

# Chapter 3.

## Constructing groups

### 10. Permutation groups

The main significance of the symmetric groups is that they contain all other groups.

**Theorem 10.1 (Cayley)** *Let  $G$  be a group, and let  $S_G$  be the symmetric group on the set  $G$ . For each  $a \in G$  the mapping  $\sigma_a : G \rightarrow G$  defined by  $x\sigma_a = xa$  is a permutation of  $G$ . The set  $H = \{\sigma_a : a \in G\}$  is a subgroup of  $S_G$  and is isomorphic to  $G$ . Therefore, every group is isomorphic to a subgroup of a symmetric group.*

**Proof.** For any  $x, y \in G$  we have

$$x\sigma_a = y\sigma_a \Rightarrow xa = ya \Rightarrow xaa^{-1} = yaa^{-1} \Rightarrow x = y,$$

and hence  $\sigma_a$  is injective. If  $b \in G$  is arbitrary, then for  $x = ba^{-1} \in G$  we have  $x\sigma_a = ba^{-1}a = b$ , so that  $\sigma_a$  is surjective as well.

Define a mapping  $f : G \rightarrow S_G$  by  $af = \sigma_a$ . Then  $f$  is a homomorphism. Indeed, if  $a, b \in G$  are arbitrary then

$$x(\sigma_a\sigma_b) = (x\sigma_a)\sigma_b = (xa)\sigma_b = x(ab) = x\sigma_{ab}$$

is true for all  $x \in G$ , so that  $\sigma_a\sigma_b = \sigma_{ab}$ , i.e.  $(af)(bf) = (ab)f$ . Actually,  $f$  is a monomorphism since

$$af = bf \Rightarrow \sigma_a = \sigma_b \Rightarrow x\sigma_a = x\sigma_b \text{ for all } x \in G \Rightarrow e\sigma_a = e\sigma_b \Rightarrow ea = eb \Rightarrow a = b.$$

The image of  $f$  is clearly  $H$ , and, by the above,  $H \cong G$ . ■

**Example 10.2.** Consider the Klein four group  $K_4 = \{e, a, b, c\}$ . The permutations corresponding to the elements are:

$$\begin{aligned} \sigma_e &= \begin{pmatrix} e & a & b & c \\ e & a & b & c \end{pmatrix}, & \sigma_a &= \begin{pmatrix} e & a & b & c \\ a & e & c & b \end{pmatrix}, \\ \sigma_b &= \begin{pmatrix} e & a & b & c \\ b & c & e & a \end{pmatrix}, & \sigma_c &= \begin{pmatrix} e & a & b & c \\ c & b & a & e \end{pmatrix}. \end{aligned}$$

After renaming  $e, a, b, c$  into  $1, 2, 3, 4$  respectively, we conclude that  $K_4$  is isomorphic to the subgroup  $\{\text{id}, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$  of  $S_4$ .

**Remark 10.3.** Cayley's theorem implies that a group of order  $n$  is isomorphic to a subgroup of  $S_n$ . However, it often happens that  $G$  is isomorphic to a subgroup of  $S_m$  for smaller than  $n$ . For example, Cayley's theorem implies that the alternating group  $A_n$  is isomorphic to a subgroup of  $S_{n!/2}$ . However,  $A_n$  is also a subgroup of  $S_n$  (that is how it is defined).

A subgroup of a symmetric group is called a permutation group. So, for example, the alternating groups and dihedral groups are permutation groups. A permutation group may be (and usually is) given by a generating set (as we did with dihedral groups). So one has a very concise way of defining groups, just by specifying a few permutations. The question then arises of how to determine various properties of the group in question, and this is the subject of the theory of permutation groups. One (naive) approach is to use the algorithm described in Section 4 to compute all the elements of the group, and then work from there. This works for groups of reasonably small orders; for groups of larger orders more sophisticated methods are needed. At present, there are algorithms working efficiently on permutation groups acting on millions of points.

We give another consequence of Cayley's theorem, which shows that the general linear groups  $GL(n, \mathbb{F})$  have the same property as symmetric groups.

