11 Fundamental Theorem of Finite Abelian Groups

Fundamental Theorem of Finite Abelian Groups

Every finite Abelian group is a direct product of cyclic groups of prime-power order. Moreover, the number of terms in the product and the orders of the cyclic groups are uniquely determined by the group.

First proved by Leopold Kronecker in 1858

Significance of the Theorem

- Reduces questions about finite Abelian groups to questions about cyclic groups
- Combined with Chapter 4 results, usually yields complete answers
- Every finite Abelian group G is isomorphic to:
  $Z_{p_1^{n_1}} \oplus Z_{p_2^{n_2}} \oplus \cdots \oplus Z_{p_k^{n_k}}$
- Prime powers $p_1^{n_1}, p_2^{n_2}, \ldots, p_k^{n_k}$ are uniquely determined by G
- This representation determines the isomorphism class of G

Isomorphism Classes of Abelian Groups

For groups of order p^k (p prime):

- One group for each partition of k (set of positive integers that sum to k)
- For partition $k = n_1 + n_2 + \cdots + n_j$, we get: $Z_{p^{n_1}} \oplus Z_{p^{n_2}} \oplus \cdots \oplus Z_{p^{n_j}}$
- Distinct partitions yield distinct isomorphism classes

Examples: Groups of Order p^k where $k \leq 4$

Order of G	Partitions of k	Possible direct products for G
p	1	Z_p
p^2	2	Z_{p^2}
	1+1	$Z_p \oplus Z_p$
p^3	3	Z_{p^3}
	2+1	$Z_{p^2} \oplus Z_p$
	1+1+1	$Z_p \oplus Z_p \oplus Z_p$

p^4	4	Z_{p^4}
	3+1	$Z_{p^3} \oplus Z_p$
	2+2	$Z_{p^2} \oplus Z_{p^2}$
	2+1+1	$Z_{p^2} \oplus Z_p \oplus Z_p$
	1+1+1+1	$Z_p \oplus Z_p \oplus Z_p \oplus Z_p$

Facts about External direct products:

- **Commutative property:** $A \oplus B \approx B \oplus A$.
- **Isomorphism invariance:** If $A \approx B$ and $C \approx D$, then $A \oplus C \approx B \oplus D$.
- **Cancellation property:** If A is finite, then $A \oplus B \approx A \oplus C$ *iff* $B \approx C$.

Example: $Z_4 \oplus Z_4$ is not isomorphic to $Z_4 \oplus Z_2 \oplus Z_2$, because Z_4 is not isomorphic to $Z_2 \oplus Z_2$.

General Construction Method:

To construct all the Abelian groups of a certain order n,

1. Begin by writing $n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$. Next, we
2. Individually form all Abelian groups of order $p_1^{n_1}$, then $p_2^{n_2}$, and so on, as described earlier.
3. Finally, form all possible external direct products of these groups.

Example: let $n = 1176 = 2^3 \cdot 3 \cdot 7^2$. Then, the complete list of the distinct isomorphism classes of Abelian groups of order 1176 is

2^3	3	7^2
Z_{2^3}	Z_3	Z_{7^2}
$Z_{2^2} \oplus Z_{2^1}$		$Z_7 \oplus Z_7$
$Z_{2^1} \oplus Z_{2^1} \oplus Z_{2^1}$		

$$Z_{2^3} \oplus Z_3 \oplus Z_{7^2},$$
$$Z_{2^2} \oplus Z_2 \oplus Z_3 \oplus Z_{7^2},$$
$$Z_2 \oplus Z_2 \oplus Z_2 \oplus Z_3 \oplus Z_{7^2},$$
$$Z_{2^3} \oplus Z_3 \oplus Z_7 \oplus Z_7,$$
$$Z_{2^2} \oplus Z_2 \oplus Z_3 \oplus Z_7 \oplus Z_7,$$
$$Z_2 \oplus Z_2 \oplus Z_2 \oplus Z_3 \oplus Z_7 \oplus Z_7.$$

Now given a particular Abelian group G of order 1176, then to know which of the six is G isomorphic to, compare the orders of the elements of G with the orders of the elements in the six direct products, since it can be shown that: **Two finite Abelian groups are isomorphic if and only if they have the same number of elements of each order**.

