# External Direct Product :-

**Defn:-** Let $G_1, G_2, \ldots, G_n$ be a finite collection of grs. The external direct product of $G_1, G_2, \ldots, G_n$. written as $G_1 \oplus G_2 \oplus \ldots \oplus G_n$, is the set of all n-tuples for which the $i^{th}$ component is an element of $G_i$, and the operation is componentwise.

In symbols,

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

**Thm:-** $G_1 \oplus G_2 \oplus \ldots \oplus G_n$ is grp under componentwise

$$(g_1, g_2, \ldots, g_n)(g_1', g_2', \ldots, g_n') = (g_1 g_1', g_2 g_2', \ldots, g_n g_n')$$

**Proof:-** associative:- check (?)

identity :- $(e_1, e_2, \ldots, e_n)$

inverse. $(g_1^{-1}, g_2^{-1}, \ldots, g_n^{-1})$

**Examples**

$U(8) = \{1, 3, 5, 7\}$

(i) $U(8) \oplus U(10)$

$U(10) = \{1, 3, 7, 9\}$

$= \{(1,1), (1,3), (1,7), (1,9), (3,1), (3,3), (3,7), (3,9), (5,1), (5,3), (5,7), (5,9), (7,1), (7,3), (7,7), (7,9)\}$

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

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

for every $k$, divisor of $n$, define
$$U_k(n) = \{x \in U(n) \mid x \bmod k = 1\}$$

Thm:- $U_k(n)$ is a subgp of $U(n)$, for every divisor $k$ of $n$.

Proof:- $1 \in U_k(n) \Rightarrow U_k(n) \neq \phi$, $U_k(n) \subseteq U(n)$

Now let $x, y \in U_k(n)$

Claim:- $xy \in U_k(n)$ (Then finite subgp test $U_k(n)$ is subgp)

As $x \in U_k(n)$ $\quad$ $y \in U_k(n)$

$\Rightarrow$ $x \bmod k = 1$ $\quad$ $y \bmod k = 1$

$\Rightarrow$ $x = 1 + q_1 k$ $\quad$ $y = 1 + q_2 k$

$$\therefore xy = (1+q_1 k)(1+q_2 k)$$
$$= 1 + q_2 k + q_1 k + q_1 q_2 k$$
$$= 1 + k(q_2 + q_1 + q_1 q_2)$$

$\Rightarrow$ $xy \bmod k = 1$ $\Rightarrow$ $xy \in U_k(n)$

$\Rightarrow$ $U_k(n)$ is a subgp of $U(n)$

Thm:- Suppose $s$ and $t$ are relatively prime. Then $U(st) \approx U(s) \oplus U(t)$.

Moreover $U_s(st) \approx U(t)$ & $U_t(st) \approx U(s)$.

Proof:- Define $\phi : U(st) \to U(s) \oplus U(t)$ as

$$\phi(x) = (x \bmod s,\ x \bmod t)$$

well-defined,

let $x \bmod st = y \bmod st$

---

Two results

1.) Let $a, b, s, t \in \mathbb{Z}$.

If $a \bmod st = b \bmod st \Rightarrow a \bmod s = b \bmod s$ and $a \bmod t = b \bmod t$

Converse is true if $\gcd(s,t) = 1$

Proof:- Since $a \bmod st = b \bmod st$

$$\Rightarrow st \mid a-b \Rightarrow \underset{\substack{\parallel \\ a \bmod s = b \bmod s}}{s \mid a-b} \ \& \ \underset{\substack{\parallel \\ a \bmod t = b \bmod t}}{t \mid a-b}$$

Now assume $\gcd(s,t) = 1$

and $a \bmod s = b \bmod s$, $a \bmod t = b \bmod t$

$\Rightarrow s \mid a-b$ $\qquad \Rightarrow t \mid a-b$

then $\operatorname{lcm}(s,t) \mid a-b \Rightarrow st \mid a-b$

2. If $\gcd(a, bc) = 1 \Leftrightarrow \gcd(a,b)=1$ & $\gcd(a,c)=1$

Proof: By fundamental thm of arithmatic

$a = p_1 p_2 \cdots p_r \quad b = q_1 q_2 \cdots q_l, \quad c = r_1 r_2 \cdots r_k$

then

$\gcd(a, bc) = 1 \Leftrightarrow p_i \neq q_j$ & $p_i \neq r_h$

$\gcd(a, b) = 1 \Leftrightarrow p_i \neq q_j$

$\gcd(a, c) = 1 \Leftrightarrow p_i \neq r_h$.

---

<u>well-defined</u>:

$x \bmod st = y \bmod st$

$\Rightarrow x \bmod s = y \bmod s$ & $x \bmod t = y \bmod t$

$\Rightarrow (x \bmod s, x \bmod t) = (y \bmod s, y \bmod t)$

(Using result ①)

$\Rightarrow \phi(x) = \phi(y)$.

