· Taha

HA AMEEN , ID @00066555

42/45

HW III: MTH 420, Spring 2018

Ayman Badawi

QUESTION 1. Let $R = Z[x]$. Find an ideal I of R such that R/I is an infinite integral domain with multiplicative identity $x+I$.

QUESTION 2. (i) Let $f(x) = 4x + 4 \in Z_{12}[x]$. Find all roots of $f(x)$ over Z_2.

(ii) Let $f(x) = 6x + 4 \in Z_{12}[x]$. Find all roots of $f(x)$ over Z_2.

QUESTION 3. If someone told you that $gcd(2,4) = 4$ over Z_1 ? Is it really right? explain.

QUESTION 4. Construct a field with 9 elements. (Show the work)

QUESTION 5. (i) Let $R = Z_6[x]$. Convince me that $f(x) = x^2 + x + 1 \in R$ is an irreducible element, but it is not a prime element. Let $\bar{I} = \langle f(x) \rangle = span\{f(x)\}$. How many elements does the ring $A = R/I$ have? How many units does A have? How many units does $Z_{36}[x]$ have? Can we conclude that the structure of A is different from the structure of Z_{36}.

(ii) Give me an example of a polynomial of degree one , say $f(x)$, in $Z[x]$ such that $f(x)$ has no roots over Z but $f(x)$ is reducible!

(iii) Give me an example of a polynomial of degree two , say $f(x)$, in $Z[x]$ such that $f(x)$ has no roots over Z but $f(x)$ is reducible!

(iv) Let $n \geq 1$ be a positive integer. How many units of degree n does the ring $R = Z_9[x]$ have ?

QUESTION 6. Let $R = Z_9[x]$, $I = \langle x^3 \rangle$ is an ideal of R, and $A = R/I$. Let $N/I = J/I$ for some ideal J of R. Find elements $a_1, ..., a_n \in R$ ($n < \infty$) such that $J = (a_1, ..., a_n) = span\{a_1, ..., a_n\}$.

Faculty information

Ayman Badawi, Department of Mathematics & Statistics American University of Sharjah, PO Box 26666, Sharjah, United Arab Emirates.
E mail. abadawi@aus.edu, www.ayman-badawi.com

Answer 1) we require $A = \mathbb{Z}[x]/I$ to be Integral domain

$\therefore$ I must be a prime Ideal of $\mathbb{Z}[x]$.

$\longrightarrow$ Claim: $I = (x-1)\mathbb{Z}[x]$.

- This is prime Ideal
- $(x+I)*(y+I) = y+I \quad \forall\ y+I \in A$.

Proof:

$x-1 \in I \Rightarrow x-1+I = I$

$\therefore x+I = 1+I. \Rightarrow (x+I)(y+I) = (1+I)(y+I) = y+I.$

- A is Infinite

clear, as $\mathbb{Z} \in A/I$. $\left(\frac{\mathbb{Z}}{I} \subset \frac{A}{I}\right)$

Answer 2) (i) $f(x) = 4x+4 \in \mathbb{Z}_{12}[x]$ ✓

Since $f(2) = f(5) = f(8) = f(11) = 0$

and $f(k) \neq 0 \ \forall\ k \in \mathbb{Z}_{12} \setminus \{2,5,8,11\}$

Roots of $f(x)$: 2, 5, 8, 11

(ii) $f(x) = 6x+4 \in \mathbb{Z}_{12}[x]$. ✓

Since $f(k) \neq 0 \ \forall\ k \in \mathbb{Z}_{12}$, $f(x)$ has NO Roots.

Answer 3: YES, $\gcd(2,4) = 4$ over $\mathbb{Z}_{10}$ is correct. ✓

Consider $M = \{m \in \mathbb{Z}_{10} : m|2 \wedge m|4\}$.

$\therefore M = \{1,2,4,6,8\}$.

Further, $1|4,\ 2|4,\ 4|4,\ 6|4,\ 8|4$.

$\therefore \gcd(2,4) = 4$ //

Answer 4) Consider $\mathbb{Z}_3[x]$.

consider $f(x) = x^2+x+2 \in \mathbb{Z}_3[x]$.

Since $f(0)=2$, $f(1)=1$, $f(2)=2$, f is Irreducible

Let $R = \dfrac{\mathbb{Z}_3[x]}{(x^2+x+2)}$, i.e. $\dfrac{\mathbb{Z}_3[x]}{I}$, where $I=(x^2+x+2)$

Then $R = \{0+I,\ 1+I,\ 2+I,\ x+I,\ 2x+I,$
$(x+1)+I,\ (x+2)+I,\ (2x+1)+I,\ (2x+2)+I\}$

Claim: R is a field. clearly $|R|=9$

since x^2+x+2 is irreducible in $\mathbb{Z}_2[x]$
(x^2+x+2) is a prime Ideal of $\mathbb{Z}_2[x]$.

$\therefore \dfrac{\mathbb{Z}_3[x]}{(x^2+x+2)}$ is an Integral domain and is finite

$\therefore R$ is a field ■ ✓

Answer 5) (i) $R = \mathbb{Z}_6[x]$.

Part I: $f(x)=x^2+x+1$ is Irreducible

$\mathbb{Z}_6[x]$ is an Integral domain & f is Monic.

Since $f(0)=1$, $f(1)=3$, $f(2)=1$, $f(3)=1$, $f(4)=3$, $f(5)=1$

$\therefore f$ has no Roots $\Rightarrow f$ is Irreducible.

