# ALGUNOS CRITERIOS DE IRREDUCIBILIDAD Y RAÍCES DE POLINOMIOS REALES EN UNA VARIABLE


LUZ HEIDY MUÑOZ GÓMEZ
PAOLA ANDREA TORO AGUIRRE

UNIVERSIDAD DEL CAUCA
FACULTAD DE CIENCIAS NATURALES, EXACTAS Y DE LA EDUCACIÓN
DEPARTAMENTO DE MATEMÁTICAS
POPAYÁN
2007

# ALGUNOS CRITERIOS DE IRREDUCIBILIDAD Y RAÍCES DE POLINOMIOS REALES EN UNA VARIABLE

LUZ HEIDY MUÑOZ GÓMEZ
PAOLA ANDREA TORO AGUIRRE

**TRABAJO DE GRADO**
**En la modalidad de seminario de grado presentado como requisito parcial para optar al título de Matemático**

**Director**
**Dr. CARLOS ALBERTO TRUJILLO**

UNIVERSIDAD DEL CAUCA
FACULTAD DE CIENCIAS NATURALES, EXACTAS Y DE LA EDUCACIÓN
DEPARTAMENTO DE MATEMÁTICAS
POPAYÁN
2007

# ALGUNOS CRITERIOS DE IRREDUCIBILIDAD Y RAÍCES DE POLINOMIOS REALES EN UNA VARIABLE

LUZ HEIDY MUÑOZ GÓMEZ
PAOLA ANDREA TORO AGUIRRE

DOCUMENTO DEL SEMINARIO DE GRADO, REALIZADO CON EL GRUPO DE INVESTIGACIÓN "ÁLGEBRA, TEORÍA DE NÚMEROS Y APLICACIONES" DE LA ESCUELA REGIONAL DE MATEMÁTICAS E.R.M

UNIVERSIDAD DEL CAUCA
FACULTAD DE CIENCIAS NATURALES, EXACTAS Y DE LA EDUCACIÓN
DEPARTAMENTO DE MATEMÁTICAS
POPAYÁN
2007

## Nota de aceptación

Director

**Doctor** Carlos Alberto Trujillo Solarte

**Comité evaluador**

**Profesor** Freddy William Bustos

**Profesor** Favián Enrique Arenas.

*Este triunfo a Dios, a la Universidad nuestros mas sinceros agradecimientos, a nuestro querido director* ***Carlos Alberto Trujillo****, quien con su apoyo y paciencia hizo posible la culminación de este trabajo, a los profesores Favian Enrique Arenas, Fredy William Bustos, Yilton Riascos y José Ignacio Téllez por sus oportunos consejos, sus valiosas indicaciones y aportes bibliográficos, a nuestra familia porque nos dieron la oportunidad de dar este gran paso, y agradecemos de todo corazón a todos nuestros amigos en especial a Olmer Folleco, Andrés Larraín y John Castillo por sus inagotables sugerencias.*

*A mi mamá, mis abuelos Lilia y Reinaldo, a mis tíos Reinaldo, Nancy y Milena y a mis queridos hermanos Deisy, Ariel, Ciro, y a mi querido hijo*

*Luz Heidy*

*A toda mi familia porque de ellos es este triunfo, en especial a mi papá y a mi tía Ady por su presencia en mi vida, a mi esposo y a mi adorado hijo*

*Paola Andrea*

# Índice general

# Resumen

En el contenido del presente trabajo hacemos una colección de algunos criterios de irreducibilidad, criterios para la resolución de ecuaciones bajo radicales, para encontrar raíces de polinomios reales en una variable y métodos de factorización, información que se encuentra dentro del Álgebra de Polinomios y que se ha repartido en cuatro capítulos formando así la monografía. El propósito de este documento es en esencia que se pueda tomar como herramienta de consulta para quienes deseen profundizar sus conocimientos en esta rama.

Para la consecución de este escrito consultamos la bibliografía que nos fue posible tener a nuestro alcance y de la que hicimos una revisión completa de los fundamentos teóricos de los temas que elegimos para el documento.

Uno de los motivos que llevó a la realización de esta monografía fue que en particular quienes la elaboramos no teníamos conocimiento de la existencia de otro criterio de irreducibilidad para polinomios que no cumplieran con las características de los criterios usuales como el de Eisenstein. Además nos pareció interesante reunir en un sólo texto métodos que nos permitieran resolver ecuaciones como las cúbicas y las bicuadráticas, así mismo el hecho de dar a conocer detalladanente algunos procedimientos para encontrar las raíces de polinomios en una variable y con coeficientes reales o por lo menos que nos permitieran averiguar cuántas raíces reales tiene este polinomio, o en que intervalo se encuentran dichas raíces.

La monografía empieza con un primer capítulo que llamamos conceptos fundamentales porque contiene definiciones y teoremas acerca de irreducibilidad y raíces de polinomios que se cumplen para cualquier campo F, el Teorema de la División, el Máximo Común

Divisor, y la Derivada de un Polinomio. Le siguen tres capítulos: Factorización e Irreducibilidad en $\mathbb{Z}_p[x]$, Irreducibilidad en $\mathbb{Q}[x]$ donde se trata la factorización de polinomios muy especiales como son los ciclotómicos partiendo de su irreducibilidad en $\mathbb{Q}[x]$ y Número de raíces de un polinomio en $\mathbb{R}[x]$, en cada uno de los cuales se muestra mediante ejemplos cómo funcionan los conceptos dados en el primer capítulo aparte de la teoría que le corresponde a cada sección. Finalmente se presenta un apéndice que contiene definiciones y teoremas que se utilizan en la sección de polinomios reducibles módulo todo primo y que debido a su complejidad no se colocaron en la sección correspondiente.

# Capítulo 1

# Conceptos Fundamentales

En esta sección, se presentan los resultados básicos de la teoría de polinomios, que serán usados luego para exponer las teorías mas específicas de los polinomios con coeficientes en $\mathbb{Z}_p$, $\mathbb{Q}$, y $\mathbb{R}$.

Para lo que sigue el lector deberá recordar los conceptos fundamentales de un anillo de polinomios, así como algunos conceptos del álgebra lineal. Se deberá tener en cuenta que en esta sección y en los demás capítulos se utilizan principalmente anillos de polinomios $F[x]$, donde $F$ es un campo y por lo tanto $F[x]$ es un dominio de integridad. En consecuencia, no se verán situaciones en las que $grad(p(x)q(x)) < grad(p(x)) + grad(q(x))$. El grado de un polinomio resultante de la suma de otros dos polinomios se define así: $grad(p(x) + q(x)) \leq \text{máx}\{grad(p(x)), grad(q(x))\}$, además se denota el elemento neutro de un campo con 0 y se usa 1 para denotar su elemento unidad.

Empieza entonces esta sección con la siguiente definición.

**Definición 1.** *Sean $R$ un anillo con elemento unidad $1$ y $p(x) \in R[x]$, con $grad(p(x)) \geq 1$. Si $r \in R$, y $p(r) = 0$, entonces $r$ es una **raíz** o **cero** del polinomio $p(x)$.*

**Ejemplo 1.** *Sea $f(x) = ax + b$ con $a$, $b \in F$, $a \neq 0$. Entonces $-b/a$ es raíz de $f(x)$ y $f(x) = a(x - (-b/a))$.*

**Ejemplo 2.** *Sea* $f(x) = ax^2 + bx + c$ *con* $a$, $b$, $c \in F$, $a \neq 0$. *Entonces*

$$f(x) = a\left(x^2 + \frac{b}{a}x + \frac{c}{a}\right) = a\left(\left(x + \frac{b}{2a}\right)^2 - \frac{b^2}{4a^2} + \frac{c}{a}\right)$$

$$= a\left(\left(x + \frac{b}{2a}\right)^2 - \frac{b^2 - 4ac}{4a^2}\right)$$

*Se define el* ***discriminante*** *de* $f(x)$ *como* $\Delta = \Delta(f(x)) = b^2 - 4ac$. *Entonces, si existe* $\beta \in F$ *tal que* $\beta^2 = \Delta$, *se tiene que:*

$$f(x) = a\left(\left(x + \frac{b}{2a}\right)^2 - \left(\frac{\beta}{2a}\right)^2\right) = a\left(x - \frac{-b + \beta}{2a}\right)\left(x - \frac{-b - \beta}{2a}\right)$$

*y se obtienen las raíces:* $\alpha_1 = \dfrac{-b + \beta}{2a}$, $\qquad \alpha_2 = \dfrac{-b - \beta}{2a}$.

**Definición 2.** *Un polinomio* $p(x) \in F[x]$ *es* ***mónico*** *si su coeficiente principal es* 1, *el elemento unidad de* $F$.

## 1.1. Polinomios Irreducibles

**Definición 3.** *Un polinomio* $p(x)$ *es una* ***unidad*** *si existe otro polinomio* $q(x)$ *con* $p(x)\, q(x) = 1$

Se puede deducir entonces, que en $F[x]$, donde $F$ es un campo, los polinomios que son unidades son los polinomios de grado cero, esto es, polinomios constantes distintos de cero, es decir los elementos de $F$.

**Definición 4.** *Un polinomio* $p(x) \neq 0$ *es* ***irreducible*** *si no es unidad, y* $p(x) = f(x)\, g(x)$, *implica que* $f(x)$ *o* $g(x)$ *debe ser una unidad.*

**Definición 5.** *Sea* $p(x) \in F[x]$, *con* $F$ *un campo y* $grad(p(x)) \geq 2$. *Se dice que* $p(x)$ *es* ***reducible*** *o* ***factorizable sobre*** $F$ *si existen* $g(x), h(x) \in F[x]$, *tales que:* $p(x) = g(x)h(x)$ *y cada uno de los polinomios* $g(x)$, $h(x)$ *tiene grado mayor o igual que 1. Si* $p(x)$ *no es reducible, entonces es* ***irreducible***.

**Teorema 1.** *Para polinomios en $F[x]$,*
***a.)*** *Cualquier polinomio $p(x) \neq 0$ de grado menor o igual que 1 es irreducible.*
***b.)*** *Si $p(x) \in F[x]$ con $grad(p(x)) = 2$ o 3, entonces $p(x)$ es* ***reducible*** *si y sólo si $p(x)$ tiene una raíz en el campo $F$.*

**Ejemplo:** $ax+b$ es irreducible en $F[x]$ para cualquier campo $F$, pues no puede existir ningún polinomio $g(x)$ tal que $1 \leq grad(g(x)) < grad(f(x)) = 1$.

**Definición 6.** *Si $p\,(x)$ es un polinomio tal que $p\,(x)$ divide a $f\,(x)\,g\,(x)$ implica que $p\,(x)$ divide a $f\,(x)$ o a $g\,(x)$, se dice que $p(x)$ es* ***primo****.*

Se puede deducir que todo polinomio $p(x)$ primo es irreducible.

**Definición 7.** *Se dice que dos polinomios $f\,(x)$ y $g\,(x)$ en $F[x]$ son* ***asociados*** *si $f(x)$ divide a $g(x)$ y $g(x)$ divide a $f(x)$.*

**Ejemplo:** Sea $f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_0$, con $a_i \in F$ y $g(x) = ka_n x^n + ka_{n-1}x^{n-1} + ... + ka_0$ con $k \in F$. Entonces $g(x)$ y $f(x)$ son asociados.

Cualquier polinomio es asociado de exactamente un polinomio mónico, pues si se toma un polinomio $f(x)$, se puede multiplicar este polinomio por el inverso multiplicativo de su coeficiente principal y así obtener el polinomio mónico $g(x)$. De esta manera, $g(x) = mf(x)$, donde $m$ es el inverso multiplicativo del coeficiente principal de $f(x)$.
Así, $f(x)$ y $g(x)$ son asociados.

**Definición 8.** *Un dominio entero $F[x]$ es un* ***dominio de factorización única*** *si:*
*(i) Todo $p(x) \neq 0$ en $F[x]$ es una unidad o puede ser escrito como el producto de un número finito de factores irreducibles de $F[x]$.*
*(ii) La descomposición en (i) es única salvo por el orden y asociados de los factores irreducibles.*

**NOTA:** Todo polinomio irreducible en un dominio de factorización única es necesa riamente primo por la definición anterior parte (ii). En consecuencia ser irreducible y primo coincide en un dominio de factorización única.

Ahora sería conveniente preguntarse ¿Qué clase de polinomios son irreducibles?.
La respuesta claramente depende del campo $F$. Por ejemplo, el polinomio $x^3 - 2$, es un polinomio con coeficientes en $\mathbb{Q}$, y $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, así que se podría preguntar acerca de su factorización en $\mathbb{Q}[x], \mathbb{R}[x]$ y $\mathbb{C}[x]$.

En $\mathbb{Q}[x]$, $x^3 - 2$ es irreducible.

En $\mathbb{R}[x], x^3 - 2 = (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + \sqrt[3]{4})$

En $\mathbb{C}[x], x^3 - 2 = (x - \sqrt[3]{2})(x - w\sqrt[3]{2})(x - w^2\sqrt[3]{2})$, donde $w = e^{2i\pi/3} = -(\frac{1}{2}) + (i\frac{\sqrt{3}}{2})$ satisface $w^3 = 1$.

