Anillos de Polinomios

Capítulo 24

A. Computaciones Elementales en Dominios de Polinomios

Para ahorrar notación, denotamos las clases de equivalencia $\bar{n}$ como n.

a) $a(x) + b(x) = (2x^2 + 3x + 1) + (x^3 + 5x^2 + x) = x^3 + 7x^2 + 4x + 1$

$$\begin{aligned} \mathbb{Z}[x]: &\quad x^3 + 7x^2 + 4x + 1 \\ \mathbb{Z}_5[x]: &\quad x^3 + 2x^2 + 4x + 1 \\ \mathbb{Z}_6[x]: &\quad x^3 + x^2 + 4x + 1 \\ \mathbb{Z}_7[x]: &\quad x^3 + 4x + 1 \end{aligned}$$

b) $a(x) - b(x) = (2x^2 + 3x + 1) - (x^3 + 5x^2 + x) = -x^3 - 3x^2 + 2x + 1$, esto se cumple en todos los anillos dados.

c) $a(x)b(x) = (2x^2 + 3x + 1)(x^2 + 5x^2 + x) = 2x^5 + 13x^4 + 18x^3 + 8x^2 + x$

$$\begin{aligned} \mathbb{Z}[x]: &\quad 2x^5 + 13x^4 + 18x^3 + 8x^2 + x \\ \mathbb{Z}_5[x]: &\quad 2x^5 + 3x^4 + 3x^3 + 3x^2 + x \\ \mathbb{Z}_6[x]: &\quad 2x^5 + x^4 + 2x^2 + x \\ \mathbb{Z}_7[x]: &\quad 2x^5 + 6x^4 + 4x^3 + x^2 + x \end{aligned}$$

2.

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

3.

$$\mathbb{Z}[x]: \quad x^3 + 2 = (2x^2 + 3x + 4)(\frac{x}{2} - \frac{3}{4}) + (\frac{x}{4} + 5)$$

El problema aquí es que se está dividiendo por un polinomio que no es mónico
por lo que toca multiplicar por 4 para tener una expresión bien definida

$$\mathbb{Z}_3[X]: \quad x^3 + 2 = (2x^2 + 3x + 4)(2x) + (x + 2)$$

Se tiene que $\mathbb{Z}_3$ sí es un campo. Hay que encontrar el inverso de 2 en este
anillo para que al restar quede un polinomio mónico.

$$\mathbb{Z}_5[x]: \quad x^3 + 2 = (2x^2 + 3x + 4)(3x + 3) + 4x$$

4. Sea k par. Vamos a probar por inducción.

a)

Sea $k = 2$:

$$x^2 + 1 = x(x + 1) + (-x + 1)$$

Supongamos que se cumple para $k = 2(n - 1)$:

$$x^{2(n-1)} + 1 = (x + 1)q(x)$$

Sea $k = 2n$:
$$\begin{aligned} x^{2n} + 1 - x^{2n-1}(x+1) &= -x^{2n-1} + 1 \\ -x^{2n-1} + 1 - (-x^{2n-2})(x+1) &= x^{2(n-1)} + 1 \end{aligned}$$
Por hipótesis inductiva se tiene que $x^{2(n-1)} + 1$ es múltiplo de $(x+1)$, por lo que:

$$x^{2n} + 1 = (x^{2n-1} + x^{2n-2})(x-1) + (x-1)q(x) = (x+1)(x^{2n-1} + x^{2n-2} + q(x))$$

$x + 1$ es factor de $x^n + 1$ para todo n par.

b)

Sea $k = 2$:
$$x^2 + x + 1 = x(x+1) + 1$$
Supongamos que se cumple para todo entero menor o igual a $k = 2(n-1)$:

$$x^{2(n-1)} + x^{2(n-1)-1} + \cdots + 1 = (x+1)q(x)$$

Sea $k = 2n$
$$x^{2n} + \cdots + 1 - (x+1)(x^{2n-1}) = x^{2n-3} + \cdots + 1$$
Por hipótesis inductiva, $x^{2n-3} + \cdots + 1$ es múltiplo de $(x+1)$, entonces:

$$x^{2n} + \cdots + 1 = (x+1)q_0(x) + (x+1)(x^{2n-1}) = (x+1)(q_0(x) + x^{2n-1})$$

