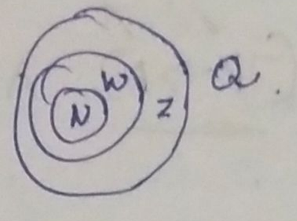
$N \to \{1, 2, 3, 4 \ldots\}$




$W \to \{0, 1, 2, 3 \ldots\}$

$Z = \{\infty -3, -2, -1, 0, 1, 2, \infty\}$

$Q \Rightarrow \{p/q, \; q \neq 0 \; 1/2, \ldots\}$

↓

Rational number.

$G = \{0, 1, 2, 3, 4 \ldots\}$

(+) $2, 3 \in G$

$2 + 3 = 5 \in G$.

1. Closure property: $\forall a, b \in G, \; a * b \in G$

2. Associative pr": $\forall a, b, c \in G, \; a * (b * c) = (a * b) * c$

3. Identity ": $\left.\begin{array}{l} a * e = a \\ e * a = a \end{array}\right\} \forall a \in G$.

4. Inverse: $\forall a, a^{-1} \in G, \; a * a^{-1} = a^{-1} * a = e$

$1 * 10 = 10$.
$0 + 10 = 10$

Iden → if we $5 + (\;) = 5$

↓

what number we add we get 5 that is identity element.

2   -2

$\frac{1}{2} = 1$

Identity element.

$+ \to 0$

$\times \to 1$

$$\boxed{\begin{array}{c} 2 + (-2) = 0. \\ \downarrow \\ \text{inverse elem} \\ x \times \left(\frac{1}{x}\right) = 1 \end{array}}$$

eg : $(Z, +)$ is a group.

Abelian group :

A group $(G, *)$ is said to be an abelian group if $a * b = b * a$, $\forall a, b \in G$.

i) commutative property.

eg : $(Z, +)$ is an AG.

Semi group :

i) Closure property

2) Associative "

eg : $(Z, \cdot)$ is a SG

$(Z, +)$ " "

Monoid :

1) Closure property

2) Associative "

3) Identity "

eg : $(Z, +)$ is a monoid.

order of group:

Let $G$ be a group under the binary operation $*$. The no of elements in $G$ is called the order of the group and is denoted by $O(G)$.

eg: ① Let $G = \{1, -1, i, -i\}$ then

$O(G) = 4$.

② $O(Z) = \infty$ , $Z \rightarrow$ set of all Integer.

---

1) Give an example of a semi group which is not a monoid.

$N = \{1, 2, 3 \ldots\ldots \infty\}$ $+$ $\checkmark$

$(N, +)$ this is not monoid.

$E = \{\cancel{-4}\ 2\ 0, 2, 4, 6, 8 \ldots\ldots \infty\}$

$(E, \cdot)$ not monoid but which is a semi group.

2) give an example of a monoid which is not a group.

$W = \{0, 1, 2, 3 \dots\}$

$(W, +)$ is monoid but not a group.

$Z = \{-\infty \dots -2, -1\ 0, 1, 2, 3 \dots \infty\}$

$(Z, \cdot)$ is monoid but not a group.

---

If $*$ is a binary operation on the set $R$ of real numbers defined by $a * b = a + b + 2ab$,

1) Prove that $(R, *)$ is a semi group.

2) Find the identity element if it exist.

3) which element has inverse and what are they?

soln:

$a, b \in R$ $\rightarrow$ closure

$a * b \in R.$

$a, b, c \in R$ $\rightarrow$ Associative.

$(a * b) * c = a * (b * c)$

i) Let $a, b \in R.$

$a * b \in R$

$a * b = a + b + 2ab \in R.$

ii) Associative.

Let us assume,

$a, b, c \in R$

T.P $(a * b) * c = a * (b * c).$ — ①.

LHS: $(a * b) * c$

$= \underbrace{(a + b + 2ab)}_{a} * \underbrace{c}_{b}$

$= (a + b + 2ab) + c + 2(a + b + 2ab)(c).$

$= a + b + 2ab + c + 2ac + 2bc + 4abc$

$= a + b + c + 2ab + 2ac + 2bc + 4abc$ — ②

$RHS = a * (b * c)$

$= \underbrace{a}_{a} * (\underbrace{b + c + 2bc}_{b})$

$= a + (b + c + 2bc) + 2(a)(b + c + 2bc)$

$= a + b + c + 2bc + 2ab + 2ac + 4abc$ — ③

By ② & ③,

$LHS = RHS$ ∴

$(a * b) * c = a * (b * c)$.