**Theorem 10.4.** *Let  $\mathbb{F}$  be a field, and let  $n$  be a positive integer. For a permutation  $\sigma \in S_n$ , define an  $n \times n$  matrix  $A_\sigma = (a_{ij})$  by*

$$a_{ij} = \begin{cases} 1 & \text{if } i\sigma = j \\ 0 & \text{otherwise.} \end{cases}$$

*The mapping  $f : S_n \rightarrow GL(n, \mathbb{F})$ ,  $\sigma f = A_\sigma$  is a monomorphism. Therefore, every group of order  $n$  is isomorphic to a subgroup of the general linear group  $GL(n, \mathbb{F})$ .*

**Proof.** Since all matrices  $A_\sigma$  are obtained by permuting rows of the identity matrix, they all have determinants  $\pm 1$ , and are in  $GL(n, \mathbb{F})$ .

Let  $\sigma, \tau \in S_n$  be arbitrary, and let  $A_\sigma = (a_{ij})$ ,  $A_\tau = (b_{ij})$ ,  $A_\sigma A_\tau = (c_{ij})$  and  $A_{\sigma\tau} = (d_{ij})$ . Then we have

$$\begin{aligned} c_{ij} &= \begin{cases} 1 & \text{if } (\exists k)(a_{ik} = b_{kj} = 1) \\ 0 & \text{otherwise} \end{cases} = \begin{cases} 1 & \text{if } (\exists k)(i\sigma = k, k\tau = j) \\ 0 & \text{otherwise} \end{cases} \\ &= \begin{cases} 1 & \text{if } i\sigma\tau = j \\ 0 & \text{otherwise} \end{cases} = d_{ij}. \end{aligned}$$

Therefore

$$(\sigma f)(\tau f) = A_\sigma A_\tau = A_{\sigma\tau} = (\sigma\tau)f,$$

and  $f$  is a homomorphism.

From the definition it follows immediately that  $f$  is injective. Therefore,  $f$  is a monomorphism. It follows that  $S_n$  is isomorphic to the image of  $f$ , which is a subgroup of  $GL(n, \mathbb{F})$ . By Cayley's theorem any group of order  $n$  is isomorphic to a subgroup of  $S_n$ , and hence to a subgroup of  $GL(n, \mathbb{F})$  as well. ■

We can find other ways of representing arbitrary groups as subgroups of  $GL(n, F)$ .

**Example 10.5.** Let  $G$  be  $D_4 = \langle \alpha, \beta : \alpha^4 = \beta^2 = e, \beta^{-1}\alpha\beta = \alpha^{-1} \rangle$ . Define matrices  $A$  and  $B$  in  $GL(2, \mathbb{F})$  to be:

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

It can be shown that  $A^4 = B^2 = I$ ,  $B^{-1}AB = A^{-1}$ . The function  $\rho : \alpha^i \beta^j \mapsto A^i B^j$  ( $0 \leq i \leq 3, 0 \leq j \leq 1$ ) is an isomorphism from  $D_4$  to a subgroup of  $GL(2, \mathbb{F})$ .

The study of different ways of representing a group as a subgroup of  $GL(n, F)$  is called *representation theory*.

## 11. Direct products

So far, we have considered two *constructions* (i.e. ways of obtaining new groups from the known ones), namely forming subgroups and quotients. In group theory (and algebra in general) there are a number of other standard constructions, and the direct product is probably the most important of them.

**Definition 11.1.** Let  $G$  and  $H$  be two groups. The direct product of  $G$  and  $H$  is the set  $G \times H$  with the component-wise multiplication:

$$(g_1, h_1)(g_2, h_2) = (g_1g_2, h_1h_2).$$

In the following theorem we list some basic properties of direct products.

**Theorem 11.2.** *Let  $G$  and  $H$  be any two groups.*

- (i)  $G \times H$  is a group.
- (ii)  $|G \times H| = |G||H|$ .
- (iii) The set  $\overline{G} = \{(g, e_H) : g \in G\}$  is a normal subgroup of  $G \times H$ , and is isomorphic to  $G$ . Similarly, the set  $\overline{H} = \{(e_G, h) : h \in H\}$  is a normal subgroup of  $G \times H$  and is isomorphic to  $H$ .
- (iv)  $\overline{G} \cap \overline{H} = \{(e_G, e_H)\}$ .
- (v)  $\overline{G}\overline{H} = G \times H$ .

