Solutions

30 November 2020 23:36

11. $(Z_4, +_4, \cdot_4)$

$Z_4 = \{0, 1, 2, 3\}$.

$+_4$

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot_4$

$\cdot_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

A1) Closure is satisfied

as $a +_4 b \in Z_4 \quad \forall a, b \in Z_4$

A2) Associativity is satisfied

as $a + (b + c) = (a + b) + c \pmod 4$

[modular addition is associative]

A3) '0' is the identity

A4) for all elements, we have the inverse

table:-

a	a^{-1} under $+_7$	a^{-1} under $\cdot_7$
0	0	–
1	3	1
2	2	–
3	1	3

Since inverse exist for $+_7$,
additive inverse exists

A5) Commutativity is satisfied as

$$a +_4 b = b +_4 a$$ [modular addition is commutative]

M1) Closed under $\cdot_4$

$a \cdot_4 b \in Z_4 \; \forall \; a, b \in Z_4$

Hence closure is true.

M2) Associativity is satisfied as

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c$$ [modular multiplication is associative]

M3) Distributivity is satisfied as

$$a \cdot (b + c) = a \cdot b + a \cdot c$$ [modular multiplication is distributive]

M4) Commutativity is also over $\cdot_4$.

as $a \cdot b = b \cdot a$

[modular multiplication is commutative]

Thus it is a commutative ring.

BUT since $2 \cdot 2 \equiv 0 \pmod 4$

and $2 \neq 0$,

we have 2 as the zero-divisor.

And (2) also doesn't have a multiplicative inverse.

∴ It is not integral domain/field.

2) Addition →

	1	i	$1+i$	0
1	1	$1+i$	$1+i$	1
i	$1+i$	0	1	i
$1+i$	i	1	0	$1+i$
0	1	i	$1+i$	0

Multiplication table :-

Multiplication table :-

	1	i	1+i	0
1	1	i	1+i	0
i	i	1	i+1	0
1+i	1+i	1+i	0	0
0	0	0	0	0

You can prove that A1 → M5 holds.

We have the inverse table :-

	a^{-1} under $+_2$	a^{-1} under $-_2$
0	0	-
1	1	1
i	i	i
1+i	1+i	—

Since $(1+i)^2 \equiv 0 \pmod 2$

and $(1+i) \not\equiv 0 \pmod 2$,

M6 doesn't hold.

and (1+i) is not having an inverse, M7 doesn't hold

Thus it is commutative ring.

1.2.4

Any two elements $x_1, x_2 \in R$.

Any $\begin{bmatrix} a_1 & -b_1 \\ \end{bmatrix} \cdot \begin{bmatrix} a_2 & -b_2 \end{bmatrix}$

A1) any two elements $x_1, x_2 \in R$

$$\begin{bmatrix} a_1 & -b_1 \\ b_1 & a_1 \end{bmatrix} + \begin{bmatrix} a_2 & -b_2 \\ b_2 & a_2 \end{bmatrix}$$

(2×2) (2×2)

$$= \begin{bmatrix} a_1+a_2 & -(b_1+b_2) \\ b_1+b_2 & a_1+a_2 \end{bmatrix} \in R.$$

$\therefore$ closure is satisfied.

A2) Trivial by matrix addition.

A3) $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ is identity.

A4) for any element $\begin{bmatrix} a & -b \\ b & a \end{bmatrix}$,

the inverse is $\begin{bmatrix} -a & b \\ -b & a \end{bmatrix}$.

A5) Trivial for matrix addition.

M1) Take any 2 $x_1, x_2 \in R$,

$$\begin{bmatrix} a_1 & -b_1 \\ b_1 & a_1 \end{bmatrix} \cdot \begin{bmatrix} a_2 & -b_2 \\ b_2 & a_2 \end{bmatrix}$$

$$= \begin{bmatrix} a_1a_2 - b_1b_2 & -(a_1b_2 + a_2b_1) \\ +(a_1b_2 + a_2b_1) & a_1a_2 - b_1b_2 \end{bmatrix} \in R //$$

Thus it is closed.

M2) Trivial by matrix multiplication

M3) Trivial by matrix multiplication & addition.

M4) Take any 2×1 matrix

$$\begin{bmatrix} a_1 & -b_1 \\ b_1 & a_1 \end{bmatrix} \begin{bmatrix} a_2 & -b_2 \\ b_2 & a_2 \end{bmatrix}$$

$$= \begin{bmatrix} a_1a_2 - b_1b_2 & -(a_1b_2 + a_2b_1) \\ +(a_1b_2 + a_2b_1) & a_1a_2 - b_1b_2 \end{bmatrix}$$

$$= \begin{bmatrix} a_2 & -b_2 \\ b_2 & a_2 \end{bmatrix} \begin{bmatrix} a_1 & -b_1 \\ b_1 & a_1 \end{bmatrix}$$

Thus we have proved it's a commutative ring.

M5) $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ is the identity.