<u>One-One</u> let. $\phi(x) = \phi(y)$

$\Rightarrow (x \bmod s, x \bmod t) = (y \bmod s, y \bmod t)$

$\Rightarrow x \bmod s = y \bmod s$ & $x \bmod t = y \bmod t$

$\Rightarrow x \bmod st = y \bmod st$ (Using ① second part)

<u>Onto</u>. Let $(a, b) \in U(s) \oplus U(t)$

$\Rightarrow \gcd(a, s) = 1, \quad \gcd(b, t) = 1$

Scanned by CamScanner

And as $\gcd(s,t) = 1$

$\Rightarrow \exists\ q_1, q_2 \in \mathbb{Z}$ s.t. $sq_1 + tq_2 = 1$

$\Rightarrow \gcd(t, q_1) = 1$ & $\gcd(s, q_2) = 1$

Now let $z = bsq_1 + atq_2$

<u>Claim</u>:- $z \in U(st)$ and $\phi(z) = (a,b)$.

Now let $p \mid st$ → prime $\Rightarrow p \mid s$ or $p \mid t$.

If $p \mid s \Rightarrow p \mid bsq_1$ but $p \nmid atq_2$ (As $\gcd(a,s) = 1$, $\gcd(t,s) = 1$, $\gcd(q_2,s) = 1$

$\Rightarrow p \nmid z$

IIIly $p \mid t \Rightarrow p \nmid z$

$\Rightarrow$ If $p \mid st$ then $p \nmid z$

$\Rightarrow \gcd(z, st) = 1$

$\Rightarrow z \in U(st)$.

Now we show that $\phi(z) = (a,b)$

Consider $z - a = bsq_1 + atq_2 - a$

$= bsq_1 + a(tq_2 - 1)$

$= bsq_1 + a(-sq_1) = s(bq_1 - aq_1)$

$\Rightarrow s \mid z - a \Rightarrow z \equiv a \bmod s$

IIIly $z \equiv b \bmod t$.

$\therefore \phi(z) = (z \bmod n, z \bmod t)$
$= (a, b)$

$\therefore$ for every $(a,b) \in U(n) \oplus U(t)$, $\exists\ z \in U(nt)$
s.t. $\phi(z) = (a,b)$.
$\Rightarrow \phi$ is onto.

<u>Operation preserve.</u>

$\phi(xy) = (xy \bmod n, xy \bmod t)$

$= (x \bmod n, x \bmod t) \cdot (y \bmod n, y \bmod t)$

$= \phi(x) \cdot \phi(y)$

$\Rightarrow \phi$ preserves operation.

$\Rightarrow \phi$ is an isomorphism.

Thus, $U(nt) \approx U(n) \oplus U(t)$.

Now, for $U_n(nt) \approx U(t)$ (for onto $b \in U(t)$, then $z = tq_2 + bnq_1$)

Consider $\phi(x) = x \bmod t$

and for $U_t(nt) \approx U(n)$

$\phi(x) = x \bmod n$.

<u>Corollary</u>:- Let $m = n_1 n_2 \cdots n_k$, where $\gcd(n_i, n_j) = 1$ for $i \neq j$.

Then $U(m) \approx U(n_1) \oplus U(n_2) \oplus \cdots \oplus U(n_k)$.

Scanned by CamScanner

Ex:-
$$U(105) \approx U(7) \oplus U(15)$$
$$U(105) \approx U(21) \oplus U(5)$$
$$U(105) \approx U(7) \oplus U(3) \oplus U(5)$$

Moreover,
$$U(7) \approx U_{15}(105) = \{1, 16, 31, 46, 61, 76\}.$$
$$U(15) \approx U_7(105) = \{1, 8, 22, 29, 43, 64, 71, 92\}.$$

$U(2) \approx \{0\}$ $\quad U(4) \approx Z_2$ $\quad U(2^n) \approx Z_2 \oplus Z_{2^{n-2}},\ n \geq 3$

and $\quad U(p^n) \approx Z_{p^n - p^{n-1}}$ for $p$ an odd prime.

Thus $\quad U(105) = U(3.5.7) \approx U(3) \oplus U(5) \oplus U(7)$
$$\approx Z_2 \oplus Z_4 \oplus Z_6.$$

and $\quad U(720) = U(16.9.5) \approx U(16) \oplus U(9) \oplus U(5)$

Now $\quad U(16) = U(2^4) \approx Z_2 \oplus Z_4$
$$U(9) = U(3^2) \approx Z_{3^2 - 3^1} = Z_6$$
$$U(5) \approx Z_4$$

Thus $\quad U(720) \approx Z_2 \oplus Z_4 \oplus Z_6 \oplus Z_4$

Thus $\quad |U(720)| = 2 \times 4 \times 6 \times 4 = 192$

And $U(720)$ ~~has~~ can have elements of order 1, 2, 3, 4, 6 & 12 only.

Q: Determine the no. of elements of order 12 in $U(720)$. → 96

Also, as $U(720) \approx Aut(\mathbb{Z}_{720})$

This tells that $|Aut(\mathbb{Z}_{720})| = 192$

and $Aut(\mathbb{Z}_{720})$ has 96 elements of order 12.

