Abstract Algebra by Pinter, Chapter 24

Amir Taaki

Chapter 24 on Rings of Polynomials

Contents

A. Elementary Computation in Domains of Polynomials

Q1

$\mathbb{Z}[x]$

$$a(x) + b(x) = x^3 + 7x^2 + 4x + 1$$
$$a(x) - b(x) = -x^3 - 3x^2 + 2x + 1$$

$$\begin{aligned} a(x)b(x) &= 2x^5 + 10x^4 + 2x^3 + 3x^4 + 15x^3 + 3x^2 + x^3 + 5x^2 + x \\ &= 2x^5 + 13x^4 + 18x^3 + 8x^2 + x \end{aligned}$$

$\mathbb{Z}_5[x]$

$$a(x) + b(x) = x^3 + 2x^2 + 4x + 1$$
$$a(x) - b(x) = 4x^3 + 2x^2 + 2x + 1$$
$$a(x)b(x) = 2x^5 + 3x^4 + 3x^3 + 3x^2 + x$$

$\mathbb{Z}_6[x]$

$$
\begin{aligned}
a(x) + b(x) &= x^3 + x^2 + 4x + 1 \\
a(x) - b(x) &= 5x^3 + 3x^2 + 2x + 1 \\
a(x)b(x) &= 2x^5 + x^4 + 2x^2 + x
\end{aligned}
$$

$\mathbb{Z}_7[x]$

$$
\begin{aligned}
a(x) + b(x) &= x^3 + 4x + 1 \\
a(x) - b(x) &= 6x^3 + 4x^2 + 2x + 1 \\
a(x)b(x) &= 2x^5 + 6x^4 + 4x^3 + x^2 + x
\end{aligned}
$$

Q2

$$
\begin{aligned}
\mathbb{Z} : x^3 + x^2 + x + 1 &= (x^2 + 3x + 1)(x - 2) + (5x - 5) \\
\mathbb{Z}_5 : x^3 + x^2 + x + 1 &= (x^2 + 3x + 2)(x + 3)
\end{aligned}
$$

Q3

$$
\begin{aligned}
\mathbb{Z} : x^3 + 2 &= (\frac{x}{2} - \frac{3}{4})(2x^2 + 3x + 4) + (\frac{x}{4} + 5) \\
\mathbb{Z}_3 : x^3 + 2 &= (2x)(2x^2 + 3x + 4) + (-2x + 2) \\
\mathbb{Z}_5 : x^3 + 2 &= (3x + 3)(2x^2 + 3x + 4) + 4x
\end{aligned}
$$

Q4

a

When $n = 1$, $x + 1$ is a factor of $x^n + 1$.

Assume $n = k$ is true

$$
\begin{aligned}
x^{k+2} + 1 &= x^2 x^k \\
&= x^2(x^k + 1) + (1 - x^2) \\
&= x^2(x^k + 1)(1 - x)(1 + x)
\end{aligned}
$$

Since $x + 1$ is a factor of $x^k + 1$, this means $x + 1$ is also a factor of x^{k+2}.

b

As before $n = 1$ is trivially true and we assume $n = k$ is true.

$$
x^{k+2} + x^{k+1} + x^k + \cdots + x + 1 = x^2(x^k + \cdots + x + 1) + (x + 1)
$$

Since $x + 1$ divides both terms, that means it is a divisor of the expression on the left.

Q5

By induction assume $m = k$ is true, then

$$
x^{k+1} + 2 = x(x^k + 2) + (x + 2)
$$

$(x + 2)$ divides both sides and so is a divisor of $x^{k+1} + 2$ in $\mathbb{Z}_3[x]$.

Likewise for $\mathbb{Z}_n[x]$

$$
\begin{aligned}
x^{k+1} + (n - 1) &= x(x^k + (n - 1)) + (x + (n - 1)) \\
&= x^{k+1} + (n - 1)x + x + (n - 1) \\
&= x^{k+1} + nx + (n - 1) \\
&= x^{k+1} + (n - 1)
\end{aligned}
$$

and so $x + (n - 1) is a factor of $x^{k+1} + (n - 1)$ in $\mathbb{Z}_n[x]$.