**Proof.** (i) It is clear that multiplication is closed, associativity follows from the associativity in  $G$  and  $H$ , the identity element is  $(e_G, e_H)$ , and the inverse of  $(g, h)$  is  $(g^{-1}, h^{-1})$ .

(ii) This is obvious.

(iii) Let  $(g, e_H) \in \overline{G}$  and  $(a, b) \in G \times H$  be arbitrary. Then

$$(a, b)^{-1}(g, e_H)(a, b) = (a^{-1}ga, b^{-1}e_Hb) = (a^{-1}ga, e_H) \in \overline{G}.$$

Therefore  $\overline{G} \trianglelefteq G \times H$ . To prove that  $\overline{G} \cong G$  check that the mapping  $f : G \longrightarrow \overline{G}$  defined by  $xf = (x, e_H)$  is an isomorphism.

(iv) This is obvious.

(v)  $(g, h) = (g, e_H)(e_G, h) \in \overline{G}\overline{H}$ . ■

**Definition 11.3.** A group  $G$  is directly decomposable if there exist non-trivial groups  $H$  and  $K$  such that  $G \cong H \times K$ ; otherwise  $G$  is directly indecomposable.

**Example 11.4.**  $D_{2n} \cong D_n \times \mathbb{Z}_2$  if  $n$  is odd.

One may ask when a group is directly decomposable. By Theorem 11.2 it follows that if  $G$  is directly decomposable then it contains two normal subgroups  $H$  and  $K$  such that  $H \cap K = \{e_G\}$  and  $HK = G$ . Actually, this is also sufficient to ensure that  $G$  is directly decomposable, as the following theorem shows.

**Theorem 11.5.** Let  $G$  be a group, and let  $H$  and  $K$  be two normal subgroups of  $G$ . If the following two conditions hold

- (i)  $HK = G$ ;
- (ii)  $H \cap K = \{e\}$ .

then  $G \cong H \times K$ .

**Proof.** Let us define a mapping  $f : H \times K \longrightarrow G$  by  $(h, k)f = hk$ . By (i) we have that  $f$  is onto. Next we prove that  $f$  is one-one:

$$\begin{aligned} (h_1, k_1)f = (h_2, k_2)f &\implies h_1k_1 = h_2k_2 \implies h_2^{-1}h_1 = k_2k_1^{-1} \in H \cap K \\ &\implies h_2^{-1}h_1 = k_2k_1^{-1} = e \implies h_1 = h_2, k_1 = k_2 \\ &\implies (h_1, k_1) = (h_2, k_2). \end{aligned}$$

In order to prove that  $f$  is a homomorphism, we take arbitrary  $h_1, h_2 \in H$ ,  $k_1, k_2 \in K$ . Consider the element  $h_2^{-1}k_1^{-1}h_2k_1$ . Since  $K \trianglelefteq G$  we have  $h_2^{-1}k_1^{-1}h_2 \in K$ , and hence  $h_2^{-1}k_1^{-1}h_2k_1 \in K$ . Similarly,  $H \trianglelefteq G$  implies  $h_2^{-1}k_1^{-1}h_2k_1 \in H$ . Therefore  $h_2^{-1}k_1^{-1}h_2k_1 \in H \cap K = \{e\}$ , and so  $h_2k_1 = k_1h_2$ . Now we have

$$((h_1, k_1)(h_2, k_2))f = (h_1h_2, k_1k_2)f = h_1h_2k_1k_2 = h_1k_1h_2k_2 = (h_1, k_1)f(h_2, k_2)f,$$

and hence  $f$  is an isomorphism. ■

The notion of a direct product can be generalised to any number of factors. Let  $H_i$ ,  $1 \leq i \leq n$ , be groups. The set  $G = H_1 \times H_2 \times \dots \times H_n$  of all  $n$ -tuples  $(h_1, h_2, \dots, h_n)$  with  $h_i \in H_i$ , is a group under the component-wise multiplication. If we let

$$\overline{H}_i = \{(e_{H_1}, \dots, e_{H_{i-1}}, h_i, e_{H_{i+1}}, \dots, e_{H_n}) : h_i \in H_i\},$$

then  $\overline{H}_i \trianglelefteq G$  and  $\overline{H}_i \cong H_i$ . Also we have

$$\begin{aligned} G &= \overline{H}_1\overline{H}_2 \dots \overline{H}_n, \\ \overline{H}_i \cap (\overline{H}_1 \dots \overline{H}_{i-1}\overline{H}_{i+1} \dots \overline{H}_n) &= \{(e_{H_1}, e_{H_2}, \dots, e_{H_n})\}. \end{aligned}$$