5.

a) Es trivial para $k = 1$. Supongamos q

6.
$$(3x^2 + 4x + m)(ax^2 + bx + c) = 3ax^4 + 3bx^3 + 4ax^3 + 4bx^2 + 4cx + amx^2 + bmx + cm = 6x^4 + 50$$
Igualando coeficientes:
$$\begin{aligned} &3a = 6 \\ &3b + 4a = 0 \\ &3c + 4b + am = 0 \\ &5c + bm = 0 \\ &cm = 50 \end{aligned}$$
Con estas ecuaciones vemos que $b = -8/3$, pero esto no puede ser. ya que estamos en $\mathbb{Z}[x]$

7.
$$\begin{aligned} (x^2+1)(x^3 + ax^2 + bx + c) &= x^5 + ax^4 + bx^3 + cx^2 + x^3 + ax^2 + bx + c \\ &= x^5 + ax^4 + (b+1)x^3 + (a+c)x^2 + bx + c \\ &= x^5 + 5x + 6 \end{aligned}$$
Igualando clases de congruencia:
$$\begin{aligned} &a \equiv 0 \pmod{n} \\ &(b+1) \equiv 0 \pmod{n} \\ &a + c \equiv 0 \pmod{n} \\ &b \equiv 5 \pmod{n} \\ &c \equiv 6 \pmod{n} \end{aligned}$$
De la segunda ecuación se obtiene que $b + 1 \equiv 5 + 1 \equiv 0 \pmod{n}$. Por lo que $n = 2, 3, 6$, viendo las demás ecuaciones, se puede apreciar que ningún valor arroja una contradicción.

B. Problemas Involviendo Conceptos y Definiciones

1. $x^8 + 1 = x^3 + 1 \iff x^8 = x^3 \iff x^3(x^5 - 1) = 0$

Las soluciones a esta ecuación son $x = 0, 1$. Entonces, los polinomios no son iguales, ya que tendrían que ser equivalentes para los valores $x = 2, 3, 4$ también.

2.

3. Los polinomios de grado 2 o menor en $\mathbb{Z}_5[x]$ son:

$$a_2x^2 + a_1x + a_0 \text{ para } a_i \in \{0, 1, 2, 3, 4\}$$

De estos, hay $5^3 = 125$ polinomios distintos. Los polinomios de grado 1 o 0 en $\mathbb{Z}_5[x]$ son:

$$b_1x + b_0 \text{ para} b_i \in \{0, 1, 2, 3, 4\}$$

De estos hay $5^2 = 25$ elementos distintos. Luego la cantidad de polinomios cuadráticos son: $5^3-5^2 = 125-25 = 100$.

Para el caso general, los polinomios de grado m o menos son de la forma:

$$a_nx^n + a_{n-1}x^{n-1} + \cdots + a_0$$

cada coeficiente es del conjunto $\{0, 1, \ldots, n - 1\}$. Entonces la cantidad de polinomios diferentes es m^n. El mismo argumento dice que hay m^{n-1} polinomios distintos de grado $m - 1$ o menor. Entonces, la cantidad de polinomios de grado m es: $m^n - m^{n-1}$.

4. Sea A dominio entero.

a) $(x + 1)^2 = x^2 + 2x + 1 = x^2 + 1 \implies 2x = 0 \iff \text{char } A = 2$

b) $(x + 1)^4 = x^4 + 4x^3 + 6x^2 + 4x + 1 = x^4 + 1 \implies 2(2x^3 + 3x^2 + 2x) = 0 \iff \text{char } A = 2$

c) $(x + 1)^6 = x^6 + 6x^5 + 15x^4 + 20x^3 + 15x^2 + 6x + 1 = x^6 + 2x^3 + 1 \implies 3(2x^5 + 5x^4 + 6x^3 + 5x^2 + 2x) \iff \text{char } A = 3$

