

# Finite Abelian Groups

## 1 Preliminaries

**Definition 1.** Let  $H_1, H_2, \dots, H_k$  be subgroups of  $G$ . We say that  $G$  is the **internal direct product** of  $H_1, \dots, H_k$  if the following hold.

1.  $H_i \triangleleft G$ , for all  $H_i$
2.  $G = H_1 H_2 \cdots H_k$
3.  $H_i \cap H_1 \cdots \widehat{H_i} \cdots H_k = \{e\}$   
( $H_1 \cdots \widehat{H_i} \cdots H_k$  means the product of all the  $H$ 's except  $H_i$ )

**Lemma 2.** Let  $G$  be the internal direct product of  $H_1, \dots, H_k$ . Then we have the following.

1.  $H_i \cap H_j = \{e\}$  for all  $i \neq j$ .
2. If  $g \in G$ , then there exists unique elements  $h_i \in H_i$  such that  $g = h_1 h_2 \cdots h_k$ .
3. If  $h_i \in H_i$  and  $h_j \in H_j$ , then  $h_i h_j = h_j h_i$ .

*Proof.* Exercise. □

**Theorem 3.** If  $G$  is the internal direct product of  $H_1, \dots, H_k$ , then  $G \cong H_1 \times \cdots \times H_k$ .

*Proof.* "Sketch"

Define  $\phi : H_1 \times \cdots \times H_k \rightarrow G$  by  $\phi(h_1, \dots, h_k) = h_1 \cdots h_k$ . Since  $G = H_1 \cdots H_k$ , we get onto. By lemma 2 part 2 we get one-to-one, and finally by lemma 2 part 3 we get that  $\phi$  is a homomorphism. □

## 2 Fundamental Theorem of Finite Abelian Groups

**Lemma 4.** Let  $G$  be an abelian group such that  $|G| = p^k a$  where  $p$  is prime and  $(p, a) = 1$ . Then there exists a unique subgroup of order  $p^k$ .

*Proof.* By corollary 2.78 (in the revised printing) we know that such a subgroup exists. So let  $H \leq G$  such that  $|H| = p^k$ , and let  $G(p) = \{x \in G \mid x^{p^k} = e\}$ . By problem #4 we know  $G(p) \leq G$ . We claim that  $H = G(p)$ . Let  $h \in H$ , then  $h^{p^k} = e$  since  $|H| = p^k$ . Hence  $h \in G(p)$ , so  $H \subseteq G(p)$ . Now let  $g \in G(p)$ . So  $g^{p^k} = e$ . Consider  $gH \in G/H$ . Since  $|G/H| = a$ ,  $\circ(gH) \mid a$ . However  $\circ(gH) \mid \circ(g)$ , so  $\circ(gH) \mid p^k$ . So  $\circ(gH) = 1$  since  $(a, p) = 1$ . Therefore  $gH = H$  and hence  $g \in H$ . Thus  $G(p) \subseteq H$  and hence  $H = G(p)$ . Therefore  $G(p)$  is the unique subgroup of  $G$  of order  $p^k$ . □

**Definition 5.** Let  $G$  be a group such that  $|G| = p^k a$  where  $p$  is prime and  $(p, a) = 1$ . A subgroup of order  $p^k$  is called a **Sylow  $p$ -subgroup** of  $G$ .

**Theorem 6.** Let  $G$  be a finite abelian group such that  $|G| = p_1^{k_1} \cdots p_l^{k_l}$  where each of the  $p_i$  are distinct primes. Then  $G \cong G(p_1) \times \cdots \times G(p_l)$ .

*Proof.* We will show that  $G$  is the internal direct product of its Sylow  $p_i$  subgroups and therefore by Theorem 3 we get our desired result. Firstly, since  $G$  is abelian all subgroups are normal, so  $G(p_i) \triangleleft G$ . Next we will show that  $G = G(p_1)G(p_2) \cdots G(p_l)$ . Clearly  $G(p_1)G(p_2) \cdots G(p_l) \subseteq G$ . Moreover, by homework problem # 3, we have that  $|G(p_1)G(p_2) \cdots G(p_l)| = |G(p_1)||G(p_2)| \cdots |G(p_l)| = p_1^{k_1} p_2^{k_2} \cdots p_l^{k_l} = |G|$ . Hence  $G = G(p_1)G(p_2) \cdots G(p_l)$ .

