Novosad Ivan

1. Find all invertible elements, all zero divisors, all nilpotents, and idempotents in the ring $\mathbb{Z}_{20}$.

1) $a \in \mathbb{Z}_{20}$ is inveutable if there exist an element b s.t. $a \cdot b \equiv 1 \pmod{20}$

it's equivalent to saying that a and 20 are co-prime

Since $20 = 2^2 5$, a must not be divisiable by 2 and 5.

Hence the inveutible element in $\mathbb{Z}_{20}$ are:

$1, 3, 7, 9, 11, 13, 17, 19$ (that is all coprimes in $(0, 20)$)

2) In $\mathbb{Z}_{20}$ an element (a) is a zero divisor if there exist a non-zero element (b) s.t. $a \times b \equiv 0 \pmod{20}$

to find all zero divisors, we need to identify elements (a) for which there exist a non-zero (b) s.t. there product is divisible by 20.

Thus zero divisors in $\mathbb{Z}_{20}$ are the element that are not coprime with 20 and aren't zero.

So they are:

- 2 $(2 \times 10 \equiv 0)$
- 4 $(4 \times 5 \equiv 0)$
- 5 $(5 \times 4 \equiv 0)$
- 6 $(6 \times 10 \equiv 0)$
- 8 $(8 \times 5 \equiv 0)$
- 10 $(10 \cdot 2 \equiv 0)$
- 12 $(12 \cdot 5 \equiv 0)$
- 14 $(14 \cdot 10 \equiv 0)$
- 15 $(15 \cdot 4 \equiv 0)$
- 16 $(16 \cdot 5 \equiv 0)$
- 18 $(18 \cdot 10 \equiv 0)$

So, the zero divisors in $\mathbb{Z}_{20}$ are: 2, 4, 5, 6, 8, 10, 12, 14, 15, 16 and 18

3) In $\mathbb{Z}_{20}$ an element (a) is nilponent if there exist some positive integer (k) s.t. $a^k \equiv 0 \pmod{20}$, so they are:

- 0 (it's trivial nilponent $0^k \equiv 0 \pmod{20}$)
- 10 $(10^2 \equiv 0 \pmod{20})$

Since $20 = 2^2 \cdot 5$, nilponents ought to be in the form $2 \cdot 5 \cdot l$, where $l \in \mathbb{Z}$ but nilponents of $\mathbb{Z}_{20}$, clearly, ought to be between 0 and 20, so there are only 1 non-trivial nilponent $\{10\}$ and one trivial $\{0\}$

4) In $\mathbb{Z}_{20}$ an element (a) is idempotent if $a^2 \equiv a \pmod{20} \Leftrightarrow a \times (a-1) \equiv 0 \pmod{20}$

- $a = 0$ $(0(0-1) \equiv 0)$
- $a = 1$ $(1(1-1) \equiv 0)$
- $a = 2$ $(2(2-1) \equiv 2)$
- $a = 3$ $(3(3-1) \equiv 6)$
- $a = 4$ $(4(4-1) \equiv 12)$
- $a = 5$ $(5(5-1) \equiv 0)$
- $a = 6$ $(6(6-1) \equiv 30)$
- $a = 7$ $(7(7-1) \equiv 42)$
- $a = 8$ $(8(8-1) \equiv 56)$
- $a = 9$ $(9(8-1) \equiv 72)$
- $a = 10$ $(10(10-1) \equiv 90)$
- $a = 11$ $(11(11-1) \equiv 110)$
- $a = 12$ $(12(12-1) \equiv 132)$
- $a = 13$ $(13(13-1) \equiv 156)$
- $a = 14$ $(14(14-1) \equiv 182)$
- $a = 15$ $(15(15-1) \equiv 210)$
- $a = 16$ $(16(16-1) \equiv 0)$
- $a = 17$ $(17(17-1) \equiv 272)$
- $a = 18$ $(18(18-1) \equiv 306)$
- $a = 19$ $(19(19-1) \equiv 342)$

So idempotent element of $\mathbb{Z}_{20}$ are $\{0, 1, 5, 16\}$

2. Let $R = \mathbb{Z}_4[x]$ and $f = a + bx$, where $a, b \in \mathbb{Z}_4$. Find all $a, b \in \mathbb{Z}_4$ such that f is nilpotent.

f is nilpotent in $\mathbb{Z}_4$ if $\left[\begin{array}{l} f = 0 \\ f = 2 \\ f = 2x \\ f = 2 + 2x \end{array}\right.$

Thus at least one element ought to be a nilponent in $\mathbb{Z}_4$

Since in $\mathbb{Z}_4$ there are two nilponents $\{0,2\}$:

$f^2 \equiv 0 \pmod 4$ holds for $(a,b) = (0,2) \cup (2,0) \cup (0,2) \cup (2,2)$

3. Suppose

$$S = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \,\middle|\, a, b \in \mathbb{R} \right\}$$

and let $\phi\colon \mathbb{C} \to S$ be the map given by the rule $a + bi \mapsto \left(\begin{smallmatrix} a & -b \\ b & a \end{smallmatrix}\right)$. Show that:

(a) S is a commutative ring.

