Capítulo 2
Polinomios

En este capítulo A denotará un anillo conmutativo y $A[X]$ el anillo de polinomios con coeficientes en A que fue introducido en el capítulo anterior.

2.1 El grado

2.1.1. Definición. Para un polinomio $f = \sum_{i\geq 0} a_i X^i \in A[X]$ su **grado** es dado por

$$\deg f := \max\{i \mid a_i \neq 0\}.$$

Para el polinomio nulo, se define

$$\deg 0 := -\infty.$$

2.1.2. Proposición. *Para cualesquera $f, g \in A[X]$ se tiene*

$$\deg(fg) \leq \deg f + \deg g,$$
$$\deg(f+g) \leq \max\{\deg f, \deg g\}.$$

Además, si A es un dominio, entonces

$$\deg(fg) = \deg f + \deg g. \tag{2.1}$$

Demostración. Para la suma de polinomios, podemos escribir

$$f = a_m X^m + \cdots + a_1 X + a_0, \quad g = b_m X^m + \cdots + b_1 X + b_0,$$

donde $m := \max\{\deg f, \deg g\}$. Luego,

$$f + g = (a_m + b_m) X^m + \cdots + (a_1 + b_1) X + (a_0 + b_0),$$

así que

$$\deg(f+g) \leq m.$$

Ahora para los productos, si $f = 0$ o $g = 0$ la identidad (2.1) se cumple gracias a nuestra definición del grado del polinomio nulo. Supongamos entonces que f y g no son nulos y que $\deg f = m$, $\deg g = n$. Luego,

$$fg = \Big(a_m X^m + \cdots + a_1 X + a_0\Big)\Big(b_n X^n + \cdots + b_1 X + b_0\Big) = a_m b_n X^{m+n} + \cdots + a_0 b_0,$$

donde $a_m, b_n \neq 0$, así que

$$\deg(fg) \leq m + n.$$

Si A es un dominio, entonces $a_m b_n \neq 0$ y se cumple la igualdad. ■

2.1.3. Observación. *Si un polinomio $f = \sum_{i\geq 0} a_i X^i \in A[X]$ es invertible, entonces su coeficiente constante es invertible en A; es decir, $a_0 \in A^\times$.*

Demostración. Si existe otro polinomio $g = \sum_{i\geq 0} b_i X^i \in A[X]$ tal que $f\,g = 1$, esto significa que los coeficientes del producto de f y g están dados por

$$c_k := \sum_{i+j=k} a_i b_j = \begin{cases} 1, & \text{si } k = 0, \\ 0, & \text{si } k > 0. \end{cases}.$$

En particular, $a_0\, b_0 = 1$, lo que significa que $b_0 = a_0^{-1}$. ■

Entonces, la condición $a_0 \in A^\times$ es necesaria para que $f = \sum_{i\geq 0} a_i X^i \in A[X]$ sea invertible, pero no es suficiente. Para simplificar la vida, supongamos que A es un dominio.

2.1.4. Proposición. *Si A es un dominio, entonces un polinomio $f = \sum_{i\geq 0} a_i X^i \in A[X]$ es invertible en $A[X]$ si y solamente si $a_0 \in A^\times$ y $a_i = 0$ para $i > 0$. En otras palabras, se tiene una identificación*

$$A[X]^\times = A^\times.$$

Demostración. Acabamos de ver que la condición $a_0 \in A^\times$ es necesaria. Ahora si f es invertible, tenemos $f\,g = 1$ para algún polinomio g y la identidad

$$0 = \deg(f\,g) = \deg f + \deg g$$

implica que $\deg f = \deg g = 0$. ■

2.1.5. Comentario. Si en A hay divisores de cero, entonces tenemos solamente la desigualdad

$$\deg(f\,g) \leq \deg f + \deg g$$

en lugar de

$$\deg(f\,g) = \deg f + \deg g$$

y el argumento de arriba no funciona. En este caso existen polinomios invertibles que no son constantes. Por ejemplo, en el anillo $\mathbb{Z}/4\mathbb{Z}[X]$ se cumple

$$(2X+1)\cdot(2X+1) = 4X^2 + 4X + 1 \equiv 1 \pmod 4.$$

2.2 División con resto

2.2.1. Definición. Se dice que un polinomio

$$a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 \in A[X]$$

es **mónico** si $a_n = 1$.

2.2.2. Teorema (División con resto). *Sean $f, g \in A[X]$ polinomios, con g mónico. Entonces, existen polinomios $q, r \in A[X]$ tales que*

$$f = q\,g + r, \quad \deg r < \deg g.$$

Además, si A es un dominio, entonces q y r están definidos de modo único.

Demostración. Escribamos

$$f = a_m X^m + a_{m-1} X^{m-1} + \cdots + a_1 X + a_0,$$
$$g = X^n + b_{n-1} X^{n-1} + \cdots + b_1 X + b_0,$$

donde $m = \deg f$, $n = \deg g$. Procedamos por inducción sobre m. Si $m < n$, podemos tomar $q = 0$ y $r = f$:

$$f = 0 \cdot g + f.$$

Para el paso inductivo, si $m \geq n$, consideremos el polinomio

$$h := f - a_m X^{m-n} g. \tag{2.2}$$

Por la definición, ambos polinomios f y $a_m X^{m-n} g$ tienen el mismo término mayor $a_m X^m$ que se cancela en h, así que $\deg h < \deg f$. Luego, por la hipótesis inductiva, existen $q_1, r \in A[X]$ tales que

$$h = q_1 g + r, \quad \deg r < \deg g.$$

Ahora

$$f = h + a_m X^{m-n} g = (q_1 + a_m X^{m-n}) g + r.$$

Esto establece la existencia de q y r.

