alpha S_\alpha$ and $S_\alpha \cap S_\beta = \emptyset$ if $\alpha \neq \beta$. Define an equivalence relation on S in such a way that the S_α are precisely all the equivalence classes.

*** 5.** Let G be a group and H a subgroup of G. Define, for $a, b \in G$, $a \sim b$ if $a^{-1}b \in H$. Prove that this defines an equivalence relation on G, and show that $[a] = aH = \{ah \mid h \in H\}$. The sets aH are called *left cosets* of H in G.

6. If G is S_3 and $H = \{i, f\}$, where $f: S \to S$ is defined by $f(x_1) = x_2, f(x_2) = x_1, f(x_3) = x_3$, list all the right cosets of H in G and list all the left cosets of H in G.

7. In Problem 6, is every right coset of H in G also a left coset of H in G?

8. If every right coset of H in G is a left coset of H in G, prove that $aHa^{-1} = H$ for all $a \in G$.

9. In $\mathbb{Z}_{16}$, write down all the cosets of the subgroup $H = \{[0], [4], [8], [12]\}$. (Since the operation in $\mathbb{Z}_n$ is $+$, write your coset as $[a] + H$. We don't need to distinguish between right cosets and left cosets, since $\mathbb{Z}_n$ is abelian under $+$.)

10. In Problem 9, what is the index of H in $\mathbb{Z}_{16}$? (Recall that we defined the index $i_G(H)$ as the number of right cosets in G.)

11. For any finite group G, show that there are as many distinct left cosets of H in G as there are right cosets of H in G.

12. If aH and bH are distinct left cosets of H in G, are Ha and Hb distinct right cosets of H in G? Prove that this is true or give a counterexample.

13. Find the orders of all the elements of U_{18}. Is U_{18} cyclic?

14. Find the orders of all the elements of U_{20}. Is U_{20} cyclic?

***15.** If p is a prime, show that the only solutions of $x^2 \equiv 1 \bmod p$ are $x \equiv 1 \bmod p$ or $x \equiv -1 \bmod p$.

***16.** If G is a finite abelian group and $a_1, \ldots, a_n$ are all its elements, show that $x = a_1 a_2 \cdots a_n$ must satisfy $x^2 = e$.

17. If G is of odd order, what can you say about the x in Problem 16?

18. Using the results of Problems 15 and 16, prove that if p is an odd prime number, then $(p-1)! \equiv -1 \bmod p$. (This is known as *Wilson's Theorem.*) It is, of course, also true if $p = 2$.

19. Find all the distinct conjugacy classes of S_3.

20. In the group G of Example 6 of Section 1, find the conjugacy class of the element $T_{a,b}$. Describe it in terms of a and b.

21. Let G be the dihedral group of order 8 (see Example 9, Section 1). Find the conjugacy classes in G.

22. Verify Euler's Theorem for $n = 14$ and $a = 3$, and for $n = 14$ and $a = 5$.

23. In U_{41}, show that there is an element a such that $[a]^2 = [-1]$, that is, an integer a such that $a^2 \equiv -1 \bmod 41$.

24. If p is a prime number of the form $4n + 3$, show that we *cannot* solve

$$x^2 \equiv -1 \bmod p$$

[**Hint:** Use Fermat's Theorem that $a^{p-1} \equiv 1 \bmod p$ if $p \nmid a$.]

25. Show that the nonzero elements in $\mathbb{Z}_n$ form a group under the product $[a][b] = [ab]$ if and only if n is a prime.

Middle-Level Problems

26. Let G be a group, H a subgroup of G, and let S be the set of all distinct right cosets of H in G, T the set of all left cosets of H in G. Prove that there is a 1-1 mapping of S onto T. (**Note:** The obvious map that comes to mind, which sends Ha into aH, is not the right one. See Problems 5 and 12.)

27. If $aH = bH$ forces $Ha = Hb$ in G, show that $aHa^{-1} = H$ for every $a \in G$.

28. If G is a cyclic group of order n, show that there are $\varphi(n)$ generators for G. Give their form explicitly.

29. If in a group G, $aba^{-1} = b^i$, show that $a^r b a^{-r} = b^{i^r}$ for all positive integers r.

30. If in G $a^5 = e$ and $aba^{-1} = b^2$, find $o(b)$ if $b \neq e$.

***31.** If $o(a) = m$ and $a^s = e$, prove that $m \mid s$.

32. Let G be a finite group, H a subgroup of G. Let $f(a)$ be the least positive m such that $a^m \in H$. Prove that $f(a) \mid o(a)$.

33. If $i \neq f \in A(S)$ is such that $f^p = i$, p a prime, and if for some $s \in S$, $f^j(s) = s$ for some $1 \leq j < p$, show that $f(s) = s$.

34. If $f \in A(S)$ has order p, p a prime, show that for every $s \in S$ the orbit of s under f has one or p elements. [**Recall:** The orbit of s under f is $\{f^j(s) \mid j \text{ any integer}\}$.]

35. If $f \in A(S)$ has order p, p a prime, and S is a finite set having n elements, where $(n, p) = 1$, show that for some $s \in S$, $f(s) = s$.

Harder Problems

36. If $a > 1$ is an integer, show that $n \mid \varphi(a^n - 1)$, where φ is the Euler φ-function. [**Hint:** Consider the integers mod$(a^n - 1)$.]

37. In a cyclic group of order n, show that for each positive integer m that divides n (including $m = 1$ and $m = n$) there are $\varphi(m)$ elements of order m.

38. Using the result of Problem 37, show that $n = \Sigma_{m \mid n} \varphi(m)$.

39. Let G be a finite abelian group of order n for which the number of solutions of $x^m = e$ is at most m for any m dividing n. Prove that G must be cyclic. [**Hint:** Let $\psi(m)$ be the number of elements in G of *order* m. Show that $\psi(m) \leq \varphi(m)$ and use Problem 38.]

40. Using the result of Problem 39, show that U_p, if p is a prime, is cyclic. (This is a famous result in number theory; it asserts the existence of a *primitive root* mod p.)

41. Using the result of Problem 40, show that if p is a prime of the form $p = 4n + 1$, then we can solve $x^2 \equiv -1 \bmod p$ (with x an integer).

42. Using Wilson's Theorem (see Problem 28), show that if p is a prime of the form $p = 4n + 1$ and if

$$y = 1 \cdot 2 \cdot 3 \cdots \frac{p-1}{2} = \left(\frac{p-1}{2}\right)!,$$

then $y^2 \equiv -1 \bmod p$. (This gives another proof of the result in Problem 41.)

43. Let G be an abelian group of order n, and $a_1, \ldots, a_n$ its elements. Let $x = a_1 a_2 \cdots a_n$. Show that:

(a) If G has exactly one element $b \neq e$ such that $b^2 = e$, then $x = b$.

(b) If G has more than one element $b \neq e$ such that $b^2 = e$, then $x = e$.

(c) If n is odd, then $x = e$ (see Problem 16).

5. HOMOMORPHISMS AND NORMAL SUBGROUPS

In a certain sense the subject of group theory is built up out of three basic concepts: that of a homomorphism, that of a normal subgroup, and that of the factor or quotient group of a group by a normal subgroup. We discuss the first two of these in this section, and the third in Section 6.

Without further ado we introduce the first of these.

Definition. Let G, G' be two groups; then the mapping $\varphi: G \to G'$ is a *homomorphism* if $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in G$.

(*Note:* This φ has nothing to do with the Euler φ-function.)

In this definition the product on the left side—in $\varphi(ab)$—is that of G, while the product $\varphi(a)\varphi(b)$ is that of G'. A short description of a homomorphism is that it *preserves* the operation of G. We do *not* insist that φ be onto; if it is, we'll say that it is. Before working out some facts about homomorphisms, we present some examples.

Examples

1. Let G be the group of all positive reals under the multiplication of reals, and G' the group of all reals under addition. Let $\varphi: G \to G'$ be defined by $\varphi(x) = \log_{10} x$ for $x \in G$. Since $\log_{10}(xy) = \log_{10} x + \log_{10} y$, we have $\varphi(xy) = \varphi(x) + \varphi(y)$, so φ is a homomorphism. It also happens to be onto and 1-1.

2. Let G be an *abelian* group and let $\varphi: G \to G$ be defined by $\varphi(a) = a^2$. Since $\varphi(ab) = (ab)^2 = a^2b^2 = \varphi(a)\varphi(b)$, φ is a homomorphism of G into itself. It need not be onto; the reader should check that in U_8 (see Section 4) $a^2 = e$ for all $a \in U_8$, so $\varphi(G) = (e)$.

3. The example of U_8 above suggests the so-called *trivial homomorphism.* Let G be any group and G' any other; define $\varphi(x) = e'$, the unit element of G', for all $x \in G$. Trivially, φ is a homomorphism of G into G'. It certainly is not a very interesting one.

Another homomorphism always present is the identity mapping, i, of any group G into itself. Since $i(x) = x$ for all $x \in G$, clearly $i(xy) = xy = i(x)i(y)$. The map i is 1-1 and onto, but, again, is not too interesting as a homomorphism.

4. Let G be the group of integers under $+$ and $G' = \{1, -1\}$, the subgroup of the reals under multiplication. Define $\varphi(m) = 1$ if m is even, $\varphi(m) = -1$ if m is odd. The statement that φ is a homomorphism is merely a restatement of:

even + even = even, even + odd = odd, and odd + odd = even.

5. Let G be the group of all nonzero complex numbers under multiplication and let G' be the group of positive reals under multiplication. Let $\varphi: G \to G'$ be defined by $\varphi(a) = |a|$; then $\varphi(ab) = |ab| = |a|\,|b| = \varphi(a)\varphi(b)$, so φ is a homomorphism of G into G'. In fact, φ is onto.

6. Let G be the group in Example 6 of Section 1, and G' the group of nonzero reals under multiplication. Define $\varphi: G \to G'$ by $\varphi(T_{a,b}) = a$. That

φ is a homomorphism follows from the product rule in G, namely, $T_{a,b}T_{c,d} = T_{ac,ad+b}$.

7. Let $G = \mathbb{Z}$ be the group of integers under $+$ and let $G' = \mathbb{Z}_n$. Define $\varphi: G \to \mathbb{Z}_n$ by $\varphi(m) = [m]$. Since the addition in $\mathbb{Z}_n$ is defined by $[m] + [r] = [m + r]$, we see that $\varphi(m + r) = \varphi(m) + \varphi(r)$, so φ is indeed a homomorphism of $\mathbb{Z}$ onto $\mathbb{Z}_n$.

8. The following general construction gives rise to a well-known theorem. Let G be any group, and let $A(G)$ be the set of all 1-1 mappings of G onto itself—here we are viewing G merely as a set, forgetting about its multiplication. Define $T_a: G \to G$ by $T_a(x) = ax$ for every $x \in G$. *What is the product, T_aT_b, of T_a and T_b as mappings on G?* Well,

$$(T_aT_b)(x) = T_a(T_bx) = T_a(bx) = a(bx) = (ab)x = T_{ab}(x)$$

(we used the associative law). So we see that $T_aT_b = T_{ab}$.

Define the mapping $\varphi: G \to A(G)$ by $\varphi(a) = T_a$, for $a \in G$. The product rule for the T's translates into $\varphi(ab) = T_{ab} = T_aT_b = \varphi(a)\varphi(b)$, so φ is a homomorphism of G into $A(G)$. We claim that φ is 1-1. Suppose that $\varphi(a) = \varphi(b)$, that is, $T_a = T_b$. Therefore, $a = T_a(e) = T_b(e) = b$, so φ is indeed 1-1. It is not onto in general—for instance, if G has order $n > 2$, then $A(G)$ has order $n!$, and since $n! > n$, φ doesn't have a ghost of a chance of being onto. It is easy to verify that the image of φ, $\varphi(G) = \{T_a \mid a \in G\}$, is a subgroup of $A(G)$.

The fact that φ is 1-1 suggests that perhaps 1-1 homomorphisms should play a special role. We single them out in the following definition.

Definition. The homomorphism $\varphi: G \to G'$ is called a *monomorphism* if φ is 1-1. A monomorphism that is onto is called an *isomorphism*. An isomorphism from G to G itself is called an *automorphism*.

One more definition.

Definition. Two groups G and G' are said to be *isomorphic* if there is an isomorphism of G onto G'.

We shall denote that G and G' are isomorphic by writing $G \simeq G'$.

This definition seems to be asymmetric, but, in point of fact, it is not. For if there is an isomorphism of G onto G', there is one of G' onto G (see Problem 2).

We shall discuss more thoroughly later what it means for two groups to be isomorphic. But now we summarize what we did in Example 8.

Theorem 2.5.1 (Cayley's Theorem). Every group G is isomorphic to some subgroup of $A(S)$, for an appropriate S.

The appropriate S we used was G itself. But there may be better choices. We shall see some in the problems to follow.

When G is finite, we can take the set S in Theorem 2.5.1 to be finite, in which case $A(S)$ is S_n and its elements are permutations. In this case, Cayley's Theorem is usually stated as: *A finite group can be represented as a group of permutations.*

(Arthur Cayley (1821–1895) was an English mathematician who worked in matrix theory, invariant theory, and many other parts of algebra.)

This is a good place to discuss the importance of "isomorphism." Let φ be an isomorphism of G onto G'. We can view G' as a relabeling of G, using the label $\varphi(x)$ for the element x. Is this labeling consistent with the structure of G as a group? That is, if x is labeled $\varphi(x)$, y labeled $\varphi(y)$, what is xy labeled as? Since $\varphi(x)\varphi(y) = \varphi(xy)$, we see that xy is labeled as $\varphi(x)\varphi(y)$, so this renaming of the elements is consistent with the product in G. So two groups that are isomorphic—although they need not be equal—in a certain sense, as described above, are equal. Often, it is desirable to be able to identify a given group as isomorphic to some concrete group that we know.

We go on with more examples.

9. Let G be any group, $a \in G$ fixed in the discussion. Define $\varphi: G \to G$ by $\varphi(x) = a^{-1}xa$ for all $x \in G$. We claim that φ is an isomorphism of G onto itself. First,

$$\varphi(xy) = a^{-1}(xy)a = a^{-1}xa \cdot a^{-1}ya = \varphi(x)\varphi(y),$$

so φ is at least a homomorphism of G into itself. It is 1-1 for if $\varphi(x) = \varphi(y)$, then $a^{-1}xa = a^{-1}ya$, so by cancellation in G we get $x = y$. Finally, φ is onto, for $x = a^{-1}(axa^{-1})a = \varphi(axa^{-1})$ for any $x \in G$.

Here φ is called the *inner automorphism* of G *induced* by a. The notion of *automorphism* and some of its properties will come up in the problems.

One final example:

10. Let G be the group of reals under $+$ and let G' be the group of all nonzero complex numbers under multiplication. Define $\varphi: G \to G'$ by

$$\varphi(x) = \cos x + i \sin x.$$

We saw that $(\cos x + i \sin x)(\cos y + i \sin y) = \cos(x + y) + i \sin(x + y)$,

hence $\varphi(x)\varphi(y) = \varphi(x + y)$ and φ is a homomorphism of G into G'. φ is not 1-1 because, for instance, $\varphi(0) = \varphi(2\pi) = 1$, nor is φ onto.

