Fundamental Theorem of Finite Abelian Groups

Th: Fundamental Theorem of finite Abelian group
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.

- The proof of this theorem is very large so before proof this theorem we solve some problem using this.

The Fundamental theorem is extremely powerful. As an application we can use it as an algorithem for constructing all Abelian group of any order. using this algorithem we can solve any problem about finite group.

- **Prob 1:** Let G be a group of order p^K ($K \leq 4$). and p is a prime. i.e. $|G| = p^K$. To find all possible isomorphic ~~group~~ direct product group of same order with G, first find set of all partition of K.

i.e. if $K = n_1 + n_2 + \cdots + n_t$
$= n_1' + n_2' + \cdots + n_t'$

Then
$$G \simeq \mathbb{Z}/p^{n_1} \oplus \mathbb{Z}/p^{n_2} \oplus \cdots \oplus \mathbb{Z}/p^{n_t}$$
$$\simeq \mathbb{Z}/p^{n_1'} \oplus \mathbb{Z}/p^{n_2'} \oplus \cdots \oplus \mathbb{Z}/p^{n_t'}.$$

each direct product are Abelian group of order p^K.

- Example:

	Order of G	partitions of K	possible direct product from G
For $K=1$	$\lvert G\rvert = p$	$1 = 1$	$\mathbb{Z}/p$
For $K=2$	$\lvert G\rvert = p^2$	$2 = 2$	$\mathbb{Z}/p^2$
		$= 1+1$	$\mathbb{Z}/p \oplus \mathbb{Z}/p$
For $K=3$	$\lvert G\rvert = p^3$	$3 = 3$	$\mathbb{Z}/p^3$
		$= 2+1$	$\mathbb{Z}/p^2 \oplus \mathbb{Z}/p$
		$= 1+1+1$	$\mathbb{Z}/p \oplus \mathbb{Z}/p \oplus \mathbb{Z}/p$
For $K=4$	$\lvert G\rvert = p^4$	$4 = 4$	$\mathbb{Z}/p^4$
		$= 3+1$	$\mathbb{Z}/p^3 \oplus \mathbb{Z}/p$
		$= 2+2$	$\mathbb{Z}/p^2 \oplus \mathbb{Z}/p^2$
		$= 2+1+1$	$\mathbb{Z}/p^2 \oplus \mathbb{Z}/p \oplus \mathbb{Z}/p$
		$= 1+1+1+1$	$\mathbb{Z}/p \oplus \mathbb{Z}/p \oplus \mathbb{Z}/p \oplus \mathbb{Z}/p$

Scanned by CamScanner

Furthermore, this direct product are unique since we take distinct partition of K.

for example, $\mathbb{Z}_9 \oplus \mathbb{Z}_3$ is not isomorphic to $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$.

because: we know if A is finite then

$$A \oplus B \simeq A \oplus C \text{ iff } B \simeq C$$

In above example $\mathbb{Z}_9 \not\simeq \mathbb{Z}_3 \oplus \mathbb{Z}_3$

because $\mathbb{Z}_9$ is cyclic but $\gcd(3,3) \neq 1$

$\Rightarrow \mathbb{Z}_3 \oplus \mathbb{Z}_3$ is not cyclic.

so $\mathbb{Z}_9 \oplus \not\simeq \mathbb{Z}_3 \oplus \mathbb{Z}_3$.

similarly $\mathbb{Z}_4 \oplus \mathbb{Z}_4 \not\simeq \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$.

problem: ② How to construct all the Abelian groups of prime-power order, as direct product of finite cyclic group.

Sol^n Let $|G| = n$, where n is a positive integer. Then by fundamental theorem of arithmatic.

$n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$ where $p_1, p_2, \cdots p_k$ are distinct prime and n_i's are positive integer.

Next, we individually form all Abelian groups of order $p_1^{n_1}$ and $p_2^{n_2}$, and so on, as described earlier. Finally, we ~~form~~ form all possible external direct products of these groups.