Para la unicidad, asumamos que A es un dominio (y por lo tanto $A[X]$ es un dominio) y

$$f = q_1 g + r_1 = q_2 g + r_2, \quad \deg r_1, \deg r_2 < \deg g.$$

Luego, tenemos

$$(q_1 - q_2) g = r_2 - r_1.$$

Dado que $g \neq 0$, esta expresión nos dice que $q_1 = q_2$ si y solo si $r_1 = r_2$. Ahora si $r_1 \neq r_2$, entonces tenemos

$$0 \leq \deg(r_2 - r_1) < \deg g,$$

pero esto contradice el hecho de que

$$\deg((q_1 - q_2) g) = \deg(q_1 - q_2) + \deg g. \qquad \blacksquare$$

Nuestra prueba por inducción contiene un algoritmo de división con resto. Consideremos un ejemplo particular para ver cómo este funciona.

2.2.3. Ejemplo. Dividamos con resto $f = X^6$ por $g = X^2 - X + 1$ en el anillo $\mathbb{Z}[X]$. Tenemos

$$h_1 := f - \boxed{X^4}\, g = X^5 - X^4,$$
$$h_2 := h_1 - \boxed{X^3}\, g = -X^3,$$
$$h_3 := h_2 - (\boxed{-X})\, g = -X^2 + X,$$
$$r := h_3 - (\boxed{-1})\, g = 1,$$

de donde

$$f = (X^4 + X^3 - X - 1) g + 1. \qquad \blacktriangle$$

2.2.4. Comentario (♣). Podemos describir el algoritmo de división con resto de diferente manera. Para un polinomio no nulo $r = \sum_{i \geq 0} c_i X^i \in A[X]$, denotemos su **coeficiente mayor** por

$$\mathrm{cm}(r) := c_{\deg r}.$$

Tenemos el siguiente algoritmo.

Entrada: $f, g \in A[X]$, donde g es mónico

$q := 0$
$r := f$

mientras $\deg r \geq \deg g$ **hacer**
$q = q + \mathrm{cm}(r) \cdot X^{\deg r - \deg g}$
$r = r - \mathrm{cm}(r) \cdot X^{\deg r - \deg g} \cdot g$

devolver (q, r)

Este algoritmo funciona porque a cada paso se cumple la identidad

$$f = qg + r;$$

en efecto, esto es cierto al principio cuando $q = 0$ y $r = f$, y luego,

$$(q + \mathrm{cm}(r) \cdot X^{\deg r - \deg g})\, g + (r - \mathrm{cm}(r) \cdot X^{\deg r - \deg g} \cdot g) = qg + r.$$

El ciclo "mientras" se termina en algún momento porque

$$\deg(r - \mathrm{cm}(r) \cdot X^{\deg r - \deg g} \cdot g) < \deg r,$$

así que el grado de r decrece a cada paso. Cuando el ciclo termina, se tiene $\deg r < \deg g$ y el polinomio r es el verdadero resto de división.

2.2.5. Corolario. *Sean k un cuerpo y $f, g \in k[X]$ polinomios, con $g \neq 0$. Entonces, existen $q, r \in k[X]$ tales que*

$$f = q\, g + r, \quad \deg r < \deg g.$$

Además, estos q y r están definidos de modo único.

Demostración. Tenemos

$$g = b_n X^n + b_{n-1} X^{n-1} + \cdots + b_1 X + b_0,$$

donde $b_n \neq 0$. Podemos modificar la prueba de 2.2.2, cambiando la fórmula (2.2) por

$$h := f - a_m\, b_n^{-1}\, X^{m-n}\, g.$$

Sino, para no repetir el mismo argumento, se puede notar que el polinomio $b_n^{-1}\, g$ es mónico, y el resultado de 2.2.2 nos da

$$f = q_1\, b_n^{-1}\, g + r, \quad \deg r < \deg g.$$

Entonces, podemos tomar $q := b_n^{-1}\, q_1$. La unicidad de q y r se verifica de la misma manera que en 2.2.2. ■

2.3 Raíces de polinomios

2.3.1. Definición. Para un polinomio $f = \sum_{0 \leq i \leq n} a_i\, X^i \in A[X]$ y un elemento $\alpha \in A$ la **evaluación de f en α** es el elemento

$$f(\alpha) := \sum_{0 \leq i \leq n} a_i\, \alpha^i \in A.$$

Si $f(\alpha) = 0$, se dice que α es una **raíz** (o un **cero**) de f.

2.3.2. Observación. *Para cualesquiera $f, g \in A[X]$ y $\alpha \in A$ se tiene*

$$(f+g)(\alpha) = f(\alpha) + g(\alpha), \quad (fg)(\alpha) = f(\alpha)\, g(\alpha). \qquad \square$$

2.3.3. Proposición. *Se tiene $f(\alpha) = 0$ para algún $\alpha \in A$ si y solamente si*

$$f = (X - \alpha) \cdot g$$

para algún polinomio $g \in A[X]$.

Demostración. En una dirección es obvio: si podemos escribir

$$f = (X - \alpha) \cdot g,$$

y entonces la evaluación en α nos da

$$f(\alpha) = (\alpha - \alpha) \cdot g(\alpha) = 0.$$

En la otra dirección, supongamos que $\deg f = n$. La división con resto de f por el polinomio lineall $X - \alpha$ nos da

$$f = q\,(X - \alpha) + r,$$

donde $r \in A$ tiene que ser constante. Pero la evaluación en α nos da

$$0 = f(\alpha) = q(\alpha)\,(\alpha - \alpha) + r,$$

así que $r = 0$. ■

2.3.4. Corolario. *Sea $f \in A[X]$ un polinomio no nulo con coeficientes en un dominio A. Entonces f tiene $\leq \deg f$ raíces distintas en A.*

Demostración. Inducción sobre $n = \deg f$. Si $n = 0$, entonces f, siendo un polinomio constante no nulo, no tiene raíces. Para el paso inductivo, notamos que si $\alpha \in A$ es una raíz de f, entonces

$$f = (X - \alpha)\, g$$

para algún polinomio $g \in A[X]$. Luego,

$$\deg f = \deg(X - \alpha) + \deg g$$

(aquí se usa la hipótesis que A es un dominio), así que $\deg g = n - 1$ y por la hipótesis de inducción sabemos que g tiene $\leq n - 1$ raíces distintas. Toda raíz de g es una raíz de f, y si $\beta \neq \alpha$ es una raíz de f, entonces la identidad en A

$$0 = f(\beta) = (\beta - \alpha) \cdot g(\beta)$$

implica que $g(\beta) = 0$ y β es una raíz de g (de nuevo, se usa la hipótesis que A es un dominio). Podemos concluir que f tiene $\leq n$ diferentes raíces. ■

2.3.5. Ejemplo. El polinomio cuadrático $f = X^2 + 1 \in \mathbb{C}[X]$ tiene dos raíces complejas $\pm i \in \mathbb{C}$. Si lo consideramos como un polinomio en $\mathbb{R}[X]$, entonces este no tiene raíces.

