This supplement is meant to provide a proof of the structure theorem for finite abelian groups employing only elementary concepts of group theory. Another proof will be provided later in the course using the structure theorem for finitely generated modules over principal ideal domains.

Direct Products

Definition 1. The *direct product* $G_1 \times G_2 \times \cdots \times G_n$ of groups G_1, G_2, ..., G_n is the set of n-tuples $(g_1, g_2, \ldots, g_n)$ where $g_i \in G_i$ with the group operation defined componentwise:

$$(g_1, g_2, \ldots, g_n)(h_1, h_2, \ldots, h_n) = (g_1h_1, g_2h_2, \ldots, g_nh_n).$$

The group operation in the above definition is written multiplicatively, but in concrete situations, whatever is the natural group operation on the G_i will be followed. In particular, abelian groups will generally be written with the group operation $+$.

Example 2.

1. Suppose $G_i = \mathbb{R}$ for $1 \leq i \leq n$. Then $\mathbb{R} \times \mathbb{R} \times \cdots \times \mathbb{R}$ (n-factors) is the ordinary Euclidean n-space $\mathbb{R}^n$ with the usual vector addition:

$$(a_1, a_2, \ldots, a_n) + (b_1, b_2, \ldots, {}_n) = (a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n).$$

2. Let $G_1 = \mathbb{R}$ and $G_2 = \mathbb{R}^*$ where the group operation in G_1 is addition and the group operation in the second group is multiplication. Then the group operation on $G_1 \times G_2$ is

$$(a, b)(c, d) = (a + c, bd).$$

3. For an even more general example of a product with different operations on each factor, let $G_1 = \mathbb{Z}$, $G_2 = S_3$, and $G_3 = \mathrm{GL}_2(\mathbb{R})$. Then the operation on $G_1 \times G_2 \times G_3$ is given by

$$(n, \alpha, \begin{bmatrix} a & b \\ c & d \end{bmatrix})(m, \beta, \begin{bmatrix} p & q \\ r & s \end{bmatrix}) = (n + m, \alpha\beta, \begin{bmatrix} ap + br & aq + bs \\ cp + dr & cq + ds \end{bmatrix}).$$

4. Do not confuse a group whose elements happen to be represented as ordered n-tuples of elements of groups G_i with the direct product $G_1 \times G_2 \times \cdots \times G_n$. As a concrete example, let $G = \{(a, b) : a \in \mathbb{R}^*, b \in \mathbb{R}\}$ where the group operation is given by

$$(a, b)(c, d) = (ac, ad + b).$$

As a set $G = \mathbb{R}^* \times \mathbb{R}$, but the group operation on G is not that of the direct product $\mathbb{R}^* \times \mathbb{R}$ group, which has the group operation

$$(a, b)(c, d) = (ac, b + d).$$

Proposition 3. *If G_1, G_2, ..., G_n are groups, their direct product G is a group of order $|G_1|\,|G_2| \cdots |G_n|$. This means that if any G_i is infinite, then so is G.*

Proof. The verification of the group axioms is straightforward from the componentwise definition of the group operation on G. We note that the identity of G is $e_G = (e_{G_1}, e_{G_2}, \ldots, e_{G_n})$, which we will, of course, continue to denote by e, and the inverse of $(g_1, g_2, \ldots, g_n)$ is $(g_1^{-1}, g_2^{-1}, \ldots, g_n^{-1})$.

The formula for the order of G is clear. □

Let $G = G_1 \times G_2 \times \cdots G_n$ and for $1 \leq i \leq n$ define homomorphisms $\pi_i : G \to G_i$ and $\mu_i : G_i \to G$ by

$$\pi_i(g_1, g_2, \ldots, g_n) = g_i \quad \text{and} \quad \mu_i(g) = (e, \ldots, e, g, e, \ldots, e),$$

where the g appears in the i^{th} component. Note the following facts:

- The image of μ_i, $\text{Im}(\mu_i)$, is a subgroup of G isomorphic to G_i. Moreover, $\mu_i \lhd G$. Thus, the direct product G contains a normal subgroup $\widetilde{G}_i = \text{Im}(\mu_i)$ isomorphic to G_i.
- Using the notation in the previous part, if $x \in \widetilde{G}_i$, $y \in \widetilde{G}_j$ for $i \neq j$, then $xy = yx$.
- The homomorphism π_i is surjective, and the kernel of π_i is the subgroup of G consisting of all n-tuples with e in the i^{th} position:

$$\text{Ker}(\pi_i) = \{(g_1, \ldots, g_{i-1}, e, g_{i+1}, \ldots, g_n) : g_j \in G_j, j \neq i\}.$$

- For each i, $\pi_i \circ \mu_i = 1_{G_i}$, where $1_{G_i} : G_i \to G_i$ is the identity homomorphism ($1_{G_i}(g) = g$ for all $g \in G_i$).

Proposition 4. *If $G = G_1 \times G_2 \times \cdots G_n$ and $g = (g_1, g_2, \ldots, g_n)$, then the order of g is*

$$o(g) = \text{lcm}\{o(g_1), o(g_2), \ldots, o(g_n)\}.$$

Proof. For all $k \in \mathbb{Z}$,

$$g^k = (g_1^k, g_2^k, \ldots, g_n^k),$$

so that $g^k = e \in G$ if and only if $g_i^k = e \in G_i$ for all i. Thus, $g^k = e$ if and only if k is a multiple of $o(g_i)$ for all i. Since the order of g is the smallest positive k such that $g^k = e$, it follows that we are looking for the smallest positive k such that k is a multiple of $o(g_i)$ for all i. Thus,

$$o(g) = \text{lcm}\{o(g_1), o(g_2), \ldots, o(g_n)\},$$

as required. □

Proposition 5. *Let m, $n \in \mathbb{N}$.*

1. *$\mathbb{Z}_m \times \mathbb{Z}_m \cong \mathbb{Z}_{mn}$ if and only if $\gcd(m, n) = 1$.*
2. *If $n = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$ is the prime factorization of n, then*

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{r_1}} \times \mathbb{Z}_{p_2^{r_2}} \times \cdots \times \mathbb{Z}_{p_k^{r_k}}.$$

Proof. Since part 2 follows immediately from part 1 by induction on k, it is only necessary to prove part 1. Let $\mathbb{Z}_m = \langle a \rangle$ and $\mathbb{Z}_n = \langle b \rangle$ where $o(a) = m$ and $o(b) = n$. Let $l = \text{lcm}\{m, n\}$. Since m and n are assumed to be relatively prime, it follows that $l = mn$. By Proposition 4 it follows that $o(a, b) = \text{lcm}\{o(a), o(b)\} = mn$. Since $|\mathbb{Z}_m \times \mathbb{Z}_n| = mn$ we conclude that $\mathbb{Z}_m \times \mathbb{Z}_n = \langle (a, b) \rangle$ so that $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic of order mn, which is what we wanted to prove. □

Example 6. 1. Let p be a prime and let $n \in \mathbb{N}$. Define a group E_{p^n} by

$$E_{p^n} = \mathbb{Z}_p \times \mathbb{Z}_p \times \cdots \mathbb{Z}_p \quad (n \text{ factors}).$$

The group E_{p^n} is an abelian group of order p^n with the property that every nonidentity element has order p. Since $\mathbb{Z}_p$ and hence E_{p^n} is written additively, what this means is that for every $x \in E_{p^n}$, $px = 0$. Such a group is said to be an *elementary abelian p-group.*

2. For p a prime, we claim that the elementary abelian group $E = E_{p^2} = \mathbb{Z}_p \times \mathbb{Z}_p$ of order p^2 has exactly $p+1$ subgroups of order p. Note that this means that there are more than the two obvious ones coming from the two coordinate copies of $\mathbb{Z}_p$. Since each nonidentity element of E has order p, each of these nonidentity elements generates a cyclic subgroup of order p. By Lagrange's theorem, distinct subgroups of order p intersect only in the identity. Thus, the $p^2 - 1$ nonidentity elements of E are partitioned into subsets of size $p-1$, where each subset consists of the nonidentity elements of some subgroup of order p. Thus, there must be

$$\frac{p^2-1}{p-1} = p+1$$

subgroups of order p. If $p = 2$ then the 3 subgroups of $\mathbb{Z}_2 \times \mathbb{Z}_2$ of order 2 are:

$$\begin{aligned} \langle (1,0) \rangle &= \{(0,0),\, (1,0)\}\,, \\ \langle (0,1) \rangle &= \{(0,0),\, (0,1)\}\,, \text{ and} \\ \langle (1,1) \rangle &= \{(0,0),\, (1,1)\}\,. \end{aligned}$$

