Fundamental Theorem on Finite Abelian Groups

Theorem: 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 order of the cyclic groups are uniquely determined by the group.

$$G \approx \mathbb{Z}_{p_1^{n_1}} \oplus \mathbb{Z}_{p_2^{n_2}} \oplus \cdots \oplus \mathbb{Z}_{p_k^{n_k}}$$

where the p_i's are not necessarily distinct primes and the prime powers $p_1^{n_1}, p_2^{n_2}, \ldots, p_k^{n_k}$ are uniquely determined by G.

MTH 339

2/17

Application: We can construct all Abelian groups of any order.

Example: groups of order p^k, p is prime and $k \leq 4$

↪ we need to find the partitions of k

$$k = n_1 + n_2 + \cdots + n_t \quad \text{(each } n_i \text{ is a positive integer)}$$

$\mathbb{Z}_{p^{n_1}} \oplus \mathbb{Z}_{p^{n_2}} \oplus \cdots \oplus \mathbb{Z}_{p^{n_t}}$ is an Abelian group of order p^k.

order of	partitions of k	possible direct products for G
p	1	$\mathbb{Z}_p$
p^2	2	$\mathbb{Z}_{p^2}$
	$1+1$	$\mathbb{Z}_p \oplus \mathbb{Z}_p$
p^3	3	$\mathbb{Z}_{p^3}$
	$2+1$	$\mathbb{Z}_{p^2} \oplus \mathbb{Z}_p$
	$1+1+1$	$\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p$

p^4

4	$\mathbb{Z}_{p^4}$
$3+1$	$\mathbb{Z}_{p^3} \oplus \mathbb{Z}_p$
$2+2$	$\mathbb{Z}_{p^2} \oplus \mathbb{Z}_{p^2}$
$2+1+1$	$\mathbb{Z}_{p^2} \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p$
$1+1+1+1$	$\mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p$

Note that $\mathbb{Z}_9$ is not isomorphic to $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$.

If A is finite: $A \oplus B \approx A \oplus C$ if and only if $B \approx C$.

Now, if we are given n as the order of an Abelian group, we can write

$$n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$$

Then we find all Abelian groups of order $p_1^{n_1}$ individually, then of $p_2^{n_2}$, and so on.

Finally, we form all possible external products of these groups.

MTH 339

Example: Let $n = 1176 = 2^3 \cdot 3 \cdot 7^2$

Complete list of distinct isomorphism classes:

$\mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{49}$

$\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{49}$

$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{49}$

$\mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_7$

$\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_7$

$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_7$

How do we figue out for $|G| = 1176$ (an G Abelian) which isomorphism class it belongs to?

Two finite Abelian groups are isomorphic if and only if they have the same number of elements of each order.

Example: Let $G = \{1, 8, 12, 14, 18, 21, 27, 31, 34, 38, 44, 47, 51, 53, 57, 64\}$ under multiplication modulo 65. $|G| = 16$

So G is isomorphic to one of

$\mathbb{Z}_{16}$, $\mathbb{Z}_8 \oplus \mathbb{Z}_2$, $\mathbb{Z}_4 \oplus \mathbb{Z}_4$, $\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$, or $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

Next step: determine order of each element:

↪ $|1| = 1$, other elements have order 2 and 4.

So only $\mathbb{Z}_4 \oplus \mathbb{Z}_4$ or $\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ are possible.

Now $\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ has a subgroup isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$, so more than 3 elements of order 2 (but in G, there are only 3 elements of order 2). Thus, $G \approx \mathbb{Z}_4 \oplus \mathbb{Z}_4$.

How can we express G as an internal direct product? Pick an element of maximum order (here 4), then $\langle 8 \rangle$ is a factor in the product. Next, choose a second element a that has order 4 and $\langle a \rangle \cap \langle 8 \rangle = \{1\}$. 12 has this property, so $G = \langle 8 \rangle \times \langle 12 \rangle$.

