Date / /
Page No.

Tutorial - 1

Krishna Pandey
U20CS110

Ans-1. $A = \{a, b, c\}$ $n = 3$

$n[P(A)] = 2^n = 2^3 = 8$

$P(A) = \{\{\}, \{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{c, a\}, \{a, b, c\}\}$

Sol- 2) $A = \{1, 2, 3, 4, 5\}$, $B = \{a, b, c, d, e\}$

★ (a) $\{(1, a), (1, b), (2, d), (3, e), (4, c)\}$
Not a function as 1 has 2 images

(b) $\{(1, a), (2, b), (3, d), (4, c), (5, c)\}$
Yes Function, neither one-one nor onto

(c) $\{(1, a), (2, b), (3, d), (4, c)\}$
it is not a function as 5 has no image

(d) $\{(1, a), (2, a), (3, b), (4, c), (5, e)\}$
Yes is a function but not one-one neither onto

(e) $\{(1, a), (2, b), (3, e), (4, c), (5, d)\}$
Yes is a function one-one and onto.

In above case every one-one function is also an onto function & vice versa because when the function will be one-one it will have all elements images and since both have equal no. of elements so must be onto also.

3 $G = \{R, \cdot\}$

(a) $(Z, \cdot)$ → Not a subgroup
for $\forall I_i \in Z$

→ Associativity follows
$$(I_1 * I_2) * I_3 = I_1 * (I_2 * I_3)$$

→ Closure follows
as $I_1 * I_2 = I$

→ Identity follows & exist
let e be identity $\boxed{e = 1}$
$$I \cdot * e = I$$
$$\boxed{e = 1}$$

→ Inverse not exist
let I^{-1} be the inverse

$$I * I^{-1} = e$$
$$I * I^{-1} = 1$$
$$I^{-1} = \frac{1}{I}$$

since $\frac{1}{I} \notin Z$ ∴ inverse not exist

(b) $(Z, +)$ → Is a subgroup
for $x_i \in Z$

① Associativity follows
$$(x_1 * x_2) * x_3 = (x_1 + x_2) + x_3$$
$$= x_1 + (x_2 + x_3)$$

$= x_1 * (x_2 * x_3)$

hence associativity follow

(ii) Closure property exist

$x_1 * x_2 = (x_1 + x_2) \in Z$

(iii) Identity exist

Let e be the identity

$x_1 * e = x_1$

$x_1 + e = x_1$

$\boxed{e = 0}$

(4) Inverse exists

$x_1 * I^{-1} = e$

$x_1 + I^{-1} = 0$

$I^{-1} = -x_1 \in Z$

hence inverse exist

thus $(Z, +)$ is subgroup

(5) $(Q, \cdot)$ Q set of all rational numbers

$\longrightarrow$ Not a subgroup

(1) Associativity follows

(2) Closure follows

$x_1 * x_2 = x \quad x \in Q \quad x_1, x_2 \in Q$

(3) Identity exist

$x * e = x \quad x, e \in Q$

$\boxed{e = 1}$

e → identity element

(iv) Inverse Not exist

$x \cdot I^{-1} = e$ $x, I^{-1}, e \in Q$

$x \cdot I^{-1} = 1$ $\boxed{e = 1}$

$$\boxed{I^{-1} = \frac{1}{x}}$$

but in case of 0 inverse not exist

Hence not a sub group

(e) $(Q^+, \cdot)$ yes is a subgroup

let $x_i \in Q^+$

→ Associativity follows

let $= (x_1 * x_2) * x_3$

$= (x_1 \times x_2) \times x_3$

$= (x_1) \times (x_2 \times x_3)$

$= x_1 * (x_2 * x_3)$

$\therefore (x_1 * x_2) * x_3 = x_1 * (x_2 * x_3)$

Associativity followed

→ Closure property exist

$x_1 * x_2 = x$ $x \in Q^+$

→ Identity exist

$x * e = x$

$\boxed{e = 1}$ $x, e \in Q^+$

→ Inverse exist

$x * I^{-1} = e$

$I^{-1} = \frac{1}{x}$ $I^{-1} = \frac{1}{x} \in Q^+$

Hence its a subgroup

Date / /
Page No.