El polinomio $f = X^2 + 1 \in \mathbb{F}_3[X]$ no tiene raíces en $\mathbb{F}_3$: tenemos

$$f([0]) = [1], \quad f([1]) = [2], \quad f([2]) = [2]^2 + [1] = [2].$$

El polinomio $f = 2\,X^4 - 3\,X^3 + 3\,X^2 - 3\,X + 1 \in \mathbb{Z}[X]$ puede ser factorizado en $\mathbb{C}[X]$ como

$$f = 2\,(X - 1)\,(X - i)\,(X + i)\,(X - 1/2).$$

Su única raíz en $\mathbb{Z}$ es 1.

El polinomio $f = 2\,X^2 + 2\,X \in \mathbb{Z}/4\mathbb{Z}$ es cuadrático, pero todo elemento de $\mathbb{Z}/4\mathbb{Z}$ es su raíz:

$$f([0]) = f([1]) = f([2]) = f([3]) = [0].$$

Esto no contradice el resultado de arriba, ya que $\mathbb{Z}/4\mathbb{Z}$ no es un dominio. ▲

2.3.6. Corolario. *Sea A un dominio infinito y sean $f, g \in A[X]$ dos polinomios tales que $f(x) = g(x)$ para todo $x \in A$. Entonces, $f = g$ como polinomios.*

Demostración. En este caso el polinomio $f - g$ tiene un número infinito de raíces, así que es necesariamente nulo. ■

2.3.7. Comentario. A veces hay cierta confusión entre los polinomios y funciones polinomiales. Para cualquier polinomio $f \in A[X]$ la evaluación define una función

$$A \to A, \quad x \mapsto f(x).$$

Sin embargo, si A es finito, no puede haber una correspondencia biyectiva entre las aplicaciones que surgen de esta manera y los elementos de $A[X]$: en este caso hay solamente $|A|^{|A|}$ diferentes aplicaciones $A \to A$, mientras que el anillo $A[X]$ es infinito: sus elementos son las expresiones formales $\sum_{0 \le i \le n} a_i X^i$ con $a_i \in A$.

Para dar un ejemplo específico: el polinomio $X^p - X \in \mathbb{F}_p[X]$ evaluado en cualquier elemento de $\mathbb{F}_p$ nos da 0, gracias al pequeño teorema de Fermat, mientras que $X^p - X$ no es nulo como un elemento de $\mathbb{F}_p[X]$ (es decir, como una *expresión formal*).

2.4 Raíces múltiples y derivadas formales

2.4.1. Definición. Sea A un anillo conmutativo. Para un polinomio

$$f = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_2 X^2 + a_0 \in A[X]$$

su **derivada formal** viene dada por

$$f' = n\, a_n X^{n-1} + (n-1)\, a_{n-1} X^{n-2} + \cdots + a_2 X + a_1.$$

Dejo al lector como un ejercicio comprobar que esta definición cumple las propiedades habituales: para cualesquiera $f, g \in A[X]$ se cumple

$$(f+g)' = f' + g', \quad (f\,g)' = f'\,g + f\,g'.$$

2.4.2. Definición. Sean A un dominio, $f \in A[X]$ un polinomio y $\alpha \in A$ una raíz de f. La **multiplicidad** de α es el número máximo $m = 1, 2, 3, \ldots$ tal que

$$f = (X - \alpha)^m\, g \quad \text{para algún } g \in A[X].$$

Si $m = 1$, se dice que α es una **raíz simple** de f y si $m > 1$, se dice que α es una **raíz multiple** de **multiplicidad** m.

2.4.3. Ejemplo. El polinomio $X^2 - 2X + 1 \in A[X]$ tiene raíz $\alpha = 1$ de multiplicidad 2 para cualquier A. ▲

2.4.4. Ejemplo. Consideremos el polinomio

$$f := X^3 - 1 \in \mathbb{F}_p[X].$$

Si $p = 2$, entonces $\alpha = 1$ es una raíz símple: tenemos

$$X^3 - 1 = (X-1)\,(X^2 + X + 1),$$

donde $X^2 + X + 1$ no tiene raíces en $\mathbb{F}_2$. Ahora si $p = 3$, entonces $\alpha = 1$ es una raíz de multiplicidad 3:

$$(X^3 - 1) = (X-1)^3 \quad \text{en } \mathbb{F}_3[X].$$ ▲

Podemos hacer más preciso el resultado de 2.3.4.

2.4.5. Observación. *Sea $f \in A[X]$ un polinomio no nulo con coeficientes en un dominio A. Entonces f tiene $\leq \deg f$ raíces en A, contando las multiplicidades.* □

2.4.6. Proposición (Fórmulas de Vieta[*]). *Si k es un cuerpo y*

$$f = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 \in k[X]$$

es un polinomio que tiene n raíces $\alpha_1, \ldots, \alpha_n \in k$ (contando las multiplicidades), entonces

$$\begin{aligned}
\alpha_1 + \cdots + \alpha_n &= -\frac{a_{n-1}}{a_n}, \\
\sum_{1 \leq i < j \leq n} \alpha_i \alpha_j &= +\frac{a_{n-2}}{a_n}, \\
\sum_{1 \leq i < j < k \leq n} \alpha_i \alpha_j \alpha_k &= -\frac{a_{n-3}}{a_n}, \\
&\cdots \\
\alpha_1 \cdots \alpha_n &= (-1)^n \frac{a_0}{a_n}.
\end{aligned}$$

