The Group of Units Modulo n as an External Direct Product.

Statement: Let us suppose s, t are relatively prime. Then $U(st) \simeq U(s) \times U(t)$.

Proof: Let us consider the mapping $\phi : U(st) \to U(s) \times U(t)$ by $\phi([x]_{st}^{*}) = ([x]_s, [x]_t)$, for each $[x]_{st} \in U(st)$.

To show: ϕ is an isomorphism.

$\circledast$ Here $[x]_{st}$ represents $x \bmod st$, and so on...

First of all to show that the map ϕ is well-defined

Let $[x]_{st} = [y]_{st} \Rightarrow y = x + k(st)$. $k \in \mathbb{Z}$.

$$\therefore \phi([y]_{st}) = ([y]_s, [y]_t) = ([x+kst]_s, [x+kst]_t)$$
$$= ([x]_s, [x]_t) = \phi([x]_{st}).$$

$\therefore$ ϕ is well-defined.

To show: ϕ is homomorphism

$$\phi([x]_{st}[y]_{st}) = \phi([xy]_{st}) = ([xy]_s, [xy]_t)$$
$$= ([x]_s [y]_s, [x]_t [y]_t)$$
$$= ([x]_s, [x]_t)([y]_s, [y]_t)$$
$$= \phi([x]_{st}) \phi([y]_{st}).$$

$\Rightarrow$ ϕ is homomorphism

To show: ϕ is injective.

$$\text{Ker}\,\phi = \{[x]_{st} \mid \phi([x]_{st}) = \text{identity element of } U(s) \times U(t) = ([1]_s, [1]_t)\}.$$
$$= \{[x]_{st} \mid [x]_s = [1]_s, [x]_t = [1]_t\}$$

Thus $[x]_{st} \in \text{Ker}\,\phi$ if and only if $x \equiv 1 \pmod{s}$, $x \equiv 1 \pmod{t}$,
$\Rightarrow x \equiv 1 \pmod{st}$.
for $\gcd(s,t) = 1$.

$\therefore$ $\text{Ker}\,\phi = \{[1]_{st}\}$. where $[1]_{st}$ is the identity element of $U(st)$.

$\therefore$ ϕ is injective.

Since $U(st)$ and $U(s) \times U(t)$ are finite; and ϕ is injective $\Rightarrow$ ϕ is a bijection.

$\therefore$ ϕ is a homomorphism & bijection $\Rightarrow$ ϕ is isomorphism

$\therefore$ $U(st) \simeq U(s) \times U(t)$. proved.

Finite Abelian Groups.

The ultimate goal of group theory is to classify all groups up to isomorphism; i.e., given a particular group, we should be able to match it up with a known group via an isomorphism.

We have already proved that —

1. Any finite cyclic group of order n is isomorphic to $\mathbb{Z}_n$. $\Rightarrow$ We know about all finite cyclic groups.
2. Every cyclic group of prime order is isomorphic to $\mathbb{Z}_p$, p being a prime.
3. $\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$, when $\gcd(m,n) = 1$.
4. Every finite abelian group is isomorphic to a direct product of cyclic groups of prime power order; $\mathbb{Z}_{p_1^{\alpha_1}} \times \cdots \mathbb{Z}_{p_n^{\alpha_n}}$; where each p_k is prime, not necessarily distinct.

This is known as Fundamental Theorem of Finite Abelian groups.

Statement: Every finite abelian group G is isomorphic to a direct product of cyclic groups of the form

$$\mathbb{Z}_{p_1^{\alpha_1}} \times \mathbb{Z}_{p_2^{\alpha_2}} \times \cdots \times \mathbb{Z}_{p_n^{\alpha_n}},$$ where p_i's are primes, not necessarily distinct.

p-group: A group G is said to be a p-group if every element in G has as its order a power of p.

eg. Both $\mathbb{Z}_2 \times \mathbb{Z}_2$ and $\mathbb{Z}_4$ are 2-groups, & $\mathbb{Z}_{27}$ is a 3-group.

Examples:

① Suppose we wish to classify all abelian groups of order $540 = 2^2 \cdot 3^3 \cdot 5$.

The Fundamental theorem of Finite Abelian Groups tells us that there are 6 possibilities:

(i) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$.