5.

a) $(ax + b)(cx + d) = acx^2 + (ad + bc)x + bd$

Entonces podemos pedir que los coeficientes cumplan que,

$ac \equiv 0 \pmod 8$

$ad + bc \equiv 0 \pmod 8$

$bd \equiv 0 \pmod 8$

Las ecuaciones se pueden realizar pidiendo que ningún coeficiente sea nulo, una solución sería: $a = b = 1$ y $c = d = 8$. Entonces $(x + 1)(8x + 8) = 8x^4 + 16x + 8 = 0$. Otras soluciones se ven bajo factorización.

b) $(ax + 1)(bx + 1) = abx^2 + (a + b)x + 1$

$ab \equiv 0 \pmod 8$

$a + b \equiv 0 \pmod 8$

Podemos pedir que $a \equiv -b \pmod 8 \implies b^2 \equiv 0 \pmod 8 \implies b \equiv 4 \pmod 8$. Reemplazando, obtenemos que $a \equiv 4 \pmod 8$. Es $(4x + 1)(4x + 1) = 16x^2 + 8x + 1 = 1$.

6. Supongamos que x es invertible en $A[x]$, entonces existe $p(x)$ de grado n tal que $xp(x) = 1$, entonces $\deg xp(x) = \deg 1 = \deg x + \deg p(x) = 1+n = 0$, pero esto significa que $n = -1$, pero por definición, el grado siempre es positivo.

7.

D. Dominios $A[x]$ Donde A Posee Característica Finita

1. Para un polinomio $a(x) = \sum_{i=0}^{n} a_ix^i$, cada $a_i \in \{0, \ldots, n\}$ pertenece a A, por lo que posee característica p,

por lo que la característica se preserva ya que $p \cdot a_i = 0$.

2. Un ejemplo de un dominio entero infinito con característica finita es Z_n, en donde en este anillo es miembro x^i para todo $i \in \mathbb{N}$.

3. Ver el ejercicio A5, es una generalización de este ejercicio.

4. Por el teorema del binomio:

$$(x+c)^p = \sum_{k=0}^{p} \binom{p}{k} x^k c^{p-k}$$

Se tiene que $\binom{p}{k} = \frac{p(p-1)(p-2)\ldots(p-k+1)}{k!}$, es decir, cada término es múltiplo de p, por lo que cada término se cancela al tener un anillo característica p, excepto el primer y último término. Entonces $(x+c)^p = x^p + c^p$.

6.

$$(a(x)+b(x))^p = \sum_{k=0}^{p} \binom{p}{k} a^k(x) b^{p-k}(x)$$

Se tiene el mismo argumento de antes, como A posee características p se anula cada coeficiente menos el primer y último coeficiente. Luego:

$$\begin{aligned}(a_0 + a_1x + \cdots + a_nx^n)^p &= a_0^p + (a_1x + \cdots + a_nx^n)^p \\ &= a_0^p + a_1^px^p + (a_2x^2 + \cdots + a_nx^n)^p\end{aligned}$$

Repitiendo este proceso inductivamente se tiene que:

$$(a_0 + a_1x + \cdots + a_nx^n)^p = a_0^p + a_1^px^p + \cdots + a_n^px^{np}$$

E. Subanillos e Ideales en A[x]

1. Mostrar que si B es un subanillo de A, entonces $B[x]$ es un subanillo de $A[x]$

Sean $b_1(x) = \sum_{i=0}^{n} b_{1,i}x^i$ y $b_2(x) = \sum_{j=0}^{n} b_{2,j}x_j$. La suma y la multiplicación se definen como:

$$\begin{aligned}a.\quad b_1(x) + b_2(x) &= \sum_{k=0}^{n} (b_{1,k} + b_{2,k})x^k \\ b.\quad b_1(x)b_2(x) &= \sum_{k=0}^{2n} \left(\sum_{i+j=k} b_{1,i}b_{2,j} \right) x^k\end{aligned}$$

Luego, la suma y multiplicación de elementos en B es cerrada en B, por que la operación en el anillo de polinomios es cerrada.