As in the case of two factors we have the converse:

**Theorem 11.6.** *Let  $G$  be a group, and let  $H_i$ ,  $1 \leq i \leq n$ , be  $n$  normal subgroups of  $G$  such that the following two conditions are satisfied:*

- (i)  $G = H_1H_2 \dots H_n$ ;
- (ii)  $H_i \cap (H_1 \dots H_{i-1}H_{i+1} \dots H_n) = \{e\}$ , for all  $i$ .

Then  $G \cong H_1 \times H_2 \dots \times H_n$ . ■

Finally, we give a result connecting direct products and quotients that we shall need in the following section.

**Theorem 11.7.** *Let  $G_i$ ,  $1 \leq i \leq n$ , be groups, and let  $H_i \trianglelefteq G_i$ ,  $1 \leq i \leq n$ . Then  $H_1 \times \dots \times H_n \trianglelefteq G_1 \times \dots \times G_n$  and*

$$\frac{G_1 \times \dots \times G_n}{H_1 \times \dots \times H_n} \cong \frac{G_1}{H_1} \times \dots \times \frac{G_n}{H_n}.$$

**Proof.** Define a mapping

$$f : G_1 \times \dots \times G_n \longrightarrow \frac{G_1}{H_1} \times \dots \times \frac{G_n}{H_n}$$

by

$$(g_1, \dots, g_n)f = (g_1H_1, \dots, g_nH_n).$$

Prove that this is an epimorphism with kernel  $H_1 \times \dots \times H_n$ , and the result follows by the First Isomorphism Theorem. ■

## 12. Finite abelian groups

In this section we shall use direct products to classify all finite abelian groups up to isomorphism. For abelian groups it is customary to use additive notation, writing  $+$  for the group operation. The following table is a ‘multiplicative–additive dictionary’:

multiplicative	additive
$ab$	$a + b$
$a^{-1}$	$-a$
$e$	$0$
$\langle e \rangle$	$0$
$a^n$	$na$
$ab^{-1}$	$a - b$
$aH$	$a + H$
$G/N$	$G/N$
$HK$	$H + K$
direct product	direct sum
$G \times H$	$G \oplus H$

Note that we retain the multiplicative notation  $G/N$  for factors, rather than using the alternative  $G - N$ .

If  $G$  is an abelian group, and  $X = \{a_1, \dots, a_n\}$ , then, by Theorem 4.3, the subgroup generated by  $X$  consists of all sums of elements of  $X$  and

their inverses. However, because of commutativity, we can collect all the summands containing  $a_i$  together for  $i = 1, \dots, n$ , and hence

$$\langle X \rangle = \{k_1 a_1 + k_2 a_2 + \dots + k_n a_n : k_1, \dots, k_n \in \mathbb{Z}\}.$$

Similarly, if  $H$  and  $K$  are subgroups of  $G$  we have

$$\langle H, K \rangle = H + K.$$

A simple class of finite abelian groups are cyclic groups  $\mathbb{Z}_n$ . The aim of this section is to show how an arbitrary abelian group can be decomposed into a direct sum of cyclic groups. As the first step we analyse the direct product of two cyclic groups.

**Theorem 12.1.** *If  $m$  and  $n$  are co-prime natural numbers, then*

$$\mathbb{Z}_m \oplus \mathbb{Z}_n \cong \mathbb{Z}_{mn}.$$

**Proof.** Clearly,  $\mathbb{Z}_m \oplus \mathbb{Z}_n$  has order  $mn$ . Therefore, to prove the theorem, it is enough to show that  $\mathbb{Z}_m \oplus \mathbb{Z}_n$  is cyclic, i.e. that it contains an element of order  $mn$ .

