D. Ideales en Dominios de Polinomios

Sea F un campo y sea J cualquier ideal de $F[x]$

1. Sean $p(x)$ y $q(x)$ generadores de J. Es decir $p(x)$ es múltplo de $q(x)$ y viceversa. Esto es equivalente a decir:

$$p(x) = q(x)a(x) \quad q(x) = p(x)b(x)$$

Juntanto las ecuaciones llegamos a que $p(x) = p(x)a(x)b(x) \iff a(x)b(x) = 1 \iff a(x)$ y $b(x)$ son constantes. Es decir $p(x)$ y $q(x)$ son asociados.

2.
$\Longleftarrow$) Trivial

$\Longrightarrow$) Por definición J consiste de todos los elementos de la forma $m(x)p(x)$ con $p(x)$ variable. Entonces $a(x) = m(x)p(x)$ si y solo si $m(x) \mid a(x)$

3.
$\Longrightarrow$) Supongamos que posee como generador $p(x)$ tal que $p(x) = a(x)b(x)$, entonces $a(x) \in J$ o $b(x) \in J$, entonces $a(x)$ es generador (sin pérdida de generalidad), si $a(x)$ es reducible volvemos a argumentar de la misma forma, este profeso es finito hasta llegar a un elemento irreducible en $F[x]$.

$\Longleftarrow$) J posee un generador irreducible, sease $p(x)$. Sea $a(x)b(x) \in J$, entonces $p(x) \mid a(x)b(x)$, o equivalentemente, $p(x) \mid a(x)$ o $p(x) \mid b(x)$. J primo por definición.

4. Supongamos que $(p(x)) \subset I$, donde I es otro ideal, sea un $a(x) \in I - (p(x))$, por lo que $a(x) \neq p(x)q(x)$, es decir $a(x)$ y $p(x)$ son coprimos, entonces existe una combinación lineal tal que $1 = r(x)a(x) + s(x)p(x)$, a su vez se tiene que $p(x) \in I$, por lo que $r(x)a(x) + s(x)p(x) \in I$ o que $1 \in I$. Pero entonces $I = F[x]$.

5. $S = \{p(x) \in F[x] \mid \sum_{i=0}^{n} a_i x i$ tal que $\sum_{i=0}^{n} a_i = 0\}$. Directamente $x - 1 \in S$ y es un polinomio irreducible, por lo que $S = (x - 1)$.

6. Existe una biyección $\varphi : F[x]/(x - 1) \to F \ (x \rightsquigarrow 1)$

E. Demostración del Teorema de Factorización Única

1. Probar el Lema de Euclides para polinomios.

Sea $p(x)$ irreducible tal que $p(x) \mid a(x)b(x)$. Si $p(x) \mid a(x)$ estamos listos. Entonces supogamos que no es el caso. Los únicos divisores comúnes de $p(x)$ y $a(x)$ son ± 1. Sigue que

$$\gcd(p(x), a(x)) = 1$$

Esto es equivalente a:

$$r(x)p(x) + s(x)a(x) = 1$$
$$r(x)p(x)b(x) + s(x)a(x)b(x) = b(x)$$

como $p(x) \mid a(x)b(x)$ hay $t(x)$ donde:

$$r(x)p(x)b(x) + s(x)t(x)p(x) = b(x)$$

Es decir $p(x)\left(r(x)b(x) + s(x)t(x)\right) = b(x)$. Sigue que $p(x) \mid b(x)$.

2. Probar los dos corolarios del lema de Euclides.

Cor1) Sean $m_1(x), \ldots, m_n(x)$ polinomios y sea $p(x)$ un polinomio irreducible. Si $p(x) \mid (m_1(x) \ldots m_n(x))$, entonces $p(x) \mid m_i(x)$ para algún $i \in \{1, \ldots, n\}$

Sea $m_1(x)\dots m_n(x)$ denotado como $m_1(x)(m_2\dots m_n(x))$, por el lema de Euclides para polinomios $p(x) \mid m_1(x)$ o $p(x) \mid (m_2(x)\dots m_n(x))$. En el primer caso estamos listos, sino argumentamos por el Lema de Euclides hasta n veces si es necesario.

