properties of external direct product

# Group Theory - II (DSE-33).

## Unit-2

Let $G_1$ and $G_2$ be two groups. Now, the cartesian product of the sets $G_1$ and $G_2$ is the set $G_1 \times G_2$ of all ordered pairs $(a_1, b_1)$, where $a_1 \in G_1$, $a_2 \in G_2$. Now define a binary operation $*$ on $G_1 \times G_2$ as follows.

$$(a_1,b_1) * (a_2,b_2) = (a_1 \cdot a_2, b_1 \cdot b_2) \quad \forall (a_1,b_1), (a_2,b_2) \in G_1 \times G_2$$

$\cdot$ is binary operation on $G_1$, $G_2$

which is denoted by $(G_1 \oplus G_2, *)$ or $(G_1 \times G_2, *)$.

**Def 2: (External Direct product).**

Let $G_1, G_2, \cdots G_n$ be a finite collection of groups, The external direct product of $G_1, G_2, \cdots, G_n$, written as $G_1 \oplus G_2 \oplus \cdots \oplus G_n$ or $G_1 \times G_2 \times \cdots \times G_n$, is the set of all n-tuples for which the $i$th component is an element of $G_i$ and the operation is component-wise.

$$G_1 \oplus G_2 \oplus \cdots \oplus G_n = \{ (g_1, g_2, \cdots g_n) \mid g_i \in G_i \};$$

where $(g_1, g_2, \cdots, g_n) * (g_1', g_2', \cdots, g_n') = (g_1 g_1', g_2 g_2', \cdots g_n g_n')$.

(H.T) Show that $(G_1 \oplus G_2 \oplus \cdots \oplus G_n, *)$ is a group.

Ex: This construction is not new, we know $\mathbb{R}^2 = \mathbb{R} \oplus \mathbb{R}$,

(i) $\mathbb{R}^3 = \mathbb{R} \oplus \mathbb{R} \oplus \mathbb{R}$.

(ii) $U(8) \oplus U(10)$.

we know $U(8) = \{ u : g.c.d(u,8) = 1 \} = \{1, 3, 5, 7\}$

$U(10) = \{ u : g.c.d(u,10) = 1 \} = \{1, 3, 7, 9\}$

$\therefore U(8) \oplus U(10) = \{ (1,1), (1,3), (1,7), (1,9), (3,1), (3,3), (3,7), (3,9), (5,1), (5,3), (5,7), (5,9), (7,1), (7,3), (7,7), (7,9) \}$

Now $(1,3)(3,7) = (3,1)$. [ $3 \times 7 = 21 \to 1$ $10\overline{)21}\ \frac{2}{20}\ 1$ ].

$(3,7)(5,9) = ?$

(iii) $\mathbb{Z}_2 \oplus \mathbb{Z}_3$

We know $\mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$, $\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$.

$\mathbb{Z}_2 \oplus \mathbb{Z}_3 = \{ (\bar{0},\bar{0}), (\bar{0},\bar{1}), (\bar{1},\bar{0}), (\bar{1},\bar{1}), (\bar{1},\bar{2}) \}$.

**Th:** Let $G_1, G_2$ be two groups. Then the set

$G_1 \oplus G_2 = \{ (g_1, g_2) \mid g_1 \in G_1, g_2 \in G_2 \}$ is a group and

(i) $H_1 = \{ (a_1, e_2) \in G_1 \oplus G_2 \mid e_2$ is identity element of $G_2 \}$ is a normal subgroup of $G_1 \oplus G_2$ and $G_1 \simeq H_1$

(ii) $H_2 = \{ (e_1, a_2) \in G_1 \oplus G_2 \mid e_1$ is identity of $G_1 \}$ is a normal subgroup of $G_1 \oplus G_2$ and $H_2 \simeq G_2$

(iii) $G_1 \oplus G_2 = H_1 H_2 = H_2 H_1$ ; $H_1 \cap H_2 = \{(e_1, e_2)\}$.

proof: (i) Show $G_1 \oplus G_2$ is a group. (H.T.)

(ii) Since $(e_1, e_2) \in H_1$, $H_1 \neq \phi$, Let $(a_1, e_2), (a_2, e_2) \in H_1$. Then

$$(a_1, e_2)^{-1}(a_2, e_2)$$
$$= (a_1^{-1}, e_2)(a_2, e_2)$$
$$= (a_1^{-1}a_2, e_2) \in H_1 \because a_1^{-1}a_2 \in G_1$$

$\therefore H_1$ is a subgroup of $G_1 \oplus G_2$.