Lastly we need to show that  $G(p_i) \cap G(p_1) \cdots \widehat{G(p_i)} \cdots G(p_l) = \{e\}$  for all  $i \in \{1, 2, \dots, k\}$ . Fix  $i \in \{1, 2, \dots, k\}$ . Then we can write the order of  $G$  as  $|G| = p_i^{k_i} a$  where  $(p_i, a) = 1$ . Again by homework problem # 3,  $|G(p_1) \cdots \widehat{G(p_i)} \cdots G(p_l)| = a$ . However,  $|G(p_i)| = p^{k_i}$ . Hence  $(|G(p_1) \cdots \widehat{G(p_i)} \cdots G(p_l)|, |G(p_i)|) = 1$  and thus  $G(p_i) \cap G(p_1) \cdots \widehat{G(p_i)} \cdots G(p_l) = \{e\}$ . Therefore  $G$  is the internal product of  $G(p_1), \dots, G(p_l)$  and hence  $G$  is isomorphic to  $G(p_1) \times \cdots \times G(p_l)$ .  $\square$

Note that the above theorem proves that  $G$  is isomorphic to the direct product of its Sylow  $p_i$ -subgroups. We will now show that each of these Sylow  $p_i$ -subgroups can be decomposed into cyclic subgroups. For the following theorem we will be working with a  $p$ -group. So  $|G| = p^n$ . Therefore all elements in  $G$  must have order  $p^j$  for some  $j \in \mathbb{Z}$ . Thus  $G$  contains an element of maximal order. That is, there exists  $a \in G$  such that  $\circ(x) \leq \circ(a)$  for all  $x \in G$ . The proof of the following theorem is not difficult, however it is very intricate. In other words, none of the steps are difficult, but there is a lot to keep track of throughout the proof.

**Theorem 7.** Let  $G$  be a finite abelian  $p$ -group and  $a$  an element of maximal order in  $G$ . Then there is a subgroup  $H$  of  $G$  such that  $G \cong \langle a \rangle \times H$ .

*Proof.* Let  $a \in G$  be an element of maximal order, say  $\circ(a) = p^k$ . Consider all subgroups  $K$  of  $G$  such that  $\langle a \rangle \cap K = \{e\}$ . Let  $H$  be maximal with respect to these subgroups. That is, if  $H < K \leq G$ , then  $\langle a \rangle \cap K \neq \{e\}$ . Since  $G$  is abelian, all subgroups are normal. Moreover,  $\langle a \rangle \cap H = \{e\}$  by definition. Therefore in order to prove that  $G \cong \langle a \rangle \times H$ , we need only show  $G = \langle a \rangle H$ .

Suppose  $G \neq \langle a \rangle H$ , then there exists  $y \in G$  such that  $y \notin \langle a \rangle H$ . Let  $r = \min\{m \in \mathbb{N} | y^{p^m} \in \langle a \rangle H\}$ . Note that by problem #5,  $y^{p^k} = e \in \langle a \rangle H$ , so  $r \leq k$ . Let  $x = y^{p^{r-1}}$ . So  $x \notin \langle a \rangle H$  since  $r$  was the smallest such power. However,  $x^p = y^{p^r} \in \langle a \rangle H$ . In other words, we have found an element  $x \in G$  such that  $x \notin \langle a \rangle H$ , but  $x^p \in \langle a \rangle H$ .

Since  $x^p \in \langle a \rangle H$ , we have  $x^p = a^q h$  for some  $q \in \mathbb{Z}$ ,  $h \in H$ . Using problem # 5 again we get the following.

$$e = x^{p^k} = (x^p)^{p^{k-1}} = (a^q h)^{p^{k-1}} = a^{qp^{k-1}} h^{p^{k-1}}$$

Hence  $a^{qp^{k-1}} = h^{-p^{k-1}} \in H$ . However  $a^{qp^{k-1}} \in \langle a \rangle$ , hence  $a^{qp^{k-1}} \in \langle a \rangle \cap H = \{e\}$ . Therefore  $a^{qp^{k-1}} = e$  implies  $\circ(a) | qp^{k-1}$ . Recall  $\circ(a) = p^k$ , so  $p^k | qp^{k-1}$  implies  $p | q$ . So  $q = ps$  for some  $s \in \mathbb{Z}$ . Recall that  $x \notin \langle a \rangle H$ , so  $xa^{-s} \notin H$ . However we have that

$$(xa^{-s})^p = x^p a^{-ps} = x^p a^{-q} = h \in H \tag{1}$$

Consider  $K = \langle xa^{-s} \rangle H$ . Note that  $H \subseteq K$ . Moreover  $xa^{-s} \in K$ , but  $xa^{-s} \notin H$ , so  $H \neq K$ . Therefore by the maximality of  $H$ ,  $\langle a \rangle \cap K \neq \{e\}$ . Let  $b \in \langle a \rangle \cap K$  where  $b \neq e$ . Therefore there exists  $t, u \in \mathbb{Z}$  and  $h' \in H$  such that  $b = a^t = (xa^{-s})^u h'$ .