Demostración. Podemos escribir

$$a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 = a_n (X - \alpha_1) \cdots (X - \alpha_n)$$

y desarrollar la expresión a la derecha. ■

2.4.7. Ejemplo. El polinomio $X^3 - 1$ tiene tres raíces complejas: $1, \zeta_3, \zeta_3^2$. Luego,

$$\begin{aligned}
1 + \zeta_3 + \zeta_3^2 &= 0, \\
\underbrace{1 \cdot \zeta_3 + 1 \cdot \zeta_3^2}_{=-1} + \underbrace{\zeta_3 \zeta_3^2}_{=1} &= 0, \\
1 \cdot \zeta_3 \cdot \zeta_3^2 &= 1.
\end{aligned}$$

▲

2.4.8. Proposición. *Un polinomio $f \in A[X]$ tiene una raíz múltiple $\alpha \in A$ si y solo si $f(\alpha) = f'(\alpha) = 0$.*

Demostración. Si α es una raíz multiple, entonces por la definición

$$f = (X - \alpha)^2 g$$

para algún polinomio $g \in A[X]$. Luego, tomando las derivadas, se obtiene

$$f' = 2 (X - \alpha) g + (X - \alpha)^2 g',$$

de donde $f'(\alpha) = 0$. Viceversa, si $\alpha \in A$ es una raíz común de f y f', entonces tenemos

$$f = (X - \alpha) g$$

para algún $g \in A[X]$ y luego

$$f' = g + (X - \alpha) g'.$$

De aquí se sigue que $g = f' - (X - \alpha) g'$ tiene α como su raíz; es decir,

$$g = (X - \alpha) h$$

para algún $h \in A[X]$. Luego,

$$f = (X - \alpha) g = (X - \alpha)^2 h.$$ ■

[*] François Viète (1540–1603) — matemático francés, uno de los primeros algebristas europeos. "Franciscus Vieta" es la versión latín de su nombre.

2.4.9. Ejemplo. Volvamos al ejemplo 2.4.4. La derivada formal de $f := X^3 - 1 \in \mathbb{F}_p[X]$ es

$$f' = 3X^2.$$

Si $p \neq 3$, entonces la única raíz de f' es $\alpha = 0$, y por lo tanto no habrá $\alpha \in \mathbb{F}_p$ tal que $f(\alpha) = f'(\alpha) = 0$, así que f no tiene raíces múltiples si $p \neq 3$. ▲

2.5 Teorema fundamental del álgebra

2.5.1. Teorema (Teorema fundamental del álgebra). *Todo polinomio complejo no constante*

$$f = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 \in \mathbb{C}[X],$$

(donde $n \geq 1$ y $a_n \neq 0$) tiene una raíz compleja: existe $\alpha \in \mathbb{C}$ tal que $f(\alpha) = 0$.

Este resultado aparece en el tratado de d'Alembert* "Recherches sur le calcul intégral" (1748) y fue probado de manera rigurosa en la tesis de doctorado de Gauss, publicada en 1799. El nombre "teorema fundamental del álgebra" parece un poco ridículo en un curso del álgebra moderna, pero es histórico y bastante común. Sin duda, es uno de los resultados más importantes en las matemáticas.

Para probar el teorema, vamos a necesitar el siguiente resultado estándar de análisis; para la prueba véase [Rud1989, Theorem 4.16].

2.5.2. Lema. *Sea $f\colon D \to \mathbb{R}$ una función continua definida sobre el disco cerrado de radio r*

$$D := \{z \in \mathbb{C} \mid |z| \leq r\}.$$

Sea $\mu := \inf_{z \in D} f(z)$. Entonces, existe un punto $z \in D$ tal que $f(z) = \mu$.

2.5.3. Comentario. Para los que conozcan topología: esto es cierto si D es cualquier espacio topológico compacto.

Demostración del teorema. Sin pérdida de generalidad, podemos asumir que $a_n = 1$ (al dividir todo polinomio por a_n, las raíces no se cambian).

Consideremos la función continua

$$\mathbb{C} \to \mathbb{R}, \quad z \mapsto |f(z)|.$$

Pongamos

$$\mu := \inf_{z \in \mathbb{C}} |f(z)|.$$

Notamos que para $z \neq 0$ tenemos

$$f(z) = z^n \left(1 + a_{n-1} z^{-1} + \cdots + a_1 z^{-n+1} + a_0 z^{-n}\right),$$

y luego,

$$|f(z)| \geq |z|^n \left(1 - |a_{n-1}| \cdot |z|^{-1} - \cdots - |a_1| \cdot |z|^{-n+1} - |a_0| \cdot |z|^{-n}\right) \xrightarrow{|z| \to \infty} \infty.$$

Esto significa que existe $r > 0$ tal que $|f(z)| > \mu$ si $|z| > r$. Luego, por el lema anterior aplicado al disco de radio r, existe $z_0 \in \mathbb{C}$ tal que $|f(z_0)| = \mu$. Nuestro objetivo es probar que $\mu = 0$. Si no es el caso, pasando de $f(z)$ a $\frac{f(z - z_0)}{f(z_0)}$, podemos asumir que $f(0) = 1$ es el mínimo de $|f(z)|$. Escribamos

$$f(z) = 1 + b_k z^k + (\text{términos de grado} \geq k+1),$$

*Jean le Rond D'Alembert (1717–1783), matemático, filósofo y enciclopedista francés, conocido por sus contribuciones en análisis, particularmente las ecuaciones diferenciales.

donde k es el mínimo índice ≥ 1 tal que $b_k \neq 0$. Sea ω una raíz k-ésima de $-b_k^{-1}$; es decir, un número complejo tal que $\omega^k = -b_k^{-1}$ (su existencia se sigue de la fórmula de de Moivre). Tenemos entonces para $x \in \mathbb{R}$

$$f(\omega x) = 1 - x^k + x^{k+1}\, g(x)$$

para algún polinomio complejo $g(x)$. Luego, para $x > 0$ suficientemente pequeño se tiene

$$|f(\omega x)| \leq |1 - x^k| + x^{k+1}\,|g(x)| = 1 - x^k\,(1 - x\,|g(x)|).$$

Podemos escoger x tan pequeño que la expresión en paréntesis sea positiva, así que $|f(\omega x)| < 1 = |f(0)|$. Hemos obtenido una contradicción. ■

2.5.4. Corolario. *Todo polinomio complejo no constante*

$$f = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 \in \mathbb{C}[X],$$

tiene precisamente n raíces complejas, contando las multiplicidades.