(ii) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_9 \times \mathbb{Z}_5$

(iii) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{27} \times \mathbb{Z}_5$

(iv) $\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$

(v) $\mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_9 \times \mathbb{Z}_5$

(vi) $\mathbb{Z}_4 \times \mathbb{Z}_{27} \times \mathbb{Z}_5$.

② Find all of the abelian groups of order 720 up to isomorphism.

$720 = 2^4 \cdot 3^2 \cdot 5$

The Fundamental Theorem of Finite Abelian Groups tells us that there are 8 possibilites:

(i) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$

(ii) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5$

(iii) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$

(iv) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_5$

(v) $\mathbb{Z}_2 \times \mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$

(vi) $\mathbb{Z}_2 \times \mathbb{Z}_8 \times \mathbb{Z}_9 \times \mathbb{Z}_5$

(vii) $\mathbb{Z}_{16} \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$

(viii) $\mathbb{Z}_{16} \times \mathbb{Z}_9 \times \mathbb{Z}_5$

③ Find all of the abelian groups of order 200 up to isomorphism.

$200 = 2^3 \cdot 5^2$.

There will be 6 possibilities.

Lemma: $\mathbb{Z}_{n_1 n_2 \cdots n_k} \simeq \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}$ iff $\gcd(n_i, n_j) = 1$ whenever $i \neq j$.

Since $|\mathbb{Z}_n| = n$ and $\mathbb{Z}_n$ is cyclic, then

$\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}$ is cyclic iff $\gcd(n_i, n_j) = 1$, $i \neq j$.

$$O(\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}) = n_1 n_2 \cdots n_k = O(\mathbb{Z}_{n_1 n_2 \cdots n_k})$$

$\therefore \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k} \simeq$ to a cyclic group of order $n_1 n_2 \cdots n_k$ and hence the result follows.

Example: Since $105 = 3.5.7$, we have

$$\mathbb{Z}_{105} \simeq \mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_7 .$$

Again, $\mathbb{Z}_{20}$ is not isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_{10}$, as ~~& and~~ $\gcd(2, 10) \neq 1$.

But $\mathbb{Z}_{20} \simeq \mathbb{Z}_4 \times \mathbb{Z}_5$ as $\gcd(4, 5) = 1$.

Order	isomorphism classes
p	$\mathbb{Z}_p$
p^2	$\mathbb{Z}_{p^2}$ $\mathbb{Z}_p \times \mathbb{Z}_p$
p^3	$\mathbb{Z}_{p^3}$ $\mathbb{Z}_{p^2} \times \mathbb{Z}_p$ $\mathbb{Z}_p \times \mathbb{Z}_p \times \mathbb{Z}_p$

Remarks:

$\mathbb{Z}_{p^2} \not\simeq \mathbb{Z}_p \times \mathbb{Z}_p$ as $\mathbb{Z}_{p^2}$ is cyclic but $\mathbb{Z}_p \times \mathbb{Z}_p$ is not cyclic.

Ex: What are the possible types of abelian groups of order 100 upto isomorphism?

$100 = 2^2 . 5^2$. We have the following choices:

$$\mathbb{Z}_4 \times \mathbb{Z}_{25} \simeq \mathbb{Z}_{100}$$
$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{25} \simeq \mathbb{Z}_2 \times \mathbb{Z}_{50}$$
$$\mathbb{Z}_4 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \simeq \mathbb{Z}_{20} \times \mathbb{Z}_5$$
$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_5 \simeq \mathbb{Z}_{10} \times \mathbb{Z}_{10} .$$

Problems on the External Direct Product

Ex. — 17 (S. K. Mapa).

① Let $G_1 = \langle a \rangle$ be a cyclic group of order 8 and $G_2 = \langle b \rangle$ be a cyclic group of order 3. Show that the group $G_1 \times G_2$ is cyclic.

Solution:

$O(G_1) = 8$, $O(G_2) = 3 \Rightarrow O(G_1 \times G_2) = O(G_1) \cdot O(G_2) = 8 \cdot 3 = 24$.

$G_1 = \langle a \rangle \Rightarrow O(a) = 8$; $G_2 = \langle b \rangle \Rightarrow O(b) = 3$.

