Polinomios

10 de diciembre de 2018

Índice

1. **Definiciones y primeras propiedades** 1

2. **El algoritmo de la división con resto** 5

3. **Factorización** 7

4. **Criterios de irreducibilidad** 10

5. **Factorización en un número finito de pasos** 13

1. Definiciones y primeras propiedades

Sea A un anillo conmutativo.

Definición 1.1. El *conjunto de polinomios* en la indeterminada X con coeficientes en A es el conjunto de todas las sumas formales finitas

$$f = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0.$$

Este conjunto se representa por $A[X]$.

Obsérvese que X *no es una variable*. Es un elemento nuevo, indeterminado que no representa a ningún elemento de A (Al final de la edad media y en el renacimiento le llamaban "la cosa", y los que manipulaban la cosa, los algebristas, se llamaban "cosistas").

En el conjunto de polinomios definimos una suma y un producto: Sean

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

dos polinomios. Supongamos que $m \leq n$, Tomamos $b_i = 0$ para todo i verificando $n \geq i > m$. Con este convenio definimos

$$f + g = (a_n + b_n)X^n + \cdots + (a_1 + b_1)X + (a_0 + b_0).$$
$$fg = a_n b_m X^{n+m} + (a_n b_{m-1} + a_{n-1} b_m)X^{n+m-1} + \cdots + (a_1 b_0 + a_0 b_1)X + a_0 b_0.$$

Teorema 1.2. *El conjunto $A[X]$ con las dos operaciones definidas forma un anillo conmutativo que se llama* anillo de polinomios en X con coeficientes en A.

Lema 1.3. *La aplicación $\lambda : A \to A[X]$ definida por $\lambda(a) = a$ es un monomorfismo de anillos.*

Normalmente se identifica cada elemento $a \in A$ con el polinomio $\lambda(a) \in A[X]$, con lo que A es un subanillo de $A[X]$.

Definición 1.4. Para un polinomio $f = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0 \neq 0$ el mayor índice n tal que $a_n \neq 0$ se llama *grado de f* y se representa por $gr(f)$. Si $f = 0$ definimos $gr(f) = -\infty$.

Cada uno de los sumandos $a_i X^i$ se llama *monomio o término (de grado i)* del polinomio f.

El término no nulo de mayor grado se llama *término líder*. El coeficiente $a_n \neq 0$ del término líder se llama *coeficiente líder* y el término de grado cero a_0 se llama *término constante*.

Un polinomio $f = X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$ cuyo coeficiente líder vale 1 se llama *polinomio mónico*.

Un polinomio f se llama *constante* si $gr(f) \leq 0$, es decir, cuando $f \in \mathrm{Im}(\lambda)$.

Teorema 1.5. *Para cualquier anillo conmutativo A y cualesquiera polinomios $f, g \in A[X]$, se verifica*

$$gr(f + g) \leq \max(gr(f), gr(g)),$$
$$gr(fg) \leq gr(f) + gr(g).$$

Si $gr(f) \neq gr(g)$, se verifica

$$gr(f + g) = \max(gr(f), gr(g)).$$

Si A es un dominio de integridad, se tiene que

$$gr(fg) = gr(f) + gr(g).$$

Corolario 1.6. *El anillo conmutativo A es un dominio de integridad si y sólo si $A[X]$ es un dominio de integridad.*

En cualquier dominio de integridad es importante determinar el grupo de unidades y los elementos irreducible y primos, para poder estudiar sus propiedades de divisibilidad. En este sentido los primeros resultados son los siguientes.

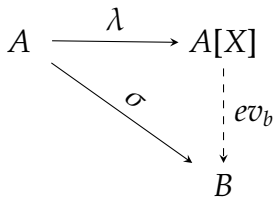
Proposición 1.7. 1. *Sea A un dominio de integridad. Los elementos invertibles de $A[X]$ son exactamente los invertibles de A.*

2. *Todo polinomio $X - a \in A[X]$ es irreducible.*

La propiedad más importante de un anillo de polinomios es la siguiente.

Teorema 1.8 (Propiedad universal del anillo de polinomios)**.** *Sea A un anillo conmutativo, $\lambda : A \to A[X]$ la inclusión de A en el anillo de polinomios. Para todo anillo conmutativo B, todo homomorfismo de anillos $\sigma : A \to B$ y todo elemento $b \in B$ existe un único homomorfismo de anillos $ev_b : A[X] \to B$ tal que $(ev_b)\lambda = \sigma$ y $ev_b(X) = b$.*

Esta propiedad se visualiza mejor en un diagrama: Dadas λ y σ existe un único ev_b que hace el siguiente diagrama conmutativo y aplica X en b:



Demostración. Sea $f = \sum_{i=0}^{n} a_i X^i$. Definimos $ev_b(f) = \sum_{i=0}^{n} \sigma(a_i) b^i$, es decir, aplicamos σ a todos los coeficientes de f, sustituimos X por b y realizamos en B las operaciones indicadas. Es rutina comprobar que ev_b es un homomorfismo de anillos, que

$$ev_b(X) = b$$

y que $ev_b \cdot \lambda = \sigma$.

Sea ahora $\tau : A[X] \to B$ otro homomorfismo de anillos que verifique las mismas propiedades y sea $f = \sum_{i=0}^{n} a_i X^i \in A[X]$ arbitrario. Entonces

$$\tau(f) = \tau(\sum_{i=0}^{n} a_i X^i) = \sum_{i=0}^{n} \tau(a_i)\tau(X)^i = \sum_{i=0}^{n} \sigma(a_i) b^i = ev_b(f),$$

luego $\tau = ev_b$ es único. □

El morfismo ev_b del teorema anterior se llama *morfismo de evaluación en b*. Se aplica sobre todo cuando σ es una inclusión, es decir que para todo $a \in A$, $\sigma(a) = a$. En este caso $ev_b(a_nX^n + \cdots + a_1X + a_0) = a_nb^n + \cdots + a_1b + a_0$ es el resultado de *evaluar f en b* y se representa por $ev_b(f) = f(b)$.

Definición 1.9. Un elemento $a \in A$ se llama *cero* o *raíz* de f si $f(a) = 0$.

Todo polinomio $f \in A[X]$ define una *aplicación polinómica* $\bar{f} : A \to A$ mediante $\bar{f}(a) = f(a)$. En general, distintos polinomios pueden definir la misma aplicación polinómica.