Demostración. Usemos la inducción sobre n. Si $n = 1$, el restultado está claro: un polinomio lineal no constante evidentemente tiene una raíz. Luego, asumiendo el resultado para los polinomios de grado $n-1$, si f tiene grado n, entonces f tiene una raíz $\alpha \in \mathbb{C}$ por el teorema, y luego

$$f = (X - \alpha)\, g,$$

donde g tiene grado $n-1$. Por la hipótesis inductiva, g tiene $n-1$ raíces, y por lo tanto f tiene n raíces. ■

2.6 Polinomios ciclotómicos

2.6.1. Definición. Consideremos las raíces n-ésimas de la unidad

$$1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1} \in \mathbb{C},$$

donde $\zeta_n = e^{2\pi i/n}$. Se dice que ζ_n^a es una raíz **primitiva** si $\operatorname{mcd}(a, n) = 1$.

El número de las raíces n-ésimas primitivas coincide entonces con la **función ϕ de Euler**:

$$\phi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times| = \#\{[a]_n \mid \operatorname{mcd}(a, n) = 1\}.$$

Recordemos el siguiente resultado de la teoría de números elemental:

2.6.2. Lema. *La función de Euler satisface la identidad*

$$\sum_{d|n} \phi(d) = n,$$

donde la suma se toma sobre todos los divisiores de n.

Demostración. Consideremos las fracciones

$$\frac{1}{n},\ \frac{2}{n},\ \frac{3}{n},\ \ldots,\ \frac{n-1}{n},\ \frac{n}{n}.$$

Podemos reducirlas a la forma $\frac{a}{b}$, donde $\operatorname{mcd}(a, b) = 1$. Al hacerlo, en los denominadores estarán los divisores $d \mid n$. El número de tales fracciones con d en el denominador será precisamente $\phi(d)$. ■

2.6.3. Ejemplo. Para $n = 6$ consideremos las fracciones

$$\frac{1}{6}, \frac{2}{6}, \frac{3}{6}, \frac{4}{6}, \frac{5}{6}, \frac{6}{6}.$$

Al cancelar los factores comunes en el numerador y denominador, tendremos

$$\frac{1}{6}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{5}{6}, \frac{1}{1}.$$

Tenemos $\phi(1) = \phi(2) = 1$, $\phi(3) = \phi(6) = 2$. ▲

2.6.4. Proposición. *Para todo $k = 0, 1, \ldots, n-1$ el número ζ_n^a es una raíz d-ésima primitiva para algún $d \mid n$. Este d está definido de modo único.*

Demostración. Si $\mathrm{mcd}(a, n) = c$, entonces podemos quitar el factor común de a y n:

$$\zeta_n^a = \zeta_d^{a/c}, \quad \text{donde } d = n/c,\ \mathrm{mcd}(a/c, d) = 1,$$

así que ζ_n^a es una raíz primitiva de orden d. Denotemos por S_d el conjunto de las raíces primitivas de orden d. Por lo que acabamos de ver, se tiene

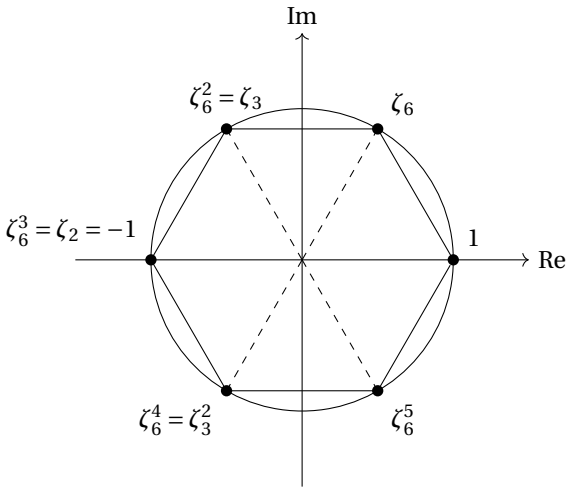
$$\{1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1}\} \subseteq \bigcup_{d \mid n} S_d.$$

Para ver que los conjuntos S_d forman una partición de las raíces n-ésimas, podemos usar el lema anterior:

$$\#\{1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1}\} = n, \quad \sum_{d \mid n} |S_d| = \sum_{d \mid n} \phi(n) = n,$$

así que $S_{d_1} \cap S_{d_2} = \emptyset$ para $d_1 \neq d_2$. ■

2.6.5. Ejemplo. Consideremos las raíces sextas de la unidad:



Tenemos

$$S_1 = \{1\},\ S_2 = \{\zeta_2\},\ S_3 = \{\zeta_3, \zeta_3^2\},\ S_6 = \{\zeta_6, \zeta_6^5\}.$$ ▲

2.6.6. Definición. El n-ésimo **polinomio ciclotómico**[*] es el polinomio mónico que tiene como sus raíces las raíces n-ésimas primitivas de la unidad:

$$\Phi_n := \prod_{\substack{0 \leq a < n \\ \mathrm{mcd}(a,n)=1}} (X - \zeta_n^k).$$

[*] La palabra "ciclotomia" significa "división del círculo" y se refiere al hecho de que las n-ésimas raíces de la unidad son vértices de un n-ágono regular inscrito en el circulo unitario.

Este polinomio tiene grado $\phi(n)$ y es mónico.