Q6

$$\begin{aligned}(2x^2+ax+b)(3x^2+4x+m) &= 6x^4+8x^3+2x^2m+3ax^3+4ax^2+max+3bx^2+4bx+mb \\ &= 6x^4+50\end{aligned}$$

grouping terms

$$6x^4+(8+3a)x^3+(2m+4a+3b)x^2+(ma+4b)x+mb = 6x^4+50$$

Writing out the roots, we have

$$8+3a=0$$

$$2m+4a+3b=0$$

$$ma+4b=0$$

$$mb=50$$

The first equation has no solution since $3 \nmid a$ and so $6x^4+50$ cannot be factored into $3x^2+4x+m$.

Q7

$$\begin{aligned}(x^3+ax^2+bx+c)(x^2+1) &= x^5+x^3+ax^4+ax^2+bx^3+bx+cx^2+c \\ &= x^5+ax^4+(1+b)x^3+(a+c)x^2+bx+c \\ &= x^5+5x+6\end{aligned}$$

Comparing terms, we have

$$\begin{aligned} a &\equiv 0 \pmod{n} \\ 1+b &\equiv 0 \pmod{n} \\ a+c &\equiv 0 \pmod{n} \\ b &\equiv 5 \pmod{n} \\ c &\equiv 6 \pmod{n} \\ \implies 1+5 &\equiv 0 \pmod{n} \\ \implies 6 &\equiv 0 \pmod{n} \end{aligned}$$

$$n = 6, 2, 3$$

B

Q1

```
>>> def foo(n):
...     print((n**8 + 1)%5, (n**3 + 1)%5)
...
>>> for i in range(5):
...     foo(i)
...
1 1
2 2
2 4
2 3
2 0
```

Both sides are not equal when $x = 2, 3, 4$.

Q2

No this is impossible. If they are equal then their difference is 0.

Q3

$$0x^2 + 0x + 0$$
$$0x^2 + 0x + 1$$
$$0x^2 + 0x + 2$$
$$...$$
$$0x^2 + 0x + 4$$
$$0x^2 + 1x + 0$$
$$...$$
$$0x^2 + 4x + 0$$
$$1x^2 + 0x + 0$$
$$...$$
$$4x^2 + 4x + 4$$

There are 5^3 polynomials in $\mathbb{Z}_5[x]$ of degree 2 or less. There are 5^2 polynomials in $\mathbb{Z}_5[x]$ of degree 1 or 0.
Thus there are $5^3 - 5^2$ quadratic polynomials in $\mathbb{Z}_5[x]$.
Cubic:

$$0x^3 + 0x^2 + 0x + 0$$
$$...$$
$$0x^3 + 0x^2 + 0x + 4$$
$$0x^3 + 0x^2 + 1x + 0$$
$$...$$
$$0x^3 + 0x^2 + 4x + 4$$
$$0x^3 + 1x^2 + 0x + 0$$
$$...$$
$$0x^3 + 4x^2 + 4x + 4$$
$$1x^3 + 0x^2 + 0x + 0$$
$$...$$
$$4x^3 + 4x^2 + 4x + 4$$

Answer: $5^4 - 5^3$
There are $n^{m+1} - n^m$ polynomials of degree m in $\mathbb{Z}_n[x]$.

