Dr. Ramjee Prasad (Mathematics). (Honours)
B.Sc. III, Title- Ring homomorphism.

Page No.:
Date:

(1) Let R be the ring of integers modulo 6.
Let $f(x) = x^3+5$, $g(x) = 2x^2+4x+1$, $h(x) = 3x+4$.
Compute $f(x)+g(x)$, $f(x).h(x)$ and $g(x).\{f(x)-h(x)\}$.

Solution: $f(x)+g(x) = x^3+5+2x^2+4x+1$.
$= x^3+2x^2+4x$.

$f(x).h(x) = (x^3+5)(3x+4)$
$= 3x^4+4x^3+15x+20$
$= 3x^4+4x^3+3x+2$.

$g(x).\{f(x)-h(x)\} = g(x)(x^3+5-3x-4)$.
$= (2x^2+4x+1)(x^3+3x+1)$
$= 2x^5+6x^3+2x+4x^4+12x^2+4x+x^3+3x+1$
$= 2x^5+4x^4+x^3+12x^2+3x+1$.
$= 2x^5+4x^4+x^3+3x+1$.

(2) Show that $x^3+2 \in F_{11}[x]$ is reducible over the field F_{11} of integers reduced modulo 11.

Solution. We have
$F_{11} = \{0,1,2,3,4,5,6,7,8,9,10\}$.
$f(0) = 2, f(1) = 3, f(2) = 10, f(3) = 5, f(4) = 66 = 0$.
$f(5) = 6, f(6) = 7, f(7) = 4, f(8) = 8, f(9) = 9, f(10) = 1$
$\because -4 \equiv 7 \pmod{11}$.

Hence, $x-4 = x+7$ divides $f(x)$.
Thus, $f(x) = (x+7)(x^2+4x+5)$.
$\Rightarrow f(x)$ is reducible over F_{11}.

(3) Prove that x^2+x+4 is irreducible over the F_{11} of integers reduced modulo 11.

Solution. $f(x) = x^2+x+4$, $\deg f(x) = 2$.
$\Rightarrow f(a) \neq 0$ for any $a \in F_{11}$.
$\therefore$ irreducible over F_{11}.

Hence (x^2+x+4) is a maximal ideal of $\mathbb{Z}[x]$.

(4) Prove that (i) $x^4+27x^2+9pc+3$ (ii) $1+7x+7x^2$ are irreducible over field $\mathbb{Q}$.

Solution: We have,

(i) $f(x) = 3+9x+27x^2+0x+x^4$.

$a_0=3, a_1=9, a_2=27, a_3=0, a_4=1$.

Take $p=3$, then

$p|a_0, p|a_1, p|a_2, p|a_3, p|a_4, p^2 \nmid a_0$.

Hence, by Eisenstein Criterion $f(x)$ is irreducible over $\mathbb{Q}$.

(ii) $f(x) = 1+7x+7x^2$.

$a_0=1, a_1=7, a_2=7$

Take $p=7$. Then

$p|a_2, p|a_1, p|a_0, p^2|a_2$.

Hence $f(x)$ is irreducible over $\mathbb{Q}$.

(5) Show that $f(x) = 1+x+x^2+\cdots+x^{p-1}$, $p>1$ is an integer is irreducible over field $\mathbb{Q}$ when p is a prime.

Solution: We have,

$$f(x) = \frac{x^p-1}{x-1}$$

Hence $g(x) = f(x+1) = \frac{(x+1)^p-1}{x+1-1} = \frac{(x+1)^p-1}{x}$

Hence $g(x) = x^{p-1} + {}^pC_1 x^{p-2} + \cdots + {}^pC_1$.

The coefficients of polynomial $g(x)$ are

$a_0 = {}^pC_1, a_1 = {}^pC_2, \ldots, a_{p-2} = {}^pC_1, a_{p-1} = 1$.

Consider a prime number p. Then

$p|a_0, p|a_1, \ldots, p|a_{p-2}, p|a_{p-1}$ and $p^2 \nmid a_0$.

Therefore by Eisenstein Criterion $g(x)$ is irreducible over $\mathbb{Q}$.

