Chapter Five : Some Applications of Groups
الفصل الخامس : بعض تطبيقات الزمر

Theorem 5.1: (Cayle's Theorem)

Every group is isomorphic to a group of permutations. That is:

If $(G, *)$ is any group, then $(G, *) \cong (F_G, o)$, where

$F_G = \{f_a : a \in G\}$, $f_a : G \to G$; $f_a(x) = a * x, \quad \forall\ x \in G$.

Proof:

Define $g : (G, *) \to (F_G, o)$ by $g(a) = f_a$, $\forall\ a \in G$.

To prove, g is homo. , 1-1, onto.

(1) Is g homo. ?

Let $a, b \in G$, $g(a*b) = f_{a*b} = f_a \text{ o } f_b = g(a) \text{ o } g(b) \Rightarrow$ g is homo.

(2) Is g 1-1 ?

Let $g(a) = g(b)\ \forall\ a, b \in G \Rightarrow f_a = f_b \Rightarrow f_a(x) = f_b(x) \Rightarrow a*x = b*x$

$\Rightarrow a = b \Rightarrow$ g is 1-1 .

(3) Is g onto ?

$Rg = \{g(a) : a \in G\} = \{f_a : a \in G\} = F_G$.

$\therefore (G, *) \cong (F_G, o)$.

Corollary5.2: Every finite group G of order n is isomorphic to a subgroup of S_n .

Example 5.3:

Consider the following Cayley table of a group G = {e, a, b, c}

*	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Then:

$f_e = \begin{pmatrix} e & a & b & c \\ e & a & b & c \end{pmatrix}$, $f_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = (1)(2)(3)(4) = (1)$

$f_a = \begin{pmatrix} e & a & b & c \\ a & e & c & b \end{pmatrix}$, $f_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} = (12)(34)$

$f_b = \begin{pmatrix} e & a & b & c \\ b & c & e & a \end{pmatrix}$, $f_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = (13)(24)$

$f_c = \begin{pmatrix} e & a & b & c \\ c & b & a & e \end{pmatrix}$, $f_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = (14)(23)$

G is isomorphic to the subgroups of S_4: {(1), (12)(34), (13)(24), (14)(23)}.

(i.e.) $G \cong \{ f_1, f_2, f_3, f_4\}$

Exercise (1): (H.W)

(1) Let $(G =\{1, -1, i, -i\}, \cdot)$ be a group using the Cayley′s Theorem of G.

(2) Show that $(Z_3, +_3) \cong$ a subgroup of S_3.

The Chain of the Group

Definition 5.4: Let $(H_i, *)$ be all subgroups of $(G, *)$, then the chain of the group $(G, *)$ is any finite sequence of subsets of G such that :

$$G = H_0 \supseteq H_1 \supseteq H_2 \supseteq \ldots \supseteq H_{n-1} \supseteq H_n = \{e\}$$

Remarks 5.5:

(1) The integer n is called the length of the chain.

(2) If each $(H_i, *)$ is normal subgroup, then the chain is called normal chain.

(3) The chain which has length 1 is called the trivial chain.

Example 5.6:

(1) The group $(Z_4, +_4)$ has two chains:

$Z_4 \supseteq \{\bar{0}\}$ (length 1, trivial chain)

$Z_4 \supseteq \{\bar{0}, \bar{2}\} \supseteq \{\bar{0}\}$ (length 2 , normal chain)

(2) The symm. group of square has normal chain of length 2 is:

$G_s \supseteq \{r_1, r_3\} \supseteq \{r_1\}$.

Composition Chain

Definition 5.7: In the group $(G, *)$, the descending sequence of sets: $G = H_0 \supseteq H_1 \supseteq H_2 \supseteq \dots \supseteq H_{n-1} \supseteq H_n = \{e\}$ forms a composition chain of G if :

(1) $(H_i, *)$ is a subgroup of $(G, *)$.

(2) $(H_i, *)$ is a normal subgroup of $(H_{i-1}, *)$.

(3) The inclusion $H_{i-1} \supseteq K \supseteq H_i$, when $(K, *)$ Is a normal subgroup of $(H_{i-1}, *)$ implies either $K = H_i$ or $K = H_{i-1}$.

