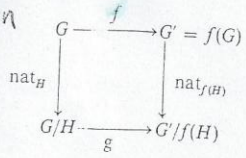
Abstract And Linear Algebra

David M. Burton

(641)



2–7 DIRECT PRODUCTS OF GROUPS

In this section, we pay special attention to finite groups: one of the richest and deepest branches of the whole of group theory. For no other general class of groups is the structure as completely known or as easily described. When one is setting up a structure theory, the overall strategy is to express—in some sense—the complicated algebraic systems in terms of those which are better behaved. We accomplish this in the present setting by introducing the concept of a direct product of groups. Our main theorem will then be to the effect that any finite commutative group can be split into the direct product of cyclic groups.

Let us begin by recalling that if H and K are subgroups of the group G, then the set HK consists of all products hk, with $h \in H$ and $k \in K$. While HK is not necessarily a subgroup of G, taking H and K to be normal in G is more than enough to assure that this will indeed be the case (Problem 13, Section 2–4). We are particularly interested in those situations in which HK is the entire group G. The significance of this assumption is that it enables us to write every member of G as a product of elements of H and K. If it also happens that H and K intersect *trivially* (in other words, $H \cap K = \{e\}$), then one speaks of G as being expressed as an internal direct product of these subgroups. To put the matter on a formal basis:

Definition 2–30 Let H and K be normal subgroups of the group G. Then G is said to be the *internal direct product* of H and K, written $G = H \otimes K$, if $G = HK$ and $H \cap K = \{e\}$.

Before attempting to set out the theory of direct products in an orderly fashion, let us look at two examples.

Example 2–57 Consider the Klein 4-group $K_4 = \{e, a, b, ab\}$, where $a^2 = b^2 = e$ and $ab = ba$. Since K_4 is commutative, all its subgroups are normal. If H is the cyclic subgroup generated by the element a and K is the cyclic subgroup generated by b, then the conditions of Definition 2–30 are satisfied. Thus $K_4 = H \otimes K$ is the internal direct product of two cyclic subgroups of order 2.

Example 2–58 Some groups cannot be expressed as the internal direct product of two nontrivial normal subgroups (technically speaking, such groups are referred

to as *indecomposable*). As an example of this situation, we mention any infir cyclic group $G = (a)$. For suppose that $G = H \otimes K$, where H, K are nontriv subgroups of G. Being subgroups of a cyclic group, H and K are themselves cy with, say, generators a^n and a^m, respectively. Then the product $a^{nm} \in H \cap$ showing that $H \cap K \neq \{e\}$, a contradiction to the definition of direct product (i equality $a^{nm} = e$ is impossible, for this would imply that G is finite).

There exist several criteria for a group to be an internal direct product of subgroups. We establish one such condition below.

Theorem 2–66 The group G is the internal direct product of its subgroups and K if and only if

1) each element $x \in G$ can be uniquely expressed in the form $x = hk$, whe $h \in H$ and $k \in K$; and

2) any element of H commutes with any element of K.

Proof. As our starting point, suppose that $G = H \otimes K$. Since $G = HK$, a element x of G has the form $x = hk$, with $h \in H$ and $k \in K$. To see that this repr sentation is uniquely determined by x, let $x = h_1k_1$ for $h_1 \in H$, $k_1 \in K$. Then hk h_1k_1 or rather $h_1^{-1}h = k_1k^{-1}$. Because $h_1^{-1}h \in H$ and $k_1k^{-1} \in K$, each side of th last equation is simultaneously in H and K. From the definition of direct produc $H \cap K = \{e\}$ and so $h_1^{-1}h = e = k_1k^{-1}$. Thus $h = h_1$ and $k = k_1$, proving (1 Now let $h \in H$ and $k \in K$ be arbitrarily given and consider the commutator $hkh^{-1}k^{-}$ Knowing that K is a normal subgroup of G, we necessarily have $hkh^{-1} \in K$, henc $(hkh^{-1})k^{-1} \in K$; similarly, the normality of H forces $h(kh^{-1}k^{-1}) \in H$. This puts th commutator $hkh^{-1}k^{-1}$ in $H \cap K = \{e\}$. As a result, $hkh^{-1}k^{-1} = e$, which leac to the required commutativity $hk = kh$.

For the other direction of the theorem, we assume that the indicated condition hold and prove that $G = H \otimes K$. It follows immediately from (1) that $G = HK$ Pick any $h \in H$ and $x \in G$. Then $x = h_1k_1$ for some choice of $h_1 \in H$, $k_1 \in K$ Observe that

$$xhx^{-1} = (h_1k_1)h(h_1k_1)^{-1} = h_1hh_1^{-1} \in H,$$

since the elements of H and K commute by (2). Thus the product xhx^{-1} belongs tc H, in consequence of which H is normal in G. For reasons entirely similar to thos just given, K is a normal subgroup of G. To complete the proof, we must show that $H \cap K = \{e\}$. Suppose that H and K have the element x in common; then x will have two representations as a member of HK:

$$x = xe \quad (x \in H, e \in K) \qquad \text{and} \qquad x = ex \quad (e \in H, x \in K).$$

The uniqueness of representation guaranteed by condition (1) would be violatec unless $x = e$. Accordingly, $H \cap K = \{e\}$, and Theorem 2–66 is finished.

to as *indecomposable*). As an example of this situation, we mention any infir cyclic group $G = (a)$. For suppose that $G = H \otimes K$, where H, K are nontriv subgroups of G. Being subgroups of a cyclic group, H and K are themselves cy with, say, generators a^n and a^m, respectively. Then the product $a^{nm} \in H \cap$ showing that $H \cap K \neq \{e\}$, a contradiction to the definition of direct product (i equality $a^{nm} = e$ is impossible, for this would imply that G is finite).

There exist several criteria for a group to be an internal direct product of subgroups. We establish one such condition below.

Theorem 2–66 The group G is the internal direct product of its subgroups and K if and only if

1) each element $x \in G$ can be uniquely expressed in the form $x = hk$, whe $h \in H$ and $k \in K$; and

2) any element of H commutes with any element of K.

Proof. As our starting point, suppose that $G = H \otimes K$. Since $G = HK$, a element x of G has the form $x = hk$, with $h \in H$ and $k \in K$. To see that this repr sentation is uniquely determined by x, let $x = h_1k_1$ for $h_1 \in H$, $k_1 \in K$. Then hk h_1k_1 or rather $h_1^{-1}h = k_1k^{-1}$. Because $h_1^{-1}h \in H$ and $k_1k^{-1} \in K$, each side of th last equation is simultaneously in H and K. From the definition of direct produc $H \cap K = \{e\}$ and so $h_1^{-1}h = e = k_1k^{-1}$. Thus $h = h_1$ and $k = k_1$, proving (1 Now let $h \in H$ and $k \in K$ be arbitrarily given and consider the commutator $hkh^{-1}k^{-}$ Knowing that K is a normal subgroup of G, we necessarily have $hkh^{-1} \in K$, henc $(hkh^{-1})k^{-1} \in K$; similarly, the normality of H forces $h(kh^{-1}k^{-1}) \in H$. This puts th commutator $hkh^{-1}k^{-1}$ in $H \cap K = \{e\}$. As a result, $hkh^{-1}k^{-1} = e$, which leac to the required commutativity $hk = kh$.