Hence $f(x+1)$ is irreducible over $\mathbb{Q}$. This gives that $f(x)$ is irreducible over $\mathbb{Q}$. //

(6) Show that ring of

Solution:

Let $\mathbb{Z}$ be ring of that $\mathbb{Z}$ is an integral mapping $d: \mathbb{Z}_0 \to \mathbb{W}$ integers and $\mathbb{W}$ is set such that

$d(n) = |n$

(i) $\forall m, n \in \mathbb{Z}_0 \Rightarrow d(mn)$

$\Rightarrow d(mn)$

$\Rightarrow d(mn)$

(ii) For any $m, n \in \mathbb{Z}_0$; b

$n = mq + r$,

$\Rightarrow n = mq + r$,

This shows that $\mathbb{Z}$ is

(7) Show that ring of G Euclidean domain

Solution: Let $\mathbb{Z}[i]$ is

i.e. $\mathbb{Z}[i] = \{a+i$

To show that $\mathbb{Z}[i]$ i

(i) $\forall z_1, z_2 \in \mathbb{Z}[i] \Rightarrow$

(ii) $\forall z_1 \in \mathbb{Z}[i] \Rightarrow \exists z \in$

(iii) $\forall z_1, z_2 \in \mathbb{Z}[i]$;

Hence, $\mathbb{Z}[i]$ is a

In order to prove th

We consider a mappi

$d(z) = |z| = \sqrt{x^2}$

(iv) For any z_1, z_2

Page No.:
Date:

⑥ ~~Show that the ring of integers is a Euclidean~~

Solution:

Let z be ring of integers and it is clear that z is an integral domain. Consider the mapping $d: z_0 \to w$ where z_0 is a set of non-zero integers and w is set of non-negative integers, such that

$$d(n) = |n| \in w \quad \forall n \in z_0. \qquad \text{—— (1)}$$

(i) $\forall m, n \in z_0 \Rightarrow d(mn) = |mn| = |m|\,|n| = d(m)\,d(n)$.

$\Rightarrow d(mn) \geq |n| \quad \because |m| \geq 1.$

$\Rightarrow d(mn) \geq d(n).$

(ii) For any $m, n \in z_0$; by division algorithm,

$n = mq + r$, $r = 0$ or $|r| < |m|$.

$\Rightarrow n = mq + r$, $r = 0$, or $d(r) < d(m)$.

This shows that z is a Euclidean domain.

⑦ Show that ring of Gaussian integers is a Euclidean domain.

Solution: Let $J[i]$ is ring of Gaussian integers

i.e. $J[i] = \{a + ib : a, b \in z\}$

To show that $J[i]$ is Euclidean domain.

(i) $\forall z_1, z_2 \in J[i] \Rightarrow z_1 + z_2 = z_2 + z_1$ (as $J[i] \subseteq C$).

(ii) $\forall z_1 \in J[i] \Rightarrow \exists 1 \in J[i]$ i.e. $1 = 1 + 0i$ such that $1 \cdot z_1 = z_1 = z_1 \cdot 1$.

(iii) $\forall z_1, z_2 \in J[i]$; $z_1 \cdot z_2 = 0 \Rightarrow z_1 = 0$ or $z_2 = 0$.

Hence, $J[i]$ is an integral domain.

In order to prove that $J[i]$ is Euclidean domain, we consider a mapping $d: (J[i] - \{0\}) \to w$ such that

$d(z) = |z| = \sqrt{x^2 + y^2} \in w \quad \forall z \in J[i]$.

For any $z_1, z_2 \neq 0 \in J[i]$

$d(z_1, z_2) = |z_1 z_2| = |z_1| \cdot |z_2|$

$\therefore d(z_1, z_2) \geq |z_1| = d(z_1)$. $\because |z_2| \geq 1$ as $z_2 \in J[i]$

(1) For $z_1, z_2 \neq 0 \in J[i]$, we have

$$\frac{z_1}{z_2} = u \Rightarrow \frac{z_1}{z_2} = p + iq = u$$

If $p, q \in \mathbb{Z}$ then $p + iq = u \in J[i]$. Hence

$z_1 = uz_2$ i.e. $z_1 = uz_2 + r$. [where $r = 0$]

If $p, q \notin \mathbb{Z}$ then $p + iq = u \notin J[i]$.

Suppose p', q' are integers such that $|p - p'| \leq 1/2$, $|q - q'| \leq 1/2$. Then

$p' + iq' = u' \in J[i]$.

Now, $\frac{z_1}{z_2} = u \Rightarrow z_1 = z_2 u \Rightarrow z_1 = z_2 u' + z_2 u - z_2 u'$

$\Rightarrow z_1 = z_2 u' + z_2 (u - u')$

$\Rightarrow z_1 = q \cdot z_2 + r$; $r = z_2 (u - u')$.

Now, $d(r) = d(z_2 (u - u')) = |z_2| |u - u'|$

$\Rightarrow d(r) = d(z_2)\, d(u - u')$

where $d(u - u') = \sqrt{(p - p')^2 + (q - q')^2} \leq \frac{1}{\sqrt{2}} < 1$.

$\Rightarrow d(r) < d(z_2)$.

Hence, in general, $z_1 = qz_2 + r$ where $z_1 = qz_2 +$

Thus, $J[i]$ is Euclidean domain.