Example 5.8: In the group $(Z_{24}, +_{24})$, the normal chain $Z_{24} \supseteq <\bar{2}> \supseteq \{\bar{0}\}$ is not composition chain since $<\bar{4}>$ and $<\bar{8}>$ least than $<\bar{2}>$ and the chain:

$$Z_{24} \supseteq <\bar{2}> \supseteq <\bar{4}> \supseteq <\bar{8}> \supseteq \{\bar{0}\}$$

$$Z_{24} \supseteq <\bar{3}> \supseteq <\bar{6}> \supseteq <\overline{12}> \supseteq \{\bar{0}\}$$

are composition chain.

Definition5.9: A normal subgroup $(H,*)$ is called a maximal normal subgroup of $(G, *)$ if $H \neq G$ and there exist no normal subgroup $(K, *)$ of $(G, *)$ such that $H \supseteq K \supseteq G$.

Remark 5.10: A chain $G = H_0 \supseteq H_1 \supseteq H_2 \supseteq \dots \supseteq H_{n-1} \supseteq H_n = \{e\}$ is a composition n chain for $(G, *)$, if each subgroup $(H_i, *)$ is a maximal subgroup of $(H_{i-1}, *)$.

Example 5.11: In $(Z_{12}, +_{12})$, the normal cyclic subgroup $<\bar{2}> = \{\bar{0}, \bar{2}, \bar{4} \dots , \overline{10}\}$ and $<\bar{3}> = \{\bar{0} ,\bar{3}\dots , \bar{9}\}$ are maximal normal subgroup of Z_{12}. The chain $Z_{12} \supseteq <\bar{2}> \supseteq <\bar{4}> \supseteq \{\bar{0}\}$ is a composition since $<\bar{2}>$ is a maximal of Z_{12}, $<\bar{4}>$ is a maximal of $<\bar{2}>$ and $\{\bar{0}\}$ is a maximal of $<\bar{4}>$.

Theorem 5.12: A normal subgroup $(H, *)$ of a group $(G, *)$ is maximal if and only if $(G/H, \otimes)$ is simple .

Proof: $(\Leftarrow)$ Let G/H be simple, to prove H is maximal.

$\therefore$ G/H simple $\Rightarrow$ G/H has only $e*H$ and G/H itself normal.

$\Rightarrow$ $e*H = H$ is maximal

$(\Rightarrow)$ Let H be a maximal , to prove G/H is a simple. (H.W)

Corollary5.13. The group $(G/H, \otimes)$ is a simple if $o(G/H)$ is a prime number.

Corollary 5.14: A chain $G = H_0 \supset H_1 \supset H_2 \supset \dots \supset H_{n-1} \supset H_n = \{e\}$ is a composition chain if $(G/H, \otimes)$ is a simple group.
$\forall\, H_i\ (H_{i-1} \mid H_i)$, $i = 0, 1, \dots, n$.

Example 5.15: The chain $Z_{60} \supset \langle\bar{3}\rangle \supset \langle\bar{6}\rangle \supset \langle\overline{12}\rangle \supset \{\bar{0}\}$ is a composition, since every normal subgroup of $(Z_{60}, +_{60})$ is normal.

$o(Z_{60} \mid \langle\bar{3}\rangle) = 3$ prime $\Rightarrow (\langle\bar{3}\rangle, +_{60})$ is max of Z_{60} and simple group.

$o(\langle\bar{3}\rangle \mid \langle\bar{6}\rangle) = 2$ prime $\Rightarrow (\langle\bar{6}\rangle, +_{60})$ is max of $(\langle\bar{3}\rangle, +_{60})$ and simple group.

$o(\langle\bar{6}\rangle \mid \langle\overline{12}\rangle) = 2$ prime $\Rightarrow (\langle\overline{12}\rangle, +_{60})$ is max of $(\langle\bar{6}\rangle, +_{60})$ and simple group.

$o(\langle\overline{12}\rangle \mid \{\bar{0}\}) = 5$ prime $\Rightarrow$ simple group and $\langle\{\bar{0}\}, +_{60}\rangle)$ is max of $\langle\overline{12}, +_{60}\rangle$.

Theorem 5.16: Every finite group $(G, *)$, $G \neq \{e\}$ has a composition chain.
(كل زمرة منتهية غير تافهة تحوي على سلسلة تركيبية او مركبة)

Jordan-Holder Theorem 5.17: If $(G, *)$ is finite group has more than one element, then any two composition chain are equivalence.

