Appendix A

The Structure of Finite Abelian Groups

A.1 The Structure Theorem

Theorem A.1. *Every finite abelian group A can be expressed as a direct sum of cyclic groups of prime-power order:*

$$A = \mathbb{Z}/(p_1^{e_1}) \oplus \cdots \oplus \mathbb{Z}/(p_r^{e_r}).$$

Moreover the powers $p_1^{e_1}, \ldots, p_r^{e_r}$ are uniquely determined by A.

Note that the primes $p_1, \ldots, p_r$ are not necessarily distinct.

We prove the result in two parts. First we divide A into its primary components A_p. Then we show that each of these components is expressible as a direct sum of cyclic groups of prime-power order.

A.2 Primary decomposition

Proposition A.1. *Suppose A is a finite abelian group. For each prime p, the elements of order p^n in A for some $n \in N$ form a subgroup*

$$A_p = \{a \in A : p^n a = 0 \text{ for some } n \in \mathbb{N}\}.$$

Proof. Suppose $a, b \in A_p$. Then

$$p^m a = 0, \; p^n b = 0,$$

for some m, n. Hence

$$p^{m+n}(a + b) = 0,$$

and so $a + b \in A_p$. $\square$

Definition A.1. *We call the* A_p *the* primary components *or* p-component *of* A.

Proposition A.2. *A finite abelian group* A *is the direct sum of its primary components* A_p*:*

$$F = \oplus_p A_p.$$

Proof. Suppose $a \in A$ By Lagrange's Theorem, $na = 0$ for some $n > 0$ Let

$$n = p_1^{e_1} \cdots p_r^{e_r};$$

and set

$$m_i = n/e_i^{p_i}.$$

Then $\gcd(m_1, \ldots, m_r) = 1$, and so we can find $n_1, \ldots, n_r$ such that

$$m_1 n_1 + \cdots + m_r n_r = 1.$$

Thus

$$a = a_1 + \cdots + a_r,$$

where

$$a_i = m_i n_i a.$$

But

$$p_i^{e_i} a_i = (p_i^{e_i} m_i) n_i a = n n_i a = 0$$

(since $na = 0$). Hence

$$a_i \in A_{p_i}.$$

Thus A is the sum of the subgroups A_p.

To see that this sum is direct, suppose

$$a_1 + \cdots + a_r = 0,$$

where $a_i \in A_{p_i}$, with distinct primes $p_1, \ldots, p_r$. Suppose

$$p_i^{e_i} a_i = 0.$$

Let

$$m_i = p_1^{e_1} \cdots p_{i-1}^{e_{i-1}} p_{i+1}^{e_{i+1}} \cdots p_r^{e_r}.$$

Then

$$m_i a_j = 0 \text{ if } i \neq j.$$

Thus (multiplying the given relation by m_i),

$$m_i a_i = 0.$$

But $\gcd(m_i, p_i^{e_i}) = 1$. Hence we can find m, n such that

$$m m_i + n p_i^{e_i} = 1.$$

But then

$$a_i = m(m_i a_i) + n(p_i^{e_i} a_i) = 0.$$

We conclude that A is the direct sum of its p-components A_p. □

Proposition A.3. *If* A *is a finite abelian group then* $A_p = 0$ *for almost all* p*, ie for all but a finite number of* p.

Proof. If A has order n then by Lagrange's Theorem the order of each element $a \in A$ divides n. Thus $A_p = 0$ if $p \nmid n$. □

A.3 Decomposition of the primary components

We suppose in this Section that A is a finite abelian p-group (ie each element is of order p^e for some e).

Proposition A.4. *A can be expressed as a direct sum of cyclic p-groups:*

$$A = \mathbb{Z}/(p^{e_1}) \oplus \cdots \oplus \mathbb{Z}/(p^{e_r}).$$

Proof. We argue by induction on $\#(A) = p^n$. We may assume therefore that the result holds for the subgroup

$$pA = \{pa : a \in A\}.$$

For pA is stricty smaller than A, since

$$pA = A \implies p^n A = A,$$

while we know from Lagrange's Theorem that $p^n A = 0$.