Consider the element  $(1 \pmod{m}, 1 \pmod{n})$ , and let  $t$  be its order. By Lagrange's Theorem we have  $t|mn$ . On the other hand we have

$$(0, 0) = t(1 \pmod{m}, 1 \pmod{n}) = (t \pmod{m}, t \pmod{n}),$$

so that  $m|t$  and  $n|t$ . Since  $\gcd(m, n) = 1$  it follows that  $mn|t$ , and therefore  $t = mn$ , as required. ■

The following theorem is an immediate corollary of Theorem 12.1:

**Theorem 12.2.** *Let  $n > 1$  be a natural number, and let  $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$  be its decomposition into a product of primes. Then*

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{\alpha_1}} \oplus \mathbb{Z}_{p_2^{\alpha_2}} \oplus \dots \oplus \mathbb{Z}_{p_k^{\alpha_k}}. \quad \blacksquare$$

In order to prove our main theorem we need the following

**Lemma 12.3.** *Let  $G = \langle a_1, \dots, a_n \rangle$  be an abelian group. If*

$$b = k_1 a_1 + k_2 a_2 + \dots + k_n a_n,$$

*with  $\gcd(k_1, \dots, k_n) = 1$  then there exist elements  $b_2, \dots, b_n \in G$  such that*

$$G = \langle b, b_2, \dots, b_n \rangle.$$

**Proof.** We prove the lemma by induction on  $n$ . If  $n = 1$  then we must have  $k_1 = 1$ , and hence  $b = a_1$ .

Let us now consider the case  $n = 2$ . Since  $k_1$  and  $k_2$  are co-prime, it follows that there exist numbers  $l_1$  and  $l_2$  such that

$$k_1 l_1 + k_2 l_2 = 1.$$

We define

$$b_2 = l_2 a_1 - l_1 a_2 \in G,$$

and show that  $G = \langle b, b_2 \rangle$ . Clearly, to prove this, it is enough to show that  $a_1, a_2 \in \langle b, b_2 \rangle$ . This is proved as follows:

$$\begin{aligned} a_1 &= (l_1 k_1 + l_2 k_2) a_1 = l_1 k_1 a_1 + l_1 k_2 a_2 + l_2 k_2 a_1 - l_1 k_2 a_2 = l_1 b + k_2 b_2 \in \langle b, b_2 \rangle, \\ a_2 &= (l_1 k_1 + l_2 k_2) a_2 = l_2 k_1 a_1 + l_2 k_2 a_2 - l_2 k_1 a_1 + l_1 k_1 a_2 = l_2 b - k_1 b_2 \in \langle b, b_2 \rangle. \end{aligned}$$

Suppose now that  $n \geq 3$ , and let

$$\gcd(k_1, \dots, k_{n-1}) = t.$$

Define  $m_i = k_i/t$  for  $1 \leq i \leq n-1$ , and let

$$\bar{b} = m_1 a_1 + \dots + m_{n-1} a_{n-1}.$$

Since  $\gcd(m_1, \dots, m_{n-1}) = 1$ , by induction we have

$$\langle a_1, \dots, a_{n-1} \rangle = \langle \bar{b}, b_2, \dots, b_{n-1} \rangle,$$

for some  $b_2, \dots, b_{n-1} \in G$ . Next we have

$$b = t\bar{b} + k_n a_n,$$

and  $\gcd(t, k_n) = \gcd(k_1, \dots, k_n) = 1$ , so that

$$\langle \bar{b}, a_n \rangle = \langle b, b_n \rangle,$$

for some  $b_n \in G$  (the case  $n=2$ ). Now

$$\begin{aligned} G &= \langle a_1, \dots, a_n \rangle = \langle a_1, \dots, a_{n-1} \rangle + \langle a_n \rangle = \langle \bar{b}, b_2, \dots, b_{n-1} \rangle + \langle a_n \rangle \\ &= \langle \bar{b}, b_2, \dots, b_{n-1}, a_n \rangle = \langle \bar{b}, a_n \rangle + \langle b_2, \dots, b_{n-1} \rangle \\ &= \langle b, b_n \rangle + \langle b_2, \dots, b_{n-2} \rangle = \langle b, b_2, \dots, b_n \rangle, \end{aligned}$$

as required. ■

**Theorem 12.4.** *Every finite abelian group  $G$  is isomorphic to the direct sum of cyclic groups, each of which has a prime power order.*