2. Sea $a(x) = \sum_{i=0}^{n} a_ix^i$ con $a_i \in A$ y $b(x) = \sum_{j=0}^{m} b_jx^j$ con $b_j \in B$:

$$a(x)b(x) = \sum_{k=0}^{n+m} \left(\sum_{i+j=k} a_ib_j \right) x^k$$

Como $\sum_{i+j=k} a_ib_j \in B$ al ser B ideal, entonces $a(x)b(x) \in B[x]$

3. Sea $S = \{\sum_{i=0}^{n} a_ix_i \in A[x] \mid a_i = 0 \quad \forall i \equiv 1 \pmod 2\}$

Sean $p(x) = \sum_{k=0}^{n} a_k x^k$ y $q(x) = \sum_{l=0}^{n} b_l x^l$

$$a. \quad p(x) + q(x) = \sum_{j=0}^{n} (a_i + b_i) x^i$$

$$b. \quad p(x)q(x) = \sum_{k=0}^{2n} \left(\sum_{i+j=k} a_i b_i \right) x_k$$

Para la suma ambos coefientes no son nulos cuando i es par. Para la multiplicación la suma de los multiplicación de coeficientes no es cero cuando $i + j = k$ par, esto solo pasa cuando i y j son pares a la vez. La condición no se cumple para indices impares, ya que en la multiplicación la suma de impares da par, por lo que se sale del conjunto.

4. $J = \{\sum_{i=0}^{n} a_i x^i \in A[x] \mid a_0 = 0\}$. Sea $a(x) = a_1 x + a_2 x^2 + \cdots + a_n x^n \in J$ y $b(x) = b_0 + b_1 x + \cdots + b_n x^n$. $a(x)b(x) = a_1 x(b_0 + b_1 x + \cdots + b_n x^n) + \cdots + a_n x^n (b_0 + b_1 x + \cdots + b_n x^n)$. Por lo que $\deg a(x)b(x) \geq 1$

5. Sea $a(x) = a_0 + a_1 x + \cdots + a_n x^n \in J$ y $b(x) = b_0 + b_1 x + \cdots + b_n x^n \in A[x]$. Luego $a(x)b(x) = a_0(b_0 + b_1 x + \cdots + b_n x^n) + a_1 x(b_0 + b_1 x + \cdots + b_n x^n) + \cdots + a_n x^n (b_0 + b_1 x + \cdots + b_n x^n)$. Entonces $(a_0 + \cdots + a_n)(b_0 + \cdots + b_n) = 0$. La implicancia sigue.

6.- $A[x]/J$ dominio entero.

F. Homomorfismos de Dominios de Polinomios

Sea A un dominio integral.

1. Sean $a(x) = \sum_{i=0}^{n} a_i x^i$ y $b(x) = \sum_{j=0}^{m} b_j x^j$ con $n \leq m$, tiene que:

$$a. \quad h\left(a(x) + b(x)\right) = h\left(\sum_{i=0}^{n} a_i x^i + \sum_{j=0}^{m} b_j x^j \right) = h\left(\sum_{k=0}^{n} (a_k + b_k x^k) + \sum_{k=n+1}^{m} b_k x^k \right) = a_0 + b_0 = h\left(\sum_{i=0}^{n} a_i x^i \right) + h\left(\sum_{j=0}^{m} b_j x^j \right)$$

$$b. \quad h\left(\sum_{k=0}^{n+m} \left(\sum_{i+j=k} a_i b_j \right) x^k \right) = a_0 b_0 = h\left(\sum_{i=0}^{n} a_i x^i \right) h\left(\sum_{j=0}^{m} b_j x^j \right)$$

Kernel:

$$\begin{aligned}
&\ker h = \{a(x) \in A[x] \mid h(a(x)) = 0\} \\
&\iff h\left(\sum_{k=0}^{n} a_k x^k \right) = 0 \\
&\iff a_0 = 0 \\
&\iff a(x) = a_1 x + \cdots + a_n x^n \\
&\iff xR(x) \quad ; R(x) \in A[x]
\end{aligned}$$