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

2	1176
2	588
2	294
3	147
7	49
	7

$\boxed{\text{partition of } 3}$

$3 = 3$

$= 2+1$

$= 1+1+1$

Then $G \simeq \mathbb{Z}_{2^3} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{7^2}$

$\simeq \mathbb{Z}_{2^2} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{7^2}$

$\simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{7^2}$

$\simeq \mathbb{Z}_{2^3} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{7^2}$ (X)

$\simeq \mathbb{Z}_{2^3} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{7^2}$ (X)

partition of 1

$1 = 1$

partation of 2

$2 = 2$

$= 2+1$

$\simeq \mathbb{Z}_{2^3} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_7$ *

$\simeq \mathbb{Z}_{2^2} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_7$ *

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

Scanned by CamScanner

Again If we given any particular Abelian group G of order 1176, then there is ~~some~~ a question about some G

① Which of the preceding six isomorphism classes represents the structure of G?

$\Rightarrow$ We can answer this by comparing the orders of elements of G with the orders of the elements in the six direct products, since "two finite Abelian groups are isomorphic iff they have the same number of elements of each order.

Ex: If G has element of order 8 then G isomorphic to which direct product

$\Rightarrow$ if G has element of order 8 then G is possible isomorphic to $\mathbb{Z}_{2^3} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{7^2}$ or

$\mathbb{Z}_{2^3} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_7$.

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

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

If we say $|G| = 1176$ and g has any 4 element of order 8 and 12 element of order 7.

Then $G \approx \mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_7 \oplus \mathbb{Z}_7$ (How) ??

② If $|G| = n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$ where p_i's are distinct primes, How can G be expressed as an internal direct product of cyclic group of prime power order?

$\Rightarrow$ For simplicity let $|G| = 2^n$ then first we must compute the orders of the elements. After this is done, pick an element of maximum order 2^r, call it a_1. Then $H = \langle a_1 \rangle$ is one of the factors in the desired internal direct product. If $G \neq \langle a_1 \rangle$, choose an element a_2 of maximum order 2^s s.t $s \leq n-r$ and none of $a_2, a_2^2, a_2^4, \ldots, a_2^{2^{s-1}}$ is in $\langle a_1 \rangle$. Then $\langle a_2 \rangle$ is second direct factors if $n \neq r+s$ select a_3 of maximum order 2^t s.t $t \leq n-r-s$ and none of $a_3, a_3^2, a_3^4 \cdots a_3^{2^{t-1}}$ $\in \langle a_1 \rangle \times \langle a_2 \rangle$

Then $\langle a_3 \rangle$ is another direct factor. We continue in this ~~fa~~ ~~[illegible]~~ fashion until our direct product has same order as G.

(III) A formal presentation of this algorithm for any Abelian group G of prime-power order p^n is as follows.

Step-1 compute the orders of the elements of the group G.

Step-2: select an element a_1 of maximum order and define $G_1 = \langle a_1 \rangle$.

Step-3: If $|G| = |G_1|$. stop otherwise replace i by $i+1$.

Step-4! select an element a_i of maximum order p^k such that $p^k \leq |G| / |G_{i-1}|$. and none of $a_i, a_i^p, a_i^{p^2} \ldots a_i^{p^{k-1}}$ in G_{i-1} and define $G_i = G_{i-1} \times \langle a_i \rangle$.

Step-5 Return to step 3.

(IV) For the general case where $|G| = n = p_1^{n_1} p_2^{n_2} \ldots p_k^{n_k}$, we simply use previous algorithm for each $p_i^{n_i}$ $i = 1, 2 \ldots k$. The direct product of all of these pieces is the desired factorization of G.

Scanned by CamScanner

Example! Let $G = \{1, 8, 17, 19, 26, 28, 37, 44, 46, 53, 62, 64, 71, 73, 82, 89, 91, 107, 109, 116, 118, 127, 134\}$

under multiplication modulo 135. ~~Since G has order 24~~

$|G| = 24 = 2^3 \cdot 3 \simeq \mathbb{Z}_{2^3} \oplus \mathbb{Z}_3 = \mathbb{Z}_8 \oplus \mathbb{Z}_3 \simeq \mathbb{Z}_{24}$

$\simeq \mathbb{Z}_{2^2} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 = \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \simeq \mathbb{Z}_{12} \oplus \mathbb{Z}_2$

$\simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \simeq \mathbb{Z}_6 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$

Now we find internal direct sum of G.