Example 5.18: In $(Z_{60}, +_{60})$, the two chains

$$Z_{60} \supset \langle\bar{3}\rangle \supset \langle\bar{6}\rangle \supset \langle\overline{12}\rangle \supset \{\bar{0}\}$$
$$Z_{60} \supset \langle\bar{2}\rangle \supset \langle\bar{6}\rangle \supset \langle\overline{30}\rangle \supset \{\bar{0}\}$$

are composition and equivalence, since

$(Z_{60} \mid \langle\bar{3}\rangle, \otimes) \cong (\langle\bar{2}\rangle \mid \langle\bar{6}\rangle, \otimes)$

$|\ Z_{60} \mid \langle\bar{3}\rangle\ | = 3 = |\ \langle\bar{2}\rangle \mid \langle\bar{6}\rangle\ |$

$(\langle\bar{3}\rangle \mid \langle\bar{6}\rangle, \otimes) \cong (Z_{60} \mid \langle\bar{2}\rangle, \otimes)$

$|\ Z_{60} \mid \langle\bar{2}\rangle\ | = 2 = |\ \langle\bar{3}\rangle \mid \langle\bar{6}\rangle\ |$

$(\langle\bar{6}\rangle \mid \langle\overline{12}\rangle, \otimes) \cong (\langle\overline{30}\rangle \mid \{\bar{0}\}, \otimes)$

$|\ \langle\bar{6}\rangle \mid \langle\overline{12}\rangle\ | = 2 = |\ \langle\overline{30}\rangle \mid \{\bar{0}\}\ |$

$(\langle\overline{12}\rangle \mid \{\bar{0}\}, \otimes) \cong (\langle\bar{6}\rangle \mid \langle\overline{30}\rangle, \otimes)$

$|\ \langle\overline{12}\rangle \mid \{\bar{0}\}\ | = 5 = |\ \langle\bar{6}\rangle \mid \langle\overline{30}\rangle\ |$

Note that each quotient group is simple and all the cyclic group has prime order.

Example 5.19: In $(Z_{12}, +_{12})$, the two chains

$$Z_{12} \supset <\bar{2}> \supset <\bar{4}> \supset \{\bar{0}\}$$

$$Z_{60} \supset <\bar{3}> \supset <\bar{6}> \supset \{\bar{0}\}$$

are composition and equivalence, since

$(Z_{12} \mid <\bar{2}>, \otimes) \cong (<\bar{3}> \mid <\bar{6}>, \otimes)$

$o(Z_{12} \mid <\bar{2}>) = o(<\bar{3}> \mid <\bar{6}>) = 2$

$\mid Z_{60} \mid <\bar{3}> \mid = 3 = \mid <\bar{2}> \mid <\bar{6}> \mid$

$(<\bar{2}> \mid <\bar{4}>, \otimes) \cong (<\bar{6}> \mid \{\bar{0}\}, \otimes)$

$o(<\bar{2}> \mid <\bar{4}>) = o(<\bar{6}> \mid \{\bar{0}\}) = 2$

$(<\bar{4}> \mid \{\bar{0}\}, \otimes) \cong (Z_{12} \mid <\bar{3}>, \otimes)$

$o(<\bar{4}> \mid \{\bar{0}\}) = o(Z_{12} \mid <\bar{3}>) = 3$

The Solvable Group الزمر القابلة للحل

Definition 5.20: A group $(G, *)$ is called solvable group if and only if $\exists$ a finite collection of subgroups of $(G,*)$ $H_0, H_1, H_2, \dots, H_{n-1}, H_n$ such that

(1) $G = H_0 \supset H_1 \supset H_2 \supset \dots \supset H_{n-1} \supset H_n = \{e\}$.

(2) $H_{i+1} \Delta H_i \quad \forall i = 0, \dots, n-1$.

(3) $H_i \mid H_{i+1}$ commutative group $\forall i = 0, \dots, n-1$.

Example 5.21: Every commutative group is a solvable group.

Solution:

Let $(G, *)$ be a commutative group.

To prove $(G, *)$ is a solvable group.

Let $H_0 = G$, $H_1 = \{e\}$

(1) $G = H_0 \supset H_1 = \{e\}$

(2) $H_1 \Delta H_0$ is true, since $\{e\} \Delta G$ or (every subgroup of a commutative group is normal).

(3) $G \mid \{e\} = G$ is a commutative group or the quotient of commutative group is commutative.

$\Rightarrow (G, *)$ is a solvable group.

Example 5.22: Show that (S_3, o) is a solvable group.

