Tema 6.-. Anillo de polinomios. División y factorización. Lema de Gauss.

6.1. Anillos de polinomios.

Definición 6.1.1.– Sea A un anillo. El anillo de polinomios en la indeterminada X con coeficientes en A, y que notaremos por $A[X]$, es el conjunto de expresiones formales de la forma

$$f(X) = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_1 X + a_0$$

con cada $a_i \in A$. El elemento a_i se denomina el coeficiente de X^i en $f(X)$, y dos polinomios se consideran iguales si para cada i los coeficientes de X^i son iguales.

Por claridad, eliminamos los coeficientes nulos. El polinomio cero tiene todos sus coeficientes igual a 0, y lo notaremos como 0.
Definición 6.1.2.– El grado de $f(X)$ es el mayor n tal que a_n es no nulo. Si $\text{grado}(f(X)) = n$ escribiremos $f(X) = \sum_{k=0}^{n} a_k X^k$. El coeficiente a_n se denomina coeficiente líder de $f(X)$. Si es igual a 1, decimos que $f(X)$ es un polinomio mónico. Asignamos $\text{grado}(0) = -\infty$, y por conveniencia en el manejo de fórmulas establecemos que $-\infty < n$ y $-\infty + n = -\infty$ para cualquier $n \in \mathbb{Z}^+$.

Se definen dos operaciones en $A[X]$. Sean $f(X) = a_n X^n + \ldots + a_1 X + a_0, g(X) = b_m X^m + \ldots + b_1 X + b_0$.

- Suma. $f(X) + g(X)$ es el polinomio con coeficiente en X^i igual a $a_i + b_i$.
- Producto. $f(X)g(X)$ es el polinomio con coeficiente en X^i igual a $a_i b_0 + a_{i-1} b_1 + \ldots + a_0 b_i$.

Proposición 6.1.3.– Con estas operaciones, $A[X]$ es un anillo.

Lema 6.1.4.– Sea $a \in k$. La aplicación $\Phi : k[X] \to k[X]$ definida por $\Phi(f(X)) = f(X - a)$ es un automorfismo de anillos.

Lema 6.1.5.– Sea A un anillo y $f(X), g(X) \in A[X]$. Entonces

1. $\text{grado}(f(X) + g(X)) \leq \text{máx}\{\text{grado}(f(X)), \text{grado}(g(X))\}$.
2. $\text{grado}(f(X)g(X)) \leq \text{grado}(f(X)) + \text{grado}(g(X))$.
3. La igualdad se tiene en el caso anterior si los coeficientes líderes de $f(X)$ y $g(X)$ no son divisores de cero. En particular, cuando A es un dominio de integridad.

Corolario 6.1.6.– Si A es un dominio de integridad, entonces

1. $A[X]$ es un dominio de integridad.
2. Las unidades de $A[X]$ son las unidades de A.

NOTA 6.1.7.– Sea $f(X) = a_0 + a_1X + \ldots + a_nX^n \in A[X]$ y $g(X) = b_0 + b_1X + \ldots b_{m-1}X^{m-1} + X^m$ un polinomio mónico, de grado $m \geq 1$. Si $n \geq m$, sea $q_1(X) = a_nX^{n-m}$. Entonces $f_1(X) = f(X) - g(X)q_1(X)$ tiene grado menor o igual que $n-1$. Si grado$(f_1(X)) \geq m$, repetimos el proceso con $f_1(X)$. Tras un número finito de pasos llegamos a un polinomio $f_s(X)$ de grado estrictamente menor que m. Si llamamos $q(X) = q_1(X) + \ldots + q_s(X)$ y $r(X) = f(X) - q(X)g(X)$ obtenemos una ecuación

$$f(X) = g(X)q(X) + r(X)$$

donde grado$(r(X)) <$ grado$(g(X))$. Este proceso no es más que la tradicional división de polinomios.