Q4

$$(x+1)^2 = x^2 + 2x + 1 = x^2 + 1 \text{ in } A[x] \implies \text{char } A = 2$$
$$(x+1)^4 = x^4 + 4x^3 + 6x^2 + 4x + 1 = x^4 + 1 \text{ in } A[x] \implies \text{char } A = \gcd(4,6) = 2$$
$$(x+1)^6 = x^6 + 6x^5 + 15x^4 + 20x^3 + 15x^2 + 6x + 1 = x^6 + 2x^3 + 1 \text{ in } A[x] \implies \text{char } A = \gcd(6, 15, 20-2) = 3$$

Q5

$$(2x+2)^3 = 8x^3 + 24x^2 + 24x + 8 = 0 \text{ in } \mathbb{Z}_8[x]$$
$$\implies 2x + 2 \text{ is a divisor of } 0$$

$$(1-4x)(1+4x) = 1 - 16x^2 = 1 \text{ in } \mathbb{Z}_8[x]$$
$$\implies 1 + 4x \text{ and } 1 - 4x \text{ are invertible elements}$$

Q6

For any polynomial $b(x) \in A[x], \deg b(x) \geq 0$. If $\deg b(x) = 0$ then $xb(x) = 0$ because $b(x) = 0$. Otherwise $\deg[x \cdot b(x)] = \deg x + \deg b(x) = 1 + \deg b(x) \implies \deg[x \cdot b(x)] \geq 1$.

Since x is in every non-zero polynomial domain, this means there are no polynomial fields.

Q7

Take $a(x) = x \in A[x]$, then $\deg a(x) = 1$ and $\deg[(a(x))^2] = 2$. In fact $\deg[(a(x))^n] = n$ in any ring and so there is no polynomial with a nonzero term that multiplied by x produces 0.

$$x(b_0 + b_1x + \cdots + b_mx^m)$$

where $b_m \neq 0$ in the ring, then

$$\deg[a(x) \cdot b(x)] = m + 1 \neq 0$$

Q8

Idempotent: $(a(x))^2 = a(x)$ Nilpotent: $(a(x))^n = 0$ for some integer n.

Let $a(x) = x$, then $(a(x))^2 = x^2$, so $(a(x))^2 \neq a(x)$ and $a(x)$ is not idempotent.

Also $(a(x))^n = x^n \neq 0$ and so $a(x)$ is not nilpotent.

C. Rings $A[x]$ Where A Is Not an Integral Domain

Q1

An integral domain is a commutative ring with unity having no divisors of 0.

Since $A[x]$ contains the elements from A, then if A has zero divisors, so does $A[x]$ and hence $A[x]$ is not an integral domain.

Q2

Degree 0: $2 \times 2 = 0$ in $\mathbb{Z}_4[x]$

Degree 1: $2x \cdot 2x = 0$

Degree 2: $2x^2 \cdot 2x^2 = 0$

Q3

$5x^3(2x + 1) = 0$ in $\mathbb{Z}_10[x]$ lacks the cancellation property whereas the term $5x^3 = 0$ in $\mathbb{Z}_5[x]$ and disappears.

Q4

Any polynomials where the coefficient of the leading term is a multiple of the field size.

$\mathbb{Z}_4[x] : (2x + 3)(2x + 1) = 3$

$\mathbb{Z}_6[x] : (3x + 1)(2x + 5) = 5x + 5$

$\mathbb{Z}_9[x] : (3x + 1)(3x + 4) = 6x + 4$

Q5

$$a(x) = a_0 + a_1x + \cdots + a_nx^n$$
$$b(x) = b_0 + b_1x + \cdots + b_mx^m$$

$$\deg a(x) = n$$
$$\deg b(x) = m$$

$$a_n, b_m \in A : a_n \neq 0, b_m \neq 0, a_n b_m = 0$$

Thus the coefficient of x^{n + m} is 0 and so

$$\deg a(x)b(x) < \deg a(x) + \deg b(x)$$

Q6

In an integral domain

$$\deg a(x)b(x) = \deg a(x) + \deg b(x)$$

Non-constant polynomials have a degree greater than one. Let $a(x)$ be such a polynomial, while $b(x)$ is a non-zero polynomial such that $\deg b(x) \geq 1$. Then $\deg a(x)b(x) > 1$, while the degree of 1 is 1. So there are no non-constant invertible polynomials in integral domains.

In $\mathbb{Z}_4[x]$, $(2x+1)^2 = 1$, so $(2x+1)$ is invertible and so are all powers of $(2x+1)^k$ since $(2x+1)$ is its own inverse.