Associative property exists.

∴ $(R, *)$ is semi group.

2) Let e be an identity element.

∴ $e * a = a$ $\quad \left\{ \begin{array}{l} e * a = a \\ a * e = a \end{array} \right.$

$e + \cancel{a} + 2ea = \cancel{a}$

$e + 2ea = 0$

$e(1 + 2a) = 0$

$\Rightarrow e = \dfrac{0}{1 + 2a}$

∴ $e = 0$, $\quad 1 + 2a \neq 0$.

3) Let $a^{-1}$ be the inverse of $a$

$a * a^{-1} = e$

$\therefore a * a^{-1} = e$

$a + a^{-1} + 2aa^{-1} = 0$

$a^{-1}(1 + 2a) = -a$

$\therefore a^{-1} = \frac{-a}{(1+2a)}$ if $1 + 2a \neq 0$.

$2a \neq -1$

$a \neq -\frac{1}{2}$

$a^{-1} = \frac{-a}{1+2a}$, $a \neq -1/2$ //.

---

Abelian group :

1. show that $(Q^{+}, *)$ is an abelian group, where $*$ is defined by $a * b = \frac{ab}{2}$, for all $a, b \in Q^{+}$.

soln :

$Q \rightarrow$ set of all +ve rational numbers.

1. closure p..

$a, b \in Q^+$

$a * b \in Q^+$

$\frac{ab}{2} \in Q^+$ (True).

2. associative.

Let $a, b, c \in Q^+$

$(a * b) * c = a * (b * c)$ — ①.

LHS: $(a * b) * c$

$= \underbrace{\left(\frac{ab}{2}\right)}_{a} * \underbrace{c}_{b}$

$= \frac{\frac{ab}{2} \times c}{2}$

$= \frac{abc}{4}$ — ②

RHS: $a * (b * c)$

$= \underbrace{a}_{a} * \underbrace{\left(\frac{bc}{2}\right)}_{b}$

$= \frac{a * \frac{bc}{2}}{2}$

$= \frac{abc}{4}.$ — ③

2 & ③, $(a * b) * c = a * (b * c)$

∴ Ass. pr. verified.

$+ \to 0$
$* \to 1$

iii) identity

Let e be an identity element.

$e * a = a$
$a * e = a.$

$\therefore e * a = a$

$$\frac{ea}{2} = a$$

$$\boxed{e = 2} \in Q^+$$

$\therefore$ exists!

iv) Inverse.

$+ \to -5$
$* = 1/5$

$a \in Q^+$

Let $a^{-1}$ be the inverse of $a$; $a^{-1} * a = e$

$$a^{-1} * a = e$$

$$\frac{a^{-1}a}{2} = 2$$

$$a^{-1}a = 4$$

$$a^{-1} = \frac{4}{a} \in Q^+$$

$\therefore$ inverse also exists.

v) Commutative

$a, b \in Q^+$

$a * b = b * a$

Let LHS $= a * b$

$= \frac{ab}{2}$ — ①

RHS $= b * a$

$= \frac{ba}{2}$

$= \frac{ab}{2}$ — ② its exists //

① & ② =

$\therefore (Q^+, *)$ is an abelian group.

---

show that $M_2$, the set of all $2 \times 2$ non singular matrices over $R$ is a group under usual matrix multiplication Is it abelian?

soln:

$$\left\{ M_2 = \left\{ \begin{matrix} \text{Non singular} \\ \text{matrix.} \end{matrix} \right\} \quad \begin{matrix} |\,| \neq 0 \\ N.S.M. \end{matrix} \right.$$

$$\left. \begin{bmatrix} a & b \\ c & d \end{bmatrix}, \quad ad - bc \neq 0 \right\}$$

$(M_2, \cdot)$ group.

i) Closure:

Let $A, B \in M_2$

$\therefore |A| = 0$ & $|B| \neq 0$

$A \cdot B \in M_2$

i.e. $|AB| \neq 0$

Let $A = \begin{bmatrix} a_1 & b_1 \\ c_1 & d_1 \end{bmatrix}$ & $B = \begin{bmatrix} a_2 & b_2 \\ c_2 & d_2 \end{bmatrix}$

$$AB = \begin{bmatrix} a_1 a_2 + b_1 c_2 & a_1 b_2 + b_1 d_2 \\ c_1 a_2 + d_1 c_2 & c_1 b_2 + d_1 d_2 \end{bmatrix}$$

T.P

$|AB| \neq 0$

$|AB| = |A| \cdot |B|$ $\quad \left( \begin{matrix} |A| \neq 0 \\ |B| \neq 0. \end{matrix} \right.$

$\quad\quad\quad \neq 0 \quad \neq 0.$

$|AB| \neq 0. \quad \therefore A \cdot B \in M_2.$

ii) Associative :

$A, B, C \in M_2$.

T.P.

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

$\therefore$ It exists.

iii) identity

$M_2 = \{ 2 \times 2$ matrix $\}$.

$e = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ $\rightarrow$ unit matrix.

$\in M_2$.

$eA = A$.

$A \cdot e = A$.

iv) inverse :

$A \in M_2$.

Let $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$, $|A| \neq 0$,

(i.e) $ad - bc \neq 0$

$A^{-1} = \frac{1}{|A|} \cdot \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$

$A^{-1} \in M_2$.

& $|A^{-1}| \neq 0$

$ad - bc \neq 0$.

$\therefore A^{-1} \in M_2$ exists.

So $M_2$ is a group under multiplicat.

$M_2$ abelian?

$A \cdot B \neq B \cdot A$

commu:

$a * b = b * a$.

$\therefore M_2$ not an abelian group.

~~Addition Modulo~~:

Prove that $(Z_5, +_5)$ is abelian.

soln:

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

Cayley Table.

| $+_5$ | 0 | 1 | 2 | 3 | 4 |
|---|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 | 4 |
| 1 | 1 | 2 | 3 | 4 | 0 |
| 2 | 2 | 3 | 4 | 0 | 1 |
| 3 | 3 | 4 | 0 | 1 | 2 |
| 4 | 4 | 0 | 1 | 2 | 3 |

$Z_5' = ?$

$Z = \{\text{integers}\}$

Additive Modulo

$\underbrace{4 + 9 = 13}_{\text{normal addition}}$ : $+5$

Modulo.

$4 \; +_5 \; 9 = 3$

$$\begin{array}{r} 2 \\ 5\overline{)13} \\ 10 \\ \hline 3 \end{array}$$

Multiplication Modulo.

$3 \times 8 = 24$

$\cdot 4$ $= 0$

$$\begin{array}{r} 6 \\ 4\overline{)24} \\ 24 \\ \hline 0 \end{array}$$

$$\begin{array}{r} 1 \\ 5\overline{)5} \\ 5 \\ \hline 0 \end{array}$$

$$\begin{array}{r} 1 \\ 5\overline{)6} \\ 5 \\ \hline 1 \end{array}$$

Closure.

1. $a, b \in G$.

$a +_5 b \in G$.

exists

from the table, closure property exist.

2. associative

$a, b, c$

$(a *_{+_5} b) * c = a * (b * c)$

(5th video) 29th video seen.

exists.

Clearly associative property exist.

3. Identity.

$+ \to 0$.

$(\ ) + id = (\ )$

0 is the identity ~~exists~~ element w.r. to $+_5$

4. Inverse.

$a +_5 a^{-1} = e$

$a^{-1}$

Inverse of

$0^{-1} = 0$

$1^{-1} = 4$ → exists.

$2^{-1} = 3$

$3^{-1} = 2$

$4^{-1} = 1$

5. commutative:

$a +_5 b = b +_5 a$

exists.

addition is commut..

Hence $(Z_5, +_5)$ is abelian group

Q2 Marks:

Determine whether the set with the binary operation form a group.

| * | -1 | 1 |
|---|---|---|
| -1 | 1 | -1 |
| 1 | -1 | 1 |

$(-1)^{-1} = -1$
$1^{-1} = 1$

$G = \{-1, 1\}$.

