Lemma (3). If G is IDP of $H_1, H_2, \ldots, H_n$. Then each member of G can be expressed uniquely in form $h_1 h_2 \ldots h_n$ where $h_i \in H_i$.

Proof:- Suppose $g = h_1 h_2 \ldots h_n$ & $g = h_1' h_2' \ldots h_n'$ where $h_i h_i' \in H_i \ \forall\ i = 1, 2, \ldots, n$.

Then $h_1 h_2 \ldots h_n = h_1' h_2' \ldots h_n'$ — (*)

$\Rightarrow$ $h_n' h_n^{-1} = (h_{n-1}')^{-1} (h_{n-2}')^{-1} \ldots (h_1')^{-1} h_1 h_2 \ldots h_{n-1}$

$= (h_1')^{-1} h_1 \, (h_2')^{-1} h_2 \ldots (h_{n-1}')^{-1} h_{n-1}$

($\because$ lemma (2) & h's commute)

But then, Thus $h_n' h_n^{-1} \in H_1 H_2 \ldots H_{n-1} \cap H_n = \{e\}$

$\Rightarrow$ $h_n' h_n^{-1} = e$

$\Rightarrow$ $\boxed{h_n = h_n'}$

Now eq. (*) become

$h_1 h_2 \ldots h_{n-1} = h_1' h_2' \ldots h_{n-1}'$

Do the same process as above, and we get

$\boxed{h_i = h_i'} \ \forall\ i = 1, 2, \ldots, n.$

$\Rightarrow$ g is uniquely expressed

New Proof of the theorem

Let $\phi : G \longrightarrow H_1 \oplus H_2 \oplus \cdots \oplus H_n$ as

$$\phi(h_1 h_2 \cdots h_n) = (h_1, h_2, \ldots, h_n).$$

well-defined & one-one

Let $h_1 h_2 \cdots h_n = h_1' h_2' \cdots h_n'$

$\Leftrightarrow h_1 = h_1', h_2 = h_2' \cdots h_n = h_n'$

$\Leftrightarrow (h_1, h_2, \ldots, h_n) = (h_1', h_2', \ldots, h_n')$

$\Leftrightarrow \phi(h_1 h_2 \cdots h_n) = \phi(h_1' h_2' \cdots h_n')$

Thus ϕ is well-defined & one-one.

onto

Let $h \in H_1 \oplus H_2 \oplus \cdots \oplus H_n$

then $h = (h_1, h_2, \ldots, h_n)$

and $h_1 h_2 \cdots h_n \in G$

and $\phi(h_1 h_2 \cdots h_n) = (h_1, h_2, \ldots, h_n) = h$

$\rightarrow \phi$ is onto.

operation preserving. Let $g_1, g_2 \in G$ $\quad g_1 = h_1 h_2 \cdots h_n$, $\quad g_2 = h_1' h_2' \cdots h_n'$

$$\phi(g_1 g_2) = \phi(h_1 h_2 \cdots h_n h_1' h_2' \cdots h_n')$$

$$= \phi(h_1 h_1' h_2 h_2' \cdots h_n h_n')$$

$$= (h_1 h_1', h_2 h_2', h_3 h_3', \ldots h_n h_n')$$

$$= (h_1, h_2 \ldots h_n)(h_1', h_2' \ldots h_n')$$

$$= \phi(h_1 h_2 \ldots h_n)\, \phi(h_1' h_2' \ldots h_n')$$

$\phi(g_1 g_2) = \phi(g_1)\, \phi(g_2)$

$\Rightarrow$ ϕ preserves operation.

Thus ϕ is an isomorphism. $=$

Ch- II

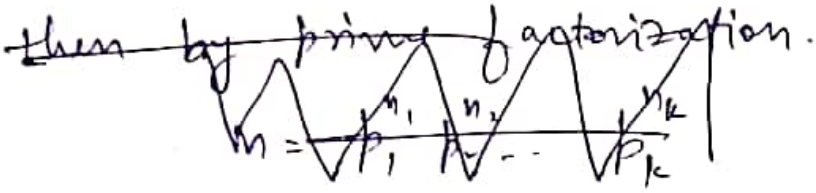
Thm: Fundamental theorem of finite Abelian g/ps

Every finite abelian group is a direct product of cyclic groups of prime-power order. Moreover, the factorization is unique except for rearrangement of the factors.

What it mean

Let $|G| = n$.

~~then by prime factorization.~~



then $G \approx Z_{p_1}^{n_1} \oplus Z_{p_2}^{n_2} \oplus \cdots \oplus Z_{p_k}^{n_k}$

where p_i's are not necessarily distinct primes

Isomorphism of abelian groups.