Ejemplo 1.10. Sea $A = \mathbb{Z}_2$ el anillo de las clases de restos módulo 2. Sean $f = 0$, $g = X^2 + X$, $h = X^3 + X$ polinomios de $\mathbb{Z}_2[X]$. Como polinomios son *distintos*, pero los tres definen la misma función polinómica $\mathbb{Z}_2 \to \mathbb{Z}_2$, a saber la función que aplica todo elemento (sólo hay dos) de $\mathbb{Z}_2$ en el cero de $\mathbb{Z}_2$.

El proceso de construir el anillo de polinomios en una indeterminada puede aplicarse a cualquier anillo conmutativo, en particular a un mismo anillo de polinomios $A[X]$: Sea Y otra indeterminada. Definimos $A[X, Y] = A[X][Y]$, el anillo de polinomios en dos indeterminadas con coeficientes en A. Sus elementos son de la forma

$$f = \sum_{i,j} a_{ij}X^iY^j,$$

donde la suma es finita (En lugar de ello se suele decir que tomamos la suma sobre todos los pares i, j pero con $a_{ij} = 0$ *para casi todo par* (i, j), es decir, para todos excepto un conjunto finito).

Mas generalmente, definimos inductivamente el anillo de polinomios en las indeterminadas $X_1, \ldots, X_n$ por la regla

$$A[X_1, \ldots, X_n] = A[X_1, \ldots, X_{n-1}][X_n]$$

. En otras palabras, consideramos a los elementos de $A[X_1, \ldots, X_n]$ como polinomios en X_n con coeficientes en $A[X_1, \ldots, X_{n-1}]$. Naturalmente existe un monomorfismo $\lambda : A \to A[X_1, \ldots, X_n]$ y A se identifica con el subanillo $\mathrm{Im}(\lambda)$ de $A[X_1, \ldots, X_n]$.

Lema 1.11. *El anillo conmutativo A es un dominio de integridad si y sólo si lo es* $A[X_1, \ldots, X_n]$

Demostración. Inducción sobre n. □

De la definición tenemos que todo elemento f de $A[X_1, \ldots, X_n]$ se escribe de manera única como

$$f = \sum a_{i_1 \ldots i_n} X_1^{i_1} \ldots X_n^{i_n}$$

Aquí $a_{i_1 \ldots i_n}$ esta determinado de manera única como el coeficiente en f del monomio $X_1^{i_1} \ldots X_n^{i_n}$. Formalmente la suma anterior es infinita, pero de hecho sólo un número finito de coeficientes son distintos de cero. Ya que las indeterminadas conmutan entre sí con los elementos de A, el anillo $A[X_1, \ldots, X_n]$ depende simétricamente de las X_i; así que X_n no juega ningún papel especial. Podíamos haber escrito f como un polinomio en X_1 con coeficientes en $A[X_2, \ldots, X_n]$ o escoger cualquier otra X_i.

Definición 1.12. Cada producto $M_i = X_1^{i_1} \dots X_n^{i_n}$ se llama *monomio primitivo*; el término correspondiente $a_{i_1 \dots i_n} X_1^{i_1} \dots X_n^{i_n}$ se llama *monomio* o *término monomial*; su *grado total* (o sencillamente *grado*) es $\sum i_j$, y el *grado en* X_j es i_j. El *grado de* f es el máximo de los grados de sus términos no nulos.

Por ejemplo $f = 2X_1^5 X_2^3 X_3 - X_1^2 X_3^3 + 7X_2^6$ es de grado 5 en X_1, de grado 6 en X_2 y de grado 3 en X_3; el grado total de f es 9.

Definición 1.13. Un polinomio en el que todos los términos tienen el mismo grado total se llama *polinomio homogéneo* o también una *forma*. En una indeterminada las únicas formas son los monomios, pero ya para dos indeterminadas puede haber otros, por ejemplo las forma cuadráticas $aX^2 + bXY + cY^2$.

Un criterio práctico de homogeneidades es el siguiente resultado.

Lema 1.14. *El polinomio $f \in A[X_1, \dots, X_n]$ es homogéneo de grado k si y sólo si para otra indeterminada t se verifica que*

$$f(tX_1, \dots, tX_n) = t^k f(X_1, \dots, X_n).$$

A veces es conveniente ordenar los monomios. Incluso para propósito tan sencillo como escribir la expresión total de un polinomio es necesario un orden total de los monomios. Con frecuencia se usa el *orden lexicográfico* definido de la siguiente forma. Entre monomios de distinto grado grado total, el de mayor grado precede al de menor grado. Entre monomios del mismo grado total, el monomio $X_1^{i_1} \dots X_n^{i_n}$ precede a $X_1^{j_1} \dots X_n^{j_n}$ si la primera diferencia no nula $i_1 - j_1, \dots i_n - j_n$ es positiva.

Por ejemplo, $X_1^3 X_2 X_3^2$ precede a $X_1^3 X_3^3$ y es precedido por $X_1^3 X_2^2 X_3$. En cualquier polinomio, el primer término monomial (en el orden lexicográfico) entre los términos de grado máximo se llama el *término líder*.

2. El algoritmo de la división con resto

Teorema 2.1 (Algoritmo general de división). *Sea A un anillo conmutativo y sean $f, g \in A[X]$ con el coeficiente líder de g invertible. Entonces existen únicos $q, r \in A[X]$ tales que $f = qg + r$ y $gr(r) < gr(g)$.*

Demostración. Inducción sobre $gr(f)$. Sean $f = a_n X^n + \dots + a_1 X + a_0$ y $g = b_m X^m + \dots + b_0$. Si $gr(f) < gr(g)$, tomamos $q = 0$ y $r = f$. Sea ahora $gr(f) = n \geq gr(g) = m$. Definimos

$$f_1 = f - (a_n b_m^{-1}) X^{n-m} g \tag{2.1}$$

Es inmediato que $gr(f_1) < gr(f)$ y por inducción existen $q_1, r \in A[X]$ tales que $f_1 = q_1 g + r$ con $gr(r) < gr(g)$. Despejando en 2.1 vemos que

$$f = (a_n b_m^{-1}) X^{n-m} g + f = ((a_n b_m^{-1}) X^{n-m} g + q_1) g + r.$$

Definimos $q = (a_n b_m^{-1}) X^{n-m} g + q_1$ y tenemos demostrada la existencia de cociente y resto.