Now that we have a few examples in hand, we start a little investigation of homomorphisms. We begin with

Lemma 2.5.2. If φ is a homomorphism of G into G', then:

(a) $\varphi(e) = e'$, the unit element of G'.

(b) $\varphi(a^{-1}) = \varphi(a)^{-1}$ for all $a \in G$.

Proof. Since $x = xe$, $\varphi(x) = \varphi(xe) = \varphi(x)\varphi(e)$; by cancellation in G' we get $\varphi(e) = e'$. Also, $\varphi(aa^{-1}) = \varphi(e) = e'$, hence $e' = \varphi(aa^{-1}) = \varphi(a)\varphi(a^{-1})$, which proves that $\varphi(a^{-1}) = \varphi(a)^{-1}$. □

Definition. The *image* of φ, $\varphi(G)$, is $\varphi(G) = \{\varphi(a) \mid a \in G\}$.

We leave to the reader the proof of

Lemma 2.5.3. If φ is a homomorphism of G into G', then the image of φ is a subgroup of G'.

We singled out certain homomorphisms and called them monomorphisms. Their property was that they were 1-1. We want to measure how far a given homomorphism is from being a monomorphism. This prompts the

Definition. If φ is a homomorphism of G into G', then the *kernel* of φ, Ker φ, is defined by Ker $\varphi = \{a \in G \mid \varphi(a) = e'\}$.

Ker φ measures the lack of *1-1' ness* at one point e'. We claim that this lack is rather uniform. What is $W = \{x \in G \mid \varphi(x) = w'\}$ for a given $w' \in G'$? We show that if $\varphi(x) = w'$ for some $x \in G$, then $W = \{kx \mid k \in \text{Ker } \varphi\} = (\text{Ker } \varphi)x$. Clearly, if $k \in \text{Ker } \varphi$ and $\varphi(x) = w'$, then $\varphi(kx) = \varphi(k)\varphi(x) = e'\varphi(x) = w'$, so $kx \in W$. Also, if $\varphi(x) = \varphi(y) = w'$, then $\varphi(x) = \varphi(y)$, hence $\varphi(y)\varphi(x)^{-1} = e'$; but $\varphi(x)^{-1} = \varphi(x^{-1})$ by Lemma 2.5.2, so $e' = \varphi(y)\varphi(x)^{-1} = \varphi(y)\varphi(x^{-1}) = \varphi(yx^{-1})$, whence $yx^{-1} \in \text{Ker } \varphi$ and so $y \in (\text{Ker } \varphi)x$. *Thus the inverse image of any element* w' in $\varphi(G) \in G'$ is the set $(\text{Ker } \varphi)x$, where x is *any* element in G such that $\varphi(x) = w'$.

We state this as

Lemma 2.5.4. If $w' \in G'$ is of the form $\varphi(x) = w'$, then $\{y \in G \mid \varphi(y) = w'\} = (\text{Ker } \varphi)x$.

We now shall study some basic properties of the kernels of homomorphisms.

Theorem 2.5.5. If φ is a homomorphism of G into G', then

(a) Ker φ is a subgroup of G.

(b) Given $a \in G$, a^{-1} (Ker φ)$a \subset$ Ker φ.

Proof. Although this is so important, its proof is easy. If $a, b \in$ Ker φ, then $\varphi(a) = \varphi(b) = e'$, hence $\varphi(ab) = \varphi(a)\varphi(b) = e'$, whence $ab \in$ Ker φ, so Ker φ is closed under product. Also $\varphi(a) = e'$ implies that $\varphi(a^{-1}) = \varphi(a)^{-1} = e'$, and so $a^{-1} \in$ Ker φ. Therefore, Ker φ is a subgroup of G. If $k \in$ Ker φ and $a \in G$, then $\varphi(k) = e'$. Consequently, $\varphi(a^{-1}ka) = \varphi(a^{-1})\varphi(k)\varphi(a) = \varphi(a^{-1})e'\varphi(a) = \varphi(a^{-1})\varphi(a) = \varphi(a^{-1}a) = \varphi(e) = e'$. This tells us that $a^{-1}ka \in$ Ker φ, hence a^{-1} (Ker φ) $a \in$ Ker φ. The theorem is now completely proved. □

Corollary. If φ is a homomorphism of G into G', then φ is a monomorphism if and only if Ker $\varphi = (e)$.

Proof. This result is really a corollary to Lemma 2.5.4. We leave the few details to the reader. □

Property (b) of Ker φ in Theorem 2.5.5 is an interesting and basic one for a subgroup to enjoy. We ran into this property in the text material and problems earlier on several occasions. We use it to define the ultra-important class of subgroups of a group.

Definition. The subgroup N of G is said to be a *normal subgroup* of G if $a^{-1}Na \subset N$ for every $a \in G$.

Of course, Ker φ, for any homomorphism, is a normal subgroup of G. As we shall see in the next section, every normal subgroup of G is the kernel of some appropriate homomorphism of G into an appropriate group G'. So in a certain sense the notions of homomorphism and normal subgroups will be shown to be equivalent.

Although we defined a normal subgroup via $a^{-1}Na \subset N$, we actually have $a^{-1}Na = N$. For if $a^{-1}Na \subset N$ for all $a \in G$, then $N = a(a^{-1}Na)a^{-1} \subset aNa^{-1} = (a^{-1})^{-1}Na^{-1} \subset N$. So $N = aNa^{-1}$ for every $a \in G$. Transposing, we have $Na = aN$; that is, every left coset of N in G is a right coset of N in G.

On the other hand, if every left coset of N in G is a right coset, then the left coset aN, which contains a, must be equal to the right coset containing a,

namely Na. Thus, $aN = Na$ and $N = a^{-1}Na$ for all $a \in G$, which is to say that N is normal in G.

We write "N is a normal subgroup of G" by the abbreviated symbol $N \lhd G$.

Note that $a^{-1}Na = N$ *does not* mean that $a^{-1}na = n$ for every $n \in N$. No—merely that the set of all $a^{-1}na$ is the same as the set of all n.

We have proved

Theorem 2.5.6. $N \lhd G$ if and only if every left coset of N in G is a right coset of N in G.

Before going any further, we pause to look at some examples of kernels of homomorphisms and normal subgroups.

If G is abelian, then every subgroup of G is normal, for $a^{-1}xa = x$ for every $a, x \in G$. The converse of this is *not* true. Nonabelian groups exist in which *every subgroup* is normal. See if you can find such an example of order 8. Such nonabelian groups are called *Hamiltonian*, after the Irish mathematician W. R. Hamilton (1805–1865). The desired group of order 8 can be found in the *quaternions* of Hamilton, which we introduce in Chapter 4, Section 1.

In Example 1, $\varphi(x) = \log_{10} x$, and Ker $\varphi = \{x \mid \log_{10} x = 0\} = \{1\}$. In Example 2, where G is abelian, and $\varphi(x) = x^2$,

$$\text{Ker } \varphi = \{x \in G \mid x^2 = e\}$$

The kernel of the trivial homomorphism of Example 3 is *all* of G. In Example 4, Ker φ is the set of all even integers. In Example 5, Ker $\varphi = \{a \in C' \mid |a| = 1\}$, which can be identified, from the polar form of a complex number, as Ker $\varphi = \{\cos x + i \sin x \mid x \text{ real}\}$. In Example 6, Ker $\varphi = \{T_{1,b} \in G \mid b \text{ real}\}$. In Example 7, Ker φ is the set of all multiples of n. In Examples 8 and 9, the kernels consists of e alone, for the maps are monomorphisms. In Example 10, we see that Ker $\varphi = \{2\pi m \mid m \text{ any integer}\}$.

Of course, all the kernels above are normal subgroups of their respective groups. We should look at some normal subgroups, intrinsically in G itself, without recourse to the kernels of homomorphism. We go back to the examples of Section 1.

1. In Example 7, $H = \{T_{a,b} \in G \mid a \text{ rational}\}$. If $T_{x,y} \in G$, we leave it to the reader to check that $T_{x,y}^{-1} H T_{x,y} \subset H$ and so $H \lhd G$.
2. In Example 9 the subgroup $\{i, g, g^2, g^3\} \lhd G$. Here too we leave the checking to the reader.
3. In Example 10 the subgroup $H = \{i, h, h^2, \ldots, h^{n-1}\}$ is normal in G. This we also leave to the reader.

4. If G is any group, $Z(G)$, the *center* of G, is a normal subgroup of G (see Example 11 of Section 3).
5. If $G = S_3$, G has the elements i, f, g, g^2, fg, and gf, where $f(x_1) = x_2$, $f(x_2) = x_1$, $f(x_3) = x_3$ and $g(x_1) = x_2$, $g(x_2) = x_3$, $g(x_3) = x_1$. We claim that the subgroup $N = \{i, g, g^2\} \lhd S_3$. As we saw earlier (or can compute now), $fgf^{-1} = g^{-1} = g^2$, $fg^2f^{-1} = g$. $(fg)\, g(fg)^{-1} = fggg^{-1}f^{-1} = fgf^{-1} = g^2$, and so on. So $N \lhd S_3$ follows.

The material in this section has been a rather rich diet. It may not seem so, but the ideas presented, although simple, are quite subtle. We recommend that the reader digest the concepts and results thoroughly before going on. One way of seeing how complete this digestion is, is to take a stab at many of the almost infinite list of problems that follow. The material of the next section is even a richer diet, and even harder to digest. Avoid a mathematical stomachache later by assimilating this section well.

PROBLEMS

Easier Problems

1. Determine in each of the parts if the given mapping is a homomorphism. If so, identify its kernel and whether or not the mapping is 1-1 or onto.
- **(a)** $G = \mathbb{Z}$ under $+$, $G' = \mathbb{Z}_n$, $\varphi(a) = [a]$ for $a \in \mathbb{Z}$.
- **(b)** G group, $\varphi: G \to G$ defined by $\varphi(a) = a^{-1}$ for $a \in G$.
- **(c)** G abelian group, $\varphi: G \to G$ defined by $\varphi(a) = a^{-1}$ for $a \in G$.
- **(d)** G group of all nonzero real numbers under multiplication, $G' = \{1, -1\}$, $\varphi(r) = 1$ if r is positive, $\varphi(r) = -1$ if r is negative.
- **(e)** G an abelian group, $n > 1$ a fixed integer, and $\varphi: G \to G$ defined by $\varphi(a) = a^n$ for $a \in G$.

2. Recall that $G \simeq G'$ means that G is isomorphic to G'. Prove that for all groups G_1, G_2, G_3:
- **(a)** $G_1 \simeq G_1$.
- **(b)** $G_1 \simeq G_2$ implies that $G_2 \simeq G_1$.
- **(c)** $G_1 \simeq G_2$, $G_2 \simeq G_3$ implies that $G_1 \simeq G_3$.

3. Let G be any group and $A(G)$ the set of all 1-1 mappings of G, as a set, onto itself. Define $L_a: G \to G$ by $L_a(x) = xa^{-1}$. Prove that:
- **(a)** $L_a \in A(G)$.
- **(b)** $L_aL_b = L_{ab}$.
- **(c)** The mapping $\psi: G \to A(G)$ defined by $\psi(a) = L_a$ is a monomorphism of G into $A(G)$.

4. In Problem 3 prove that for all $a, b \in G$, $T_a L_b = L_b T_a$, where T_a is defined as in Example 8.
5. In Problem 4, show that if $V \in A(G)$ is such that $T_a V = V T_a$ for all $a \in G$, then $V = L_b$ for some $b \in G$. (**Hint:** Acting on $e \in G$, find out what b should be.)
6. Prove that if $\varphi: G \to G'$ is a homomorphism, then $\varphi(G)$, the image of G, is a subgroup of G'.
7. Show that $\varphi: G \to G'$, where φ is a homomorphism, is a monomorphism if and only if Ker $\varphi = (e)$.
8. Find an isomorphism of G, the group of all real numbers under $+$, *onto* G', the group of all positive real numbers under multiplication.
9. Verify that if G is the group in Example 6 of Section 1, and $H = \{T_{a,b} \in G \mid a \text{ rational}\}$, then $H \lhd G$, the dihedral group of order 8.
10. Verify that in Example 9 of Section 1, the set $H = \{i, g, g^2, g^3\}$ is a normal subgroup of G, the dihedral group of order 8.
11. Verify that in Example 10 of Section 1, the subgroup

$$H = \{i, h, h^2, \ldots, h^{n-1}\}$$

is normal in G.

12. Prove that if $Z(G)$ is the center of G, then $Z(G) \lhd G$.
13. If G is a finite abelian group of order n and $\varphi: G \to G$ is defined by $\varphi(a) = a^m$ for all $a \in G$, find the necessary and sufficient condition that φ be an isomorphism of G onto itself.
14. If G is abelian and $\varphi: G \to G'$ is a homomorphism of G *onto* G', prove that G' is abelian.
15. If G is any group, $N \lhd G$, and $\varphi: G \to G'$ a homomorphism of G *onto* G', prove that the image, $\varphi(N)$, of N is a normal subgroup of G'.
16. If $N \lhd G$ and $M \lhd G$ and $MN = \{mn \mid m \in M, n \in N\}$, prove that MN is a subgroup of G and that $MN \lhd G$.
17. If $M \lhd G$, $N \lhd G$, prove that $M \cap N \lhd G$.
18. If H is any subgroup of G and $N = \cap_{a \in G} a^{-1} H a$, prove that $N \lhd G$.
19. If H is a subgroup of G, let $N(H)$ be defined by the relation $N(H) = \{a \in G \mid a^{-1} H a = H\}$. Prove that:
    (a) $N(H)$ is a subgroup of G and $N(H) \supset H$.
    (b) $H \lhd N(H)$.
    (c) If K is a subgroup of G such that $H \lhd K$, then $K \subset N(H)$. [So $N(H)$ is the largest subgroup of G in which H is normal.]
20. If $M \lhd G$, $N \lhd G$, and $M \cap N = (e)$, show that for $m \in M, n \in N$, $mn = nm$.

21. Let S be any set having more than two elements and $A(S)$ the set of all 1-1 mappings of S onto itself. If $s \in S$, we define $H(s) = \{f \in A(S) \mid f(s) = s\}$. Prove that $H(s)$ *cannot* be a normal subgroup of $A(S)$.

22. Let $G = S_3$, the symmetric group of degree 3 and let $H = \{i, f\}$, where $f(x_1) = x_2, f(x_2) = x_1, f(x_3) = x_3$.

(a) Write down all the left cosets of H in G.

(b) Write down all the right cosets of H in G.

(c) Is every left coset of H a right coset of H?

23. Let G be a group such that all subgroups of G are normal in G. If $a, b \in G$, prove that $ba = a^j b$ for some j.

24. If G_1, G_2 are two groups, let $G = G_1 \times G_2$, the Cartesian product of G_1, G_2 [i.e., G is the set of all ordered pairs (a, b) where $a \in G_1$, $b \in G_2$]. Define a product in G by $(a_1, b_1)(a_2, b_2) = (a_1a_2, b_1b_2)$.

(a) Prove that G is a group.

