

## 14 Finite abelian groups

When dealing exclusively with abelian groups it is customary to use *additive notation*. An abelian group whose operation is written as addition is called an *additive group*.

multiplicative notation	additive notation	comments
$G, H, K, N$	$A, B, C$	new names of groups
$gh$	$a + b$	operation is now addition
$e = 1$	$0$	$0$ is the neutral element
$g^{-1}$	$-a$	inverse is given by minus
$g^n = 1$	$na = 0$	if $g$ , resp. $a$ , has order $n$
$f(gh) = f(g)f(h)$	$f(a + b) = f(a) + f(b)$	$f$ is a homomorphism
$HK$	$A + B$	$A + B$ is always a subgroup
$A \times B$	$A \oplus B$	same set, different operation
$H \leq G, N \trianglelefteq G$		all subgroups are normal

**Definition 14.1.** If  $A, B$  are additive groups then the *external direct sum*  $A \oplus B$  is the cartesian product  $A \times B$  considered as an additive group under coordinate-wise addition:

$$(a, b) + (a', b') = (a + a', b + b')$$

**Theorem 14.2.** Suppose that  $A, B$  are subgroups of an additive group  $C$  satisfying the following two conditions.

1.  $A \cap B = 0$  (Note: by  $0$  we actually mean  $\{0\}$ .)
2.  $A + B = C$  ( $A + B = \{a + b \mid a \in A, b \in B\}$ )

Then  $C$  is isomorphic to the direct sum  $A \oplus B$ .

**Definition 14.3.** Under the conditions of the above theorem we say that  $C$  is the *internal direct sum* of  $A$  and  $B$  and we write:

$$C = A \oplus B.$$

*Proof.* We will use the first isomorphism theorem. Let

$$\phi : A \oplus B \rightarrow C$$

be given by  $\phi(a, b) = a + b$ .

1.  $\phi$  is a homomorphism:

$$\phi((a, b) + (a', b')) = \phi(a + a', b + b') = a + a' + b + b'$$

$$\phi(a, b) + \phi(a', b') = a + b + a' + b'$$

These are equal since addition is commutative in  $C$ .

2.  $\ker \phi = \{(a, b) \mid \phi(a, b) = a + b = 0\}$  But  $a + b = 0$  implies that  $a = -b \in A \cap B = 0$  so  $a = b = 0$  and  $\ker \phi = 0$ .
3.  $\text{im } \phi = \{a + b \mid a \in A, b \in B\} = A + B = C$

By the first isomorphism theorem we have:

$$A \oplus B \cong \frac{A \oplus B}{\ker \phi} \cong \text{im } \phi = C$$

□

The main theorem about finite abelian groups is the following.

**Theorem 14.4 (Fundamental theorem of finite abelian groups).** *Every finite additive group is a direct sum of cyclic groups of prime power order.*

The proof of this theorem is in two steps.

1. Every finite additive group is a direct sum of  $p$ -groups.
2. Every finite  $p$ -group is a direct sum of cyclic groups.

These two lemmas will imply the theorem because internal direct sum ( $\oplus$ ) is commutative and associative (and external direct sum is commutative and associative up to isomorphism). For example, if  $A$  has order 36 and  $A = P \oplus Q$  where  $P$  is a 2-group and  $Q$  is a 3-group and  $P \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$ ,  $Q \cong \mathbb{Z}_3 \oplus \mathbb{Z}_3$  then

$$A = P \oplus Q \cong (\mathbb{Z}_2 \oplus \mathbb{Z}_2) \oplus (\mathbb{Z}_3 \oplus \mathbb{Z}_3) \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3.$$

The first step is something we already did. The same argument that we used to prove that

$$\mathbb{Z}_{nm} \cong \mathbb{Z}_n \times \mathbb{Z}_m$$

for  $n, m$  relatively prime proves the following.

**Lemma 14.5.** *Suppose that  $A$  is a finite additive group of order  $nm$  where  $(n, m) = 1$ . Then  $A$  is a direct sum of two subgroups:*

$$A = B \oplus C$$

where  $|B| = n$  and  $|C| = m$ .