For normal:

Let $(a_1, b_1) \in G_1 \oplus G_2$ and $(g_1, e_2) \in H_1$

Then $(a_1, b_1)(g_1, e_2)(a_1, b_1)^{-1}$

$= (a_1 g_1 a_1^{-1}, b_1 b_1^{-1}) = (a_1 g_1 a_1^{-1}, e_2)$.

Since $a_1 g_1 a_1^{-1} \in G_1 \therefore (a_1 g_1 a_1^{-1}, e_2) \in H_1$

$\Rightarrow H_1$ is normal subgroup of $G_1$.

For Isomorphism:

Let $f: G_1 \to H_1$ be a mapping defined by

$f(a_1) = (a_1, e_2)$. $\forall a_1 \in G_1$

Now for one-one: Let $a_1, a_2 \in G_1$, then $f(a_1) = f(a_2)$

$\Rightarrow (a_1, e_2) = (a_2, e_2)$

$\Rightarrow a_1 = a_2$

$\Rightarrow f$ is one-one.

For onto: Let $(a_1, e_2) \in H_1$ then by the definition of $f$ clearly $\exists\ a_1 \in G_1$ s.t $f(a_1) = (a_1, e_2)$.

For homomorphism.

Let $a_1, a_2 \in G_1$ $f(a_1 a_2) = (a_1 a_2, e_2) = (a_1, e_2)(a_2, e_2)$
$= f(a_1) f(a_2)$

$\therefore f$ is isomorphism $\therefore G_1 \simeq H_1$

(ii) The proof is similar to (i)

(iii) Let $(a_1, a_2) \in G_1 \oplus G_2$. and $(a_1, e_2) \in H_1$, $(e_1, a_2) \in H_2$

Then $(a_1, e_2)(e_1, a_2) = (a_1, a_2)$

$\Rightarrow$ any arbitrary element of $G_1 \oplus G_2$ can be represent as product of two element of $H_1$ and $H_2$

we shall show that this representation is unique.

for this let $(a_1, a_2) = (a_1', e_2)(e_1, a_2')$.

$\Rightarrow (a_1', a_2') = (a_1, a_2)$

$\Rightarrow a_1' = a_1$, $a_2' = a_2$

$\Rightarrow$ the representation is unique.

To show $H_1 \cap H_2 = \{e\}$

Let $a \in H_1 \cap H_2$.

$\Rightarrow a \in H_1, \; a \in H_2$

$\Rightarrow a = (a_1, e_2) = (e_1, a_2)$.

$\Rightarrow a_1 = e_1$

$a_2 = e_2$

$\Rightarrow a = (e_1, e_2) = e$.

$\Rightarrow H_1 \cap H_2 = \{ e = (e_1, e_2) \}$.

Therefore $G_1 \oplus G_2 = H_1 H_2 = H_2 H_1$

Note: In general let $G = G_1 \oplus G_2 \oplus \cdots \oplus G_n$ and each $G_i$ are group then $(G, *)$ is a group with $e = (e_1, e_2, \cdots e_n)$ each $e_i$ are identity of $G_i$ and for $\forall (a_1, a_2, \cdots a_n) \in G$.

$(a_1, a_2, \cdots a_n)^{-1} = (a_1^{-1}, a_2^{-1}, \cdots a_n^{-1})$.

Furthermore, let

$H_i = \{ (e_1, e_2, \cdots, h_i, e_{i+1}, \cdots e_n) \mid h_i \in G_i \}. \; \forall i \in I_n$.

Then following hold

(i) $H_i \trianglelefteq G, \; \forall i \in I_n$

(ii) $\forall a \in G$, $a$ can be uniquely expressed as $a = h_1, h_2 \cdots h_n$ where $h_i \in H_i, \; \forall i \in I_n$

(iii) $H_i \cap (H_1, H_2, \cdots H_{i-1}, H_{i+1}, \cdots H_n) = \{e\} \; \forall i \in I_n$

(iv) $G = H_1 H_2 \cdots H_n$.

Th: (Order of an element in a Direct product).

The order of an element in a direct product of a finite number of finite group is the least common multiple of the orders of the components of the element, in symbols.

$$o(g_1, g_2, \cdots, g_n) = l.c.m\,(o(g_1), o(g_2), \cdots, o(g_n))$$

or $|(g_1, g_2, \cdots g_n)| = l.c.m\,(|g_1|, |g_2|, \cdots |g_n|)$.