Theorem 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: Suppose, G is Abelian and of order n and m divides n. We induct on the order of G, $n=1$ is trivial.
Let p divide m, then G has a subgroup K of order p. Then G/K is Abelian and $|G/K| = \frac{n}{p}$ and $\frac{m}{p}$ divides $\frac{n}{p}$.

By our assumption (induction), we know that G/K has a subgroup of the form H/K where H is a subgroup of G and $|H/K| = m/p$. Then $|H| = (|H|/|K|)|K|$

$$= \frac{m}{p} \cdot p = m.$$

$\square$

<u>Example</u>: Assume G is Abelian, $|G| = 72$ and we wish to produce a subgroup of order 12. G is isomorphic to one of the following groups

$\mathbb{Z}_8 \oplus \mathbb{Z}_9$, $\mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$, $\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$,
$\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9$, $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9$,
$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$.

Now, $\mathbb{Z}_8 \oplus \mathbb{Z}_9 \approx \mathbb{Z}_{72}$ and $\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \approx \mathbb{Z}_{12} \oplus \mathbb{Z}_6$ so both have a subgroup of order 12.

In $\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9$ we proceed as follows: Piece together $\mathbb{Z}_4$ and a subgroup of order 3 of $\mathbb{Z}_9$.

So $\{(a,0,b) \mid a \in \mathbb{Z}_4,\ b \in \{0,3,6\}\}$.

In $\mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$ this works in a similar way (→ do now!).

Proof of the Fundamental Theorem:

Lemma 1: Let G be a finite Abelian group of order $p^n m$, where p is a prime that does not divide m. Then $G = H \times K$, where
$H = \{x \in G \mid x^{p^n} = e\}$ and $K = \{x \in G \mid x^m = e\}$
Moreover, $|H| = p^n$.

Proof: Clearly, H and K are subgroups of G. Since G is Abelian, to prove $G = H \times K$, we need to show that $G = HK$ and $H \cap K = \{e\}$
Since $\gcd(m, p^n) = 1$, there are integers s and t such that $1 = sm + tp^n$.

MTH 339

For any x in G, we have

$$x = x^1 = x^{sm+tp^n} = x^{sm}x^{tp^n} \quad \text{and } |G| = p^n m$$

Then, $x^{sm} \in H$ and $x^{tp^n} \in K$

$$\left((x^{sm})^{p^n} = x^{smp^n} = (x^{mp^n})^s = (x^{|G|})^s = e^s = e \right)$$

$$\left((x^{tp^n})^m = x^{tmp^n} = (x^{|G|})^t = e \right)$$

Therefore, $x = x^{sm}x^{tp^n} \in HK$.

Now suppose $x \in H \cap K$. Then $x^{p^n} = e = x^m$ and $|x|$ needs to divide both p^n and m. Since p does not divide m, we have $|x| = 1$ and, therefore, $x = e$. This proves $G = H \times K$.

Now we show $|H| = p^n$.

$p^n m = |HK| = |H||K| / |H \cap K| = |H||K|$ and p does not divide $|K|$, so $|H| = p^n$

$\square$

Significance of this lemma: Given an Abelian G,
$|G| = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$ where the p's are distinct primes,
we let $G(p_i)$ denote the set $\{ x \in G \mid x^{p_i^{n_i}} = e \}$.
It follows from the above lemma that

$$G = G(p_1) \times G(p_2) \times \cdots \times G(p_k) \text{ and}$$

$|G(p_i)| = p_i^{n_i}$ (use induction)

Therefore, we can now turn our attention to groups of prime-power order.

Lemma 2: Let G be an Abelian group of prime-power order and let a be an element of maximum order in G. Then G can be written in the form $\langle a \rangle \times K$.

Proof: Assume $|G| = p^n$, induction on n.

If $n=1$, then $G = \langle a \rangle \times \langle e \rangle$.