Part II: $f(x) = x^2+x+1$ is NOT Prime

Since $x^2+x+1 \mid 4x^2+4x+4$

However: $4x^2+4x+4 = (4x+2)(x+2)$ ✓

and $x^2+x+1 \nmid 4x+2$ and $x^2+x+1 \nmid x+2$,

we conclude: x^2+x+1 cannot Be Prime

→ Let $A = R/I$ where $I = (f(x))$

PART III: $|A| = ?$ claim: $|A| = 36$.

Proof: $g(x) \in A/I \Rightarrow g(x) = a_1 x + a_2 + I$

and $a_1, a_2 \in \mathbb{Z}_6[x]$

∴ we have 6 choices for a_1 and 6 for a_2

∴ $|A/I| = 6 * 6 = 36$

PART IV: $|U(A)| = ?$ claim: $|U(A)| = 2$

$g(x) \in A \Rightarrow g(x) = ax + b$. $ax+b \in U(A) \Rightarrow b \in U(\mathbb{Z}), a \in N(\mathbb{Z}_6)$

∴ $a = 0$ and $b = 1, 5$

(VERIFICATION) Assume $(a,b) = a(x) + b(1) \in U(A)$

∴ $\exists\ (u,v) = u(x) + v(1) \in U(A)$

s.t. $(a,b) \cdot (u,v) = (au,\ av+bu,\ bv) = (0,0,1)$

∴ $bv = 1 \Rightarrow$ we have two cases: $b = v = 1$ (OR) $b = v = 5$

Case 1: $b = v = 1$.

$au = 0 \Rightarrow$

- $a = 3,\ u = 2$
- $a = 2,\ u = 3$
- $a = 3,\ u = 4$
- $a = 4,\ u = 3$
- $a = 0$
- $u = 0$

} ONLY 4 ways such that $au = 0$. (we treat $a=0, u=0$ later)

In all 4 cases:

$av + bu =$

- $3(1) + 2(1) = 5 \neq 0$
- $2(1) + 3(1) = 5 \neq 0$
- $3(1) + 4(1) = 1 \neq 0$
- $4(1) + 3(1) = 1 \neq 0$.

The ONLY way to get $(au, av+bu, bv) = (0,0,1)$: $(a,b) = (0,1)$, $(u,v) = (0,1)$

Case II: $b = v = 5$

Similarly,

$au = 0$

- $a = 3, u = 2$
- $a = 2, u = 3$
- $a = 3, u = 4$
- $a = 4, u = 3$
- $a = 0$
- $u = 0$

Then $av + bu$

- $3(5) + 2(5) = 1$
- $2(5) + 3(5) = 1$ $\neq 0$.
- $3(5) + 4(5) = 5$
- $4(5) + 3(5) = 5$

$\therefore$ ONLY way to get $(au, av + bu, bv) = (0,0,1)$ is: $(a,b) = (0,5)$, $(u,v) = (0,5)$

$\therefore U(A) = \{1, 5\}$.

$\therefore$ Structure of A is different from structure of $\mathbb{Z}_{36}$ as $|U(\mathbb{Z}_{36})| \neq 2$.

(iii) Let $f(x) = 4x + 2$.

- $f(x)$ has no roots in $\mathbb{Z}[x]$
- $4x + 2 = 2(2x+1)$ and $2, 2x+1 \notin U(\mathbb{Z}[x])$

(iii) Let $f(x) = 2x^2 + 2x + 2$ in $\mathbb{Z}[x]$.

- $f(x)$ has no roots in $\mathbb{Z}[x]$.
- $f(x) = 2(x^2 + x + 1)$ and $2, x^2 + x + 1 \notin U(\mathbb{Z}[x])$

(iv) $R = \mathbb{Z}_q[x]$ and $\deg(f(x)) = n$.

$\therefore f = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$

If $f \in U(\mathbb{Z}_q[x])$

we require $a_n, a_{n-1}, a_{n-2}, \dots, a_2, a_1 \in Nil(\mathbb{Z}_q)$ and $a_0 \in U(\mathbb{Z}_q)$ (and $a_n \neq 0$)

∴ Since $|U(\mathbb{Z}_q)| = 3(2) = 6$ ✓

and $|N(\mathbb{Z}_q)| = |\mathbb{Z}_q \setminus U(\mathbb{Z}_q)| = 9 - 6 = 3$ ✓

$\because q = 3^2 = p^m$

$\Downarrow$

$Z(\mathbb{Z}_q) = Nil(\mathbb{Z}_q)$

∴ No. of units of degree 'n': $3^{n-1} * 6$

$2 \cdot 3^{n-1} \cdot 6$ ✓ (note $a_n \neq 0$)

ANSWER 6: $R = \mathbb{Z}_q[x]$, $I = (x-3)R$, $A = R/I$

Let $N(A) = J/I$. Find $a_1, a_2, \dots, a_n$ s.t. $J = (a_1, a_2, \dots, a_n)$

Solution: $R/I = \{0+I, 1+I, \dots, 7+I, 8+I\}$. ✓

$\therefore N(A) = J/I = \{3+I, 6+I, 0+I\}$.

∴ $J = 3\mathbb{Z}_q[x]$ → I must live in J

$\because J = \dfrac{3\mathbb{Z}_q[x] + I}{(x-3)\mathbb{Z}_q[x]} = \{0+I, 3+I, 6+I\}$.

∴ $a_1 = 3$ generates J.

$J = 3\mathbb{Z}_q[x] + I = (3, x-3)$

So $a_1 = 3$, $a_2 = (x-3)$