Cor2) Sean $q_1(x),\dots,q_n(x)$ y $p(x)$ polinomios irreducibles. Si $p(x) \mid (q_1(x)\dots q_n(x))$, entonces $p(x)$ equivale uno de los $q_i(x)$ para algún $i \in \{i,\dots,n\}$

Por corolario anterior, se tiene que $p(x) \mid q_i(x)$ para algún $i \in \{i,\dots,n\}$, como los únicos divisores de $p_i(x)$ son $\pm p_i(x)$ y ± 1 y $p(x) \neq \pm 1$, entonces si $p(x) \mid q_i(x)$, necesariamente $p(x) = q_i(x)$.

F. Un método para calcular el gcd

1.

Sea $d(x) = s(x)a(x) + r$

G. Una Transformación de F[x]

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

$$\begin{aligned}
h(a(x))h(b(x)) &= h\left(a(x) = \sum_{i=0}^{n} a_i x^i\right) h\left(\sum_{j=0}^{m} b_j x^j\right) \\
&= \left(\sum_{i=0}^{n} a_{n-i} x^i\right)\left(\sum_{j=0}^{m} b_{m-j} x^j\right). \\
&= \sum_{k=0}^{n+m}\left(\sum_{i+j=k} a_{n-i} b_{m-j}\right) x^k \\
&= h\left(\sum_{k=0}^{n+m}\left(\sum_{i+j=k} a_i b_j\right) x^k\right) \\
&= h(a(x)b(x))
\end{aligned}$$

2.
Inyectividad: Sea $p(x) \in \ker h$, es decir $h(p(x)) = 0$ donde $h\left(\sum_{i=0}^{n} a_i x^i\right) = \sum_{i=0}^{n} a_{n-i} x^i = 0$ si y solo si $a_{n-i} = 0$ (equiv a $a_i = 0$ en orden), es decir $p(x) \equiv 0$

Sobreyectividad: Para $p(x) = \sum_{i=0}^{n} a_{n-i} x^i$ siempre se puede encontrar $q(x) = \sum_{i=0}^{n} a_i x^i$, donde $h(q(x)) = p(x)$

Sea $p(x) = \sum_{i=0}^{n} a_i x^i$. Luego:

$$h(p(x)) = \sum_{i=0}^{n} a_{n-i} x^i$$

Luego

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

3. Sea $a(x) = a_0 + a_1 x + \cdots + a_n x^n$ irreducible, pero $b(x) = a_n + a_{n-1} x + \cdots + a_0 x^n$ reducible, de modo que:

$$b(x) = c(x)d(x).$$

Entonces:

$$a(x) = h[b(x)] = h[c(x)d(x)] = h[c(x)]h[d(x)].$$

Esto implica que $a(x)$ es, de hecho, reducible, contradiciendo la hipótesis inicial. Por lo tanto, el supuesto de que $b(x)$ es reducible lleva a una contradicción.

4. Sea $a_0+a_1x+\cdots+a_nx^n = (b_0+\cdots+b_mx^m)(c_0+\cdots+c_qx^q)$. Se tiene bajo el mapeo que $h(a_0+a_1x+\cdots+a_nx^n) = h(b_0+\cdots+b_mx^m)h(c_0+\cdots+c_qx^q)$. Entonces,

$$a_n + a_{n-1}x + \cdots + a_0x^n = (b_m + \cdots + b_0x^m)(c_q + \cdots + c_0x^q)$$

Sea $a(c) = 0$, entonces

$$\begin{aligned} & a_0 + a_1c + a_2c^2 + \cdots + a_nc^n = 0 \quad / \quad \frac{1}{c^n} \\ & \frac{a_0}{c^n} + \frac{a_1}{c^{n-1}} + \cdots + a_n = 0 \end{aligned}$$

La implicancia contraria se obtiene ponderando por c^n la ecuación.