Ex-2 Let $G = \{1, 8, 17, 19, 26, 28, 37, 44, 46, 53, 62, 64, 71, 73, 82, 89, 91, 98, 107, 109, 116, 118, 127, 134\}$ $\otimes_{135}$.

then $|G| = 24$

$$\therefore G \cong Z_8 \oplus Z_3 \cong Z_{24}$$

$$Z_4 \oplus Z_2 \oplus Z_3 \cong Z_{12} \oplus Z_2$$

$$Z_2 \oplus Z_2 \oplus Z_2 \oplus Z_3 \cong Z_6 \oplus Z_2 \oplus Z_2$$

Then 8 has order 12. This rules out (3).

Thus $8^6 = 109$ and $8^{12} = 1$

also $|109| = 2 = |134|$ → this rules out (1)

Thus, $G \cong Z_{12} \oplus Z_2$.

and $G = \langle 8 \rangle \times \langle 134 \rangle$.

Corollary:- Existance of subgroups of Abelian gps

If m divides the order of a finite Abelian gp G, then G has a subgp of order m. (Proof not included)

Ex:- Suppose $|G| = 72 = 2 \times 2 \times 2 \times 3 \times 3 = 2^3 \cdot 3^2$

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

$Z_{2^2} \oplus Z_2 \oplus Z_{3^2}$ $\qquad$ $Z_{2^2} \oplus Z_2 \oplus Z_3 \oplus Z_3$

$Z_2 \oplus Z_2 \oplus Z_2 \oplus Z_{3^2}$ $\qquad$ $Z_2 \oplus Z_2 \oplus Z_2 \oplus Z_3 \oplus Z_3$

then, $\mathbb{Z}_8 \oplus \mathbb{Z}_9 \cong \mathbb{Z}_{72}$ which has a subgp of order 12. $\langle 6 \rangle$.

and $\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \cong \mathbb{Z}_{12} \oplus \mathbb{Z}_6$ this also has a subgp of order 12.

$\mathbb{Z}_4 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9 \approx \mathbb{Z}_4 \oplus \mathbb{Z}_{18}$ → also a subgp of order 12.

"

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

Thm :- For two finite subgroups H and K of a gp G,

$$|HK| = \frac{|H|\,|K|}{|H \cap K|}.$$

Proof :- first the set $\{HK\}$ has $|H||K|$ products, all not need be distinct. i.e. we may have $hk = h'k'$ where $h' = h$ & $k = k'$.

Now, to determine $|HK|$, we need to determine the extent to which this happens.

Now let $t \in H \cap K$, then

$$hk = (ht)(t^{-1}k) = h'k'$$

so each element in HK is represented by atleast $|H \cap K|$ products in HK.

But if $hk = h'k'$ $\Rightarrow$ $h^{-1}h' = kk'^{-1} \in H \cap K$. say t

so $h' = ht$ and $k' = t^{-1}k$.

$\therefore$ Each element in HK is represented by exactly $|H \cap K|$ products

$$\therefore \quad |HK| = \frac{|H||K|}{|H \cap K|}$$

<u>Lemma 1</u> :- Let G be a finite Abelian group of order $p^n m$ where p is 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 $|H| = p^n$.

<u>Proof</u> :- first check H & K are subgps.

Hence they are normal subgps.

Now to prove $G = H \times K$ we need to show

$G = HK$ and $H \cap K = \{e\}$.

Since $\gcd(m, p^n) = 1$

$\exists$ integers s and t s.t.

$$sm + tp^n = 1$$

$$\Rightarrow \quad x = \cancel{x^{sm} + x^{tp^n}} \; x^{sm+tp^n}$$

$$= x^{sm} \cdot x^{tp^n}$$

$\Rightarrow x^{sm} \in H$ & $x^{tp^n} \in K$

Thus $G = HK$.

Now let $x \in H \cap K$

$\Rightarrow x \in H$ and $x \in K$

$\Rightarrow x^{p^n} = e$ $\quad x^m = e$

let $|x| = k \Rightarrow k / p^n$ & k / x^m

$\Rightarrow k / \gcd(p^n, m) \Rightarrow k = 1$

$\Rightarrow x = \{e\}$

Thus $G = H \times K$.

Claim!- $|H| = p^n$

$|HK| = |H||K| = p^n \cdot m$

p does not divide $|K|$ (if p divides $|K|$, then K has an element of order p)

$\Rightarrow |H| = p^n$.

Now let $|G| = p_1^{n_1} p_2^{n_2} \dots p_k^{n_k}$, where p's are distinct prime.

$G(p_i) = \{x \in G \mid x^{p_i^{n_i}} = e\}$.

then $G = G(p_1) \times G(p_2) \times \dots \times G(p_k)$.

and $|G(p_i)| = p_i^{n_i}$.

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

Proof:- Let $|G| = p^n$, we prove it by induction.

