G_1, G_2 groups.

$$G_1 \oplus G_2 = \{(g_1, g_2) \mid g_1 \in G_1, g_2 \in G_2\}$$

$$(g_1, g_2)(g_1', g_2') = (g_1 g_1', g_2 g_2') \in G_1 \oplus G_2$$

$\underline{e} = (e_1, e_2)$ identity

$$(g_1, g_2)^{-1} = (g_1^{-1}, g_2^{-1}) \in G_1 \oplus G_2$$

$\therefore$ $G_1 \oplus G_2$ is a group, called the direct product (= direct sum) of G_1 and G_2.

In general,

$G_1, G_2, \cdots, G_K$ groups

$$G_1 \oplus G_2 \oplus \cdots \oplus G_K = \{(g_1, g_2, \cdots, g_K) \mid g_i \in G_i\}$$

$$(g_1, g_2, \cdots, g_K)(g_1', g_2', \cdots, g_K') = (g_1 g_1', \cdots, g_K g_K')$$

$$\underline{e} = (e_1, e_2, \cdots, e_K)$$

$$(g_1, g_2, \cdots, g_K)^{-1} = (g_1^{-1}, g_2^{-1}, \cdots, g_K^{-1})$$

(1) $|G_1| = m$, $|G_2| = n$

$\Rightarrow |G_1 \oplus G_2| = mn$

(2) $g_1 \in G_1$, $o(g_1) = m$

$g_2 \in G_2$, $o(g_2) = n$

$\Rightarrow o(g_1, g_2) = ?$

$g_1^m = e_1$, $g_2^n = e_2$

$(g_1, g_2) \in G_1 \oplus G_2$

$(g_1, g_2)^k = (g_1^k, g_2^k) = (e_1, e_2)$ if

$k = \operatorname{lcm}(m, n)$

$\Rightarrow o(g_1, g_2) = \operatorname{lcm}(m, n)$

Ex(1) $G_1 = \mathbb{Z}_2 = \{0,1\}$, $G_2 = \mathbb{Z}_3 = \{0, 1, 2\}$

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

$o(0,0) = 1$, $o(0,1) = 3$, $o(0,2) = 3$, $o(1,0) = 2$, $o(1,1) = 6$, $o(1,2) = 6$

$\Rightarrow \langle (1,1) \rangle = \mathbb{Z}_2 \oplus \mathbb{Z}_3 = \langle (1,1)^{-1} \rangle = \langle (1,2) \rangle$

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

$o(0,0)=1,\ o(0,1)=2,\ o(1,0)=2,\ o(1,1)=2$

$\Rightarrow \mathbb{Z}_2 \oplus \mathbb{Z}_2$ not cyclic.

Thm: $\mathbb{Z}_r \oplus \mathbb{Z}_s$ is cyclic $\Leftrightarrow \gcd\{r,s\}=1$.

$G_1, G_2, \cdots, G_k$

$G_1 \oplus G_2 \oplus \cdots \oplus G_k = \{(g_1, g_2, \cdots, g_k) \mid g_i \in G_i\}$

$(g_1, g_2, \cdots, g_k)(g_1', g_2', \cdots, g_k') = (g_1 g_1', g_2 g_2', \cdots g_k g_k')$

$\underline{e} = (e_1, e_2, \cdots, e_k)$

$(g_1, g_2, \cdots, g_k)^{-1} = (g_1^{-1}, g_2^{-1}, \cdots, g_k^{-1})$

(1) $|G_1 \oplus G_2 \oplus \cdots \oplus G_k| = |G_1||G_2| \cdots |G_k|$

(2) $o(g_1, g_2, \cdots, g_k) = \text{lcm}\{o(g_1), o(g_2), \cdots, o(g_k)\}$

(3) $G_1, G_2, \cdots, G_k$ abelian

$\Rightarrow G_1 \oplus G_2 \oplus \cdots \oplus G_k$ abelian.