(e) $(Q^-, \cdot)$

for $q_i \in Q^-$

① Associativity exist

② Closure not follow

$\bar{q}_1 * \bar{q}_2 = +q \qquad +q \notin Q^-$

③ Identity ~~exist~~ not exist

$\bar{q}_1 * e = \bar{q}_1$

$e = 1 \notin Q^-$

④ Inverse ~~also not exist~~

$\bar{q}_1 * \bar{q}_1^{-1} = e$

$\bar{q}_1^{-1} = \frac{1}{q} \qquad \frac{1}{q} \in Q^-$

Hence inverse exist

So $\{Q^-, \cdot\}$ is not a group ~~as a~~

(f) $(R-Q, \cdot)$

① Associative exist

$(q_1 * q_2) * q_3 = q_1 * (q_2 * q_3) \quad q_1, q_2, q_3 \in R-Q$

② Closure Not followed

$q_1 * q_2 = q \rightarrow$ may not be in $(R-Q)$

$\boxed{\text{e.g. } (\sqrt{2} \times \sqrt{2}) = 2 \quad 2 \notin R-Q}$ $\quad q \notin (R-Q)$

③ Identity $e = 1 \qquad 1 \notin R-Q$

④ inverse exist

So $(R-Q, \cdot)$ not a group

Sol- 4. given $n \geq 2$ Z_n is not a group of (R_1) class for $n > 2$

let $n = 3$

So $Z_3 = \{0, 1, 2\}$

inverse for 0 & 2 not exist in Z_3

Hence proved that for $n \geq 2$ Z_n is not a group under multiplication of residue classes

Now $S = \{1, 2, 3, \ldots n-1\}$ is a set under multiplication module

let's prove it by contradiction
let n is not a prime

Then $n = pq$ [some composite
where p, q are some number

$\therefore$ $1 < p$ & $q < n-1$

$pq = 0$ [mod n]
but 0 is not in H

It is a contradiction to our assumption

$\therefore$ n is a prime number
Hence proved

Sol- 5 Order of Z_{12} (additive).

$\boxed{e=0} \rightarrow$ identity element

$Z_{12} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}, \bar{8}, \bar{9}, \bar{10}, \bar{11}\}$

element ($\bar{n}$)	order
$\bar{0}$	1
$\bar{1}$	12
$\bar{2}$	6
$\bar{3}$	4
$\bar{4}$	3
$\bar{5}$	12
$\bar{6}$	2
$\bar{7}$	12
$\bar{8}$	3
$\bar{9}$	4
$\bar{10}$	6
$\bar{11}$	12

$U_{12} = \{\bar{1}, \bar{5}, \bar{7}, \bar{11}\}$ under multiplication

$\boxed{e=1}$ = identity

element ($\bar{n}$)	order
$\bar{1}$	1
$\bar{5}$	2
$\bar{7}$	2
$\bar{11}$	2

Sol- 6 — $\{(R-\theta)^+ + \{1\}, \cdot\}$ to prove is a group

① Associativity

$$(q_1 * q_2) * q_3 = q_1 * (q_2 * q_3)$$

$$q_1, q_2, q_3 \in \{(R-\theta)^+ + \{1\}\}$$

② Closure $\not\vdash$ (no)

$$q_1 * q_2 = q \rightarrow \text{may be rational or irrational}$$

Hence Closure don't exist

③ Identity

$$q_1 * e = q_1$$

$$e = 1 \qquad e \notin \text{given set}$$

$$e \notin [(R-\theta)^+ + \{0\}]$$

So identity not exist

④ Inverse [not exist for $q = 0$]

$$q_1 * q^{-1} = e$$

$$q * q^{-1} = 1$$

$$q q^{-1} = 1$$

$$q^{-1} = \frac{1}{q} \qquad \frac{1}{q} \in [(R-\theta)^+ + \{0\}]$$

for $q = 0$ inverse not exist

So it is not a group

Ans- 7 →

$$\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}_{2\times 2} \quad a, b, c \in R$$

$ac \neq 0$ (given)

is a group or not ?

under ~~for~~ multiplication

① Associativity :