Solution: Let $H_0 = S_3$, $H_1 = \{ f_1, f_2, f_3 \}$, $H_2 = \{ f_1 \}$

(1) $S_3 = H_0 \supset H_1 \supset H_2 = \{ f_1 \}$

(2) $H_2 \Delta H_1$ is true, since $\{ f_1 \} \Delta \{ f_1, f_2, f_3 \}$

$H_1 \Delta H_0$ is true, since $[S_3:H_1] = 2 \Rightarrow H_1 \Delta S_3$

(3) To prove $H_i \mid H_{i+1}$ commutative group $\forall$ i = 0, 1

$o(H_1 \mid H_2) = \frac{o(H_1)}{o(H_2)} = \frac{3}{1} = 3 < 6 \Rightarrow H_1 \mid H_2$ is a commutative group.

$o(H_0 \mid H_1) = \frac{o(H_0)}{o(H_1)} = \frac{6}{3} = 2 < 6 \Rightarrow H_0 \mid H_1$ is a commutative group.

$\therefore$ (S_3, o) is a solvable group.

Exercise (2): Show that (G_s, o) is a solvable group. (H.W)

Theorem 5.23: Every subgroup of a solvable group is a solvable.

Proof: **(Without Proof).**

Theorem 5.24: Let $H \Delta G$ and $(G, *)$ is a solvable group, then $(G \mid H, \otimes)$ is a solvable group.

Proof: **(Without Proof).**

Theorem 5.25: Let $H \Delta G$ and both $(H, *)$ and $(G \mid H, \otimes)$ are solvable groups, then $(G, *)$ is a solvable group.

Proof: **(Without Proof).**

Finite P-Groups الزمر الاولية المنتهية

Definition 5.26: Let p a prime number. A finite group $(G, *)$ is called p-group iff the order of G is a power of p.

i.e. G is a p-group $\Leftrightarrow o(G) = p^k$, $k \in Z^+$.

Example 5.27:

$(Z_4, +_4)$, $o(Z_4) = 4 = 2^2$ is a 2-group .

$(Z_8, +_8)$, $o(Z_8) = 8 = 2^3$ is a 2-group .

$(Z_9, +_9)$, $o(Z_9) = 9 = 3^2$ is a 3-group .

$(Z_7, +_7)$, $o(Z_7) = 7 = 7^1$ is a 7-group .

(S_3,o) , $o(S_3) = 6 \neq p^k \Rightarrow (S_3,o)$ is not a p=group.

Definition 5.28: A finite group (G, *) is called p-group iff the order of each element of G has power of p.

Example 5.29: Prove that each of the following groups are p-groups by two ways:

(1) $(Z_4, +_4)$

- $o(Z_4) = 4 = 2^2 \Rightarrow Z_4$ is a 2-group
- $Z_4 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$

$$\left.\begin{array}{l} o(\bar{0}) = 1 = 2^0 = p^0 \\ o(\bar{1}) = 4 = 2^2 = p^2 \\ o(\bar{2}) = 2 = 2^1 = p^1 \\ o(\bar{3}) = 4 = 2^2 = p^2 \end{array}\right\} \Rightarrow \forall\, a \in Z_4,\ o(a) = 2^x,\ x \in Z^+$$

$\therefore (Z_4, +_4)$ is a 2- group.

(2) (Gs, o) (H.W)

Theorem 5.30: Let $H \Delta G$, then (G, *) is a p-group iff (H, *) and $(G \mid H, \otimes)$ are p-groups.

Proof: **(Without Proof).**

Remark 5.31: If G is non-trivial p-group , then $Cent(G) \neq e$.

Theorem 5.32: Every group of order p^2 is abelian.

Proof:

Let (G, *) be a group and $o(G) = p^2$, to prove G is abelian?

(Cent(G), *) is a subgroup of (G, *).

By Lagrange Theorem $o(Cent(G)) \mid o(G)$

$\Rightarrow o(Cent(G)) \mid p^2 \Rightarrow o(Cent(G)) = p^0$ or p^1 or p^2

If $o(Cent(G)) = p^0 \Rightarrow Cent(G) = \{e\}$ C! $\therefore o(Cent(G)) \neq p^0$

If $o(Cent(G)) = p^2 = o(G) \Rightarrow Cent(G) = G \Rightarrow G$ is comm.