Suppose

$$pA = \langle pa_1 \rangle \oplus \cdots \oplus \langle pa_r \rangle.$$

Then the sum

$$\langle a_1 \rangle + \cdots + \langle a_r \rangle = B,$$

say, is direct. For suppose

$$n_1 a_1 + \cdots + n_r a_r = 0.$$

If $p \mid n_1, \ldots, n_r$, say $n_i = pm_i$, then we can write the relation in the form

$$m_1(pa_1) + \cdots + m_r(pa_r) = 0,$$

whence $m_i pa_i = n_i a_i = 0$ for all i.

On the other hand, if p does not divide all the n_i then

$$n_1(pa_1) + \cdots + n_r(pa_r) = 0,$$

and so $pn_i a_i = 0$ for all i. But if $p \nmid n_i$ this implies that $pa_i = 0$. (For the order of a_i is a power of p, say p^e; while $p^e \mid n_i p$ implies that $e \leq 1$.) But this contradicts our choice of pa_i as a generator of a direct summand of pA. Thus the subgroup $B \subset A$ is expressed as a direct sum

$$B = \langle a_1 \rangle \oplus \cdots \oplus \langle a_r \rangle.$$

Let

$$K = \{a \in A : pa = 0\}.$$

Then

$$A = B + K.$$

For suppose $a \in A$. Then $pa \in pA$, and so

$$pa = n_1(pa_1) + \cdots + n_r(pa_r)$$

for some $n_1, \ldots, n_r \in \mathbb{Z}$. Thus

$$p(a - n_1 a_1 - \cdots - n_r a_r) = 0,$$

and so

$$a - n_1 a_1 - \cdots - n_r a_r = k \in K.$$

Hence

$$a = (n_1 a_1 + \cdots + n_r a_r) + k \in B + K.$$

If $B = A$ then all is done. If not, then $K \not\subset B$, and so we can find $k_1 \in K, k_1 \notin B$. Now the sum

$$B_1 = B + \langle k_1 \rangle$$

is direct. For $\langle k_1 \rangle$ is a cyclic group of order p, and so has no proper subgroups. Thus

$$B \cap \langle k_1 \rangle = \{0\},$$

and so

$$B_1 = B \oplus \langle k_1 \rangle$$

If now $B_1 = A$ we are done. If not we can repeat the construction, by choosing $k_2 \in K, k_2 \notin B_1$. As before, this gives us a direct sum

$$B_2 = B_1 \oplus \langle k_2 \rangle = B \oplus \langle k_1 \rangle \oplus \langle k_2 \rangle.$$

Continuing in this way, the construction must end after a finite number of steps (since A is finite):

$$\begin{aligned} A = B_s &= B \oplus \langle k_1 \rangle \oplus \cdots \oplus \langle k_s \rangle \\ &= \langle a_1 \rangle \oplus \cdots \oplus \langle a_r \rangle \oplus \langle k_1 \rangle \oplus \cdots \oplus \langle k_s \rangle. \end{aligned}$$

□

A.4 Uniqueness

Proposition A.5. *The powers $p^{e_1}, \ldots, p^{e_r}$ in the above decomposition are uniquely determined by A.*

Proof. This follows by induction on $\#(A)$. For if A has the form given in the theorem then

$$pA = \mathbb{Z}/(p^{e_1 - 1}) \oplus \cdots \oplus \mathbb{Z}/(p^{e_r - 1}).$$

Thus if $e > 1$ then $\mathbb{Z}/(p^e)$ occurs as often in A as $\mathbb{Z}/(p^{e-1})$ does in pA. It only remains to deal with the factors $\mathbb{Z}/(p)$. But the number of these is now determined by the order $\|A\|$ of the group. □

A.5 Note

Note that while the Structure Theorem states that A can be expressed as a direct sum of cyclic subgroups of prime-power order, these subgroups will not in general be unique, although their orders will be.

The only case in which the expression will be unique is if A is cyclic, ie if $A = \mathbb{Z}/(n)$. For in this case each p-component A_p is also cyclic, since every subgroup of a cyclic abelian group is cyclic. Thus the expression for A as a direct sum in the Theorem is just the splitting of A into its p-components A_p; and we know that this is unique.

Conversely, if A is not cyclic, then some component A_p is not cyclic, and we have seen that in this case the splitting is not unique.