Q7

$\mathbb{Z}_9[x]$

$$(x + 3)(x + 6)$$
$$(2x + 3)(5x + 6)$$
$$(4x + 3)(7x + 6)$$
$$(5x + 3)(8x + 6)$$
$$(2x + 6)(5x + 3)$$
$$(4x + 6)(7x + 3)$$
$$(5x + 6)(8x + 3)$$

$\mathbb{Z}_5[x]$

$$5 \mid (a + b) \qquad 5 \mid ab$$

but $\gcd(a, 5) = 1$ and $\gcd(b, 5) = 1$ since 5 is prime. So there is only 1 factorization which is x^2.

Q8

$\mathbb{Z}_5[x]$

$$\begin{aligned} a + b &\equiv 1 \pmod 5 \\ ab &\equiv 4 \pmod 5 \end{aligned}$$

$$\begin{aligned} 2 + 4 &\equiv 1 \pmod 5 \\ 3 + 3 &\equiv 1 \pmod 5 \\ 2 \times 2 &\equiv 4 \pmod 5 \\ 3 \times 3 &\equiv 4 \pmod 5 \end{aligned}$$

$$\begin{aligned} (x + 3)^2 &= x^2 + x + 4 \\ [4(x + 3)]^2 &= 16x^2 + 96x + 144 \\ &= x^2 + x + 4 \\ &= (4x + 2)^2 \end{aligned}$$

$\mathbb{Z}_8[x]$

Any polynomial of the form $1 + 4x + 4x^2 + \cdots + 4x^n$ when squared will equal 1, because every coefficient apart from the constant and leading term is greater than or equal to 2, and $4 \times 2 = 8 = 0$, and the leading term is $16x^{2n} = 0$. So there are infinite polynomial square roots in $\mathbb{Z}_8[x]$.

D. Domains $A[x]$ Where A Has Finite Characteristic

Q1

Every coefficient in $A[x]$ is a member of A. For all $a(x), b(x) \in A[x], c(x) = a(x) + b(x)$ then $c_i = a_i + b_i$, and therefore the characteristic is preserved since $\underbrace{1_A + 1_A + \cdots + 1_A}_{\text{char } A} = 0$.

Q2

Consider the ring $\mathbb{Z}_n[x]$ of polynomials in one variable x with coefficients in $\mathbb{Z}_n$. It is an infinite ring since $x^m \in \mathbb{Z}_n[x]$ for all positive integers m, and $x^{m_1} \neq x^{m_2}$ for $m_1 \neq m_2$. But the characteristic of $\mathbb{Z}_n[x]$ is clearly n.

Q3

$$
\begin{aligned}
(x+2)(x^{m-1} + x^{m-2} + \cdots + x^2 + x + 1) &= x(x^{m-1} + x^{m-2} + \cdots + x^2 + x + 1) + 2(x^{m-1} + x^{m-2} + \cdots + x^2 + x + 1) \\
&= x^m + (x^{m-1} + x^{m-2} + \cdots + x^3 + x^2 + x) + 2(x^{m-1} + x^{m-2} + \cdots + x^2 + x) + 2 \\
&= x^m + 2
\end{aligned}
$$

Likewise the above applies for $(p-1)$ in any domain of characteristic p.

Q4

By the cancellation property, the characteristic of every integral domain is prime, since if the characteristic was composite that would imply $rs = 0$ for some $r, s \in A$ which violates the zero divisor rule.

Thus the coefficients for all terms in the expansion $(x+c)^p$ except x^p and c^p, by the binomial formula are equal to $\binom{p}{k} = \frac{p!}{k!(p-k)!}$. Since p is prime and indivisible the coefficient becomes zero.

$$(x+c)^p = x^p + c^p$$

Q5

They aren't the same since $x \notin A$, and $\forall a \in A$, $a = a^2$ but $x \neq x^2$.