Para ver la unicidad, sea $f = qg + r = q_1 g + r_1$. Trasponiendo términos tenemos $(q - q_1)g = r_1 - r$. Como el coeficiente líder de g es invertible se verifica

$$gr(g) > \text{máx}(gr(r), gr(r_1) \geq gr(r - r_1) = gr((q - q_1)g) = gr(q - q_1) + gr(g),$$

lo que implica que $gr(q - q_1) = -\infty$ y $q - q_1 = 0$. Luego $q = q_1$ y por tanto $r = r_1$. □

Corolario 2.2. *Sea K un cuerpo. Entonces $K[X]$ es un anillo euclídeo*

Demostración. En un cuerpo, todo elemento no nulo es invertible. Así que para todo polinomio no nulo g el coeficiente líder es invertible. Por el teorema anterior, para cualesquiera polinomios f, g con $g \neq 0$ existen únicos q, r tales que $f = qg + r$ con $gr(r) < gr(g)$. Esta es la segunda condición en la definición de anillo euclídeo.

Por otro lado todo cuerpo es un dominio de integridad, así que para dos polinomios no nulos f, g se verifica $gr(fg) = gr(f) + gr(g) \geq gr(f)$. Ésta es la primera condición de dicha definición.

Por tanto $K[X]$ es euclídeo respecto a la función grado. □

Corolario 2.3 (Teorema del resto)**.** *Sea A un anillo conmutativo, a un elemento de A y $f \in A[X]$ un polinomio. Entonces existe un $q \in A[X]$ tal que*

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

y $(X - a)$ divide a f si y sólo si $f(a) = 0$.

Teorema 2.4. *Sea A un dominio de integridad y sea $f \in A[X]$. Sean $a_1, \ldots, a_m \in A$ elementos distintos tales que $f(a_i) = 0$ para $i \in \{1, \ldots m\}$. Entonces $((X - a_1) \ldots (X - a_m))$ divide a f.*

Demostración. Inducción sobre m. Para $m = 1$ esto es parte del teorema del resto. Sea $m > 1$. Por inducción, $f = (X - a_1) \ldots (X - a_{m-1})g$ con $g \in A[X]$. Evaluamos en a_m:

$$0 = f(a_m) = (a_m - a_1) \ldots (a_m - a_{m-1})g(a_m)$$

Como los a_i distintos, $a_m - a_i \neq 0$ para $i \in \{1, \ldots m - 1\}$. Como A es un dominio de integridad, $g(a_m) = 0$. Por el teorema del resto $g = (X - a_m)g_1$. Sustituyendo en la expresión de f nos queda $f = (X - a_1) \ldots (X - a_{m-1})(X - a_m)g_1$ y por tanto el producto $((X - a_1) \ldots (X - a_m))$ divide a f. □

Corolario 2.5. *Sea A un dominio de integridad y $f \in A[X]$, $f \neq 0$. El número de raíces de f en A es menor o igual al grado de f.*

Ejemplo 2.6. El teorema y corolarios anteriores son falsos para anillos conmutativos generales: Sea $f = X^2 - 1 \in \mathbb{Z}_8[X]$. En $\mathbb{Z}_8$ el polinomio f tiene cuatro raíces distintas: $1, 3, 5, 7$. Además $(X - 1)(X - 3)$ no divide a f.

Corolario 2.7. *Sea A un dominio de integridad, $a_1, \ldots, a_{n+1}$ elementos distintos de A y $f, g \in A[X]$ tales que $gr(f), gr(g) \leq n$ y $f(a_i) = g(a_i)$ para $i \in \{1, \ldots n + 1\}$. Entonces $f = g$.*

Demostración. El polinomio $f - g$ tiene grado menor o igual a n y tiene $n + 1$ raíces distintas. Luego tiene que ser el polinomio cero. □

Corolario 2.8. *Sea A un dominio de integridad infinito y sean $f, g \in A[X]$ tales que para todo $a \in A$ se verifica $f(a) = g(a)$. Entonces $f = g$.*

Este último corolario nos dice que si A es un dominio de integridad infinito, la correspondencia entre polinomios y funciones polinómicas es biyectiva.

El anterior corolario se generaliza a varias indeterminadas:

Teorema 2.9. *Sea A un dominio de integridad infinito y sea $f \in A[X_1, \ldots, X_n]$ tal que para cualesquiera $a_1, \ldots, a_n \in A$ se verifica $f(a_1, \ldots, a_n) = 0$. Entonces $f = 0$.*

Demostración. Inducción sobre n. □

Corolario 2.10 (Principio de irrelevancia de desigualdades algebraicas)**.** *Sea A un dominio de integridad infinito y sean $f, g, h \in A[X]$, $h \neq 0$ tales que para $a_1, \ldots, a_n \in A$, $h(a_1, \ldots, a_n) \neq 0$ implica $f(a_1, \ldots, a_n) = g(a_1, \ldots, a_n)$. Entonces $f = g$.*

Demostración. El polinomio $(f - g)h$ se anula sobre todos los $a_1, \ldots, a_n \in A$. Luego $(f - g)h = 0$. Como $A[X_1, \ldots, X_n]$ es un dominio de integridad y $h \neq 0$, necesariamente $f - g = 0$. □

El principio de irrelevancia de desigualdades algebraicas se llama también *propiedad de densidad*, por su interpretación en geometría algebraica.

3. Factorización

Sea K un cuerpo. El anillo $K[X]$ es un dominio euclídeo y por tanto también es un dominio de factorización única.Vamos ahora a estudiar la factorización de polinomios en ese anillo. En primer lugar caracterizamos los elementos invertibles.

Lema 3.1. *Las unidades de $K[X]$ son los polinomios constantes no nulos.*

El primer teorema proporciona algunos polinomios irreducibles:

Teorema 3.2. *Los polinomios de grado uno son irreducibles en $K[X]$.*
Estos son los únicos irreducibles si y sólo si todo polinomio de $K[X]$ de grado positivo tiene una raíz en K.

Demostración. El primer resultado se deduce del teorema del grado.

Supongamos que todo polinomio irreducible es de grado uno. El anillo $K[X]$ es un dominio de factorización única, por tanto todo polinomio f no constante es divisible por un irreducible, así que existe un $b_1X - b_0$ con $b_1 \neq 0$ tal que $f = (b_1X - b_0)q$. Pero entonces $f(b_0/b_1) = 0$ y f tiene una raíz $b_0/b_1 \in K$.

