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 $N \triangleleft G$. Let the set $HN = \{hn \mid h \in H, n \in N\}$. Prove that:

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

(b) HN is a subgroup of G.

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

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

***6.** If G is a group and $N \triangleleft G$, 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 $N \triangleleft G$, show that $\varphi(N) \triangleleft G'$.

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 $s, f(s), f^2(s), \dots, f^{p-1}(s)$; 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 $a_1 a_2 \cdots a_{p-1} a_p = e$. 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 $a_p = (a_1 a_2 \cdots a_{p-1})^{-1}$, the p-tuple $(a_1, a_2, \ldots, a_{p-1}, a_p)$ then satisfies

$$a_1 a_2 \cdots a_{p-1} a_p = a_1 a_2 \cdots a_{p-1}(a_1 a_2 \cdots a_{p-1})^{-1} = e,$$

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

Note that if $a_1 a_2 \cdots a_{p-1} a_p = e$, then $a_p a_1 a_2 \cdots a_{p-1} = e$ (for if $xy = e$ in a group, then $yx = e$). So the mapping $f: S \rightarrow S$ 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 $A \triangleleft G$.

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 $A \triangleleft G$. □

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 $ab = ba$, $e = (ab)^i = a^ib^i$; 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 $e = c^0, c, c^2, \dots, c^{14}$ 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 $s = (a_1, a_2, \dots, a_p)$ 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 $\pi_i\colon \overline{G}_i \to G_i$ 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 $N_1, \mathrm{N}_2, \ldots, N_n$, 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 $\psi(a_1, a_2) = a_1a_2$, is an isomorphism if and only if $N_1N_2 = G$ 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 $G = N_1N_2 \cdots N_k$ 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. $G = N_1N_2 \cdots N_k$.
2. For each i, $N_i \cap (N_1N_2 \cdots N_{i-1}N_{i+1} \cdots N_k) = (e)$.

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 $n_1 \geq n_i$, $p^{n_i} \mid p^{n_1}$, 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