If $p = 3$ then the 4 subgroups of $\mathbb{Z}_3 \times \mathbb{Z}_3$ of order 3 are:

$$\begin{aligned} \langle (1,0) \rangle &= \{(0,0),\, (1,0),\, (2,0)\}\,, \\ \langle (0,1) \rangle &= \{(0,0),\, (0,1),\, (0,2)\}\,, \\ \langle (1,1) \rangle &= \{(0,0),\, (1,1),\, (2,2)\}\,, \text{ and} \\ \langle (2,1) \rangle &= \{(0,0),\, (2,1),\, (1,2)\}\,. \end{aligned}$$

We now consider how to recognize if a group G can be written as a direct product of subgroups. The main result is the following *recognition theorem.*

Theorem 7. *Suppose that G is a group with subgroups H and K such that*

1. *H and K are normal in G,*
2. *$H \cap K = \langle e \rangle$, and*
3. *$G = HK = \{hk : h \in H, k \in K\}$.*

Then $G \cong H \times K$.

Proof. First note that hypotheses 1 and 2 imply that $hk = kh$ for all $h \in H$ and $k \in K$. To see this, consider the element $c = hkh^{-1}k^{-1}$. Since K is normal, $hkh^{-1} \in K$ so that $c = (hkh^{-1})k^{-1} \in K$. But since H is normal, $kh^{-1}k^{-1} \in H$ so that $c = h(kh^{-1}k^{-1}) \in H$. Hence $c \in H \cap K = \langle e \rangle$ so $hkh^{-1}k^{-1} = e$, i.e, $hk = kh$. Thus every element of h commutes with every element of k. Define a function $\varphi : H \times K \to G$ by

$$\varphi((h,\, k)) = hk.$$

Since

$$\varphi((h,\, k)(h',\, k')) = \varphi((hh',\, kk')) = hh'kk' = hkh'k' = \varphi((h,\, k))\varphi((h',\, k')),$$

it follows that φ is a group homomorphism. (Note that the third equality used the fact that $h'k = kh'$.) By assumption 3, φ is surjective. Suppose that $\varphi((h,\, k)) = e$. Thus assume that $hk = e$. Then $h = k^{-1}$ so that $h \in H \cap K = \langle e \rangle$. Hence $h = e$ and also $k = e$ so that $\mathrm{Ker}(\varphi) = \langle e \rangle$. Thus, we have shown that φ is an isomorphism. □

Definition 8. When a group G has subgroups H and K satisfying the conditions of Theorem 7, then we say that G is the *internal direct product* of H and K. When emphasis is called for, we will say that $H \times K$ is the *external direct product*.

Theorem 7 can be extended by induction to any number of subgroups of G. The proof of the following such extension is left as an exercise.

Theorem 9. *Suppose that G is a group with subgroups G_i $(1 \leq i \leq n)$ such that*

1. *G_i is normal in G for all i,*
2. *$G_i \cap (G_1 \cdots G_{i-1} G_{i+1} \cdots G_n) = \langle e \rangle$, and*
3. *$G = G_1 G_2 \cdots G_n = \{g_1 g_2 \cdots g_n : g_i \in G_i \text{ for all } i\}$.*

Then $G \cong G_1 \times G_2 \times \cdots \times G_n$.

Proof. Exercise. □

Finite Abelian Groups

Our goal is to prove that every finite abelian group can be written as a direct product of cyclic subgroups, and that certain uniqueness properties of this decomposition are valid. We start with the following lemma.