Sobreyectividad:

Se tiene que para $a \in A$ se puede definir el polinomio constante $a(x) = a \in A[x]$ tal que $h(a(x)) = h(a) = a$

2. Por punto anterior el kernel es de la forma $xq(x)$ con $q(x) \in A[x]$, es decir $xq(x) \in (x)$

3. Usando el primer teorema del isomorfismo se tiene que existe una biyección φ entre el espacio cocientado por el kernel y la imagen. Se tiene que la imagen es todo A (argumento de sobreyectividad). Luego $A[x]/(x) \xrightarrow{\varphi} A$

4. Sean $a(x) = \sum_{i=0}^{n} a_i x^i$ y $b(x) = \sum_{j=0}^{m} b_j x^j$ tal que $n \leq m$.

Homomorfismo:

$a.$ $g(a(x))+g(b(x))=(a_0+\cdots+a_n)+(b_0+\cdots+b_m)=(a_0+b_0)+(a_1+b_1)+\cdots+(a_n+b_n)+b_{n+1}+\cdots+b_m$

$$= g((a_0+b_0)+(a_1+b_1)x+\cdots+(a_n+b_n)x^n+b_{n+1}x^{n+1}+\cdots+b_m x^m)$$
$$= g(a(x)+b(x))$$

$$b.\quad g(a(x))g(b(x))=\left(\sum_{i=0}^{n}a_ix^i\right)\left(\sum_{j=0}^{m}b_jx^j\right)=\left(\sum_{k=0}^{n+m}\sum_{i+j=k}a_ib_j\right)=g\left(\sum_{k=0}^{n+m}\left(\sum_{i+j=k}a_ib_j\right)x^k\right)=g(a(x)b(x))$$

Sobreyectividad: Para todo $a\in A$ se puede definir el polinomio constante $a(x)=a$ donde $g(a(x))=g(a)=a$

Kernel:

$$\begin{aligned}&\ker g=\{a(x)\in A[x]\mid g(a(x))=0\}\\&\iff g(a_0+a_1x+\cdots+a_nx^n)=0\\&\iff a_0+a_1+\cdots+a_n=0\end{aligned}$$

5.- Sean $a(x)=\sum_{i=0}^{n}a_ix^i$ y $b(x)=\sum_{j=0}^{m}b_jx^j$ tal que $n\leq m$.

Homomorfismo:

$$a.\quad h(a(x)+b(x))=\sum_{k=0}^{n}(a_k+b_k)c^kx^k+\sum_{k=n+1}^{m}b_kc^kx^k=h\left(\sum_{i=0}^{n}a_ix^i\right)+h\left(\sum_{j=0}^{m}b_jx^j\right)=h(a(x))+h(b(x))$$

$$b.\quad h(a(x))h(b(x))=\left(\sum_{i=0}^{n}a_ic^ix^i\right)\left(\sum_{j=0}^{m}b_jc^jx^j\right)=\sum_{k=0}^{n+m}\left(\sum_{i+j=k}a_ib_j\right)c^kx^k=h\left(\sum_{k=0}^{n+m}\left(\sum_{i+j=k}a_ib_j\right)x^k\right)=h(a(x)b(x))$$

Kernel:

$$\begin{aligned}&\ker h=\{a(x)\in A[x]\mid h(a(x))=0\}\\&\iff \sum_{i=0}^{n}a_ic^ix^i=0\\&\iff a_i=0\quad\forall i\in\{1,\ldots,n\}\\&\iff a(x)\equiv 0\end{aligned}$$

6.

$\Longrightarrow$) Sea h un automorfismo, es decir, un isomorfismo entre mismos anillos, en particular se tiene que es una biyección, por lo que $\ker h=(0)\iff a(x)\cong 0$, suponiendo que c no es invertible, entonces $c=0$m por lo que $h(a(x))=a(cx)=a(0)$, por lo que ker contendía los polinomios divisibles por x, contradiciendo la inyectividad.

