PROBLEMS

1. Prove that the set $M_2(\mathbb{R})$ does not form a group under Matrix multiplication.

$\Rightarrow$ $M_2(\mathbb{R})$ $\longrightarrow$ Set of all 2×2 matrices whose entries are real no's.

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \qquad a, b, c, d \in \mathbb{R}$$

$AB \neq BA$

i) Closure property holds.

ii) $(AB)C = A(BC)$, $\Rightarrow$ property holds.

iii) $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = 'e'$, $\Rightarrow$ identity property.

iv) 'A' $\longrightarrow$ singular matrix

$AB = BA = I_2$, so $\nexists$ don not exist any such B.

$M_2(R)$ under matrix multiplication is not a group.

Finite Groups

A group $(G, \circ)$ is said to be finite group if G contains finite number of elements.

The order of a finite group $(G, \circ)$ is the no. of elements of G. The order of a finite group G is denoted by $o(G)$ or $|G|$.

Example:

Let $S = \{1, \omega, \omega^2\}$ when $\omega^3 = 1$.

The S.T S is an abelian group w.r.t multiplication.

Ans: Composition table

$\times$	1	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

$1, \omega, \omega^2$

1

?

i) So, it is closed under multiplication.

ii) $S \subseteq \mathbb{C}$, multiplication on $\mathbb{C}$ is associative

So, S being subset of $\mathbb{C}$ is also associative.

iii) 1 being the identity element.

iv) Inverse of $1 \to 1$ ✓

Inverse of $\omega \to \omega^2$ ✓

Inverse of $\omega^2 \to \omega$ ✓

$x \times = 1$

Inverse criteria fulfilled.

v) Checking the commutativity

Composition table

$\times$	$\perp$	ω	ω^2
1	1	ω	ω^2
ω	ω	ω^2	1
ω^2	ω^2	1	ω

So, the table is symmetric about the principal diagonal. Therefore multiplication is commutative.

So, the group S is commutative group w.r.t Multiplication.

H.W $S = \{1, i, -1, i\}$ where $i^4 = 1$

P.T. $(S, \cdot)$ is an abelian group.

H.W $S = \{ z \in \mathbb{C} ; z^n = 1 \}$. S is the set of n distinct n^{th} roots of unity.

P.T. $(S; \cdot)$ is an abelian group.

Classes of Residues of integers modulo n

Set $\rightarrow \mathbb{Z}_3$ form an abelian group w.r.t '+' "addition (modulo 3).

$\mathbb{Z}_3 \rightarrow \{ \bar{0}, \bar{1}, \bar{2} \}$ $\quad \mathbb{Z}_n \rightarrow \bar{0}, \ldots \overline{n-1}$.

+	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{0}$	$\bar{1}$

$\bar{3}$

i) It appears from table that the set is closed under '+'.

ii) So it is also associative.

iii) $\bar{0}$ is the identity element.

iv) $\bar{n} + \bar{0} = \bar{n}$ $\quad \bar{1} + \bar{0} = \bar{1}$

iv) $\bar{0} + \boxed{?} = \bar{0}$, $\bar{1} + \boxed{?} = \bar{0}$

$\boxed{?} \to \bar{0}$; $\boxed{?} \to \bar{2}$

$\bar{2} + \bar{1} = \bar{3} = \bar{0}$.

So, the inverse of each element belongs to the set.

v) So, the table is symmetric about the principal diagonal. Therefore it is abelian

$(\mathbb{Z}_3, +) \to$ abelian group

Check $(\mathbb{Z}_n, \cdot)$ forms an abelian group?

$\bar{0} \times ? = \bar{0}$.

There does not exist any inverse of class zero $(\bar{0})$. So, it does not form a group

$(\mathbb{Z}_n - \{0\}, \cdot)$ check group or not?

(n) $\to$ prime.

Group U_n (Group of units modulo n)

Units in $\mathbb{Z}_n$ → the elements which have multiplicative inverses — you do get a group under multiplication mod n. It is denoted by U_n (units in $\mathbb{Z}_n$).

Proof Suppose $a, b \in U_n$

$a \longrightarrow a^{-1}$ (multiplicative inverse).