For the other direction of the theorem, we assume that the indicated condition hold and prove that $G = H \otimes K$. It follows immediately from (1) that $G = HK$ Pick any $h \in H$ and $x \in G$. Then $x = h_1k_1$ for some choice of $h_1 \in H$, $k_1 \in K$ Observe that

$$xhx^{-1} = (h_1k_1)h(h_1k_1)^{-1} = h_1hh_1^{-1} \in H,$$

since the elements of H and K commute by (2). Thus the product xhx^{-1} belongs tc H, in consequence of which H is normal in G. For reasons entirely similar to thos just given, K is a normal subgroup of G. To complete the proof, we must show that $H \cap K = \{e\}$. Suppose that H and K have the element x in common; then x will have two representations as a member of HK:

$$x = xe \quad (x \in H, e \in K) \qquad \text{and} \qquad x = ex \quad (e \in H, x \in K).$$

The uniqueness of representation guaranteed by condition (1) would be violatec unless $x = e$. Accordingly, $H \cap K = \{e\}$, and Theorem 2–66 is finished.

The next theorem exhibits the interplay between the notions of internal direct product and quotient group.

Theorem 2–67 If H and K are normal subgroups of the group G such that $G = H \otimes K$, then $G/H \simeq K$ and $G/K \simeq H$.

Proof. Consider the mapping $f: G \to K$ defined as follows: If $x = hk$, with $h \in H$ and $k \in K$, then $f(x) = k$. It is to be noted that the uniqueness of this representation for x assures that f is well defined. We also see at once that f carries G onto K. Given two elements $x = hk$ and $y = h_1k_1$ of G, the product

$$xy = (hk)(h_1k_1) = (hh_1)(kk_1),$$

where the last equality makes use of (2) of Theorem 2–66. This entails that $f(xy) = kk_1 = f(x)f(y)$, which shows the mapping in question to be a homomorphism. Finally we have,

$$\begin{aligned} \ker f &= \{hk \in HK | f(hk) = e\} \\ &= \{hk \in HK | k = e\} = H. \end{aligned}$$

The Fundamental Homomorphism Theorem now enables us to assert that $G/H \simeq K$. In the same way, the function g defined by $g(x) = g(hk) = h$ gives rise to the isomorphism $G/K \simeq H$.

An immediate consequence is

Corollary If G is a finite group and if $G = H \otimes K$, then $o(G) = o(H)o(K)$.

Proof. By Lagrange's Theorem, the order of G is the product of the order of H and the index of H in G. The foregoing result shows that $[G:H] = o(K)$, so all is proved.

A quicker, but more sophisticated, route to Theorem 2–67 is via the Second Isomorphism Theorem; indeed, if $G = H \otimes K$, then

$$G/H = HK/H \simeq K/H \cap K = K/\{e\} = K.$$

Similarly, the quotient group $G/K \simeq H$.

If G is a finite group, the definition of internal direct product may be restated as the criterion of our next theorem. This result requires a "counting" lemma which is of interest in its own right.

Lemma If H and K are finite subgroups of the group G, then

$$o(HK) = \frac{o(H)o(K)}{o(H \cap K)}.$$

Proof. That the set HK contains at most $o(H)o(K)$ elements is clear from its definition. The problem is that there may be some duplication; to put the matter more precisely, it is entirely possible that a given element $hk \in HK$ might equal h_1k_1

for $h_1 \in H, k_1 \in K$, where $h_1 \neq h$ or $k_1 \neq k$. The idea is to show that this takes place as many times as there are elements in $H \cap K$.

Suppose that $x \in H \cap K$ and $hk \in HK$. We may then write $hk = (hx)(x^{-1}k)$, where hx belongs to H (since $x \in H$) and $x^{-1}k$ belongs to K (since $x \in K$). Thus the element hk is duplicated in HK at least $o(H \cap K)$ times. On the other hand, every duplication of hk arises in the manner just described. For if $hk = h_1k_1$, then $x = h^{-1}h_1 = kk_1^{-1}$ lies in $H \cap K$; hence $h_1 = hx, k_1 = x^{-1}k$, and so $hk = (hx)(x^{-1}k)$. The implication is that hk appears in HK exactly $o(H \cap K)$ times. The number of distinct elements in HK is $o(H)o(K)$ divided by the number of times each element appears, namely $o(H \cap K)$.

Theorem 2–68 Let H and K be normal subgroups of the finite group G with $o(G) = o(H)o(K)$. If either $G = HK$ or $H \cap K = \{e\}$, then $G = H \otimes K$.

Proof. If $G = HK$, then the foregoing lemma implies that

$$o(G) = o(HK) = \frac{o(H)o(K)}{o(H \cap K)}$$

or rather, $o(H \cap K)o(G) = o(H)o(K)$. But we are assuming that $o(G) = o(H)o(K)$. Hence $o(H \cap K) = 1$ and so $H \cap K = \{e\}$. This fact, together with $G = HK$, yields $G = H \otimes K$.

In the event that $H \cap K = \{e\}$, then the following equalities are obvious:

$$o(HK) = \frac{o(H)o(K)}{o(H \cap K)} = o(H)o(K) = o(G).$$

Since $HK \subseteq G$ with $o(HK) = o(G)$, one concludes that $HK = G$ and, again, $G = H \otimes K$.

To see how all this works in a specific instance, let us write the group Z_{10} as a direct product of subgroups. This particular group contains only two nontrivial (normal) subgroups, namely, $H = \{0, 5\}$ and $K = \{0, 2, 4, 6, 8\}$. Evidently $o(Z_{10}) = 10 = 2 \cdot 5 = o(H)o(K)$. Since $H \cap K = \{0\}$, it follows from Theorem 2–68 that Z_{10} is decomposable into the internal direct product of H and K. A quick check reveals that the elements of Z_{10} can be represented as

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

where the right-hand sides are all in HK.

Thus far we have restricted our attention to the internal direct product of two subgroups. The definition lends itself to the following generalization:

Definition 2–31 A group G is said to be the *internal direct product* of the normal subgroups $H_1, H_2, \ldots, H_n$, indicated by writing $G = H_1 \otimes H_2 \otimes \cdots \otimes H_n$, if

1) $G = H_1 H_2 \cdots H_n$; that is, every element $x \in G$ is a product $x = h_1 h_2 \cdots h_n$, with $h_i \in H_i$, and
2) $H_i \cap H_i' = \{e\}$, where $H_i' = H_1 \cdots H_{i-1} H_{i+1} \cdots H_n$, for each i.

In the interests of completeness, we record the analog of Theorem 2–66; its proof is left as an exercise.

Theorem 2–69 The group G is the internal direct product of the subgroups $H_1, H_2, \ldots, H_n$ if and only if

1) every element $x \in G$ is uniquely expressible in the form $x = h_1 h_2 \cdots h_n$, with $h_i \in H_i$;
2) $h_i \in H_i$ and $h_j \in H_j$ $(i \neq j)$ imply $h_i h_j = h_j h_i$.

We digress a little to consider the following question: Given two groups G_1 and G_2, is there a group G which is the internal direct product of subgroups H and K isomorphic to G_1 and G_2? For an answer, take G to be the Cartesian product

$$G_1 \times G_2 = \{(a, b) | a \in G_1, b \in G_2\}.$$

We endow $G_1 \times G_2$ with the structure of a group by defining multiplication of elements componentwise; that is,

$$(a, b)(a', b') = (aa', bb'),$$

aa' being the product in G_1 and bb' that in G_2. The reader is left the straightforward verification that, in this way, $G_1 \times G_2$ really can be made into a group. This new group is called the *external direct product* of G_1 and G_2 and is denoted by $G_1 \times G_2$, the same notation as that used for the Cartesian product. (Since $G_1 \times G_2$ and $G_2 \times G_1$ are isomorphic as groups, we may speak of the direct product of two groups without specifying the order of the factors.) One finds that the identity element of $G_1 \times G_2$ is just (e_1, e_2), where e_i is the identity of G_i, and that the inverse of (a, b) is (a^{-1}, b^{-1}).