Por sobreyectividad existe $a\in A[x]$ constante, se puede definir $c^{-1}a$ en donde $c(c^{-1}a)\mapsto a$. Esto solo pasa si c es invertible.

$\Longleftarrow$) Sea c invertible. Como h^{-1} un homomorfismo tal que $\varphi(a(x))=a(c^{-1}x)$ (probar que es homomorfismo es directo). Hay que ver que es isomorfismo y la inversa de h.

$$\ker\varphi=\{a(x)\in A[x]\mid\varphi(a(x))=0\}\iff\sum_{i=0}^{n}a_i(c^{-1})^ix^i=0\iff a_i=0$$

$$\text{Im }\varphi=\{a(x)\in A[x]\mid\varphi(p(x))=a(x)\}\iff\forall a(x)\in A[x],\exists p(x)\in A[x]\text{ con }p(x)=\sum_{i=1}^{n}a_ic^ix^i\iff\text{Im }=A[x]$$

Ver que $\varphi\equiv h^{-1}$ es directo, sea $a(x)=\sum_{i=0}^{n}a_ix^i$

$$\begin{aligned}&\varphi\left(h(a(x))\right)=\varphi\left(\sum_{i=0}^{n}a_ic^ix^i\right)=\sum_{i=0}^{n}a_ix^i=a(x)\\&h\left(\varphi(a(x))\right)=a(x)\end{aligned}$$

Entonces $\varphi \equiv h^{-1}$. Por lo que h automorfismo.

G. Homomorfismos de Dominios Polinomiales inducidos por un Homomorfismos de Anillos de Coeficientes

1. Sean $a(x) = \sum_{i=0}^{n} a_i x^i$ y $b(x) = \sum_{j=0}^{m} b_j x^j$ tal que $n \leq m$.

$$\begin{aligned}
\bar{h}(a(x)) + \bar{h}(b(x)) &= \bar{h}\left(\sum_{i=0}^{n} a_i x^i\right) + \bar{h}\left(\sum_{j=0}^{m} b_j x^j\right) \\
&= \sum_{i=0}^{n} h(a_i)x^i + \sum_{j=0}^{m} h(b_j)x^j \\
&= \sum_{i=0}^{n} h(a_i + b_i)x^i + \sum_{i=n+1}^{m} b_i x^i \\
&= \bar{h}(a(x) + b(x))
\end{aligned}$$

$$\bar{h}(a(x)b(x)) = \bar{h}\left(\sum_{k=0}^{n+m}\left(\sum_{i+j=k} a_i b_j\right) x^k\right) = \sum_{k=0}^{n+m} h\left(\sum_{i+j=k} a_i b_j\right) x^k = \sum_{k=0}^{n+m}\left(\sum_{i+j=k} h(a_i)h(b_j)\right) x^k = \bar{h}(a(x))\bar{h}(b(x))$$

2. Descubrir el kernel de $\bar{h}$

$$\ker \bar{h} = \{a(x) \in A[x] \ \mid \bar{h}(a(x)) = 0\} \Longleftrightarrow \sum_{i=0}^{n} h(a_i)x^i = 0 \Longleftrightarrow h(a_i) = 0 \quad \forall i \in \{1, \ldots, n\} \Longleftrightarrow a_i = 0 \Longleftrightarrow a(x) \equiv 0$$

3.

$\Longrightarrow$) Sea $\bar{h}$ sobreyectivo, entonces para cualquier polinomio $b(x) \in B[x]$ existe $a(x) \in A[x]$ tal que $\bar{h}(a(x)) = b(x)$. Entonces para cualquier polinomio constante $b(x) = b$ existe un polinomio constante $a(x) = a$ tal que $\bar{h}(a) = b$. Por lo que h sobreyectivo.