Proof: Denote the identity of $G_i$ by $e_i$, let $S = l.c.m\,(|g_1|, |g_2|, \cdots |g_n|)$ and $t = |(g_1, g_2, \cdots g_n)|$. Since $S = l.c.m\,(|g_1|, |g_2|, \cdots |g_n|)$.

so $(g_1, g_2, \cdots g_n)^S = (g_1^S, g_2^S, \cdots g_n^S) = (e_1, e_2, \cdots e_n)$, we know that $t \leq S$. on the other hands, $(g_1, g_2, \cdots g_n)^t = (e_1, e_2, \cdots e_n)$

$\Rightarrow g_i^t = e_i$

$\Rightarrow t$ is common multiple of $|g_i| \; \forall i$

$\Rightarrow S \leq t$.

$\therefore \boxed{t = S}$

**Th!** Let $G_1, G_2$ be two groups. Then $G_1 \oplus G_2$ is abelian iff both $G_1$ and $G_2$ are abelian. (HT)

**Th!** Let $G_1$ and $G_2$ be two finite cyclic groups. Then $G_1 \oplus G_2$ is cyclic iff $|G_1|$, and $|G_2|$ are relatively prime.

**proof:** Let $|G_1| = m$, $|G_2| = n$ so that $|G_1 \oplus G_2| = mn$. To prove first part of this theorem, let $G_1 \oplus G_2$ is cyclic - we shall show that $m$ and $n$ are relatively prime. Suppose that $g.c.d(m,n) = d$, $(g_1, g_2)$ is generator of $G_1 \oplus G_2$:

$\therefore |(g_1, g_2)| = mn$.

$\therefore g.c.d(m,n) = d \Rightarrow d|m, d|n$

$\Rightarrow \frac{m}{d}, \frac{n}{d}$ are integers.

Now $(g_1, g_2)^{\frac{mn}{d}} = \left((g_1, g_2)^m\right)^{n/d} = (g_1^m, g_2^m)^{n/d}$

$= \left(g_1^{\frac{mn}{d}}, g_2^{\frac{mn}{d}}\right)$

$= \left((g_1^m)^{\frac{n}{d}}, (g_2^n)^{\frac{n}{d}}\right)$.

$= (e_1, e_2)$

$\therefore (g_1, g_2)^{mn} = (e_1, e_2)$ and $(g_1, g_2)^{\frac{mn}{d}} = (e_1, e_2) \Rightarrow mn \leq \frac{mn}{d}$.

$\Rightarrow d = 1$

To prove other part, let $g.c.d(m,n) = 1$. $G_1 = \langle g_1 \rangle$, $G_2 = \langle g_2 \rangle$ and

$\therefore |(g_1, g_2)| = l.c.m(|g_1|, |g_2|) = l.c.m(m,n)$.

$\Rightarrow |(g_1, g_2)| = mn$ $\because m, n$ are relatively prime

$\Rightarrow |(g_1, g_2)| = |G_1 \oplus G_2|$ so $G_1 \oplus G_2$ has an element of order $mn$ so $G_1 \oplus G_2$ is cyclic.

**corollary** (i) An external direct product $G_1 \oplus G_2 \oplus \cdots \oplus G_n$ of a finite number of finite cyclic group is cyclic iff $|G_i|$ and $|G_j|$ are relatively prime when $i \neq j$

(ii) prove that $\mathbb{Z}_m \oplus \mathbb{Z}_n \simeq \mathbb{Z}_{mn}$ iff $g.c.d(m,n) = 1$

**proof:** Since $g.c.d(m,n) = 1 \Rightarrow \mathbb{Z}_m \oplus \mathbb{Z}_n$ is cyclic and $|\mathbb{Z}_m \oplus \mathbb{Z}_n| = mn$ we now every (by previous theorem) finite cyclic group of order $K$ is isomorphic to $\mathbb{Z}_K$

$\therefore \mathbb{Z}_m \oplus \mathbb{Z}_n \simeq \mathbb{Z}_{mn}$.

**Conversely** $\mathbb{Z}_m \oplus \mathbb{Z}_n \simeq \mathbb{Z}_{mn}$ $\Rightarrow \mathbb{Z}_m \oplus \mathbb{Z}_n$ is cyclic

$\Rightarrow g.c.d(m,n) = 1$ $\Rightarrow$

(iii) VIV Show that the direct product $\mathbb{Z} \oplus \mathbb{Z}$ is not cyclic.

proof: Suppose that $\mathbb{Z} \oplus \mathbb{Z}$ is a cyclic group, let $(m,n)$ be a generator of $\mathbb{Z} \oplus \mathbb{Z}$ i.e, $\mathbb{Z} \oplus \mathbb{Z} = \langle (m,n) \rangle$.
We see that $(1,0), (0,1) \in \mathbb{Z} \oplus \mathbb{Z}$. so $\exists\ r, t$ s.t

$(1,0) = r(m,n)$, $(0,1) = t(m,n)$

$\Rightarrow rm = 1$, $nr = 0$ | $tm = 0$, $nt = 1$

But $rm = 1$ and $tm = 0$

$\Rightarrow t = 0$ [$\because rm = 1 \Rightarrow m \neq 0$].