If $o(Cent(G)) = p^1$, $o(\,(G) \mid Cent(G)\,) = \frac{p^2}{p} = p$, but p is a prime number

$\therefore G \mid cent(G)$ is cyclic

$\therefore$ G is comm.

Remark 5.33: The converse of Theorem 5.32 is not true in general.

Example 5.34: $(Z_8, +_8)$ is a comm. group , $o(Z_8) = 8 = 2^3 \neq p^2$.

First sylow Theorem 5.35: (نظرية سايلو الاولى)

Let p be a prime number and (G, *) be a finite group such that $p^x \mid o(G)$, $x > 0$, then G has a subgroup of order p^x which is called p-sylow subgroup of G.

If $m \mid o(G) \rightarrow \nexists$ H such that o(H) = m

If $p^x \mid o(G) \rightarrow \exists$ subgroup H , $o(H) = p^x$ p-sylow group.

Example 5.36: Is the following groups have p-sylow subgroup?

(1) (S_3, o), $o(S_3) = G = 6 = 2^1.3^1$

$2^1/6 \Rightarrow \exists$ subgroup H such that o(H) = 2 which is called 2-sylow subgroup.

$3^1/6 \Rightarrow \exists$ subgroup K such that o(K) = 3 which is called 3-sylow subgroup.

(2) (Gs, o) , $o(Gs) = 8 = 2^3$ is a 2-group.

Every subgroup H of Gs is 2-sylow subgroup, $o(H) = 2^0$ or 2^1 or 2^2 or 2^3

Second sylow Theorem 5.37: (نظرية سايلو الثانية)

The number of distinct p-sylow subgroups is 1+tp, t = 0, 1, … which is divides the order of G.

i.e. the number k = 1+tp , t = 0, 1, … and k/o(G) .

k.هو عدد الزمر الجزئية من نوع سايلو

Example 5.38: Find the distinct p-sylow subgroups of (S_3, o).

Solution:

$o(S_3) = 6 = (2)(3)$

$2/6 \Rightarrow \exists$ H is a subgroup s.t. o(H) = 2

The number of 2-sylow subgroups is k_1

$k_1 = 1+2t$, t = 0, 1, 2, … and $k_1/6$

$t=0 \Rightarrow k_1 = 1$ and $1/6$

$t=1 \Rightarrow k_1 = 3$ and $3/6$

$t=2 \Rightarrow k_1 = 5$ and $5 \nmid 6$

$t=3 \Rightarrow k_1 = 7$ and $7 \nmid 6$

$\therefore$ There are two 2-sylow subgroups.

$3/6 \Rightarrow \exists$ a subgroup K s.t. $o(K) = 3$

The number of 3-sylow subgroups is k_2

$K_2 = 1+3t$, $t = 0, 1, 2, \ldots$ and $k_2/6$

$t=0 \Rightarrow k_2 = 1$ and $1/6$

$t=1 \Rightarrow k_2 = 4$ and $4 \nmid 6$

$t=2 \Rightarrow k_2 = 7$ and $7 \nmid 6$

$\therefore$ There is one 3-sylow subgroup.

Example 5.39: Find the number of p-sylow subgroups of G such that $o(G) = 12$.

Solution: $o(G) = 12 = 3.2^2$

$3/12 \Rightarrow \exists$ H a subgroup H s.t. $o(H) = 3$

The number of 3-sylow subgroups is k_1

$k_1 = 1+3t$, $t = 0, 1, 2, \ldots$ and $k_1/12$

$t=0 \Rightarrow k_1 = 1$ and $1/12$

$t=1 \Rightarrow k_1 = 4$ and $4/12$

$t=2 \Rightarrow k_1 = 7$ and $7 \nmid 12$

$t=3 \Rightarrow k_1 = 10$ and $10 \nmid 12$

$\therefore$ There are two 3-sylow subgroups of G.

The number of 2-sylow subgroups of G is k_2

$K_2 = 1+2t$, $t = 0, 1, 2, \ldots$ and $k_2/12$

$t=0 \Rightarrow k_2 = 1$ and $1/12$

$t=1 \Rightarrow k_2 = 3$ and $3/12$

$t=2 \Rightarrow k_2 = 5$ and $5 \nmid 12$

$t=3 \Rightarrow k_2 = 7$ and $7 \nmid 12$

$\therefore$ There are two 2-sylow subgroups of G.

Remark 5.40: G has exactly one p-sylow subgroup H iff HΔG.