Q6

It is trivial to see that

$$
\begin{aligned}
[a_0 + (a_1 x + \cdots + a_n x^n)]^p &= a_0^p + [a_1 x + (a_2 x^2 + \cdots + a_n x^n)]^p \\
&= a_0^p + a_1^p x^p + [a_2 x^2 + (a_3 x^3 + \cdots + a_n x^n)]^p \\
&= a_0^p + a_1^p x_1^p + \cdots + a_n^p x^{np}
\end{aligned}
$$

E. Subrings and Ideals in A[x]

Q1

$B[x]$ contains all the polynomials with coefficients in B. Since B is a subring of A, so $B[x]$ is a subring of $A[x]$.

Q2

Likewise B absorbs all products with A, and hence so does $B[x]$,

Q3

Every coefficient a_i with odd i equal to zero, means the polynomial only has non-zero coefficients for even powers.

When adding polynomials, we add the coefficients. So the odd numbered powers remain zero, and even powers remain non-zero.

For multiplying two polynomials $a(x)b(x)$, the corresponding powers of each term are added together, $a_i b_j x^{i+j}$. Since both i and j are even, so is the resulting term and hence the result of $a(x)b(x)$ remains inside the set S making it a subring.

The above statement does not apply when talking about odd non-zero coefficients, since multiplying two odd terms might result in an even power, for example $c(x) = a(x)b(x)$, $a_3 b_5 x^{3+5}$.

Q4

Let $b(x) \in A[x]$ and $a(x) \in J$, then the constant term in $b(x)$ is b_0. Since $b(x)a(x) = b_0 a(x) + b_1 x a(x) + \cdots + b_m x^n a(x)$, and the powers of all terms in $a(x)$ are ≥ 1, so $b_0 a(x)$ has no constant term. So $\forall a(x) \in J$ absorbs products from $A[x]$ and is an ideal.

Q5

Let $a(x) = a_0 + a_1 x + \cdots + a_n x^n \in J$ and $b(x) = b_0 + b_1 x + \cdots + b_m x^m \in A[x]$. Then $a(x)b(x) = a_0(b_0 + b_1 x + \cdots + b_m x^m) + a_1 x(b_0 + b_1 x + \cdots + b_m x^m) + \cdots + a_n x^n (b_0 + b_1 x + \cdots + b_m x^m)$. Then it can be seen plainly that the sum of cofficients for the result is $(a_0 + a_1 + \cdots + a_n)(b_0 + b_1 + \cdots + b_m) = 0$. Therefore J is an ideal of $A[x]$.

Q6

Since A is an integral domain, there are no divisors of zero. Therefore the values cannot be made to equal 0 unless one of the terms is zero. In the case of Q4, the polynomial is an ideal in J with a zero constant coefficient and in Q5, the polynomial can be factorized into a polynomial where one of the terms has coefficients that sum to zero.

F. Homomorphisms of Domains of Polynomials

Q1

$$a(x) = a_0 + a_1 x + \cdots + a_n x^n$$
$$b(x) = b_0 + b_1 x + \cdots + b_m x^m$$

$$h(a(x) + b(x)) = h((a_0 + b_0) + \cdots) = a_0 + b_0 = h(a(x)) + h(b(x))$$
$$h(a(x)b(x)) = h(a_0 b_0 + \cdots) = a_0 b_0 = h(a(x))h(b(x))$$

Q2

$$\forall a(x) \in A[x], h(x \cdot a(x)) = h(x(a_0 + \cdots + a_n x^n)) = h(a_0 x + \cdots + a_n x^{n+1}) = 0$$
$$\implies \ker h = \{x \cdot a(x) : a(x) \in A[x]\} = \langle x \rangle$$

By the definition of a principal ideal, let x remain fixed as it is multiplied by elements from $A[x]$.