Next observe that $G_1 \times G_2$ contains normal subgroups which are isomorphic copies of G_1 and G_2, namely the subgroups $H = G_1 \times \{e_2\}$ and $K = \{e_1\} \times G_2$. The only element of $G_1 \times G_2$ simultaneously of the forms (a, e_2) and (e_1, b) is the identity (e_1, e_2), whence H and K must intersect in the identity element. Furthermore, a typical member (a, b) of $G_1 \times G_2$ can be expressed as

$$(a, b) = (a, e_2)(e_1, b) \in HK,$$

which signifies that $G_1 \times G_2 = HK$. These remarks make it plain that $G_1 \times G_2$ is the internal direct product of its subgroups H and K:

$$G_1 \times G_2 = H \otimes K \qquad \text{with } G_1 \simeq H, \quad G_2 \simeq K.$$

For a somewhat different approach to the subject, we now start with a group G which is decomposable into the internal direct product of two normal subgroups H and K; in symbols, $G = H \otimes K$. Construct the external direct product $H \times K$ of the groups H and K. Since $G = HK$, every element $x \in G$ is uniquely expressible in the form $x = hk$ with $h \in H$, $k \in K$. It is therefore possible to define a function $f: G \to H \times K$ by setting

$$f(x) = f(hk) = (h, k).$$

Our purpose is to show that f is an isomorphism of G onto $H \times K$, so that $G \simeq H \times K$.

Pursuing this aim, let $x = hk$ and $y = h'k'$ be any two members of G. In compliance with Theorem 2–66, the elements of H commute with those of K and so $xy = (hk)(h'k') = (hh')(kk')$. This means that

$$f(xy) = (hh', kk') = (h, k)(h', k') = f(x)f(y),$$

confirming that f is a homomorphism. It is equally clear that $f(G) = H \times K$.

To verify that f is a one-to-one mapping, suppose that $x = hk$ belongs to the kernel of f. Then

$$f(x) = f(hk) = (h, k) = (e, e).$$

The criterion for equality of ordered pairs forces $h = k = e$, whence $x = e$. Accordingly, $\ker f = \{e\}$ and, as a result, f is one-to-one.

Altogether, we have proved the following theorem.

Theorem 2–70 Let G be a group with normal subgroups H and K such that $G = H \otimes K$. Then $G \simeq H \times K$.

The notion of external direct product can easily be broadened to allow for three or more factors. Let $G_1, G_2, \ldots, G_n$ be a finite collection of groups (not necessarily distinct) and consider their Cartesian product

$$G = G_1 \times \cdots \times G_n = \{(a_1, \ldots, a_n) | a_i \in G_i\}.$$

Multiplication is defined in G by

$$(a_1, \ldots, a_n)(b_1, \ldots, b_n) = (a_1 b_1, \ldots, a_n b_n),$$

where $a_i b_i$ denotes the product in G_i. Under this binary operation G is a group, known as the external direct product of the set $\{G_i\}$. As before, G contains subgroups H_i which are isomorphic to G_i for $i = 1, 2, \ldots, n$ and such that the group $G = H_1 \otimes \cdots \otimes H_n$. We need only take H_i to be the set of elements of G having

(6)

all components equal to the identity save for the ith; in other words, if e_i denotes the identity of G_i, let

$$H_i = \{(e_1, \ldots, e_{i-1}, a, e_{i+1}, \ldots, e_n) | a \in G_i\}.$$

To summarize, the external direct product G of the groups G_i $(i = 1, 2, \ldots, n)$ is also the internal direct product of the subgroups H_i, where for each i, $G_i \simeq H_i$. If one agrees to identify groups which are isomorphic, then the distinction between external and internal direct products disappears. In the future, we shall use the term *direct product* (without the qualifying adjective) for both, leaving the context to clarify which one is meant.

Let us take advantage of these ideas to obtain a direct-product decomposition of the group Z_n of integers modulo n. First, a collateral result:

Lemma If gcd $(m, n) = 1$, then $Z_{mn} \simeq Z_m \times Z_n$.

Proof. In the group Z_{mn}, the integer n generates a cyclic subgroup

$$H = \{0, n, 2n, \ldots, (m-1)n\}$$

of order m. Likewise, the integer m in Z_{mn} generates a cyclic subgroup

$$K = \{0, m, 2m, \ldots, (n-1)m\},$$

having order n. Clearly, $o(Z_{mn}) = mn = o(H)o(K)$. If the integer $a \in H \cap K$, then $m|a$ and $n|a$. But m and n are relatively prime, hence $mn|a$, and consequently $a = 0$; viewed otherwise, $H \cap K = \{0\}$. An appeal to Theorem 2–68 being legitimate, we see in this way that

$$Z_{mn} = H \otimes K.$$

Theorem 2–57 now tells us that $H \simeq Z_m$ and $K \simeq Z_n$, from which the stated result is apparent. (Indeed, the reader will experience no difficulty in showing that if f and g are isomorphisms from H onto Z_m and K onto Z_n, respectively, then $H \otimes K \simeq Z_m \times Z_n$ via the mapping F, where $F(hk) = (f(h), g(k))$.)

This enables us to prove the following.

Theorem 2–71 If the integer $n > 1$ has the prime factorization $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ (distinct primes), then

$$Z_n \simeq Z_{n_1} \times Z_{n_2} \times \cdots \times Z_{n_r}$$

where $n_i = p_i^{k_i}$ for $i = 1, 2, \ldots, r$.

Proof. The assertion is trivial when $r = 1$. In general, we argue by induction on r, the number of distinct primes appearing in the prime factorization of n. Let $r > 1$ and assume that the theorem is true for all integers containing $r - 1$ distinct primes. From this, we wish to prove that the result holds for $n = p_1^{k_1} \cdots p_{r-1}^{k_{r-1}} p_r^{k_r}$. Now n

(7)

all components equal to the identity save for the ith; in other words, if e_i denotes the identity of G_i, let

$$Z_n \simeq Z_{m_1} \times Z_{m_2}.$$

Our induction hypothesis states that

$$Z_{m_1} \simeq Z_{n_1} \times Z_{n_2} \times \cdots \times Z_{n_{r-1}}.$$

When we set $n_r = m_2$, the result is

$$Z_n \simeq Z_{n_1} \times Z_{n_2} \times \cdots \times Z_{n_r},$$

where the integers $n_i = p_i^{k_i}$ for every $i = 1, 2, \ldots, r$.

The task that lies ahead is to generalize this theorem from Z_n to arbitrary finite commutative groups. That is, we intend to prove that any commutative group of order $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ splits into a direct product of r cyclic subgroups of orders $p_1^{k_1}, p_2^{k_2}, \ldots, p_r^{k_r}$. As a step toward this goal, it is expedient to introduce a new class of groups, the p-groups. These groups are not only essential to the whole theory of this section, but become all the more so in the next section when we develop the Sylow theorems.

Definition 2–32 Let p be a prime number. A group G is said to be a *p-group* if the order of each element of G is some power of p (not necessarily the same power).