A la inversa, si todo polinomio no constante tiene una raíz en K, sea f un polinomio irreducible y sea $a \in K$ tal que $f(a) = 0$. Por el teorema del resto $X - a$ divide a f. Como f es irreducible, debe ser asociado a $X - a$ y por tanto es de grado uno. □

Definición 3.3. Un cuerpo en que todo polinomio no constante tiene una raíz se llama *algebraicamente cerrado*.

El llamado *teorema fundamental del álgebra* dice que el cuerpo $\mathbb{C}$ de los números complejos es algebraicamente cerrado. Este hecho fue conjeturado por D'Alembert y demostrado por primera vez por el gran Gauss en su tesis doctoral. Dicha demostración tenía una laguna, pero a lo largo de su vida Gauss proporcionó cinco demostraciones correctas distintas. Sin embargo todas esas demostraciones utilizan bastante maquinaria analítica (como es propio, porque la construcción de $\mathbb{C}$ se basa en $\mathbb{R}$ que es el objeto de estudio del análisis matemático). Desde un punto de vista puramente algebraico, el hecho de que $\mathbb{C}$ sea algebraicamente cerrado es relativamente poco importante. Es más importante demostrar que todo cuerpo K es un subcuerpo de otro cuerpo $\bar{K}$ algebraicamente cerrado.

La factorización de polinomios con coeficientes en un cuerpo algebraicamente cerrado (como $\mathbb{C}$) es muy sencilla: todo polinomio no constante es un producto de polinomios de grado uno.

Sobre los números reales es casi igual de fácil: todo polinomio no constante es un producto de polinomios irreducibles de grado uno y dos. Sobre el cuerpo $\mathbb{Q}$ de los números racionales la situación es muy diferente: existen polinomios irreducibles de todos los grados y para un polinomio $f \in \mathbb{Q}[X]$ dado puede ser penoso hallar sus factores. El resto de esta sección y las dos siguientes van encaminadas a intentar factorizar polinomios en $\mathbb{Q}[X]$.

Vamos a establecer los teoremas en un contexto más general. Sea A un dominio de factorización única y sea K su cuerpo de fracciones.

Definición 3.4. Para todo polinomio no nulo $f = a_nX^n + \cdots + a_0 \in A[X]$ llamamos *contenido de* f a $\mathrm{c}(f) = \mathrm{m.\,c.\,d.}(a_n, \ldots, a_0)$.

Un polinomio $f \in A[X]$ se llama *primitivo* si $\mathrm{c}(f) = 1$.

Lema 3.5. *Todo polinomio $f \in A[X]$ se expresa como $f = \mathrm{c}(f)f_1$ con f_1 primitivo. Además, si $f = ag$ con g primitivo y $a \in A$, entonces a es asociado a $\mathrm{c}(f)$.*

Teorema 3.6 (Lema de Gauss)**.** *El producto de dos polinomios primitivos es primitivo.*

Demostración. Sean $f = a_nX^n + \cdots + a_0$, $g = b_mX^m + \cdots + b_0$ dos polinomios primitivos de $A[X]$. Sea $p \in A$ un primo de A arbitrario. Como f, g son primitivos, $\mathrm{m.\,c.\,d.}(a_n, \ldots, a_0) = 1 = \mathrm{m.\,c.\,d.}(b_m, \ldots, b_0)$ y en cada uno de ellos existe por lo menos un coeficiente no

divisible por p. Sean a_i y b_j los primeros coeficientes no divisibles por p, de forma que para todo $k > i$, p divide a a_k y para todo $l > j$, p divide a b_l. En el polinomio producto fg consideramos el coeficiente del término de grado $i + j$:

$$c_{i+j} = (a_{i+j}b_0 + \cdots + a_{i+1}b_{j-1}) + a_ib_j + (a_{i-1}b_{j+1} + \cdots + a_0b_{i+j}).$$

Todos los términos del primer paréntesis (que puede ser vacío) son divisibles por p, como también lo son todos los términos del segundo paréntesis (que también puede ser vacío). Así que $c_{i+j} = q_1p + a_ib_j + q_2p$ con $q_1, q_2 \in A$. Si p dividiese a c_{i+j}, necesariamente $p \mid a_ib_j$ y como p es primo, dividiría a uno de los factores, lo cual es imposible. Luego p no divide a c_{i+j}.

Hemos demostrado que para todo primo $p \in A$ existe un coeficiente del producto $h = fg$ que no es divisible por p. Luego el máximo común divisor de los coeficientes de h es 1 y h es primitivo. □

Corolario 3.7. *Para dos polinomios $f, g \in A[X]$, el contenido del producto es el producto de los contenidos, es decir* $\mathrm{c}(fg) = \mathrm{c}(f)\,\mathrm{c}(g)$.

Teorema 3.8. *Sea $f \in A[X]$ primitivo. Entonces f es irreducible en $A[X]$ si y sólo si es irreducible en $K[X]$.*

Demostración. Supongamos que $f = gh$ es una factorización de f en $K[X]$. Multiplicando por un denominador común obtenemos $k = af = bg_1h_1$, donde $a, b \in A$ y los polinomios g_1, h_1 son primitivos. Por el lema de Gauss el producto g_1h_1 también es primitivo. Luego a y b son ambos contenidos del polinomio k, luego son asociados. Sea $b = ua$ con u invertible. Sustituyendo y simplificando nos queda $f = (ug_1)h_1$ donde $ug_1, h_1 \in A[X]$ son primitivos y $gr(ug_1) = gr(g)$, $gr(h_1) = gr(h)$. Luego f es factorizable en $A[X]$.

A la inversa, sea $f = gh$ una factorización en $A[X]$. Los polinomios f, g no son constantes y tienen sus coeficientes en K, luego esa misma es una factorización en $K[X]$.