$(G, *)$

1. closure
2. associative
3. identity
4. inverse.

soln:

closure property exist (from the Table)

associative exists under usual multiplication.

1 is the identity element.
inverse of -1 is -1 & inverse of 1 is 1.

Assume,

i) $a, b \in G$.

$a * b \in G$.

| | |
|---|---|
| 1 | -1 |
| -1 | 1 |

ii) oru set kulla numbers iruku na Associative property check panna vena.

iii) $+ \rightarrow 0$

$\times \rightarrow 1$

iv) $a \times a^{-1} = 1$

Prove that $G = \{[1], [2], [3], [4]\}$ is an abelian group under multiplication modulo 5.

soln:

cayley Table:

| $\times_5$ | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| 1 | 1 | 2 | 3 | 4 |
| 2 | 2 | 4 | 1 | 3 |
| 3 | 3 | 1 | 4 | 2 |
| 4 | 4 | 3 | 2 | 1 |

$5 \times 8 = 40$ Normal

$\times_5$

1. closure
2. Associative
3. Identity
4. Inverse
5. commutative

$5 \overline{)40}$ 8, 40, 0

1) closure:

$a, b \in G$

$a * b \in G$.

$a \times_5 b \in G$

2) Associative.

$a, b, c \in G$.

$(a * b) * c = a * (b * c)$.

$a \circledast (b \circledast c)$.

$\times_5$ $\times_5$

3. Identity:

$+ \longrightarrow 0$

$\times \longrightarrow 1$

1 is inside the Table so it exists.

$Z_5 \{0, 1, 2, 3, 4\}$.

$Z_7 = \{0 \ldots 6\}$.

4. Inverse element:

$a * a^{-1} = e \ (1)$

$a \times_5 a^{-1} = 1$

$G = Z_5 - \{0\}$

$= Z_5^*$

$1^{-1} = 1$

$2^{-1} = 3$

$3^{-1} = 2$

$4^{-1} = 4$

$+ \quad Z_n$.

$\times \quad Z_n$

$\times - 0$

not exists

5. commutative property:

$a * b = b * a$.

$Z_p^* \to$ prime numbers.

$a \times_5 b = b \times_5 a$.

Addition, Multiplication numbers la vanthu china commutative property check panna vena. yen na values vanthu yepdi add or Multiply pannalum Ans same tha.

Closure:

From the cayley Table closure property exists.

Associative:

usual multiplication is always associative.

Identity element:

here 1 is the identity element and $1 \in G$ $\therefore$ Identity element exists.

Inverse:

Inverse of 1 = 1

" " 2 = 3

" " 3 = 2

" " 4 = 4

Commutative:

It exists under usual Multiplication

$\therefore$ commutative property exists under Multiplication Modulo.

$\therefore$ G is an abelian group

---

Prove that $Z_5^*$ is an abelian group under multiplication Modulo 5.

Theorem :

oru group ka only one

1) show that the identity element the inulu
of a group is unique. ka proof Parhnaum

Proof :

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

Let $e_1$ & $e_2$ be two identity element in $G$.

$G = \{e_1, e_2, a_1, a_2 \ldots\}$

$e_1$:

$\overset{e}{e_1} * \overset{a}{e_2} = e_2$ ($\because e_1$ identity). — ①

$e * a = a$
$a * e = a$

$e_2$:

$\overset{a}{e_1} * \overset{e}{e_2} = e_1$ ($\because$ identity). — ②

$e_1 * a_1 = a_1$
$e_1 * a_2 = a_2$

by ① & ②,

$e_2 = e_1$

$\therefore$ Identity element of any group is unique.

---

For any element a in a group G, the inverse is unique.

2) Let $a$ be any element of a group $G$.

only 1 inverse exists $G = \{ \ldots \}$

suppose $a_1^{-1}$ & $a_2^{-1}$ be two inverse of $a$.

$a * a^{-1} = e$

$a^{-1} * a = e$

$a * a^{-1} = e$ & $a^{-1} * a = e$ ($\because a_1^{-1}$)

$\boxed{a * a_2^{-1} = e}$ & $a_2^{-1} * a = e$. ($\because a_2^{-1}$ is the inverse of $a$).