$a \in G_1$, $b \in G_2 \Rightarrow (a, b) \in G_1 \times G_2$.

Now $O((a,b)) =$ l.c.m. of $O(a)$ and $O(b)$.

$=$ l.c.m. of 8 and 3 $= 24 = O(G_1 \times G_2)$.

$\Rightarrow G_1 \times G_2$ is a cyclic group. [NOTE: $\gcd(O(G_1), O(G_2)) = 1$]

② Let $G_1 = \langle a \rangle$ be a cyclic group of order 9 and $G_2 = \langle b \rangle$ be a cyclic group of order 3. Show that the group $G_1 \times G_2$ is not cyclic.

Solution: $O(G_1) = 9$, $O(G_2) = 3 \Rightarrow O(G_1 \times G_2) = 9 \cdot 3 = 27$.

$G_1 = \langle a \rangle \Rightarrow O(a) = 9$; $G_2 = \langle b \rangle \Rightarrow O(b) = 3$.

Let $(e_1, e_2) \in G_1 \times G_2$ be the identity and also let $(x, y) \in G_1 \times G_2$ " " generator (if possible). Then $(x, y) \neq (e_1, e_2)$. As $O(e_1, e_2) = 1$, $O((x,y)) = 27$.

Now every element of the group $G_1 \times G_2$ must be expressed as $((x,y))^n$ or (x^n, y^n) for some $n \in \mathbb{Z}$.

Now $G_1 = \langle a \rangle = \{e_1, a, a^2, a^3, a^4, a^5, a^6, a^7, a^8\}$

and $G_2 = \langle b \rangle = \{e_2, b, b^2\}$.

So let us take $(x^4, y^2) \in G_1 \times G_2$; as $x \in G_1$, $y \in G_2$.

Now if $(x^4, y^2) = (x^n, y^n)$ for some $n \in \mathbb{Z}$, then

$x^n = x^4$ and $y^n = y^2 \Rightarrow n = 4, n = 2$ which is not possible.

$\therefore (x^4, y^2)$ cannot be expressed as $((x,y))^n$ for any integer n.

$\therefore G_1 \times G_2$ cannot be a cyclic group. proved

NOTE: $\gcd(O(G_1), O(G_2)) \neq 1$.

(3) If $\gcd(m,n)=1$, prove that $Z_m \times Z_n$ and Z_{mn} are isomorphic.

We know Z_m, Z_n, Z_{mn} are all finite cyclic groups with $m, n \in Z^+$.

$\therefore$ The group $Z_m \times Z_n$ is cyclic, since $\gcd(m,n)=1$, i.e., $\gcd(o(Z_m), o(Z_n)) = 1$.

Now $o(Z_m \times Z_n) = o(Z_m) \cdot o(Z_n) = mn = o(Z_{mn})$.

So we have two finite cyclic groups $Z_m \times Z_n$ and Z_{mn} of the same order mn.

Hence $\underline{Z_m \times Z_n \simeq Z_{mn}}$. Proved.

(6) Find the number of elements of order 5 in the group $Z_{15} \times Z_{10}$.

Let $(a,b) \in Z_{15} \times Z_{10}$ and let $o((a,b)) = 5$.

Here $a \in Z_{15}$, $b \in Z_{10}$; Z_{15}, Z_{10} are both additive cyclic groups.

Now $o((a,b)) =$ l.c.m. of $o(a)$ and $o(b) = 5$.

$\Rightarrow$ either (i) $o(a) = 5$; $o(b) = 1$ or 5

or (ii) $o(a) = 1$ or 5; $o(b) = 5$.