Identifying a Group's Isomorphism Class

To determine which isomorphism class a given Abelian group G belongs to:

- Compare the orders of elements in G with those in possible direct products
- Two finite Abelian groups are isomorphic if and only if they have the same number of elements of each order.
- Example: If G has elements of order 8, it must be isomorphic to a group containing Z_8 so only the first and the fourth groups work.

Example 1: Internal Direct Product

G = {1, 8, 12, 14, 18, 21, 27, 31, 34, 38, 44, 47, 51, 53, 57, 64} under multiplication modulo 65

Element	1	8	12	14	18	21	27	31	34	38	44	47	51	53	57	64
Order	1	4	4	2	4	4	4	4	4	4	4	4	2	4	4	2

- G has order 16, so it must be isomorphic to one of:
  $Z_{16}, Z_8 \oplus Z_2, Z_4 \oplus Z_4, Z_4 \oplus Z_2 \oplus Z_2, Z_2 \oplus Z_2 \oplus Z_2 \oplus Z_2$
- The table rules out all but $Z_4 \oplus Z_4$ and $Z_4 \oplus Z_2 \oplus Z_2$ as possibilities.
- Since $Z_4 \oplus Z_2 \oplus Z_2$ has a subgroup isomorphic to $Z_2 \oplus Z_2 \oplus Z_2$, it has more than three elements of order 2, and therefore we must have $G \approx Z_4 \oplus Z_4$.

Example 2: Internal Direct Product

G = {1, 8, 17, 19, 26, 28, 37, 44, 46, 53, 62, 64, 71, 73, 82, 89, 91, 98, 107, 109, 116, 118, 127, 134} under multiplication modulo 135

- G has order 24, so it must be isomorphic to one of:

$$Z_8 \oplus Z_3 \approx Z_{24},$$
$$Z_4 \oplus Z_2 \oplus Z_3 \approx Z_{12} \oplus Z_2,$$
$$Z_2 \oplus Z_2 \oplus Z_2 \oplus Z_3 \approx Z_6 \oplus Z_2 \oplus Z_2.$$

- Direct calculations show $|8| = 12$ and $|109| = 2 = |134|$ (Two elements of order 2)
- G must be $Z_{12} \oplus Z_2$
- Internal direct product: G = $\langle 8 \rangle \times \langle 134 \rangle$

Alternative Direct Product Form

- Often more convenient to combine cyclic factors of relatively prime order
- Example: $Z_4 \oplus Z_4 \oplus Z_2 \oplus Z_9 \oplus Z_3 \oplus Z_5$ would be written as $Z_{180} \oplus Z_{12} \oplus Z_2$
- We can always obtain a direct product of the form $Z_{n_1} \oplus Z_{n_2} \oplus \cdots \oplus Z_{n_k}$, where n_{i+1} divides n_i.

Corollary Existence of Subgroups of Abelian Groups

If m divides the order of a finite Abelian group G, then G has a subgroup of order m.

Proof: Let G be finite Abelian with $|G| = n$ and let $m \mid n$. Induct on n.

- Base case: $n = 1$ or $m = 1$ are trivial.
- Choose a prime $p \mid m$.
- By Theorem 11.1 (and properties of cyclic groups), G has a subgroup K with $|K| = p$.
- Then G/K is Abelian of order n/p, and $m/p \mid |G/K|$.
- By induction, G/K has a subgroup H/K with $|H/K| = m/p$, for some $K \leq H \leq G$.
- Hence $|H| = |H/K||K| = (m/p) \cdot p = m$. So G has a subgroup of order m.

Lemma 1

If $|G| = p^n m$ *with* $\gcd(p, m) = 1$, *then* $G = H \times K$, *where*

$$H = \{x \in G \mid x^{p^n} = e\}, \qquad K = \{x \in G \mid x^m = e\},$$

and $|H| = p^n$.

Complete proof.