Let

$$A = \begin{bmatrix} a_1 & b_1 \\ 0 & c_1 \end{bmatrix} \quad B = \begin{bmatrix} a_2 & b_2 \\ 0 & c_2 \end{bmatrix}, \quad C = \begin{bmatrix} a_3 & b_3 \\ 0 & c_3 \end{bmatrix}$$

where $a_i, b_i, c_i \in R$
$i \in N$

for associativity

$$(A \star B) \star C = A \star (B \star C)$$

taking L.H.S $= (A \star B) \star C$

$$= \left\{ \begin{bmatrix} a_1 & b_1 \\ 0 & c_1 \end{bmatrix} \times \begin{bmatrix} a_2 & b_2 \\ 0 & c_2 \end{bmatrix} \right\} \begin{bmatrix} a_3 & b_3 \\ 0 & c_3 \end{bmatrix}$$

$$= \begin{bmatrix} a_1 a_2 & a_1 b_2 + b_1 c_2 \\ 0 & c_1 c_2 \end{bmatrix} \times \begin{bmatrix} a_3 & b_3 \\ 0 & c_3 \end{bmatrix}$$

$$= \begin{bmatrix} a_1 a_2 a_3 & a_1 a_2 b_3 + a_1 b_2 c_3 + b_1 c_2 c_3 \\ 0 & c_1 c_2 c_3 \end{bmatrix}$$

Date / /
Page No.

taking R.H.S $A \star (B \star C)$

$$= \begin{bmatrix} a_1 & b_1 \\ 0 & c_1 \end{bmatrix} \times \left\{ \begin{bmatrix} a_2 & b_2 \\ 0 & c_2 \end{bmatrix} \times \begin{bmatrix} a_3 & b_3 \\ 0 & c_3 \end{bmatrix} \right\}$$

$$\begin{bmatrix} a_1 & b_1 \\ 0 & c_1 \end{bmatrix} \times \left\{ \begin{bmatrix} a_2a_3 & a_2b_3 + b_2c_3 \\ 0 & c_2c_3 \end{bmatrix} \right.$$

$$= \begin{bmatrix} a_1a_2a_3 & a_1a_2b_3 + a_1b_2c_3 + b_1c_2c_3 \\ 0 & c_1c_2c_3 \end{bmatrix}$$

$= L.H.S$

thus $(A \star B) \star C = A \star (B \star C)$

thus associativity follows.

(2) Closure property

$A = \begin{bmatrix} a_1 & b_1 \\ 0 & c_1 \end{bmatrix}$ $B = \begin{bmatrix} a_2 & b_2 \\ 0 & c_2 \end{bmatrix}$

$\star \rightarrow$ multiplication property

$A \star B = A \times B$

$$= \begin{bmatrix} a_1 & b_1 \\ 0 & c_1 \end{bmatrix} \times \begin{bmatrix} a_2 & b_2 \\ 0 & c_2 \end{bmatrix}$$

$= (2 \times 2)$ matrix

Clearly (2×2) will also belongs to set as under multiplication

Closure followed

Date / /
Page No.

③ Identity

$$A = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \qquad a, b, c \in R$$

Let e be identity element

$$A * e = e * A = A$$

$$\begin{bmatrix} a & b \\ 0 & c \end{bmatrix} * e = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$$

$$\begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \times e = \begin{bmatrix} a & b \\ 0 & c \end{bmatrix}$$

$ac \neq 0$ (given)

$$e = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}_{2 \times 2}$$

$e \in \theta$ thus identity exis

④ Inverse

$$\begin{bmatrix} a & b \\ 0 & c \end{bmatrix} * B = e$$

B → inverse
e → identity

$$\begin{bmatrix} a & b \\ 0 & c \end{bmatrix} \times B = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

$|A| = ac \neq 0$ ∴ inverse exist

thus it is a group.

Proved

Date / /
Page No.

Sol-8 $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}_{2\times 2}$ $|A| = 1$

$a, b, c, d \in Z_5$

$Z_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$

to find inverse of $A = \begin{bmatrix} 3 & 4 \\ 4 & 4 \end{bmatrix}$ in $SL(2, Z_5)$

$$\text{adj}(A) = \begin{bmatrix} 4 & -4 \\ -4 & 3 \end{bmatrix}$$

we know $\bar{-4} = \bar{1}$ under Z_5

$$\text{adj}(A) = \begin{bmatrix} 4 & 1 \\ 1 & 3 \end{bmatrix}$$

$|A| = 12 - 16 = -4 =$ $[-\bar{4} = \bar{1}$ under Z_5
$= 1$

$|A| = 1$

$$A^{-1} = \frac{\text{adj}(A)}{|A|} = \frac{1}{1}\begin{bmatrix} 4 & 1 \\ 1 & 3 \end{bmatrix}$$

$$\boxed{A^{-1} = \begin{bmatrix} 4 & 1 \\ 1 & 3 \end{bmatrix}}$$ Ans

Date / /

Page No.

