MA268 Algebra 3, Assignment 3

Dyson Dyson

Question 1

> Let
> $$f = X^3 + X + 1, \qquad g = X^5 + X^2 + 3$$
> in $\mathbb{F}_7[X]$. Determine the quotient and remainder you obtain on dividing g by f.

$$
\begin{array}{rrrrrr}
 & & & X^2 & & +6 \\ \cline{2-6}
X^3+X+1 \big) & X^5 & & +X^2 & & +3 \\
 & X^5 & +X^3 & +X^2 & & \\ \cline{2-4}
 & & 6X^3 & & & +3 \\
 & & 6X^3 & & +6X & +6 \\ \cline{3-6}
 & & & & X & +4
\end{array}
$$

So the quotient is $X^2 + 6$ and the remainder is $X + 4$.

Question 2

> Let R be an integral domain. Show that $R[x]$ is an integral domain.

For $R[x]$ to be an integral domain, it needs to have no zero divisors. For some coefficients $a_i, b_i \in R$, where at least one $a_i \neq 0$ and at least one $b_i \neq 0$, we have $\sum_{i=0}^{\infty} a_i x^i, \sum_{i=0}^{\infty} b_i x^i \in R[x]$. Their product is some other polynomial in $R[x]$ whose coefficients are all of the form $a_i b_j$. For this product to be 0, we would need all the coefficients to be 0.

But we know there exists at least one $a_k \neq 0$ and $b_\ell \neq 0$. Then $a_k b_\ell \neq 0$, so that term of the product is non-zero. That means the product must be non-zero, so $R[x]$ has no zero divisors and is thus an integral domain.

$\square$

Question 3

Let R be an integral domain. Show that $R[x]^* = R^*$.

Let $f \in R[x]$. Then $f \in R[x]^*$ if and only if there is some $g \in R[x]$ such that $fg = 1$. We shall suppose $f \neq 0$ and $g \neq 0$, and since R is an integral domain, $fg \neq 0$.

The degree of a product is the sum of the degrees, so $\deg fg = \deg f + \deg g$. So if $\deg f > 0$ or $\deg g > 0$ then $\deg fg > 0$. But $\deg 1 = 0$, so we need $\deg f = \deg g = 0$.

Therefore all elements of $R[x]^*$ have degree 0, meaning they are just elements of R. Those elements must also all be units in R, so $R[x]^* \subset R^*$.

Clearly any unit in R is a unit in $R[x]$, so $R^* \subset R[x]^*$. Therefore $R[x]^* = R^*$.

$\square$

Note that if R were not an integral domain, we might have $\deg fg = \deg 0$, which would break things.

Question 4

Let R be a ring. An element $a \in R$ is called *nilpotent* if there is some positive integer n such that $a^n = 0$.

(i) Show that if a is nilpotent, then $1 + a$ is a unit.

(ii) Let p be a prime and $r \geq 2$. Show that $\overline{1} + \overline{p}X$ is a unit $(\mathbb{Z}/p^r\mathbb{Z})[X]$. Why doesn't this contradict **Q3**?

Q4 (i)

Clearly $\sum_{k=0}^{n-1} (-1)^k a^k \in R$. Then

$$\begin{aligned}
\left(\sum_{k=0}^{n-1} (-1)^k a^k\right)(1+a) &= \sum_{k=0}^{n-1} (-1)^k a^k + \left(\sum_{k=0}^{n-1} (-1)^k a^k\right) a \\
&= \sum_{k=0}^{n-1} (-1)^k a^k + \sum_{k=0}^{n-1} (-1)^k a^{k+1} \\
&= 1 + a^n \\
&= 1 + 0 \\
&= 1
\end{aligned}$$

Likewise,

$$\begin{aligned}
(1+a)\left(\sum_{k=0}^{n-1} (-1)^k a^k\right) &= \sum_{k=0}^{n-1} (-1)^k a^k + a\left(\sum_{k=0}^{n-1} (-1)^k a^k\right) \\
&= 1 + a^n \\
&= 1
\end{aligned}$$

So $1 + a$ is a unit.

Q4 (ii)

$(\overline{p}X)^r = \overline{p}^{\,r} X^r = 0$, so $\overline{p}X$ is nilpotent. Therefore $\overline{1} + \overline{p}X$ is a unit by part **(a)**.

This doesn't contradict **Q3** because $\mathbb{Z}/p^r\mathbb{Z}$ is not an integral domain. If $s + t = r$ then $\overline{p}^{\,s}\,\overline{p}^{\,t} = \overline{p}^{\,r} = 0$, so $\overline{p}^{\,s}$ and $\overline{p}^{\,t}$ are zero divisors.

Question 5

Often the easiest way to show that a subset of a ring is an ideal is to find a homomorphism whose kernel is this set. Let I be the subset of $\mathbb{R}[X]$ consists of all polynomials $a_0 + a_1X + \cdots + a_nX^n$ with $a_0 + a_1 + \cdots + a_n = 0$.

(i) Show that I is an ideal.

(ii) Show that $I = (X - 1)\mathbb{R}[X]$.

(iii) Show that $\mathbb{R}[X]/I \cong \mathbb{R}$.

Q5 (i)

Let $\phi : \mathbb{R}[X] \to \mathbb{R}$ be defined by $\phi(f) = f(1)$. It is easy to see that $\phi(f + g) = f(1)+g(1) = \phi(f)+\phi(g)$, that $\phi(fg) = f(1)g(1) = \phi(f)\phi(g)$, and that $\phi(1) = 1$. Therefore ϕ is a ring homomorphism. Clearly $\ker\phi = I$ by the definition of I. Therefore I is an ideal.

Q5 (ii)

Suppose $f \in I$. Then $f(1) = 0$, so $X - 1$ is a factor of f. Therefore we can factor out $X - 1$ from any $f \in I$. Therefore $I = \ker\phi = (X - 1)\mathbb{R}[X]$.

Q5 (iii)

Clearly ϕ is surjective, so $\operatorname{Im}\phi = \mathbb{R}$. Then the First Isomorphism Theorem tells us that $\mathbb{R}[X]/I \cong \mathbb{R}$, where the isomorphism $\hat{\phi}$ is defined by $\hat{\phi}(f + I) = \phi(f) = f(1)$.

Question 6

Let $I = (X^2 - X)\mathbb{R}[X] \subset \mathbb{R}[X]$ (i.e. I is the principal ideal generated by $X^2 - X$). Let

$$\phi : \mathbb{R} \to \mathbb{R}[X]/I, \qquad \phi(a) = aX + I.$$

(i) Show that $\phi(a+b) = \phi(a) + \phi(b)$ and $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in \mathbb{R}$.

(ii) Show that ϕ is not a homomorphism.

Q6 (i)

By the rules of addition and multiplication in quotient rings,

$$\begin{aligned}
\phi(a+b) &= (a+b)X + I \\
&= (aX + bX) + I \\
&= (aX + I) + (bX + I) \\
&= \phi(a) + \phi(b)
\end{aligned}$$

$$\begin{aligned}
\phi(ab) &= abX + I \\
&= (aX + I)(bX + I) \\
&= \phi(a)\phi(b)
\end{aligned}$$

Q6 (ii)

To be a homomorphism, we would need $\phi(1) = 1 + I$. However, $\phi(1) = X + I$. For this to equal $1 + I$, we would need $X - 1 \in I$. This is impossible since the lowest-degree term of any polynomial in I is X, so $X - 1 \notin I$. Therefore ϕ is not a homomorphism.