(4) G_1, G_2 groups

$$\begin{aligned} \varphi : G_1 \oplus G_2 &\longrightarrow G_2 \oplus G_1 \\ (g_1, g_2) &\longmapsto (g_2, g_1) \end{aligned}$$

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

<u>Exer:</u> φ is an isomorphism.

<u>Thm:</u> G_1 and G_2 cyclic groups and

$|G_1| = m, \quad |G_2| = n.$

Then $G_1 \oplus G_2$ cyclic $\Leftrightarrow \gcd(m,n) = 1.$

Suppose $\gcd(m,n) = 1 \Rightarrow \operatorname{lcm}(m,n) = mn$

$G_1 = \langle a_1 \rangle, \quad G_2 = \langle a_2 \rangle$

$\Rightarrow o(a_1) = m, \quad o(a_2) = n$

$\Rightarrow o(a_1, a_2) = \operatorname{lcm}(m,n) = mn$

$\Rightarrow \langle (a_1, a_2) \rangle = G_1 \oplus G_2 \Rightarrow G_1 \oplus G_2$ cyclic.

Conversely, suppose $G_1 \oplus G_2$ cyclic

Let $\gcd(m,n) = d > 1$

$\Rightarrow m = sd, \quad n = td$

$\Rightarrow o(a_1^s) = d, \quad o(a_2^t) = d$

$(a_1^s, e_2), (e_1, a_2^t) \in G_1 \oplus G_2$

$|\langle (a_1^s, e_2) \rangle| = d, \quad |\langle (e_1, a_2^t) \rangle| = d$

$(a_1^s, e_2) \neq (e_1, a_2^t)$

which is a contradiction.

$\Rightarrow \gcd(m,n) = 1.$

Example:

(1) Is $\mathbb{Z}_2 \oplus \mathbb{Z}_3 \approx \mathbb{Z}_6$? yes

(2) Is $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \approx \mathbb{Z}_4$? No.

Ex(3) $G = \mathbb{Z}_{25} \oplus \mathbb{Z}_5$

(i) How many elements of order 5 G has?

$(a,b) \in G$, $a \in \mathbb{Z}_{25}$, $b \in \mathbb{Z}_5$

$o(a,b) = \operatorname{lcm}(o(a), o(b))$

$o(a,b) = 5$

(1) $o(a) = 5$, $o(b) = 1$ 4

$(5,0), (10,0), (15,0), (20,0)$

(2) $o(a) = 1$, $o(b) = 5$ 4

$(0,1), (0,2), (0,3), (0,4)$

(3) $o(a) = 5$, $o(b) = 5$ 16

$(5,1), (5,2), (5,3), (5,4)$

$(10,1), (10,2), (10,3), (10,4)$

$(15,1), (15,2), (15,3), (15,4)$

$(20,1), (20,2), (20,3), (20,4)$.

$\therefore$ There are 24 elements of order 5 in $\mathbb{Z}_{25} \oplus \mathbb{Z}_5$.

(ii) How many subgroups of order 5 are there?

Each subgroup of order 5 has 4 elements of order 5.

$\Rightarrow$ # of (cyclic) subgroups of order 5

$$= \frac{24}{4} = 6$$

What are they?

$\langle(5,0)\rangle = \{(5,0),(10,0),(15,0),(20,0),(0,0)\}$

$\langle(0,1)\rangle = \{(0,1),(0,2),(0,3),(0,4),(0,0)\}$

$\langle(5,1)\rangle = \{(5,1),(10,2),(15,3),(20,4),(0,0)\}$

$\langle(5,2)\rangle = \{(5,2),(10,4),(15,1),(20,3),(0,0)\}$

$\langle(5,3)\rangle = \{(5,3),(10,1),(15,4),(20,2),(0,0)\}$

$\langle(5,4)\rangle = \{(5,4),(10,3),(15,2),(20,1),(0,0)\}$

HW P167 # 3, 4, 5, 6, 8, 10, 11, 15, 16, 17, 22, 23, 26, 27, 29, 30.