PROPOSICIÓN 6.1.8.– Algoritmo de división. Sea A un anillo, $f(X), g(X) \in A[X]$ con $g(X)$ mónico. Entonces existen unos únicos $q(X), r(X) \in A[X]$ con grado$(r(X)) <$ grado$(g(X))$ tales que

$$f(X) = g(X)q(X) + r(X).$$

NOTA 6.1.9.–

1. Decimos que $g(X)$ divide a $f(X)$ si en lo anterior se obtiene $r(X) = 0$.
2. En el caso $A = k$ un cuerpo el algoritmo anterior se tiene siempre, pues el coeficiente líder de $g(X)$ es una unidad.
3. Si $g(X)$ no es mónico, se puede conseguir una pseudo-división de la forma $c \cdot f(X) = g(X)q(X) + r(X)$ con $c \in A$.

COROLARIO 6.1.10.– Sea A un anillo y $a \in A$. Entonces para cualquier $f(X) \in A[X]$ existe $q(X) \in A[X]$ tal que

$$f(X) = (X - a)q(X) + f(a).$$

COROLARIO 6.1.11.– Sea $f(X) \in A[X]$ y $a \in A$. Entonces $f(a) = 0$ si y solamente si $X - a$ divide a $f(X)$.

COROLARIO 6.1.12.– Sea A un dominio de integridad y $f(X) \neq 0 \in A[X]$ un polinomio de grado n. Entonces existen a lo más n raíces de $f(X)$ en A.

COROLARIO 6.1.13.– Sea A un dominio de integridad y $f(X), g(X) \in A[X]$ de grado menor o igual que n. Si $f(a) = g(a)$ para $n+1$ valores distintos de $a \in A$, entonces $f(X) = g(X)$.

DEFINICIÓN 6.1.14.– Sea $f(X) \in A[X]$ un polinomio no nulo y $a \in A$ una raíz de $f(X)$. Entonces $X - a$ divide a $f(X)$ en $A[X]$. Al máximo entero $s > 0$ tal que $(X-a)^s | f(X)$ se le llama la *multiplicidad de a como raíz de* $f(X)$. Se dirá que a es una raíz simple de $f(X)$ si $s = 1$. En caso contrario se dirá que es múltiple.

6.2. Factorización.

TEOREMA 6.2.1.– Sea k un cuerpo. Todo ideal de $k[X]$ está generado por un único elemento.

DEFINICIÓN 6.2.2.– Sea A un anillo. Si $x, y \in A$, decimos que x divide a y, y lo notaremos por $x|y$ si existe $a \in A$ tal que $y = ax$.

DEFINICIÓN 6.2.3.– Sean $x, y \in A$. Un máximo común divisor de x, y es un elemento $w \in A$ tal que

- $w|x$ y $w|y$.
- Si $v|x$ y $v|y$ entonces $v|w$.

Lo escribiremos como $w = \mathrm{mcd}(x, y)$.

DEFINICIÓN 6.2.4.– Sea A un dominio de integridad. Un elemento no nulo $x \in A$ se dice irreducible si $x = uv$, con $u, v \in A$ implica que u o v es una unidad en A. Dos elementos $x, y \in A$ se dicen asociados si existe una unidad $u \in A$ tal que $x = uy$.

PROPOSICIÓN 6.2.5.– Sean $f(X), g(X) \in k[X]$. Entonces existe $d(X)$ el máximo común divisor de $f(X)$ y $g(X)$, y podemos encontrar $a(X), b(X) \in k[X]$ tales que $d(X) = a(X)f(X) + b(X)g(X)$.

Demostración. Sabemos que existe $d(X) \in k[X]$ tal que $\langle f(X), g(X)\rangle = \langle d(X)\rangle$. Entonces $d(X)|f(X), d(X)|g(X)$, y existen $a(X), b(X)$ con $d(X) = a(X)f(X)+b(X)g(X)$. Si $e(X)|f(X), e(X)|g(X)$ entonces

$$f(X) = e(X)f_1(X), g(X) = e(X)g_1(X) \text{ y}$$
$$d(X) = a(X)f_1(X)e(X) + b(X)g_1(X)e(X),$$

de donde $e(X)|d(X)$. □

PROPOSICIÓN 6.2.6.– Sea $f(X)$ irreducible en $k[X]$ y consideremos el ideal $I = \langle f(X)\rangle$. Entonces $k[X]/I$ es un cuerpo.