Let G be a gp s.t. $|G| = p^k$, where p is prime.

order of G	Partition of k	possible direct products of 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}
	$3+1$	$Z_{p^3} \oplus Z_p$
	$2+2$	$Z_{p^2} \oplus Z_{p^2}$
	$1+1+1+1$	$Z_p \oplus Z_p \oplus Z_p \oplus Z_p$
	$2+1+1$	$Z_{p^2} \oplus Z_p \oplus Z_p$

and, the uniqueness portion of F.T.A.G. guarantees that distinct partitions of k yield distinct isomorphism classes.

e.g. $Z_4 \oplus Z_3 \not\cong Z_3 \oplus Z_3 \oplus Z_3$.

Cancelation property of Direct product!

If A is finite, then

$$A \oplus B \approx A \oplus C \iff B \approx C.$$

Proof: Suppose $A \oplus B \cong A \oplus C$

Claim $B \cong C$.

Let $\phi : A \oplus B \to A \oplus C$ is an isomorphism

and $\phi(a,b) = (a,c)$

for fixed a, $\phi_a(b) = \phi(a,b) = (a,c) = c$

define $\phi_a : B \to C$ as $\phi_a(b) = c \left(\because \phi(a,b) = (a,c) \right)$

then ϕ_a is an isomorphism.

hence $B \cong C$

Conversely let $B \cong C$.

then $\phi : B \to C$ is an isomorphism

$\phi(b) = c$

define $\psi : A \oplus B \to A \oplus C$ as

$\psi(a,b) = (a, \phi(b))$

then ψ is an isomorphism.

$\Rightarrow A \oplus B \cong A \oplus C$. =

Now let $|G| = n$

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

then form all abelian gp of $p_1^{n_1}, p_2^{n_2}$ respectively

e.g. Let $n = 1176 = 2^3 \cdot 3 \cdot 7^2$, then distinct isomorphism classes is

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

$Z_{2^2} \oplus Z_2 \oplus Z_3 \oplus Z_{7^2}$

$Z_2 \oplus Z_2 \oplus Z_2 \oplus Z_3 \oplus Z_{7^2}$

$Z_2 \oplus Z_3 \oplus Z_7 \oplus Z_7$

$Z_2 \oplus Z_2 \oplus Z_3 \oplus Z_7 \oplus Z_2$

$Z_2 \oplus Z_2 \oplus Z_2 \oplus Z_3 \oplus Z_7 \oplus Z_7$

Now, suppose G has an element of order 8 then either $G \cong Z_8 \oplus Z_3 \oplus Z_{49}$

or $G \cong Z_8 \oplus Z_3 \oplus Z_7 \oplus Z_7$.

Now, G also has an element of order 49, then

$G \cong Z_8 \oplus Z_3 \oplus Z_{49}$.

Writing G as an product of internal direct product

Suppose $|G| = 2^n$

then pick an element a_1 of maximum order say 2^r.

then $\langle a_1 \rangle$ is one of the factor in desired internal direct product.

If $G = \langle a_1 \rangle$, we are done., If not,

then pick 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 a second factor. If $n \neq r+s$, select a_3 of maximum order 2^t such that $t \leq n-r-s$ and none of $a_3, a_3^2, a_3^4, \ldots a_3^{2^{t-1}}$ is in $\langle a_1 \rangle \times \langle a_2 \rangle = \{ a_1^i a_2^j \mid 0 \leq i \leq 2^r, 0 \leq j \leq 2^s \}$

Then $\langle a_3 \rangle$ is another direct factor. We continue in this fashion until our direct product has the order as G.

eg: Same can be done for p^m.

Algorithm for an Abelian group of Order p^n

1.) Compute the order of the elements of the group G.

2.) select an element a_1 of maximum order and define $G_1 = \langle a_1 \rangle$.
set $i = 1$.

3.) If $|G| = |G_i|$, stop. Otherwise replace $i = i+1$.

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

5.) Return to step 3.

Ex ① Let $G = \{1, 8, 12, 14, 18, 21, 27, 31, 34, 38, 44, 47, 51, 53, 57, 64\}$ under $\otimes_{65}$.

Since $|G| = 16 = 2^4$

G is isomorphic to one of the following.

Z_{16}

$Z_8 \oplus Z_2$

$Z_4 \oplus Z_4$

$Z_4 \oplus Z_2 \oplus Z_2$

$Z_2 \oplus Z_2 \oplus Z_2 \oplus Z_2$

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

64
2

No. of elements of order 4 = 12

No. ——————— 2 = 3

Then either $G \cong Z_4 \oplus Z_4$ or $G \cong Z_4 \oplus Z_2 \oplus Z_2$.

$Z_4 \oplus Z_2 \oplus Z_2$ has 7 elements of order 2.

Thus, $G \cong Z_4 \oplus Z_4$.

Express G as IDP.

First Pick an element of maximum order, say 8.

Then $\langle 8 \rangle = \{1, 8, 64, 57\}$.

Let $a_2 = 12$ $\langle 12 \rangle = \{1, 12, 144, 38\}$

$G = \langle 8 \rangle \times \langle 12 \rangle$.