2.6.7. Ejemplo. Los primeros polinomios ciclotómicos son

$$\begin{aligned}
&\Phi_1 = X-1,\\
&\Phi_2 = X+1,\\
&\Phi_3 = (X-\zeta_3)(X-\zeta_3^2) = X^2-(\zeta_3+\zeta_3^2)X+\zeta_3^3 = X^2+X+1,\\
&\Phi_4 = (X-\zeta_4)(X-\zeta_4^3) = (X-i)(X+i) = X^2+1.
\end{aligned}$$

▲

2.6.8. Teorema.

1) Para todo primo p se tiene

$$\Phi_p = \frac{X^p-1}{X-1} = X^{p-1}+X^{p-2}+\cdots+X^2+X+1.$$

2) Para todo primo p y $k\geq 1$ se tiene

$$\Phi_{p^k} = \frac{X^{p^k}-1}{X^{p^{k-1}}-1} = \Phi_p(X^{p^{k-1}}) = X^{(p-1)p^{k-1}}+X^{(p-2)p^{k-1}}+\cdots+X^{2p^{k-1}}+X^{p^{k-1}}+1.$$

3) Para todo n se tiene

$$\prod_{d|n}\Phi_d = X^n-1.$$

4) Todos los polinomios Φ_n tienen coeficientes enteros.

Demostración. Observamos que

$$\prod_{0\leq a<n}(X-\zeta_n^a) = X^n-1.$$

En la parte 1), basta notar que entre las raíces p-ésimas, todas son primitivas, salvo la raíz trivial 1, así que

$$\Phi_p = \prod_{1\leq a<p}(X-\zeta_p^a) = \prod_{0\leq a<p}(X-\zeta_p^a)\Big/(X-1) = \frac{X^p-1}{X-1}.$$

De la misma manera, en 2) notamos que un número $0\leq a<p^k$ tal que $\operatorname{mcd}(a,p^k)\neq 1$ es necesariamente divisible por p, así que las raíces de orden p^k que no son primitivas tienen forma $\zeta_{p^k}^{pb} = \zeta_{p^{k-1}}^b$ y son precisamente todas las raíces de orden p^{k-1}:

$$\Phi_{p^k} = \prod_{\substack{0\leq a<p^k\\ \operatorname{mcd}(a,p^k)=1}}(X-\zeta_{p^k}^a) = \prod_{0\leq a<p^k}(X-\zeta_{p^k}^a)\Big/\prod_{0\leq b<p^{k-1}}(X-\zeta_{p^{k-1}}^b) = \frac{X^{p^k}-1}{X^{p^{k-1}}-1}.$$

En la parte 3), basta notar que

$$X^n-1 = \prod_{0\leq a<n}(X-\zeta_n^a) = \prod_{d|n}\prod_{\substack{0\leq a<n\\ \operatorname{mcd}(a,d)=1}}(X-\zeta_n^a) = \prod_{d|n}\Phi_d,$$

usando el resultado de 2.6.4.

La parte 4) se demuestra por inducción sobre n. Esto es cierto, por ejemplo, para $\Phi_1 = X-1$. Luego, si $\Phi_m\in\mathbb{Z}[X]$ para todo $m<n$, entonces podemos considerar el polinomio

$$g := \prod_{\substack{d|n\\ d\neq n}}\Phi_d \in \mathbb{Z}[X].$$

Este es mónico, siendo un producto de polinomios mónicos. La división con resto en el anillo $\mathbb{Z}[X]$ nos da

$$X^n - 1 = q\,g + r, \quad \deg r < \deg g$$

para algunos $q, r \in \mathbb{Z}[X]$, mientras que en el anillo más grande $\mathbb{Q}[X] \supset \mathbb{Z}[X]$ se cumple

$$X^n - 1 = \Phi_n\, g.$$

Pero para la división con resto en $\mathbb{Q}[X]$ el cociente y el resto están definidos de modo único, así que $r = 0$ y $\Phi_n = q \in \mathbb{Z}[X]$. ■

2.6.9. Ejemplo. Tenemos

$$\begin{aligned}
\Phi_4 &= \Phi_2(X^2) = X^2 + 1,\\
\Phi_5 &= X^4 + X^3 + X^2 + X + 1,\\
\Phi_6 &= \frac{X^6 - 1}{\Phi_1\Phi_2\Phi_3} = \frac{(X^3-1)(X^3+1)}{\Phi_1\Phi_2\Phi_3} = \frac{X^3+1}{\Phi_2} = \frac{X^3+1}{X+1} = X^2 - X + 1,\\
\Phi_7 &= X^6 + X^5 + X^4 + X^3 + X^2 + X + 1,\\
\Phi_8 &= \Phi_2(X^4) = X^4 + 1,\\
\Phi_9 &= \Phi_3(X^2) = X^6 + X^3 + 1,\\
\Phi_{10} &= \frac{X^{10} - 1}{\Phi_1\Phi_2\Phi_5} = \frac{(X^5+1)(X^5-1)}{(X^5-1)\Phi_2} = \frac{X^5+1}{X+1} = X^4 - X^3 + X^2 - X + 1.
\end{aligned}$$

Notamos que

$$\begin{aligned}
\Phi_3 = X^2 + X + 1, &\quad \Phi_6 = X^2 - X + 1 = \Phi_3(-X),\\
\Phi_5 = X^4 + X^3 + X^2 + X + 1, &\quad \Phi_{10} = X^4 - X^3 + X^2 - X + 1 = \Phi_5(-X).
\end{aligned}$$

Esto no es una coincidencia: en general, $\Phi_{2m} = \Phi_m(-X)$ para todo $m > 1$ impar. ▲

2.6.10. Comentario. Aunque revisando los primeros Φ_n uno puede pensar que los coeficientes son siempre iguales a ± 1, para $n = 105 = 3\cdot 5\cdot 7$ en Φ_n aparecen por primera vez coeficientes diferentes:

$$\begin{aligned}
\Phi_{105} = X^{48} + X^{47} + X^{46} - X^{43} - X^{42} - 2X^{41} - X^{40} - X^{39} + X^{36} + X^{35} + X^{34}\\
+ X^{33} + X^{32} + X^{31} - X^{28} - X^{26} - X^{24} - X^{22} - X^{20} + X^{17} + X^{16} + X^{15}\\
+ X^{14} + X^{13} + X^{12} - X^9 - X^8 - 2X^7 - X^6 - X^5 + X^2 + X + 1.
\end{aligned}$$