Con esto queda claro que la irreducibilidad depende del campo donde el polinomio tenga sus coeficientes.

## 1.2. Algoritmo de la división

**Definición 9.** *Sea $F$ un campo. Sean $p(x)$ y $d(x)$ dos polinomios en $F[x]$, con $d(x) \neq 0$. Se dice que $d(x)$* ***es un divisor de*** *$p(x)$, si existe $q(x) \in F[x]$ tal que $d(x)q(x) = p(x)$. En este caso, también se dice que $d(x)$* ***divide a*** *$p(x)$ y que $p(x)$* ***es un múltiplo de*** *$d(x)$.*

**Teorema 2.** ***(Teorema de la División):*** *Sea $F$ un campo. Sean $p(x)$ y $d(x)$ dos polinomios en $F[x]$, con $d(x) \neq 0$. Existen polinomios únicos $q(x)$ y $r(x)$ tal que $p(x) = d(x)q(x) + r(x)$, donde el $grad(r(x)) < grad(d(x))$ o $r(x) = 0$.*

**Demostración:** Se denota $n$ el grado de $p(x)$ y como $m$ el grado del divisor $d(x)$.

**i.)** Sea $grad(p(x)) < grad(d(x))$, entonces $p(x) = d(x)\cdot 0 + p(x)$ que satisface el teorema de la división.

**ii.)** Sea $grad(p(x)) \geq grad(d(x))$, con $p(x) \neq 0$. Se establecerá la unicidad después de probar la existencia de $q(x)$ y $r(x)$.
Se aplica ahora inducción en el grado $n$ de $p(x)$.

Si $n = 0$ entonces $p(x) = c$ donde $c$ es una constante, y por tanto $d(x) = k$ donde $k$ es una constante y como $d(x) \neq 0$, $k \neq 0$.

Escogiendo $q(x) = \dfrac{c}{k}$ y $r = 0$.

Entonces $d(x)q(x) + r(x) = k\dfrac{c}{k} + 0 = c = p(x)$, en este caso $r(x) = 0$

Ahora se asume la existencia de polinomios $q_1(x)$ y $r_1(x)$ tal que $p_1(x) = d(x)q_1(x) + r_1(x)$ siempre que $p_1(x)$ sea cualquier polinomio que tenga un grado menor o igual a $k$ y así $grad(r_1(x)) < grad(d(x))$ o $r_1(x) = 0$.

Sea $p(x)$ un polinomio de grado $k+1$, entonces $p(x) = a_{k+1}x^{k+1} + a_kx^k + ... + a_1x + a_0$, donde $a_{k+1} \neq 0$.

Se muestra el teorema para $p(x)$.

**Caso 1**: $m = 0$

$d(x) = k$ donde $k$ es una constante y como $d(x) \neq 0$ se sabe que $k \neq 0$.

Sea $q(x) = \dfrac{1}{k}p(x)$ y sea $r(x) = 0$.

Entonces $d(x)q(x) + r(x) = k\dfrac{1}{k}p(x) + 0 = p(x) + 0 = p(x)$.

**Caso 2**: $m > 0$

Sea $d(x) = d_0 + d_1x + ... + d_mx^m$ con $d_m \neq 0$ . Note que $\dfrac{a_{k+1}}{d_m} \neq 0$ porque las dos constantes son distintas de cero.

Sea $p_1(x) = p(x) - \left(\dfrac{a_{k+1}}{d_m}x^{k+1-m}\right) d(x)$. Entonces la sustracción de la derecha cancela el término principal de $p(x)$, así $p_1(x)$ es un polinomio de grado $k$ o menor y se puede aplicar hipótesis de inducción a $p_1(x)$ para concluir la existencia de los polinomios $q_1(x)$ y $r_1(x)$ tal que $p_1(x) = d(x)q_1(x) + r_1(x)$ donde $grad(r_1(x)) < grad(d(x))$.

$$p_1(x) = d(x)q_1(x) + r_1(x) = p(x) - \frac{a_{k+1}}{d_m}x^{k+1-m}d(x).$$

Ahora se resuelve la segunda ecuación para $p(x)$.

$$p(x) = \frac{a_{k+1}}{d_m}x^{k+1-m}\ d(x) + \ d(x)\ q_1(x) + \ r_1(x)$$

$$p(x) = d(x)\ \left(\frac{a_{k+1}}{d_m}x^{k+1-m} + q_1(x)\right) + r_1(x)$$

Sea $q(x) = \dfrac{a_{k+1}}{d_m}x^{k+1-m} + q_1(x)$ y sea $r\,(x) = r_1(x)$, se ha demostrado el teorema para $p(x)$ de grado $k + 1$.

Para establecer la unicidad, se supone que

$p(x) = d(x)q_1(x) + r_1(x) = d(x)q_2(x) + r_2(x)$, entonces se tiene que

$d(x)\,(q_1(x) - q_2(x)) = r_2(x) - r_1(x) \qquad (*)$,

en donde $d(x) \neq 0$, $grad(r_1(x)) < grad(d(x))$, $grad(r_2(x)) < grad(d(x))$.

**Caso 1**: $m = 0$

Como $d(x)$ divide a $p(x)$, en este caso los dos residuos deben ser cero, es decir $r_1(x) = r_2(x)$.

$d(x)[q_1(x) - q_2(x)] = 0$, y como $d(x) \neq 0$ se debe tener

$q_1(x) - q_2(x) = 0$, lo cual implica que $q_1(x) = q_2(x)$.

**Caso 2**: $m > 0$

Si $q_1(x) - q_2(x) \neq 0$ entonces se puede deducir el grado de los polinomios en ambos lados de la ecuación $(*)$.

El grado en el lado izquierdo es mayor o igual al grado de $d(x)$. Pero en el lado derecho ambos residuos tienen grado menor que el grado de $d(x)$, así su diferencia tiene un grado menor o igual al polinomio de mayor grado, el cual es menor que $grad(d(x))$. Esto es una contradicción. Luego $q_1(x) - q_2(x) = 0$ y todo el lado izquierdo de la ecuación $(*)$ es cero, así que los dos residuos son también iguales.

**Teorema 3.** ***(Teorema del Residuo):*** *Para $p(x) \in F[x]$ y $a \in F$. Cuando el polinomio $p(x)$ se divide entre $(x - a)$ el residuo es $p(a)$.*

**Demostración:** Por el algoritmo de la división se tiene $p(x) = (x - a)q(x) + r$, donde $r(x) = 0$ o $grad(r(x)) < grad(x - a) = 1$. Por lo tanto, $r(x) = r$ es un elemento de $F$. Ahora, sea $x = a$. Se ve que $p(a) = (a-a)q(a)+r(a)$. Luego $p(a) = 0q(a)+r(a) = 0+r = r$. Por tanto $p(a) = r$.

**Teorema 4.** ***(Teorema del Factor):*** *Si $p(x) \in F[x]$ y $a \in F$, entonces $(x - a)$ es un factor del polinomio $p(x)$ si y solo si $a$ es una raíz de $p(x)$.*

**Demostración: i)** Sea $(x - a)$ un factor de $p(x)$.

Entonces $p(x) = (x - a)q(x)$. Como $p(a) = (a - a)q(a) = 0$, $a$ es una raíz de $p(x)$.

**ii)** Recíprocamente, sea $a$ una raíz de $p(x)$. Por el algoritmo de la división $p(x) = (x - a)q(x) + r(x)$, donde $r(x) \in F[x]$. Como $grad(r(x)) < grad(x - a) = 1$, $r(x)$ debe ser una constante, llámese $r$, en $F$. Así $p(x) = (x - a)q(x) + r$. Como $p(a) = 0$ se tiene que $r = 0$, de modo que $p(x) = (x - a)q(x)$ y $(x - a)$ es un factor de $p(x)$.

### 1.2.1. Método de Horner

El proceso llamado **Método de Horner**, es el mismo algoritmo de la división que se acaba de ver, sólo que se omite la indeterminada $x$ para facilitar el proceso; el método es para divisores de la forma $x - x_0$.

Cuando se realizan normalmente los cálculos con el método de Horner, se construye una tabla que sugiere el nombre de **División Sintética** comunmente aplicado a esta técnica. Para ilustrar el proceso se usarán ejemplos en los que se muestra la manera de construir la tabla de la división sintética y se describe como funciona el algoritmo que a continuación se enuncia formalmente.

**Teorema 5.** ***(Método de Horner:)*** *Sea* $p(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$. *Si* $a_n = b_n$ *y* $b_k = a_k + b_{k+1}x_0$, *para* $k = n-1, n-2, ..., 1, 0$ *entonces,*

$$b_0 = p(x_0).$$

*Mas aún, si* $q(x) = b_n x^{n-1} + b_{n-1}x^{n-2} + ... + b_2 x + b_1$ *entonces,*

$$p(x) = (x - x_0)q(x) + b_0$$

**Demostración:** Sea $q(x) = b_n x^{n-1} + b_{n-1}x^{n-2} + ... + b_2 x + b_1$.

$$(x - x_0)q(x) + b_0 = (x - x_0)(b_n x^{n-1} + b_{n-1}x^{n-2} + ... + b_2 x + b_1) + b_0$$

$$= (b_n x^n + b_{n-1}x^{n-1} + ... + b_2 x^2 + b_1 x) - (b_n x_0 x^{n-1} + b_{n-1}x_0 x^{n-2} + ... + b_2 x_0 x + b_1 x_0) + b_0$$

$$= b_n x^n + (b_{n-1} - b_n x_0)x^{n-1} + ... + (b_1 - b_2 x_0)x + (b_0 - b_1 x_0).$$

Pero $a_n = b_n$ y $b_k - b_{k+1}x_0 = a_k$ por hipótesis.

Por tanto,

$$(x - x_0)q(x) + b_0 = p(x)$$

y

$$b_0 = p(x_0)$$

**Ejemplo 3.** *Aplique el método de Horner para evaluar* $p(x) = 2x^3 - 9x^2 + 10x - 7$ *en* $x_0 = 3$

*Se escriben los coeficientes de* $p(x)$ *en orden descendente teniendo en cuenta incluso los coeficientes iguales a cero de tal manera, que ningún coeficiente de* $p(x)$ *falte entre el grado mayor del polinomio y el término constante.*

*Ahora, como* $a_n = b_n = 2$ *entonces, se inicia el procedimiento multiplicando* 2 *por* 3*, se suma* 6 *y* $-9$ *para obtener* $-3$*. Se repite el proceso ahora multiplicando* $-3$ *por* 3 *para obtener* $-9$ *y se repite este proceso hasta el final.*

*En este problema, la tabla es la siguiente:*

| | | | | |
|---|---|---|---|---|
| *Coeficientes de* $p(x)$ $\rightarrow a_3 = 2$ | $a_2 = -9$ | $a_1 = 10$ | $a_0 = -7$ | $\lfloor\ 3 \rightarrow x_0$ |
| | $b_3x_0 = 6$ | $b_2x_0 = -9$ | $b_1x_0 = 3$ | |
| | --- | --- | --- | |
| *Coeficientes de* $q(x)$ $\rightarrow b_3 = 2$ | $b_2 = -3$ | $b_1 = 1$ | $\boxed{b_0 = -4}$ $\leftarrow$ *Residuo* | |

$q(x) = 2x^2 - 3x + 1$ *y* $p(3) = -4$.

*Como* $p(x)$ *comienza con* $x^3$*,* $q(x)$ *comienza con* $x^2$*. Por tanto,*

$$p(x) = (x - 3)(2x^2 - 3x + 1) - 4.$$

*Se habrá podido observar que en la división sintética interesa saber qué sucede con los coeficientes de los polinomios involucrados en la evaluación; además se debe observar que el residuo es siempre una constante.*

**Ejemplo 4.** *Aplique el método de Horner para evaluar* $p(x) = x^3 + 1$ *en* $x_0 = 2$.

*Aquí los coeficientes de* $x^2$ *y* $x$ *son ceros, así que serán organizados de la siguiente manera:*

| | | | | |
|---|---|---|---|---|
| *1* | *0* | *0* | *1* | $\lfloor\ 2$ |
| | *2* | *4* | *8* | |
| | --- | --- | --- | |
| *1* | *2* | *4* | $\boxed{9}$ $\leftarrow$ *Residuo* | |

$q(x) = x^2 + 2x + 4$

**Teorema 6.** ***(Teorema del máximo número de raíces):*** *Un polinomio $p(x)$ distinto de cero en $F[x]$, de grado $n \geq 1$ ,tiene a lo sumo $n$ raíces distintas en $F$.*

**Demostración:** La demostración es por inducción matemática sobre el grado de $p(x)$. Si $n = 1$, entonces $p(x) = ax + b$, para $a, b \in F, a \neq 0$. Como $p(-a^{-1}b) = 0$, $p(x)$ tiene al menos una raíz en $F$. Si $c_1$ y $c_2$ son dos raíces, entonces $p(c_1) = ac_1 + b = 0 = ac_2 + b = p(c_2)$. Por la ley de cancelación en un anillo, $ac_1 + b = ac_2 + b$ entonces $ac_1 = ac_2$. Como $F$ es un campo y $a \neq 0$, se tiene que $ac_1 - ac_2 = 0$ lo que implica que $a(c_1 - c_2) = 0$, por ser un dominio entero $a = 0$ o $c_1 - c_2 = 0$, entonces $c_1 = c_2$ por lo que $p(x)$ solo tiene una raíz en $F$. Se supone ahora que el resultado del teorema es verdadero para todos los polinomios de grado $k \geq 1$ en $F[x]$. Sea un polinomio $p(x)$ de grado $k+1$. Si $p(x)$ no tiene raíces en $F$, el teorema queda demostrado. En caso contrario, sea $r \in F$ tal que $p(r) = 0$. Por el teorema del factor, $p(x) = (x - r)q(x)$, donde $q(x)$ tiene grado $k$. En consecuencia, por la hipótesis de inducción, $q(x)$ tiene a lo sumo $k$ raíces en $F$ y $p(x)$ tiene, a su vez, a lo sumo $k + 1$ raíces en $F$.