1. **Subgroups.** Both sets are kernels of the maps $x \mapsto x^{p^n}$ and $x \mapsto x^m$; kernels are subgroups.
2. **Product is the whole group.**
   By Bézout, $1 = sp^n + tm$. For any $x \in G$,
   $$x = x^1 = x^{sp^n + tm} = x^{sp^n} x^{tm} \in HK.$$
   Hence $G = HK$.
3. **Trivial intersection.**
   If $x \in H \cap K$ then $x^{p^n} = e = x^m$. Order of x divides both p^n and m; by coprimality it must be 1.
4. **Orders.** Since $|G| = |H||K|$ and p does not divide $|K|$ (all elements of K have orders dividing m), it follows that $|H| = p^n$.

Lemma 2

If $|G| = p^n$ and a has maximal order p^m, then $G = \langle a \rangle \times K$ for some subgroup K.

Complete proof.

- **Induction on n.** The case $n = 1$ is trivial. Assume true for groups of order p^k with $k < n$.
- Pick $b \notin \langle a \rangle$ of *minimal* positive order. Show that $|b| = p$:
  - If $b^p = a^i$ then $|a^i| \leq p^{m-1}$. Since a is of maximal order, $p \mid i$; write $i = pj$.
  - Define $c = a^{-j}b$. Then $c^p = e$ but $c \notin \langle a \rangle$. Minimality forces $|b| = |c| = p$.
- Thus $\langle a \rangle \cap \langle b \rangle = \{e\}$.
- Consider $G/\langle b \rangle$ (order p^{n-1}). The coset $\overline{a}$ still has order p^m (else its order divides p^{m-1}, contradicting maximality). By the induction hypothesis

$$G/\langle b \rangle = \langle \overline{a} \rangle \times \overline{K}$$

  for some $\overline{K}$. Pulling $\overline{K}$ back to G gives a subgroup K with $G = \langle a \rangle K$ and trivial intersection. Hence the internal direct product decomposition holds.

Lemma 2

If $|G| = p^n$ and a has maximal order p^m, then $G = \langle a \rangle \times K$ for some subgroup K.

Complete proof.

- **Induction on n.** The case $n = 1$ is trivial. Assume true for groups of order p^k with $k < n$.
- Pick $b \notin \langle a \rangle$ of *minimal* positive order. Show that $|b| = p$:
  - If $b^p = a^i$ then $|a^i| \leq p^{m-1}$. Since a is of maximal order, $p \mid i$; write $i = pj$.
  - Define $c = a^{-j}b$. Then $c^p = e$ but $c \notin \langle a \rangle$. Minimality forces $|b| = |c| = p$.
- Thus $\langle a \rangle \cap \langle b \rangle = \{e\}$.
- Consider $G/\langle b \rangle$ (order p^{n-1}). The coset $\overline{a}$ still has order p^m (else its order divides p^{m-1}, contradicting maximality). By the induction hypothesis

$$G/\langle b \rangle = \langle \overline{a} \rangle \times \overline{K}$$

for some $\overline{K}$. Pulling $\overline{K}$ back to G gives a subgroup K with $G = \langle a \rangle K$ and trivial intersection. Hence the internal direct product decomposition holds.

Lemma 3

A finite abelian p-group is an internal direct product of cyclic p-groups.

Proof.

Apply Lemma 2 repeatedly: choose a maximal-order element, split it off, work inside the complement.

Terminate after at most n steps.

Lemma 4 (Uniqueness)

Suppose

$$G = \langle h_1 \rangle \times \cdots \times \langle h_m \rangle = \langle k_1 \rangle \times \cdots \times \langle k_n \rangle,$$

with non-trivial cyclic p-groups arranged so that $|h_1| \geq \cdots \geq |h_m|$ and $|k_1| \geq \cdots \geq |k_n|$.

Then $m = n$ and $|h_i| = |k_i|$ for every i.

Proof of the Fundamental Theorem

1. **Primary decomposition.** Apply Lemma 1 recursively to split G as

$$G = G(p_1) \times \cdots \times G(p_r),$$

   where each factor has order a power of a single prime.

2. **Cyclic decomposition inside each primary component.**
   Lemma 3 writes every $G(p_i)$ as an internal direct product of cyclic p_i-groups.

3. **Uniqueness.** Lemma 4 shows those cyclic factors are unique up to order and permutation.□