~~From the algorithm possible order of element in G~~
~~$= 1, 2, 3, 8, 4, 8, 12, 24$~~
~~Highest order is 12 let $a_1 = 8 \in G$ is the element of order~~

For 2^3, maximum order element is 8, because

$8^6 = 109$, $8^{12} = 1$

$\therefore o(8) = 12$

$o(109) = 2 = o(134)$.

$\therefore$ G has no element of order 24.

$\therefore G \not\simeq \mathbb{Z}_{24}$

$\therefore G \simeq \mathbb{Z}_{12} \oplus \mathbb{Z}_2$

$G = \langle 8 \rangle \oplus \langle 134 \rangle$.

[$\because \gcd(2, 135) = 1$

$\therefore 2^{\varphi(135)} \equiv 1 \pmod{135}$

$\therefore 2^{72} \equiv 1 \pmod{135}$

$(2^3)^{24} \equiv 1 \pmod{135}$

$8^{24} \equiv 1 \pmod{135}$.

$\therefore o(8) \mid 24$

]

Example: 1 ! Let $G = \{1, 8, 12, 14, 18, 21, 27, 31, 34, 38, 44, 47, 51, 53, 57, 64\}$ under multiplication modulo 65. $|G| = 16 = 2^4$

$G \simeq \mathbb{Z}_{16}$

$\simeq \mathbb{Z}_{2^3} \oplus \mathbb{Z}_2 = \mathbb{Z}_8 \oplus \mathbb{Z}_2$

$\simeq \mathbb{Z}_{2^2} \oplus \mathbb{Z}_{2^2} = \mathbb{Z}_4 \oplus \mathbb{Z}_4$

$\simeq \mathbb{Z}_{2^2} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 = \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$

$\simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$

$4 = 4$
$= 3+1$
$= 2+2$
$= 2+1+1$
$= 1+1+1+1$

To find the correct direct product we find order of every element

$o(1) = 1$
$o(8) = 4$
$o(12) = 4$
$o(14) = 2$
$o(18) = 4$
$o(21) = 4$
$o(27) = 4$
$o(31) = 4$
$o(34) = 4$
$o(38) = 4$
$o(44) = 4$
$o(47) = 4$
$o(51) = 2$
$o(53) = 4$
$o(57) = 4$
$o(64) = 2$

$8^2 = 64$
$8^3 = 512$

$65\overline{)512}$ 7

Since G has no element of order 16 so $G \not\simeq \mathbb{Z}_{16}$

in $\mathbb{Z}_8 \oplus \mathbb{Z}_2$

1, 2, 4, 8   1, 2

possible order

$(1,1) = 1$ $(4\,1) = 4$
$(1\,2) = 2$ $(4\,2) = 4$
$(2\,1) = 2$ $(8\,1) = 8$
$(2\,2) = 2$

So $\mathbb{Z}_8 \oplus \mathbb{Z}_2$ has element of order 8 but G has no element of order 8

$\therefore G \not\simeq \mathbb{Z}_8 \oplus \mathbb{Z}_2$

in $\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$

1, 2, 4   (1, 2)   (1, 2)

$(1,1,1) = 1$ # element $\to 1$
$(1,2,1) \to 2$ # $\to 1$
$(1,2,2) \to 2$ # $\to 1$
$(1,1,2) \to 2$ # $\to 1$
$(2,1,1) \to 2$ $\to 1$
$(2,1,2) \to 2$ $\to 1$
$(2,2,1) \to 2$ $\to 1$
$(2,2,2) \to 2$ $\to 1$

$\therefore$ Total number of element of order 2 is 8 but G has 3 element of order 2

Scanned by CamScanner

$\therefore G \ncong \mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$

Similarly $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ has ~~more~~ more than 3 element of order 2.

$\therefore G \ncong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$

$$\therefore \boxed{G \simeq \mathbb{Z}_4 \oplus \mathbb{Z}_4}$$

For internal direct product:

First pick an element of maximum order. Say the element 8. Then $\langle 8 \rangle$ is a factor in the product. $\langle 8 \rangle = \{1, 8, 64, 57\}$. $o(8) = 4$ next

~~$\langle 12 \rangle \ \{\ \}$~~

we chose an element of order ~~4~~ 4, chose 12.

$G \simeq \langle 8 \rangle \times \langle 12 \rangle$

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.

Scanned by CamScanner