Demostración. Sea $g(X) + I \neq 0 + I$. Debemos probar que tiene inverso en $k[X]/I$. Tenemos que $g(X)$ no es múltiplo de $f(X)$. Como existe el máximo común divisor, no puede ser más que 1, dado que $f(X)$ es irreducible. Entonces existen $a(X), b(X) \in k[X]$ tales que $1 = a(X)f(X) + b(X)g(X)$ y $(g(X) + I)(b(X) + I) = 1 + I$. □

LEMA 6.2.7.– Sea $f(X) \in k[X]$ irreducible tal que $f(X)|a(X)b(X)$. Entonces $f(X)|a(X)$ o $f(X)|b(X)$.

Demostración. Si $I = \langle f(X)\rangle$, entonces $a(X)b(X) + I = 0 + I$. Como $k[X]/I$ es un cuerpo, es un dominio de integridad, por lo que $a(X) + I$ o $b(X) + I$ es nulo. □

PROPOSICIÓN 6.2.8.– Sea $f(X) \in k[X]$. Entonces $f(X)$ se puede escribir como $f(X) = uq_1(X)\cdots q_m(X)$ donde u es una unidad y cada $q_i(X)$ es irreducible. Además, esta factorización es única en el sentido de que si $f(X) = vp_1(X)\cdots p_n(X)$ con v unidad y cada $p_i(X)$ irreducible entonces $m = n$ y existe una permutación σ de $\{1,\ldots,n\}$ tal que $p_i(X) = w_i q_{\sigma(i)}(X)$ con w_i unidad.

Demostración. La existencia de la factorización es por inducción sobre el grado de $f(X)$. Si $f(X)$ es irreducible, hemos acabado. En otro caso, se puede expresar como producto $f(X) = f_1(X)f_2(X)$, con

$$\text{grado}(f(X)) > \text{grado}(f_1(X)), \text{grado}(f_2(X)).$$

Veamos la unicidad. Si

$$uq_1(X)\cdots q_m(X) = vp_1(X)\cdots p_n(X)$$

entonces $q_1(X)$ divide a algún $p_i(X)$. Como son irreducibles, existe w_i unidad tal que $q_1(X) = w_i p_i(X)$. Por inducción tenemos el resultado. □

6.3. Lema de Gauss.

DEFINICIÓN 6.3.1.– Sea $f(X) \in \mathbb{Z}[X]$ un polinomio no nulo. Llamamos contenido de $f(X)$ a un máximo común divisor de los coeficientes de $f(X)$, y lo notaremos por $c(f(X))$. Decimos que el polinomio $f(X)$ es primitivo si $c(f) = 1$.

Observemos que el contenido de $f(X)$ está unívocamente determinado salvo multiplicación por una unidad de $\mathbb{Z}$. Si $f(X) \in \mathbb{Z}[X]$ es un polinomio no nulo entonces podemos escribir $f(X) = cf_1(X)$, donde c es el contenido de $f(X)$ y $f_1(X)$ es primitivo.

LEMA 6.3.2.– Sean $f(X), g(X)$ polinomios no nulos de $\mathbb{Z}[X]$. Entonces

$$c(f(X)g(X)) = c(f(X))c(g(X)).$$

En particular, si $f(X)$ y $g(X)$ son primitivos entonces el producto $f(X)g(X)$ es primitivo.

Demostración. Sea $p \in \mathbb{Z} = A$ un elemento irreducible. Entonces $A/\langle p\rangle$ es un dominio de integridad. Por tanto, $A/\langle p\rangle[X]$ es también dominio. Consideremos el homomorfismo

$$\phi : A[X] \to A/\langle p\rangle[X]$$

inducido por el paso al cociente de A en $A/\langle p\rangle$. Sean $f(X), g(X)$ polinomios no nulos de $A[X]$. Como $\phi(f(X)g(X)) = \phi(f(X))\phi(g(X))$, se tiene que $\phi(f(X)g(X)) = 0$ si y solamente si $\phi(f(X)) = 0$ o $\phi(g(X)) = 0$. En otras palabras, p es un factor irreducible de $c(f(X)g(X))$ si y solamente si p es factor irreducible de $c(f(X))c(g(X))$. En concreto, $f(X)g(X)$ es primitivo si y solamente si $f(X)$ y $g(X)$ lo son. A partir del caso particular obtenemos el caso general. Escribamos $f(X) = cf_1(X), g(X) = dg_1(X)$, con $f_1(X), g_1(X)$ primitivos. Entonces $f(X)g(X) = cdf_1(X)g_1(X)$, con $f_1(X)g_1(X)$ primitivo y se deduce que $c(f(X)g(X)) = cd = c(f(X))c(g(X))$. □