Consider:

$e * a = a$

$\boxed{a_1^{-1} = a_1^{-1} * e}$

$= a^{-1} * (a * a_2^{-1})$

$= (a^{-1} * a) * a_2^{-1}$

$= e * a_2^{-1}$

$\boxed{a_1^{-1} = a_2^{-1}}$

Left cancellation Law :

In a group $(G, *)$, the left and right cancellation laws are true.

that is $a * b = a * c \Rightarrow b = c$

(Left cancellation)

And $b * a = c * a \Rightarrow b = c$

(Right cancellation).

Proof :

given $(G, *)$ be a group.

Left cancellation Law.

To prove,

$$a * b = a * c \Rightarrow b = c$$

Let $a * b = a * c$

pre multiply by $a^{-1}$ $\boxed{a^{-1} * a = e}$

$$a^{-1} * (a * b) = a^{-1} * (a * c)$$

by Associative Pro..

$$(a^{-1} * a) * b = (a^{-1} * a) * c$$

$e * b = e * c.$

$b = c.$

$e * a = a$
$a * e = a$

Right cancellation Law:

To prove $b * a = c * a \Rightarrow b = c.$

Let $b * a = c * a$

post multiply by $a^{-1}$,

$(b * a) * a^{-1} = (c * a) * a^{-1}$

[$\because$ by Associative property].

$b * (a * a^{-1}) = c * (a * a^{-1})$

$b * e = c * e$

$b = c.$

Theorem: (*·*)

If $a$ and $b$ are any two element of a group $(G, *)$, then show that $G$ is an abelian group if and only if $(a*b)^2 = a^2 * b^2$

proof:

given $(G, *)$ is a group. (4 property)

Assume $(G, *)$ is abelian. (commutative),

T.P $(a*b)^2 = a^2 * b^2$.

$$(a*b)^2 = (a*b)(a*b).$$

$$\underset{a}{(a*b)} \; (\underset{b}{a} * \underset{c}{b})$$

$a*(b*c)$

$$= ((a*b)*a)*b$$

$$= (a*(b*a))*b.$$

} by associative law,

$$= (\underset{a}{a} * \underset{b}{(a*b)}) * \underset{c}{b}.$$

by commutative law.

$$= a*((a*b)*b)$$

$$= a*(a*(b*b))$$

$= (a * a) * (b * b)$

$(a*b)^2 = a^2 * b^2$

Conversely assume that $(a*b)^2 = a^2 * b^2$

T.P. $(G,*)$ is abelian.

by our assumption. $(a*b)^2 = a^2 * b^2$

$(a*b) * (a*b) = (a*a) * (b*b)$

Left
by cancellation law

$a * b = a * c$

$\Rightarrow b = c$

$a * (b * (a*b)) = a * ((a*(b*b))$.

$b * (a*b) = a * (b*b)$ by left cancellation.

~~by right~~

$(b*a) * b = (a*b) * b$ → by Right cancellation.

$\boxed{(b*a) = (a*b)}$

$\therefore (G,*)$ is abelian group.

## Semi group :

1) Idempotent element :

Let $(G, *)$ be a group. An element $a \in G$ is said to be an idempotent element if $a \times a = a$ $\forall a \in G$.

---

1) Show that a semi group with more than one idempotents cannot be a group. Give an example of a semi group which is not a group.

soln :

Let $(S, *)$ be a semi group.

Let $a$ & $b$ are the two idempotent element of $S$.

$\therefore a * a = a$ & $b * b = b$

T.P $(S, *)$ not a group. (contradiction method)

Let $(S, *)$ be a $\boxed{\text{group}}$ $\rightarrow$ 4 property

$a * a^{-1} = e$

$(a * a) * a^{-1} = a * (a * a^{-1})$

$a * a^{-1} = a * e$

$\boxed{e = a}$ ——— (1)

$(b * b) * b^{-1} = b * (b * b^{-1})$

$b * b^{-1} = b * e$

$\boxed{e = b}$ — ②

e element should be unique

we got 2 identity element which is a contradiction.

$\therefore (S, *)$ is not a group.

ii) Let $G = \{0, 1, -1\}$ inverse. $\frac{1}{0} = \infty$ not exists.