Lemma 10. *Let G be a finite abelian group of order m. If p is a prime that divides m, then G has an element of order p.*

Proof. Write $m = pn$. The proof is by induction on n. If $n = 1$ then $|G| = p$ and G is cyclic of prime order p. In this case any nonidentity element of G has order p. Now suppose that $n > 1$ and that any abelian group G' with $|G'| = pn'$ for $n' < n$ has an element of order p. Let H be a maximal subgroup of G. If p divides $|H|$, then H (and hence G) has an element of order p by the induction hypothesis. If p does not divide $|H|$, we proceed as follows. Since G is abelian, H is a normal subgroup of G and we can form the quotient group G/H. Let $\pi : G \to G/H$ be the projection map $(\pi(a) = a + H)$. If $\overline{K}$ is a proper subgroup of G/H, then $\pi^{-1}(\overline{K})$ is a subgroup of G properly between G and H. Since H is assumed to be maximal, this is not possible. Hence G/H must be a cyclic group of prime order. Since $|G/H| = |G| \,/\, |H|$ and since p does not divide the order of $|H|$, but it does divide $|G|$, it follows that $|G/H| = p$. Thus, there is a $y \in G$ such that $\langle y + H \rangle = G/H$. This means that if $\overline{\pi} = \pi|_{\langle y \rangle}$ then $\mathrm{Im}(\overline{\pi}) = G/H$ and $\mathrm{Ker}(\overline{\pi}) = \langle y \rangle \cap H$. Hence $p = |G/H| = [\langle y \rangle : H \cap \langle y \rangle]$ divides $|\langle y \rangle|$, and then an application of the fundamental theorem on finite cyclic groups shows that the cyclic group $\langle y \rangle$ has an element of order p . □

If G is a group and p is a prime, we will let G_p denote the subset of G consisting of all elements whose order is a power of p.

Proposition 11. *If G is an abelian group and p is a prime, then G_p is a subgroup of G.*

Proof. Since the group G is abelian, we will use additive notation for the group operation. Then, the order of $a \in G$ is the smallest positive m such that $ma = 0$, so that

$$G_p = \{a \in G : p^r a = 0 \text{ for some } r \geq 0\}.$$

Thus, if a, $b \in G_p$, then $p^r a = 0$ and $p^s b = 0$ so that, if t is the larger of r and s, $p^t(a - b) = p^t a - p^t b = 0$. Hence $a - b \in G_p$, so G_p is a subgroup. □

Remark 12. The above result is not true if G is not abelian. For example, if $G = S_3$, then $G_2 = \{(1), (1, 2), (1, 3), (2, 3)\}$, which is not a subgroup of S_3.

A group G is a *p-group*, where p is a prime, if every element of G has order a power of p. By Lemma 10, an abelian group is a p-group if and only if $|G| = p^k$ for some k. Our first decomposition theorem is that every finite abelian group can be decomposed as a direct product of p-groups, where the primes p are those that divide $|G|$.

Theorem 13. *Let G be a finite abelian group and let $m = |G| = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$, where p_1, p_2, …, p_k are the distinct primes that divide m. Then*

$$G \cong G_{p_1} \times G_{p_2} \times \cdots \times G_{p_k}.$$

Proof. First note that Lemma 10 implies that $G_{p_j} \neq \langle 0 \rangle$ for each j. Now, define a homomorphism

$$\varphi : G_{p_1} \times G_{p_2} \times \cdots \times G_{p_k} \to G$$

by $\varphi(a_1, a_2, \ldots, a_k) = a_1 + a_2 + \cdots + a_k$. It is clear that φ is a group homomorphism. Our proof will be completed by showing that φ is both injective and surjective.

Injective. Suppose that $a = (a_1, a_2, \ldots, a_k) \in \mathrm{Ker}(\varphi)$. Then $a_1 + a_2 + \cdots a_k = 0$ so that

$$a_1 = -(a_2 + \cdots + a_k). \tag{1}$$

Since $a_j \in G_{p_j}$, we have that $p_j^{t_j} a_j = 0$ for some $t_j > 0$. If $n = p_2^{t_2} \cdots p_k^{t_k}$, then $na_j = 0$ for $2 \leq j \leq k$ and Equation (1) shows that $na_1 = 0$ so that the order of a_1 divides n, the order of a_1 is also a power $p_1^{t_1}$, and since n and p_1 are relatively prime, this means that $t_1 = 0$. Hence $a_1 = 0$. The same argument works to show that $a_j = 0$ for all j, so that $a = 0$ and φ is injective.