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

Now assume that statement is true for all Abelian gps of order p^k s.t. $k < n$.

Now we prove the statement for a gp of order p^n.

Choose 'a' of maximal order in G say p^m.

then $x^{p^m} = e \quad \forall\, x \in G$,

and we may assume that $G \neq \langle a \rangle$

Now choose a element 'b' from G ~~of~~ of smallest order s.t. $b \notin \langle a \rangle$.

Claim:- $|b| = p$.

and since $|b^p| = \dfrac{|b|}{p} \Rightarrow |b^p| < |b|$

so $b^p \in \langle a \rangle$ ($\because$ if not, then our choice would be b^p not b)

$\therefore \Rightarrow \quad b^p = a^i$ for some i

And $e = (b^p)^{p^{m-1}} = (a^i)^{p^{m-1}} = e$

$\Rightarrow \quad |a^i| \leq p^{m-1}$

$\Rightarrow$ a^i is not a generator of $\langle a \rangle$.

$\Rightarrow \quad \gcd(p^{m-1}, i) \neq 1$

$\Rightarrow \quad p$ divides i

$\Rightarrow \quad i = pj$ for some j.

Then $\quad b^p = a^i = a^{pj}$

Consider $\quad c = a^{-j} b$, then $c \in G$ but $c \notin \langle a \rangle$
(if it does then $b \in \langle a \rangle$ N.P.)

Claim:- $\quad |c| = p$

$c^p = (a^{-j} b)^p = a^{-jp} . b^p = a^{-i} . b^p$
$= b^{-p} . b^p = e$

$\Rightarrow \quad c^p = e$

$\Rightarrow \quad |c| = p$

$\Rightarrow \quad |b| = p$ (As if $|b| \neq p$, then $|c| \not< |b|$ & $c \notin \langle a \rangle$ so our choice would be c)

$\Rightarrow \quad \langle a \rangle \cap \langle b \rangle = \{e\}$

(if intersection is not empty, then $b \in \langle a \rangle$)

Now, Consider the factor group $\bar{G} = \frac{G}{\langle b \rangle}$

then $|\bar{G}| = p^{n-1}$ $\qquad \bar{x} = x\langle b \rangle$.

and If $|\bar{a}| = |a\langle b \rangle| < |a| = p^m$

then $\bar{a}^{p^{m-1}} = \bar{e} = e\langle b \rangle = \langle b \rangle$

$\bar{a}^{p^{m-1}} = a^{p^{m-1}}\langle b \rangle = \langle b \rangle$

$\Rightarrow a^{p^{m-1}} \in \langle b \rangle$ (Not possible)

Hence $|\bar{a}| = |a| = p^m$

$\Rightarrow$ $\bar{a}$ is the element of maximal order in $\bar{G}$.

and by induction $\bar{G} = \bar{a} \times \bar{K}$ for some subgp $\bar{K}$ of $\bar{G}$.

Now let K be the pullback of $\bar{K}$ under natural homomorphism from G to $\bar{G}$.

$K = \{x \in G \mid \bar{x} \in \bar{K}\}$

Claim!- $G = \langle a \rangle \times K$.

K is subgp!- Let $x, y \in K$ $\Rightarrow \bar{x}, \bar{y} \in \bar{K}$

$\Rightarrow \bar{x}\bar{y} \in \bar{K}$

$\Rightarrow \bar{x}\bar{y} = x\langle b \rangle y\langle b \rangle$

$= xy\langle b \rangle$

$= \overline{xy}$

$\Rightarrow xy \in K$.

$\underline{\langle a\rangle \cap K = \{e\}}$, let $x \in \langle a\rangle \cap K$

$\Rightarrow x \in \langle a\rangle$ & $x \in K$

$\Rightarrow \bar{x} \in \langle \bar{a}\rangle$ & $\bar{x} \in \bar{K}$

$\Rightarrow \bar{x} \in \langle \bar{a}\rangle \cap \bar{K} = \{e\}$

$\Rightarrow \bar{x} = \{e\} \Rightarrow x \in \langle b\rangle$

$\Rightarrow x \in \langle a\rangle \cap \langle b\rangle$

Hence $x = \{e\}$

$\Rightarrow \langle a\rangle \cap K = \{e\}$

$\underline{G = \langle a\rangle K}$. We can see that $\bar{K} = \dfrac{K}{\langle b\rangle}$

$\Rightarrow p|\bar{K}| = K$

Now $|\langle a\rangle K| = \dfrac{|\langle a\rangle||K|}{|\langle a\rangle \cap K|} = |\langle a\rangle||K|$

$= |\langle \bar{a}\rangle||\bar{K}|p$

$= |\bar{G}|p = |G|$

$\Rightarrow |G| = |\langle a\rangle K|$

$\Rightarrow G = \langle a\rangle \times K$.

So lemma proved.