(b) Show that there is a monomorphism φ_1 of G_1 into G such that $\varphi_1(G_1) \lhd G$, given by $\varphi_1(a_1) = (a_1, e_2)$, where e_2 is the identity element of G_2.

(c) Find the similar monomorphism φ_2 of G_2 into G.

(d) Using the mappings φ_1, φ_2 of Parts (b) and (c), prove that $\varphi_1(G_1)\varphi_2(G_2) = G$ and $\varphi_1(G_1) \cap \varphi_2(G_2)$ is the identity element of G.

(e) Prove that $G_1 \times G_2 \simeq G_2 \times G_1$.

25. Let G be a group and let $W = G \times G$ as defined in Problem 24. Prove that:

(a) The mapping $\varphi: G \to W$ defined by $\varphi(a) = (a, a)$ is a monomorphism of G into W.

(b) The image $\varphi(G)$ in W [i.e., $\{(a, a) \mid a \in G\}$] is normal in W if and only if G is abelian.

Middle-Level Problems

***26.** If G is a group and $a \in G$, define $\sigma_a: G \to G$ by $\sigma_a(g) = aga^{-1}$. We saw in Example 9 of this section that σ_a is an isomorphism of G onto itself, so $\sigma_a \in A(G)$, the group of all 1-1 mappings of G (as a set) onto itself. Define $\psi: G \to A(G)$ by $\psi(a) = \sigma_a$ for all $a \in G$. Prove that:

(a) ψ is a homomorphism of G into $A(G)$.

(b) Ker $\psi = Z(G)$, the center of G.

27. If θ is an automorphism of G and $N \lhd G$, prove that $\theta(N) \lhd G$.

28. Let θ, ψ be automorphisms of G, and let $\theta\psi$ be the product of θ and ψ as mappings on G. Prove that $\theta\psi$ is an automorphism of G, and that θ^{-1} is an automorphism of G, so that the set of all automorphisms of G is itself a group.

*29. A subgroup T of a group W is called *characteristic* if $\varphi(T) \subset T$ for all automorphisms, φ, of W. Prove that:
   (a) M characteristic in G implies that $M \triangleleft G$.
   (b) M, N characteristic in G implies that MN is characteristic in G.
   (c) A normal subgroup of a group *need not* be characteristic. (This is quite hard; you must find an example of a group G and a noncharacteristic normal subgroup.)

30. Suppose that $|G| = pm$, where $p \nmid m$ and p is a prime. If H is a normal subgroup of order p in G, prove that H is characteristic.

31. Suppose that G is an abelian group of order $p^n m$ where $p \nmid m$ is a prime. If H is a subgroup of G of order p^n, prove that H is a characteristic subgroup of G.

32. Do Problem 31 even if G is not abelian if you happen to know that for some reason or other $H \triangleleft G$.

33. Suppose that $N \triangleleft G$ and $M \subset N$ is a characteristic subgroup of N. Prove that $M \triangleleft G$. (It is *not* true that if $M \triangleleft N$ and $N \triangleleft G$, then M must be normal in G. See Problem 50.)

34. Let G be a group, $\mathcal{A}(G)$ the group of all automorphisms of G. (See Problem 28.) Let $I(G) = \{\sigma_a \mid a \in G\}$, where σ_a is as defined in Problem 26. Prove that $I(G) \triangleleft \mathcal{A}(G)$.

35. Show that $Z(G)$, the center of G, is a characteristic subgroup of G.

36. If $N \triangleleft G$ and H is a subgroup of G, show that $H \cap N \triangleleft H$.

Harder Problems

37. If G is a nonabelian group of order 6, prove that $G \simeq S_3$.

38. Let G be a group and H a subgroup of G. Let $S = \{Ha \mid a \in G\}$ be the set of all right cosets of H in G. Define, for $b \in G$, $T_b : S \to S$ by $T_b(Ha) = Hab^{-1}$.
   (a) Prove that $T_b T_c = T_{bc}$ for all $b, c \in G$ [therefore the mapping $\psi : G \to A(S)$ defined by $\psi(b) = T_b$ is a homomorphism].
   (b) Describe Ker ψ, the kernel of $\psi : G \to A(S)$.
   (c) Show that Ker ψ is the largest normal subgroup of G lying in H [largest in the sense that if $N \triangleleft G$ and $N \subset H$, then $N \subset$ Ker ψ].

39. Use the result of Problem 38 to redo Problem 37.

Recall that if H is a subgroup of G, then the *index* of H in G, $i_G(H)$, is the number of distinct right cosets of H and G (if this number is finite).

40. If G is a finite group, H a subgroup of G such that $n \nmid i_G(H)!$ where $n = |G|$, prove that there is a normal subgroup $N \neq (e)$ of G contained in H.

41. Suppose that you know that a group G of order 21 contains an element a of order 7. Prove that $A = (a)$, the subgroup generated by a, is normal in G. (**Hint:** Use the result of Problem 40.)

42. Suppose that you know that a group G of order 36 has a subgroup H or order 9. Prove that either $H \lhd G$ or there exists a subgroup $N \lhd G$, $N \subset H$, and $|N| = 3$.

43. Prove that a group of order 9 must be abelian.

44. Prove that a group of order p^2, p a prime, has a normal subgroup of order p.

45. Using the result of Problem 44, prove that a group of order p^2, p a prime, must be abelian.

46. Let G be a group of order 15; show that there is an element $a \neq e$ in G such that $a^3 = e$ and an element $b \neq e$ such that $b^5 = e$.

47. In Problem 46, show that both subgroups $A = \{e, a, a^2\}$ and $B = \{e, b, b^2, b^3, b^4\}$ are normal in G.

48. From the result of Problem 47, show that any group of order 15 is cyclic.

Very Hard Problems

49. Let G be a group, H a subgroup of G such that $i_G(H)$ is finite. Prove that there is a subgroup $N \subset H$, $N \lhd G$ such that $i_G(N)$ is finite.

50. Construct a group G such that G has a normal subgroup N, and N has a normal subgroup M (i.e., $N \lhd G$, $M \lhd N$), yet M is not normal in G.

51. Let G be a finite group, φ an automorphism of G such that φ^2 is the identity automorphism of G. Suppose that $\varphi(x) = x$ implies that $x = e$. Prove that G is abelian and $\varphi(a) = a^{-1}$ for all $a \in G$.

52. Let G be a finite group and φ an automorphism of G such that $\varphi(x) = x^{-1}$ for *more than three-fourths* of the elements of G. Prove that $\varphi(y) = y^{-1}$ for *all* $y \in G$, and so G is abelian.

6. FACTOR GROUPS

Let G be a group and N a normal subgroup of G. In proving Lagrange's Theorem we used, for an arbitrary subgroup H, the equivalence relation $a \sim b$ if $ab^{-1} \in H$. Let's try this out when N is normal and see if we can say a little more than one could say for just any old subgroup.

So, let $a \sim b$ if $ab^{-1} \in N$ and let $[a] = \{x \in G \mid x \sim a\}$. As we saw earlier, $[a] = Na$, the right coset of N in G containing a. Recall that in looking at $\mathbb{Z}_n$ we defined for it an operation $+$ via $[a] + [b] = [a + b]$. Why

not try something similar for an arbitrary group G and a normal subgroup N of G?

So let $M = \{[a] \mid a \in G\}$, where $[a] = \{x \in G \mid xa^{-1} \in N\} = Na$. We define a product in M via $[a][b] = [ab]$. We shall soon show that M is a group under this product. *But first and foremost we must show that this product in M is well-defined.* In other words, we must show that if $[a] = [a']$ and $[b] = [b']$, then $[ab] = [a'b']$, for this would show that $[a][b] = [ab] = [a'b'] = [a'][b']$; equivalently, that *this product of classes does not depend on the particular representatives we use for the classes.*

Therefore let us suppose that $[a] = [a']$ and $[b] = [b']$. From the definition of our equivalence we have that $a' = na$, where $n \in N$. Similarly, $b' = mb$, where $m \in N$. Thus $a'b' = namb = n(ama^{-1})ab$; since $N \lhd G$, ama^{-1} is in N, so $n(ama^{-1})$ is also in N. So if we let $n_1 = n(ama^{-1})$, then $n_1 \in N$ and $a'b' = n_1ab$. But this tells us that $a'b' \in Nab$, so that $a'b' \sim ab$, from which we have that $[a'b'] = [ab]$, the exact thing we required to ensure that our product in M was well-defined.

Thus M is now endowed with a well-defined product $[a][b] = [ab]$. We now verify the group axioms for M. Closure we have from the very definition of this product. If $[a]$, $[b]$, and $[c]$ are in M, then $[a]([b][c]) = [a][bc] = [a(bc)] = [(ab)c]$ (since the product in G is associative) $= [ab][c] = ([a][b])[c]$. Therefore, the associative law has been established for the product in M. What about a unit element? Why not try the obvious choice, namely $[e]$? We immediately see that $[a][e] = [ae] = [a]$ and $[e][a] = [ea] = [a]$, so $[e]$ does act as the unit element for M. Finally, what about inverses? Here, too, the obvious choice is the correct one. If $a \in G$, then $[a][a^{-1}] = [aa^{-1}] = [e]$, hence $[a^{-1}]$ acts as the inverse of $[a]$ relative to the product we have defined in M.

We want to give M a name, and better still, a symbol that indicates its dependence on G and N. The symbol we use for M is G/N (read "G over N or G mod N") and G/N is called the *factor group* or *quotient group* of G by N.

What we have shown is the very important

Theorem 2.6.1. If $N \lhd G$ and

$$G/N = \{[a] \mid a \in G\} = \{Na \mid a \in G\},$$

then G/N is a group relative to the operation $[a][b] = [ab]$.

One observation must immediately be made, namely

Theorem 2.6.2. If $N \lhd G$, then there is a homomorphism ψ of G onto G/N such that Ker ψ, the kernel of ψ, is N.

Proof. The most natural mapping from G to G/N is the one that does the trick. Define $\psi: G \to G/N$ by $\psi(a) = [a]$. Our product as defined in G/N makes of ψ a homomorphism, for $\psi(ab) = [ab] = [a][b] = \psi(a)\psi(b)$. Since every element $X \in G/N$ is of the form $X = [b] = \psi(b)$ for some $b \in G$, ψ is onto. Finally, what is the kernel, Ker ψ, of ψ? By definition, Ker $\psi = \{a \in G \mid \psi(a) = E\}$, where E is the unit element of G/N. But what is E? Nothing other than $E = [e] = Ne = N$, and $a \in$ Ker ψ if and only if $E = N = \psi(a) = Na$. But $Na = N$ tells us that $a = ea \in Na = N$, so we see that Ker $\psi \subset N$. That $N \subset$ Ker ψ—which is easy—we leave to the reader. So Ker $\psi = N$. □

Theorem 2.6.2 substantiates the remark we made in the preceding section that every normal subgroup N of G is the kernel of some homomorphism of G onto some group. The "some homomorphism" is the ψ defined above and the "some group" is G/N.

This construction of the factor group G by N is possibly the single most important construction in group theory. In other algebraic systems we shall have analogous constructions, as we shall see later.

One might ask: Where in this whole affair did the normality of N in G enter? Why not do the same thing for any subgroup H of G? So let's try and see what happens. As before, we define

$$W = \{[a] \mid a \in G\} = \{Ha \mid a \in G\}$$

where the equivalence $a \sim b$ is defined by $ab^{-1} \in H$. We try to introduce a product in W as we did for G/N by defining $[a][b] = [ab]$. Is this product well defined? If $h \in H$, then $[hb] = [b]$, so for the product to be well defined, we would need that $[a][b] = [a][hb]$, that is, $[ab] = [ahb]$. This gives us that $Hab = Hahb$, and so $Ha = Hah$; this implies that $H = Haha^{-1}$, whence $aha^{-1} \in H$. That is, for all $a \in G$ and all $h \in H$, aha^{-1} must be in H; in other words, H must be normal in G. *So we see that in order for the product defined in W to be well-defined, H must be a normal subgroup of G.*

We view this matter of the quotient group in a slightly different way. If A, B are subsets of G, let $AB = \{ab \mid a \in A, b \in B\}$. If H is a subgroup of G, then $HH \subset H$ is another way of saying that H is closed under the product of G.

Let $G/N = \{Na \mid a \in G\}$ be the set of all right cosets of the normal subgroup N in G. Using the product of subsets of G as defined above, what is $(Na)(Nb)$? By definition, $(Na)(Nb)$ consists of all elements of the form $(na)(mb)$, where $n, m \in N$, and so

$$(na)(mb) = (nama^{-1})(ab) = n_1ab,$$

where $n_1 = nama^{-1}$ is in N, since N is normal. Thus $(Na)(Nb) \subset Nab$. On the other hand, if $n \in N$, then

$$n(ab) = (na)(eb) \in (Na)(Nb),$$

so that $Nab \subset (Na)(Nb)$. In short, we have shown that the product—as subsets of G—of Na and Nb is given by the formula $(Na)(Nb) = Nab$. All the other group axioms for G/N, as defined here, are now readily verified from this product formula.

Another way of seeing that $(Na)(Nb) = Nab$ is to note that by the normality of N, $aN = Na$, hence $(Na)(Nb) = N(aN)b = N(Na)b = NNab = Nab$, since $NN = N$ (because N is a subgroup of G).

However we view G/N—as equivalence classes or as a set of certain subsets of G—we do get a group whose structure is intimately tied to that of G, via the natural homomorphism ψ of G onto G/N.

We shall see very soon how we combine induction and the structure of G/N to get information about G.

When G is a finite group and $N \lhd G$, then the number of right cosets of N in G, $i_G(N)$, is given—as the proof of Lagrange's Theorem showed—by $i_G(n) = |G|/|N|$. But this is the order of G/N, which is the set of all the right cosets of N in G. Thus $|G/N| = |G|/|N|$. We state this more formally as

Theorem 2.6.3. If G is a finite group and $N \lhd G$, then $|G/N| = |G|/|N|$.

As an application of what we have been talking about here, we shall prove a special case of a theorem that we shall prove in its full generality later. The proof we give—for the abelian case—is not a particularly good one, but it illustrates quite clearly a general technique, that of pulling back information about G/N to get information about G itself.

The theorem we are about to prove is due to the great French mathematician A. L. Cauchy (1789–1857), whose most basic contributions were in complex variable theory.

Theorem 2.6.4 (Cauchy). If G is a finite abelian group of order $|G|$ and p is a prime that divides $|G|$, then G has an element of order p.

Proof. Before getting involved with the proof, we point out to the reader that the theorem is true for *any* finite group. We shall prove it in the general case later, with a proof that will be much more beautiful than the one we are about to give for the special, abelian case.

We proceed by induction on $|G|$. What does this mean precisely? We shall

assume the theorem to be true for all abelian groups of order less than $|G|$ and show that this forces the theorem to be true for G. If $|G| = 1$, there is no such p and the theorem is vacuously true. So we have a starting point for our induction.