*Proof.* We use the fact that multiplication by  $n$  is a homomorphism:

$$n(a + b) = na + nb$$

Let  $B, C$  be subsets of  $A$  given by

$$\begin{aligned} B &= \{x \in A \mid nx = 0\} \\ C &= \{x \in A \mid mx = 0\} \end{aligned}$$

These are subgroups of  $A$  since they are the kernels of the homomorphisms given by multiplication by  $n$  and multiplication by  $m$ . We want to show that  $A = B + C$  using Theorem 14.2.

Since  $(n, m) = 1$  there are integers  $a, b$  so that

$$an + bm = 1$$

This implies that, for any  $x \in A$ ,

$$x = 1x = (an + bm)x = anx + bmx$$

But,  $anx \in C$  since  $m(anx) = a(mnx) = 0$ . (The order of  $x$  divides  $|A| = mn$ .) Also  $bm x \in B$  since  $n(bmx) = b(nmx) = 0$ . Therefore,

$$A = B + C.$$

We just need to show that  $B \cap C = 0$ . So, suppose that  $x \in B \cap C$ . Then  $nx = 0 = mx$  so  $x = anx + bmx = 0 + 0 = 0$ .  $\square$

**Theorem 14.6.** *Suppose that  $A$  is an additive group of order  $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$  where  $p_1, \dots, p_k$  are distinct primes. Then*

$$A = P_1 \oplus P_2 \oplus \cdots \oplus P_k$$

where  $P_i$  is a  $p_i$ -group of order  $p_i^{e_i}$ .

*Proof.* Since  $p_1^{e_1}$  is relatively prime to  $p_2^{e_2} \cdots p_k^{e_k}$ , Lemma 14.5 gives us subgroups  $B, C$  of order  $p_1^{e_1}$  and  $p_2^{e_2} \cdots p_k^{e_k}$  so that

$$A = B \oplus C$$

By induction on the number of prime factors,  $C$  is also a direct sum of  $p$ -groups. This proves the theorem.  $\square$

The proof of Lemma 14.5 also gives us a formula for each group  $P_i$ :

$$P_i = \{x \in A \mid o(x) \text{ is a power of } p_i\}$$

## 14.1 Pure subgroups

The second step in the proof of the fundamental theorem uses pure subgroups. I defined them both in general and for the particular case of  $p$ -groups where they are needed.

**Definition 14.7 (general def of pure subgroup).** A subgroup  $P$  of an additive group  $A$  is called *pure* if any element of  $P$  which is divisible by any positive integer  $n$  in  $A$  is also divisible by  $n$  in  $P$ . In symbols:  $P$  is pure if  $\forall x \in P, \forall y \in A$  and  $\forall n \geq 1$  in  $\mathbb{Z}$  so that  $x = ny$ , there exists an element  $z \in P$  so that  $x = nz$ . In the book this condition is written:

$$nP = P \cap nA.$$

$P \cap nA$  is the set of all elements of  $P$  which are divisible by  $n$  in  $A$  and  $nP$  is the set of all elements of  $P$  divisible by  $n$  in  $P$ .

**Example 14.8.** Let  $A = \mathbb{Z}_6 = \{0, \bar{1}, \dots, \bar{5}\}$ . Then  $P = \{0, \bar{3}\}$  is pure. For example,  $x = \bar{3} \in P$  is divisible by  $n = 3$  in  $A$  since  $y = \bar{1} \in A$  and  $3y = x$ . Since  $P$  is pure, the element  $x$  must also be divisible by 3 in  $P$  and it is since  $x = 3x$ . ( $9 \equiv 3 \pmod{6}$ ) To prove that  $P$  is pure, note that  $x = \bar{3}$  is divisible in  $P$  by any odd number (since  $x^{2n+1} = x$ ) and is not divisible by any even number in either  $P$  or  $A$ . (Only  $\bar{2}, \bar{4}$  and 0 are divisible by even numbers.)