Hemos visto que f es reducible en $A[X]$ si y sólo si es reducible en $K[X]$. El contrarrecíproco es el resultado buscado. □

Corolario 3.9. *Los elementos irreducibles en $A[X]$ son de uno de los siguientes tipos:*

1. *polinomios de grado cero que son irreducibles en A,*
2. *polinomios primitivos que son irreducibles en $K[X]$.*

Teorema 3.10. *Sea A un dominio de integridad. El anillo A es un dominio de factorización única si y sólo si $A[X]$ es un dominio de factorización única.*

Demostración. En primer lugar supongamos que $A[X]$ es un dominio de factorización única. Los elementos de A pertenecen a $A[X]$ y por tanto descomponen de manera única como producto de irreducibles en $A[X]$, necesariamente todos de grado cero. Por tanto todo $a \in A$ descompone de manera única como producto de irreducibles en A. Luego A es un dominio de factorización única.

A la inversa sea A un dominio de factorización única. Sea $f \in A[X]$ no cero. Descomponemos $f = \mathrm{c}(f)f_1$ con f_1 primitivo. Descomponemos $\mathrm{c}(f) = p_1 \dots p_t$ en producto de irreducibles en A y $f_1 = q_1 \dots q_s$ en producto de primitivos irreducibles en $K[X]$. Entonces $f = p_1 \dots p_t q_1 \dots q_s$ es una descomposición de f en producto de irreducibles en $A[X]$.

Sea ahora p un irreducible en $A[X]$ y sean $f, g \in A[X]$ tales que p divide al producto fg.

Si $gr(p) = 0$, entonces p es irreducible y primo en A y p divide al contenido $c(fg) = c(f)\,c(g)$. Luego p divide a $c(f)$ (en cuyo caso divide a f) o divide a $c(g)$ (en cuyo caso divide a g. Luego p es primo.

Si $gr(p) > 0$, entonces p es un polinomio primitivo irreducible y por tanto primo en $K[X]$. Luego p divide a f o a g en $K[X]$. Sea q un polinomio en $K[X]$ tal que $f = pq$. Extrayendo contenidos, vemos que q pertenece a $A[X]$ y por tanto p divide a f en $A[X]$. Luego p es primo en $A[X]$.

Hemos demostrado que todo polinomio de $A[X]$ descompone como producto de irreducibles y que todo irreducible es primo. Luego $A[X]$ es un dominio de factorización única. □

Corolario 3.11. *Sea A un dominio de integridad. Entonces A es un dominio de factorización única si y sólo si $A[X_1, \ldots, X_n]$ es un dominio de factorización única.*

Corolario 3.12. *Sea K un cuerpo. El anillo $K[X_1, \ldots, X_n]$ es un dominio de factorización única.*

4. Criterios de irreducibilidad

En esta sección A es un dominio de factorización única y K es su cuerpo de fracciones, salvo mención expresa en contrario.

La factorización en el anillo de polinomios $A[X]$ presenta dos problemas prácticos relacionados entre sí.

1. Dado un polinomio $f \in A[X]$ determinar si es reducible o irreducible.
2. Si f es reducible, factorizarlo en irreducibles.

Para el primer caso muchas veces basta tener criterios suficientes (es decir, que si un polinomio satisface el criterio, es irreducible. Si no lo satisface no podemos decir nada). Evidentemente, una solución general del segundo punto incluiría criterios necesarios y suficientes para que un polinomio dado sea irreducible.

Empezamos determinando los factores de grado uno.

Proposición 4.1. *Sean $f = a_nX^n + \cdots + a_0, g = b_mX + b_0 \in A[X]$ con $a_n, b_m \neq 0$. Si g divide a f, necesariamente b_m divide a a_n y b_0 divide a a_0.*

Demostración. Sea $h = c_kX^k + \cdots + c_0 \in A[X]$ tales que $f = gh$. Entonces el coeficiente líder del producto es $a_n = b_mc_k$ y el término independiente es $a_0 = b_0c_0$. □

Corolario 4.2 (Regla de Ruffini). *Sea $f = a_nX^n + \cdots + a_0$ y sea $a/b \in K$ tal que $\text{m. c. d.}(a, b) = 1$ y $f(a/b) = 0$. Entonces a divide a a_0 y b divide a a_n.*

La regla de Ruffini la describió ya Newton en su libro *Arithmetica Universalis* (publicado en 1707, cincuenta y ocho años antes del nacimiento de Ruffini), para determinar las raíces racionales y enteras de polinomios con coeficientes enteros. El corolario anterior permite usarla para hallar las raíces de polinomios con coeficientes en cualquier dominio de fatorización única.

Ejemplo 4.3. Sea $f = X^4 + 4 \in \mathbb{Z}[X]$. Cualquier raíz racional suya debe ser de la forma a/b con $b \mid 1$ y $a \mid 4$. Luego las posibles raíces racionales de f son $1, -1, 2, -2, 4, -4$. Un cálculo rápido muestra que ninguno de estos números es raíz de f, luego el polinomio f no tiene raíces en $\mathbb{Q}$.

Ejemplo 4.4. Sea ahora $f = X^4 + 4 \in \mathbb{J}[X]$. Los divisores de 4 son ahora $1, 1+i, 2, 2+2i, 4$ y sus asociados (todos los productos por las unidades $\pm 1, \pm i$). Un nuevo cálculo muestra que $f(1+i) = f(1-i) = f(-1+i) = f(-1-i) = 0$, luego f tiene cuatro raíces en $\mathbb{J}$ y factoriza como

$$X^4 + 4 = (X - (i+i))(X - (i-i))(X - (-i+i))(X - (-i-i)).$$

Un criterio de aplicación muy rápida es debido a un discípulo de Gauss.

Teorema 4.5 (Criterio de Eisenstein). *Sea $f = a_n X^n + \cdots + a_0$ un polinomio primitivo y sea $p \in A$ un primo tal que $p \nmid a_n$, $p \mid a_i$ para $i \in \{n-1, \ldots, a_0\}$ y $p^2 \nmid a_0$. Entonces f es irreducible en $A[X]$.*

Demostración. Supongamos que f es reducible, $f = gh$ con $g = b_m X^m + \cdots + b_0$ y $h = c_r X^r + \cdots + c_0$ con $m, r \geq 1$ y $n = m + r$. Como p no divide a $a_n = b_m c_r$, necesariamente $p \nmid b_m$ y $p \nmid c_r$. Como p divide a $a_0 = b_0 c_0$, p debe dividir a uno de los factores, sea $p \mid b_0$. Entonces p no divide a c_0 porque $p^2 \nmid a_0 = b_0 c_0$. Sea i tal que $p \nmid b_i$ pero $p \mid b_j$ para todo $j < i$. El coeficiente en f del término de grado i es $a_i = b_i c_0 + (b_{i-1} c_1 + \cdots + b_0 c_i)$. Todos los términos del paréntesis son divisibles por p y $p \nmid b_i c_0$, luego $p \nmid a_i$. Pero $i \leq m < n$, luego por la hipótesis $p \mid a_i$, contradicción. □

Ejemplo 4.6. Sea $f = 2X^5 - 6X^3 + 9X^2 - 15 \in \mathbb{Z}[X]$. El polinomio f es primitivo porque m. c. d.$(2, -6, 9, -15) = 1$. El primo 3 divide a todos los coeficientes menos al líder, y $3^2 = 9$ no divide al término independiente, luego f es irreducible en $\mathbb{Z}[X]$.