**Definición 10.** *Así como a los números enteros se hace su descomposición en números primos, también se puede escribir la factorización de un polinomio $f(x)$ en $F[x]$ como:*

$$f(x) = p_1^{e_1}(x)\, p_2^{e_2}(x) \ldots p_r^{e_r}(x), \text{ con } e_i \in \mathbb{N}; \text{ donde } \sum_{j=1}^{r} e_j = n$$

*Si cualquier $e_i > 1$ se dice que $f(x)$ tiene un* ***factor múltiple****. Si $f(x)$ tiene un factor múltiple lineal se dice que $f(x)$ tiene una* ***raíz múltiple*** *en $F$.*

## 1.3. Máximo Común Divisor

**Definición 11.** *El polinomio $d(x) \in F[x]$ es el máximo común divisor de $f(x)$, $g(x) \in F[x]$ con al menos uno de ellos no nulo, si $d(x)$ es un polinomio mónico tal que:*

***a.)*** *$d(x)$ divide a $f(x)$ y a $g(x)$; y*

***b.)*** *si $h(x) \in F[x]$ divide a $f(x)$ y a $g(x)$, entonces $h(x)$ divide a $d(x)$.*

Se establecerán ahora los siguientes resultados relativos a la existencia y unicidad de lo que se llamará **el máximo común divisor**, que se dará en forma abreviada como $MCD$.

Se puede encontrar el máximo común divisor de dos polinomios usando el teorema de la división varias veces. El proceso para determinar el $MCD$ de dos polinomios llamado **algoritmo de Euclides para polinomios** funciona como se describe en el siguiente teorema:

**Teorema 7.** ***( Teorema Del Algoritmo Euclideano Para Polinomios):*** *Sean* $p(x)$ *y* $q(x) \in F[x]$ *dos polinomios con* $grad(q(x)) \leq grad(p(x))$ *y* $q(x) \neq 0$. *Entonces existe un polinomio* $d(x)$ *tal que* $d(x)$ *divide a* $p(x)$ *y a* $q(x)$. *El polinomio* $d(x)$ *es llamado el* ***máximo común divisor*** *de* $p(x)$ *y* $q(x)$ *a veces denotado por* $MCD(p(x), q(x))$.

Aplicando el algoritmo de la división, se tiene

$$\begin{aligned}
&p(x) = f(x)q(x) + r(x), && grad(r(x)) < grad(q(x)) \text{ o } r(x) = 0.\\
&q(x) = f_1(x)r(x) + r_1(x), && grad(r_1(x)) < grad(r(x)) \text{ o } r_1(x) = 0.\\
&r(x) = f_2(x)r_1(x) + r_2(x), && grad(r_2(x)) < grad(r_1(x)) \text{ o } r_2(x) = 0.\\
&\quad\vdots && \quad\vdots\\
&r_k(x) = f_{k+1}(x)r_{k+1}(x)+r_{k+2}(x), && grad(r_{k+2}(x)) < grad(r_{k+1}(x)) \text{ o } r_{k+2}(x) = 0
\end{aligned}$$

Sea $r_0(x) = q(x)$ y sea $n$ el menor entero tal que $r_{n+1} = 0$ (tal $n$ existe ya que $F[x]$ con $F$ un campo es un dominio euclidiano con $\varphi(f(x)) = grad(f(x))$, y $\varphi(r_k(x))$ forma una sucesión estrictamente decreciente de enteros no negativos), entonces $r_n(x)$ es el máximo común divisor de $p(x)$ y $q(x)$.

**Teorema 8.** ***Lema de Bezout:*** *Sean* $p(x)$, $q(x) \in F[x]$, *con al menos uno de ellos no nulo. Entonces cualquier polinomio de grado mínimo que se pueda escribir como combinación lineal de* $p(x)$ *y* $q(x)$ *(es decir, de la forma* $s(x)p(x) + t(x)q(x)$, *para* $s(x)$, $t(x) \in F[x]$*) será un máximo común divisor de* $p(x)$ *y* $q(x)$.

**Teorema 9.** *Dos máximos comunes divisores de* $e(x)$ *y* $d(x)$ *de* $f(x)$ *y* $g(x)$ *pueden diferir únicamente por un múltiplo constante:* $d(x) = ae(x)$ *para algún* $a \in F$.

**Demostración:** Por la condición de divisibilidad mutua en $d(x)$ y $e(x)$ se tiene que $grad(d(x)) \leq grad(e(x)) \leq grad(d(x))$, así que $grad(d(x)) = grad(e(x))$. Pero $d(x) = a(x)e(x)$, así que $grad(d(x)) = grad(a(x)) + grad(e(x)) = grad(a(x)) + grad(d(x))$, en

consecuencia se debe tener que $grad(a(x)) = 0$, así $a(x) = a$, un elemento de $F$.
De las definiciones y teoremas anteriores se puede concluir que el único máximo común divisor entre dos polinomios $f(x)$ y $g(x)$ es aquel polinomio **mónico** $d(x)$ que divida a $f(x)$ y a $g(x)$. Los otros polinomios que sean divisores comunes de $f(x)$ y $g(x)$ son múltiplos del polinomio $d(x)$.

**Definición 12.** *Si $p(x)$ y $q(x) \in F[x]$ y su MCD es 1, se dice que $p(x)$ y $q(x)$ son* ***primos relativos****.*

**Teorema 10.** *Si $p(x)$ y $q(x) \in F[x]$ son primos relativos, entonces*

$a(x)\,p(x) + b(x)\,q(x) = 1$ *para algunos polinomios* $a(x), b(x) \in F[x]$.

*Recíprocamente si* $a(x)\,p(x) + b(x)\,q(x) = 1$ *para algunos polinomios* $a(x), b(x) \in F[x]$, *entonces $p(x)$ y $q(x)$ son primos relativos.*

**Teorema 11.** *Si $p(x)$ y $q(x)$ son primos relativos y si $p(x)$ divide a $q(x)f(x)$, entonces $p(x)$ divide a $f(x)$.*

**Demostración:** Por el teorema **10**, $a(x)\,p(x)+b(x)\,q(x) = 1$ para algunos polinomios $a(x), b(x) \in F[x]$. Por consiguiente, $a(x)\,p(x)\,f(x) + b(x)\,q(x)\,f(x) = f(x)$. Como $p(x)$ divide a $b(x)q(x)f(x)$ y $p(x)$ divide a $q(x)f(x)$ por hipótesis, $p(x)$ divide al lado derecho de la relación anterior, esto es, $p(x)$ divide a $f(x)$.

## 1.4. Derivada de un Polinomio

Para hacer una discusión lo más general posible, se debe observar inicialmente que la diferenciación de polinomios es una operación netamente algebraica. Es decir, se puede diferenciar sin usar límites; así es posible asumir que los coeficientes del polinomio pertenecen a un campo arbitrario; y no necesariamente al campo de los números reales.

**Definición 13.** *Sean $F$ un campo y $f(x)$ un polinomio con coeficientes en $F$. Se define la* ***derivada*** *de $f(x)$, denotada como $D(f(x)) = f'(x)$, como otro polinomio en $F[x]$ sujeto a las siguientes reglas:*

***i)*** *Para $a \in F$ y $n$ entero no negativo,*

$$D(ax^0) = 0$$

$$D(ax^n) = a(\underbrace{x^{n-1} + ... + x^{n-1}}_{n\text{-veces}}) = nax^{n-1}.$$

***ii)*** *Dados $f(x)$ y $g(x)$ en $F[x]$, se tiene:*

$$D(f(x) + g(x)) = D(f(x)) + D(g(x))$$

**Nota 1.** *La regla **(i)** es ligeramente engañosa, porque el exponente "n" en $ax^n$ es un entero no negativo, mientras el coeficiente "n" en $nax^{n-1}$ denota $1 + 1... + 1(n - veces)$ en $F$.*

**Ejemplo 5.** *Así, en cualquier campo $F$, si $p(x) = x^3$, entonces $D(x^3) = 3x^2$.*

*Si $f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0 \in F[x]$, entonces por* (**i**), (**ii**) *e inducción es claro que:*

$f'(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + ... + a_1$

Para completar esta herramienta algebraica sobre derivación solo se necesita de la regla usual para diferenciar productos.

**Proposición 1.** *Sean $f(x), g(x) \in F[x]$. Entonces,*

$$D(f(x)\,g(x)) = f(x)\,D(g(x)) + D(f(x))g(x).$$

**Demostración:** Sea $n =$máx$\{grad(f(x)), grad(g(x))\}$. Entonces se escribe

$$f(x) = \sum_{i=0}^{n} a_i x^i,\ g(x) = \sum_{j=0}^{n} b_j x^j$$

haciendo $a_i = 0$ o $b_j = 0$ para valores grandes de $i, j$ si fuera necesario.
Para ver la propiedad, se calcula primero

$$D(a_i x^i b_j x^j) = D(a_i b_j x^{i+j}) = (i+j)a_i b_j x^{i+j-1}$$

$$= ia_i x^{i-1} b_j x^j + a_i x^i j b_j x^{j-1} = D(a_i x^i) b_j x^j + a_i x^i D(b_j x^j)$$

así que el enunciado vale para el producto de dos términos cualquiera de $f(x)$ y $g(x)$. En el caso general, usando la validez de la regla (ii) de la definición **13** y lo que se acabó de demostrar, se tendrá:

$$D(f(x)g(x)) = D\left(\left(\sum_{i=0}^{n} a_i x^i\right)\left(\sum_{j=0}^{n} b_j x^j\right)\right) = D\left(\sum_{i,j=0}^{2n} a_i x^i b_j x^j\right)$$

$$= \sum_{i,j=0}^{2n-1} D(a_i x^i b_j x^j) = \sum_{i,j=0}^{2n-1} D(a_i x^i) b_j x^j + \sum_{i,j=0}^{2n-1} a_i x^i D(b_j x^j)$$

$$= \left(\sum_{i=0}^{n-1} D(a_i x^i)\right)\left(\sum_{j=0}^{n} b_j x^j\right) + \left(\sum_{i=0}^{n} a_i x^i\right)\left(\sum_{j=0}^{n-1} D(b_j x^j)\right)$$

$$= D\left(\sum_{i=0}^{n} a_i x^i\right)\left(\sum_{j=0}^{n} b_j x^j\right) + \left(\sum_{i=0}^{n} a_i x^i\right) D\left(\sum_{j=0}^{n} b_j x^j\right)$$

$$= D(f(x))g(x) + f(x)\, D(g(x)).$$

**Corolario 1.** *Sean $g(x) \in F(x), n \geq 1$ un entero. Entonces, $D((g(x))^n) = n((g(x))^{n-1}) D(g(x))$.*

Para terminar esta sección se presenta una razón algebraica que justifica en alguna forma la necesidad de introducir el concepto de derivada de un polinomio.

**Proposición 2.** *Sean $F$ un subcampo de $\mathbb{C}$ (Números complejos), y $f(x) \in F[x]$. El polinomio $f(x)$* ***no tiene factores múltiples****(repetidos más de una vez), sí y solo si, el máximo común divisor de $f(x)$ y $f'(x)$ es 1, (los únicos divisores comunes de $f(x)$ y $f'(x)$ son constantes).*

**Demostración:** Si $f(x)$ tiene algún factor múltiple, existen $p(x), q(x) \in F[x]$ y un entero $k > 1$ tales que: $f(x) = (p(x))^k q(x)$; entonces,

$f'(x) = (p(x))^k q'(x) + k(p(x))^{k-1} p'(x) q(x) = (p(x))^{k-1} [p(x)q'(x) + kp'(x)q(x)]$;

así, $(p(x))^{k-1}$ es un divisor común, no trivial, de $f(x)$ y $f'(x)$; en consecuencia el máximo común divisor de $f(x)$ y $f'(x)$ no es uno.

Recíprocamente, se supone que $d(x)$ es el máximo común divisor de $f(x)$ y $f'(x)$ y que tiene grado mayor o igual que uno. Sea $p(x)$ un factor irreducible del polinomio $d(x)$; entonces:

$f(x) = p(x)g(x)$ y $f'(x) = p(x)g'(x) + p'(x)g(x)$.

De esto es claro que $p(x)$ divide a $p'(x)g(x)$; y como $p(x)$ es irreducible, él debe dividir a $p'(x)$ o a $g(x)$. Pero como en este caso, $F \subseteq \mathbb{C}$, $p'(x)$ es un polinomio no cero de grado menor que el de $p(x)$, $p(x)$ no puede dividir a $p'(x)$, y así $p(x)$ divide a $g(x)$. Entonces $g(x) = p(x)h(x)$ para algún $h\,(x) \in F[x]$; y así $f(x) = (p(x))^2 h(x)$.