2.7 Polinomios de diversas variables

La construcción de polinomios puede ser generalizada al **anillo de polinomios con coeficientes en** A **en** n **variables** $X_1, \ldots, X_n$ **que se denota por** $A[X_1, \ldots, X_n]$. En este caso los elementos son las expresiones formales de la forma

$$f = \sum_{i_1,\ldots,i_n \geq 0} a_{i_1,\ldots,i_n} X_1^{i_1} \cdots X_n^{i_n},$$

donde $a_{i_1,\ldots,i_n} = 0$, salvo un número finito de $(i_1, \ldots, i_n)$. Las sumas y productos están definidos por

$$\begin{aligned}
\left(\sum_{i_1,\ldots,i_n \geq 0} a_{i_1,\ldots,i_n} X_1^{i_1} \cdots X_n^{i_n}\right) + \left(\sum_{i_1,\ldots,i_n \geq 0} b_{i_1,\ldots,i_n} X_1^{i_1} \cdots X_n^{i_n}\right)\\
:= \sum_{i_1,\ldots,i_n \geq 0} (a_{i_1,\ldots,i_n} + b_{i_1,\ldots,i_n})\, X_1^{i_1} \cdots X_n^{i_n}
\end{aligned}$$

y

$$\left(\sum_{i_1,\dots,i_n\geq 0} a_{i_1,\dots,i_n} X_1^{i_1}\cdots X_n^{i_n}\right)\cdot\left(\sum_{j_1,\dots,j_n\geq 0} b_{j_1,\dots,j_n} X_1^{j_1}\cdots X_n^{j_n}\right)$$
$$:= \sum_{k_1,\dots,k_n\geq 0}\left(\sum_{\substack{(k_1,\dots,k_n)=\\(i_1,\dots,i_n)+(j_1,\dots,j_n)}} a_{i_1,\dots,i_n}\, b_{j_1,\dots,j_n}\right) X_1^{k_1}\cdots X_n^{k_n}.$$

Si quitamos la condición que $a_{i_1,\dots,i_n}=0$, salvo un número finito de $(i_1,\dots,i_n)$, se obtiene el **anillo de las series formales de potencias en** n **variables** $A[[X_1,\dots,X_n]]$.

2.7.1. Proposición. *Si A es un dominio, entonces $A[X_1,\dots,X_n]$ es también un dominio.*

Para los polinomios en una variable, lo probamos considerando los términos mayores: si

$$f = a_m X^m + \cdots + a_1 X + a_0, \quad g = b_n X^n + \cdots + b_1 X + b_0,$$

donde $a_m, b_n \neq 0$, entonces

$$fg = a_m b_n X^{m+n} + \cdots + a_0 b_0,$$

donde $a_m b_n \neq 0$. Para los polinomios en diversas variables, ya no está claro qué termino se puede llamar mayor—considere, por ejemplo, el polinomio

$$f = X^2 Y + X^2 + XY + Y^2 + 1$$

en dos variables X e Y.

Como un remedio, podemos considerar el **orden lexicográfico** sobre los monomios $X_1^{i_1}\cdots X_n^{i_n}$: se dice que

$$X_1^{i_1}\cdots X_n^{i_n} \succ_{lex} X_1^{j_1}\cdots X_n^{j_n}$$

si la primera entrada no nula del vector $(i_1-j_1,\dots,i_n-j_n)$ es positiva. Esto nos permite definir el término mayor de un polinomio, y cuando A es un dominio, el término mayor de fg es el producto de los términos mayores de f y g. Dejo los detalles al lector.

Otra opción (pero esencialmente equivalente) es aislar una variable y expresar cada polinomio como una suma $\sum_i f_i X_n^i$, donde $f_i \in A[X_1,\dots,X_{n-1}]$. Por ejemplo, para el polinomio de arriba

$$f = Y^2 + (X^2+X)\,Y + (X^2+1).$$

Demostración de 2.7.1. Para $n=1$ esto ya fue probado arriba. Procedamos por inducción sobre n. Sean

$$f = \sum_{i_1,\dots,i_n} a_{i_1,\dots,i_n} X_1^{i_1}\cdots X_n^{i_n}, \quad g = \sum_{j_1,\dots,j_n} b_{j_1,\dots,j_n} X_1^{j_1}\cdots X_n^{j_n}$$

dos polinomios no nulos. Podemos escribirlos como

$$f = \sum_{0\leq i\leq p} f_i(X_1,\dots,X_{n-1})\, X_n^i, \quad g = \sum_{0\leq j\leq q} g_j(X_1,\dots,X_{n-1})\, X_n^j$$

donde f_i, g_j son polinomios en variables $X_1,\dots,X_{n-1}$ y $f_p, g_q \neq 0$. Luego, el coeficiente mayor de fg es $f_p g_q$ que no es nulo por la hipótesis de inducción. ∎

2.7.2. Proposición. *Si A es un dominio, entonces los elementos invertibles en $A[X_1,\dots,X_n]$ son los polinomios constantes invertibles en A.*

Demostración. Por inducción sobre el número de variables se demuestra que el término constante debe ser invertible:

$$fg = \sum_{k\geq 0}\left(\sum_{i+j=k} f_i g_j\right) X_n^k = 1,$$

y luego,

$$f_0 g_0 = 1.$$

Para ver que no puede haber términos no constantes, hay que usar el hecho de que si A es un dominio, entonces el término mayor de fg es el producto de los términos mayores. ■

Los polinomios en diversas variables no funcionan de la misma manera que los polinomios en una variable. En particular, en $k[X_1,\ldots,X_n]$ no existe la división con resto que hemos ocupado en este capítulo para probar varios resultados sobre $k[X]$. La teoría de ecuaciones polinomiales en diversas variables es también mucho más sofisticada. El lector interesado puede consultar el libro introductorio [CLO2015].

2.8 Ejercicios

Ejercicio 2.1. Para una serie de potencias $f = \sum_{i\geq 0} a_i X^i \in A[[X]]$ la noción de grado no existe, pero se puede considerar el mínimo índice tal que el coeficiente correspondiente no es nulo:

$$v(f) := \text{mín}\{i \mid a_i \neq 0\};$$

y si $f = 0$, pongamos

$$v(0) := +\infty.$$

Demuestre que para cualesquiera $f, g \in A[[X]]$ se cumplen las desigualdades

$$v(f\,g) \geq v(f) + v(g),$$
$$v(f+g) \geq \text{mín}\{v(f), v(g)\},$$

y la igualdad

$$v(fg) = v(f) + v(g)$$

si A es un dominio.