## Application

(1.) Determine the last two digit of $23^{123}$.

$$23^{123} \bmod 100$$

as $23 \in U(100) \approx U(4) \oplus U(25) \approx \mathbb{Z}_2 \oplus \mathbb{Z}_{20}$

$\Rightarrow \quad x^{20} = 1 \quad \forall\, x \in U(100)$

Thus $\quad 23^{20} = 1$

$$(23)^{123} = (23)^{120} \cdot (23)^3 = (23)^3 = (23)^2 \cdot 23$$

$$= 29 \cdot 23 = 67.$$

## Internal Direct Product

Suppose $H$ and $K$ are subgps of $G$, then

$$HK = \{ hk \mid h \in H,\ k \in K \}$$

Ex. 1 $U(24) = \{1, 5, 7, 11, 13, 17, 19, 23\}$

Let $H = \{1, 17\}$ $K = \{1, 13\}$

Then $HK = \{1, 13, 17, 15\}$ $\rightarrow$ HK is subgp of G

Ex. 2 In $S_3$, $H = \{(1), (12)\}$ $K = \{(1), (13)\}$

$HK = \{(1), (13), (12), (12)(13)\}$

$= \{(1), (13), (12), (132)\}$ $\rightarrow$ HK is not a subgp of G.

**Internal Direct Product of H and K**

Let H and K be normal subgroups of a group G. We say that G is the internal direct product of H and K and write $G = H \times K$ if

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

Ex:- $G = S_3$ $H = \langle (123) \rangle$

$= \{(123), (132), (1)\}$

$K = \langle (12) \rangle$ $\rightarrow$ Not normal.

$= \{(1), (12)\}$

$HK = \{(1), (123), (132), (12), (13), (23)\}$

But $G \not\approx H \oplus K$ As H & K are cyclic & $\gcd(|H|, |K|) = 1 \Rightarrow S_3$ is cyclic.

**Def$^n$:-** Internal Direct Product of $H_1 \times H_2 \times \dots \times H_n$

Let $H_1, H_2, \dots, H_n$ be a finite collection of normal subgps of $G$. We say that $G$ is the internal direct product of $H_1, H_2, \dots, H_n$ and write $G = H_1 \times H_2 \times \dots \times H_n$ if

(i) $G = H_1 H_2 \dots H_n = \{h_1 h_2 \dots h_n \mid h_i \in H_i\}$

(ii) $(H_1 H_2 \dots H_i) \cap H_{i+1} = \{e\}$ for $i = 1, 2, \dots, n-1$

**Thm:-** If a group $G$ is the internal direct product of a finite number of subgps $H_1, H_2, \dots, H_n$, then $G \approx H_1 \oplus H_2 \oplus \dots \oplus H_n$

or $H_1 \times H_2 \times \dots \times H_n \approx H_1 \oplus H_2 \oplus \dots \oplus H_n$.

**Proof:-**

**Lemma ①:-** If $G$ is the internal ~~idea~~ direct product of $H_1, H_2, \dots, H_n$ and $i \neq j$ with $1 \leq i \leq n$, $1 \leq j \leq n$, then $H_i \cap H_j = \{e\}$.

**Proof:-** ~~Let~~ As $i \neq j$ and let $i < j$

then By defination.

$H_1 H_2 \dots H_i H_{i+1} \dots H_{j-1} \cap H_j = \{e\}$

Now let $x \in H_i \cap H_j$

$\Rightarrow x \in H_i$ & $x \in H_j$

Thus $(e\, e \ldots x \ldots e \ldots e) \in H_1 H_2 \ldots H_i H_{i+1} \ldots H_{j-1}$

$\Rightarrow x \in H_1 H_2 \ldots H_i H_{i+1} \ldots H_{j-1}$

and also $x \in H_j$

$\Rightarrow x \in H_1 H_2 \ldots H_i H_{i+1} \ldots H_{j-1} \cap H_j$

Thus $x = \{e\}$

Hence $H_i \cap H_j = \{e\} \quad \forall\ i \neq j$

**Lemma 2.** If $G$ is IDP of $H_1, H_2, \ldots, H_n$, Then $h$'s from different $H_i$'s commute.

**Proof:-** **Claim:-** $\left.\begin{array}{l}\text{let } h_i \in H_i \text{ \& } h_j \in H_j \\ \text{then } h_i h_j = h_j h_i\end{array}\right\}$.

let $h_i \in H_i$ and $h_j \in H_j$ with $i \neq j$

then $(h_i h_j h_i^{-1}) h_j^{-1} \in H_j h_j^{-1} = H_j$

and $h_i (h_j h_i^{-1} h_j^{-1}) \in h_i H_i = H_i$

Thus $h_i h_j h_i^{-1} h_j^{-1} \in H_i \cap H_j$

$\Rightarrow h_i h_j h_i^{-1} h_j^{-1} = e \qquad$ ( By lemma 1 )

$\Rightarrow h_i h_j = h_j h_i$

$\Rightarrow h$'s from different $H_i$'s commute.