Example 2–59 The group G_s of symmetries of the square is a p-group, with $p = 2$. For each of its elements has order 2, save for r_1 and r_3, which have order 4.

Example 2–60 If p is a prime, then Z_{p^n} is a p-group for any $n > 0$. This follows directly from Lagrange's theorem: Every element of Z_{p^n} must have order dividing p^n, the order of the group; hence every element has order a power of p.

Example 2–61 Let G be a commutative group. For a fixed prime p, define

$$G_p = \{a \in G | o(a) = p^n \text{ for some } n\}.$$

Our assertion is that G_p forms a subgroup of G which, by its nature, is automatically a p-group. We establish that G_p is a subgroup by applying the usual subgroup criterion (quite possibly, $G_p = \{e\}$). Suppose then that a, b are elements of G_p with respective orders p^r and p^s. Since G is commutative,

$$(ab^{-1})^{p^{r+s}} = (a^{p^r})^{p^s}(b^{p^s})^{-p^r} = e.$$

Taking Theorem 2–33 into account, we infer that the order of ab^{-1} divides p^{r+s} and therefore will be a power of p. This puts ab^{-1} into G_p, which is the desired conclusion.

We should point out that this result is false for noncommutative groups: for

instance, in the symmetric group S_3, the elements having order some power of 2 do not comprise a group.

The only additional remark called for here is that G_p is the largest (in the sense of inclusion) p-subgroup of G. Indeed, if H is an arbitrary p-subgroup, then every element of H has order a power of p, hence by the definition of G_p, each element of H must lie in G_p; that is to say, $H \subseteq G_p$.

In the course of the next section, we shall characterize finite p-groups as those groups having p-power order. It will be convenient to pause and derive the commutative case now. For this, a brief lemma is needed.

Lemma Let H be a normal subgroup of the group G. If G is a p-group, then both H and G/H are p-groups.

Proof. The assertion is obvious for H, even without the normality requirement. That the quotient group G/H forms a p-group follows directly from the fact that $o(aH)$ divides $o(a)$ for all $a \in G$.

Theorem 2–72 A finite commutative group G is a p-group if and only if $o(G)$ is a power of p.

Proof. From Lagrange's theorem, it is clear that any group of order p^n is a p-group. Concentrating on the less obvious direction of the theorem, let G be a p-group. We prove that G has p-power order by using induction on $o(G)$. That is, we assume this to be true for all finite commutative p-groups of orders less than that of G. The stated result is obvious for groups of order 1, which starts the inductive process. Let $o(G) > 1$. If G has no nontrivial subgroups, then G is cyclic and any generator is an element of p-power order; hence, G will have order a power of p. On the other hand, when G contains a nontrivial subgroup H, then both $o(H)$ and $o(G/H)$ are strictly less than $o(G)$. Apply the induction assumption (as one may by the previous lemma) to conclude that H and G/H each have p-power order. Since

$$o(G) = o(H)o(G/H),$$

it follows that the order of G is necessarily a power of p, and the proof is completed.

With the needed preliminaries out of the way, we are now ready to deal with the central topic of the present section, to wit, the description of all finite commutative groups. The first step in this program ties the structure of such groups to that of p-groups.

Theorem 2–73 Any finite commutative group $G \neq \{e\}$ is the direct product of p-groups.

Proof. Let $o(G) = n$. We claim that if $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ is the prime factorization of n, then G is the direct product of the subgroups G_{p_i} for $i = 1, 2, \ldots, r$ (notation

Proof (Z3) Any finite comgroup G is the direct product of p-groups

$\because |G| = n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$

① $G = G_{p_1} \times G_{p_2} \times \cdots \times G_{p_r}$

② $|G_{p_i}| = p_i^{k_i}$, $i = 1, \ldots, r$ cor

$|G| = 2^4 \cdot 3^6 \cdot 11^2$
$= G_2 \times G_3 \times G_{11}$

Proof :- ① To proof $G = G_{p_1} \times G_{p_2} \times \cdots \times G_{p_n}$ we have to show

(i) $G_{p_i} \triangleleft G$: G is com. $\cdots G_{p_i} < G \Rightarrow G_{p_i} \triangleleft G$

(ii) $G = G_{p_1} G_{p_2} \cdots G_{p_r}$

(iii) $G_{p_i} \cap (G_{p_1} G_{p_2} \cdots G_{p_{i-1}} G_{p_{i+1}} \cdots G_{p_r}) = e$

power of $\neq$ prime
$2^3 = 8 \neq$

$|G_2| = 2^4$
$|G_3| = 3^6$
$|G_{11}| = 11^2$
$G = H \times K$

(ii) $G = G_{p_1} G_{p_2} \cdots G_{p_r}$

we have to show that $a \in G$, $a = a_1 a_2 \cdots a_r$: $a_i \in G_{p_i}$??

Let $a \in G$ s.t $O(a) = p^n \Rightarrow a^m = e$ (3)

by lagrange $m \mid n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$

$\Rightarrow m = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}$ $0 \le n_i \le k_r$ (4)

Put $m_i = \frac{m}{p_i^{n_i}}$ (5) Then clearly, are relatively primes

$1 = abc$
$a \in G_2$
$b \in G_3$
$c \in G_{11}$
$m \mid 2^4 \cdot 3^6 \cdot 11^2$
$m = 2^3 \cdot 3^4 \cdot 11$
$m_1 = \frac{2^3 \cdot 3^4 \cdot 11}{2^3} = 3^4 \cdot 11$
$m_2 = \frac{2^3 \cdot 3^4 \cdot 11}{3^4} = 2^3 \cdot 11$
$m_3 = 2^3 \cdot 3^4$
$(m_1, m_2, m_3) = 1$ نسبياً

$(m_1, m_2, \ldots, m_r) = 1 \Rightarrow \exists$ integers u_i s.t

$u_1 m_1 + u_2 m_2 + \cdots + u_r m_r = 1$

$a \Rightarrow a^{u_1 m_1 + u_2 m_2 + \cdots + u_r m_r} = a^1 \Rightarrow a^{u_1 m_1} a^{u_2 m_2} \cdots a^{u_r m_r} = a$

set $a_1 = a^{u_1 m_1}$, $a_2 = a^{u_2 m_2}$ (6) $a_i = a^{u_i m_i}$

$a = a_1 a_2 a_3 \cdots a_r$

It remains to show that $a_i = a^{u_i m_i} \in G_{p_i}$??