Ejemplo 4.7. Sea $f = Y^3 + X^2Y^2 + XY + X \in K[X, Y]$ con K un cuerpo arbitrario. Como $K[X, Y] = A[Y]$ con $A = K[X]$ dominio euclídeo, aplicando el criterio de Eisenstein con el primo $X \in A[X]$ vemos que f es irreducible en $K[X, Y]$.

A veces el polinomio dado no satisface las condiciones del criterio de Eisenstein pero un transformado sencillo sí las satisface. Del siguiente lema podemos deducir entonces la irreducibilidad del polinomio original.

Lema 4.8. *Sea A un dominio de integridad y sea $f \in A[X]$. Sea $a \in A$ arbitrario y sea $f_a(X) = f(X + a)$. Entonces f descompone como $f = gh$ con $gr(g) > 0$ y $gr(h) > 0$ si y sólo si $f_a = g_a h_a$. En este caso $gr(g_a) = gr(g) > 0$ y $gr(h_a) = gr(h) > 0$.*

Demostración. Cálculo trivial. □

Corolario 4.9. *Sea A un dominio de factorización única y sea $f \in A[X]$ primitivo. Sea $a \in A$ arbitrario tal que f_a sea primitivo. Entonces f es irreducible si y sólo si f_a es irreducible.*

Ejemplo 4.10. Sea $f = X^4 + 1 \in \mathbb{Z}[X]$. No podemos aplicar directamente el criterio de Eisenstein a f. Pero

$$f_1 = f(X+1) = (X+1)^4 + 1 = X^4 + 4X^3 + 6X^2 + 4X + 2$$

satisface las condiciones del criterio de Eisenstein con $p = 2$. Luego f_1 es irreducible en $\mathbb{Z}[X]$ y por tanto también lo es f.

Ejemplo 4.11. (Este ejemplo se remonta a Gauss). Sea $p \in \mathbb{Z}$ un primo. El polinomio

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

se llama *p-ésimo polinomio ciclotómico*. Vamos a comprobar que Φ_p es irreducible en $\mathbb{Z}[X]$ (y por tanto en $\mathbb{Q}[X]$): Calculamos el desarrollo de $f = \Phi_p(X+1)$:

$$f = \frac{(X+1)^p - 1}{(X+1) - 1} = \frac{(\sum_{i=0}^{p} \binom{p}{i} X^i) - 1}{X} = \sum_{i=1}^{p} \binom{p}{i} X^{i-1}.$$

Ahora p no divide al coeficiente líder $\binom{p}{p} = 1$, p divide a $\binom{p}{i}$ para $i \in \{p-1, \ldots, 1\}$ y p^2 no divide al término independiente $\binom{p}{1} = p$. Luego f es irreducible en $\mathbb{Z}[X]$ y por tanto también lo es Φ_p.

A veces se utiliza otra transformación del polinomio.

Definición 4.12. Sea $f = a_n X^n + a_{n-1} X^{n-1} \cdots + a_1 X + a_0 \in A[X]$ un polinomio con $a_n, a_0 \neq 0$. Se llama *polinomio recíproco de* f al polinomio

$$f_{rec} = a_0 X^n + a_1 X^{n-1} + \cdots + a_{n-1} X + a_n = X^n f\left(\frac{1}{X}\right).$$

Lema 4.13. *Sea $f \in A[X]$ primitivo. Entonces f es irreducible en $A[X]$ si y sólo si f_{rec} es irreducible.*

Demostración. Los coeficientes de f_{rec} son los mismos que los de f, luego f_{rec} es primitivo. Sea ahora $f = gh$ con $m = gr(g), r = gr(h)$ y $n = gr(f) = m + r$. Entonces

$$f_{rec} = X^n f\left(\frac{1}{X}\right) = X^m X^r g\left(\frac{1}{X}\right) h\left(\frac{1}{X}\right) = g_{rec} h_{rec}. \qquad \square$$

Ejemplo 4.14. Sea $f = 6X^4 + 9X^3 - 3X^2 + 1 \in \mathbb{Z}[X]$. El primo $p = 3$ divide a todos los coeficientes menos al término independiente y $3^2 = 9$ no divide al coeficiente líder, luego f es irreducible.

Cuando se puede aplicar, el criterio de Eisenstein es una prueba muy rápida de irreducibilidad. Pero son muy pocos los polinomios a los que es aplicable. Existe otro criterio que se puede aplicar a mas polinomios y aunque falle, los resultados que se obtienen en su aplicación son útiles para intentar posteriormente la factorización del polinomio.

Todo homomorfismo de anillos $\sigma : A \to B$ define un homomorfismo $A[X] \to B[X]$ que también se denota por σ de la siguiente forma: Sea $f = a_n X^n + \cdots + a_0$. Entonces $\sigma(f) = \sigma(a_n) X^n + \cdots + \sigma(a_0)$.

Proposición 4.15. *Sean A, B dos dominios de integridad con cuerpos de fracciones respectivos K y L. Sea $\sigma : A \to B$ un homomorfismo de anillos y sea $f \in A[X]$ un polinomio tal que $gr(\sigma(f)) = gr(f)$. Si $f = gh$, entonces $\sigma(f) = \sigma(g)\sigma(h)$ con $gr(\sigma(g)) = gr(g)$ y $gr(\sigma(h)) = gr(h)$.*

Corolario 4.16 (Criterio de reducción)**.** *Si $\sigma(f)$ es irreducible en $L[X]$, entonces f es irreducible en $K[X]$.*

Usualmente este criterio se aplica con $A = \mathbb{Z}$, $K = \mathbb{Q}$, $B = L = \mathbb{Z}_p$ y $\sigma : \mathbb{Z} \to \mathbb{Z}_p$ la proyección canónica que lleva cada entero n en su clase módulo p, o sea $\sigma(n) = \bar{n} = [n]_p$. En este caso se suele denotar $\sigma(f) = \bar{f}$.