Case (i): $o(a) = 5$; $o(b) = 1$ or 5

$o(a) = 5 \Rightarrow o(a \cdot 1) = 5$

$\Rightarrow \dfrac{o(1)}{\gcd(a, o(1))} = 5$

$\Rightarrow \dfrac{15}{\gcd(a,15)} = 5$

$\Rightarrow \gcd(a,15) = 3$

$\Rightarrow \gcd(\frac{a}{3}, 5) = 1$

$\Rightarrow \frac{a}{3} = 1, 2, 3, 4$

$\Rightarrow \boxed{a = 3, 6, 9, 12}$ 4 elements

$o(b) = 1 \Rightarrow \boxed{b = 0}$ → one element

$o(b) = 5 \Rightarrow o(b \cdot 1) = 5$

$\Rightarrow \dfrac{o(1)}{\gcd(b, o(1))} = 5$

$\Rightarrow \dfrac{10}{\gcd(b,10)} = 5$

$\Rightarrow \gcd(b,10) = 2$

$\Rightarrow \gcd(\frac{b}{2}, 5) = 1$

$\Rightarrow \frac{b}{2} = 1, 2, 3, 4$

$\Rightarrow \boxed{b = 2, 4, 6, 8}$ → 4 elements

$\therefore$ For case (i) we have $4 \times (1+4) = \underline{20}$ elements of order 5 in the group $Z_{15} \times Z_{10}$.

Case (ii): $o(a) = 1$; $o(b) = 5 \Rightarrow \boxed{a = 0}$; $\boxed{b = 2, 4, 6, 8}$.

$\therefore$ For case (ii) we have $1 \times 4 = \underline{4}$ elements of order 5 in the group $Z_{15} \times Z_{10}$. So, total no. of elements $= 20 + 4 = \underline{24}$.

(7) Find the number of elements of order 3 in the group $Z_9 \times Z_6$.

Let $(a,b) \in Z_9 \times Z_6$, and let $o((a,b)) = 3$.

$o((a,b)) =$ l.c.m. of $o(a)$ and $o(b) = 3$.

$\Rightarrow$ either (i) $o(a) = 3$; $o(b) = 1$ or 3

or (ii) $o(a) = 1, 3$; $o(b) = 3$.

Case (i). $o(a) = 3$; $o(b) = 1$ or 3

$o(a) = 3 \Rightarrow o(a \cdot 1) = 3$

$\Rightarrow \dfrac{o(1)}{\gcd(a, o(1))} = 3$

$\Rightarrow \dfrac{9}{\gcd(a,9)} = 3$

$\Rightarrow \gcd(\frac{a}{3}, 3) = 1$

$\Rightarrow \boxed{a = 3, 6}$

2 elements

$o(b) = 1 \Rightarrow \boxed{b = 0}$ one element

$o(b) = 3$

$\Rightarrow \dfrac{o(1)}{\gcd(b, o(1))} = 3$

$\Rightarrow \dfrac{6}{\gcd(b,6)} = 3$

$\Rightarrow \gcd(\frac{b}{2}, 3) = 1$

$\Rightarrow \boxed{b = 2, 4} \longrightarrow$ 2 elements

$\therefore$ In case (i) there exist $2 \times (1+2) = 6$ elements of order 3 in the group $Z_9 \times Z_6$.

Case (ii) ; $o(a) = 1$; $o(b) = 3$

$\Rightarrow \boxed{a = 0}$; $o(b) = 3 \Rightarrow \boxed{b = 2, 4}$

$\therefore$ In case (ii) there exists $1 \times 2 = 2$ elements only of order 3 in the group $Z_9 \times Z_6$.

$\therefore$ Total no. of elements of order 3 in the group $Z_9 \times Z_6$ is $(6+2) = \underline{8 \text{ elements}}$.

(8) Find the number of distinct cyclic subgroups of order 10 in the group $Z_{50} \times Z_{25}$.

Let us first find the elements of order 10 in the group $Z_{50} \times Z_{25}$.

Let $(a,b) \in Z_{50} \times Z_{25}$ and $o((a,b)) = 10$.

As $o((a,b)) =$ l.c.m. of $o(a)$ and $o(b) = 10$.

$\Rightarrow$ either (i) $o(a) = 10$; $o(b) = 1$ or 5 $[o(b) \neq 10, 2]$

or (ii) $o(a) = 2$; $o(b) = 5$.

Case (i): $o(a) = 10$; $o(b) = 1$ or 5.