The book only defines purity for  $p$ -groups. This is because, in  $p$ -groups divisibility by all integers relatively prime to  $p$  is assured.

**Definition 14.9 (def of purity for  $p$ -groups).** A subgroup  $P$  of a  $p$ -group  $A$  is *pure* if, for any  $x \in P$  and any  $y \in A$  so that  $p^k y = x$  there is another element  $z \in P$  so that  $p^k z = x$ . In other words,  $x \in P$  is divisible by  $p^k$  in  $A$  if and only if it is divisible by  $p^k$  in  $P$ . In the book this condition is written as

$$p^k P = P \cap p^k A.$$

We are trying to prove the following theorem.

**Theorem 14.10.** *Every finite  $p$ -group is a direct sum of cyclic  $p$ -groups.*

This theorem is proved in two steps.

1. Every nontrivial finite  $p$ -group has a nontrivial cyclic pure subgroup.
2. If  $P$  is a pure subgroup of a finite  $p$ -group  $A$  then  $A = P \oplus Q$  for some subgroup  $Q$ .

**Lemma 14.11.** *Every nontrivial finite  $p$ -group  $A$  has a nontrivial cyclic pure subgroup  $P$ .*

*Proof.* Let  $a$  be an element of  $A$  with the largest possible order. Say,  $o(a) = p^k$ . This means that every other element of  $A$  has order  $p^i$  for some  $i \leq k$ . Let  $P = \langle a \rangle$ . Then

$$P = \{na \mid 0 \leq n < p^k\}.$$

I want to show that  $P$  is pure. First note that, to figure out the order of the element  $na$ , you have to factor the number  $n$ .

$$n = p^s m, \quad p \nmid m$$

Then  $o(na) = p^{k-s}$  since

$$p^{k-s} na = p^{k-s} p^s m a = p^k m a = 0$$

and lower powers of  $p$  don't work:

$$p^{k-s-1} na = p^{k-s-1} p^s m a = p^{k-1} m a \neq 0 \quad \text{since } o(a) = p^k \nmid p^{k-1} m.$$

Suppose that  $x = na \in P$  and  $y \in A$  so that  $p^j y = x$ . Then I have to find another element  $z \in P$  so that  $p^j z = x$ . I can assume that  $x$  is not zero since 0 is divisible ( $0 = p^j z$  for  $z = 0 \in P$ ).

Suppose that  $o(y) = p^i$ . Then  $j < i \leq k$  and the order of  $x = na = p^j y$  must be  $p^{i-j}$ . But then in the prime factorization  $n = p^s m$  we must have

$$o(na) = p^{k-s} = p^{i-j}$$

so  $k - s = i - j$  and  $s = k + j - i$ . This means that

$$x = na = p^{k+j-i} ma = p^j (p^{k-i} ma) = p^j z \quad \text{where } z = p^{k-i} ma \in P.$$

□

We need one more lemma which we do in two stages.

**Lemma 14.12.** *Suppose that  $a \in A$  and  $na = 0$ . Then there exists a unique homomorphism*

$$f : \mathbb{Z}/n \rightarrow A$$

so that  $f(\bar{1}) = a$ .

*Proof.* There is no choice about  $f$ . It must be given by

$$f(\bar{m}) = ma$$

But we need to show that this is well-defined.

Suppose that the same element can be written in a different way:

$$\bar{m} = \bar{m}' \in \mathbb{Z}/n$$

Then  $m' = m + kn$  for some integer  $k$  and

$$f(\bar{m}') = m'a = (m + kn)a = m + kna = ma = f(\bar{m}).$$

□

**Lemma 14.13.** *Suppose that  $C_1, C_2, \dots, C_k$  are cyclic groups of order  $n_1, \dots, n_k$  with generators  $x_1, \dots, x_k$ . In other words,*

$$C_i = \langle x_i \rangle \cong \mathbb{Z}/n_i.$$

*Suppose  $A$  is any additive group. Suppose you have elements  $a_1, a_2, \dots, a_k$  in  $A$  so that*