Now as $|K| < |G|$

By induction $K = \langle a'\rangle \times K'$ and so on

$\therefore G = \langle a\rangle \times \langle a'\rangle \times \langle a''\rangle \times \ldots \times \langle a^{m}\rangle$

So By lemma (1) if $|G| = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$

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

and $|G(p_i)| = p_i^{n_i}$

If we do it

So $G(p_i) = \langle a_1^i \rangle \times \langle a_2^i \rangle \times \cdots \times \langle a_{k_i}^i \rangle$ (By lemma (2))

So $G = \langle a_1^1 \rangle \times \langle a_2^1 \rangle \times \cdots \times \langle a_{l_1}^1 \rangle \times \langle a_1^2 \rangle \times \langle a_2^2 \rangle \times \cdots$

Hence G can be written as the direct product of cyclic gps.

<u>Lemma 3</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 H's and K's are non-trivial cyclic subgps 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 prove it by induction, $|G| = p^n$

for $n = 1$, $|G| = p \rightarrow$ done.

Now suppose that the statement is true for all abelian gps of order less than $|G|$.

(for any Abelian gp G, $G^p = \{x^p \mid x \in G\}$ is a subgp of G)

Scanned by CamScanner

then $G^p = H_1^p \times H_2^p \times \dots \times H_{m'}^p$ are subgps of G.
& $G^p = K_1^p \times K_2^p \times \dots \times K_{n'}^p$

where m' is the largest integer i s.t. $|H_i| > p$.
and n' ———————— i s.t. $|K_i| > p$.

Since $|G^p| < |G|$
By induction, $m' = n'$ and $|H^p_i| = |K^p_i|$

$\Rightarrow \frac{|H_i|}{p} = \frac{|K_i|}{p}$

$\Rightarrow |H_i| = |K_i|$ $\forall i = 1, \dots, m'$

Claim:- $m = n$ or $m - m' = n - n'$

$|H_1||H_2| \dots |H_{m'}| p^{m-m'} = |G| = |K_1||K_2| \dots |K_{n'}| p^{n-n'}$

$\Rightarrow p^{m-m'} = p^{n-n'}$ $[\because |H_i| = |K_i|)$

$\Rightarrow m - m' = n - n'$

$\Rightarrow m = n$.

$\Rightarrow$ If $|G| = p^n$, then its direct product is unique

$\Rightarrow$ If $|G| = p_1^{n_1} p_2^{n_2} \dots p_k^{n_k}$

then its direct product is unique.

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

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

previously:- $G = \langle 8 \rangle \times \langle 12 \rangle$ $|G| = 2^4$

Acc. to lemma:- let $\langle a \rangle = \langle 8 \rangle$

then we have to find b, s.t. $b \notin \langle a \rangle$. so let $b = 14$

$\langle 8 \rangle = \{1, 8, 64, 57\}$ $\langle 14 \rangle = \{1, 14\}$

$$\bar{G} = \frac{G}{\langle b \rangle} = \frac{G}{\langle 14 \rangle}$$

$\bar{G} = \{ \{1,14\}, \underset{8\langle 14\rangle}{\{8, 47\}}, \underset{12\langle 14\rangle}{\{12, 38\}}, \underset{14\langle 14\rangle}{\{1, 14\}}, \underset{18\langle 14\rangle}{\{18, 57\}},$
$\{21, 34\}, \{27, 53\}, \{31, 44\}, \{34, 21\}, \{38, 12\},$
$\{44, 31\}, \{47, 8\}, \{51, 64\}, \{53, 27\}, \{57, 18\}, \{64, 51\}\}$

$|\bar{G}| = 8$

$\bar{G} = \{ \underset{\langle 14\rangle}{\{1,14\}}, \underset{8\langle 14\rangle}{\{8, 47\}}, \underset{12\langle 14\rangle}{\{12, 38\}}, \underset{18\langle 14\rangle}{\{18, 57\}}, \underset{21\langle 14\rangle}{\{21, 34\}}, \underset{27\langle 14\rangle}{\{27, 53\}},$
$\underset{31\langle 14\rangle}{\{31, 44\}}, \underset{51\langle 14\rangle}{\{51, 64\}}\}$.

$\bar{8} = \{ \{1, 14\}, \underset{8\langle 14\rangle}{\{8, 47\}}, \underset{64\langle 14\rangle}{\{51, 64\}}, \underset{18\langle 14\rangle}{\{18, 57\}} \}$

$\bar{G} = \bar{8} \times \bar{K}$ here $\bar{K} = \langle \bar{12} \rangle = \{\langle 14\rangle, 12\langle 14\rangle\}$

$\bar{12} = \{ \{1, 14\}, \{12, 38\}\}$ $\langle 12 \rangle = \{1, 12, 14, 38\}$

$K = \langle 12 \rangle = \{x \in G \mid \bar{x} \in \bar{K}\}$

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