Surjective. Let $m_i = m/p_i^{r_i}$ for $1 \leq i \leq k$. Then m_1, m_2, …, m_k are relatively prime integers, and hence we can find integers v_1, v_2, …, v_k such that $1 = m_1 v_1 + m_2 v_2 + \cdots + m_k v_k$. If $a \in G$, multiply this equation by a to get

$$a = m_1 v_1 a + m_2 v_2 a + \cdots + m_k v_k a = a_1 + a_2 + \cdots + a_k,$$

where $a_i = m_i v_i a$. Since $p_i^{r_i} m_i = m = |G|$ it follows that $p_i^{r_i} a_i = m v_i a = 0$ so $a_i \in G_{p_i}$. Hence $a = \varphi(a_1, a_2, \ldots, a_k)$ so that φ is surjective. □

Our next step is to show that any finite abelian p-group can be decomposed as a direct product of cyclic groups. According to Theorem 13, it is sufficient to show that any abelian group of prime power order can be written as a product of cyclic groups. The proof will make use of the following characterization of cyclic abelian p-groups.

Lemma 14. *Suppose that G is a finite abelian p-group. If G has a unique subgroup of order p, then G is cyclic.*

Proof. Since G is a p-group, $|G| = p^r$ for some $r \geq 1$. We argue by induction on the exponent r. If $r = 1$, then $|G| = p$ is prime and G is cyclic. Now suppose that $r > 1$ and that any abelian p group of order less than p^r which has a unique subgroup of order p is cyclic. Let $\varphi : G \to G$ be the homomorphism $\varphi(x) = px$. Then $K = \mathrm{Ker}(\varphi)$ is the unique subgroup of G of order p, and $G/K \cong \varphi(G) = pG$. Since every subgroup of pG is also a subgroup of G, it follows that pG has a unique subgroup of order p, and $|pG| = p^{r-1}$. By induction, we conclude that pG is cyclic, say $pG = \langle y \rangle$. But $y = px$ since $y \in pG$. We claim that $G = \langle x \rangle$. To see this, note that $p^r x = p^{r-1} y = 0$, but $p^k x = p^{k-1} y \neq 0$ for any $k \leq r$ since the order of y is p^{r-1}. Thus, the order of x is p^r, and hence x is a generator of G. □

Lemma 15. *Let G be a finite abelian p-group, and let H be a cyclic subgroup of maximal order. Then there is a subgroup K of G such that G is the internal direct product of H and K*

Proof. The proof is by induction on $|G| = p^r$. If $|G| = 1$ then $G = \langle 0 \rangle$ and we are done. Suppose that $|G| = p^r > 1$. If G has an element of order p^r, then G is cyclic, and we are done (let $K = \langle 0 \rangle$). If not, $|H| = p^t$ with $1 \leq t < r$. Since G is not cyclic, the previous lemma implies that there must be a cyclic subgroup L of G of order p other than the unique subgroup of H of order p. Hence, we must have $L \cap H = \langle 0 \rangle$. Now consider the standard homomorphism $\pi : G \to G/L$. Since no homomorphic image of G can have a cyclic subgroup of order larger that $|H|$, it follows that $\pi(H) = (H + L)/L \cong H$ is cyclic of maximal order in G/L. By the induction hypothesis, $G/L = \pi(H) \times \overline{K}$ for some subgroup $\overline{K}$ of G/L. Let $K = \pi^{-1}(\overline{K}) \subset G$. Since $G/L = ((H + L)/L) + K/L$ it follows that $G = (H+L)+K = H+K$ because $L \subseteq K$. If $a \in H \cap K$ then $\pi(a) \in \pi(H) \cap \pi(K) = 0 \in G/L$. Thus $a \in L$ and $a \in H$ so $a = 0$. Thus $G \cong H \times K$ by Theorem 7. □

A finite abelian p-group G is said to be of *type* $(p^{r_1}, \cdots, p^{r_k})$ if G is isomorphic to the product of cyclic groups of orders p^{r_i} for $1 \leq i \leq k$.

Theorem 16. *Every finite abelian p-group G is isomorphic to a product of cyclic p-groups. If G is of type $(p^{r_1}, \cdots, p^{r_k})$ with*

$$r_1 \geq r_2 \geq \cdots \geq r_k \geq 1,$$

then the sequence of integers $(r_1, \ldots, r_k)$ is uniquely determined by G.