Por lo tanto, $f(x)$ tiene un factor múltiple. Esto completa la prueba.

En todo lo que sigue se consideraran campos numéricos, es decir, subcampos de $\mathbb{C}$. Así mismo la aplicación y ampliación de algunos conceptos vistos en este capítulo se verán ilustrados en cada campo.

# Capítulo 2

# Factorización e Irreducibilidad en $\mathbb{Z}_P[x]$

Factorizar en $\mathbb{Z}_P[x]$, $p$ un primo, no solo es ventajoso sino que también es de gran uti lidad para factorizar en $\mathbb{Z}[x]$. Por ejemplo, puede mostrarse que $x^4+3x+7$ es irreducible en $\mathbb{Z}[x]$ (y por tanto en $\mathbb{Q}[x]$) mostrando que es irreducible en $\mathbb{Z}_2$.

Cualquier polinomio de grado $d$ en $\mathbb{Z}_P[x]$ puede ser factorizado en un número finito de pasos, porque existen únicamente finitos polinomios posibles de grado menor que $d$ en $\mathbb{Z}_P$ ($p^d$, de ellos, para ser más precisos), y se puede simplemente inspeccionarlos a todos, usando el teorema de la división (de hecho necesitamos únicamente mirar los factores de grado menor o igual que $d/2$) pero llegar por tanteo es muy ineficiente.

En esta sección se presenta un algoritmo para factorizar polinomios en $\mathbb{Z}_P[x]$. Este fué descubierto en 1967 por E.R. Berlekamp.
Con los siguientes ejemplos se ilustra como funcionan en $\mathbb{Z}_p$ algunos de los teoremas vistos en el capítulo 1 antes de ilustrar el tema central de esta sección.

**Ejemplo 6.** *Sean* $p(x) = 4x^3 + 2x^2 + 3x + 1$ *y* $q(x) = 3x^2 + x + 2$ *polinomios de* $\mathbb{Z}_5[x]$. *En este caso,* $a_3 = 4, a_2 = 2, a_1 = 3, a_0 = 1$, *y* $b_2 = 3, b_1 = 1, b_0 = 2$. *Para todo* $n \geq 4$ *se tiene que* $a_n = 0$. *Si* $m \geq 3$, *se tiene que* $b_m = 0$. *En este caso las sumas y productos de los polinomios son módulo* 5.

$$p(x)+q(x) = (4+0)x^3+(2+3)x^2+(3+1)x+(1+2)$$

$$= 4x^3+0x^2+4x+3 = 4x^3+4x+3$$

*y*

$$p(x)q(x) = \left(\sum_{k=0}^{5} a_{5-k}b_k\right)x^5 + \left(\sum_{k=0}^{4} a_{4-k}b_k\right)x^4 +$$

$$\left(\sum_{k=0}^{3} a_{3-k}b_k\right)x^3 + \left(\sum_{k=0}^{2} a_{2-k}b_k\right)x^2 + \left(\sum_{k=0}^{1} a_{1-k}b_k\right)x + \left(\sum_{k=0}^{0} a_{0-k}b_k\right)$$

$$= (0\cdot 2+0\cdot 1+4\cdot 3+2\cdot 0+3\cdot 0+1\cdot 0)x^5+(0\cdot 2+4\cdot 1+2\cdot 3+3\cdot 0+1\cdot 0)x^4+$$

$$(4\cdot 2+2\cdot 1+3\cdot 3+1\cdot 0)x^3+(2\cdot 2+3\cdot 1+1\cdot 3)x^2+(3\cdot 2+1\cdot 1)x+(1\cdot 2)$$

$$= 2x^5+0x^4+4x^3+0x^2+2x+2 = 2x^5+4x^3+2x+2.$$

**Ejemplo 7.** *(Raíz de un polinomio) Para* $p(x) = x^2+3x+2 \in \mathbb{Z}_5[x]$*, se nota que*

$p(0) = (0)^2+3(0)+2 = 2$ $\qquad$ $p(3) = (3)^2+3(3)+2 = 20 = 0$

$p(1) = (1)^2+3(1)+2 = 6 = 1$ $\qquad$ $p(4) = (4)^2+3(4)+2 = 30 = 0$

$p(2) = (2)^2+3(2)+2 = 12 = 2$

*En consecuencia,* $p(x)$ *tiene dos raíces:* 3 *y* 4*.*

**Ejemplo 8.** *(Teorema de la división) El algoritmo de la división también se aplica cuando los coeficientes de los polinomios se toman de un campo finito. Si* $p(x) = 6x^4+4x^3+5x^2+3x+1$ *y* $d(x) = 3x^2+4x+2$ *son polinomios en* $\mathbb{Z}_7[x]$*, entonces del proceso de la división obtenemos los siguientes resultados:* $d(x)q(x)+r(x) = (3x^2+4x+2)(2x^2+x+6)+(5x+3) = 6x^4+4x^3+5x^2+3x+1 = p(x)$*.*

**Ejemplo 9.** *(Polinomios Irreducibles)*

***a.)*** *En* $\mathbb{Z}_2[x]$*,* $p(x) = x^3+x^2+x+1$ *es reducible pues* $p(1) = 0$*. Pero* $q(x) = x^3+x+1$ *es irreducible pues* $q(0) = q(1) = 1$*.*

***b.)*** *Sea* $h(x) = x^4+x^3+x^2+x+1 \in \mathbb{Z}_2[x]$*. ¿Es* $h(x)$ *reducible en* $\mathbb{Z}_2[x]$*? Como* $h(0) = h(1) = 1$*,* $h(x)$ *no tiene factores de primer grado, pero se podría encontrar* $a, b, c, d \in \mathbb{Z}_2$ *tales que* $(x^2+ax+b)(x^2+cx+d) = x^4+x^3+x^2+x+1$*. Se desarrolla* $(x^2+ax+b)(x^2+cx+d)$

*y se comparan los coeficientes de las potencias similares de* $x$*, con lo que se obtiene* $a+c=1$*,* $ac+b+d=1$*,* $ad+bc=1$ *y* $bd=1$*. Como* $bd=1$*, se tiene que* $b=1$ *y* $d=1$*, por lo que* $ac+b+d=1 \Rightarrow ac=1 \Rightarrow a=c=1 \Rightarrow a+c=0$*. Esto contradice el hecho de que* $a+c=1$*. En consecuencia,* $h(x)$ *es irreducible en* $\mathbb{Z}_2[x]$*.*

***c.)*** $x^2+1$ *es irreducible en* $\mathbb{Z}_3[x]$*.*

***d.)*** $x^2+x+1$ *es irreducible en* $\mathbb{Z}_2[x]$*.*

**Ejemplo 10.** *(MCD)*

*a.) Encontrar el MCD de* $x^2+1$ *y* $x^5+1$ *en* $\mathbb{Z}_2[x]$

**Solución:** *Al dividir* $x^5+1$ *entre* $x^2+x+1$ *en* $\mathbb{Z}_2[x]$*, el residuo es* $x+1$*. Como todavía no se tiene residuo cero se continua con el proceso de la división, esta vez dividiendo* $x^2+x+1$ *entre* $x+1$ *y se obtiene residuo cero. Como ya se obtuvo el residuo cero termina el proceso. Entonces el* $MCD$ *entre los polinomios* $x^5+1$ *y* $x^2+x+1$ *es el último residuo distinto de cero, que en este caso es el polinomio* $x+1$*.*

*b.) Encontrar el MCD de* $x^3+2x^2+3x+2$ *y* $x^2-x+4$ *en* $\mathbb{Z}_3[x]$

**Solución:** *Siguiendo el procedimiento del ejemplo anterior se obtienen los siguientes resultados: Al dividir* $x^3+2x^2+3x+2$ *entre* $x^2-x+4$ *que es lo mismo que dividir* $x^3+2x^2+2$ *entre* $x^2+2x+1$ *en* $\mathbb{Z}_3[x]$*, el primer residuo es* $2x+2$*; al dividir* $x^2+2x+1$ *entre* $2x+2$ *el residuo es* $x+1$*, y finalmente al dividir* $2x+2$ *entre* $x+1$ *el residuo es cero; por consiguiente el* $MCD(x^3+2x^2+3x+2, x^2-x+4)=x+1$*.*

**Ejemplo 11.** *(Derivada)*

*Sea* $F=\mathbb{Z}_3$*,entonces* $D(x^3)=3x^2=0$ *puesto que* $3=0$ *en* $\mathbb{Z}_3$*.*

## 2.1. Algoritmo de Factorización de Berlekamp

La estrategia del método de Berlekamp para factorizar un polinomio $f(x)$ en $\mathbb{Z}_P[x]$ consiste en traducir el problema en solucionar un sistema de ecuaciones lineales con coeficientes en $\mathbb{Z}_P$, y encontrar un $MCD$.
La matriz **Q** que involucra el algoritmo de factorización de Berlekamp se describe en la siguiente nota.

**NOTA:** Las filas de la matriz **Q** son los coeficientes de los polinomios residuales que se obtienen al aplicar el algoritmo de la división entre $x^{ip}$ y $f(x)$, donde $p$ es primo, $f(x)$ es el polinomio que se desea factorizar, y si $grad(f(x)) = d$, entonces $i = 0, 1, ..., d-1$.

**Teorema 12.** ***( Algoritmo de Factorización de Berlekamp):*** *Para encontrar una factorización* ***no trivial*** *de $f(x)$ en $\mathbb{Z}_P[x]$ de grado $d$, se halla la matriz* **Q** *y la solución* $\mathbf{b} = (b_0, ..., b_{d-1})$ *de* $\mathbf{b}(\mathbf{Q} - \mathbf{I}) = \mathbf{0}$. *Sea* $g(x) = b_0 + b_1x + ... + b_{d-1}x^{d-1}$; *si* $grad(g(x)) \geq 1$, *entonces para algún $s$ en $\mathbb{Z}_P$, $g(x) - s$ y $f(x)$ tienen un máximo común divisor de grado $\geq 1$ y,*

$$f(x) = \prod_{s=0}^{p-1} MCD(f(x), g(x) - s)$$

**Demostración:**

Sea $f(x) \in \mathbb{Z}_p[x]$ de grado $d$, el polinomio a factorizar.
Existe un polinomio $g(x) \in \mathbb{Z}_p[x]$, con $1 \leq grad(g(x)) < d$, tal que $f(x)$ divide a $(g(x))^p - g(x)$.
Si el grado de $g(x) = e \geq 1$ entonces $(g(x))^p - g(x) \neq 0$ porque el coeficiente de $x^{pe}$ es distinto de cero. Por el teorema de Fermat (**A7**), el polinomio $u^p - u$ tiene $p$ raices en $\mathbb{Z}_p$, sean $u = 0, 1, 2, ..., p-1$. Así,

$u^p - u$ se factoriza módulo $p$ en $u^p - u = u(u-1)(u-2)...(u-(p-1))$.

Haciendo $u = g(x)$, se obtiene que: $(g(x))^p - g(x) = g(x)(g(x)-1)(g(x)-2)...(g(x)-(p-1))$
Sea $g(x) = b_0 + b_1x + b_2x^2 + ... + b_{d-1}x^{d-1}$.

$(g(x))^p = (b_0 + b_1x + b_2x^2 + ... + b_{d-1}x^{d-1})^p$.

Por una aplicación del teorema del binomio que dice: Si $R$ es un campo de característica $p$ y $a, b$ son elementos de $R$, entonces $(a+b)^p = a^p + b^p$, (pues los términos entre $a^p$ y $b^p$ quedan multiplicados por $p$, anulándose.) se tiene que

$(g(x))^p = b_0^p + b_1^p x^p + ... + b_{d-1}^p x^{(d-1)p}$

Por el teorema de Fermat (**A7**) aplicado a cada $b_0, b_1, ..., b_{d-1}$, se tiene:

$b_i^p = b_i$ en $\mathbb{Z}_p$ para todo $i$, luego

$(g(x))^p = b_0 + b_1x^p + b_2x^{2p} + ... + b_{d-1}x^{(d-1)p}$

Si $f(x)$ divide a $(g(x))^p - g(x)$, entonces $(g(x))^p - g(x) \equiv 0(mod f(x))$.

Por propiedad de la congruencia $(g(x))^p \equiv g(x) mod(f(x))$.

Ahora, utilizando el teorema de la división, se divide cada $x^{pi}$ entre $f(x)$, para $i = 0, 1, 2, ..., d-1$, obteniendo:

$x^{pi} = f(x)q_i(x) + r_i(x)$.

Sustituyendo en $(g(x))^p$ se obtiene:

$(g(x))^p = b_0(f(x)q_0(x) + r_0(x)) + b_1(f(x)q_1(x) + r_1(x)) + b_2(f(x)q_2(x) + r_2(x)) + ... + b_{d-1}(f(x)q_{d-1}(x) + r_{d-1}(x))$.