Ejercicio 2.2.

1) Sea $f \in \mathbb{R}[X]$ un polinomio real. Demuestre que si $z \in \mathbb{C}$ es una raíz compleja de f, entonces $\overline{z}$ es también una raíz.
2) Deduzca que un polinomio real de grado impar debe tener por lo menos una raíz real.
3) Demuéstrelo usando el análisis real, sin recurrir al teorema fundamental del álgebra.

Ejercicio 2.3. Demuestre que si $m > 1$ es impar, entonces $\Phi_{2m}(X) = \Phi_m(-X)$.
Sugerencia: compare las expresiones

$$\prod_{d|2m} \Phi_d(X) = X^{2m} - 1 = (X^m - 1)\,(X^m + 1) = -(X^m - 1)\,((-X)^m - 1) = -\prod_{d|m} \Phi_d(X)\,\Phi_d(-X)$$

usando la inducción sobre m.

Ejercicio 2.4. Encuentre los coeficientes en la expansión de los polinomios ciclotómicos

$$\Phi_{11}, \Phi_{12}, \Phi_{13}, \Phi_{14}, \Phi_{15}, \Phi_{16}, \Phi_{17}, \Phi_{18}, \Phi_{19}, \Phi_{20}.$$

Ejercicio 2.5 (Determinante de Vandermonde). Sea k un cuerpo y $x_0, \ldots, x_n \in k$. Demuestre que

$$V(x_0, x_1, \ldots, x_n) := \det \begin{pmatrix} 1 & x_0 & x_0^2 & \cdots & x_0^{n-1} & x_0^n \\ 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} & x_1^n \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & x_{n-1} & x_{n-1}^2 & \cdots & x_{n-1}^{n-1} & x_{n-1}^n \\ 1 & x_n & x_n^2 & \cdots & x_n^{n-1} & x_n^n \end{pmatrix} = \prod_{0\leq i<j\leq n} (x_j - x_i).$$

Ejercicio 2.6 (Interpolación polinomial). Sea k un cuerpo. Consideremos n puntos $(x_i, y_i) \in k^2$, donde $i = 0, \ldots, n$ y $x_i \neq x_j$ para $i \neq j$. Usando el ejercicio anterior, demuestre que existe un polinomio único

$$f = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 \in k[X]$$

de grado $\leq n$ tal que $f(x_i) = y_i$ para todo i.
Sugerencia: use el ejercicio anterior.

Ejercicio 2.7. Consideremos el polinomio $f = X^n - 1 \in \mathbb{F}_p[X]$. Demuestre que f no tiene raíces múltiples si y solo si $p \nmid n$.

Ejercicio 2.8. Sea A un anillo conmutativo. Para una serie de potencias $f = \sum_{n\geq 0} a_n X^n \in A[[X]]$ definamos su **derivada formal** como la serie

$$f' := \sum_{n\geq 1} n\, a_n X^{n-1}.$$

1) Demuestre que para cualesquiera $f, g \in A[[X]]$ se cumple

$$(f+g)' = f' + g', \quad (f\,g)' = f'\,g + f\,g'.$$

2) Calcule las derivadas de las siguientes series formales en $\mathbb{Q}[[X]]$:

$$\exp(X) := \sum_{n\geq 0} \frac{X^n}{n!}, \quad \log(1+X) := \sum_{n\geq 0} (-1)^{n+1} \frac{X^n}{n},$$
$$\operatorname{sen}(X) := \sum_{n\geq 0} (-1)^n \frac{X^{2n+1}}{(2n+1)!}, \quad \cos(X) := \sum_{n\geq 0} (-1)^n \frac{X^{2n}}{(2n)!}.$$

Ejercicio 2.9. Demuestre la identidad $\operatorname{sen}(X)^2 + \cos(X)^2 = 1$ en el anillo de series formales $\mathbb{Q}[[X]]$

a) calculando la derivada formal de $\operatorname{sen}(X)^2 + \cos(X)^2$;

b) directamente, analizando los coeficientes de $\operatorname{sen}(X)^2 + \cos(X)^2$.

Ejercicio 2.10 (Serie de Taylor). Demuestre que si $\mathbb{Q} \subseteq A$, entonces para $f \in A[[X]]$ se cumple

$$f = \sum_{n\geq 0} \frac{f^{(n)}(0)}{n!} X^n,$$

donde $f^{(0)} := f$ y $f^{(n)} := (f^{(n-1)})'$ para $n \geq 1$.

Ejercicio 2.11. Si $\mathbb{Q} \subseteq A$, definamos las **integrales formales** por

$$\int_0^X \left(\sum_{n\geq 0} a_n X^n \right) dX := \sum_{n\geq 0} \frac{a_n}{n+1} X^{n+1}.$$

1) Demuestre que se cumple el **teorema fundamental del cálculo**:

$$\int_0^X f'(X)\, dX = f(X) - f(0) \quad \text{y} \quad \left(\int_0^X f(X)\, dX \right)' = f(X),$$

donde $f(0)$ denota el término constante de f.

2) Demuestre que se cumple la **integración por partes**:

$$f(X)\, g(X) - f(0)\, g(0) = \int_0^X f(X)\, g'(X)\, dX + \int_0^X f'(X)\, g(X)\, dX.$$

3) Calcule las series

$$\int_0^X \exp(X)\, dX, \ \int_0^X \log(1+X)\, dX, \ \int_0^X X \exp(X)\, dX.$$

Bibliografía

[CLO2015] David A. Cox, John Little, and Donal O'Shea, *Ideals, varieties, and algorithms: An introduction to computational algebraic geometry and commutative algebra*, fourth ed., Undergraduate Texts in Mathematics, Springer, 2015. http://dx.doi.org/10.1007/978-3-319-16721-3

[Rud1989] Walter Rudin, *Principles of mathematical analysis*, 3 ed., McGraw-Hill, 1989.