Suppose that there is a subgroup $(e) \neq N \neq G$. Since $|N| < |G|$, if p divides $|N|$, by our induction hypothesis there would be an element of order p in N, hence in G, and we would be done. So we may suppose that $p \nmid |N|$. Since G is abelian, every subgroup is normal, so we can form G/N. Because p divides $|G|$ and $p \nmid |N|$, and because $|G/N| = |G|/|N|$, we have that p divides $|G/N|$. The group G/N is abelian, since G is (Prove!) and since $N \neq (e)$, $|N| > 1$, so $|G/N| = |G|/|N| < |G|$. Thus, again by induction, there exists an element in G/N of order p. In other words, there exists an $a \in G$ such that $[a]^p = [e]$, but $[a] \neq [e]$. This translates to $a^p \in N$, $a \notin N$. So if $m = |N|$, then $(a^p)^m = e$. So $(a^m)^p = e$. If we could show that $b = a^m \neq e$, then b would be the required element of order p in G. But if $a^m = e$, then $[a]^m = [e]$, and since $[a]$ has order p, $p \mid m$ (see Problem 31 of Section 4). But, by assumption, $p \nmid m = |N|$. *So we are done if G has a nontrivial subgroup.*

But if G has no nontrivial subgroups, it must be cyclic of prime order. (See Problem 16 of Section 3, which you should be able to handle more easily now.) What is this "prime order"? Because p divides $|G|$, we must have $|G| = p$. But then any element $a \neq e \in G$ satisfies $a^p = e$ and is of order p. This completes the induction, and so proves the theorem. □

We shall have other applications of this kind of group-theoretic argument in the problems.

The notion of a factor group is a very subtle one, and of the greatest importance in the subject. The formation of a new set from an old one by using as elements of this new set subsets of the old one is strange to the neophyte seeing this kind of construction for the first time. So it is worthwhile looking at this whole matter from a variety of points of view. We consider G/N from another angle now.

What are we doing when we form G/N? Sure, we are looking at equivalences classes defined via N. Let's look at it another way. What we are doing is *identifying* two elements in G if they satisfy the relation $ab^{-1} \in N$. In a sense we are blotting out N. So although G/N is *not* a subgroup of G, we can look at it as G, with N blotted out, and two elements as equal if they are equal "up to N."

For instance, in forming $\mathbb{Z}/N$, where $\mathbb{Z}$ is the group of integers and N is the set of all multiples of 5 in $\mathbb{Z}$, what we are doing is *identifying* 1 with 6, 11, 16, -4, -9, and so on, and we are identifying all multiples of 5 with 0. The nice thing about all this is that this identification jibes with addition in $\mathbb{Z}$ when we go over to $\mathbb{Z}/N$.

Let's look at a few examples from this point of view.

1. Let $G = \{T_{a,b} \mid a \neq 0, b \text{ real}\}$ (Example 6 of Section 1). Let $N = \{T_{1,b} \mid b \text{ real}\} \subset G$; we saw that $N \lhd G$, so it makes sense to talk about G/N. Now $T_{a,b}$ and $T_{a,0}$ are in the same left coset of N in G, so in G/N we are getting an element by identifying $T_{a,b}$ with $T_{a,0}$. The latter element just depends on a. Moreover, the $T_{a,b}$ multiply according to $T_{a,b}T_{c,d} = T_{ac,ad+b}$ and if we identify $T_{a,b}$ with $T_{a,0}$, $T_{c,d}$ with $T_{c,0}$, then their product, which is $T_{ac,ad+b}$, is identified with $T_{ac,0}$. So in G/N multiplication is like that of the group of nonzero real numbers under multiplication, and in some sense (which will be made more precise in the next section) G/N can be identified with this group of real numbers.

2. Let G be the group of real numbers under $+$ and let $\mathbb{Z}$ be the group of integers under $+$. Since G is abelian, $\mathbb{Z} \lhd G$, and so we can talk about $G/\mathbb{Z}$. What does $G/\mathbb{Z}$ really look like? *In forming $G/\mathbb{Z}$, we are identifying any two real numbers that differ by an integer.* So 0 is identified with $-1, -2, -3, \ldots$ and $1, 2, 3, \ldots$; $\frac{3}{2}$ is identified with $\frac{1}{2}, \frac{5}{2}, -\frac{1}{2}, -\frac{3}{2}, \ldots$. Every real number a thus has a mate, $\tilde{a}$, where $0 \leq \tilde{a} < 1$. So, in $G/\mathbb{Z}$, the whole real line has been compressed into the unit interval $[0, 1]$. But a little more is true, for we have also identified the end points of this unit interval. So we are bending the unit interval around so that its two end points touch and become one. What do we get this way? A circle, of course! So $G/\mathbb{Z}$ is like a circle, in a sense that can be made precise, and this circle is a group with an appropriate product.

3. Let G be the group of nonzero complex numbers and let $N = \{a \in G \mid |a| = 1\}$ which is the unit circle in the complex plane. Then N is a subgroup of G and is normal since G is abelian. In going to G/N we are declaring that any complex number of absolute value 1 will be identified with the real number 1. Now any $a \in G$, in its polar form, can be written as $a = r(\cos\theta + i \sin\theta)$, where $r = |a|$, and $|\cos\theta + i \sin\theta| = 1$. In identifying $\cos\theta + i \sin\theta$ with 1, we are identifying a with r. So in passing to G/N every element is being identified with a positive real number, and this identification jibes with the products in G and in the group of positive real numbers, since $|ab| = |a||b|$. So G/N is in a very real sense (no pun intended) the group of positive real numbers under multiplication.

PROBLEMS

1. If G is the group of all nonzero real numbers under multiplication and N is the subgroup of all positive real numbers, write out G/N by exhibiting the cosets of N in G, and construct the multiplication in G/N.
2. If G is the group of nonzero real numbers under multiplication and

$N = \{1, -1\}$, show how you can "identify" G/N as the group of all positive real numbers under multiplication. What are the cosets of N in G?

3. If G is a group and $N \lhd G$, show that if $\overline{M}$ is a subgroup of G/N and $M = \{a \in G \mid Na \in \overline{M}\}$, then M is a subgroup of G, and $M \supset N$.
4. If $\overline{M}$ in Problem 3 is normal in G/N, show that the M defined is normal in G.
5. In Problem 3, show that M/N must equal $\overline{M}$.
6. Arguing as in the Example 2, where we identified $G/\mathbb{Z}$ as a circle, where G is the group of reals under $+$ and $\mathbb{Z}$ integers, consider the following: let $G = \{(a, b) \mid a, b \text{ real}\}$, where $+$ in G is defined by $(a, b) + (c, d) = (a + c, b + d)$ (so G is the plane), and let $N = \{(a, b) \in G \mid a, b \text{ are integers}\}$. Show that G/N can be identified as a torus (donut), and so we can define a product on the donut so that it becomes a group. Here, you may think of a torus as the Cartesian product of two circles.
7. If G is a cyclic group and N is a subgroup of G, show that G/N is a cyclic group.
8. If G is an abelian group and N is a subgroup of G, show that G/N is an abelian group.
9. Do Problems 7 and 8 by observing that G/N is a homomorphic image of G.
10. Let G be an abelian group of order $p_1^{a_1}p_2^{a_2} \cdots p_k^{a_k}$, where $p_1, p_2, \ldots, p_k$ are distinct prime numbers. Show that G has subgroups $S_1, S_2, \ldots, S_k$ of orders $p_1^{a_1}, p_2^{a_2}, \ldots, p_k^{a_k}$, respectively. (**Hint:** Use Cauchy's Theorem and pass to a factor group.) This result, which actually holds for all finite groups, is a famous result in group theory known as *Sylow's Theorem*. We prove it in Section 11.
11. If G is a group and $Z(G)$ the center of G, show that if $G/Z(G)$ is cyclic, then G is abelian.
12. If G is a group and $N \lhd G$ is such that G/N is abelian, prove that $aba^{-1}b^{-1} \in N$ for all $a, b \in G$.
13. If G is a group and $N \lhd G$ is such that

$$aba^{-1}b^{-1} \in N$$

for all $a, b \in G$, prove that G/N is abelian.

14. If G is an abelian group of order $p_1 p_2 \cdots p_k$, where $p_1, p_2, \ldots, p_k$ are distinct primes, prove that G is cyclic. (See Problem 15.)

15. If G is an abelian group and if G has an element of order m and one of order n, where m and n are relatively prime, prove that G has an element of order mn.

16. Let G be an abelian group of order $p^n m$, where p is a prime and $p \nmid m$. Let $P = \{a \in G \mid a^{p^k} = e \text{ for some } k \text{ depending on } a\}$. Prove that:

(a) P is a subgroup of G.

(b) G/P has no elements of order p.

(c) $|P| = p^n$.

17. Let G be an abelian group of order mn, where m and n are relatively prime. Let $M = \{a \in G \mid a^m = e\}$. Prove that:

(a) M is a subgroup of G.

(b) G/M has no element, x, other than the identity element, such that $x^m =$ unit element of G/M.

18. Let G be an abelian group (possibly infinite) and let the set $T = \{a \in G \mid a^m = e, m > 1 \text{ depending on } a\}$. Prove that:

(a) T is a subgroup of G.

(b) G/T has no element—other than its identity element—of finite order.

7. THE HOMOMORPHISM THEOREMS

Let G be a group and φ a homomorphism of G *onto* G'. If K is the kernel of φ, then K is a normal subgroup of G, hence we can form G/K. It is fairly natural to expect that there should be a very close relationship between G' and G/K. The *First Homomorphism Theorem*, which we are about to prove, spells out this relationship in exact detail.

But first let's look back at some of the examples of factor groups in Section 6 to see explicitly what the relationship mentioned above might be.

1. Let $G = \{T_{a,b} \mid a \neq 0, b \text{ real}\}$ and let G' be the group of nonzero reals under multiplication. From the product rule of these T's, namely $T_{a,b}T_{c,d} = T_{ac,ad+b}$, we determined that the mapping $\varphi: G \to G'$ defined by $\varphi(T_{a,b}) = a$ is a homomorphism of G onto G' with kernel $K = \{T_{1,b} \mid b \text{ real}\}$. On the other hand, in Example 1 of Section 6 we saw that $G/K = \{KT_{a,0} \mid a \neq 0 \text{ real}\}$. Since

$$(KT_{a,0})(KT_{x,0}) = KT_{ax,0}$$

the mapping of G/K onto G', which sends each $KT_{a,0}$ onto a, is readily seen to be an *isomorphism* of G/K onto G'. Therefore, $G/K \simeq G'$.

2. In Example 3, G was the group of nonzero complex numbers under multiplication and G' the group of all positive real numbers under multiplication.

Let $\varphi: G \to G'$ defined by $\varphi(a) = |a|$ for $a \in G$. Then, since $|ab| = |a|\,|b|$, φ is a homomorphism of G onto G' (can you see why it is onto?). Thus the kernel K of φ is precisely $K = \{a \in G \mid |a| = 1\}$. But we have already seen that if $|a| = 1$, then a is of the form $\cos\theta + i \sin\theta$. So the set $K = \{\cos\theta + i \sin\theta \mid 0 \leq \theta < 2\pi\}$. If a is any complex number, then $a = r(\cos\theta + i \sin\theta)$, where $r = |a|$, is the polar form of a. Thus $Ka = Kr(\cos\theta + i \sin\theta) = K(\cos\theta + i \sin\theta)r = Kr$, since $K(\cos\theta + i \sin\theta) = K$ because $\cos\theta + i \sin\theta \in K$. So G/K, whose elements are the cosets Ka, from this discussion, has all its elements of the form Kr, where $r > 0$. The mapping of G/K onto G' defined by sending Kr onto r then defines an *isomorphism* of G/K onto G'. So, here, too, $G/K \simeq G'$.

With this little experience behind us we are ready to make the jump the whole way, namely, to

Theorem 2.7.1 (First Homomorphism Theorem). Let φ be a homomorphism of G *onto* G' with kernel K. Then $G' \simeq G/K$, the isomorphism between these being effected by the map

$$\psi: G/K \to G'$$

defined by $\psi(Ka) = \varphi(a)$.

Proof. The best way to show that G/K and G' are isomorphic is to exhibit explicitly an isomorphism of G/K onto G'. The statement of the theorem suggests what such an isomorphism might be.

So define $\psi: G/K \to G'$ by $\psi(Ka) = \varphi(a)$ for $a \in G$. As usual, our first task is to show that ψ is well defined, that is, to show that if $Ka = Kb$, then $\psi(Ka) = \psi(Kb)$. This boils down to showing that if $Ka = Kb$, then $\varphi(a) = \varphi(b)$. But if $Ka = Kb$, then $a = kb$ for some $k \in K$, hence $\varphi(a) = \varphi(kb) = \varphi(k)\varphi(b)$. Since $k \in K$, the kernel of φ, then $\varphi(k) = e'$, the identity element of G', so we get $\varphi(a) = \varphi(b)$. This shows that the mapping ψ is well defined.

Because φ is onto G', given $x \in G'$, then $x = \varphi(a)$ for some $a \in G$, thus $x = \varphi(a) = \psi(Ka)$. This shows that ψ maps G/K onto G'.

Is ψ 1-1? Suppose that $\psi(Ka) = \psi(Kb)$; then $\varphi(a) = \psi(Ka) = \psi(Kb) = \varphi(b)$. Therefore, $e' = \varphi(a)\varphi(b)^{-1} = \varphi(a)\varphi(b^{-1}) = \varphi(ab^{-1})$. Because ab^{-1} is thus in the kernel of φ—which is K—we have $ab^{-1} \in K$. This implies that $Ka = Kb$. In this way ψ is seen to be 1-1.

Finally, is ψ a homomorphism? We check: $\psi((Ka)(Kb)) = \psi(Kab) = \varphi(ab) = \varphi(a)\varphi(b) = \psi(Ka)\psi(Kb)$, using that φ is a homomorphism and that $(Ka)(Kb) = Kab$. Consequently, ψ is a homomorphism of G/K onto G', and Theorem 2.7.1 is proved. □

Having talked about the *First* Homomorphism Theorem suggests that there are others. The next result, however, is an extension of the First Homomorphism Theorem, and is traditionally called the *Correspondence Theorem*. In the context of the theorem above, it exhibits a 1-1 correspondence between subgroups of G^1 and those subgroups of G that contain K.

Theorem 2.7.2 (Correspondence Theorem). Let the map $\varphi: G \to G'$ be a homomorphism of G onto G' with kernel K. If H' is a subgroup of G' and if

$$H = \{a \in G \mid \varphi(a) \in H'\},$$

then H is a subgroup of G, $H \supset K$, and $H/K \simeq H'$. Finally, if $H' \lhd G'$, then $H \lhd G$.

Proof. We first verify that the H above is a subgroup of G. It is not empty, since $e \in H$. If $a, b \in H$, then $\varphi(a), \varphi(b) \in H'$, hence $\varphi(ab) = \varphi(a)\varphi(b) \in H'$, since H' is a subgroup of G'; this puts ab in H, so H is closed. Further, if $a \in H$, then $\varphi(a) \in H'$, hence $\varphi(a^{-1}) = \varphi(a)^{-1}$ is in H', again since H' is a subgroup of G', whence $a^{-1} \in H$. Therefore, H is a subgroup of G.

Because $\varphi(K) = \{e'\} \subset H'$, where e' is the unit element of G', we have that $K \subset H$. Since $K \lhd G$ and $K \subset H$, it follows that $K \lhd H$. The mapping φ restricted to H defines a homomorphism of H onto H' with kernel K. By the First Homomorphism Theorem we get $H/K \simeq H'$.