De donde $(g(x))^p - g(x) = (b_0r_0(x) + b_1r_1(x) + b_2r_2(x) + ... + b_{d-1}r_{d-1}(x)$+ múltiplo de $f(x)) - (b_0 + b_1x + b_2x^2 + ... + b_{d-1}x^{d-1})$

Al hacer la congruencia módulo $f(x)$ se tiene que: $(g(x))^p - g(x) = (b_0r_0(x) + b_1r_1(x) + b_2r_2(x) + ... + b_{d-1}r_{d-1}(x)) - (b_0 + b_1x + b_2x^2 + ... + b_{d-1}x^{d-1})$.

$f(x)$ divide a $(g(x))^p - g(x)$ sí y sólo si $f(x)$ divide al polinomio $(b_0r_0(x) + b_1r_1(x) + b_2r_2(x) + ... + b_{d-1}r_{d-1}(x)) - (b_0 + b_1x + b_2x^2 + ... + b_{d-1}x^{d-1})$

Pero este polinomio tiene grado menor o igual que $d-1$, por consiguiente es divisible por $f(x)$ de grado $d$ sí y sólo si este es igual a cero, es decir sí y sólo si los coeficientes $b_0, b_1, ..., b_{d-1}$ de $g(x)$ satisfacen

$(b_0r_0(x) + b_1r_1(x) + b_2r_2(x) + ... + b_{d-1}r_{d-1}(x)) - (b_0 + b_1x + b_2x^2 + ... + b_{d-1}x^{d-1}) = 0$

Reuniendo los coeficientes de $1, x, x^2, ..., x^{d-1}$ se obtienen $d$ ecuaciones lineales con $d$ incógnitas $b_0, b_1, b_2, ..., b_{d-1}$. Solucionando este sistema de ecuaciones se obtienen los coeficientes del polinomio $g(x)$.

Aplicando conceptos del álgebra lineal se va a encontrar $\mathbf{b} = (b_0, b_1, ..., b_{d-1})$ en $\mathbf{b(Q\text{-}I)=0}$.
Las filas de la matriz $\mathbf{Q}$ son los coeficientes de los residuos ordenados, de izquierda a derecha, incrementando potencias de $x$.
Como $f(x)$ divide a $(g(x))^p - g(x)$, entonces $f(x) = MCD(f(x), g(x)(g(x)-1)(g(x)-2)...(g(x)-(p-1)))$.
Por lo tanto,

$$f(x) = MCD(f(x), g(x)) \cdot MCD(f(x), g(x)-1) \cdot ... \cdot MCD(f(x), g(x)-(p-1)) \qquad (1),$$

debido a que $g(x) - r$ y $g(x) - s$ son primos relativos para $r \neq s$.
Cada factor del lado derecho tiene grado a lo más el grado de $g(x)$, el cual es menor que $d$ , el grado de $f(x)$. Luego debe haber como mínimo dos factores no triviales de $f(x)$ en el lado derecho de (1), esto es, como mínimo dos factores de $f\ (x)$ de grado mayor o igual que 1, y (1) es una factorización no trivial de $f(x)$.
Usando notación matricial.

$$\text{Sea } \mathbf{Q} = \begin{bmatrix} r_{0,0} & r_{0,1} & ... & r_{0,d-1} \\ r_{1,0} & r_{1,1} & ... & r_{1,d-1} \\ . & & & . \\ . & & & . \\ . & & & . \\ r_{d-1,0} & r_{d-1,1} & ... & r_{d-1,d-1} \end{bmatrix}$$

la matriz cuyas filas son los coeficientes de los polinomios residuales $r_0(x), ..., r_{d-1}(x)$

**Ejemplo 12.** *En* $\mathbb{Z}_2[x]$, *sea* $f(x) = 1 + x + x^2 + x^3 + x^4 + x^5 + x^6$, $d = 6$.
*Se divide* $x^{2i}$ *entre* $f(x)$, $i = 0, 1, 2, 3, 4, 5$

$r_0(x) = 1;$
$r_1(x) = x^2;$
$r_2(x) = x^4;$
$r_3(x) = 1 + x + x^2 + x^3 + x^4 + x^5;$
$r_4(x) = x;$

$r_5(x) = x^3$;

$$\boldsymbol{Q} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix} \quad \textit{luego} \quad \boldsymbol{Q\text{-}I} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}$$

*Para encontrar a* $g(x) = b_0 + b_1x + b_2x^2 + b_3x^3 + b_4x^4 + b_5x^5$ *se soluciona* $\mathbf{b}(\mathbf{Q} - \mathbf{I}) = \mathbf{0}$. *Luego,*

$$\begin{aligned} b_3 &= 0 \\ b_1 + b_3 + b_4 &= 0 \\ b_1 + b_2 + b_3 &= 0 \\ b_5 &= 0 \\ b_2 + b_3 + b_4 &= 0 \\ b_3 + b_5 &= 0. \end{aligned}$$

*Esto se reduce rápidamente a* $b_3 = b_5 = 0$, $b_1 = b_2 = b_4$. *Las únicas soluciones con* $grad(g(x)) \geq 1$ *son* $g(x) = b_0 + x + x^2 + x^4$ *con* $b_0 = 0$ *o* $b_0 = 1$.

*Así* $f(x) = MCD(f(x), x^4 + x^2 + x) \cdot MCD(f(x), x^4 + x^2 + x + 1)$

$MCD(f(x), x^4 + x^2 + x) = x^3 + x + 1$

$MCD(f(x), x^4 + x^2 + x + 1) = x^3 + x^2 + 1$

*y ambos son irreducibles, luego la factorización de* $f(x)$ *en un producto de polinomios irreducibles en* $\mathbb{Z}_2[x]$ *es*

$f(x) = 1 + x + x^2 + x^3 + x^4 + x^5 + x^6 = (x^3 + x + 1)(x^3 + x^2 + 1)$.

**Ejemplo 13.** *Sea* $f(x) = x^5 + x^2 + 1 \in \mathbb{Z}_2[x]$

*Dividiendo* $x^{2i}$ *entre* $f(x)$, $i = 0, 1, 2, 3, 4$

$r_0(x) = 1$;

$r_1(x) = x^2$;

$r_2(x) = x^4$;

$r_3(x) = x^3 + x;$

$r_4(x) = x^3 + x^2 + 1;$

$$\boldsymbol{Q} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 \end{bmatrix} \qquad \boldsymbol{Q\text{-}I} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

$$\begin{aligned} b_4 &= 0 \\ b_1 + b_3 &= 0 \\ b_1 + b_2 + b_4 &= 0 \\ b_2 + b_4 &= 0 \\ b_1 = b_2 = b_3 = b_4 &= 0. \end{aligned}$$

*Por tanto,* $g(x) = b_0$*, luego*

$f(x) = MCD(f(x), b_0) \cdot MCD(f(x), b_0 + 1)$

*Si* $b_0 = 1$ *o* $b_0 = 0$ *se obtiene*

$f(x) = MCD(f(x), 0) \cdot MCD(f(x), 1)$

$f(x) = x^5 + x^2 + 1.$

$f(x)$ *es irreducible.*

No todos los valores posibles de $b_0, b_1, b_2, ..., b_{d-1}$ dan la factorización que se está buscando para $f(x)$, por eso lo que sigue da una muy buena orientación para saber que valores de $b_0, b_1, b_2, ..., b_{d-1}$ elegir.

Sea $N$ el conjunto de vectores $\mathbf{b} = (b_0, b_1, ..., b_{d-1})$ con $\mathbf{b}(\mathbf{Q} - \mathbf{I}) = \mathbf{0}$, $N$ es el **espacio nulo** de $\mathbf{Q} - \mathbf{I}$. Sea $\{\mathbf{v}_1, \mathbf{v}_2, ..., \mathbf{v}_r\}$ un conjunto de vectores en $N$ tal que todo vector $\mathbf{b}$ en $N$ es una combinación lineal de $\mathbf{v}_1, \mathbf{v}_2, ..., \mathbf{v}_r$ : para cualquier $\mathbf{b}$ en $N$ existen $x_1, ..., x_r$ en $\mathbb{Z}_p$ con $\mathbf{b} = x_1\mathbf{v}_1 + ... + x_r\mathbf{v}_r$. El $r$ más pequeño para el cual el conjunto $\{\mathbf{v}_1, \mathbf{v}_2, ..., \mathbf{v}_r\}$ existe es llamado la **dimensión** de $N$. Observe que el vector $\mathbf{b} = (a, 0, ..., 0)$ es siempre una solución de $\mathbf{b}(\mathbf{Q} - \mathbf{I}) = \mathbf{0}$, ya que $g(x)^p - g(x) = 0$ cuando $g(x)$ es el polinomio

constante $a$. Si las únicas soluciones de $\mathbf{b}(\mathbf{Q}-\mathbf{I})=\mathbf{0}$ son de la forma $\mathbf{b}=(a,0,...,0)$, entonces la dimensión de $N$ es 1, todo vector en el espacio nulo de $\mathbf{Q}-\mathbf{I}$ es un múltiplo de $\mathbf{v}_1=(1,0,...,0)$.

Para factorizar $f(x)$ se necesita encontrar otro vector $\mathbf{b}=(b_0,...,b_{d-1})$ con $\mathbf{b}(\mathbf{Q}-\mathbf{I})=\mathbf{0}$.

**Teorema 13.** *La dimensión del espacio nulo de* $\mathbf{Q}-\mathbf{I}$ *es igual al número de factores irreducibles distintos de* $f\,(x)$.

**Demostración:**

Suponga que $f(x)$ tiene $k$ factores irreducibles distintos, $f(x)=\prod_{i=1}^{k}(q_i(x))^{r_i}$ donde $q_i(x)$ es irreducible, y suponga que $f(x)$ divide a $(g(x))^p-g(x)$ para algún $g(x)$.
**Si** $f(x)$ **divide a** $(g(x))^p-g(x)=\prod_{s=0}^{p-1}(g(x)-s)$**, entonces cada factor irreducible** $q_i(x)$ **divide a** $g(x)-s$ **para alguna** $s$, y como $g(x)-s$ y $g(x)-t$ son primos relativos para $s\neq t$, el $s$ para el cual $q_i(x)$ divide a $g(x)-s$ no puede dividir tambien a $g(x)-t$.
Denote el único $s$, $0\leq s\leq p-1$ por $s_i$.
Ahora se define el recíproco de la implicación construida en el primer párrafo de la prueba.
Por el Teorema Chino del Residuo **(A1)**, dado cualquier $s_1,...,s_k$ elementos no necesariamente distintos en $\mathbb{Z}_p$ existe un polinomio único $g(x)$ en $\mathbb{Z}_p[x]$ tal que:

$$g(x)\equiv s_1(mod(q_1(x))^{r_1}),$$

$$\vdots$$

$$g(x)\equiv s_k(mod(q_k(x))^{r_k}),$$

donde los $(q_1(x))^{r_1},(q_2(x))^{r_2},...,(q_k(x))^{r_k}$ son primos relativos por parejas en $\mathbb{Z}_p[x]$ y el grado de $g(x)$ es menor que el grado de $(q_1(x))^{r_1}(q_2(x))^{r_2}...(q_k(x))^{r_k}$ es decir, menor que $d$. Así, $(q_i(x))^{r_i}$ divide a $g(x)-s_i$. Para tal $g(x)$, $(q_i(x))^{r_i}$ con $i=1,...,k$, divide a

$$\prod_{s=0}^{p-1}(g(x)-s)=(g(x))^p-g(x)$$

Por consiguiente, $f(x)=\prod_{i=1}^{k}(q_i(x))^{r_i}$ divide a $(g(x))^p-g(x)$.
Note que al variar algún $s_i$ se obtiene otra $k-upla$, $t_1,...,t_k$, para el $g(x)$, y de esta

manera se obtienen $p^k, \quad k-uplas$, dando $p^k$ posibles $g(x)$.

Por tanto, dado $s_1, ..., s_k$ se ha obtenido $g(x)$ de grado menor que $d$ tal que $f(x)$ divide a $(g(x))^p - g(x)$.

A $g(x)$, entonces, le corresponde el vector $(s_1, ..., s_k)$ de elementos de $\mathbb{Z}_p$. Esto define una función del conjunto de polinomios $g(x)$ al conjunto de $k-uplas$ $(s_1, ..., s_k)$ de elementos de $\mathbb{Z}_p$. Así se tiene una correspondencia $1-1$ entre polinomios $g(x)$ de grado menor que $d$ y las $k-uplas$ de elementos de $\mathbb{Z}_p$, donde $k$ es el número de factores irreducibles distintos de $f(x)$.

Hay ahora una correspondencia $1-1$ entre vectores del espacio nulo de **Q-I** y polinomios $g(x)$ de grado menor que $d$ correspondiendo al polinomio $g(x) = b_0 + b_1 x + ... + b_{d-1}x^{d-1}$ con el vector fila $(b_0, b_1, ..., b_{d-1})$ como en el Algoritmo de Berlekamp.

Dado que el espacio nulo de **Q-I** es de dimensión finita sobre $\mathbb{Z}_p$, entonces el espacio nulo de **Q-I** es isomorfo a las $k-uplas$ para un único entero $k$, de hecho $k$ es el número de elementos de cualquier base del espacio nulo de **Q-I** sobre $\mathbb{Z}_p$. Ese entero $k$ es llamado la dimensión del espacio nulo de **Q-I** sobre $\mathbb{Z}_p$. Se tenía que $k$ es el número de factores irreducibles distintos de $f(x)$.