Now since the cyclic group Z_{50} has a unique cyclic subgroup of order 10, and any cyclic group of order 10 has
(*) $\phi(10) = 4$ generators; so there are 4 choices for a in the group Z_{50}.
Similarly, there are $(1+4)$ choices for b in the group Z_{25}. $\left[\begin{array}{l} o(b)=1 \Rightarrow b=0. \\ o(b)=5 \Rightarrow \phi(5)=4 \text{ generators} \end{array}\right]$
$\therefore$ In case (i) we have $4 \times 5 = 20$ elements (a, b) of order 10 in $Z_{50} \times Z_{25}$.

(*) By the theorem: If d is a +ve divisor of n, the no. of elements of order d in a cyclic group of order n is $\phi(d)$.

Case (ii): $o(a) = 2$ and $o(b) = 5$.
Similar to case (i), there exists only one generator as $\phi(2) = 1$. So only 1 elements for a of order 2 in the group Z_{50}.
And $o(b) = 5 \Rightarrow$ there are $\phi(5) = 4$ elements for b of order 5 in the group Z_{25}.
$\therefore$ In case (ii) we have $1 \times 4 = 4$ elements (a, b) of order 10 in $Z_{50} \times Z_{25}$
$\therefore$ Total no. of elements of order 10 in $Z_{50} \times Z_{25}$
$= 20 + 4 = 24$.

Because each cyclic subgroup of order 10 has $(\phi(10) =)$ 4 (generators) elements of order 10 and no two of the cyclic subgroups can have an element of order 10 in common, there must be $24/4 = 6$ distinct cyclic subgroups of order 10.

⑨ Find the number of distinct cyclic subgroups of order 4 in the group $Z_4 \times Z_4$.

Let us first find the elements of order 4 in the group $Z_4 \times Z_4$.

Let $(a,b) \in Z_4 \times Z_4$ and $o((a,b)) = 4$.

$o((a,b))$ = l.c.m. of $o(a)$ and $o(b) = 4$

$\Rightarrow$ either (i) $o(a) = 4$; $o(b) = 1$ or 4

or (ii) $o(a) = 1$; $o(b) = 4$

or (iii) $o(a) = 2$; $o(b) = 4$

or (iv) $o(a) = 4$; $o(b) = 2$.

Case (i): $o(a) = 4$; $\Rightarrow a = 1, 3$ | $o(b) = 1$ or 4.

$\Rightarrow \phi(4) = 2$ elements for a of order 4 in the group Z_4 | $o(b) = 1 \Rightarrow \boxed{b=0}$ one element; $o(b) = 4 \Rightarrow \phi(4) = 2$ elements for b of order 4 in Z_4.

$\therefore$ In case (i), there are $2 \times (1+2) = \underline{6 \text{ elements}}$ of order 4 in $Z_4 \times Z_4$.

Case (ii): $o(a) = 1$; | $o(b) = 4 \Rightarrow b = 1, 3$.

$\Rightarrow \boxed{a = 0}$, one element for a of order 1. | $\Rightarrow$ 2 elements for b of order 4.

$\therefore$ In case (ii) there are $1 \times 2 = \underline{2 \text{ elements}}$ of order 4 in $Z_4 \times Z_4$.

Case (iii): $o(a) = 2$; $\Rightarrow a = 2$ | $o(b) = 4$

$\Rightarrow \phi(2) = 1$ element | $\Rightarrow \phi(4) = 2$ elements.

$\therefore$ In case (iii) there are $1 \times 2 = \underline{2 \text{ elements}}$ of order 4 in $Z_4 \times Z_4$

Case (iv): there are $2 \times 1 = \underline{2 \text{ elements}}$ of order 4 in $Z_4 \times Z_4$.

$\therefore$ Total no. of elements of order 4 in $Z_4 \times Z_4$
$= 6 + 2 + 2 + 2 = \underline{12}$.

Because each cyclic subgroup of order 4 has $\underline{\phi(4) = 2 \text{ elements}}$ of order 4 and no two of the cyclic subgroups can have an element of order 4 in common, there must be $12/2 = \underline{6 \text{ distinct cyclic subgroups of order } 4}$.

(12) Prove that a cyclic group of order 16 cannot be expressed as a direct product of two of its proper subgroups.

Let $G = \langle a \rangle$, $O(G) = 16 = O(a) \rightarrow$ finite cyclic group

For every positive divisor $d\,(= 1, 2, 4, 8, 16)$ of $O(G)$ there exists a unique subgroup of order d.