Q3

$$h : A[x] \to A, \ker h = \langle x \rangle \implies A[x]/\langle x \rangle \cong A$$

Q4

$$g(a(x)) = g(a_0 + \cdots + a_n x^n) = a_0 + \cdots + a_n$$

$$\begin{aligned} g(a(x)+b(x)) &= g(a_0 + a_1 x + \cdots + a_m x^m + \cdots + a_n x^n + b_0 + b_1 x + \cdots + b_m x^m) \\ &= (a_0 + b_0) + (a_1 + b_1) + \cdots + (a_m + b_m) + \cdots + a_n \\ &= g(a(x)) + g(b(x)) \end{aligned}$$

$$\begin{aligned} g(a(x)b(x)) &= g(a_0 b(x) + a_n x^n b(x)) \\ &= g(a_0 b_0 + \cdots + a_0 b_m x^m + \cdots + a_n b_0 x^n + \cdots + a_n b_m x^{n+m}) \\ &= a_0 b_0 + \cdots + a_0 b_m + \cdots + a_n b_m = g(a(x))g(b(x)) \end{aligned}$$

Let $a \in A$, then $a(x) \in J + a$, where J is the ideal of g (coefficients that sum to zero). Thus every value in A is an image of an element in $A[x]$ and so h is surjective.

The kernel of g is described in 24E5: let J consist of all the polynomials $a_0 + a_1 x + \cdots + a_n x^n$ in $A[x]$ such that $a_0 + a_1 + \cdots + a_n = 0$.

Q5

$$\begin{aligned} h(a(x)+b(x)) &= (a_0 + b_0) + (a_1 + b_1)cx + (a_2 + b_2)c^2x^2 + \cdots + (a_n + b_n)c^n x^n \\ &= (a_0 + a_1 cx + a_2 c^2 x^2 + \cdots + a_n c^n x^n) + (b_0 + b_1 cx + b_2 c^2 x^2 + \cdots + b_n c^n x^n) \\ &= h(a(x)) + h(b(x)) \end{aligned}$$

$$\begin{aligned} h(a(x)b(x)) &= a_0 b_0 + (a_0 b_1 + a_1 b_0)cx + (a_0 b_2 + a_1 b_1 + a_0 b_2)c^2x^2 + \cdots + \sum_{i+j=n} a_i b_j c^n x^n \\ &= h(a(x))h(b(x)) \end{aligned}$$

Since A is an integral domain and there are no zero divisors, then $\ker h = \{0\}$.

Q6

Any polynomial $a(x) = a_0 + a_1 x + \cdots + a_n x^n$ can be produced by h iff c is invertible by setting the input to $a_0 + c^{-1} a_1 x + \cdots + c^{-n} a_n x^n$. Then the output of h on this value will produce $a(x)$. Thus h is an automorphism in this case.

G. Homomorphisms of Polynomial Domains Induced by a Homomorphism of the Ring of Coefficients

Q1

$$\bar{h}(a_0 + a_1 x + \cdots + a_n x^n) = h(a_0) + h(a_1)x + \cdots + h(a_n)x^n$$

$$\begin{aligned} \bar{h}(a(x)+b(x)) &= \bar{h}((a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_n + b_n)x^n) \\ &= h(a_0 + b_0) + h(a_1 + b_1)x + \cdots + h(a_n + b_n)x^n \\ &= (h(a_0) + h(b_0)) + (h(a_1) + h(b_1))x + \cdots + (h(a_n) + h(b_n))x^n \\ &= \bar{h}(a(x)) + \bar{h}(b(x)) \end{aligned}$$

$$\begin{aligned} \bar{h}(a(x)b(x)) &= \bar{h}(a_0 b_0 + a_0 b_1 x + \cdots + a_n b_n x^{2n}) = h(a_0 b_0) + h(a_0 b_1)x + \cdots + h(a_n b_n)x^{2n} \\ &= h(a_0)h(b_0) + h(a_0)h(b_1)x + \cdots + h(a_n)h(b_n)x^{2n} \\ &= \bar{h}(a(x))\bar{h}(b(x)) \end{aligned}$$

Q2

$$\forall a_i : 0 \leq i \leq n, a_i \in \ker h$$
$$a(x) = a_0 + \cdots + a_n x^n$$

Q3

If h is surjective, then every element of B is of the form $h(a)$ for some a in A. Thus, any polynomial with coefficients in B is of the form $h(a_0) + h(a_1)x + \cdots + h(a_n)x^n = \bar{h}(a_0 + a_1 x + \cdots + a_n x^n)$.