$b \longrightarrow b^{-1}$ (")

$$(b^{-1}a^{-1})ab = b^{-1}(a^{-1}a)b = 1.$$

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = 1.$$

$(b^{-1}a^{-1})$ is a multiplicative inverse of ab

So, multiplication mod n is a binary operation on U_n.

So, U_n is group under multiplication mod n.

Note. The comp...

7. Group U_n (Group of units modulo n).

The set $\mathbb{Z}_n$ forms a commutative monoid under multiplication (mod n). Let us find the units in the monoid $(\mathbb{Z}_n, .)(n > 1)$.

Let $\bar{u}$ be a unit. Then there exists an element $\bar{v}$ in $\mathbb{Z}_n$ such that $\bar{u}.\bar{v} = \bar{1} \Rightarrow uv - 1 = kn$, or $uv - kn = 1$, where v, k are integers. This shows that $gcd(u, n) = 1$.

Conversely, let u be an integer less than n and prime to n. Then there exist integers p, q such that $up + nq = 1$, or $up - 1 = -qn$, or $up \equiv 1 \pmod{n}$. Clearly, p is not a multiple of n.

Let $p \equiv r \pmod{n}$, where $0 < r < n$. Then $\bar{r} \in \mathbb{Z}_n$.

$r \equiv p \pmod{n} \Rightarrow ur \equiv up \pmod{n} \Rightarrow ur \equiv 1 \pmod{n}$. This gives $\bar{u}.\bar{r} = \bar{1}$. Since the monoid is commutative, $\bar{u}.\bar{r} = \bar{r}.\bar{u} = \bar{1}$. This shows that $\bar{u}$ is a unit.

Thus $\bar{u}$ in the monoid is a unit if and only if u is less than n and prime to n.

Let us consider the set S of all units (i.e., the elements $\bar{u}$ satisfying $gcd(u, n) = 1$) in the monoid $(\mathbb{Z}_n, .)(n > 1)$. We prove that the set S forms a commutative group under multiplication (mod n).

(i) Let $\bar{u}, \bar{v} \in S$. Then u is prime to n and v is prime to n. This implies uv is prime to n and therefore $\bar{u}.\bar{v} \in S$. This shows that the set S is closed under multiplication (mod n).

(ii) Multiplication (mod n) is associative on the set $\mathbb{Z}_n$. S being a subset of $\mathbb{Z}_n$, multiplication (mod n) is associative on the set S.

(iii) $\bar{1} \in S$ and $\bar{1}.\bar{u} = \bar{u}.\bar{1} = \bar{u}$ for all $\bar{u} \in S$. Therefore $\bar{1}$ is the identity element.

(iv) Let $\bar{u} \in S$. Then $\bar{u}$ is a unit in the monoid $(\mathbb{Z}_n, .)$. So there exists an element $\bar{v} \in \mathbb{Z}_n$ such that $\bar{u}.\bar{v} = \bar{v}.\bar{u} = \bar{1}$. This shows that $\bar{v}$ is a unit in $\mathbb{Z}_n$. So $\bar{v} \in S$ and $\bar{v}$ is the inverse of $\bar{u}$.

(v) Multiplication (mod n) is commutative on the set $\mathbb{Z}_n$. S being a subset of $\mathbb{Z}_n$, multiplication (mod n) is commutative on the set S.

Therefore the set S forms a commutative group under multiplication (mod n). This group is denoted by U_n. $U_n = \{\bar{u} : gcd(u, n) = 1\}$.

Note. U_n is a finite group of $\phi(n)$ elements, where $\phi(n)$ is the number of integers less than n and prime to n.

For example, the group U_4 contains $2(= \phi(4))$ elements. $U_4 = \{\bar{1}, \bar{3}\}$. The group U_{10} contains $4(= \phi(10))$ elements. $U_{10} = \{\bar{1}, \bar{3}, \bar{7}, \bar{9}\}$.

In particular, if n be a prime then every integer less than n is prime to n and in this case $U_n = \{\bar{1}, \bar{2}, \ldots, \overline{n-1}\}$, a group of order $n - 1$.