Ejemplo 4.17. Sea $p \in \mathbb{Z}$ un número primo. El polinomio $X^p - X - 1 \in \mathbb{Z}_p[X]$ es irreducible, luego $f = X^p - X - 1$ es irreducible en $\mathbb{Z}[X]$.

De la misma forma el polinomio $f = X^5 - 5X^4 - 6X - 1 \in \mathbb{Z}[X]$ es irreducible en $\mathbb{Z}[X]$ (porque módulo 5, $\sigma(f) = X^5 - X - 1 \in \mathbb{Z}_5[X]$).

El inverso del criterio de irreducibilidad es falso.

Ejemplo 4.18. El polinomio $f = X^3 - 3 \in \mathbb{Z}[X]$ es irreducible por el criterio de Eisenstein, pero módulo 2 $\sigma(f) = (X + 1)(X^2 + X + 1)$, luego puede ocurrir perfectamente que f sea irreducible y $\sigma(f)$ no lo sea.

La proposición 4.15 puede usarse combinando la información sobre los factores de f que se obtiene utilizando diversos primos.

Ejemplo 4.19. Sea $f = X^5 - 6X^4 + 5X^2 - X + 2$. Módulo 2 tenemos $\bar{f} = X^5 + X^2 + X = X(X^4 + X + 1)$ con ambos factores irreducibles. Si f es reducible, debe factorizar como producto de un polinomio de grado 1 por otro de grado 4.

Reduciendo módulo 3 queda $\bar{f} = X^5 - X^2 - X - 1 = (X^2 + 1)(X^3 - X - 1)$ con ambos factores irreducibles, así que si f fuese reducible debería factorizar como producto de un polinomio de grado 2 por otro de grado 3. Luego las factorizaciones módulo 2 y tres son incompatibles y f es irreducible en $\mathbb{Z}[X]$.

Ejemplo 4.20. Sea $f = X^4 - 22X^2 + 1 \in \mathbb{Z}[X]$. Reduciendo módulo 2 obtenemos $\bar{f} = X^4 + 1 = (X + 1)^4$, lo que no nos da información interesante. Módulo 3 es $\bar{f} = X^4 + 2X^2 + 1 = (X^2 + 1)^2$, luego si f factoriza en $\mathbb{Z}[X]$, debe hacerlo como producto de dos polinomios de grado 2, $f = gh$. Además los términos constantes de g y h deben ser divisores de 1 y congruentes con 1 módulo 3, luego ambos valen 1.

Supongamos que $f = (X^2 + aX + 1)(X^2 + bX + 1) = X^4 + (a + b)X^3 + (ab + 2)X^2 + (a + b)X + 1)$. Comparando coeficientes debe ser $a + b = 0$ y $ab + 2 = -22$, así que $b = -a$ y $a^2 = 24$. Esta última ecuación no tiene solución con a entero, luego la factorización es imposible y f es irreducible.

5. Factorización en un número finito de pasos

Si el polinomio dado f es reducible, el problema es determinar los factores de f en un número finito de pasos (y en un tiempo razonable). En el libro *Arithmetica Universalis* citado antes, Newton describe cómo hallar los factores cuadráticos de un polinomio con coeficentes enteros. Esta es la traslación de dicho método a dominios de factorización única.

Sea A un dominio de factorización única con un número finito de unidades y sea $f = gh \in A[X]$ con

$$f = a_n X^n + \cdots + a_0$$
$$g = b_2 X^2 + b_1 X + b_0$$

Entonces b_2 divide a a_n, b_0 divide a a_0 y $g(1) = b_2 + b_1 + b_0$ divide a $f(1) = a_n + \cdots + a_0$. Estas condiciones limitan a un número finito las posibilidades para b_2, b_0 y b_1. Para cada una de las ternas (b_2, b_1, b_0) posibles construimos el polinomio g y probamos a dividir f por g. Así se determinan todos los factores cuadráticos de f.

Para limitar aún más el conjunto de posibles divisores se utiliza la condición de que $g(-1) = b_2 - b_1 + b_0$ divide a la suma alternada $(-1)^n f(-1) = a_n - a_{n-1} + \cdots \pm 1$. Además podemos utilizar la información que hayamos obtenido reduciendo diversos primos.

Ejemplo 5.1. Sea $f = X^4 + 4 \in \mathbb{Z}[X]$. Usando la regla de Ruffini vemos que f no tiene raíces enteras. Sea $g = b_2X^2 + b_1X + b_0$ un factor de f. Como f es mónico, podemos tomar $b_2 = 1$. Reduciendo módulo 2 tenemos $\bar{f} = X^4 = \bar{g}\bar{h}$, luego los términos constantes de g y del cociente h son pares. Como su producto es 4, necesariamente $b_0 = \pm 2$. Módulo 3 tenemos $\bar{f} = X^4 + 1 = (X^2 + X - 1)(X^2 - X - 1)$, luego $b_0 \equiv -1 \pmod 3$, lo que nos deja $b_0 = 2$.

Ahora $1 + b_1 + 2 = b_1 + 3$ divide a $f(1) = 5$, lo que se verifica sólo para $b_1 \in \{-8, -4, -2, 2\}$ y $1 - b_1 + 2 = -b_1 + 3$ divide a $f(-1) = 5$, lo que reduce las posibilidades a $b_1 \in \{-2, 2\}$. Así que los únicos divisores de grados dos posibles son $g_1 = X^2 + 2X + 2$ y $g_2 = X^2 - 2X + 2$. Un cálculo fácil muestra que $f = g_1 g_2$.

El anterior método de Newton fué extendido en 1793 por Friedrich von Schubert, quien mostró cómo hallar todos los factores de grado m en un número finito de pasos. Unos 90 años después Leopoldo Kronecker descubrió independientemente el método de Schubert. Desgraciadamente el método es muy ineficiente cuando $gr(f) \geq 5$ y es mejor utilizar métodos de reducción (descritos en [**?**] y [**?**]) . El método de Kronecker se describe en la siguiente demostración.