10/25

P169 #26

$|S_3 \oplus \mathbb{Z}_2| = 12$

$S_3 = \{(1), (12), (2,3), (13), (123), (132)\}$
orders: 1, 2, 2, 2, 3, 3

$\mathbb{Z}_2 = \{0, 1\}$
orders: 1, 2

$(a,b) \in S_3 \oplus \mathbb{Z}_2$
$o(a,b) = \text{lcm}\{o(a), o(b)\}$

$o(a)$	$o(b)$
1	1
2	2
3	

Possible orders
1
2
3
6

$\Rightarrow S_3 \oplus \mathbb{Z}_2$ does not have an element of order 12
$\therefore S_3 \oplus \mathbb{Z}_2 \not\approx \mathbb{Z}_{12}$

$\mathbb{Z}_6 \oplus \mathbb{Z}_2$: # of elts of order $2 = 1+1+1 = 3$
$S_3 \oplus \mathbb{Z}_2$: # of elts of order $2 = 1+3+3 = 7$
$\Longrightarrow \mathbb{Z}_6 \oplus \mathbb{Z}_2 \not\approx S_3 \oplus \mathbb{Z}_2$

D_6 : # of elts of order $2 \doteq 7$

$\{I, R, R^2, R^3, R^4, R^5, H, HR, HR^2, HR^3, HR^4, HR^5\}$
orders: 1, 6, 3, 2, 3, 6, 2, 2, 2, 2, 2, 2

$\cancel{\Rightarrow D_6 \not\approx S_3 \oplus \mathbb{Z}_2}$

$S_3 \oplus \mathbb{Z}_2$: # of elements of order 3 = 2

# of elements of order 6 = 2

Possible orders in A_4:

1

2

3

So A_4 has no elt. of order 6

$\Rightarrow S_3 \oplus \mathbb{Z}_2 \not\approx A_4$

$\therefore S_3 \oplus \mathbb{Z}_2 \approx D_6$.

#29: $\mathbb{Z}_9 \oplus \mathbb{Z}_3$

$(a, b) \in \mathbb{Z}_9 \oplus \mathbb{Z}_3$

$o(a, b) = 3$	$o(a)$	$o(b)$	
	1	3	$(0,1), (0,2)$
	3	1	$(3,0), (6,0)$
	3	3	$(3,1), (3,2)$ $(6,1), (6,2)$

# of elts of order 3 = 8

# of subgroups of order 3 $= \frac{8}{2} = 4$

$\langle(0,1)\rangle = \{(0,1), (0,2), (0,0)\}$

$\langle(3,0)\rangle = \{(3,0), (6,0), (0,0)\}$

$\langle(3,1)\rangle = \{(3,1), (6,2), (0,0)\}$

$\langle(3,2)\rangle = \{(3,2), (6,1), (0,0)\}$

#30 $\mathbb{Z}_4 \oplus \mathbb{Z}_4$

noncyclic subgroup of order 4:

$\{(0,0), (2,0), (0,2), (2,2)\}$

Cyclic subgroups of order 4:

$o(a,b) = 4$:

$o(a)$	$o(b)$	Elements
1	4	$(0,1), (0,3)$
4	1	$(1,0), (3,0)$
4	4	$(1,1), (1,3)$ $(3,1), (3,3)$
2	4	$(2,1), (2,3)$
4	2	$(1,2), (3,2)$
	~~total #~~	12

$\Rightarrow$ There are $\frac{12}{2} = 6$ cyclic subgroups of order 4.

$\langle(0,1)\rangle = \{(0,1), (0,2), (0,3), (0,0)\}$

$\langle(1,0)\rangle = \{(1,0), (2,0), (3,0), (0,0)\}$

$\langle(1,1)\rangle = \{(1,1), (2,2), (3,3), (0,0)\}$

$\langle(1,3)\rangle = \{(1,3), (2,2), (3,1), (0,0)\}$

$\langle(1,2)\rangle = \{(1,2), (2,0), (3,2), (0,0)\}$

$\langle(2,1)\rangle = \{(2,1), (0,2), (2,3), (0,0)\}$