**Corolario 2.** *$f(x)$ es irreducible en $\mathbb{Z}_p[x]$ sí y sólo si el espacio nulo de $\mathbf{Q}-\mathbf{I}$ tiene dimensión 1 y $f(x)$ y $f'(x)$ son primos relativos.*

**Demostración:**

De la demostración del teorema anterior, se tiene que el espacio nulo de **Q-I** es unidimensional sí y sólo si $f(x) = (p(x))^r$, una potencia de un polinomio irreducible. Entonces $r = 1$ y por la **proposición 2**, se tiene que $f(x)$ es irreducible sí y sólo si $f(x)$ y $f'(x)$ son primos relativos.

La dimensión del espacio nulo puede calcularse de la siguiente manera.

Como $\mathbf{Q}-\mathbf{I}$ es una matriz $d \times d$, la dimensión del espacio nulo de $\mathbf{Q}-\mathbf{I}$ puede calcularse como $d$ menos $R_{Q-I}$ o $C_{Q-I}$ ($R_{Q-I}$ = posición de las filas de $\mathbf{Q}-\mathbf{I}$, $C_{Q-I}$ = posición de las columnas de $\mathbf{Q}-\mathbf{I}$).

La posición de las columnas de $\mathbf{Q}-\mathbf{I}$ es igual al número de columnas distintas de cero después de operar en forma escalonadalas columnas en $\mathbf{Q}-\mathbf{I}$. Del ejemplo **12**, se tiene

$$\mathbf{Q}-\mathbf{I}=\begin{bmatrix}0&0&0&0&0&0\\0&1&1&0&0&0\\0&0&1&0&1&0\\1&1&1&0&1&1\\0&1&0&0&1&0\\0&0&0&1&0&1\end{bmatrix}\xrightarrow{(1)}\begin{bmatrix}0&0&0&0&0&0\\1&0&0&1&0&0\\0&1&0&1&0&0\\1&1&1&1&0&1\\1&1&0&0&0&0\\0&0&0&0&1&1\end{bmatrix}\xrightarrow{(2)}\begin{bmatrix}0&0&0&0&0&0\\1&0&0&0&0&0\\0&1&0&1&0&0\\1&1&1&0&0&1\\1&1&0&1&0&0\\0&0&0&0&1&1\end{bmatrix}$$

$$\xrightarrow{(3)}\begin{bmatrix}0&0&0&0&0&0\\1&0&0&0&0&0\\0&1&0&0&0&0\\1&1&1&1&0&1\\1&1&0&0&0&0\\0&0&0&0&1&1\end{bmatrix}\xrightarrow{(4)}\begin{bmatrix}0&0&0&0&0&0\\1&0&0&0&0&0\\0&1&0&0&0&0\\1&1&1&0&0&0\\1&1&0&0&0&0\\0&0&0&0&1&0\end{bmatrix}\xrightarrow{(5)}\begin{bmatrix}0&0&0&0&0&0\\1&0&0&0&0&0\\0&1&0&0&0&0\\0&0&1&0&0&0\\1&1&0&0&0&0\\0&0&0&1&0&0\end{bmatrix}=\mathbf{E}$$

En (1) se intercambian columnas

(2) Se adiciona la primera columna a la cuarta.

(3) Se adiciona la segunda columna a la cuarta.

(4) Se adiciona la tercera columna a la cuarta y sexta, y se adiciona la quinta columna a la sexta.

(5) Se adiciona la tercera columna a las primeras dos y se intercambian la cuarta y quinta.

La matriz $\mathbf{E}$ tiene cuatro columnas distintas de cero, entonces el espacio nulo tiene dimensión $6-4=2$ . De hecho una base del espacio nulo puede obtenerse solucionando $\mathbf{bE}=\mathbf{0}$ (hacer operaciones a las columnas de $\mathbf{Q}-\mathbf{I}$ corresponde a hacerle manipulaciones a la ecuación $\mathbf{b}\left(\mathbf{Q}-\mathbf{I}\right)=\mathbf{0}$ , las cuales no cambian el conjunto solución de $\mathbf{b}\left(\mathbf{Q}-\mathbf{I}\right)=\mathbf{0}$ y se llega a la ecuación simple $\mathbf{bE}=\mathbf{0}$). Al solucionar $\mathbf{bE}=\mathbf{0}, b_0$ y $b_4$ pueden escogerse arbitrarios, y, una vez elegidos, se determina una solución $\mathbf{b}$ única. Las soluciones a $\mathbf{bE}=\mathbf{0}$ tienen la forma:

$(b_0, b_1, b_2, b_3, b_4, b_5) = (b_0, b_4, b_4, 0, b_4, 0) = b_0 (1, 0, 0, 0, 0, 0) + b_4 (0, 1, 1, 0, 1, 0)$

Se escoge $b_4 = 1$.

**Ejemplo 14.** *¿Cuántos factores irreducibles distintos dividen a* $f(x) = x^5 + 2x^4 + x^3 + x^2 + 2$ *en* $\mathbb{Z}_3[x]$*?*

*Se calcula* $\mathbf{Q} - \mathbf{I}$

$1 = f(x)\, 0 + 1;$

$x^3 = f(x)\, 0 + x^3;$

$x^6 = f(x)(x+1) + 1 + x + 2x^2 + x^3$

$x^9 = f(x)(x^4 + x^3 + x) + x$

$x^{12} = f(x)(x^7 + x^6 + x^4) + x^4$

*Así*

$$\mathbf{Q} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 2 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} \quad , \quad \mathbf{Q} - \mathbf{I} = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

*Despues de hacer operaciones columna se obtiene:*

$$\begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

*Por tanto, el espacio nulo de* $\mathbf{Q} - \mathbf{I}$ *tiene dimensión* 3*,* $f(x)$ *tiene* 3 *factores irreducibles distintos, y cualquier polinomio* $g(x)$ *de la forma*

$b_0 + b_1 x + b_2 x^2 + b_3 x^3 + b_4 x^4 = b_0 + b_3 x + 0x^2 + b_3 x^3 + b_4 x^4$

*está en el espacio nulo, donde* $b_0, b_3, b_4$ *son arbitrarios.*

$(b_0, b_1, b_2, b_3, b_4) = (b_0, b_3, 0, b_3, b_4) =$

$$b_0(1, 0, 0, 0, 0) + b_3(0, 1, 0, 1, 0) + b_4(0, 0, 0, 0, 1)$$

*Si* $b_3 = 1$ *y* $b_0 = b_4 = 0$, *entonces* $g(x) = x + x^3$.

*Por tanto,*

$$f(x) = MCD(f(x), x + x^3 + 2)MCD(f(x), x + x^3 + 1)MCD(f(x), x + x^3)$$

$f(x) = (2x + 2)(x^2 + x + 2)(2x^2 + 2)$

$f(x) = (x + 1)(x^2 + x + 2)(x^2 + 1)$

# Capítulo 3

# Irreducibilidad en $\mathbb{Q}[x]$

En esta sección se consideraran problemas como: ¿qué polinomios con coeficientes en $\mathbb{Q}$ son irreducibles?, ¿cómo encontrar las raíces racionales, o más generalmente los factores irreducibles de un polinomio en $\mathbb{Q}[x]$?.

La situación en $\mathbb{Q}[x]$ es diferente a $\mathbb{R}[x]$ o $\mathbb{C}[x]$. Mientras que en $\mathbb{R}[x]$ o $\mathbb{C}[x]$ se pueden describir explícitamente todos los polinomios irreducibles, en $\mathbb{Q}[x]$ no, pero sí se pueden describir ciertos criterios que implican irreducibilidad. Esta sección está dedicada a describir estos criterios. Como en el capítulo 2, se muestra como funcionan algunas de las definiciones y teoremas del capítulo 1 en $\mathbb{Q}[x]$.

**Ejemplo 15.** *(Raíz de un polinomio)*

*(1.) Si se considera $p(x) = x^2 - 2$ como elemento de $\mathbb{Q}[x]$, entonces $p(x)$ no tiene raíces, pues $\sqrt{2}$ y $-\sqrt{2}$ son números irracionales. En consecuencia, la existencia de las raíces de un polinomio depende del anillo correspondiente para los coeficientes.*

*(2.) Sea $f(x) = ax^2 + bx + c$ con $a$, $b$, $c \in \mathbb{Q}$, $a \neq 0$. Si $\Delta$ tiene una raíz cuadrada en $\mathbb{Q}$, entonces el polinomio tiene dos raíces racionales. Pero en este caso también existen polinomios de grado 2 con raíces reales pero sin raíces racionales como en (1).*

**Ejemplo 16.** *(Polinomios asociados) $x^2 + 3x + 1$ y $5x^2 + 15x + 5$ son asociados.*

**Ejemplo 17.** *(Teorema de la división)*

*Si se divide el polinomio* $f(x) = x^5 - x^3 + x^2 + 7$ *entre* $g(x) = x^3 + 3x^2 + x + 5$, *por el algoritmo de la división se obtienen los polinomios* $q(x)$ *y* $r(x)$ *de tal manera que* $f(x) = g(x)q(x) + r(x)$, *así*

$$x^5 - x^3 + x^2 + 7 = (x^3 + 3x^2 + x + 5)(x^2 - 3x + 7) + (-22x^2 + 8x - 28).$$

**Ejemplo 18.** *(Polinomios Irreducibles)*

***a.)*** *Al aplicar la parte (b) del teorema 1 (capítulo 1) al polinomio* $x^2 + 1$ *se puede deducir que es irreducible en* $\mathbb{Q}[x]$, *pues este polinomio no tiene raíces en* $\mathbb{Q}$.

***b.)*** *Si* $f(x) \in \mathbb{Q}[x]$ *es reducible no implica que* $f(x)$ *tiene raíces en* $\mathbb{Q}$. *Por ejemplo el polinomio* $(x^2 - 2)^n$ *es reducible y sin raíces racionales.*

**Ejemplo 19.** *(Lema de Bezout (Teorema 8, capítulo 1))*

***(a)*** *Si* $d(x)$ *es el MCD de* $f(x) = x^3 - x^2 - 3x + 6$ *y* $g(x) = x^3 + 3x^2 - 4$, *escribir* $d(x)$ *como* $a(x)f(x) + b(x)g(x)$ *para algunos* $a(x)$, $b(x)$ *en* $\mathbb{Q}[x]$.

**Solución:**

*Aplicando el algoritmo de la división se obtiene:*

$$x^3 - x^2 - 3x + 6 = (x^3 + 3x^2 - 4)1 + (-4x^2 - 3x + 10)x^3 + 3x^2 - 4$$

$$= \left(-4x^2 - 3x + 10\right)\left(\frac{-1}{4}x - \frac{9}{16}\right) + \left(\frac{13}{16}x + \frac{13}{8}\right) - 4x^2 - 3x + 10$$

$$= \left(\frac{13}{16}x + \frac{13}{8}\right)\left(\frac{-64}{13}x + \frac{80}{13}\right) + 0$$

*Como en la última ecuación el residuo es cero, el* $MCD(f(x), g(x)) = \dfrac{13}{16}x + \dfrac{13}{8}$; *que se puede expresar como una combinación lineal de* $f(x)$ *y* $g(x)$ *así:*

$$(-4x^2 - 3x + 10) = (x^3 - x^2 - 3x + 6) - (x^3 + 3x^2 - 4)1x^3 + 3x^2 - 4$$

$$= \left(\left(x^3 - x^2 - 3x + 6\right) - \left(x^3 + 3x^2 - 4\right)1\right)\left(\frac{-1}{4}x - \frac{9}{16}\right) + \left(\frac{13}{16}x + \frac{13}{8}\right)\frac{13}{16}x + \frac{13}{8}$$

$$= \left(x^3+3x^2-4\right) - \left(\left(x^3-x^2-3x+6\right) - \left(x^3+3x^2-4\right)1\right)\left(\frac{-1}{4}x-\frac{9}{16}\right)\frac{13}{16}x+\frac{13}{8}$$

$$= -\left(\frac{-1}{4}x-\frac{9}{16}\right)\left(x^3-x^2-3x+6\right)+\left(1+\left(\frac{-1}{4}x-\frac{9}{16}\right)\right)\left(x^3+3x^2-4\right)$$

***(b)*** *Si $d(x)$ es el MCD de $f(x) = x^{11} - 1$ y $g(x) = x^9 - 1$, escribir $d(x)$ como $a(x)f(x) + b(x)g(x)$ para algunos $a(x)$, $b(x)$ en $\mathbb{Q}[x]$.*

**Solución:**

*Siguiendo el proceso del ejemplo anterior se obtiene el $MCD(f(x), g(x)) = x - 1$, que se puede escribir como: $x-1 = -(x^{11}-1)(x^7+x^5+x^3+x)+(x^9-1)[1+x^2(x^7+x^5+x^3+x)]$*

**Ejemplo 20.** *(Combinación Lineal)*

*Encontrar $a(x)$y $b(x)$ tal que $a(x)(2x^3 - 7x^2 + 7x - 2) + b(x)(2x^3 + x^2 + x - 1) = 2x - 1$*