We claim that  $p$  does not divide  $u$ . Suppose it does. Then  $u = pv$  for some  $v \in \mathbb{Z}$ , so we have the following.

$$b = (xa^{-s})^u h' = (xa^{-s})^{pv} h' = ((xa^{-s})^p)^v h'$$

By equation (1),  $(xa^{-s})^p \in H$ . Therefore,  $((xa^{-s})^p)^v h' \in H$  and thus  $b \in H$ . Recall that  $b \in \langle a \rangle$  as well, hence  $b \in \langle a \rangle \cap H = \{e\}$ . This is a contradiction since  $b \neq e$ . Therefore  $p$  does not divide  $u$ .

Now, since  $p$  is prime,  $(p, u) = 1$ . So there exists integers  $w$  and  $d$  such that  $1 = pw + ud$ . Therefore  $x = x^{pw+ud} = (x^p)^w (x^u)^d$ , but since  $x^p \in \langle a \rangle H$ , then  $(x^p)^w \in \langle a \rangle H$ . Moreover,  $a^t = (xa^{-s})^u h'$ , so  $x^u = a^t a^{su} (h')^{-1} \in \langle a \rangle H$ . Therefore  $x \in \langle a \rangle H$  and this is a contradiction to how  $x$  was chosen. Thus  $G = \langle a \rangle H$ , and hence  $G$  is the internal direct product of  $\langle a \rangle$  and  $H$ . Therefore  $G \cong \langle a \rangle \times H$ .  $\square$

Using the theorem above we can repeat this process on  $H$  to get  $H \cong \langle c \rangle \times H_1$  for some  $c \in H$ ,  $H_1 \leq H$ , etc. Since  $G$  is finite, eventually this process will end and consequently will have expressed  $G$  as a direct product of cyclic groups. In other words, any  $p$ -group  $G$  can be expressed as an internal direct product of cyclic subgroups. Note, of course, that the order of each of these subgroups is a power of  $p$ . Finally we are able to state (and prove) the Fundamental Theorem of Finite Abelian Groups.

### Theorem 8. (The Fundamental Theorem of Finite Abelian Groups)

*Every finite abelian group  $G$  is isomorphic to a direct product of cyclic groups of prime power order. Furthermore, any two such decompositions have the same number of factors of each order.*

*Proof.* Let  $|G| = p_1^{k_1} p_2^{k_2} \cdots p_l^{k_l}$  where each of the  $p_i$  are distinct primes. By Theorem 6 we get  $G \cong G(p_1) \times \cdots \times G(p_l)$ . Then by Theorem 7 each of the  $G(p_i)$  can be decomposed further such that  $G(p_i) \cong C_{p_i^{n_1}} \times C_{p_i^{n_2}} \times \cdots \times C_{p_i^{n_t}}$  where  $C_x$  is a cyclic group of order  $x$ . Therefore we have that  $G$  is isomorphic to a direct product of cyclic groups of prime power order.

Finally, the uniqueness of the decomposition follows from problems #6 and 7.  $\square$

**Definition 9.** Consider the decomposition into cyclic groups of a finite abelian group  $G$ . In the decomposition, the orders of the cyclic subgroups are called the **elementary divisors** of  $G$ .

We now want to be able to apply the Fundamental Theorem of Finite Abelian Groups to specific groups, but let's first explore the idea in general. Let  $G$  be a finite abelian group such that  $|G| = p_1^{k_1} p_2^{k_2} \cdots p_l^{k_l}$ . Then the first step is to recognize that  $G$  can be decomposed into a product of its Sylow subgroups,  $G(p_i)$ . Each of these subgroups have order  $p_1^{k_1}, p_2^{k_2}, \dots, p_l^{k_l}$  respectively. Furthermore, each of these subgroups can be decomposed into a product of cyclic groups. Let's just consider  $G(p_i)$ . Suppose we have the following decomposition.

$$G(p_i) \cong C_{p_i^{n_1}} \times C_{p_i^{n_2}} \times \cdots \times C_{p_i^{n_t}}$$