Finally, if $H' \lhd G'$ and if $a \in G$, then $\varphi(a)^{-1}H'\varphi(a) \subset H'$, so $\varphi(a^{-1})H'\varphi(a) \subset H'$. This tells us that $\varphi(a^{-1}Ha) \subset H'$, so $a^{-1}Ha \subset H$. This proves the normality of H in G. □

It is worth noting that if K is any normal subgroup of G, and φ is the natural homomorphism of G onto G/K, then the theorem gives us a 1-1 correspondence between all subgroups H' of G/K and those subgroups of G that contain K. Moreover, this correspondence preserves normality in the sense that H' is normal in G/K if and only if H is normal in G. (See Problem 7, as well as the last conclusion of the theorem.)

We now state the *Second Homomorphism Theorem*, leaving its proof to the reader in Problem 5.

Theorem 2.7.3 (Second Homomorphism Theorem). Let H be a subgroup of a group G and N a normal subgroup of G. Then $HN = \{hn \mid h \in H, n \in N\}$ is a subgroup of G, $H \cap N$ is a normal subgroup of H, and $H/(H \cap N) \simeq (HN)/N$.

Finally, we go on to the *Third Homomorphism Theorem*, which tells us a little more about the relationship between N and N' when $N' \lhd G'$.

Theorem 2.7.4 (Third Homomorphism Theorem). If the map $\varphi: G \to G'$ is a homomorphism of G onto G' with kernel K then, if $N' \lhd G'$ and $N = \{a \in G \mid \varphi(a) \in N'\}$, we conclude that $G/N \simeq G'/N'$. Equivalently, $G/N \simeq (G/K)/(N/K)$.

Proof. Define the mapping $\psi: G \to G'/N'$ by $\psi(a) = N'\varphi(a)$ for every $a \in G$. Since φ is onto G' and every element of G'/N' is a coset of the form $N'x'$, and $x' = \varphi(x)$ for some $x \in G$, we see that ψ maps G onto G'/N'.

Furthermore, ψ is a homomorphism of G onto G'/N', for $\psi(ab) = N'\varphi(ab) = N'\varphi(a)\varphi(b) = (N'\varphi(a))(N'\varphi(b)) = \psi(a)\psi(b)$, since $N' \lhd G'$. What is the kernel, M, of ψ? If $a \in M$, then $\psi(a)$ is the unit element of G'/N', that is, $\psi(a) = N'$. On the other hand, by the definition of ψ, $\psi(a) = N'\varphi(a)$. Because $N'\varphi(a) = N'$ we must have $\varphi(a) \in N'$; but this puts a in N, by the very definition of N. Thus $M \subset N$. That $N \subset M$ is easy and is left to the reader. Therefore, $M = N$, so ψ is a homomorphism of G onto G'/N' with kernel N, whence, by the First Homomorphism Theorem, $G/N \simeq G'/N'$.

Finally, again by Theorems 2.7.1 and 2.7.2, $G' \simeq G/K$, $N' \simeq N/K$, which leads us to $G/N \simeq G'/N' \simeq (G/K)/(N/K)$. □

This last equality is highly suggestive; we are sort of "canceling out" the K in the numerator and denominator.

PROBLEMS

1. Show that $M \supset N$ in the proof of Theorem 2.7.3.
2. Let G be the group of all real-valued functions on the unit interval $[0, 1]$, where we define, for $f, g \in G$, addition by $(f + g)(x) = f(x) + g(x)$ for every $x \in [0, 1]$. If $N = \{f \in G \mid f(\frac{1}{4}) = 0\}$, prove that $G/N \simeq$ real numbers under $+$.
3. Let G be the group of nonzero real numbers under multiplication and let $N = \{1, -1\}$. Prove that $G/N \simeq$ positive real numbers under multiplication.
4. If G_1, G_2 are two groups and $G = G_1 \times G_2 = \{(a, b) \mid a \in G_1, b \in G_2\}$, where we define $(a, b)(c, d) = (ac, bd)$, show that:
   (a) $N = \{(a, e_2) \mid a \in G_1\}$, where e_2 is the unit element of G_2, is a normal subgroup of G.
   (b) $N \simeq G_1$.
   (c) $G/N \simeq G_2$.

5. Let G be a group, H a subgroup of G, and $N \lhd G$. Let the set $HN = \{hn \mid h \in H, n \in N\}$. Prove that:

(a) $H \cap N \lhd H$.

(b) HN is a subgroup of G.

(c) $N \subset HN$ and $N \lhd HN$.

(d) $(HN)/N \simeq H/(H \cap N)$.

***6.** If G is a group and $N \lhd G$, show that if $a \in G$ has finite order $o(a)$, then Na in G/N has finite order m, where $m \mid o(a)$. (Prove this by using the homomorphism of G onto G/N.)

7. If φ is a homomorphism of G onto G' and $N \lhd G$, show that $\varphi(N) \lhd G'$.

8. CAUCHY'S THEOREM

In Theorem 2.6.4—Cauchy's Theorem—we proved that if a prime p divides the order of a finite *abelian* group G, then G contains an element of order p. We did point out there that Cauchy's Theorem is true even if the group is not abelian. We shall give a very neat proof of this here; this proof is due to McKay.

We return for a moment to set theory, doing something that we mentioned in the problems in Section 4.

Let S be a set, $f \in A(S)$, and define a relation on S as follows: $s \sim t$ if $t = f^i(s)$ for some integer i (i can be positive, negative, or zero). We leave it to the reader as a problem that this does indeed define an equivalence relation on S. The equivalence class of s, $[s]$, is called the *orbit* of s under f. So S is the disjoint union of the orbits of its elements.

When f is of order p, p a prime, we can say something about the size of the orbits under f; those of the readers who solved Problem 34 of Section 4 already know the result. We prove it here to put it on the record officially.

[If $f^k(s) = s$, of course $f^{tk}(s) = s$ for every integer t. (Prove!)]

Lemma 2.8.1. If $f \in A(S)$ is of order p, p a prime, then the orbit of any element of S under f has 1 or p elements.

Proof. Let $s \in S$; if $f(s) = s$, then the orbit of s under f consists merely of s itself, so has one element. Suppose then that $f(s) \neq s$. Consider the elements $s, f(s), f^2(s), \ldots, f^{p-1}(s)$; we claim that these p elements are distinct and constitute the orbit of s under f. If not, then $f^i(s) = f^j(s)$ for some $0 \leq i < j \leq p - 1$, which gives us that $f^{j-i}(s) = s$. Let $m = j - i$; then $0 < m \leq p - 1$ and $f^m(s) = s$. But $f^p(s) = s$ and since $p \nmid m$, $ap + bm = 1$ for some integers a and b. Thus $f^1(s) = f^{ap+bm}(s) = f^{ap}(f^{bm}(s)) = f^{ap}(s) = s$,

since $f^m(s) = f^p(s) = s$. This contradicts that $f(s) \neq s$. Thus the orbit of s under f consists of $s, f(s), f^2(s), \ldots, f^{p-1}(s)$, so as p elements. □

We now give McKay's proof of Cauchy's Theorem.

Theorem 2.8.2 (Cauchy). If p is a prime and p divides the order of G, then G contains an element of order p.

Proof. If $p = 2$, the result amounts to Problem 18 in Section 1. Assume that $p \neq 2$. Let S be the set of all *ordered* p-tuples $(a_1, a_2, \ldots, a_{p-1}, a_p)$, where $a_1, a_2, \ldots, a_p$ are in G and where $a_1a_2 \cdots a_{p-1}a_p = e$. We claim that S has n^{p-1} elements where $n = |G|$. Why? We can choose $a_1, \ldots, a_{p-1}$ arbitrarily in G, and by putting $a_p = (a_1a_2 \cdots a_{p-1})^{-1}$, the p-tuple $(a_1, a_2, \ldots, a_{p-1}, a_p)$ then satisfies

$$a_1a_2 \cdots a_{p-1}a_p = a_1a_2 \cdots a_{p-1}(a_1a_2 \cdots a_{p-1})^{-1} = e,$$

so is in S. Thus S has n^{p-1} elements.

Note that if $a_1a_2 \cdots a_{p-1}a_p = e$, then $a_pa_1a_2 \cdots a_{p-1} = e$ (for if $xy = e$ in a group, then $yx = e$). So the mapping $f: S \to S$ defined by $f(a_1, \ldots, a_p) = (a_p, a_1, a_2, \ldots, a_{p-1})$ is in $A(S)$. Note that $f \neq i$, the identity map on S, and that $f^p = i$, so f is of order p.

If the orbit of s under f has one element, then $f(s) = s$. On the other hand, if $f(s) \neq s$, we know that the orbit of s under f consists precisely of p distinct elements; this we have by Lemma 2.8.1. Now when is $f(s) \neq s$? We claim that $f(s) \neq s$ if and only if when $s = (a_1, a_2, \ldots, a_p)$, then for some $i \neq j$, $a_i \neq a_j$. (We leave this to the reader.) So $f(s) = s$ if and only if $s = (a, a, \ldots, a)$ for some $a \in G$.

Let m be the number of $s \in S$ such that $f(s) = s$; since for $s = (e, e, \ldots, e)$, $f(s) = s$, we know that $m \geq 1$. On the other hand, if $f(s) \neq s$, the orbit of s consists of p elements, and these orbits are disjoint, for they are equivalence classes. If there are k such orbits where $f(s) \neq s$, we get that $n^{p-1} = m + kp$, for we have accounted this way for every element of S.

But $p \mid n$ by assumption and $p \mid (kp)$. So we must have $p \mid m$, since $m = n^{p-1} - kp$. Because $m \neq 0$ and $p \mid m$, we get that $m > 1$. But this says that there is an $s = (a, a, \ldots, a) \neq (e, e, \ldots, e)$ in S; from the definition of S this implies that $a^p = e$. Since $a \neq e$, a is the required element of order p. □

Note that the proof tells us that the number of solutions in G of $x^p = e$ is a positive multiple of p.

We strongly urge the reader who feels uncomfortable with the proof just given to carry out its details for $p = 3$. In this case the action of f on S becomes clear and our assertions about this action can be checked explicitly.

Cauchy's Theorem has many consequences. We shall present one of these, in which we determine completely the nature of certain groups of order pq, where p and q are distinct primes. Other consequences will be found in the problem set to follow, and in later material on groups.

Lemma 2.8.3. Let G be a group of order pq, where p, q are primes and $p > q$. If $a \in G$ is of order p and A is the subgroup of G generated by a, then $A \lhd G$.

Proof. We claim that A is the *only* subgroup of G of order p. Suppose that B is another subgroup of order p. Consider the set $AB = \{xy \mid x \in A, y \in B\}$; we claim that AB has p^2 distinct elements. For suppose that $xy = uv$ where $x, u \in A$, $y, v \in B$; then $u^{-1}x = vy^{-1}$. But $u^{-1}x \in A$, $vy^{-1} \in B$, and since $u^{-1}x = vy^{-1}$, we have $u^{-1}x \in A \cap B$. Since $B \neq A$ and $A \cap B$ is a subgroup of A and A is of prime order, we are forced to conclude that $A \cap B = (e)$ and so $u^{-1}x = e$, that is, $u = x$. Similarly, $v = y$. Thus the number of distinct elements in AB is p^2. But all these elements are in G, which has only $pq < p^2$ elements (since $p > q$). With this contradiction we see that $B = A$ and A is the only subgroup of order p in G. But if $x \in G$, $B = x^{-1}Ax$ is a subgroup of G of order p, in consequence of which we conclude that $x^{-1}Ax = A$; hence $A \lhd G$. □

Corollary. If G, a are as in Lemma 2.8.3 and if $x \in G$, then $x^{-1}ax = a^i$, where $0 < i < p$, for some i (depending on x).

Proof. Since $e \neq a \in A$ and $x^{-1}Ax = A$, $x^{-1}ax \in A$. But every element of A is of the form a^i, $0 \leq i < p$, and $x^{-1}ax \neq e$. In consquence, $x^{-1}ax = a^i$, where $0 < i < p$. □

We now prove a result of a different flavor.

Lemma 2.8.4. If $a \in G$ is of order m and $b \in G$ is of order n, where m and n are relatively prime and $ab = ba$, then $c = ab$ is of order mn.

Proof. Suppose that A is the subgroup generated by a and B that generated by b. Because $|A| = m$ and $|B| = n$ and $(m, n) = 1$, we get $A \cap B = (e)$, which follows from Lagrange's Theorem, for $|A \cap B| \mid n$ and $|A \cap B| \mid m$.

Suppose that $c^i = e$, where $i > 0$; thus $(ab)^i = e$. Since $ab = ba$, $e = (ab)^i = a^i b^i$; this tells us that $a^i = b^{-i} \in A \cap B = (e)$. So $a^i = e$, whence $m \mid i$, and $b^i = e$, whence $n \mid i$. Because $(m, n) = 1$ and m and n both divide i, mn divides i. So $i \geq mn$. Since $(ab)^{mn} = a^{mn}b^{mn} = e$, we see that mn is the smallest positive integer i such that $(ab)^i = e$. This says that ab is of order mn, as claimed in the lemma. □

Before considering the more general case of groups of order pq, let's look at a special case, namely, a group G of order 15. By Cauchy's Theorem, G has elements b of order 3 and a of order 5. By the Corollary to Lemma 2.8.3, $b^{-1}ab = a^i$, where $0 < i < 5$. Thus

$$b^{-2}ab^2 = b^{-1}(b^{-1}ab)b = b^{-1}a^ib = (b^{-1}ab)^i = (a^i)^i = a^{i^2}$$

and similarly, $b^{-3}ab^3 = a^{i^3}$. But $b^3 = e$, so we get $a^{i^3} = a$, whence $a^{i^3-1} = e$. Since a is of order 5, 5 must divide $i^3 - 1$, that is, $i^3 \equiv 1(5)$. However, by Fermat's Theorem (Corollary to Theorem 2.4.8), $i^4 \equiv 1(5)$. These two equations for i tell us that $i \equiv 1(5)$, so, since $0 < i < 5$, $i = 1$. In short, $b^{-1}ab = a^i = a$, which means that $ab = ba$. Since a is of order 5 and b of order 3, by Lemma 2.8.4, $c = ab$ is of order 15. This means that the 15 powers $e = c^0, c, c^2, \ldots, c^{14}$ are distinct, so must sweep out all of G. In a word, *G must be cyclic.*

The argument given for 15 could have been made shorter, but the form in which we did it is the exact prototype for the proof of the more general

Theorem 2.8.5. Let G be a group of order pq, where p, q are primes and $p > q$. If $q \nmid p - 1$, then G must be cyclic.