$O(a_i)$ is power of p_i , i.e $O(a_i) = p_i^{\square}$??, $a_i^{p^{\square}} = e$??

consider $a_i^{p_i^{n_i}} = (a^{u_i m_i})^{p_i^{n_i}}$ (5) $= a^{u_i m \cdot p_i^{n_i}}$ $= a^{u_i m} = (a^m)^{u_i}$ (3) $= e$

$\Rightarrow O(a_i) \mid p_i^{n_i} \Rightarrow O(a_i)$ is some power of p_i

$\Rightarrow a_i \in G_{p_i}$

theorm 73 إكمال البرهان

(iii) $G_{p_i} \cap (G_1 G_2 \cdots G_{p_{i-1}} G_{p_{i+1}} \cdots G_{p_r}) = e$

let $a \in G_{p_i} \cap (G_{p_1} G_{p_2} \cdots G_{p_{i-1}} G_{p_{i+1}} \cdots G_{p_r})$ $(j = 1, 2, \ldots, i-1, i+1, \ldots r)$

$\Rightarrow a \in G_{p_i}$ and $a = b_1 b_2 \cdots b_{i-1} b_{i+1} \cdots b_r$ $b_j \in G_{p_j}$

$\Rightarrow O(a) = p_i^s$ (say) (7) and $O(b_1) = p_1^{t_1}$, $O(b_2) = p_2^{t_2}$, ... $O(b_j) = p_j^{t_j}$

$\Rightarrow a^{p_i^s} = e$ (8)

$b_1^{p^{t}} = e$, $b_2^{p^{t_2}} = e$, ... $b_j^{p^{t_j}} = e$

Take $t = p_1^{t_1} p_2^{t_2} \cdots p_{i-1}^{t_{i-1}} p_{i+1}^{t_{i+1}} \cdots p_r^{t_r}$ clearly t $\Rightarrow a^t = e$ (9)

(8)

from (7), (a) :- $a^{p_i^s} = e$, $a^t = e$

$(p_i^s, t) = 1 \Rightarrow \exists$ integers u, v

$u p_i^s + t v = 1$

$\xrightarrow{a}$ $a^{u p_i^s + t v} = a^1$

$\Rightarrow a^{u p_i^s} \cdot a^{tv} = a$

$\Rightarrow a = (a^{p_i^s})^u \cdot (a^t)^v \overset{7.9}{=} e.e = e$

(2) $|G_{p_i}| = p_i^{k_i}$ $i = 1, \ldots, r$

$\because G_{p_1}, G_{p_2}, \ldots, G_{p_r}$ are p-groups

Then by therom 72,

$|G_{p_1}| = p_1^{n_1}$, $|G_{p_2}| = p_2^{n_2}$.

But $|G| = |G_{p_1}| \cdot |G_{p_2}| \cdots |G_{p_r}|$

given $n = p_1^{n_1} \cdot p_2^{n_2} \cdots p_r^{n_r}$

$p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}$

للتوضيح

$b_1 \quad b_2$

$a = b_1 b_2$ (?)

$O(b_1) = 2^4$, $O(b_2) = 5^6$

$t = 2^4 \cdot 5^6$

$a^t = (b_1 b_2)^t = (b_1 b_2)^{2^4 \cdot 5^6}$

$= b_1^{2^4 \cdot 5^6} \cdot b_2^{2^4 \cdot 5^6} = (b_1^{2^4})^{5^6}$.

$(b_2^{5^6})^{2^4} = e.e = e$

$G = 2^4 \cdot 5^6 \cdot 11^2$

$|G|_p = G_2 \, G_5 \, G_{11}$

$|G_2| = 2^j$

$|G_5| = 5^j$

$|G_{11}| = 11^j$

from the uniquenes of the prime factorization

then $k_1 = n_1$, $k_2 = n_2$, ----, $n_r = k_r$

i.e $|G_{p_1}| = p_1^{k_1}$ $|G_{p_2}| = p_2^{k_2}$, $|G_{p_i}| = p_i^{k_i}$

as in Example 2–61). To support this contention, let us apply the criterion of Definition 2–31. First, it is necessary to show that an arbitrary element $a \in G$ can be represented in the form $a = a_1 a_2 \cdots a_r$, where $a_i \in G_{p_i}$. If a has order m, then the corollary to Theorem 2–40 asserts that $m|n$; hence $m = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}$ for certain integers n_i $(0 \leqslant n_i \leqslant k_i)$. Put $m_i = m/p_i^{n_i}$. The m_i are relatively prime and so, with reference to Problem 22, Section 1–3, there exist integers u_i for which the sum $u_1 m_1 + u_2 m_2 + \cdots + u_r m_r = 1$. Then

$$a = a^{u_1 m_1 + \cdots + u_r m_r} = a^{u_1 m_1} a^{u_2 m_2} \cdots a^{u_r m_r}.$$

Setting $a_i = a^{u_i m_i}$ for $i = 1, 2, \ldots, r$, it follows that $a = a_1 a_2 \cdots a_r$, and if $v_i = p_i^{n_i}$, then

$$a_i^{v_i} = (a^{u_i m_i})^{v_i} = a^{u_i m} = (a^m)^{u_i} = e^{u_i} = e.$$

Being of p_i-power order, the element a_i necessarily lies in G_{p_i}. All in all, we have shown that

$$G = G_{p_1} G_{p_2} \cdots G_{p_r}.$$

The proof will be finished as soon as we can establish that each G_{p_i} has trivial intersection with the product of the remaining ones. To see that this is so, choose any element

$$a \in G_{p_i} \cap (G_{p_1} \cdots G_{p_{i-1}} G_{p_{i+1}} \cdots G_{p_r}).$$

On the one hand, $a^{p_i^s} = e$ for some integer s. On the other hand, a can be expressed as a product $a = b_1 \cdots b_{i-1} b_{i+1} \cdots b_r$ where the order of b_j is a power of p_j; say, to be definite, that by raising b_j to the $p_j^{t_j}$th power one can produce the identity. Letting $t = p_1^{t_1} \cdots p_r^{t_r}$, we can get $a^t = e$. Furthermore, p_i^s and t are relatively prime, so that $up_i^s + vt = 1$ for appropriate integers u and v. This forces

$$a = a^{up_i^s + vt} = (a^{p_i^s})^u (a^t)^v = e$$

which proves what we wanted.

We can recast Theorem 2–73 in a form which gives more precise information:

Corollary If the commutative group $G \neq \{e\}$ has order $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ (distinct primes) and if $G_{p_i} = \{x \in G | o(x) \text{ is a power of } p_i\}$, then

$$G = G_{p_1} \otimes G_{p_2} \otimes \cdots \otimes G_{p_r}$$

where $o(G_{p_i}) = p_i^{k_i}$ for every i.

Proof. Only the last statement needs further justification. By Theorem 2–72, $o(G_{p_i}) = p_i^{j_i}$ for some nonnegative integer j_i. Since the order of the direct product of a finite number of subgroups is the product of their respective orders, we obtain

$$\begin{aligned} p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} &= o(G) = o(G_{p_1}) o(G_{p_2}) \cdots o(G_{p_r}) \\ &= p_1^{j_1} p_2^{j_2} \cdots p_r^{j_r}. \end{aligned}$$

(10)

The uniqueness of the prime factorization of $o(G)$ then implies that $j_i = k_i$ for every $i = 1, 2, \ldots, r$; hence $o(G_{p_i}) = p_i^{k_i}$, as asserted.

The preceding proof establishes that a finite commutative group G is the direct product of its subgroups G_p for all primes p such that $G_p \neq \{e\}$; which is simply to say, for all primes p dividing $o(G)$. This reduces the study of arbitrary finite commutative groups to the study of finite commutative p-groups. The basic result on p-groups from which the whole structure theory can be pinned down is derived below.

Theorem 2–74 A finite commutative p-group G is the direct product of a finite number of cyclic p-subgroups.

Proof. It is already known that $o(G) = p^n$ for some $n \geqslant 0$. Our method is to perform induction on n. The starting point is the case where $n = 1$, the theorem being trivial when $n = 0$; here there is really nothing to prove, for G is cyclic of order p. Next, suppose that $n > 1$ and that the result in question holds for all groups of order p^m with $m < n$.