**Proof.** We prove the theorem by induction on the minimal number  $n$  of elements needed to generate  $G$ . If  $n = 1$  then  $G$  is cyclic, and the theorem follows from Theorem 12.2. Let us now assume that  $n \geq 2$ , and let  $\{a_1, a_2, \dots, a_n\}$  be a generating set for  $G$  with the property that  $a_1$  has the minimal possible order. Define

$$H = \langle a_1 \rangle, \quad K = \langle a_2, \dots, a_n \rangle.$$

The group  $H$  is cyclic and is isomorphic to a direct sum of cyclic groups of prime power order by Theorem 12.2. Also,  $K$  is a finite abelian group which can be generated by  $n - 1$  elements, and hence, by induction, it follows that  $K$  is isomorphic to the direct sum of cyclic groups of prime power order. Therefore, to complete the proof of the theorem, it is enough to show that  $G \cong H \oplus K$ . We shall prove this by proving that

$$G = H + K, \quad H \cap K = \{0\}$$

(see Theorem 11.5). The first of these equalities is obvious, for

$$H + K = \langle a_1 \rangle + \langle a_2, \dots, a_n \rangle = \langle a_1, a_2, \dots, a_n \rangle = G.$$

For the second assume that  $x \in H \cap K$  and that  $x \neq 0$ . This means that

$$x = k_1 a_1 = k_2 a_2 + \dots + k_n a_n,$$

with  $k_1 \neq 0$ . Note that the above equalities imply

$$-k_1 a_1 + k_2 a_2 + \dots + k_n a_n = 0.$$

If  $\gcd(k_1, \dots, k_n) = t$ , then  $t \neq 0$  since  $k_1 \neq 0$ . We let  $m_i = k_i/t$  for  $1 \leq i \leq n$ , and define

$$b = -m_1 a_1 + m_2 a_2 + \dots + m_n a_n.$$

Since  $\gcd(m_1, \dots, m_n) = 1$  it follows by Lemma 12.3 that  $G = \langle b, b_2, \dots, b_n \rangle$  for some  $b_2, \dots, b_n \in G$ . On the other hand we have  $tb = -k_1 a_1 + k_2 a_2 + \dots + k_n a_n = 0$ , and, if  $t \leq k_1 < |a_1|$ , which contradicts our choice of the generating set  $\{a_1, \dots, a_n\}$ . Therefore,  $H \cap K = \{0\}$ , and this completes the proof of the theorem. ■

Next we want to prove that the decomposition given in Theorem 12.4 is unique up to the order of direct summands. To this end we introduce some notation. Let  $G$  be an abelian group, and let  $n \in \mathbb{Z}$ . Then

$$nG = \{na : a \in G\}.$$

**Lemma 12.5.** (i)  $nG \leq G$ .

(ii) If  $n$  divides  $m$  then  $mG \leq nG$ .

(iii)  $n\mathbb{Z}_m \cong \mathbb{Z}_{m/\gcd(m,n)}$ . In particular, if  $\gcd(m,n) = 1$  then  $n\mathbb{Z}_m \cong \mathbb{Z}_m$ , while if  $m|n$  then  $n\mathbb{Z}_m$  is trivial.

(iv)  $n(G_1 \oplus \dots \oplus G_k) = (nG_1) \oplus \dots \oplus (nG_k)$ .

**Proof.** (i)  $na - nb = n(a - b) \in nG$ .

(ii) If  $m = nt$  then for arbitrary  $ma \in mG$  we have  $ma = n(ta) \in nG$ .

(iii) Let us denote  $\gcd(m,n)$  by  $d$ , so that  $m = m_1d$ ,  $n = n_1d$  and  $\gcd(m_1, n_1) = 1$ . By (i),  $n\mathbb{Z}_m \leq \mathbb{Z}_m$ , and hence  $n\mathbb{Z}_m$  is a cyclic group by Theorem 5.2. Therefore, it is enough to show that  $n\mathbb{Z}_m$  contains exactly  $m/d = m_1$  elements. Clearly we have  $n\mathbb{Z}_m = \{0, n, 2n, \dots, (m-1)n\}$ , where all the numbers are reduced modulo  $m$ . The first  $m_1$  numbers in the above set are all distinct. Indeed, if  $in = jn \pmod{m}$ , with  $i, j < m_1$ , then  $(i-j)n = km$  for some  $k$ , so that  $(i-j)n_1 = km_1$ , which is impossible since  $\gcd(m_1, n_1) = 1$ , unless  $i = j$ . On the other hand we have  $m_1n = m_1n_1d = mn_1 = 0 \pmod{m}$ , and therefore  $n\mathbb{Z}_m$  indeed has  $m_1$  elements.