Now assume that the statement is true for all Abelian groups of order p^k, with $k<n$.

Among all the elements of G, choose a of maximum order p^m, so $x^{p^m} = e$ for all x in G. Assume $G \neq \langle a \rangle$ (otherwise the statement is trivial). Among all the elements of G, choose b of smallest order such that $b \notin \langle a \rangle$.

<u>Claim</u>: $\langle a \rangle \cap \langle b \rangle = \{e\}$

First note that $|b^p| = |b|/p$, $|b| = p^\alpha = \xi$

(if $|b| = \xi$, we have $b^\xi = e$ and $(b^p)^\xi = e$ so $|b^p| = p^\alpha / p = |b| / p$)

Therefore, $b^p \in \langle a \rangle$ by the way b was chosen.

Say $b^p = a^i$ and, clearly, $e = b^{p^m} = (b^p)^{p^{m-1}} = (a^i)^{p^{m-1}}$, so $|a^i| \leq p^{m-1}$. Hence, a^i is not a generator of $\langle a \rangle$, and, therefore, see Corollary 3 of Thm 4.2 (p. 83), $\gcd(p^m, i) \neq 1$. Therefore, p divides i

and we can write $i = pj$. Then $b^p = a^i = a^{pj}$.

Consider now $c = a^{-j}b$. Clearly, $c \notin \langle a \rangle$ because if it was, b would be in $\langle a \rangle$ as well.

$$c^p = (a^{-j}b)^p \underset{\substack{\uparrow \\ \text{Abelian}}}{=} a^{-jp}\, b^p = a^{-i}\, b^p = e$$

Thus, we have found an element c of order p such that $c \notin \langle a \rangle$. Since b was chosen to have smallest order such that $b \notin \langle a \rangle$, we conclude that b also has order p.

From here, we see that $\langle a \rangle \cap \langle b \rangle = \{e\}$

(Assume $c \neq e$ and $c \in \langle a \rangle \cap \langle b \rangle$, so

$c = a^i = b^j$ with $1 \leq j < p$. Then, since p is prime, c generates $\langle b \rangle$. But then there is a k such that $c^k = b = (a^i)^k = a^{ik}$, so $b \in \langle a \rangle$ which contradicts the assumption that $b \notin \langle a \rangle$.

We consider now the factor group $\overline{G} = G/\langle b \rangle$.

Let $\overline{x}$ denote the coset $x\langle b \rangle$ in $\overline{G}$.

First, we show $|\overline{a}| = |a| = p^m$ (*)

<u>Proof:</u> Assume $|\overline{a}| < |a| = p^m$, then $(\overline{a})^{p^k} = \overline{e}$ with $k < m$. Then $(a\langle b \rangle)^{p^k} = a^{p^k}\langle b \rangle = \langle b \rangle$, so $a^{p^k} \in \langle a \rangle \cap \langle b \rangle = \{e\}$ and hence $a^{p^k} = e$ which leads to a contradiction.

Therefore, due to $|\overline{a}| = |a| = p^m$, $\overline{a}$ is an element of maximum order in $\overline{G}$. By induction, we know that $\overline{G} = \langle \overline{a} \rangle \times \overline{K}$ for some subgroup $\overline{K}$ of $\overline{G}$. Let K be the pullback of $\overline{K}$ under the natural homomorphism from G to $\overline{G}$ (so $K = \{x \in G \mid \overline{x} \in \overline{K}\}$). We claim $\langle a \rangle \cap K = \{e\}$. Note that if $x \in \langle a \rangle \cap K$, $\overline{x} \in \langle \overline{a} \rangle \cap \langle \overline{K} \rangle = \{\overline{e}\} = \langle b \rangle$ and $x \in \langle a \rangle \cap \langle b \rangle = \{e\}$. Therefore (ex 37) $G = \langle a \rangle K$ and hence $G = \langle a \rangle \times K$

$\square$

(Ex 37: $|\langle a\rangle K| = \dfrac{|a||K|}{|\langle a\rangle \cap K|} = |a||K|$

$= |a||\bar{K}|p = |\bar{G}|p = |G|$.)