In the above, we may assume  $n_1 \geq n_2 \geq \dots \geq n_t$ . Therefore we have the following:

$$\begin{aligned}
 p_i^{k_i} &= |G(p_i)| \\
 &= |C_{p_i}^{n_1} \times C_{p_i}^{n_2} \times \dots \times C_{p_i}^{n_t}| \\
 &= |C_{p_i}^{n_1}| |C_{p_i}^{n_2}| \dots |C_{p_i}^{n_t}| \\
 &= p_i^{n_1} p_i^{n_2} \dots p_i^{n_t} \\
 &= p_i^{n_1+n_2+\dots+n_t}
 \end{aligned}$$

Therefore we see that  $n_1+n_2+\dots+n_t = k_i$ . Therefore the possibilities for the cyclic decomposition of each Sylow  $p$ -subgroup comes from looking at all possible elementary divisors of  $G(p)$ , which has order  $p^k$ . Since each elementary divisor must be a power of  $p$ , we can find them by finding all possible lists of values that sum to  $k$ . This idea gives us a method to apply the Fundamental Theorem of Finite Abelian Groups. Let's start with a simple example first, that of a  $p$ -group. Then move on to an example in which there is more than one prime involved.

**Example 10.** Determine all abelian groups, up to isomorphism, of order 16.

$|G| = 16 = 2^4$ . So  $k = 4$  in this case, therefore we have the following five lists of possibilities.

4  
3, 1  
2, 2  
2, 1, 1  
1, 1, 1, 1

Therefore there are five possibilities for  $G$ . In particular,  $G$  must be isomorphic to one of the following groups:

$$\begin{aligned}
 \mathbb{Z}_{2^4} &= \mathbb{Z}_{16} \\
 \mathbb{Z}_{2^3} \times \mathbb{Z}_{2^1} &= \mathbb{Z}_8 \times \mathbb{Z}_2 \\
 \mathbb{Z}_{2^2} \times \mathbb{Z}_{2^2} &= \mathbb{Z}_4 \times \mathbb{Z}_4 \\
 \mathbb{Z}_{2^2} \times \mathbb{Z}_{2^1} \times \mathbb{Z}_{2^1} &= \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \\
 \mathbb{Z}_{2^1} \times \mathbb{Z}_{2^1} \times \mathbb{Z}_{2^1} \times \mathbb{Z}_{2^1} &= \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2
 \end{aligned}$$

**Example 11.** Determine all abelian groups of order 56.

$|G| = 56 = 2^3 \cdot 7$ . We know that  $G \cong G(2) \times G(7)$  where  $|G(2)| = 2^3$  and  $|G(7)| = 7$ . Therefore the possible exponents for elementary divisors are given by the following lists:

$G(2)$	$G(7)$
3	1
2, 1	
1, 1, 1	

Therefore  $G$  must be isomorphic to one of the following groups:

$$\begin{aligned}
 \mathbb{Z}_{2^3} \times \mathbb{Z}_{7^1} &= \mathbb{Z}_8 \times \mathbb{Z}_7 \\
 \mathbb{Z}_{2^2} \times \mathbb{Z}_{2^1} \times \mathbb{Z}_{7^1} &= \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_7 \\
 \mathbb{Z}_{2^1} \times \mathbb{Z}_{2^1} \times \mathbb{Z}_{2^1} \times \mathbb{Z}_{7^1} &= \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_7
 \end{aligned}$$

In the previous two examples, we could have expressed these groups in different ways. For example using problem #1 below, we see that we could have written  $\mathbb{Z}_8 \times \mathbb{Z}_7$  as  $\mathbb{Z}_{56}$  since they are isomorphic. We could have made similar adjustments in the others as well. In fact, every finite abelian group is isomorphic to a product of cyclic groups of orders  $m_1, m_2, \dots, m_t$  where  $m_1 | m_2, m_2 | m_3, \dots, m_{t-1} | m_t$ . The values  $m_1, m_2, \dots, m_t$  are called **invariant factors** of  $G$ .

**Example 12.** Suppose the elementary divisors of a finite abelian group  $G$  are  $2, 2, 2^2, 2^3, 3, 3, 3, 5, 5^2$ . Determine the invariant factors of  $G$ .

Since we know the elementary divisors, we have the following.

$$G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_{25}$$

To find the invariant factors we arrange our elementary divisors in increasing order, with one row for each prime.

$$\begin{array}{cccc} 2 & 2 & 2^2 & 2^3 \\ & 3 & 3 & 3 \\ & & 5 & 5^2 \end{array}$$

Now we can rearrange the cyclic factors of  $G$  using the columns of this array and problem #1.

$$\begin{array}{ccccccc} G \cong & \mathbb{Z}_2 & \times & (\mathbb{Z}_2 \times \mathbb{Z}_3) & \times & (\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_5) & \times & (\mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_{25}) \\ G \cong & \mathbb{Z}_2 & \times & \mathbb{Z}_6 & \times & \mathbb{Z}_{60} & \times & \mathbb{Z}_{600} \end{array}$$

So the invariant factors are  $2, 6, 60, 600$ .