(iv) This is straightforward. ■

**Theorem 12.6.** Let  $G$  be a finite abelian group. The decomposition of  $G$  into a direct sum of cyclic groups of prime power orders is unique up to the order of summands.

**Proof.** Let us assume that a decomposition of  $G$  into a direct sum of cyclic groups of prime power orders is given. Let  $n$  be the order of  $G$ , and let  $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$  be the decomposition of  $n$  into a product of primes. Denote by  $A_i$  the direct sum of all summands of  $G$  with order a power of  $p_i$ . Then

$$G \cong A_1 \oplus \dots \oplus A_m. \quad (3.3)$$

For each  $i = 1, \dots, m$  let  $n_i = n/p_i^{\alpha_i}$ . Note that  $n_i$  is divisible by  $p_j^{\alpha_j}$  for  $j \neq i$ , so that by Lemma 12.5 (iii) and (iv) we have  $n_i A_j = 0$ . On the other

hand,  $n_i$  and  $p_i$  are co-prime, and hence  $n_i A_i = A_i$ . If we bear this in mind and multiply (3.3) by  $n_i$  we obtain

$$\begin{aligned} n_i G &\cong n_i(A_1 \oplus \dots \oplus A_m) \\ &= n_i A_1 \oplus \dots \oplus n_i A_{i-1} \oplus n_i A_i \oplus n_i A_{i+1} \oplus \dots \oplus n_i A_m \\ &\cong 0 \oplus \dots \oplus 0 \oplus A_i \oplus 0 \oplus \dots \oplus A_m \cong A_i. \end{aligned}$$

Therefore, each  $A_i$  is uniquely determined by  $G$ .

Now we want to show that the decomposition of  $A_i$  into a direct sum of cyclic groups of order power of  $p_i$  is uniquely determined by  $A_i$  (and hence by  $G$ ). So we fix one  $A_i = A$ , and we let

$$p_i = p, \alpha_i = \alpha.$$

Then  $A$  can be written as

$$A = B_1 \oplus B_2 \oplus \dots \oplus B_\alpha,$$

where each  $B_i$  is a direct sum of several copies of  $\mathbb{Z}_{p^i}$ , say  $t_i$  of them:

$$B_i = \underbrace{\mathbb{Z}_{p^i} \oplus \mathbb{Z}_{p^i} \oplus \dots \oplus \mathbb{Z}_{p^i}}_{t_i}.$$

We aim to prove that the numbers  $t_i$  are uniquely determined by  $A$ .

Let  $j$  be arbitrary with  $0 \leq j < \alpha$ . By Lemma 12.5 (ii) we have  $p^{j+1}A \leq p^j A$ . If we now use Theorem 11.7 and Lemma 12.5 (iv), we obtain

$$\frac{p^j A}{p^{j+1} A} = \frac{p^j B_1 \oplus \dots \oplus p^j B_\alpha}{p^{j+1} B_1 \oplus \dots \oplus p^{j+1} B_\alpha} \cong \frac{p^j B_1}{p^{j+1} B_1} \oplus \dots \oplus \frac{p^j B_\alpha}{p^{j+1} B_\alpha}.$$

A general summand in the above direct sum looks like

$$\frac{p^j B_k}{p^{j+1} B_k} = \frac{\underbrace{p^j \mathbb{Z}_{p^k} \oplus \dots \oplus p^j \mathbb{Z}_{p^k}}_{t_k}}{\underbrace{p^{j+1} \mathbb{Z}_{p^k} \oplus \dots \oplus p^{j+1} \mathbb{Z}_{p^k}}_{t_k}} \cong \underbrace{\frac{p^j \mathbb{Z}_{p^k}}{p^{j+1} \mathbb{Z}_{p^k}} \oplus \dots \oplus \frac{p^j \mathbb{Z}_{p^k}}{p^{j+1} \mathbb{Z}_{p^k}}}_{t_k}.$$