Example 5.41:

(S_3, o) , H = $\{f_1, f_2, f_3\}$, HΔ S_3

H is a 3-sylow subgroup of S_3

$\therefore$ $\exists$ one 3-sylow subgroup of S_3

Definition 5.42: Let (H,*) and (K,*) be two normal subgroups of (G,*), then (G,*) is called an internal direct product of H and K

{G is decomposition by H and K} iff G = H*K and H$\cap$K = {e}.

Example 5.43:

Let G = {e, a, b, c}, $a^2 = b^2 = c^2 = e$

H = {e, a}ΔG since G is comm. group.

K = {e, b}ΔG since G is comm. group.

H*K = {e, a, b, c} = G and H$\cap$K = {e}

$\therefore$G = H$\otimes$K is decomposition by H and K.

Example 5.44:

Let (G,×) be any group and H=G, K={e}, then HΔG, KΔG.

(1) H*K= G*{e} = G

(2) H$\cap$K= G$\cap${e} = {e}

$\therefore$G = H$\otimes$K = G$\otimes${e}

G has a trivial decomposition.

Example 5.45: Let $(Z_4, +_4)$ be a group. Is Z_4 has proper decomposition?

Solution: The subgroups of Z_4 are Z_4, $\{\bar{0}\}$, $\{\bar{0}, \bar{2}\}$.

Let H = Z_4 , K= $\{\bar{0}, \bar{2}\}$

H $\oplus_4$ K = Z_4 $\oplus_4$ $\{\bar{0}, \bar{2}\}$ = Z_4

H$\cap$K = Z_4 $\cap$ $\{\bar{0}, \bar{2}\}$ =$\{\bar{0}, \bar{2}\}$

$\therefore$ $Z_4 \neq Z_4 \otimes \{\bar{0}, \bar{2}\}$

Let H= $\{\bar{0}\}$, K = $\{\bar{0}, \bar{2}\}$

H $\oplus_4$ K = K $\neq Z_4$

$\therefore$ Z_4 has no proper decomposition.

Theorem 5.46: Let H and K be two normal subgroups of G and $G = H \otimes K$, then $G|H \cong K$ and $G|H \cong H$.

Proof:

Since $G = H \otimes K \Rightarrow H*K = G$ and $H \cap K = \{e\}$.

$G|H = (H*K)|H$, $(H*K)|H \cong K|(H \cap K)$ (By second theorem of isomorphism)

$G|H \cong K|\{e\} \Rightarrow G|H \cong K$

And $G|H = (H*K)|K$, $(H*K)|K \cong H|(H \cap K)$

$\therefore G|H \cong H|\{e\} \Rightarrow G|H \cong H$

Definition 5.47: Let $(G_1, *)$, $(G_2, \cdot)$ be two groups, define

$$G_1 \times G_2 = \{(a, b) : a \in G_1, b \in G_2\} \text{ such that}$$

$$(a, b) \odot (c, d) = (a*c, b \cdot d) \ni a, c \in G_1, b, d \in G_2.$$

Then $(G_1 \times G_2, \odot)$ is a group and called external direct product of G_1 and G_2.

Remark 5.48: Prove that $(G_1 \times G_2, \odot)$ is a group. (H.W)

Example 5.49: Let $G_1 = (Z_3, +_3)$, $G_2 = (Z_2, +_2)$. Find $G_1 \times G_2$.

Solution:

$Z_3 \times Z_2 = \{(\bar{0}, \bar{0}), (\bar{0}, \bar{1}), (\bar{1}, \bar{0}), (\bar{1}, \bar{1}), (\bar{2}, \bar{0}), (\bar{2}, \bar{1})\}$

$(\bar{1}, \bar{1}) \odot (\bar{2}, \bar{1}) = (\bar{0}, \bar{0})$

$o(Z_3 \times Z_2) = o(Z_3) \cdot o(Z_2) = 6$

Theorem 5.50: Let $(G_1, *)$, $(G_2, \cdot)$ be two groups, then:

(1) $(G_1 \times G_2, \odot)$ is abelian iff both G_1 and G_2 are abelian.

(2) $G_1 \times \{e_2\} \Delta G_1 \times G_2$.

(3) $\{e_1\} \times G_2 \Delta G_1 \times G_2$.

(4) $G_1 \cong G_1 \times \{e_2\}$.

(5) $G_2 \cong \{e_1\} \times G_2$.

Proof:

(1) ($\Rightarrow$) Suppose that $G_1 \times G_2$ is abelian.