$\Longleftarrow$) Sea $\bar{h}$ sobreyectivo, entonces siempre puedo encontrar $a(x) \in A[x]$ para $b(x) \in B[x]$, donde $\bar{h}\left(\sum_{i=0}^{n} a_i x^i\right) = \sum_{j=0}^{n} b_j x^j$, dado que $h(a_i) = b_j$ por sobreyectividad.

4-

$\Longrightarrow$) Supongamos que $\bar{h}$ es inyectivo. Supongamos que $a \in \ker h$, entonces considerando el polinomio constante $a(x) = a$, se tiene que $\bar{h}(a(x)) = h(a) = 0$, como $\bar{h}$ es inyectivo, esto implica que $a(x) = 0$, es decir $a = 0$, por lo que h es inyectivo. ($\ker h = (0)$)

$\Longleftarrow$) Supongamos que h es inyectivo. Sea $a(x) = \sum_{i=0}^{n} a_i x^i \in \ker \bar{h}$. Por definición se tiene que:

$$\bar{h}\left(\sum_{i=0}^{n} a_i x^i\right) = \sum_{i=0}^{n} h(a_i)x^i$$

Esto implica que $h(a_i) = 0$ para todo i, como h es inyectivo, esto implica que $a_i = 0$, es decir $a(x) = 0$, por lo que $\ker \bar{h} = (0)$

5.-
Si $a(x)$ es factor de $b(x)$, entonces $b(x) = a(x)q(x)$ con $q(x) \in A[x]$, aplicando el mapeo se tiene que:

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

6.-
Si $h : \mathbb{Z} \to \mathbb{Z}_n$ es el homomorfismo natural, se tiene que:

$$\ker \bar{h} = \{a(x) \in \mathbb{Z}_n[x] \mid a(\bar{x}) = 0\} \iff \bar{h}\left(\sum_{i=0}^{n} a_i x^i\right) = \sum_{i=0}^{n} h(a_i)x^i = 0 \iff h(a_i) = \bar{0} \iff \bar{a_i} \equiv 0\ (n) \iff n \mid a_i$$

(Aparte, $\ker \bar{h} = n\mathbb{Z}$)

7.
Sea $\bar{h} : \mathbb{Z} \to \mathbb{Z}_n[x]$, se tiene que $\ker \bar{h} = n\mathbb{Z}[x]$. Como $a(x)b(x) \in n\mathbb{Z}[x]$, se cumple que $n \mid a(x)b(x)$. Entonces, $n \mid a(x)$ o $n \mid b(x)$, ya que n es primo.

H. Polinomios en Varias Variables

1.- Vamos a demostrar por inducción.

Sea $k = 1$. Entonces hay que mostrar que $A[x_1]$ es dominio integral, sean $a(x)$ y $b(x)$ polinomios no nulos, debemos mostrar que $a(x)b(x)$ no es nulo. Sea a_n el coeficiente principal de $a(x)$ y b_m el coeficiente principal de $b(x)$. Por definición $a_n \neq 0 \neq b_m$. Entonces $a_n b_n \neq 0$ por que A es dominio entero. Sigue que $a(x)b(x)$ posee almenos un coeficiente no nulo. Entonces no es el polinomio nulo

Supogamos que se cumple para $k = n - 1$ ($A[x_1, \dots, x_{i-2}]$ dominio entero, entonces $A[x_1, \dots, x_{o-1}]$ es dominio entero)

Sea $k = n$. Sean $a(x_1, \dots, x_n)$ y $b(x_1, \dots, x_n)$ polinomios en n variables no nulos. Por hipótesis se tiene que $A[x_1, \dots, x_{n-1}]$ es dominio integral. Sean $a(x_1, \dots, x_n) = \sum_{i=0}^{m_1} p_i(x_1, \dots, x_n)x_n^i$ y $b(x_1, \dots, x_n) = \sum_{j_0}^{m_2} q_j(x_1, \dots, x_{n-1})x_n^j$. Hay que mostrar que $a(x)b(x) \neq 0$.

$$a(x)b(x) = \sum_{k=0}^{m_1+m_2} \left(\sum_{i+j=k} p_i q_j(x_1, \dots, x_{n-1})\right) x_n^k$$

Si $p_i(x_1, \dots, x_{n-1}) \neq 0 \neq q_j(x_1, \dots, x_{n-1})$, entonces $a(x)b(x)$ no es nulo ya que hay unos i, j tal que $p_i(x_1, \dots, x_{n-1})q_j(x_1, \dots, x_{n-1}) \neq 0$.