**Solución:**

*Siguiendo el proceso de los ejemplos anteriores se llega a que $a(x) = \frac{5}{16} - \frac{1}{4}x$ y $b(x) = 1 + \frac{1}{16}(4x - 5)$*

**Ejemplo 21.** *(Derivada de un Polinomio: Factores Múltiples) Sean $f(x) = x^3 - 7x - 6$ y su derivada $f'(x) = 3x^2 - 7$, $f(x)$ y $f'(x)$ son primos relativos, por tanto $f(x)$ no tiene factores múltiples.*

Formalmente empieza el capítulo con el siguiente teorema:

**Teorema 14.** ***(Teorema de las Raíces Racionales):***

*Sea $p(x) = a_nx^n + a_{n-1}x^{n-1} + ... + a_3x^3 + a_2x^2 + a_1x + a_0$ cualquier polinomio con coeficientes enteros. Si el número racional $\frac{c}{d}$ es una raíz de $p(x) = 0$, con $c$, $d$ enteros primos relativos, entonces $c$ debe ser un factor de $a_0$ y $d$ debe ser un factor de $a_n$.*

**Demostración:** Si $\frac{c}{d}$ es una raíz de $p(x)$, $p(\frac{c}{d}) = 0$.
$p\left(\frac{c}{d}\right) = a_n\left(\frac{c}{d}\right)^n + a_{n-1}\left(\frac{c}{d}\right)^{n-1} + ... + a_3\left(\frac{c}{d}\right)^3 + a_2\left(\frac{c}{d}\right)^2 + a_1\left(\frac{c}{d}\right) + a_0 = 0.$
Multiplicando este resultado por $d^n$ se obtiene:
$a_nc^n + a_{n-1}c^{n-1}d + ... + a_3c^3d^{n-3} + a_2c^2d^{n-2} + a_1cd^{n-1} + a_0d^n = 0.$
$a_nc^n + a_{n-1}c^{n-1}d + ... + a_3c^3d^{n-3} + a_2c^2d^{n-2} + a_1cd^{n-1} = -a_0d^n.$
$c(a_nc^{n-1} + a_{n-1}c^{n-2}d + ... + a_3c^2d^{n-3} + a_2cd^{n-2} + a_1d^{n-1}) = -a_0d^n.$
Entonces $c$ debe dividir a $a_0d^n$, pero como $c$ y $d$ son primos relativos, $c$ divide a $a_0$. Similarmente, $d$ debe dividir a $a_nc^n$, y por la misma razón, $d$ divide a $a_n$.

**Ejemplo 22.** ***a.)*** *Las posibles raíces racionales del polinomio* $x^4 + 8x^3 + 15x^2 - 6x - 9$ *son* $x = 1, -1, 3, -3, 9,$ *o* $-9$, *ya que estos son los únicos divisores de* $-9$.

*Como* $a_n$ *y* $a_0$ *tienen solo un número finito de divisores, el teorema limita las posibles raíces racionales de un polinomio con coeficientes enteros a sólo un número finito.*

***b.)*** *Sea* $p(x) = 15x^3 + 53x^2 - 30x - 8$. *Se tiene que el producto de las raíces de este polinomio es la fracción* $(-1)^3(-8/15)$. *Así que las únicas raíces racionales posibles son* $\pm1, \pm1/3, \pm1/5, \pm1/15, \pm2, \pm2/3, \pm2/5, \pm2/15, \pm4, \pm4/3, \pm4/5, \pm4/15, \pm8, \pm8/3, \pm8/5, \pm8/15$. *Después de realizar los cálculos correspondientes se ve que, en efecto* $-1/5$, $2/3$, *y* $-4$ *son raíces del polinomio.*

**Corolario 3.** *Sea* $p(x) = x^n + a_{n-1}x^{n-1} + ... + a_3x^3 + a_2x^2 + a_1x + a_0$ *cualquier polinomio con coeficientes enteros y coeficiente principal 1. Si* $p(x)$ *tiene ceros racionales, entonces todos deben ser enteros.*

**Demostración:** Por el teorema **14** se sabe que el denominador de cualquier cero racional divide al coeficiente principal que en este caso es 1. Así cualquier denominador debe ser $\pm1$ haciendo el cero racional un entero.

## 3.1. Lema de Gauss

Sea $f(x) = a_nx^n + ... + a_1x + a_0$ un polinomio con coeficientes racionales $a_n, ..., a_1$, $a_0$. Se puede multiplicar $f(x)$ por el mínimo común múltiplo de los denominadores de los

coeficientes, llamése $s$, y se obtiene un polinomio con coeficientes enteros, $sf(x) = g(x)$. Como $g(x)$ y $f(x)$ son asociados, $g(x)$ **será irreducible** en $\mathbb{Q}[x]$ **si y sólo si** $f(x)$ lo es. Así en el estudio de polinomios en $\mathbb{Q}[x]$, se puede asumir siempre que ellos tienen coeficientes enteros.

**Definición 14.** *Un polinomio $f(x)$ de grado $n \geq 1$ con coeficientes racionales es* ***primitivo*** *si $f(x)$ tiene coeficientes enteros y el máximo común divisor de estos coeficientes es* 1.

**Proposición 3.** *Cualquier polinomio con coeficientes enteros es un asociado en $\mathbb{Q}[x]$ de un polinomio primitivo.*

**Demostración:** Si el máximo común divisor de los coeficientes de $f(x)$ es $t$, donde $t$ es un entero distinto de cero, entonces $(\frac{1}{t})f(x)$ es un polinomio con coeficientes enteros, el máximo común divisor de los coeficientes de $(\frac{1}{t})f(x)$ es uno y $f(x)$ con $(\frac{1}{t})f(x)$ son asociados en $\mathbb{Q}[x]$. Por tanto cualquier polinomio en $\mathbb{Q}[x]$ es un asociado de un polinomio primitivo.

**Lema 1.** ***(Lema de Gauss):*** *El producto de dos polinomios primitivos es de nuevo un polinomio primitivo.*

**Demostración:** Sea $f(x) = a_n x^n + ... + ax + a_0$ y $g(x) = b_n x^n + ... + bx + b_0$. Supóngase que el lema es falso; entonces todos los coeficientes de $f(x)g(x)$ serían divisibles por algún entero mayor que 1, en consecuencia por algún primo $p$. Como $f(x)$ es primitivo, $p$ no divide a algún coeficiente $a_i$. Sea $a_j$ el primer coeficiente de $f(x)$ que no divide $p$. Similarmente sea $b_k$ el primer coeficiente de $g(x)$ que no divide $p$. En $f(x)g(x)$ el coeficiente de $x^{j+k}$, $c_{j+k}$ es:

$$c_{j+k} = a_j b_j + (a_{j+1}b_{k-1} + a_{j+2}b_{k-2} + ... + a_{j+k}b_0) + (a_{j-1}b_{k+1} + a_{j-2}b_{k+2} + ... + a_0 b_{j+k}). \qquad (1)$$

Ahora por la forma en que se escogió $b_k$, $p \mid b_{k-1}, b_{k-2}, ...$ así que $p \mid a_{j+1}b_{k-1} + a_{j+2}b_{k-2} + ... + a_{j+k}b_0$. Similarmente, por la forma en que se escogió $a_j$, $p \mid a_{j-1}, a_{j-2}, ...$ así que $p \mid a_{j-1}b_{k+1} + a_{j-2}b_{k+2} + ... + a_0 b_{k+j}$. Como $p \mid f(x)g(x)$, entonces $p \mid c_{j+k}$. Así por (1), $p \mid a_j b_k$, lo cual es una contradicción ya que $p \nmid a_j$ y $p \nmid b_k$.

El resultado más importante de esta sección es:

**Lema 2.** *Sea $f(x)$ un polinomio con coeficientes enteros. Si $f(x) = a(x)b(x)$ en $\mathbb{Q}[x]$, entonces $f(x) = a_1(x)b_1(x)$ con $a_1(x)$ y $b_1(x)$ polinomios con coeficientes enteros, y con $a_1(x)$ y $b_1(x)$ asociados de $a(x)$ y $b(x)$ respectivamente.*

El **lema 2** implica que para mostrar que $f(x)$ en $\mathbb{Z}[x]$ es irreducible en $\mathbb{Q}[x]$, es suficiente probar que $f(x)$ no se factoriza en el producto de dos polinomios con coeficientes enteros.

**Demostración:** Si $f(x) = a(x)b(x)$ en $\mathbb{Q}[x]$, entonces $rf(x) = ra(x)b(x)$ para cualquier racional $r \neq 0$.Si se prueba el lema para $rf(x)$, entonces queda probado para $f(x)$. Se puede asumir sin pérdida de generalidad que $f(x)$ es un polinomio primitivo. Ahora si $f(x) = a(x)b(x)$, donde $a(x)$ y $b(x)$ son polinomios con coeficientes racionales, entonces existen números racionales $s \neq 0, t \neq 0$, tal que $sa(x)$ y $tb(x)$ son primitivos. Por el lema **1**, se tiene que $sta(x)b(x) = stf(x)$ es entonces un polinomio primitivo asociado a $f(x)$.

**Observación 1.** *Si $r$ es un número racional tal que $rf(x)$ y $f(x)$ son polinomios primitivos, entonces $r = 1$ o $r = -1$.*

Teniendo en cuenta esto, $st = \pm 1$, luego $f(x) = \pm sa(x)tb(x)$. Se puede colocar $a_1(x) = \pm sa(x), b_1(x) = tb(x)$ para completar la demostración del **lema 2**.
El **lema 2** afirma que si un polinomio es irreducible en $\mathbb{Z}[x]$, entonces es irreducible como polinomio en $\mathbb{Q}[x]$.

## 3.2. Prueba para la Irreducibilidad

Encontrar raíces es lo mismo que encontrar factores de grado uno. Es difícil encontrar todos los factores de un polinomio de cualquier grado con coeficientes racionales. El resto de esta sección es una introducción a este problema.

**Teorema 15.** ***(Criterio de Irreducibilidad de Eisenstein):***

*Si* $f(x) = a_n x^n + ... + a_1 x + a_0$ *un polinomio con coeficientes enteros. Suponga que para algún primo* $p$, $p \nmid a_n$, $p \mid a_{n-1}, p \mid a_{n-2}, ..., p \mid a_1, p \mid a_0$, *pero* $p^2 \nmid a_0$. *Entonces* $f(x)$ *es irreducible sobre los racionales.*

El teorema muestra que existen polinomios irreducibles en $\mathbb{Q}[x]$ de cualquier grado, por ejemplo, $f(x) = x^n - 2$.

**Demostración:** Sin pérdida de generalidad se asume que $f(x)$ es primitivo para que al tomar el $MCD$ de los coeficientes no se altere la hipótesis, ya que $p \nmid a_n$. Si $f(x)$ se factoriza como el producto de dos polinomios con coeficientes racionales, del lema 2 $f(x)$ se factoriza como el producto de dos polinomios con coeficientes enteros. Suponga que $f(x)$ es reducible, entonces

$$f(x) = (b_r x^r + ... + b_1 x + b_0)(c_s x^s + ... + c_1 x + c_0),$$

donde los $b_i$ y $c_j$ son enteros, y $r, s > 0$. Ahora $a_0 = b_0 c_0$. Como $p \mid a_0$, $p$ debe dividir a $b_0$ o a $c_0$. Pero $p^2 \nmid a_0$, así que $p$ no divide a $b_0$ y $c_0$. Suponga que $p \mid b_0$, $p \nmid c_0$. No todos los coeficientes $b_r, ..., b_1, b_0$ pueden ser divisibles por $p$, pues de ser así todos los coeficentes de $f(x)$ serían divisibles por $p$, lo cual es evidentemente falso puesto que $p \nmid a_n$. Sea $b_k$ el primer $b_i$ que no es divisible por $p$, $k < r < n$. Entonces $p \mid b_{k-1}$ y a los $b_i$ que siguen. Pero $a_k = b_k c_0 + b_{k-1} c_1 + b_{k-2} c_2 + ... + b_0 c_k$, y $p \mid a_k$, entonces $p \mid b_{k-1}$, $b_{k-2}$,...,$b_0$, por tanto $p \mid b_k c_0$. Sin embargo, $p \nmid c_0$, $p \nmid b_k$, lo que se contradice con el hecho de que $p \mid b_k c_0$. Esta contradicción prueba que no se puede obtener una factorización para $f(x)$ y por tanto $f(x)$ es irreducible.

El siguiente teorema se enuncia para un polinomio con coeficientes enteros, pero debe ser claro que se puede aplicar a cualquier polinomio con coeficientes racionales.

**Teorema 16.** *Sea* $f(x) = a_n x^n + ... + a_1 x + a_0$ *un polinomio con coeficientes enteros. Suponga que para algún* $n$, $n \nmid a_n$, $\overline{f}(x)$ *en* $\mathbb{Z}_n[x]$ *es irreducible. Entonces* $f(x)$ *es irreducible en* $\mathbb{Q}[x]$.

**Demostración:** Se prueba por el contrarrecíproco.

Si $f(x)$ es un polinomio con coeficientes enteros el cual es primitivo, entonces se pueden reducir los coeficientes módulo $n$ para cualquier $n$ y obtener un polinomio distinto de cero $\overline{f}(x)$ en $\mathbb{Z}_n[x]$. Si $n$ no divide al coeficiente principal de $f(x)$, entonces $\overline{f}(x)$ en $\mathbb{Z}_n[x]$ tiene el mismo grado de $f(x)$.