Proof. By Cauchy's Theorem, G has an element a of order p and an element b of order q. By the Corollary to Lemma 2.8.3, $b^{-1}ab = a^i$ for some i with $0 < i < p$. Thus $b^{-r}ab^r = a^{i^r}$ for all $r \geq 0$ (Prove!), and so $b^{-q}ab^q = a^{i^q}$. But $b^q = e$; therefore, $a^{i^q} = a$ and so $a^{i^q-1} = e$. Because a is of order p, we conclude that $p \mid i^q - 1$, which is to say, $i^q \equiv 1(p)$. However, by Fermat's Theorem, $i^{p-1} \equiv 1(p)$. Since $q \nmid p - 1$, we conclude that $i \equiv 1(p)$, and since $0 < i < p$, $i = 1$ follows. Therefore, $b^{-1}ab = a^i = a$, hence $ab = ba$. By Lemma 2.8.4, $c = ab$ has order pq, so the powers of c sweep out all of G. Thus G is cyclic, and the theorem is proved. □

PROBLEMS

Middle-Level Problems

1. In the proof of Theorem 2.8.2, show that if some two entries in $s = (a_1, a_2, \ldots, a_p)$ are different, then $f(s) \neq s$, and the orbit of s under f has p elements.
2. Prove that a group of order 35 is cyclic.
3. Using the result of Problem 40 of Section 5, give another proof of Lemma 2.8.3. (**Hint:** Use for H a subgroup of order p.)
4. Construct a nonabelian group of order 21. (**Hint:** Assume that $a^3 = e$,

$b^7 = e$ and find some i such that $a^{-1}ba = a^i \neq a$, which is consistent with the relations $a^3 = b^7 = e$.)

5. Let G be a group of order $p^n m$, where p is prime and $p \nmid m$. Suppose that G has a normal subgroup P of order p^n. Prove that $\theta(P) = P$ for every automorphism θ of G.
6. Let G be a finite group with subgroups A, B such that $|A| > \sqrt{|G|}$ and $|B| > \sqrt{|G|}$. Prove that $A \cap B \neq (e)$.
7. If G is a group with subgroups A, B of orders m, n, respectively, where m and n are relatively prime, prove that the subset of G, $AB = \{ab \mid a \in A, b \in B\}$, has mn distinct elements.
8. Prove that a group of order 99 has a nontrivial normal subgroup.
9. Prove that a group of order 42 has a nontrivial normal subgroup.
10. From the result of Problem 9, prove that a group of order 42 has a normal subgroup of order 21.

Harder Problems

11. If G is a group and A, B finite subgroups of G, prove that the set $AB = \{ab \mid a \in A, b \in B\}$ has $(|A|\,|B|)/|A \cap B|$ distinct elements.
12. Prove that any two nonabelian groups of order 21 are isomorphic. (See Problem 4.)

Very Hard Problems

13. Using the fact that any group of order 9 is abelian, prove that any group of order 99 is abelian.
14. Let $p > q$ be two primes such that $q \mid p - 1$. Prove that there exists a nonabelian group of order pq. (**Hint:** Use the result of Problem 40 of Section 4, namely that U_p is cyclic if p is a prime, and the idea needed to do Problem 4 above.)
15. Prove that if $p > q$ are two primes such that $q \mid p - 1$, then any two nonabelian groups of order pq are isomorphic.

9. DIRECT PRODUCTS

In several of the problems and examples that appeared earlier, we went through the following construction: If G_1, G_2 are two groups, then $G = G_1 \times G_2$ is the set of all ordered pairs (a, b), where $a \in G_1$ and $b \in G_2$ and

where the product was defined *component-wise* via $(a_1, b_1)(a_2, b_2) = (a_1a_2, b_1b_2)$, the products in each component being carried out in the respective groups G_1 and G_2. We should like to formalize this procedure here.

Definition. If $G_1, G_2, \ldots, G_n$ are n groups, then their (*external*) *direct product* $G_1 \times G_2 \times G_3 \times \cdots \times G_n$ is the set of all ordered n-tuples $(a_1, a_2, \ldots, a_n)$ where $a_i \in G_i$, for $i = 1, 2, \ldots, n$, and where the product in $G_1 \times G_2 \times \cdots \times G_n$ is defined component-wise, that is,

$$(a_1, a_2, \ldots, a_n)(b_1, b_2, \ldots, b_n) = (a_1b_1, a_2b_2, \ldots, a_nb_n).$$

That $G = G_1 \times G_2 \times \cdots \times G_n$ is a group is immediate, with $(e_1, e_2, \ldots, e_n)$ as its unit element, where e_i is the unit element of G_i, and where $(a_1, a_2, \ldots, a_n)^{-1} = (a_1^{-1}, a_2^{-1}, \ldots, a_n^{-1})$.

G is merely the Cartesian product of the groups $G_1, G_2, \ldots, G_n$ with a product defined in G by component-wise multiplication. We call it *external*, since the groups $G_1, G_2, \ldots, G_n$ are any groups, with no relation necessarily holding among them.

Consider the subsets $\overline{G}_i \subset G_1 \times G_2 \times \cdots \times G_n = G$, where

$$\overline{G}_i = \{(e_1, \ldots, e_{i-1}, a_i, e_{i+1}, \ldots, e_n) \mid a_i \in G_i\};$$

in other words, $\overline{G}_i$ consists of all n-tuples where in the ith component any element of G_i can occur and where every other component is the identity element. Clearly, $\overline{G}_i$ is a group and is isomorphic to G_i by the isomorphism $\pi_i: \overline{G}_i \to G_i$ defined by $\pi_i(e_1, e_2, \ldots, a_i, \ldots, e_n) = a_i$. Furthermore, not only is $\overline{G}_i$ a subgroup of G but $\overline{G}_i \lhd G$. (Prove!)

Given any element $a = (a_1, a_2, \ldots, a_n) \in G$, then

$$a = (a_1, e_2, \ldots, e_n)(e_1, a_2, e_3, \ldots, e_n) \cdots (e_1, e_2, \ldots, e_{n-1}, a_n);$$

that is, every $a \in G$ can be written as $a = \bar{a}_1\bar{a}_2 \cdots \bar{a}_n$, where each $\bar{a}_i \in \overline{G}_i$. Moreover, a can be written in this way in a unique manner, that is, if $a = \bar{a}_1\bar{a}_2 \cdots \bar{a}_n = \bar{b}_1\bar{b}_2 \cdots \bar{b}_n$, where the $\bar{a}_i \in \overline{G}_i$ and $\bar{b}_i \in \overline{G}_i$, then $\bar{a}_1 = \bar{b}_1, \ldots, \bar{a}_n = \bar{b}_n$. So G is built up from certain normal subgroups, the $\overline{G}_i$, as $G = \overline{G}_1\overline{G}_2 \cdots \overline{G}_n$ in such a way that every element $a \in G$ has a *unique* representation in the form $a = \bar{a}_1\bar{a}_2 \cdots \bar{a}_n$ with $\bar{a}_i \in \overline{G}_i$.

This motivates the following

Definition. The group G is said to be the (*internal*) *direct product* of its *normal* subgroups $N_1, N_2, \ldots, N_n$ if every $a \in G$ has a *unique* representation in the form $a = a_1a_2 \cdots a_n$, where each $a_i \in N_i$ for $i = 1, 2, \ldots, n$.

From what we have discussed above we have the

Lemma 2.9.1. If $G = G_1 \times G_2 \times \cdots \times G_n$ is the external direct product of $G_1, G_2, \ldots, G_n$, then G is the internal direct product of the normal subgroups $\overline{G}_1, \overline{G}_2, \ldots, \overline{G}_n$ defined above.

We want to go in the other direction, namely to prove that if G is the internal direct product of its normal subgroups $N_1, N_2, \ldots, N_n$, then G is isomorphic to $N_1 \times N_2 \times \cdots \times N_n$. To do so, we first get some preliminary results.

The result we are about to prove has already occurred as Problem 20, Section 5. For the sake of completeness we prove it here.

Lemma 2.9.2. Let G be a group, M, N normal subgroups of G such that $M \cap N = (e)$. Then, given $m \in M$ and $n \in N$, $mn = nm$.

Proof. Consider the element $a = mnm^{-1}n^{-1}$. Viewing a as bracketed one way, $a = (mnm^{-1})n^{-1}$; then, since $N \lhd G$ and $n \in N$, $mnm^{-1} \in N$, so $a = (mnm^{-1})n^{-1}$ is also in N. Now bracket a in the other way, $a = m(nm^{-1}n^{-1})$. Since $M \lhd G$ and $m^{-1} \in M$, we have $nm^{-1}n^{-1} \in M$ and so $a = m(nm^{-1}n^{-1}) \in M$. Thus $a \in M \cap N = (e)$, which is to say, $mnm^{-1}n^{-1} = e$. This gives us that $mn = nm$, as required. □

If G is the internal direct product of the normal subgroups $N_1, N_2, \ldots, N_n$, we claim that $N_i \cap N_j = (e)$ for $i \neq j$. For suppose that $a \in N_i \cap N_j$; then $a = e \cdot e \cdots eae \cdots e$, where the a occurs in the ith place. This gives us one representation of a in $G = N_1N_2 \cdots N_n$. On the other hand, $a = e \cdot e \cdots e \cdot a \cdot e \cdots e$, where the a occurs in the jth place, so a has the second representation as an element of $N_1N_2 \cdots N_n$. By the uniqueness of the representation, we get $a = e$, and so $N_i \cap N_j = (e)$.

Perhaps things would be clearer if we do it for $n = 2$. So suppose that $N_1 \lhd G$, $N_2 \lhd G$, and every element $a \in G$ has a unique representation as $a = a_1 \cdot a_2$, where $a_1 \in N_1$, $a_2 \in N_2$. Suppose that $a \in N_1 \cap N_2$; then $a = a \cdot e$ is a representation of $a = a_1 \cdot a_2$ with $a_1 = a \in N_1$, $a_2 = e \in N_2$. However $a = e \cdot a$, so $a = b_1 \cdot b_2$, where $b_1 = e \in N_1$, $b_2 = a \in N_2$. By the uniqueness of the representation we must have $a_1 = b_1$, that is, $a = e$. So $N_1 \cap N_2 = (e)$.

The argument given above for $N_1, \ldots, N_n$ is the same argument as that given for $n = 2$, but perhaps is less transparent. At any rate we have proved

Lemma 2.9.3. If G is the internal direct product of its normal subgroups $N_1, N_2, \ldots, N_n$, then, for $i \neq j$, $N_i \cap N_j = (e)$.

Corollary. If G is as in Lemma 2.9.3, then if $i \neq j$ and $a_i \in N_i$ and $a_j \in N_j$, we have $a_ia_j = a_ja_i$.

Proof. By Lemma 2.9.3, $N_i \cap N_j = (e)$ for $i \neq j$. Since the N's are normal in G, by Lemma 2.9.2 we have that any element in N_i *commutes* with any element in N_j, that is, $a_i a_j = a_j a_i$ for $a_i \in N_i$, $a_j \in N_j$. □

With these preliminaries out of the way we can now prove

Theorem 2.9.4. Let G be a group with normal subgroups $N_1, N_2, \ldots, N_n$. Then the mapping $\psi(a_1, a_2, \ldots, a_n) = a_1 a_2 \cdots a_n$ is an isomorphism from $N_1 \times N_2 \times \cdots \times N_n$ (external direct product) onto G if and only if G is the internal direct product of $N_1, N_2, \ldots, N_n$.

Proof. Suppose G is an internal direct product of $N_1, \ldots, N_n$. Since every element a in G has a representation $a = a_1 a_2 \cdots a_n$, with the $a_i \in N_i$, we have that the mapping ψ is onto. We assert that it is also 1-1. For if $\psi((a_1, a_2, \ldots, a_n)) = \psi((b_1, b_2, \ldots, b_n))$, then by the definition of ψ, $a_1 a_2 \cdots a_n = b_1 b_2 \cdots b_n$. By the uniqueness of the representation of an element in this form we deduce that $a_1 = b_1, a_2 = b_2, \ldots, a_n = b_n$. Hence ψ is 1-1.

All that remains is to show that ψ is a homomorphism. So, consider

$$\begin{aligned}\psi((a_1, a_2, \ldots, a_n)(b_1, b_2, \ldots, b_n)) &= \psi((a_1 b_1, a_2 b_2, \ldots, a_n b_n)) \\ &= (a_1 b_1)(a_2 b_2) \cdots (a_n b_n) \\ &= a_1 b_1 a_2 b_2 \cdots a_n b_n.\end{aligned}$$

Since $b_1 \in N_1$, it commutes with a_i, b_i for $i > 1$ by the Corollary to Lemma 2.9.3. So we can pull the b_1 across all the elements to the right of it to get $a_1 b_1 a_2 b_2 \cdots a_n b_n = a_1 a_2 b_2 a_3 b_3 \cdots a_n b_n b_1$. Now repeat this procedure with b_2, and so on, to get that $a_1 b_1 a_2 b_2 \cdots a_n b_n = (a_1 a_2 \cdots a_n)(b_1 b_2 \cdots b_n)$. Thus

$$\begin{aligned}\psi((a_1, a_2, \ldots, a_n)(b_1, b_2, \ldots, b_n)) &= a_1 b_1 a_2 b_2 \cdots a_n b_n \\ &= (a_1 a_2 \cdots a_n)(b_1 b_2 \cdots b_n) \\ &= \psi((a_1, a_2, \ldots, a_n))\psi((b_1 b_2, \ldots, b_n)).\end{aligned}$$

In other words, ψ is a homomorphism.

On the other hand, suppose that ψ is an isomorphism. Then the conclusion that G is the internal direct product of $N_1, N_2, \ldots, N_n$ easily follows from the fact that ψ is onto and 1-1.

With this the proof of Theorem 2.9.4 is complete. □

Corollary. Let G be a group with normal subgroups N_1, N_2. Then G is the internal direct product of N_1 and N_2 if and only if $G = N_1 N_2$ and $N_1 \cap N_2 = (e)$.

Proof. This follows easily from the fact that $\psi: N_1 \times N_2 \to G$, which is given by $\psi(a_1, a_2) = a_1 a_2$, is an isomorphism if and only if $N_1 N_2 = G$ and $N_1 \cap N_2 = (e)$. □

In view of the result of Theorem 2.9.4 and its corollary, we drop the adjectives "internal" and "external" and merely speak about the "direct product." When notation $G = N_1 \times N_2$ is used it should be clear from context whether it stands for the internal or external direct product.

The objective is often to show that a given group is the direct product of certain normal subgroups. If one can do this, the structure of the group can be completely determined if we happen to know those of the normal subgroups.

PROBLEMS

1. If G_1 and G_2 are groups, prove that $G_1 \times G_2 \simeq G_2 \times G_1$.

2. If G_1 and G_2 are cyclic groups of orders m and n, respectively, prove that $G_1 \times G_2$ is cyclic if and only if m and n are relatively prime.

3. Let G be a group, $A = G \times G$. In A let $T = \{(g, g) \mid g \in G\}$.
(a) Prove that $T \simeq G$.
(b) Prove that $T \lhd A$ if and only if G is abelian.

4. Let G be an abelian group of order $p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}$, where $p_1, p_2, \ldots, p_k$ are distinct primes and $m_1 > 0$, $m_2 > 0, \ldots, m_k > 0$. By Problem 10 of Section 6, for each i, G has a subgroup P_i of order $p_i^{m_i}$. Show that $G \simeq P_1 \times P_2 \times \cdots \times P_k$.

5. Let G be a finite group, $N_1, N_2, \ldots, N_k$ normal subgroups of G such that $G = N_1 N_2 \cdots N_k$ and $|G| = |N_1|\,|N_2| \cdots |N_k|$. Prove that G is the direct product of $N_1, N_2, \ldots, N_k$.