$$n_i a_i = 0$$

*for all  $i$ . Then there exists a unique homomorphism*

$$f : C_1 \oplus C_2 \oplus \dots \oplus C_k \rightarrow A$$

*so that  $f(x_1, 0, \dots, 0) = a_1, f(0, x_2, 0, \dots, 0) = a_2$ , etc.*

*Proof.* This is easy. The elements of  $C_1 \oplus \cdots \oplus C_k$  are given by  $(m_1x_1, m_2x_2, \dots, m_kx_k)$  and the homomorphism  $f$  must be given by

$$f(m_1x_1, m_2x_2, \dots, m_kx_k) = m_1a_1 + \cdots + m_k a_k.$$

This is well-defined for the same reason as Lemma 14.12 □

Now we will prove Theorem 14.10 by induction on the size of the group. There is only one step left (step 2), but we need the theorem itself as an induction hypothesis.

**Lemma 14.14.** *Suppose that  $P$  is a nontrivial pure subgroup of a finite  $p$ -group  $A$  and suppose that we are given that all  $p$ -groups of order less than that of  $A$  are direct sums of cyclic groups. Then*

$$A = P \oplus Q$$

for some subgroup  $Q$  of  $A$ .

*Proof.* The quotient group  $A/P$  is smaller than  $A$ . Thus,  $A/P$  is a direct sum of cyclic groups

$$A/P \cong C_1 \oplus C_2 \oplus \cdots \oplus C_k$$

where  $C_i$  is cyclic of order  $n_i = p^{e_i}$  with generators  $x_i$ . Since  $x_i \in A/P$  its true form is

$$x_i = y_i + P$$

The condition  $p^{e_i}x_i = 0$  means that

$$p^{e_i}y_i \in P$$

But  $P$  is pure. So there is another element  $z_i \in P$  so that

$$p^{e_i}z_i = p^{e_i}y_i \quad \text{or} \quad p^{e_i}(y_i - z_i) = 0$$

By the lemma this implies that there is a homomorphism

$$f : A/P = C_1 \oplus \cdots \oplus C_k \rightarrow A$$

so that  $f(x_i) = y_i - z_i$ . The composition

$$q \circ f : A/P = C_1 \oplus \cdots \oplus C_k \xrightarrow{f} A \xrightarrow{q} A/P$$

sends each  $x_i$  to  $y_i - z_i + P = y_i + P = x_i$  so it is the identity mapping on  $A/P$ . Therefore,  $f$  is a monomorphism with image  $Q = f(A/P)$ . Then I claim that

$$A = P \oplus Q.$$

1.  $P \cap Q = 0$ : Suppose that  $x \in P \cap Q$ .  $x \in P \Rightarrow q(x) = 0$ ,  $x \in Q = f(A/P)$  implies  $x = f(z)$ . But  $qf(z) = z = q(x) = 0$  so  $x = f(0) = 0$ .
2.  $A = P + Q$ : Take any  $x \in A$ . Then

$$x = (x - fq(x)) + fq(x) \in P + Q.$$

$(x - fq(x)) \in P = \ker q$  since  $q(x - fq(x)) = qx - qfq(x) = 0$  and  $fq(x) \in \text{im}(f) = Q$ .)

□

## 14.2 Fancy language

There is a fancy way to say that same thing that we just did. We have a *short exact sequence*

$$0 \rightarrow P \rightarrow A \rightarrow A/P \rightarrow 0.$$

The word *exact* means the image of each map is the kernel of the next one. The mapping  $f : A/P \rightarrow A$  is called a *splitting* of the map  $q : A \rightarrow A/P$  and we say that the short exact sequence *splits*. When a short exact sequence splits, the middle terms is a direct sum of the two end terms:

$$A \cong P \oplus A/P$$

So the theorem that we just proved can be stated as follows.

**Theorem 14.15.** *A short exact sequence  $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$  of finite abelian groups splits if  $A$  maps to a pure subgroup of  $B$ .*

(Actually we only proved this for  $p$ -groups but the same proof works for any finite group.)