Lemma 2 says that we can write any G (Abelian) of prime-power order as $G = \langle a\rangle \times K$.
We can iterate: Clearly K is Abelian and of prime-power order $\Rightarrow G = \langle a\rangle \times \langle a_1\rangle \times K_1$ and so on. So any Abelian group G, we can write

$$G = G(p_1) \times G(p_2) \times \cdots \times G(p_n)$$

where each $G(p_i)$ is a group of prime-power order and each of these factors is a internal direct product of cyclic group.
Therefore, all that is left to prove is the uniqueness of the factors.

<u>Lemma 4</u>: Suppose that G is a finite Abelian group of prime-power order. If $G = H_1 \times H_2 \times \cdots \times H_m$ and $G = K_1 \times K_2 \times \cdots \times K_n$, where the H's and K's are nontrivial cyclic subgroups with
$|H_1| \geq |H_2| \geq \cdots \geq |H_m|$ and $|K_1| \geq |K_2| \geq \cdots \geq |K_n|$, then $m = n$ and $|H_i| = |K_i|$ for all i.

<u>Proof</u>: We proceed by induction on $|G|$.

If $|G| = p$, there is nothing to prove.

Now suppose the statement is true for all Abelian groups of order less than $|G|$.

Note that, for any Abelian group L, the set $L^p = \{x^p \mid x \in L\}$ is a subgroup of L.

$G^p = H_1^p \times H_2^p \times \cdots \times H_{m'}^p$ and

$G^p = K_1^p \times K_2^p \times \cdots \times K_{n'}^p$

where m' is the largest integer i such that $|H_i| > p$ and n' is the largest integer j such that $|K_j| > p$ (this ensures that the two direct products for G^p do not have trivial factors).

Note that $|G^p| < |G|$ ($|G| = p^n$ and G^p is a proper subgroup)

Now we can use the induction assumption and it follows $m' = n'$ and $|H_i^p| = |K_i^p|$ for $i = 1, \dots, m'$. Since $|H_i| = p|H_i^p|$, it follows that $|H_i| = |K_i|$ for all $i = 1, \dots, m'$.

All that remains to be shown is that the number of H_i of order p equals the number of K_i of order p

Note: In the statement $|G^p| < |G|$ we use the following fact:

If L is an Abelian group, L^p is a subgroup of L. If L is finite and p divides n, then L^p is a proper subgroup.

To show that L^p is a proper subgroup, we need to show that the map $g \to g^p$ is not injective. From Cauchy's Theorem (9.5) we know that $\exists\, x \in L$ such that $x^p = e$ and $e^p = e$. So the map $g \to g^p$ is not one-to-one and, therefore, L^p is a proper subgroup.

MTH 339 - Do Now

1./ Construct a subgroup of order 12 in $\mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$. (see p.246)

2./ How many Abelian groups (up to isomorphism) are there of order 6?

3./ The symmetry group of a nonsquare rectangle is an Abelian group of order 4. Is it isomorphic to $\mathbb{Z}_4$ or $\mathbb{Z}_2 \oplus \mathbb{Z}_2$?

MTH 339 HW

1./ What is the smallest positive integer n such that there are exactly four nonisomorphic Abelian groups of order n? Name the four groups.

2./ Prove that any Abelian group of order 45 has an element of order 15. Does every Abelian group of order 45 have an element of order 9?

3./ 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.

4./ The set $\{1, 9, 16, 22, 29, 53, 74, 79, 81\}$ is a group under multiplication modulo 91. Determine the isomorphism class of this group.

5./ Determine the isomorphism class of

$(\mathbb{Z}_{16} \oplus \mathbb{Z}_{16}) / \langle (2,2) \rangle$.