(b) ϕ is an isomorphism.

A. 1) Abelian group:

1.1 $G \times G \to G$ (Closed under addition)

$$\begin{bmatrix} a & -b \\ b & a \end{bmatrix} + \begin{bmatrix} c & -d \\ d & c \end{bmatrix} = \begin{bmatrix} a+c & -b-d \\ b+d & a+c \end{bmatrix}$$

Clearly $a+c \in \mathbb{R}$, $-b-d \in \mathbb{R}$, and so on, thus it's closed

1.2

$$\begin{bmatrix} a & -b \\ b & -a \end{bmatrix} + \left(\begin{bmatrix} c & -d \\ d & c \end{bmatrix} + \begin{bmatrix} m & -k \\ k & m \end{bmatrix} \right) = \left(\begin{bmatrix} a & -b \\ b & a \end{bmatrix} + \begin{bmatrix} c & -d \\ d & c \end{bmatrix} \right) + \begin{bmatrix} m & -k \\ k & m \end{bmatrix} = \begin{bmatrix} a+c+m & -(b+d+k) \\ b+d+k & a+c+m \end{bmatrix}$$

1.3 Neutral element

$$\begin{bmatrix} a & -b \\ b & a \end{bmatrix} + \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} a & -b \\ b & a \end{bmatrix} = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$$

1.4 Inverses:

$$\begin{bmatrix} a & -b \\ b & a \end{bmatrix} + \begin{bmatrix} -a & b \\ -b & -a \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} -a & b \\ -b & -a \end{bmatrix} + \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$$

1.5 Commutativity

$$\begin{bmatrix} a & -b \\ b & a \end{bmatrix} + \begin{bmatrix} a' & -b' \\ b' & a' \end{bmatrix} = \begin{bmatrix} a' & -b' \\ b' & a' \end{bmatrix} + \begin{bmatrix} a & -b \\ b & a \end{bmatrix} = \begin{bmatrix} a+a' & -b-b' \\ b+b' & a+a' \end{bmatrix}$$

2) Commutative ring:

2.1 Close under multiplication: Matrix multiplication is closed

2.2 Multiplication is left and right distributive:

$$\begin{bmatrix} a & -b \\ b & a \end{bmatrix} \cdot \left(\begin{bmatrix} c & -d \\ d & c \end{bmatrix} + \begin{bmatrix} m & -k \\ k & m \end{bmatrix} \right) = \begin{bmatrix} ac+am-bd-bk & -ad-ak-bc-bm \\ bc+bm+ad+ak & -bd-bk+ac+am \end{bmatrix}$$

$$\begin{bmatrix} a & -b \\ b & a \end{bmatrix} \begin{bmatrix} c & -d \\ d & c \end{bmatrix} + \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \begin{bmatrix} m & -k \\ k & m \end{bmatrix} = \begin{bmatrix} ac+am-bd-bk & -ad-ak-bc-bm \\ bc+bm+ad+ak & -bd-bk+ac+am \end{bmatrix}$$

$$\left(\begin{bmatrix} c & -d \\ d & c \end{bmatrix} + \begin{bmatrix} m & -k \\ k & m \end{bmatrix} \right) \cdot \begin{bmatrix} a & -b \\ b & a \end{bmatrix} = \begin{bmatrix} ac+am-bd-bk & -ad-ak-bc-bm \\ bc+bm+ad+ak & -bd-bk+ac+am \end{bmatrix}$$

$$\begin{bmatrix} a & -b \\ b & a \end{bmatrix} \begin{bmatrix} m & -k \\ k & m \end{bmatrix} + \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \begin{bmatrix} c & -d \\ d & c \end{bmatrix} = \begin{bmatrix} ac+am-bd-bk & -ad-ak-bc-bm \\ bc+bm+ad+ak & -bd-bk+ac+am \end{bmatrix}$$

2.3 Multiplication is associative

$$\begin{bmatrix} a & -b \\ b & a \end{bmatrix} \left(\begin{bmatrix} c & -d \\ d & c \end{bmatrix} \cdot \begin{bmatrix} m & -k \\ k & m \end{bmatrix} \right) = \begin{bmatrix} acm-adk-bdm-bck & -ack-adm+bdk-bcm \\ bcm-bdk+adm+ack & -bck-bdm-adk+acm \end{bmatrix}$$

$$\begin{bmatrix} a & -b \\ b & a \end{bmatrix} \begin{bmatrix} c & -d \\ d & c \end{bmatrix} + \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \begin{bmatrix} m & -k \\ k & m \end{bmatrix} = \begin{bmatrix} acm-adk-bdm-bck & -ack-adm+bdk-bcm \\ bcm-bdk+adm+ack & -bck-bdm-adk+acm \end{bmatrix}$$