6. Let G be a group, $N_1, N_2, \ldots, N_k$ normal subgroups of G such that:
1. $G = N_1 N_2 \cdots N_k$.
2. For each i, $N_i \cap (N_1 N_2 \cdots N_{i-1} N_{i+1} \cdots N_k) = (e)$.

Prove that G is the direct product of $N_1, N_2, \ldots, N_k$.

10. FINITE ABELIAN GROUPS (OPTIONAL)

We have just finished discussing the idea of the direct product of groups. If we were to leave that topic at the point where we ended, it might seem like a nice little construction, but so what? To give some more substance to it,

we should prove at least one theorem which says that a group satisfying a certain condition is the direct product of some particularly easy groups. Fortunately, such a class of groups exists, the finite abelian groups. What we shall prove is that any finite abelian group is the direct product of cyclic groups. This reduces most questions about finite abelian groups to questions about cyclic groups, a reduction that often allows us to get complete answers to these questions.

The results on the structure of finite abelian groups are really special cases of some wider and deeper theorems. To consider these would be going too far afield, especially since the story for finite abelian groups is so important in its own right. The theorem we shall prove is called the *Fundamental Theorem on Finite Abelian Groups*, and rightfully so.

Before getting down to the actual details of the proof, we should like to give a quick sketch of how we shall go about proving the theorem.

Our first step will be to reduce the problem from any finite abelian group to one whose order is p^n, where p is a prime. This step will be fairly easy to carry out, and since the group will have order involving just one prime, the details of the proof will not be cluttered with elements whose orders are somewhat complicated.

So we shall focus on groups of order p^n. Let G be an abelian group of order p^n. We want to show that there exist cyclic subgroups of G, namely $A_1, A_2, \ldots, A_k$, such that every element $x \in G$ can be written as $x = b_1 b_2 \cdots b_k$, where each $b_i \in A_i$, in a unique way. Otherwise put, since each A_i is cyclic and generated by a_i, say, we want to show that $x = a_1^{m_1} a_2^{m_2} \cdots a_k^{m_k}$, where the elements $a_i^{m_i}$ are unique.

A difficulty appears right away, for there is not just one choice for these elements $a_1, \ldots, a_k$. For instance, if G is the abelian group of order 4 with elements e, a, b, ab, where $a^2 = b^2 = e$ and $ab = ba$, then we can see that if A, B, C are the cyclic subgroups generated by a, b, and ab, respectively, then $G = A \times B = A \times C = B \times C$. So there is a lack of uniqueness in the choice of the a_i. How to get around this?

What we need is a mechanism for picking a_1 and which, when applied after we have picked a_1, will allow us to pick a_2, and so on. What should this mechanism be? Our control on the elements of G lies only in specifying their orders. It is the order of the element—when properly used—that will give us the means to prove the theorem.

Suppose that $G = A_1 \times A_2 \times \cdots \times A_k$, where $|G| = p^n$ and the A's have been numbered, so that $|A_i| = p^{n_i}$ and $n_1 \geq n_2 \geq \cdots \geq n_k$, and each A_i is cyclic generated by a_i. If this were so and $x = a_1^{m_1} \cdots a_k^{m_k}$, then

$$x^{p^{n_1}} = (a_1^{m_1} \cdots a_k^{m_k})^{p^{n_1}} = a_1^{m_1 p^{n_1}} a_2^{m_2 p^{n_1}} \cdots a_k^{m_k p^{n_1}}$$

because $n_1 \geq n_i$, $p^{n_i} | p^{n_1}$, so since every $a_i^{m_i p^{n_i}} = e$, thus $x^{p^{n_1}} = e$. *In other words, a_1 should be an element of G whose order is as large as it can possibly be.* Fine, we can now pick a_1. What do we do for a_2? If $\overline{G} = G/A_1$, then to get the first element needed to represent $\overline{G}$ as a direct product of cyclic groups, we should pick an element in $\overline{G}$ whose order is maximal. What does this translate into in G itself? We want an element a_2 such that *a_2 requires as high a power as possible to fall into A_1*. So that will be the road to the selection of the second element. However, if we pick an element a_2 with this property, it may not do the trick; we may have to adapt it so that it will. The doing of all this is the technical part of the argument and does go through. Then one repeats it appropriately to find an element a_3, and so on.

This is the procedure we shall be going through to prove the theorem. But to smooth out these successive choices of $a_1, a_2, \ldots$, we shall use an induction argument and some subsidiary preliminary results.

With this sketch as guide we hope the proof of the theorem will make sense to the reader. One should not confuse the basic idea in the proof—which is quite reasonable—with the technical details, which may cloud the issue. So we now begin to fill in the details of the sketch of the proof that we outlined above.

Lemma 2.10.1. Let G be a finite abelian group of order mn, where m and n are relatively prime. If $M = \{x \in G \mid x^m = e\}$ and $N = \{x \in G \mid x^n = e\}$, then $G = M \times N$. Moreover, if neither m nor n is 1, then $M \neq (e)$ and $N \neq (e)$.

Proof. The sets M and N defined in the assertion above are quickly seen to be subgroups of G. Moreover, if $m \neq 1$, then by Cauchy's Theorem (Theorem 2.6.4) we readily obtain $M \neq (e)$, and similarly if $n \neq 1$, that $N \neq (e)$. Furthermore, since $M \cap N$ is a subgroup of both M and N, by Lagrange's Theorem, $|M \cap N|$ divides $|M| = m$ and $|N| = n$. Because m and n are relatively prime, we obtain $|M \cap N| = 1$, hence $M \cap N = (e)$.

To finish the proof, we need to show that $G = MN$ and $G = M \times N$. Since m and n are relatively prime, there exist integers r and s such that $rm + sn = 1$. If $a \in G$, then $a = a^1 = a^{sn+rm} = a^{sn}a^{rm}$; since $(a^{sn})^m = a^{snm} = e$, we have that $a^{sn} \in M$. Similarly, $a^{rm} \in N$. Thus $a = a^{sn}a^{rm}$ is in MN. In this way $G = MN$. It now follows from Corollary to Theorem 2.9.4 that $G = M \times N$. □

An immediate consequence is the

Corollary. Let G be a finite abelian group and let p be a prime such that p divides $|G|$. Then $G = P \times T$ for some subgroups P and T, where $|P| = p^m$, $m > 0$, and $|T|$ is not divisible by p.

Proof. Let $P = \{x \in G \mid x^{p^s} = e \text{ for some } s\}$ and let the subset $T = \{x \in G \mid x^t = e \text{ for } t \text{ relatively prime to } p\}$. By Lemma 2.10.1, $G = P \times T$ and $P \neq (e)$. Since every element in P has order a power of p, $|P|$ is not divisible by any other prime (by Cauchy's Theorem), so $|P| = p^m$ for some m.

It is easy to see that $p \nmid |T|$ by making use of Lagrange's Theorem. Thus we really have that P is not merely some subgroup of G but is what is called a p-Sylow subgroup of G. (See Section 11). □

We now come to the key step in the proof of the theorem we seek. The proof is a little difficult, but once we have this result the rest will be easy.

Theorem 2.10.2. Let G be an abelian group of order p^n, p a prime, and let $a \in G$ have maximal order of all the elements in G. Then $G = A \times Q$, where A is the cyclic subgroup generated by a.

Proof. We proceed by induction on n. If $n = 1$, then $|G| = p$ and G is already a cyclic group generated by any $a \neq e$ in G.

We suppose the theorem to be true for all $m < n$. We first show that the theorem is correct if there exists an element $b \in G$ such that $b \notin A = (a)$ and $b^p = e$. Let $B = (b)$, the subgroup of G generated by b; thus $A \cap B = (e)$ (see Problem 1).

Let $\overline{G} = G/B$; by assumption $B \neq (e)$, hence $|\overline{G}| < |G|$. In $\overline{G}$, what is the order of $\bar{a} = Ba$? We claim that $o(\bar{a}) = o(a)$. To begin with, we know that $o(\bar{a}) \mid o(a)$ (see Problem 6 of Section 2.7). On the other hand, $\bar{a}^{o(\bar{a})} = \bar{e}$, so $a^{o(\bar{a})} \in B$. Since $a^{o(\bar{a})} \in A$, we see that $a^{o(\bar{a})} \in A \cap B = (e)$, whence $a^{o(\bar{a})} = e$. This tells us that $o(a) \mid o(\bar{a})$. Hence $o(a) = o(\bar{a})$.

Since $\bar{a}$ is an element of maximal order in $\overline{G}$, by the induction we know that $\overline{G} = (\bar{a}) \times T$ for some subgroup T of $\overline{G}$. By the Correspondence Theorem we also know that $T = Q/B$ for some subgroup Q of G. We claim that G is the internal direct product $A \times Q$. That $G = AQ$ is left to the reader. It remains to show that $A \cap Q = (e)$. Let $a^i \in A \cap Q$. Then $\bar{a}^i \in Q/B = T$, and since $(\bar{a}) \cap T = (\bar{e})$, we have that $\bar{a}^i = \bar{e}$. But since $o(a) = o(\bar{a})$, this implies $a^i = e$. Therefore, $A \cap Q = (e)$ and we obtain that $G = A \times Q$.

Suppose, then, that there is *no* element b in G, b not in A, such that $b^p = e$. We claim that this forces $G = A = (a)$, in which case G is a cyclic group. Suppose that $G \neq A$ and let $x \in G$, $x \notin A$ have smallest possible order. Because $o(x^p) < o(x)$, we have, by our choice of x, that $x^p \in A$, hence $x^p = a^i$ for some i.

We claim that $p \mid i$. Let $o(a) = p^s$, and note that the maximality

of the order of a implies that $x^{p^s} = e$. But $x^{p^s} = (x^p)^{p^{s-1}} = (a^i)^{p^{s-1}} = e$. Since $o(a) = p^s$, we have $p \mid i$.

Thus $x^p = a^i$, where $p \mid i$. Let $y = a^{-i/p} \cdot x$. Then $y^p = a^{-i}x^p = a^{-i}a^i = e$. Moreover, $y \notin (a) = A$, because $x \notin A$. But this puts us back in the situation discussed above, where there exists a $b \in G$, $b \notin A$ such that $b^p = e$; in that case we saw that the theorem was correct. So we must have $G = (a)$, and G is a cyclic group. This finishes the induction and proves the theorem. □

We are now able to prove the very basic and important

Theorem 2.10.3 (Fundamental Theorem on Finite Abelian Groups). A finite abelian group is the direct product of cyclic groups.

Proof. Let G be a finite abelian group and p a prime that divides $|G|$. By the Corollary to Lemma 2.10.1, $G = P \times T$, where $|P| = p^n$. By Theorem 2.10.2, $P = A_1 \times A_2 \times \cdots \times A_k$, where the A_i are cyclic subgroups of P. Arguing by induction on $|G|$, we may thus assume that $T = T_1 \times T_2 \times \cdots \times T_q$, where the T_i are cyclic subgroups of T. Thus

$$\begin{aligned} G &= (A_1 \times A_2 \times \cdots \times A_k) \times (T_1 \times T_2 \times \cdots \times T_q) \\ &= A_1 \times A_2 \times \cdots \times A_k \times T_1 \times T_2 \times \cdots \times T_q. \end{aligned}$$

This very important theorem is now proved. □

We return to abelian groups G of order p^n. We now have at hand that $G = A_1 \times A_2 \times \cdots \times A_k$, where the A_i are cyclic groups of order p^{n_i}. We can arrange the numbering so that $n_1 \geq n_2 \geq \cdots \geq n_k$. Also, $|G| = |A_1 \times A_2 \times \cdots \times A_k| = |A_1|\,|A_2| \cdots |A_k|$, which gives us that

$$p^n = p^{n_1}p^{n_2} \cdots p^{n_k} = p^{n_1+n_2+\cdots+n_k},$$

hence $n = n_1 + n_2 + \cdots + n_k$. Thus the integers $n_i \geq 0$ give us a *partition* of n. It can be shown that these integers $n_1, n_2, \ldots, n_k$—which are called the *invariants* of G—are *unique*. In other words, two abelian groups of order p^n are isomorphic if and only if they have the same invariants. Granted this, it follows that the number of nonisomorphic abelian groups of order p^n is equal to the number of partitions of n.

For example, if $n = 3$, it has the following three partitions: $3 = 3$, $3 = 2 + 1$, $3 = 1 + 1 + 1$, so there are three nonisomorphic abelian groups of order p^3 (independent of p). The groups corresponding to these partitions are a cyclic group of order p^3, the direct product of a cyclic group of order p^2 by one of order p, and the direct product of three cyclic groups of order p, respectively.

For $n = 4$ we see the partitions are $4 = 4$, $4 = 3 + 1$, $4 = 2 + 2$, $4 = 2 + 1 + 1$, $4 = 1 + 1 + 1 + 1$, which are five in number. Thus there are five nonisomorphic groups of order p^4. Can you describe them via the partitions of 4?

Given an abelian group of order $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, where the p_i are distinct primes and the a_i are all positive, then G is the direct product of its so-called p_i– Sylow subgroups (see, e.g., the Corollary to Lemma 2.10.1). For each prime p_i there are as many groups of order $p_i^{a_i}$ as there are partitions of a_i. So the number of nonisomorphic abelian groups of order $n = p_1^{a_1} \cdots p_k^{a_k}$ is $f(a_1)f(a_2) \cdots f(a_k)$, where $f(m)$ denotes the number of partitions of m. Thus we know how many nonisomorphic finite abelian groups there are for any given order.

For instance, how many nonisomorphic abelian groups are there of order 144? Since $144 = 2^4 3^2$, and there are five partitions of 4, two partitions of 2, there are 10 nonisomorphic abelian groups of order 144.

The material treated in this section has been hard, the path somewhat tortuous, and the effort to understand quite intense. To spare the reader too much further agony, we assign only three problems to this section.

PROBLEMS

1. Let A be a normal subgroup of a group G, and suppose that $b \in G$ is an element of prime order p, and that $b \notin A$. Show that $A \cap (b) = (e)$.

2. Let G be an abelian group of order p^n, p a prime, and let $a \in G$ have maximal order. Show that $x^{o(a)} = e$ for all $x \in G$.

3. Let G be a finite group, with $N \lhd G$ and $a \in G$. Prove that:

(a) The order of aN in G/N divides the order of a in G, that is, $o(aN) \mid o(a)$.

(b) If $(a) \cap N = (e)$, then $o(aN) = o(a)$.

11. CONJUGACY AND SYLOW'S THEOREM (OPTIONAL)

In discussing equivalence relations in Section 4 we mentioned, as an example of such a relation in a group G, the notion of *conjugacy*. Recall that the element b in G is said to be *conjugate* to $a \in G$ (or merely, a conjugate of a) if there exists an $x \in G$ such that $b = x^{-1}ax$. We showed in Section 4 that this defines an equivalence relation on G. The equivalence class of a, which we denote by $\mathrm{cl}(a)$, is called the *conjugacy class* of a.