Q4

Every coefficient of $A[x]$ maps to a distinct coefficient in $B[x]$ because h is an injective function.

Q5

$$b(x) = q(x)a(x)$$
$$\bar{h}(b(x)) = \bar{h}(q(x))\bar{h}(a(x))$$

Q6

Every coefficient $a_i = qn$ and so $h(a_i) = 0$ because $n \mid a_i$. Thus $\bar{h}(a(x)) = 0$.

Q7

$\mathbb{Z}_n$ where n is prime, means the domain of $\bar{h}$ is an integral domain.

$$\bar{h} : \mathbb{Z}[x] \underset{\ker \bar{h}}{\twoheadrightarrow} \mathbb{Z}_n[x]$$

From 19F2, J is a prime ideal iff A/J is an integral domain. So in our case this means $\ker \bar{h}$ is a prime ideal.

An ideal J of a commutative ring is said to be a prime ideal if for any two elements a and b in the ring,

$$\text{If } ab \in J \text{ then } a \in J \text{ or } b \in J$$

$$a(x)b(x) \in \ker \bar{h} \implies a(x) \text{ or } b(x) \in \ker \bar{h}$$

H. Polynomials in Several Variables

Q1

*Prove A is an integral domain $\implies$ $A[x]$ is an integral domain.$

Given any $A_i[x_{i+1}]$ is an integral domain, we know that the leading term $a_k \neq 0$ (which includes the other non-zero x values), multiplied by another $b_l \neq 0$, and so $a_k b_l \neq 0$ and therefore $A_i[x_{i+1}]$ has a non-zero coefficient.

Q2

Degree of $p(x, y)$ is the greatest n such that the coefficient a_n is non-zero for the powers $x^i y^j$ such that $i + j = n$.

$$0, 1, 2$$
$$x, x + 1, x + 2$$
$$2x, 2x + 1, 2x + 2$$
$$x^2, x^2 + 1, x^2 + 2$$
$$x^2 + x, x^2 + x + 1, x^2 + x + 2$$
$$\cdots$$
$$2x^3 + 2x^2 + 2x, 2x^3 + 2x^2 + 2x + 1, 2x^3 + 2x^2 + 2x + 2$$

Q3

$$\begin{aligned} a(x,y)+b(x,y) &= (a_{0,0}+b_{0,0})+(a_{1,0}+b_{1,0})x+\cdots+(a_{n,0}+b_{n,0})x^n \\ &\quad+(a_{0,1}+b_{0,1})y+(a_{1,1}+b_{1,1})xy+\cdots+(a_{n,1}+b_{n,1})x^n y+\cdots \\ &\quad+(a_{0,n}+b_{0,n})y^n+(a_{1,n}+b_{1,n})xy^n+\cdots+(a_{n,n}+b_{n,n})x^n y^n \\ &= \sum_{i=0}^{n}\sum_{j=0}^{n}(a_{i,j}+b_{i,j})x^i y^j \end{aligned}$$