Proof. **Existence.** The existence of the factorization is now easy. If G is not cyclic, let G_1 be a maximal cyclic subgroup of G. By Lemma 15, G has a subgroup K such that $G \cong G_1 \times K$. By induction K is isomorphic to a product of cyclic subgroups, and hence G is also.

Uniqueness. We will prove uniqueness of the type by induction on $|G|$. Suppose that G can be written in two ways as a direct sum of cyclic groups, say of type

$$(p^{r_1}, \ldots, p^{r_k}) \quad \text{and} \quad (p_1^m, \ldots, p^{m_t})$$

with $r_1 \geq \cdots \geq r_k \geq 1$ and $m_1 \geq \cdots \geq m_t \geq 1$. If

$$G = G_1 \times G_2 \times \cdots \times G_s$$

then the subgroup pG can also be written as a direct product

$$pG = (pG_1) \times (pG_2) \times \cdots \times (pG_2).$$

This follows immediately from Theorem 9. Thus pG is a finite abelian p-group of order strictly less than $|G|$ (since any elements of order p are in the kernel of the map $x \mapsto px$). Moreover, pG is of type

$$(p^{r_1-1}, \ldots, p^{r_k-1}) \quad \text{and} \quad (p^{m_1-1}, \ldots, p^{m_t-1}),$$

where we adopt the convention that if some exponent r_i or m_j is 1, then the factor corresponding to p^{r_i-1} or p^{m_j-1} in pG is the trivial group 0. By our induction hypothesis, the subsequence of

$$(r_1 - 1, \ldots, r_k - 1)$$

consisting of those integers ≥ 1 is uniquely determined by the group pG, and hence is the same as the corresponding subsequence of

$$(m_1 - 1, \ldots, m_t - 1).$$

That is, we have $r_i - 1 = m_i - 1$ for all those integers i such that $r_i - 1$ or $m_i - 1 \geq 1$. Hence $r_i = m_i$ for all these integers i, and the two sequences

$$(p^{r_1}, \ldots, p^{r_k}) \quad \text{and} \quad (p_1^m, \ldots, p^{m_t})$$

can differ only in their last components, which are equal to p. These correspond to the factors of type $(p, \ldots, p)$ where the p occurs u times in the first sequence and v times in the second sequence. Thus, there is an natural number n such that G is of type

$$(p^{r_1}, \ldots, p^{r_n}, \underbrace{p, \ldots, p}_{u \text{ times}}) \quad \text{and} \quad (p_1^r, \ldots, p^{r_n}, \underbrace{p, \ldots, p}_{v \text{ times}}).$$

Then the order of G is given by

$$p^{r_1+\cdots+r_n} p^u = p^{r_1+\cdots+r_n} p^v,$$

so that $u = v$, and the number of p factors is also the same in every factorization of G. □

Combining Theorems 13 and 16 gives what is known as the *elementary divisor form of the structure theorem for finite abelian groups.*

Theorem 17. *Let G be an abelian group of order $m > 1$ and let*

$$m = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$$

be the factorization of m into distinct prime powers. Then

1. *$G \cong G_1 \times G_2 \times \cdots \times G_k$ where $|G_i| = p^{r_i}$.*
2. *For $1 \leq i \leq k$,*

$$G_i \cong \mathbb{Z}_{p_i^{t_{1i}}} \times \mathbb{Z}_{p_i^{t_{2i}}} \times \cdots \times \mathbb{Z}_{p_i^{t_{s_i i}}},$$

   where $t_{i1} \geq t_{2i} \geq \cdots \geq t_{s_i i} \geq 1$ and $t_{1i} + t_{2i} + \cdots + t_{s_i i} = r_i$.

3. *The decompositions given by parts 1 and 2 are unique.*

Definition 18. The prime powers $p_i^{t_{ji}}$ described in the preceding theorem are called the *elementary divisors* of G, and the decomposition described in the theorem is known as the *elementary divisor decomposition* of G.

The content of Theorem 17 is that a finite abelian group is uniquely determined, up to group isomorphism, by the elementary divisors. For example, the elementary abelian group E_{p^n} (see Example 6) has elementary divisors p, p, …, p (n copies).