Since G is a p-group, the order of every element of G is necessarily a power of p. Let $a \in G$ be an element of maximal order, say $o(a) = p^k$ $(k \leqslant n)$, and consider the cyclic subgroup $H = (a)$ generated by a. If $k = n$, then $H = G$, so that G itself is cyclic; in such an event the theorem is trivial. Thus we may assume that $k < n$. The implication is that the quotient group G/H will have order $p^{n-k} < o(G)$. By the hypothesis of our induction, G/H is the direct product

$$G/H = \overline{H}_1 \otimes \overline{H}_2 \otimes \cdots \otimes \overline{H}_r$$

of cyclic p-subgroups $\overline{H}_i$ $(i = 1, 2, \ldots, r)$.

Let these subgroups $\overline{H}_i$ be generated by the cosets b_iH and let their respective orders be p^{j_i}. The next step is to produce a representative c_i of b_iH such that the order of c_i in G is equal to the order of b_iH in G/H. As a temporary device, let us write b for b_i and j for j_i. Since $(bH)^{p^j} = H$, the element b^{p^j} lies in H, hence is some power of a, say $b^{p^j} = a^s$. By the maximal nature of k, $o(b) \leqslant p^k$, so that $b^{p^k} = e$; as a result

$$e = b^{p^k} = (b^{p^j})^{p^{k-j}} = (a^s)^{p^{k-j}} = a^{sp^{k-j}}.$$

This reveals that $p^k | sp^{k-j}$. Thus there exists an element t with $tp^k = sp^{k-j}$, leading to $tp^j = s$. If we now set $c = ba^{-t}$, then $cb^{-1} \in H$ and

$$c^{p^j} = (ba^{-t})^{p^j} = b^{p^j}a^{-tp^j} = a^s a^{-s} = e.$$

Restoring the index i, the situation stands as follows: For each i $(i = 1, 2, \ldots, r)$, there is an element $c_i \in G$ and an integer $v_i = p^{j_i}$ with the properties

1) $c_iH = b_iH$ and
2) $c_i^{v_i} = e$.

The 74 :— A finite comp. group is the direct product of finite number of cyclic p-subgroups $G_{p_1} \otimes G_{p_2} \otimes \cdots \otimes G_{p_r}$ (1)

proof :—

$\because G$ is a p-group $\Rightarrow |G| = p^n$ for some $n \neq 0$

we are going to prove this theorem by induction on $n \neq 0$

(1) For $n = 1 \Rightarrow |G| = p \Rightarrow G$ is cyclic it is true.

(2) Suppose the theorem is hold for all subgroup of order $m < p^n$, $m < n$.

$\because G$ is a p-group $\Rightarrow \exists\ a \in G : o(a) =$ Some power of p.

let $a \in G$ be a maximal order say $o(a) = p^k$, $k \leq n$ $\quad a^k = e$ (4)

consider the cyclic subgroup generated by the element $a \in G$.

$H = \langle a \rangle = \{e, a, a^2, a^3, \ldots, a^p\} \leq G$ (2)

i.e. $|H| = |\langle a \rangle| = p^k$

case1 :- $k = n \Rightarrow o(a) = p^n = |\langle a \rangle| = |H| = |G|$

$\Rightarrow G = \langle a \rangle$ is a cyclic group.

case2 :- $k < n \Rightarrow H = \langle a \rangle$ is a proper subgroup of G which is normal. consider the quotient group G/H.

Then G/H is a commutitive p-subgroup of G of order

$$|G||H| = \frac{p^n}{p^k} = p^{n-k} < |G| = p^n \quad (3)$$

by induction the theorem is hold for G/H.

$$G/H = \bar{H}_1 \otimes \bar{H}_2 \otimes \cdots \otimes \bar{H}_r \quad (4)$$

where $\bar{H}_i = \frac{H_i}{H}$, $H_i < G$.

and $\bar{H}_i$ is cyclic p-subgroups (5)

let $\bar{H}_1 = \langle b_1 H \rangle, \bar{H}_2 = \langle b_2 H \rangle \cdots \bar{H}_r = \langle b_r H \rangle$

and $|\bar{H}_1| = p^{j_1}, |\bar{H}_2| = p^{j_2}, \ldots |\bar{H}_r| = p^{j_r}$ (6)

The next step is to produce representative c_i of $b_i H$ such that order of c_i in $G = o(b_i H)$ in G/H

~~let $\bar{a} \in G/H$ s.t $\bar{a} = 3 + \langle 6 \rangle$~~

$\mathbb{Z}_{18} = \{\bar{0}, \bar{1}, \ldots, \overline{17}\}$

$H = \langle 6 \rangle = \{0, 6, 12\}$

$G/H = \mathbb{Z}_{18}/\langle 6 \rangle =$

$\{\langle 6 \rangle, 1 + \langle 6 \rangle,$

$2 + \langle 6 \rangle, 3 + \langle 6 \rangle,$

$4 + \langle 6 \rangle, 5 + \langle 6 \rangle\}$

let $\bar{a} \in G/H$

s.t

$\bar{a} = 3 + \langle 6 \rangle$

$\bar{a} = 3 + H = \{3, 9, 15\}$

$|\bar{a}| = 3, o(a)$ in

$G/H = ??$

$(3+H) + (3+H)$

$= 6 + H = H$

$o(3 + \langle 6 \rangle) = ??$

$(3 + \langle 6 \rangle) + (3 + \langle 6 \rangle)$

$= 6 + \langle 6 \rangle = \langle 6 \rangle$

$o(3 + \langle 6 \rangle) = 2$

in G/H

Notic that

$c_i = q \in \bar{a}$

s.t $o(q) = 2$

in $\mathbb{Z}_{18}$.

$a + q \sim_{\mathbb{Z}_{18}} 3$

$|G| = 2^{10}$

$o(a) = 2, 2^2, \ldots$

$H = \langle a \rangle \leq G$

$H = G \quad H \leq G$

We contend that if K is the subgroup generated by $c_1, c_2, \ldots, c_r$, then $G = H \otimes K$. Starting with an arbitrary $x \in G$, we can write the coset $xH \in G/H$ as

$$xH = (b_1H)^{n_1}(b_2H)^{n_2} \cdots (b_rH)^{n_r}$$

for suitable integers n_i. Since $b_iH = c_iH$ for $i = 1, 2, \ldots, r$, we obtain

$$xH = (c_1H)^{n_1}(c_2H)^{n_2} \cdots (c_rH)^{n_r}.$$

This is scarcely more than a statement that

$$x = c_1^{n_1}c_2^{n_2} \cdots c_r^{n_r}y$$

for some choice of y in H. In consequence, the element $x \in HK$, thereby confirming that $G = HK$.

There remains the verification that $H \cap K = \{e\}$. Pick a typical element x in $H \cap K$. Because $x \in K$, there exist integers m_i for which

$$x = c_1^{m_1}c_2^{m_2} \cdots c_r^{m_r}$$

and so, passing to the quotient group G/H,

$$xH = (c_1H)^{m_1}(c_2H)^{m_2} \cdots (c_rH)^{m_r}.$$

When we use the fact that $c_iH = b_iH$ (as well as the assumption that $x \in H$), this equation translates into

$$H = (b_1H)^{m_1}(b_2H)^{m_2} \cdots (b_rH)^{m_r}.$$

Since G/H is the direct product of the cyclic subgroups $\overline{H}_i$ with generators b_iH, the uniqueness of representation of an element implies that each factor on the right-hand side must equal the identity of G/H; that is, $(b_iH)^{m_i} = H$ for $i = 1, 2, \ldots, r$. The conclusion to be drawn is that p^{j_i}, the order of the coset b_iH, divides m_i. But this in its turn yields $c_i^{m_i} = e$ (recall that c_i raised to the p^{j_i}th power gives the identity), hence our expression for x reduces to $x = e$.