M6) Any non-zero element x_1

$$x_1 = \begin{bmatrix} a_1 & -b_1 \\ b_1 & a_1 \end{bmatrix},$$

To prove

Thus if

To prove

Then if

$$x_1 x_2 = 0 \Rightarrow x_2 = 0$$

$$x_2 = \begin{bmatrix} a_2 & -b_2 \\ b_2 & a_2 \end{bmatrix}$$

$$\begin{bmatrix} a_1 & -b_1 \\ b_1 & a_1 \end{bmatrix} \begin{bmatrix} a_2 & -b_2 \\ b_2 & a_2 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$$

$$\Rightarrow a_1 a_2 - b_1 b_2 = 0$$

$$a_1 b_2 + a_2 b_1 = 0$$

$$\therefore a_1 a_2 = b_1 b_2$$

$$a_1 b_2 = a_2 b_1$$

$$\therefore \frac{a_2}{b_2} = \frac{-b_2}{a_2}$$

$$\therefore \boxed{a_2^2 + b_2^2 = 0}$$

This condition, when you test in Z_7, is never true, [for non-zero a_2, b_2]

that is

$$a_2^2 + b_2^2 = 0 \Rightarrow a_2 = 0, b_2 = 0$$

$a_2^2 + b_2^2 = 0 \Rightarrow a_2 = 0, b_2 = 0$

✡ [Note that for $\mathbb{Z}_5$, we have

$3^2 + 4^2 \equiv 0 \pmod 5$,

which is why M6 doesn't hold].

M7)

If $x_1 = \begin{bmatrix} a_1 & -b_1 \\ b_1 & a_1 \end{bmatrix}$, [non-zero]

$$x_1^{-1} = \frac{\begin{bmatrix} a_1 & +b_1 \\ -b_1 & a_1 \end{bmatrix}}{a_1^2 + b_1^2}$$

(by adjoint method)

Thus it is a field over $\mathbb{Z}_7$

but a commutative ring over $\mathbb{Z}_5$.

2.)

If

let $x, y \in R$, we need to show $xy = yx$

we take

$a = x$

$b = yx$

$c = xy$.

$ab = x(yx)$

$= (xy)x$ ... & associativity of $\cdot$, property of ring}

$= ca$

Thus $ab = ca$,
which implies $b = c$ & $\underline{yx = xy}$

2) we have

$(\underbrace{a+a\cdots}_{m \text{ times}})(\underbrace{b+\cdots b}_{n \text{ times}})$

$= \underline{a(\overbrace{b+b+\cdots b}^{n \text{ times}}) + a(b+b+b\cdots)} \cdots$ & distributive property

$\underbrace{+ \cdots\cdots \quad a(b+b+a\cdots)}_{m \text{ times}}$

$= \underbrace{ab+ab+\cdots}_{mn \text{ times}}$

3) Since it is cyclic group,

$\forall a \in R$,

we must have an integer 'm'

such that $a = \underbrace{g + \cdots g}_{\text{'m' times}}$

where 'g' → generator.

$\therefore$ we use (2)'s result :-

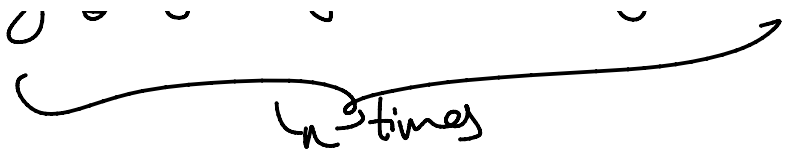
Let $b = \underbrace{g + g + \cdots}_{\text{'n' times}}$.

$\therefore$

$$\underbrace{(g + g + \cdots)}_{\text{'n' times}} \underbrace{(g + g + \cdots g)}_{\text{'n' times}}$$

$$= \underbrace{gg + \cdots \quad gg}_{\text{'mn' times}}$$

$$= \underbrace{g(g + g + \cdots g) + \cdots g(g + g + \cdots g)}_{\text{'m' times}} \quad \text{--- [distribute law]}$$



$= (g+g+\cdots g)\ (g+\cdots g)$

n^2 times cn^2 times

$= ba$.

$\therefore ab = ba$ always

Hence proved.

3.6

1) [Will post later]

2) x^3+6 in GF(7)

we note that $x=1$, is a root.

$\therefore \underline{x+6 \mid x^3+6}$ [$\because x-1$, same as $x+6$]

x^2-6x+1

$\therefore$ $x+6 \;\big)\; x^3+6$

x^3+6x^2

$-6x^2+6$

$-6x^2-x-\cdots$ [$-36x$ worken as $-x$]

$6+x$

$6+x$

0

$\therefore \boxed{x^3+6 = (x+1)(x^2-6x+1)}$

3) (x^3+1) over G.F(2)

we notice that $x=-1$ is the zero,

$\therefore x-1 \mid x^3+1$

& $x+1 \mid x^3+1$.

x^2-x+1

$x+1 \;\big)\; x^3+1$

x^3+x^2

$1-x^2$

$-x^2-x$

$1+x$

$1+x$

0

$\therefore$ $\boxed{x^3+1 = (x+1)(x^2-x+1)}$

2) [coiw post later]