For $d = 1$, it is the trivial subgroup $\{e\}$ of G.

& For $d = 16$, " " " improper " G.

So non-trivial proper subgroups of G are of order 2, 4 and 8.

Let us assume that $G = H \times K$, where H, K are proper subgroups of G.

Then (i) $G = HK$, (ii) $H \cap K = \{e\}$, (iii) $hk = kh, \forall h \in H, \forall k \in K$.

Now, if H be the trivial subgroup $\{e\}$, then K becomes the improper subgroup G, by (i). $[\because O(G) = O(H).O(K)]$

So, both the groups H & K are non-trivial proper subgroups which are of order 2, 4 and 8.

Now, by (i) if $O(H) = 2$ then $O(K) = 8$ as $O(G) = 16$.

Now $O(H) = 2 \Rightarrow H = \{e, a^8\}$, since $O(a^8) = 2$, $H = \langle a^8 \rangle$.

& $O(K) = 8 \Rightarrow K = \langle a^2 \rangle$, $O(a^2) = 8$; $K = \{e, a^2, a^4, a^6, a^8, a^{10}, a^{12}, a^{14}\}$.

We see that $H \cap K = \{e, a^8\} \neq \{e\}$, and this violates (ii).

$\therefore$ G cannot be expressed as a direct product of two of its proper subgroups.

(13) G is a cyclic group of order 18. Express G as a direct product of two of its proper subgroups.

As in the problem (12), $d = 1, 2, 3, 6, 9, 18$.

$d = 1 \Rightarrow$ trivial subgroup $\{e\}$ and $d = 18 \Rightarrow$ improper subgroup G.

Here also both the groups H and K are non-trivial proper subgroups which are of order 2, 3, 6, 9.

Now if $O(H) = 2$ then $O(K) = 9$ as $O(G) = 18$.

$\Rightarrow$ $H = \langle a^9 \rangle = \{e, a^9\}$. And $K = \langle a^2 \rangle = \{e, a^2, a^4, a^6, \ldots, a^{16}\}$

And we see $H \cap K = \{e\}$.

$\therefore$ G can be expressed as a direct product of two of its proper subgroups $H = \langle a^9 \rangle$ & $K = \langle a^2 \rangle$.

(11) Prove that the symmetric group S_3 cannot be expressed as a direct product of two of its proper subgroups.

$S_3 = \{\rho_0, \rho_1, \rho_2, \rho_3, \rho_4, \rho_5\}$, $O(S_3) = 6$.

All its subgroups (cyclic) are:

$\{\rho_0\}$, $\{\rho_0, \rho_1, \rho_2\}$, $\{\rho_0, \rho_3\}$, $\{\rho_0, \rho_4\}$, $\{\rho_0, \rho_5\}$, S_3.

If we take the direct product of trivial subgroup $\{\rho_0\}$ & improper subgroup S_3 then $S_3 = H \times K$, where $H = \{\rho_0\}$, $K = S_3$.

But S_3 is not here the direct product of two of its proper subgroups.

So, both the subgroups H & K are non-trivial proper subgroups.

Let us take $H = \{\rho_0, \rho_1, \rho_2\}$ & $K = \{\rho_0, \rho_3\}$, then if $h = \rho_1 \in H$ & $k = \rho_3 \in K$, then $hk \neq kh$, since

$hk = \rho_1\rho_3 = \rho_5$ and $kh = \rho_3\rho_1 = \rho_4$.

$\therefore$ $S_3 \neq H \times K$ for this case.

Again, if we take $H = \{\rho_0, \rho_1, \rho_2\}$ & $K = \{\rho_0, \rho_4\}$ or $K = \{\rho_0, \rho_5\}$, then also $hk \neq kh$, as $\rho_1\rho_4 = \rho_3$ & $\rho_4\rho_1 = \rho_5$ for $K = \{\rho_0, \rho_4\}$

and $\rho_1\rho_5 = \rho_4$ & $\rho_5\rho_1 = \rho_3$ for $K = \{\rho_0, \rho_5\}$

$\therefore$ In any case, S_3 cannot be expressed as the direct product of two of its proper subgroups.