$\therefore nt = 0$ but $nt = 1$.

which is contradiction.

so $\mathbb{Z} \oplus \mathbb{Z}$ is not cyclic.

Some problem: (1) Find the number of element of order 5 in $\mathbb{Z}_{25} \oplus \mathbb{Z}_5$. (V.V.I, ***).

Soln Here possible order of a element in $\mathbb{Z}_{25}$ are $\to 1, 5, 25$

" " " " $\mathbb{Z}_5 \to 1, 5$,

$\therefore$ possible order of element in $\mathbb{Z}_{25} \oplus \mathbb{Z}_5$ are.

$l.c.m(1,1) = 1$ $l.c.m(5,1) = 5$ $l.c.m(25,1) = 25$

$l.c.m(1,5) = 5$ $l.c.m(5,5) = 5$ $l.c.m(25,5) = 25$

case 1: $l.c.(1,5) = 5$

let $(a,b) \in \mathbb{Z}_{25} \oplus \mathbb{Z}_5$ s.t $o(a,b) = 5$.

$\therefore o(a) = 1$

$o(b) = 5$

$\therefore$ Number of element in $\mathbb{Z}_{25} \oplus \mathbb{Z}_5$ s.t $l.c.m(1,5) = 5$ are $= \phi(1)\,\phi(5) = 1 \cdot 4 = 4$. [$\because$ number of elem of order $d$, in $\mathbb{Z}_n$ $(d/n)$ is $\phi(d)$].

Case 2: $l.c.m(5,1) = 5$

let $(a,b) \in \mathbb{Z}_{25} \oplus \mathbb{Z}_5$ s.t $o(a,b) = 5$.

$\Rightarrow l.c.5(o(a), o(b)) = 5 = l.c.m(5,1)$

$\therefore o(a) = 5$

$o(b) = 1$

~~$\therefore$ Number of element in $\mathbb{Z}_{25} \oplus \mathbb{Z}_5$ s.t $l.c.m(5,1) = 5$~~

Number of element of order 5 in $\mathbb{Z}_{25}$ is $\phi(5) = 4$

" " " 1 in $\mathbb{Z}_5$ is $(\phi(1) = 1$

$\therefore$ Number of elemnt in $\mathbb{Z}_{25} \oplus \mathbb{Z}_5$ s.t $l.c.m(5,1) = 5$ are $= \phi(5)\phi(1) = 4 \times 1 = 4$

Case-III $l.c.m(5,5) = 5$.

Let $(a,b) \in \mathbb{Z}_{25} \oplus \mathbb{Z}_5$ s.t

$o(a,b) = 5 \Rightarrow o(a) = 5, o(b) = 5$

∴ Number of element of order 5 in $\mathbb{Z}_{25} \oplus \mathbb{Z}_5$ s.t $l.c.m(5,5) = 5$ are $\varphi(5)\varphi(5) = 4 \cdot 4 = 16$

∴ Total number of elements of order 5 in $\mathbb{Z}_{25} \oplus \mathbb{Z}_5$

$= 1 + 4 + 16 = 21$

(2) Find the number of element of order 5 in $\mathbb{Z}_{15} \oplus \mathbb{Z}_5$.

(3) " " " " " 10 in $\mathbb{Z}_{100} \oplus \mathbb{Z}_{25}$

(4) " " 2 in $\mathbb{Z}_2 \oplus \mathbb{Z}_2$

(5) Write " $\mathbb{Z}_2 \oplus \mathbb{Z}_{30}$ " possible different forms.

Ans:

$$\mathbb{Z}_2 \oplus \mathbb{Z}_{30} \simeq \mathbb{Z}_{60}$$

$$\simeq \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$$

$$\simeq \mathbb{Z}_2 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_5$$

$$\simeq \mathbb{Z}_2 \oplus \mathbb{Z}_{15} \oplus \mathbb{Z}_{15}$$

This are all possible ways by

$\mathbb{Z}_2 \oplus \mathbb{Z}_{30} \not\simeq \mathbb{Z}_{60}$ (Why).