~~Cayley~~ Table:

~~Cayley~~.

| $\times$ | 0 | 1 | -1 |
|---|---|---|---|
| 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | -1 |
| -1 | 0 | -1 | 1 |

semi group.

i) closure

ii) Associative.

i) closure ✓.

ii) Associative ✓.

Group.

i) closure

ii) Associative

iii) identity ✗

iv) inverse ✗

Q) For any commutative monoid $(M, *)$, the set of all idempotent elements of M forms a sub monoid.

3 proper closure associative identity

Proof :

given $(m, *)$ is a commutative monoid.

Let S be the set of all idempotent element of m.

T.p $(S, *)$ sub monoid.

clearly $S \subseteq M$

closure :

$a, b = a * b$

Let $a, b \in S$.

$\therefore$ $a * a = a$ & $b * b = b$.

T.p $a * b \in S$

(ie) T.P $(a * b) * (a * b) = (a * b)$

LHS = $(a * b) * (a * b)$.

a b c

$$= a * (b * (a * b))$$ } by associative Law.

$$= a * ((b * a) * b)).$$

$$= a * ((a * b) * b). \quad (\because a * b = b * a)$$

$$= (a * (a * b)) * b)$$

$$= ((\underbrace{a * a}_{a}) * \underset{b}{b}) * \underset{c}{b}$$

$$= (a * a) * (b * b).$$

$$(a * b) * (a * b) = a * b$$

$\therefore (a * b)$ is an idempotent element.

$\therefore (a * b) \in S.$

$\therefore$ closure property exists.

Assoi :

clearly $(S, *)$ is associative.

Identity :

$$e * e = e$$

$$\therefore e \in S.$$

$$S \subseteq M$$

$\boxed{\therefore (S, *) \text{ is a submonoid.}}$

$\therefore (a * b^{-1}) \in H.$

$H$ is a subgroup of $G$.

---

Cyclic Group:

A group $G$ is called a cyclic group if, for some $a \in G$, every element of $G$ is of the form $a^n$, where $n$ is some integer. The element $a$ is called the generator of $G$.

$G = \{$power value$\}$ $(G, *)$

$\to$ pa

$G = \{\cancel{1, -1}\}$

$\{1, -1\} = \{\cancel{1} \times \cancel{1} (-1)^{2}\}$ Same

$= \{-1, 1\}$

Cyclic group generated by $-1$ $\langle -1 \rangle = \{-1, 1\}$

$G = \langle -1 \rangle \longrightarrow$ It is a generator of $G$.

$\downarrow$

so $g$ is a cyclic group.

Q) Find all the subgroups of $(Z_9, +_9)$.

$10-9$

$\boxed{10-9=1}$

soln:-

$9-9=0$

$Z_9 = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$.

$9 \overline{)9}$ 1, 9, 0

$\langle 0 \rangle = \{0\}$.

$9-9$

$Z_9 = \langle 1 \rangle = \{1, 2, 3, 4, 5, 6, 7, 8, 0\}$

$9-9$

$Z_9 = \langle 2 \rangle = \{2, 4, 6, 8, 1, 3, 5, 7, 0\}$.

$12-9=3$

$11-9=2$

$10-9=1$

$\cancel{Z_9}\ \langle 3 \rangle = \{3, 6, 0\}$.

$Z_9\ \langle 4 \rangle = \{4, 8, 3, 7, 2, 6, 1, 5, 0\}$.

$\cancel{Z_9}\ \langle 5 \rangle = \{5, 1, 6, 2, 7, 3, 8, 4, 0\}$.

$Z_9\ \langle 6 \rangle = \{6, 3, 0\}$.

$Z_9 = \langle 7 \rangle = \{7, 5, 3, 1, 8, 6, 4, 2, 0\}$.

$Z_9 = \langle 8 \rangle = \{8, 7, 6, 5, 4, 3, 2, 1, 0\}$

$\therefore$ sub groups of $Z_9$ are $\underbrace{\{0\}, Z_9}_{I.P.}$,

& $\{0, 3, 6\} \rightarrow$ proper

proper sub group. → (non trivial) Remaining.

improper sub group. ( Trivial ) → $\{e\}$, $G$

20 video seen