Teorema 5.2 (Kronecker)**.** *Sea A un dominio de factorización única con un número finito de unidades. Entonces es posible descomponer cualquier polinomio $f \in A[X]$ en factores irreducibles en un número finito de pasos.*

Demostración. Dado un polinomio $f \in A[X]$, el método consiste en determinar para cada $m < n/2$ un conjunto finito $\mathcal{S}$ de polinomios entre los que están todos los divisores de f de grado menor o igual a m. Posteriormente se prueba a dividir f por cada uno de los polinomios del conjunto $\mathcal{S}$ y así determinamos los divisores de grado menor o igual a m.

Si $f = gh$, para todo $a \in A$ se verifica que $f(a) = g(a)h(a)$, luego $g(a)$ divide a $f(a)$. Sean $a_0, \ldots, a_m \in A$ elementos distintos. Para cada $i \in \{0, \ldots, m\}$ sea D_i el conjunto de divisores de $f(a_i)$. Para cada sucesión $\mathbf{b} = (b_0, \ldots, b_m) \in D_0 \times \cdots \times D_m$ sea $g_{\mathbf{b}}$ el único polinomio de grado menor o igual a m que verifica $g_{\mathbf{b}}(a_i) = b_i$, $i \in \{0, \ldots, m\}$ (el polinomio $g_{\mathbf{b}}$ es el *polinomio de interpolación*, que se obtiene por uno de los métodos de Newton o de Lagrange). El conjunto $\mathcal{S} = \{g_{\mathbf{b}} \mid \mathbf{b} \in D_0 \times \cdots \times D_m\}$ es finito y contiene a todos los divisores de f de grado menor o igual a m. □

En la práctica se achica bastante el conjunto $\mathcal{S}$ utilizando la información que hayamos obtenido por reducción módulo diversos primos, igual que hicimos antes en el ejemplo 5.1.

Ejemplo 5.3. Sea $f = X^6 - X^5 - X^4 + X^3 + X^2 - X - 1 \in \mathbb{Z}[X]$. Queremos encontrar los factores de grado menor o igual a tres, así que evaluamos f en cuatro (=3+1) puntos distintos. Elegimos los puntos $-2, -1, 0, 1$. Evaluamos: $f(-2) = 77$, $f(-1) = 1$, $f(0) = -1$, $f(1) = -1$. El conjunto $D_0 \times \cdots \times D_3 = \{\pm 1, \pm 7, \pm 11, \pm 77\} \times \{\pm 1\} \times \{\pm 1\} \times \{\pm 1\}$,así que en total hay que calcular $8 \cdot 2 \cdot 2 \cdot 2 = 64$ polinomios. Usando los interpoladores de Lagrange, estos polinomios son

$$\begin{aligned} f_b &= b_0 \frac{(X+1)X(X-1)}{(-2+1)(-2)(-2-1)} + b_1 \frac{(X+2)X(X-1)}{(-1+2)(-1)(-1-1)}, \\ &+ b_2 \frac{(X+2)(X+1)(X-1)}{(0+2)(0+1)(0-1)} + b_3 \frac{(X+2)(X+1)X}{(1+2)(1+1)(1)}, \\ &= b_0 \frac{X^3 - X}{-6} + b_1 \frac{X^3 + X^2 - 2X}{2} + b_2 \frac{X^3 + 2X^2 - X - 2}{-2} + b_3 \frac{X^3 + 3X^2 + 2X}{6}. \end{aligned}$$

Calculamos los 64 polinomios. La mitad de ellos no tiene coeficientes enteros y los restantes se agrupan de dos en dos salvo el signo. Eligiendo uno de cada par de opuestos, nos quedan dieciséis polinomios:

b_0	b_1	b_2	b_3	g_b,
1	1	1	1	1,
7	1	1	1	$-X^3 + X + 1$,
−11	1	1	1	$2X^3 - 2X + 1$,
−77	1	1	1	$13X^3 - 13X + 1$,
1	−1	1	1	$-X^3 - X^2 + 2X + 1$,
7	−1	1	1	$-2X^3 - X^2 + 3X + 1$,
−11	−1	1	1	$X^3 - X^2 + 1$,
−77	−1	1	1	$12X^3 - X^2 - 11X + 1$,
1	1	−1	1	$X^3 + 2X^2 - X - 1$,
7	1	−1	1	$2X^2 - 1$,
−11	1	−1	1	$3X^3 + 2X^2 - 3X - 1$,
−77	1	−1	1	$14X^3 + 2X^2 - 14X - 1$,
1	−1	−1	1	$X^2 + X - 1$,
7	−1	−1	1	$-X^3 + X^2 + 2X - 1$,
−11	−1	−1	1	$2X^3 + X^2 - X - 1$,
−77	−1	−1	1	$13X^3 + X^2 - 12X - 1$.

El polinomio f dado es mónico, así que buscamos factores mónicos. Repasando la lista anterior nos queda que sus posibles divisores mónicos de grado menor o igual que tres son

$$\begin{aligned}
&1,\\
&X^3 - X - 1,\\
&X^3 + X^2 - 2X + 1,\\
&X^3 - X^2 + 1,\\
&X^3 + 2X^2 - X - 1,\\
&X^2 + X - 1,\\
&X^3 - X^2 - 2X + 1.
\end{aligned}$$

El 1 es trivial. Probando a dividir sucesivamente por cada uno de los otros obtenemos la factorización

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

y los dos factores son irreducibles (son de grado 3 y no tienen raíces enteras).

Índice alfabético

anillo de polinomios, 2
aplicación polinómica, 4

cero de un polinomio, 4
coeficiente líder, 2
conjunto de polinomios, 1
contenido, 8
criterio de reducción, 13
cuerpo algebraicamente cerrado, 8

evaluar, 4

forma, 5

grado, 2, 5
    total, 5

lema de Gauss, 8

método de Kronecker, 14
monomio, 2, 5
    primitivo, 5
morfismo de evaluación, 4

orden lexicográfico, 5

polinomio
    ciclotómico, 12
    constante, 2
    de interpolación, 14
    homogéneo, 5
    mónico, 2
    primitivo, 8
    recíproco, 12
propiedad de densidad, 7

raíz de un polinomio, 4
regla de Ruffini, 10

término
    constante, 2
    líder, 2, 5
    monomial, 5