### 3 Exercises.

1. Prove that  $\mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{nm}$  if and only if  $(n, m) = 1$ .
2. Prove that  $\mathbb{Z}_n \times \mathbb{Z}_m$  is cyclic if and only if  $(n, m) = 1$ .
3. Let  $H_1, \dots, H_k$  be subgroups of a group  $G$  such that  $(|H_i|, |H_j|) = 1$  for all  $i \neq j$  in  $\{1, \dots, k\}$ . Prove that  $|H_1 H_2 \cdots H_k| = |H_1| |H_2| \cdots |H_k|$ . (Hint: Induct on  $k$ .)
4. Let  $G$  be a finite abelian group of order  $p^k a$  where  $(p, a) = 1$  and let  $G(p) = \{x \in G | x^{p^k} = e\}$ . Prove that  $G(p) \leq G$ .
5. Let  $G$  be a finite abelian  $p$ -group and  $a$  an element of maximal order in  $G$ . If  $\circ(a) = p^k$ , prove that  $x^{p^k} = e$  for all  $x \in G$ .
6. Let  $G_1$  and  $G_2$  be abelian groups of order  $p_1^{k_1} p_2^{k_2} \cdots p_l^{k_l}$ . Prove that  $G_1 \cong G_2$  if and only if  $G_1(p_i) \cong G_2(p_i)$  for all  $i \in \{1, 2, \dots, l\}$ .
7. Let  $n_1 \geq n_2 \geq \cdots \geq n_r$  and  $m_1 \geq m_2 \geq \cdots \geq m_s$  where  $n_1 + n_2 + \cdots + n_r = m_1 + m_2 + \cdots + m_s$  and let  $p$  be a prime. Let  $C_t$  be a cyclic subgroup of order  $t$ .  
Prove that  $C_{p^{n_1}} \times C_{p^{n_2}} \times \cdots \times C_{p^{n_r}} \cong C_{p^{m_1}} \times C_{p^{m_2}} \times \cdots \times C_{p^{m_r}}$  if and only if  $r = s$  and  $n_i = m_i$  for all  $i$ .
8. Find all, up to isomorphism, abelian groups of order

- (a) 105
  - (b) 270
  - (c) 9801
  - (d) 320
  - (e) 44100
9. What is the smallest positive integer  $n$  such that
- (a) there are two nonisomorphic groups of order  $n$ ?
  - (b) there are three nonisomorphic abelian groups of order  $n$ ?
  - (c) there are exactly four nonisomorphic abelian groups of order  $n$ ?
10. Calculate the number of elements of order 2 and of order 4 in each of the following groups:
- (a)  $\mathbb{Z}_{16}$
  - (b)  $\mathbb{Z}_8 \times \mathbb{Z}_2$
  - (c)  $\mathbb{Z}_4 \times \mathbb{Z}_4$
  - (d)  $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2$
  - (e)  $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$
11. There are six abelian groups, up to isomorphism, of order 108. Prove that
- (a) two of them have exactly one subgroup of order 3, and
  - (b) two of them have exactly four subgroups of order 3, and
  - (c) two of them have exactly 13 subgroups of order 3.
12. How many abelian groups, up to isomorphism, are there
- (a) of order  $pq$ , where  $p$  and  $q$  are distinct primes?
  - (b) of order  $pqr$ , where  $p, q$  and  $r$  are distinct primes?
13. Suppose that  $G$  is an abelian group of order 120 and that  $G$  has exactly three elements of order 2. Determine the isomorphism class of  $G$ .
14. Suppose that  $G$  is an abelian group of order 16 with at least one element of order 8 and at least two elements of order 2. Determine the isomorphism class of  $G$ .
15. Suppose that  $G$  is an abelian group of order 16 and that  $a, b \in G$  with  $\circ(a) = \circ(b) = 4$  and  $a^2 \neq b^2$ . Determine the isomorphism class of  $G$ .
16. Let  $G = U(\mathbb{Z}_{16}) = \{[1], [3], [5], [7], [9], [11], [13], [15]\}$ . Recall that this is a group with respect to multiplication.
- (a) Determine the isomorphism class of  $G$ .
  - (b) Write  $G$  as an internal direct product of cyclic groups.