Capítulo 24

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:

$$a. \quad b_1(x) + b_2(x) = \sum_{k=0}^{n} (b_{1,k} + b_{2,k})x^k$$

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

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

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

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

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

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:

$$\begin{aligned}&\ker h=\{a(x)\in A[x]\mid h(a(x))=0\}\\ &\iff h\left(\sum_{k=0}^{n} a_k x^k\right)=0\\ &\iff a_0=0\\ &\iff a(x)=a_1x+\cdots+a_nx^n\\ &\iff xR(x)\quad ;\, R(x)\in A[x]\end{aligned}$$

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:

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

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

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

Homomorfismo:

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

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

Kernel:

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

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.

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

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

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

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

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:

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

(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 $k = n - 1$ ($A[x_1, \ldots, x_{i-2}]$ dominio entero, entonces $A[x_1, \ldots, x_{o-1}]$ 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 $p(x,y) = \sum_{(i,j)\in\mathbb{N}^2} a_{i,j}x^iy^j$ 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 $p(x,y) = \sum_{(i,j)\in\mathbb{N}^2} a_{i,j}x^iy^j$ y $q(x,y) = \sum_{(i,j)\in\mathbb{N}^2} b_{(i,j)x^iy^j}$. La suma se puede definir como:

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

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

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:

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

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:

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

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

b) Sea $b(x) = \sum_{k=0}^{n} b_kx^k$, 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.