2.
a) Sea $p(x, y) = \sum_{(i,j)\in\mathbb{N}^2} a_{i,j}x^i y^j$ con $a_{i,j} \in A$. El grado de $p(x, y)$ se define como:

$$\deg(p(x, y)) = \max\{i + j \mid a_{i,j} \neq 0\}$$

b) Se tiene que todos los polinomios de grado ≤ 3 en $\mathbb{Z}_3[x, y]$ son combinaciones lineales de $\{1, x, y, x^2, xy, y^2, x^3, x^2y, xy^2, y^3\}$

3. Sea $p(x, y) = \sum_{(i,j)\in\mathbb{N}^2} a_{i,j}x^i y^j$ y $q(x, y) = \sum_{(i,j)\in\mathbb{N}^2} b_{(i,j)x^i y^j}$. La suma se puede definir como:

$$p(x, y) + q(x, y) = \sum_{(i,j)\in\mathbb{N}^2} (a_{i,j} + b_{i,j})x^i y^j$$

$$\text{Sean } p(x, y) = \sum_{(i,j)\in\mathbb{N}^2} a_{i,j}x^i y^j \quad \text{y} \quad q(x, y) = \sum_{(k,\ell)\in\mathbb{N}^2} b_{k,\ell}x^k y^\ell,$$

donde $a_{i,j}, b_{k,\ell} \neq 0$ solo para un número finito de pares (i, j) y (k, ℓ).
La multiplicación de $p(x, y)$ y $q(x, y)$ está definida como:

$$p(x, y) \cdot q(x, y) = \sum_{(m,n)\in\mathbb{N}^2} \left(\sum_{\substack{(i,j),(k,\ell)\in\mathbb{N}^2 \\ i+k=m,\, j+\ell=n}} a_{i,j} b_{k,\ell} \right) x^m y^n.$$

I. Cuerpos de Cocientes de Polinomios

3.
a) Sea $a(x) \in \ker \bar{h} = \{p(x) \in A(x) \mid \bar{h}(p(x)) = 0\}$, sea tal que:

$$\bar{h}\left(\sum_{k=0}^{n} a_k x^k\right) = \sum_{k=0}^{n} h(a_k)x^k = 0 \Longleftrightarrow h(a_k) = 0$$

Como h es isomorfismo, entonces $h(a_k)$ si y solo si $a_k = 0 \quad \forall k \in \{i, \ldots, n\}$, es decir $a(x) \equiv 0$. $\ker \bar{h} = (0)$

b) Sea $b(x) = \sum_{k=0}^{n} b_k x^k$, como h es un isomorfismo, existe a_k tal que $h(a_k) = b_k$ para todo k. Equivalente a decir que existe siempre $a(x)$ tal que $b(x) = \bar{h}(a_k)$.

J. Algoritmo de División: Unicidad del Cuociente y del Resto

Suponer que $a(x) = b(x)q_1(x) + r_1(x) = b(x)q_2(x) + r_2(x)$. Entonces $b(x)(q_1(x) - q_2(x)) + (r_1(x) - r_2(x)) = 0$m esta expresión la reduciré a $b(x)q(x) + r(x) = 0$, donde $\deg b(x) > \deg r(x)$, esto es equivalente a que $\deg b(x) > \deg r_1(x)$, $\deg r_2(x)$. A su ves se tiene que $b(x)q(x)$ es múltiplo de $b(x)$. Suponiendo que $q(x) \neq 0$, se tiene que $\deg b(x)q(x) \geq \deg b(x)$. Esto quiere decir que $\deg r(x) > \deg b(x)$. Esto es una contradicción.