For a finite group an immediate question presents itself: How large is $\mathrm{cl}(a)$? Of course, this depends strongly on the element a. For instance, if $a \in Z(G)$, the center of G, then $ax = xa$ for all $x \in G$, hence $x^{-1}ax = a$; in other words, the conjugacy class of a in this case consists merely of the element a itself. On the other hand, if $\mathrm{cl}(a)$ consists only of the element a, then $x^{-1}ax = a$ for all $x \in G$. This gives us that $xa = ax$ for all $x \in G$, hence $a \in Z(G)$. So $Z(G)$ is characterized as the set of those elements a in G whose conjugacy class has only one element, a itself.

For an abelian group G, since $G = Z(G)$, two elements are conjugate if and only if they are equal. So conjugacy is not an interesting relation for abelian groups; however, for nonabelian groups it is a highly interesting notion.

Given $a \in G$, $\mathrm{cl}(a)$ consists of all $x^{-1}ax$ as x runs over G. So to determine which are the distinct conjugates of a, we need to know when two conjugates of a coincide, which is the same as asking: When is $x^{-1}ax = y^{-1}ay$? In this case, transposing, we obtain $a(xy^{-1}) = (xy^{-1})a$; in other words, xy^{-1} must commute with a. This brings us to a concept introduced as Example 10 in Section 3, *that of the centralizer of a in G*. We repeat something we did there.

Definition. If $a \in G$, then $C(a)$, the *centralizer of a in G*, is defined by $C(a) = \{x \in G \mid xa = ax\}$.

When $C(a)$ arose in Section 3 we showed that it was a subgroup of G. We record this now more officially as

Lemma 2.11.1. For $a \in G$, $C(a)$ is a subgroup of G.

As we saw above, the two conjugates $x^{-1}ax$ and $y^{-1}ay$ of a are equal only if $xy^{-1} \in C(a)$, that is, only if x and y are in the same right coset of $C(a)$ in G. On the other hand, if x and y are in the same right coset of $C(a)$ in G, then $xy^{-1} \in C(a)$, hence $xy^{-1}a = axy^{-1}$. This yields that $x^{-1}ax = y^{-1}ay$. So x and y give rise to the same conjugate of a if and only if x and y are in the same right coset of $C(a)$ in G. *Thus there are as many conjugates of a in G as there are right cosets of* $C(a)$ *in* G. This is most interesting when G is a finite group, for in that case the number of right cosets of $C(a)$ in G is what we called the *index*, $i_G(C(a))$, of $C(a)$ in G, and is equal to $|G|/|C(a)|$.

We have proved

Theorem 2.11.2. Let G be a finite group and $a \in G$; then the number of distinct conjugates of a in G equals the index of $C(a)$ in G.

In other words, the number of elements in $\mathrm{cl}(a)$ equals $i_G(C(a)) = |G|/|C(a)|$.

This theorem, although it was relatively easy to prove, is very important and has many consequences. We shall see a few of these here.

One such consequence is a kind of bookkeeping result. Since conjugacy is an equivalence relation on G, G is the union of the disjoint conjugacy classes. Moreover, by Theorem 2.11.2, we know how many elements there are in each class. Putting all this information together, we get

Theorem 2.11.3 (The Class Equation). If G is a finite group, then

$$|G| = \sum_a i_G(C(a)) = \sum_a \frac{|G|}{|C(a)|},$$

where the sum runs over one a from each conjugacy class.

It is almost a sacred tradition among mathematicians to give, as the first application of the class equation, a particular theorem about groups of order p^n, where p is a prime. Not wanting to be accused of heresy, we follow this tradition and prove the pretty and important

Theorem 2.11.4. If G is a group of order p^n, where p is a prime, then $Z(G)$, the center of G, is not trivial (i.e., there exists an element $a \neq e$ in G such that $ax = xa$ for all $x \in G$).

Proof. We shall exploit the class equation to carry out the proof. Let $z = |Z(G)|$; as we pointed out previously, z is then the number of elements in G whose conjugacy class has only one element. Since $e \in Z(G)$, $z \geq 1$. For any element b outside $Z(G)$, its conjugacy class contains more than one element and $|C(b)| < |G|$. Moreover, since $|C(b)|$ divides $|G|$ by Lagrange's theorem, $|C(b)| = p^{n(b)}$, where $1 \leq n(b) < n$. We divide the pieces of the class equation into two parts: that coming from the center, and the rest. We get, this way,

$$p^n = |G| = z + \sum_{b \notin Z(G)} \frac{|G|}{|C(b)|} = z + \sum_{n(b)<n} \frac{p^n}{p^{n(b)}} = z + \sum_{n(b)<n} p^{n-n(b)}.$$

Clearly, p divides the left-hand side, p^n, and divides $\Sigma_{n(b)<n} p^{n-n(b)}$. The net result of this is that $p \mid z$, and since $z \geq 1$, we have that z is *at least* p. So since $z = |Z(G)|$, there must be an element $a \neq e$ in $Z(G)$, which proves the theorem. □

This last theorem has an interesting application, which some readers may have seen in solving Problem 45 of Section 5. This is

Theorem 2.11.5. If G is a group of order p^2, where p is a prime, then G is abelian.

Proof. By Theorem 2.11.4, $Z(G) \neq (e)$, so that there is an element, a, of order p in $Z(G)$. If $A = (a)$, the subgroup generated by a, then $A \subset Z(G)$, hence $A \subset C(x)$ for all $x \in G$. Given $x \in G$, $x \notin A$, then $C(x) \supset A$ and $x \in C(x)$; so $|C(x)| > p$, yet $|C(x)|$ must divide p^2. The net result of this is that $|C(x)| = p^2$, so $C(x) = G$, whence $x \in Z(G)$. Since every element of G is in the center of G, G must be abelian. □

In the problems to come we shall give many applications of the nature of groups of order p^n, where p is a prime. *The natural attack on virtually all these problems follows the lines of the argument we are about to give.* We choose one of a wide possible set of choices to illustrate this technique.

Theorem 2.11.6. If G is a group of order p^n, p a prime, then G contains a normal subgroup of order p^{n-1}.

Proof. We proceed by induction on n. If $n = 1$, then G is of order p and (e) is the required normal subgroup of order $p^{1-1} = p^0 = 1$.

Suppose that we know that for some k every group of order p^k has a normal subgroup of order p^{k-1}. Let G be of order p^{k+1}; by Theorem 2.11.4 there exists an element a of order p in $Z(G)$, the center of G. Thus the subgroup $A = (a)$ generated by a is of order p and is normal in G. Consider $\Gamma = G/A$; Γ is a group of order $|G|/|A| = p^{k+1}/p = p^k$ by Theorem 2.6.3. Since Γ has order p^k, we know that Γ has a normal subgroup M of order p^{k-1}. Since Γ is a homomorphic image of G, by the Correspondence Theorem (Theorem 2.7.2) there is a normal subgroup N in G, $N \supset A$, such that $N/A = M$. But then we have

$$p^{k-1} = |M| = |N/A| = \frac{|N|}{|A|},$$

that is, $p^{k-1} = |N|/p$, leading us to $|N| = p^k$. Thus N is our required normal subgroup in G of order p^k. This completes the induction and so proves the theorem. □

By far the most important application we make of the class equation is the proof of a far-reaching theorem due to Sylow, a Norwegian mathematician, who proved it in 1871. We already showed this theorem to be true for abelian groups. We shall now prove it for any finite group. It is impossible to overstate the importance of *Sylow's Theorem* in the study of finite groups. Without it the subject would not get off the ground.

Theorem 2.11.7 (Sylow's Theorem). Suppose that G is a group of order $p^n m$, where p is a prime and $p \nmid m$. Then G has a subgroup of order p^n.

Proof. If $n = 0$, this is trivial. We therefore assume that $n \geq 1$. Here, again, we proceed by induction on $|G|$, assuming the result to be true for all groups H such that $|H| < |G|$.

Suppose that the result is false for G. Then, by our induction hypothesis, p^n *cannot divide* $|H|$ for any subgroup H of G if $H \neq G$. *In particular, if* $a \notin Z(G)$, *then* $C(a) \neq G$, *hence* $p^n \nmid |C(a)|$. Thus p divides $|G|/|C(a)| = i_G(C(a))$ for $a \notin Z(G)$.

Write down the class equation for G following the lines of the argument in Theorem 2.11.4. If $z = |Z(G)|$, then $z \geq 1$ and

$$p^n m = |G| = z + \sum_{a \notin Z(G)} i_G(C(a)).$$

But $p \mid i_G(C(a))$ if $a \notin Z(G)$, so $p \mid \Sigma_{a \notin Z(G)} i_G(C(a))$. Since $p \mid p^n m$, we get $p \mid z$. By Cauchy's Theorem there is an element a of order p in $Z(G)$. If A is the subgroup generated by a, then $|A| = p$ and $A \lhd G$, since $a \in Z(G)$. Consider $\Gamma = G/A$; $|\Gamma| = |G|/|A| = p^n m/p = p^{n-1} m$. Since $|\Gamma| < |G|$, by our induction hypothesis Γ has a subgroup M of order p^{n-1}. However, by the Correspondence Theorem there is a subgroup P of G such that $P \supset A$ and $P/A = M$. Therefore, $|P| = |M|\,|A| = p^{n-1} p = p^n$ and P is the sought-after subgroup of G of order p^n, contradicting our assumption that G had no such subgroup. This completes the induction, and Sylow's Theorem is established. □

Actually, Sylow's Theorem consists of three parts, of which we only proved the first. The other two are (assuming $p^n m = |G|$, where $p \nmid m$):

1. Any two subgroups of order p^n in G are conjugate; that is, if $|P| = |Q| = p^n$ for subgroups P, Q of G, then for some $x \in G$, $Q = x^{-1} P x$.
2. The number of subgroups of order p^n in G is of the form $1 + kp$ and divides $|G|$.

Since these subgroups of order p^n pop up all over the place, they are called *p-Sylow subgroups* of G. An abelian group has one p-Sylow subgroup for every prime p dividing its order. This is far from true in the general case. For instance, if $G = S_3$, the symmetric group of degree 3, which has order $6 = 2 \cdot 3$, there are three 2-Sylow subgroups (of order 2) and one 3-Sylow subgroup (or order 3).

For those who want to see several proofs of that part of Sylow's Theorem which we proved above, and of the other two parts, they might look at the appropriate section of our book *Topics in Algebra*.

PROBLEMS

Easier Problems

1. In S_3, the symmetric group of degree 3, find all the conjugacy classes, and check the validity of the class equation by determining the orders of the centralizers of the elements of S_3.
2. Do Problem 1 for G the dihedral group of order 8.
3. If $a \in G$, show that $C(x^{-1}ax) = x^{-1}C(a)x$.
4. If φ is an automorphism of G, show that $C(\varphi(a)) = \varphi(C(a))$ for $a \in G$.
5. If $|G| = p^3$ and $|Z(G)| \geq p^2$, prove that G is abelian.
6. If P is a p-Sylow subgroup of G and $P \lhd G$, prove that P is the only p-Sylow subgroup of G.
7. If $P \lhd G$, P a p-Sylow subgroup of G, prove that $\varphi(P) = P$ for every automorphism φ of G.
8. Use the class equation to give a proof of Cauchy's Theorem.

   If H is a subgroup of G, let $N(H) = \{x \in G \mid x^{-1}Hx = H\}$. This *does not mean* that $xa = ax$ whenever $x \in N(H)$, $a \in H$. For instance, if $H \lhd G$, then $N(H) = G$, yet H need not be in the center of G.
9. Prove that $N(H)$ is a subgroup of G, $H \subset N(H)$ and in fact $H \lhd N(H)$.
10. Prove that $N(x^{-1}Hx) = x^{-1}N(H)x$.
11. If P is a p-Sylow subgroup of G, prove that P is a p-Sylow subgroup of $N(P)$ and is the only p-Sylow subgroup of $N(P)$.
12. If P is a p-Sylow subgroup and $a \in G$ is of order p^m for some m, show that if $a^{-1}Pa = P$ then $a \in P$.
13. Prove that if G is a finite group and H is a subgroup of G, then the number of distinct subgroups $x^{-1}Hx$ of G equals $i_G(N(H))$.
14. If P is a p-Sylow subgroup of G, show that the number of distinct $x^{-1}Px$ *cannot* be a multiple of p.
15. If $N \lhd G$, let $B(N) = \{x \in G \mid xa = ax \text{ for all } a \in N\}$. Prove that $B(N) \lhd G$.

Middle-Level Problems

16. Show that a group of order 36 has a normal subgroup of order 3 or 9. (**Hint:** See Problem 40 of Section 5.)
17. Show that a group of order 108 has a normal subgroup of order 9 or 27.
18. If P is a p-Sylow subgroup of G, show that $N(N(P)) = N(P)$.
19. If $|G| = p^n$, show that G has a subgroup of order p^m for all $1 \leq m \leq n$.

20. If p^m divides $|G|$, show that G has a subgroup of order p^m.

21. If $|G| = p^n$ and $H \neq G$ is a subgroup of G, show that $N(H) \supsetneq H$.

22. Show that any subgroup of order p^{n-1} in a group G of order p^n is normal in G.

Harder Problems

23. Let G be a group, H a subgroup of G. Define for $a, b \in G$, $a \sim b$ if $b = h^{-1}ah$ for some $h \in H$. Prove that

(a) this defines an equivalence relation on G.

(b) If $[a]$ is the equivalence class of a, show that if G is a finite group, then $[a]$ has m elements where m is the index of $H \cap C(a)$ in H.

24. If G is a group, H a subgroup of G, define a relation $B \sim A$ for subgroups A, B of G by the condition that $B = h^{-1}Ah$ for some $h \in H$.

(a) Prove that this defines an equivalence relation on the set of subgroups of G.

(b) If G is finite, show that the number of distinct subgroups equivalent to A equals the index of $N(A) \cap H$ in H.

25. If P is a p-Sylow subgroup of G, let S be the set of all p-Sylow subgroups of G. For $Q_1, Q_2 \in S$ define $Q_1 \sim Q_2$ if $Q_2 = a^{-1}Q_1a$ with $a \in P$. Prove, using this relation, that if $Q \neq P$, then the number of distinct $a^{-1}Qa$, with $a \in P$, is a multiple of p.

26. Using the result of Problem 25, show that the number of p-Sylow subgroups of G is of the form $1 + kp$. (This is the third part of Sylow's Theorem.)

27. Let P be a p-Sylow subgroup of G, and Q another one. Suppose that $Q \neq x^{-1}Px$ for any $x \in G$. Let S be the set of all $y^{-1}Qy$, as y runs over G. For $Q_1, Q_2 \in S$ define $Q_1 \sim Q_2$ if $Q_2 = a^{-1}Q_1a$, where $a \in P$.

(a) Show that this implies that the number of distinct $y^{-1}Qy$ is a multiple of p.

(b) Using the result of Problem 14, show that the result of Part (a) cannot hold.

(c) Prove from this that given any two p-Sylow subgroups P and Q of G, then $Q = x^{-1}Px$ for some $x \in G$.
(This is the second part of Sylow's Theorem.)

28. If H is a subgroup of G of order p^m show that H is contained in some p-Sylow subgroup of G.

29. If P is a p-Sylow subgroup of G and $a, b \in Z(P)$ are conjugate in G, prove that they are already conjugate in $N(P)$.