$$\begin{aligned} a(x,y)b(x,y) = a_{0,0}b_{0,0} &+ (a_{0,0}b_{1,0}+a_{0,1}b_{0,0})x \\ &+ (a_{0,0}b_{2,0}+a_{1,0}b_{1,0}+a_{2,0}b_{0,0})x^2+\cdots+a_{n,0}b_{n,0}x^{2n} \\ &+ (a_{0,1}b_{1,0}+a_{1,1}b_{0,0}+a_{0,0}b_{1,1}+a_{1,0}b_{0,1})xy \\ &+ (a_{0,1}b_{2,0}+a_{0,0}b_{2,1}+a_{1,1}b_{1,0}+a_{1,0}b_{1,1}+a_{2,1}b_{0,0}+a_{2,0}b_{0,1})x^2y \\ &+\cdots+a_{n,n}b_{n,n}x^{2n}y^{2n} \qquad = (c_{0,0}+c_{1,0}x+\cdots+c_{2n,0}x^{2n}) \\ &+ c_{0,1}y+c_{1,1}xy+\cdots+c_{2n,1}x^{2n}y \\ &+\cdots+c_{0,2n}y^{2n}+c_{1,2n}xy^{2n}+\cdots+c_{2n,2n}x^{2n}y^{2n} \\ = &\sum_{i=0}^{2n}\sum_{j=0}^{2n}c_{i,j}x^i y^j \end{aligned}$$

$$c_{k,l} = \sum_{i_x+j_x=k,\ i_y+j_y=l} a_{i_x,i_y}b_{j_x,j_y}$$

Q4

If there are two or more terms with the same degree, we ignore them since they do not cancel. For example xy and y^2.

The coefficient for the leading term is of the form

$$a_{m,s}b_{n,t} \text{ for } a(x,y)b(x,y)$$

Thus $\deg a(x,y)b(x,y) = (m+n)+(s+t)$

$$\deg a(x,y)b(x,y) = \deg a(x,y) + \deg b(x,y)$$

I. Fields of Polynomial Quotients

Q1

A is a finite integral domain means it is a field with $\text{char}(A)$ for 1_A. The unity for $A(x)$ is $[1_A, 1_A]$ and $[a,b]+[c,d]=[ad+bc,bd]$.

$$[1_A,1_A]+[1_A,1_A]=[2_A,1_A]$$
$$[k_A,1_A]+[1_A,1_A]=[k_A+1_A,1_A]$$

$$\begin{aligned} \underbrace{[1_A,1_A]+\cdots+[1_A,1_A]}_{\text{char}(A)} &= [\text{char}(A),1_A] \\ &= [0_A,1_A] \end{aligned}$$

Q2

$\mathbb{Z}_p$ is a finite field with characteristic p. Therefore the field of quotients $\mathbb{Z}_p(x)$ will have characteristic p yet it is infinite because terms have any positive integer value (and indeed negative since $\mathbb{Z}_p$ has inverses because it is a field).

Q3

$$
\begin{aligned}
\bar{h}\left(\frac{a(x)}{s(x)}\right) &= \bar{h}\left(\frac{a_0 + \cdots + a_n x^n}{s_0 + \cdots + s_n x^n}\right) \\
&= \frac{h(a_0) + \cdots + h(a_n)x^n}{h(s_0) + \cdots + h(s_n)x^n}
\end{aligned}
$$

Because h is isomorphic, each element of $B(x)$ is the image of no more than one element of $A(x)$, so $\bar{h}$ is injective.

Likewise every element of $B(x)$ is the image of an element in $A(x)$, so $\bar{h}$ is surjective.

$\therefore \bar{h}$ is an isomorphism.

J. Division Algorithm: Uniqueness of Quotient and Remainder

In the division algorithm, prove that $q(x)$ and $r(x)$ are uniquely determined. [HINT: Suppose $a(x) = b(x)q_1(x) + r_1(x) = b(x)q_2(x) + r_2(x)$, and subtract these two expressions, which are both equal to $a(x)$.]

$$0 = b(x)(q_1(x) - q_2(x)) + (r_1(x) - r_2(x))$$

Assume $\deg b(x) > 0$.

If $q_1(x) \neq q_2(x)$, then $\deg[q_1(x) - q_2(x)] > 0$ so $\deg[b(x)(q_1(x) - q_2(x)] > 0$.

But the entire expression is 0 and so its degree is zero. Hence $b(x)(q_1(x) - q_2(x))$ cannot have a degree higher than 0 so the term can only equal 0, which means $q_1(x) = q_2(x)$ since $b(x) \neq 0$.

$$\implies r_1(x) - r_2(x) = 0$$