Now, if  $k \leq j$  then

$$p^j \mathbb{Z}_{p^k} = 0,$$

while if  $k > j$  then

$$p^j \mathbb{Z}_{p^k} \cong \mathbb{Z}_{p^{k-j}}$$

by Lemma 12.5 (iii). In particular, for  $k > j$  we have  $|p^j \mathbb{Z}_{p^k}| = p^{k-j}$ , and similarly,  $|p^{j+1} \mathbb{Z}_{p^k}| = p^{k-j-1}$ . Consequently

$$\left| \frac{p^j \mathbb{Z}_{p^i}}{p^{j+1} \mathbb{Z}_{p^i}} \right| = \frac{p^{k-j}}{p^{k-j-1}} = p,$$

and therefore

$$\frac{p^j \mathbb{Z}_{p^i}}{p^{j+1} \mathbb{Z}_{p^i}} \cong \mathbb{Z}_p,$$

by Theorem 6.10. To sum all this up, we have

$$\frac{p^j B_k}{p^{j+1} B_k} \cong \begin{cases} 0 & \text{if } k \leq j \\ \underbrace{\mathbb{Z}_p \oplus \dots \oplus \mathbb{Z}_p}_{t_k} & \text{if } k > j, \end{cases}$$

and hence

$$\frac{p^j A}{p^{j+1} A} \cong \underbrace{0 \oplus \dots \oplus 0}_j \oplus \underbrace{\mathbb{Z}_p \oplus \dots \oplus \mathbb{Z}_p}_{t_{j+1} + \dots + t_\alpha}.$$

In particular

$$\left| \frac{p^j A}{p^{j+1} A} \right| = p^{t_{j+1} + \dots + t_\alpha}.$$

This shows that each of the numbers  $s_1 = t_1 + \dots + t_\alpha$ ,  $s_2 = t_2 + \dots + t_\alpha$ ,  $\dots$ ,  $s_\alpha = t_\alpha$  is uniquely determined by  $A$ . But then so are the numbers  $t_1 = s_1 - s_2$ ,  $t_2 = s_2 - s_3$ ,  $\dots$ ,  $t_\alpha = s_\alpha$ . ■

We can summarise Theorems 12.4 and 12.6 into the following

**Theorem 12.7. (The fundamental theorem for finite abelian groups)**

*Every finite abelian group  $G$  is isomorphic to a direct sum of cyclic groups, each of which has a prime power order, and any two such decompositions of  $G$  have the same numbers of summands of each order.*

**Remark 12.8.** The above theorem can be generalised to finitely generated (possibly infinite) abelian groups: every finitely generated abelian group is isomorphic to a direct sum of cyclic groups, each of which is either isomorphic to  $\mathbb{Z}$  or has a prime power order.

**Example 12.9.** By Theorem 12.7, the following is the list of all non-isomorphic abelian groups of order  $1800 = 2^3 3^2 5^2$ :

$$\begin{aligned}
 &\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \\
 &\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{25} \\
 &\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \\
 &\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_{25} \\
 &\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \\
 &\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{25} \\
 &\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \\
 &\mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_{25} \\
 &\mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \\
 &\mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{25} \\
 &\mathbb{Z}_8 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5 \\
 &\mathbb{Z}_8 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_{25}
 \end{aligned}$$

The largest order of an element in each of these groups is the lowest common multiple of the prime powers which occur: respectively  $lcm(2, 3, 5) = 2 \cdot 3 \cdot 5 = 30$ ,  $lcm(2, 3, 25) = 2 \cdot 3 \cdot 25 = 150$ ,  $2 \cdot 9 \cdot 5 = 90$ ,  $2 \cdot 9 \cdot 25 = 450$ ,  $4 \cdot 3 \cdot 5 = 60$ ,  $4 \cdot 3 \cdot 25 = 300$ ,  $4 \cdot 9 \cdot 5 = 180$ ,  $4 \cdot 9 \cdot 25 = 900$ ,  $8 \cdot 3 \cdot 5 = 120$ ,  $8 \cdot 3 \cdot 25 = 600$ ,  $8 \cdot 9 \cdot 5 = 360$  and  $8 \cdot 9 \cdot 25 = 1800$ .

This observation can be useful in proving that two groups are non-isomorphic.