Having exhibited that $G = H \otimes K$, our proof proceeds rapidly to its conclusion. For the induction assumption tells us that K admits a direct product decomposition into cyclic p-subgroups. Inasmuch as H is itself cyclic, the net result is that G is expressible as a direct product of cyclic p-subgroups. This is the contention of the theorem.

Before we go further, it is worth remarking that a given finite commutative p-group G can usually be written as a direct product of cyclic subgroups in several ways. However, the number of subgroups and their orders are the same in all such representations; more precisely, if

$$G = (a_1) \otimes \cdots \otimes (a_n) = (b_1) \otimes \cdots \otimes (b_m),$$

then $n = m$ and, after renumbering, $o(a_i) = o(b_i)$. This implies that the decomposition of G is unique up to isomorphism of the factors.

Theorems 2–73 and 2–74 may be brought together to give a complete description of the groups under consideration. Without delay, we present what is sometimes called the Fundamental Theorem for Finite Commutative Groups:

Theorem 2–75 (*Frobenius*) Every finite commutative group is the direct product of finitely many cyclic p-subgroups.

Switching to external direct products, and using the fact that any cyclic group of order k is isomorphic to Z_k, one could just as well express Theorem 2–75 as follows:

Corollary 1 If G is a finite commutative group, then

$$G \simeq Z_{p_1^{n_1}} \times Z_{p_2^{n_2}} \times \cdots \times Z_{p_r^{n_r}}$$

for suitable primes p_i, not necessarily distinct, and integers $n_i \in Z_+$.

So far, we have learned that any finite commutative group is a direct product of cyclic groups, each of which is a p-group. There can be no further factorization, since a finite cyclic group, say $G = (a)$, of p-power order is indecomposable. To clarify this point, let $o(G) = p^n, n \geqslant 1$, and suppose, in anticipation of contradiction, that G has the (nontrivial) representation $G = H \otimes K$. Then $o(H) = p^j$ and $o(K) = p^k$, where $j + k = n (1 \leqslant j, k < n)$. If m is the larger of j and k, then certainly $m < n$. Writing the generator a as $a = hk$, with $h \in H$ and $k \in K$, it follows that

$$a^{p^m} = (hk)^{p^m} = h^{p^m} k^{p^m} = e.$$

This being so, $o(G) \leqslant p^m$, which is absurd. These considerations allow us to rephrase Theorem 2–75 in the following form, which we state as a corollary:

Corollary 2 Any finite commutative group is the direct product of a finite number of indecomposable cyclic groups.

We are now in a position to identify, up to isomorphism, all possible commutative groups of a given order. By Frobenius' theorem, any finite commutative group G is the direct product of prime-power order cyclic groups. Thus, it will be sufficient to consider the case wherein $o(G) = p^n$, p a prime. In terms of external direct products, Theorem 2–75 may be viewed as asserting that

$$G \simeq Z_{p^{n_1}} \times Z_{p^{n_2}} \times \cdots \times Z_{p^{n_r}}.$$

Since the order of G is the product of the orders of these $Z_{p^{n_i}}$, it follows that $p^n = p^{n_1 + n_2 + \cdots + n_r}$, or rather, $n = n_1 + n_2 + \cdots + n_r$.

For any positive integer n, a summation $n = n_1 + n_2 + \cdots + n_r$, where $0 < n_i \leqslant n_j$ for $i < j$, is called a *partition* of n. The remarks of the last paragraph indicate that each commutative group of order p^n gives rise to a partition of n. From the opposite point of view, starting with a partition $n = n_1 + \cdots + n_r$, we can always produce a commutative group G of order p^n; simply take G to be the external

direct product of $Z_{p^{n_1}}, \ldots, Z_{p^{n_r}}$. In brief, there are just as many nonisomorphic commutative groups of order p^n as there are ways to express n as a sum of positive integers. There are, to cite an example, only two commutative groups of order p^2, either Z_{p^2} or $Z_p \times Z_p$. These groups are not isomorphic, for Z_{p^2} contains an element of order p^2, but every element of $Z_p \times Z_p$ other than the identity has order p.

In general, the number of nonisomorphic commutative groups of order $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$ (distinct primes) is $\pi(k_1)\pi(k_2)\cdots\pi(k_r)$, where $\pi(k_i)$ denotes the number of partitions of the integer k_i. As a typical illustration, there are three commutative groups of order $24 = 2^3 \cdot 3$; specifically,

$$Z_8 \times Z_3 \simeq Z_{24},$$

and

$$Z_4 \times Z_2 \times Z_3 \simeq Z_{12} \times Z_2,$$

$$Z_2 \times Z_2 \times Z_2 \times Z_3 \simeq K_4 \times Z_6.$$

There are other theorems which give insight into the structure of finite commutative groups. A second basic result states that any finite commutative group G is isomorphic to a direct product

$$Z_{n_1} \times Z_{n_2} \times \cdots \times Z_{n_r}$$

where $n_i | n_{i+1}$ for $1 \leqslant i \leqslant r - 1$. To arrive at this, all one need do is to write G as a direct product of cyclic groups of prime power order and assemble the latter judiciously; the formal proof is left as an exercise. Suppose, for example, that a group G of order 360 has the direct product decomposition

$$G \simeq Z_2 \times Z_2 \times Z_2 \times Z_3 \times Z_3 \times Z_5.$$

Rearranging factors, we can put this in the form

$$G \simeq Z_2 \times (Z_2 \times Z_3) \times (Z_2 \times Z_3 \times Z_5) \simeq Z_2 \times Z_6 \times Z_{30},$$

with $2|6$ and $6|30$.

Our final theorem provides an application of the results of this section.

Theorem 2–76 If $n > 1$ is a square-free integer (that is, n is not divisible by the square of any prime), then any commutative group of order n is isomorphic to the group Z_n.

Proof. Since n is a square-free integer, we have $o(G) = n = p_1 p_2 \cdots p_r$, where the p_i are distinct primes. Now the corollary to Theorem 2–73 asserts that

$$G = G_{p_1} \otimes G_{p_2} \otimes \cdots \otimes G_{p_r}$$

with $o(G_{p_i}) = p_i$; hence $G_{p_i} \simeq Z_{p_i}$. This implies that

$$G \simeq Z_{p_1} \times Z_{p_2} \times \cdots \times Z_{p_r} \simeq Z_{p_1 p_2 \cdots p_r} = Z_n,$$

the second isomorphism being achieved by use of Theorem 2–71.

Corollary If n is a square-free integer, then all commutative groups of order n are isomorphic.