Shivalal

Sol-9 $3^m 6^n \in Q \quad m, n \in Z$

To check group under multiplication

① Associativity property

$(A*B)*C = A*(B*C) \quad m_1 m_2 m_3, n_1 n_2 n_3 \in Z$

$L.H.S = \{[3^{m_1} 6^{n_1}] * [3^{m_2} 6^{n_2}]\} [3^{m_3} 6^{n_3}]$

$(3^{m_1+m_2} \; 6^{n_1+n_2}) [3^{m_3} \; 6^{n_3}]$

$3^{m_1+m_2+m_3} \; 6^{n_1+n_2+n_3}$

$R.H.S = [3^{m_1} \; 6^{n_1}] * \{(3^{m_2} \; 6^{n_2}) * (3^{m_3} \; 6^{n_3})\}$

$3^{m_1+m_2+m_3} \; 6^{n_1+n_2+n_3}$

$L.H.S = R.H.S$

Associativity followed

② Closure property

$= (3^{m_1} \; 6^{n_1}) * (3^{m_2} \; 6^{n_2})$

$= 3^{m_1+m_2} \; 6^{n_1+n_2}$

$(n_1+n_2), (m_1+m_2) \in Z$

hence closure also followed

③ Identity

let e be the identity

$A * e = A$

$e = 1 \qquad 1 \in Q$

identity exist

Inverse

$A \star B = e$ $\quad$ B = inverse

$A, B, e \in Q$

$(3^m 6^n) \star B = 1$

$B = \dfrac{1}{3^m 6^n} \in Q$

Hence inverse exist

Hence $3^m 6^n$ is a group under multiplication

Date / /
Page No.

Ans-10 ① $O(\bar{4})$ in $Z_5 - \{\bar{0}\}$ under multiplication

$Z_5 - \{\bar{0}\} = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}\}$

$O(\bar{4}) = 2$

② $O(i)$ in $\{1, -1, i, -i\}$

$\boxed{e = 1}$

$O(\bar{i}) = 4$

$i = i$
$i^2 = -1$
$i^3 = -i$
$i^4 = 1$

③ $\{\omega^{15} = 1, \omega^1, \omega^2, \ldots \omega^{14}\}$

is a cyclic group

if $(K, n) = 1$ then a^K will be a generator
thus
$[\omega, \omega^2, \omega^4, \omega^7, \omega^8, \omega^{11}, \omega^{13}, \omega^{14}]$
are generators

e.g

$\omega^2 = \omega^2$
$(\omega^2)^2 = \omega^4$
$(\omega^2)^3 = \omega^6$
$(\omega^2)^4 = \omega^8$
$(\omega^2)^5 = \omega^{10}$
$(\omega^2)^6 = \omega^{12}$
$(\omega^2)^7 = \omega^{14}$
$(\omega^2)^8 = \omega$
$(\omega^2)^9 = \omega^3$

$(\omega^2)^{10} = \omega^5$
$(\omega^2)^{11} = \omega^7$
$(\omega^2)^{12} = \omega^9$
$(\omega^2)^{13} = \omega^{11}$
$(\omega^2)^{14} = \omega^{13}$
$(\omega^2)^{15} = 1$

④ $$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

$$f^2 = f \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

$$f \circ f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

⑤ $U(16) = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}, \bar{9}, \bar{11}, \bar{13}, \bar{15}\}$
↳ cyclic group

$Z_8 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}, \bar{7}\}$
~~↳ cyclic~~

order of $U(16)$

$o(\bar{1}) = 1$ $\quad$ $o(\bar{9}) = 2$
$o(\bar{3}) = 4$ $\quad$ $o(\bar{11}) = 4$
$o(\bar{5}) = 4$ $\quad$ $o(\bar{13}) = 4$
$o(\bar{7}) = 2$ $\quad$ $o(\bar{15}) = 2$

order of $Z_8 = 8$
~~order of $Z_8 = 8$~~

↳ $\boxed{\text{no element of order 8}}$

$|U(16)| = 8 = 2^3$
possible isomorphic classes of $U(16)$.

↳ Z_8, $Z_4 \oplus Z_2$, $Z_2 + Z_2 + Z_2$

To be isomorphic to Z_8, $U(16)$ must have an element of order 8, which is not there thus $U(16)$ is not isomorphic to Z_8