To prove G_1 and G_2 are abelian.

Let $(a, e_2), (b, e_2) \in G_1 \times G_2$ such that $a, b \in G_1$, $e_2 \in G_2$

Since $G_1 \times G_2$ is abelian, then $(a, e_2) \odot (b, e_2) = (b, e_2) \odot (a, e_2)$

$(a*b, e_2) = (b*a, e_2) \Rightarrow a*b = b*a \Rightarrow (G_1, *)$ is an abelian group.

Similarly we prove that $(G_2, \cdot)$ is an abelian group.

($\Leftarrow$) Suppose that $(G_1, *)$ and $(G_2, \cdot)$ are abelian.

To prove $G_1 \times G_2$ is abelian.

Let $(a, b), (c, d) \in G_1 \times G_2$. To prove $(a, b) \odot (c, d) = (c, d) \odot (a, b)$

$(a, b) \odot (c, d) = (a*c, b.d)$ …. 1

$(c, d) \odot (a, b) = (c*a, d.b)$ …. 2

$a*c = c*a$ (G_1 is abelian)

$b.d = d.b$ (G_2 is abelian)

$\therefore (a, b) \odot (c, d) = (c, d) \odot (a, b) \Rightarrow G_1 \times G_2$ is abelian.

(2) To prove $G_1 \times \{e_2\} \Delta G_1 \times G_2$.

$G_1 \times \{e_2\} = \{(a,e_2), a \in G_1\} \neq \emptyset$

To prove $(G_1 \times \{e_2\}, \odot)$ is a subgroup of $G_1 \times G_2$.

Let $(a,e_2), (b,e_2) \in G_1 \times \{e_2\}$

$(a,e_2)\odot(b,e_2)^{-1} = (a,e_2)\odot(b^{-1},e_2^{-1}) = (a*b^{-1}, e_2) \in G_1 \times \{e_2\}$ $(a*b^{-1} \in G_1)$

$\therefore (G_1 \times \{e_2\}, \odot)$ is a subgroup of $G_1 \times G_2$.

To prove $G_1 \times \{e_2\} \Delta G_1 \times G_2$.

Let $(x, y) \in G_1 \times G_2 \wedge (a, e_2) \in G_1 \times \{e_2\}$

To prove $(x, y) \odot (a, e_2) \odot (x, y)^{-1} \in G_1 \times \{e_2\}$

$(x*a*x^{-1}, y \cdot e_2 \cdot y^{-1}) = (x*a*x^{-1}, e_2) \in G_1 \times \{e_2\}$

$\therefore G_1 \times \{e_2\} \Delta G_1 \times G_2$.

(3) $\{e_1\} \times G_2 \Delta G_1 \times G_2$. (H.W)

(4) To prove $G_1 \cong G_1\times\{e_2\}$.

Define $f : (G_{1,*}) \rightarrow (G_1\times\{e_2\}, \Theta) \ni f(a) = (a, e_2)$

f is a map?

Let $a_1, a_2 \in G_1$ and $a_1 = a_2$

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

$\therefore$ f is a map.

f is 1-1?

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

$\therefore$ f is 1-1.

f is a homo. map?

$f(a*b) = (a*b, e_2) = (a, e_2)\ \Theta\ (b, e_2) = f(a)\ \Theta\ f(b)$

$\therefore$ f is a homo. map.

f is onto?

$R_f = \{ f(a) : a\in G_1\} = \{(a, e_2) : a\in G_1\} = G_1\times\{e_2\}$

$\therefore$ f is onto.

$\Rightarrow (G_{1,*}) \cong (G_1\times\{e_2\}, \Theta)$

(5) $G_2 \cong \{e_1\}\times G_2$. (H.W)

<u>Theorem 5.51:</u> Let $(G_1, *)$ and $(G_2, \cdot)$ be two groups, then $G_1\times G_2$ is a p-group.

<u>Proof:</u>

Since G_1 is a p-group $\Rightarrow o(G_1) = p^{k1}$, where $k_1 \in Z^+$

And Since G_2 is a p-group $\Rightarrow o(G_2) = p^{k2}$, where $k_2 \in Z^+$

$o(G_1\times G_2) = o(G_1) \times o(G_2)$

$= p^{k1} \times p^{k2} = p^{k1+ k2}$, $k_1+ k_2 \in Z^+$

$\therefore G_1\times G_2$ is a p-group.