2.4 Multiplication is commutative:

$$\begin{bmatrix} a & -b \\ b & a \end{bmatrix} \begin{bmatrix} c & -d \\ d & c \end{bmatrix} = \begin{bmatrix} ac-bd & -ad-bc \\ bc+ad & -bd+ac \end{bmatrix} = \begin{bmatrix} c & -d \\ d & c \end{bmatrix} \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$$

B. 1) Homomorphism

$$\varphi(1) = I_2$$

$$\varphi(a+bi+c+di) = \begin{bmatrix} a+c & -b-d \\ b+d & a+c \end{bmatrix}$$

$$\varphi(a+bi) + \varphi(c+di) = \begin{bmatrix} a & -b \\ b & a \end{bmatrix} + \begin{bmatrix} c & -d \\ d & c \end{bmatrix} = \begin{bmatrix} a+c & -b-d \\ b+d & a+c \end{bmatrix}$$

$$\varphi((a+bi)(c+di)) = \varphi(ac-bd+(ad+bc)i) = \begin{bmatrix} ac-bd & -ad-bc \\ ad+bc & ac-bd \end{bmatrix}$$

$$\varphi(a+bi) \cdot \varphi(c+di) = \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \begin{bmatrix} c & -d \\ d & c \end{bmatrix} = \begin{bmatrix} ac-bd & -ad-bc \\ ad+bc & ac-bd \end{bmatrix}$$

2) Bijectivity:

2.1 Injectivity:

Suppose $z_1 = a+bi$; $z_2 = c+di$

$$\varphi(z_1) = \varphi(z_2) \iff \begin{bmatrix} a & -b \\ b & a \end{bmatrix} = \begin{bmatrix} c & -d \\ d & c \end{bmatrix} \iff \begin{cases} a = c \\ b = d \end{cases} \iff \text{injective}$$

2.2 Surjectivity

let $\begin{bmatrix} a & -b \\ b & a \end{bmatrix} \in S$ and $z = c+di$ s.t. $\varphi(z) = \begin{bmatrix} a & -b \\ b & a \end{bmatrix}$

$$\varphi(z) = \begin{bmatrix} c & -d \\ d & c \end{bmatrix} = \begin{bmatrix} a & -b \\ b & a \end{bmatrix} \iff \begin{cases} c = a \\ b = d \end{cases} \iff \varphi \text{ is surjective}$$

4. Let $R = \mathbb{R}[x]$ and we are given a map $\phi\colon \mathbb{R}[x] \to \mathrm{M}_2(\mathbb{R})$ by the rule

$$f(x) \mapsto \begin{pmatrix} f(2) & f'(2) \\ 0 & f(2) \end{pmatrix}$$

Show that the map is a homomorphism of rings and compute $\operatorname{Im}\phi$.

1. $\varphi(a+b) = \varphi(a) + \varphi(b)$

$$\varphi(f(x)) + \varphi(g(x)) = \begin{bmatrix} f(2) & f'(2) \\ 0 & f(2) \end{bmatrix} + \begin{bmatrix} g(2) & g'(2) \\ 0 & g(2) \end{bmatrix} = \begin{bmatrix} (f+g)(2) & (f+g)'(2) \\ 0 & (f+g)(2) \end{bmatrix}$$

$$\varphi(f(x) + g(x)) = \begin{bmatrix} (f+g)(2) & (f+g)'(2) \\ 0 & (f+g)(2) \end{bmatrix}$$

2. $\varphi(ab) = \varphi(a)\varphi(b)$

$$\varphi(f(x)g(x)) = \begin{bmatrix} (f\circ g)(2) & (f\circ g)'(2) \\ 0 & (f\circ g)(2) \end{bmatrix}$$

$f'(2)g(2) + f(2)g'(2)$

$$\varphi(f(x)) \circ \varphi(g(x)) = \begin{bmatrix} f(2) & f'(2) \\ 0 & f(2) \end{bmatrix} \begin{bmatrix} g(2) & g'(2) \\ 0 & g(2) \end{bmatrix} = \begin{bmatrix} (f\circ g)(2) & (f\circ g)'(2) \\ 0 & (f\circ g)(2) \end{bmatrix}$$

$\varphi(1) = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, Hence it's isomaphic

$$\operatorname{Im}(\varphi) = \left\{ \begin{bmatrix} a & b \\ 0 & a \end{bmatrix} \,\middle|\, a, b \in \mathbb{R} \right\}$$

Note: we in fact can obtain any a and b, i.e.

if $f(x) = a$, $f'(x) = b$ $\Rightarrow \begin{cases} kx + c = a \\ k = b \end{cases} \Rightarrow \begin{cases} 2k + c = a \\ k = b \end{cases} \Rightarrow \begin{cases} c = \frac{a}{2b} \\ k = b \end{cases}$

Thus for $\forall a \in \mathbb{R}\ \forall b \in \mathbb{R}$, we can take $f(x) = \frac{a}{2b}x + b$