LEMA 6.3.3.– Si $f(X) \in \mathbb{Q}[X]$ es un polinomio no nulo, entonces $f(X) = \alpha f_1(X)$ con $\alpha \in \mathbb{Q}$ y $f_1(X)$ un elemento primitivo de $\mathbb{Z}[X]$. Esta factorización es única salvo producto por una unidad de $\mathbb{Z}$.

Demostración. Consideremos d un denominador común de los coeficientes de $f(X)$, y podemos escribir $f(X) = (1/d)g(X)$ donde $g(X) \in \mathbb{Z}[X]$. Sea $\alpha = c(g(X))/d \in \mathbb{Q}$. Entonces $f(X) = \alpha f_1(X)$ con $f_1(X)$ polinomio primitivo. Consideremos ahora la unicidad. Supongamos que $f(X) = \beta f_2(X)$, con $f_2(X)$ polinomio primitivo de $\mathbb{Z}[X]$, y $\beta = a/b$. Entonces

$$adf_2(X) = cbf_1(X).$$

El contenido de la parte izquierda es ad y el de la parte derecha es cb, luego existe $u \in \mathbb{Z}$ unidad tal que $ad = ucb$. Entonces $uf_2(X) = f_1(X)$ y los coeficientes satisfacen la misma relación $\beta = a/b = u(c/d) = u\alpha$. □

LEMA 6.3.4.– Sea $f(X) \in \mathbb{Z}[X]$. Son equivalentes:

1. $f(X)$ tiene grado positivo y es irreducible en $\mathbb{Z}[X]$.
2. $c(f(X)) = 1$ y $f(X)$ es irreducible en $\mathbb{Q}[X]$.

Demostración. Supongamos que $f(X) \in \mathbb{Z}[X]$ es irreducible y de grado positivo. Entonces $f(X)$ es primitivo ya que $c(f(X))$ divide a $f(X)$, y todo elemento irreducible de $\mathbb{Z}$ lo es también en $\mathbb{Z}[X]$. Para ver que es irreducible en $\mathbb{Q}[X]$, pongamos $f(X) = g_1(X)g_2(X)$, con $g_1(X) \in \mathbb{Q}[X], i = 1, 2$, y $g_2(X)$ de grado positivo. Entonces $g_i(X) = \alpha_i f_i(X)$, donde $\alpha_i \in \mathbb{Q}$ y $f_i(X) \in \mathbb{Z}[X]$ primitivo. Se sigue que

$$f(X) = \alpha_1\alpha_2 f_1(X)f_2(X),$$

y el producto $f_1(X)f_2(X)$ es primitivo por el lema de Gauss. Entonces, por el lema anterior, $f(X)$ y $f_1(X)f_2(X)$ se diferencian en el producto por una unidad de $\mathbb{Z}$. Esto obliga a que $f_1(X)$ sea unidad en $\mathbb{Z}[X]$, esto es, $f_1(X)$ es una unidad de $\mathbb{Z}$.
Recíprocamente, sea $f(X) \in \mathbb{Z}[X]$ primitivo e irreducible en $\mathbb{Q}[X]$. Si se tiene que $f(X) = g(X)h(X)$, con $g(X), h(X) \in \mathbb{Z}[X]$, y $h(X)$ de grado positivo, entonces $g(X)$ tiene grado cero (una descomposición en $\mathbb{Z}[X]$ lo es también en $\mathbb{Q}[X]$). Como $1 = c(f(X)) = gc(h(X))$, se sigue que $g(X)$ es, además, unidad de $\mathbb{Z}$. □