PROBLEMS

1. Establish the following assertions:
   a) The group Z_{15} is the internal direct product of $\{0, 5, 10\}$ and $\{0, 3, 6, 9, 12\}$.
   b) The group G_s of symmetries of the square is indecomposable.
   c) The additive groups Z and Q are both indecomposable.
2. Let $G = H \otimes K$ for subgroups H and K of the group G. Given that N is a normal subgroup of G, prove that either $N \subseteq \text{cent } G$ or N has nontrivial intersection with one of H or K.
3. Assume that H and K are normal subgroups of the finite group G. If $o(G) = o(H)o(K)$, where $o(H)$ and $o(K)$ are relatively prime, prove that $G = H \otimes K$.
4. Show that the symmetric group S_3 is indecomposable by proving that any direct product of subgroups of orders 2 and 3 must be cyclic.
5. Let the group $G = H_1 \otimes H_2 \otimes \cdots \otimes H_n$ for subgroups H_i. Consider the representation $a = a_1 a_2 \cdots a_n$, where $a_i \in H_i$, of an element $a \in G$. If the mappings $\pi_i : G \to H_i$ are defined by $\pi_i(a) = a_i$ for $i = 1, 2, \ldots, n$, verify that:
   a) π_i is a homomorphism from G onto H_i, called the ith *projection*.
   b) A mapping $f : G' \to G$ from an arbitrary group G' into G is a homomorphism if and only if the composition $\pi_i \circ f : G' \to H_i$ is a homomorphism for each value of i.
6. Suppose that $f : G \to G'$ is a homomorphism from the group G onto the group G' and that H is a normal subgroup of G. If the restriction $f|H$ is an isomorphism from H onto G', prove that $G = H \otimes \ker f$.
7. Let H and K be normal subgroups of the group G. Verify that if the natural mapping $\text{nat}_K : G \to G/K$ induces an isomorphism of H onto G/K, then $G = H \otimes K$. [*Hint:* See Problem 6.]
8. Assuming that $G = H \otimes K$ for subgroups H and K of the group G, prove that:
   a) Any normal subgroup of H (or K) is also a normal subgroup of G.
   b) If N is a normal subgroup of H, then $G/N \simeq (H/N) \times K$.
9. Given that G_i $(i = 1, 2, 3)$ are groups, establish the following facts concerning (external) direct products:
   a) $G_1 \times G_2 \simeq G_2 \times G_1$
   b) $(G_1 \times G_2) \times G_3 \simeq G_1 \times (G_2 \times G_3)$
   c) If $G_1 \simeq G_2$, then $G_1 \times G_3 \simeq G_2 \times G_3$.
   d) $G_1 \times G_2$ is a commutative group if and only if G_1 and G_2 are both commutative.
10. Show that if G_1 and G_2 are finite groups and the element $(a, b) \in G_1 \times G_2$, then $o((a, b)) = \text{lcm } (o(a), o(b))$.

11. Prove the following:
    a) The Klein 4-group K_4 is isomorphic to $Z_2 \times Z_2$.
    b) Z_{n^2} is not isomorphic to $Z_n \times Z_n$ for any integer $n > 1$. [*Hint:* Z_{n^2} has only one subgroup of order n, but $Z_n \times Z_n$ has two such subgroups.]

12. Given that $G = G_1 \times G_2 \times \cdots \times G_n$, where the G_i are groups, verify that:
    a) cent G = cent $G_1 \times$ cent $G_2 \times \cdots \times$ cent G_n.
    b) $[G, G] = [G_1, G_1] \times [G_2, G_2] \times \cdots \times [G_n, G_n]$.

13. Let H_i be normal subgroups of the groups G_i $(i = 1, 2)$. Prove that $H_1 \times H_2$ is a normal subgroup of $G_1 \times G_2$ and that

$$(G_1 \times G_2)/(H_1 \times H_2) \simeq G_1/H_1 \times G_2/H_2.$$

14. Show that if H and K are normal subgroups of the group G, with $H \cap K = \{e\}$, then G is isomorphic to a subgroup of $G/H \times G/K$. [*Hint:* Use the mapping $f: G \to G/H \times G/K$ defined by $f(x) = (xH, xK)$.]

15. Show by example that the direct product of cyclic groups (p-groups) need not be a cyclic group (p-group).

16. Verify the following statements:
    a) Any homomorphic image of a p-group is again a p-group.
    b) A finite commutative p-group is generated by its elements of highest order.
    c) If G is a cyclic p-group, then G is a finite p-group.

17. Let G and G' be finite commutative groups. Prove that:
    a) If $f: G \to G'$ is a homomorphism, then $f(G_p) \subseteq G'_p$.
    b) $G \simeq G'$ if and only if $G_p \simeq G'_p$ for all primes p.

18. Given that G is a finite cyclic group, prove that, for every prime p dividing $o(G)$, there are exactly $p - 1$ elements in G having order p. [*Hint:* If $p | o(G)$, then $G_p \simeq Z_{p^n}$ for some $n \in Z_+$.]

19. Show that a finite commutative group $G \neq \{e\}$ is cyclic if and only if

$$G \simeq Z_{n_1} \times Z_{n_2} \times \cdots \times Z_{n_r}$$

where $n_i = p_i^{k_i}$ for $i = 1, 2, \ldots, r$ (p_i distinct primes, $k_i \in Z_+$).

20. Show that there are three nonisomorphic commutative groups of order 8; namely, Z_8, $Z_4 \times Z_2$, and $K_4 \times Z_2$.

21. Determine, up to isomorphism, all commutative groups of the following orders: p^4 (p a prime), 144, and 360.

22. Prove that a cyclic group G is indecomposable if and only if G is either infinite or of prime power order.

23. Characterize those positive integers n for which the only commutative groups of order n are cyclic.

24. Prove that if G is a finite commutative group, then

$$G \simeq Z_{n_1} \times Z_{n_2} \times \cdots \times Z_{n_r},$$

where $n_i | n_{i+1}$ for $1 \leqslant i \leqslant r-1$.

2–8 THE SYLOW THEOREMS

Given a group G of order n, and an integer m dividing n, one cannot always be certain that G will possess a subgroup of order m. To be sure, under special circumstances (for example, in a finite cyclic group) it is true that such subgroups always do exist. In general, the problem of finding subgroups of a prescribed order in an arbitrary finite group is one of considerable difficulty and constitutes the subject matter of this, our final section on group theory. The main object of study are the theorems in the title of this section, the Sylow theorems. Broadly speaking, these provide information about the existence and number of subgroups of prime-power order.

We begin with a survey of facts, some previously encountered in the exercises, arranged rather haphazardly around the notion of conjugacy. Despite the familiarity of the ground covered, the relevant definitions and results are collected here for the reader's convenience.

Starting with any subgroup H of the group G and an arbitrary element $a \in G$, consider the following subset of G:

$$aHa^{-1} = \{aha^{-1} | h \in H\}.$$

If x and y are members of aHa^{-1}, then there exist certain $h_1, h_2 \in H$ for which $x = ah_1a^{-1}$ and $y = ah_2a^{-1}$. Thus

$$xy^{-1} = (ah_1a^{-1})(ah_2a^{-1})^{-1} = a(h_1h_2^{-1})a^{-1},$$

where, since H is a subgroup of G, the product $h_1h_2^{-1}$ lies in H. But this means that $xy^{-1} \in aHa^{-1}$, so that aHa^{-1} is itself a subgroup of G. We are therefore led to the theorem below.

Theorem 2–77 If H is a subgroup of the group G and if $a \in G$, then aHa^{-1} is also a subgroup of G, called the *conjugate subgroup of H induced by the element a.*

Not all the subgroups conjugate to H are necessarily distinct from H or, for that matter, distinct from each other. If $aHa^{-1} = H$ for some $a \in G$, we say that the subgroup H is *self-conjugate under a.* Any subgroup is, for example, self-conjugate under each one of its own elements. In terms of this definition, the concept of a normal subgroup can be arrived at in an alternative way: The subgroup H is normal in G if and only if H is self-conjugate under every element of G.

Another point of interest is that the conjugate subgroups of H are all isomorphic to H, hence isomorphic to each other. Given a conjugate aHa^{-1} of H, define the mapping $f: H \to aHa^{-1}$ by taking $f(h) = aha^{-1}$; there is no particular trouble in