Supóngase que $f(x) = a(x)b(x)$, donde $a(x), b(x)$ tienen coeficientes enteros, con $grad(a(x)) < grad(f(x))$, $grad(b(x)) < grad(f(x))$. Por el lema de Gauss $a(x)$ y $b(x)$ son primitivos. Entonces $\overline{f}(x) = \overline{a}(x)\overline{b}(x)$, en $\mathbb{Z}_n[x]$ por el lema 2. Por lo tanto,$\overline{f}(x)$ se puede factorizar.

La prueba para la irreducibilidad de $\overline{f}(x)$ en $\mathbb{Z}_n[x]$ es un problema finito, porque existe solo un número finito de posibles divisores de $\overline{f}(x)$.

**Ejemplo 23.** *Sea* $f(x) = 3x^5 - 4x^4 + 2x^3 + x^2 + 18x + 31$ *en* $\mathbb{Q}[x]$, $f(x)$ *es congruente a* $\overline{f}(x) = x^5 + x^2 + 1$ *en* $\mathbb{Z}_2[x]$.
*Por el algoritmo de Berlekamp* $\overline{f}(x) = x^5 + x^2 + 1$ *es irreducible en* $\mathbb{Z}_2[x]$ *(**Ejemplo 13**).*
*Por lo tanto* $f(x) = 3x^5 - 4x^4 + 2x^3 + x^2 + 18x + 31$ *es irreducible en* $\mathbb{Q}[x]$.

## 3.3. Polinomios Reducibles Módulo Todo Primo

Como se vió en el teorema **16** un polinomio con coeficientes enteros es irreducible sobre los racionales si es irreducible módulo algún primo, sin embargo el recíproco "Si un polinomio es irreducible sobre los racionales entonces es irreducible módulo algún primo" no es verdad en general como se podrá ver en lo que sigue.
Solomon W. Golomb mostró que el polinomio ciclotómico $\phi_k(x)$ es irreducible en $\mathbb{Q}[x]$ pero es reducible módulo todo primo para ciertos valores de $k$; recuérdese que los polinomios $\phi_n(x)$ se definen inductivamente por:

**a)** $\phi_1(x) = x - 1$

**b)** Si **n>1**, entonces $\phi_n(x) = \dfrac{x^n - 1}{\prod_{\phi d(x)}}$, donde en el productorio del denominador, $d$ recorre todos los divisores positivos de $n$ excepto para $n$ mismo.

**Ejemplo 24.** ***1***.$\phi_2(x) = \dfrac{x^2-1}{\phi_1(x)} = \dfrac{x^2-1}{x-1} = \dfrac{(x-1)(x+1)}{x-1} = x+1$

***2***.$\phi_3(x) = \dfrac{x^3-1}{\prod_{\phi d(x)}} = \dfrac{(x-1)(x^2+x+1)}{x-1} = x^2+x+1$

***3***.$\phi_4(x) = \dfrac{x^4-1}{(x-1)(x+1)} = \dfrac{(x^2-1)(x^2+1)}{(x-1)(x+1)} = \dfrac{(x^2+1)(x-1)(x+1)}{(x-1)(x+1)} = x^2+1$

***4***.$\phi_5(x) = \dfrac{x^5-1}{(x-1)} = \dfrac{(x-1)(x^4+x^3+x^2+x+1)}{x-1} = x^4+x^3+x^2+x+1$

***5***.$\phi_6(x) = \dfrac{x^6-1}{(x-1)(x+1)(x^2+x+1)} = \dfrac{(x^3-1)(x^3+1)}{(x^3-1)(x+1)} = \dfrac{x^3+1}{x+1} = x^2-x+1$

Para la demostración de la que se habla, Golomb utilizó los siguientes teoremas:

**Teorema 17.** *Sea $\phi_n(x)$ el polinomio ciclotómico de orden $n$. Entonces $\phi_n(x^r)$ es irreducible sobre el campo de los racionales si y sólo si todo factor primo de $r$ es también un factor primo de $n$.*

**Demostración:** la demostración se deduce directamente de lo siguiente:

$\phi_n(x^r) = \phi_{rn}(x)$ si todo primo que divide a $r$ divide tambien a $n$.

$\phi_n(x^r) = \phi_n(x^w)\,\phi_{np}(x^w)$ si $r = pw$ y el primo $p \nmid n$.

**Teorema 18.** *El polinomio ciclotómico $\phi_n(x)$ se factoriza módulo $q$ para todo primo $q$, excepto cuando $n = 1, 2, 4, p^k$ o $2p^k$ , donde $p$ es un primo impar y $k$ es un entero positivo, en tal caso $\phi_n(x)$ permanece irreducible módulo $q$ para infinitos primos $q$, mientras que se factoriza módulo $q$ si $n > 2$ para otros infinitos primos $q$.*

**Demostración:** La idea de la demostración del teorema 18 es la siguiente:

**Caso 1**: $n \neq 1, 2, 4, p^k$ o $2p^k$.

En este caso el grupo de Galois del polinomio no es cíclico módulo $q$, así que $\phi_n(x)$ se factoriza módulo $q$ para infinitos primos $q$.

**Caso 2:** Cuando $n = 1$ o $n = 2$, $\phi_n(x)$ es lineal, así que permanecen irreducibles módulo $q$, para todo $q$.

**Caso 3:** Si $n = 4, p^k$ o $2p^k$ se garantiza que existe por lo menos una raíz primitiva. Sea $g$

tal raíz.

Entonces $\phi_n(x)$ permanece irreducible para aquellos primos $q$ tales que $q \equiv g(\mod n)$ mientras que $\phi_n(x)$ siempre se factorizará para aquellos primos $q$ tales que $q \equiv h(\mod n)$, donde $h$ no es raíz primitiva módulo $n$ y $(h,n)=1$.

La demostración formal de este teorema se encuentra en **A15**.

**Ejemplo 25.** $\phi_{12}(x) = x^4 - x^2 + 1$. *En este caso* $n = 12$ *y su grupo de Galois es isomorfo a* $\overline{Z}_{12} = \{1,5,7,11\}$. *Así que* $\phi_{12}(x)$ *se factorizará para aquellos primos que sean congruentes con cualquiera de los elementos de* $\overline{Z}_{12}$ *módulo* 12. *Por ejemplo, sea* $q = 13$, $13 \equiv 1(mod 12)$.

*Así que en* $\mathbb{Z}_{13}$: $\phi_{12}(x) = x^4 - x^2 + 1 = (x+2)(x+6)(x+7)(x+11)$.

$\phi_{12}(x)$ *no tiene raíces ni* $\mathbb{Z}_5$, *ni en* $\mathbb{Z}_7$, *ni en* $\mathbb{Z}_{11}$, *pero utilizando el algoritmo de Berlekamp, se obtiene la respectiva factorización en cada campo. En* $\mathbb{Z}_5$, $\phi_{12}(x) = (4x^2+2x+1)(4x^2+3x+1)$.

**Ejemplo 26.** $\phi_6(x) = x^2 - x + 1$, *donde* $6 = 2 * 3^1$. *El grupo multiplicativo módulo* 6 *consiste de* 1 *y* 5, *en el cual* 5 *es raíz primitiva y* 1 *no lo es. De este modo* $\phi_6(x)$ *permanece irreducible módulo q siempre que* $q \equiv 5(\mod 6)$, *mientras que* $\phi_6(x)$ *se factoriza en dos factores lineales (módulo q) siempre que* $q \equiv 1(\mod 6)$. *Asi,* $x^2 - x + 1$ *es irreducible* mod 5, *mientras que* $x^2 - x + 1 = (x+2)(x-3)(\mod 7)$.

Estos dos teoremas pueden combinarse para obtener el siguiente:

**Teorema 19.** $\phi_n(x^r)$ *es irreducible módulo q, para todo primo q, excepto en los siguientes casos:*

$n = 1, r = 1$; $n = 2, r = 1, 2$; $n = 4, r = 1$; $n = p^k, r = p^l \quad (l \geq 0)$; $n = 2p^k, r = p^l$ $(l \geq 0)$.

En estos casos excepcionales, $\phi_n(x^r)$ es de nuevo ciclotómico, y su factorización módulo $q$ es como se especifica en el Teorema **18**.

**Demostración:** Para que $\phi_n(x^r)$ sea irreducible módulo $q$, debe ser irreducible sobre los racionales, lo cual impone la condición del Teorema **17** sobre $r$, y $\phi_n(x)$ debe ser irreducible módulo $q$, lo cual imponen las condiciones del Teorema **18** sobre $n$.

El requisito final es que $\phi_n(x^r) = \phi_{rn}(x)$ debe tener un grupo cíclico de Galois módulo $q$. Combinando estas condiciones se obtiene el resultado indicado.

**Ejemplo 27.** *$\phi_6(x^r) = x^{2r} - x^r + 1$ es irreducible sobre los racionales si y sólo si $r = 3^k$. Ahora, todos los polinomios $x^{2*3^k} - x^{3^k} + 1$ permanecen irreducibles módulo algún primo $q$ con $q \equiv 5 (\mod 6)$, mientras que se puede factorizar módulo $q$ para todo primo $q$ con $q \equiv 1 (\mod 6)$.*

**Teorema 20.** *Sea $n \neq 1$ un entero positivo. Entonces existe un polinomio entero mónico, irreducible de grado $n$ que es reducible módulo todo primo si y sólo si $n$ no es un primo.*

La demostración de este resultado está fuera de los objetivos de este trabajo; sin embargo se presenta en **B6.**

**Ejemplo 28.** *Sean $g(x) = x^5 - x - 1$ y $v_1, ..., v_5$ las raíces de $g$; $g$ tiene un grupo de Galois isomorfo al grupo simétrico $S_5$. Sea $v = v_1v_2 + v_3v_4$ y sea $f(x)$ el polinomio minimal **(B2)** de $v$ sobre los racionales.*

*Un procedimiento computacional muestra que:*

$f(x) = x^{15} + 6x^{13} + 7x^{11} - 21x^{10} - 8x^9 - 109x^8 - 17x^7 - 144x^6 - 355x^5 - 48x^4 + 103x^3 + 5x^2 - 56x + 29$

*Como $S_5$ no contiene un elemento de orden 15, el argumento anterior muestra que $f(x)$ es reducible módulo todo primo. Pero $f(x)$ es polinomio minimal asi que es irreducible sobre los racionales **[15]**.*

# Capítulo 4

# Número de raíces de un polinomio en $\mathbb{R}[x]$

En este capítulo además de presentar cómo funcionan algunos de los conceptos vistos en el capítulo 1 tratando el tema de la irreducibilidad no como ejemplo sino como una sección del capítulo, también se da a conocer la resolución de ecuaciones bajo radicales, a la vez que se muestra un algoritmo que permite hallar el número de raíces reales en un intervalo. Sin más preámbulo se da inicio a este interesante capítulo.

**Ejemplo 29.** *(Raíz de un polinomio)*

***(a.)*** *Si* $p(x) = x^2 - 2 \in \mathbb{R}[x]$*, entonces* $p(x)$ *tiene raíces* $\sqrt{2}$ *y* $-\sqrt{2}$*, puesto que* $(\sqrt{2})^2 - 2 = 0 = (-\sqrt{2})^2 - 2$.
*Además se puede escribir* $p(x) = (x - \sqrt{2})(x + \sqrt{2})$*, con* $x - \sqrt{2}, x + \sqrt{2} \in \mathbb{R}[x]$.

**Ejemplo 30.** *(Máximo número de raíces)*

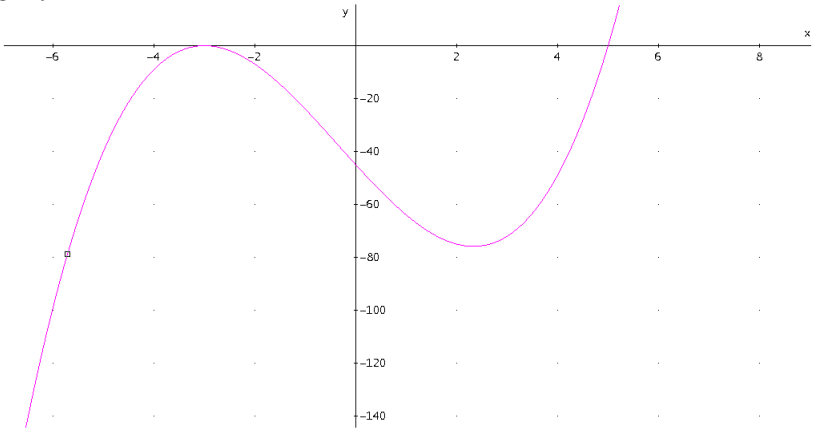
*(a) Sea* $f(x) = x^3 - 2x^2 - 13x + 6$ *en* $\mathbb{R}$*. El polinomio tiene tres raíces distintas en* $\mathbb{R}$*,* $-3$*,* $\frac{5}{2} + \frac{1}{2}\sqrt{17}$*,y* $\frac{5}{2} - \frac{1}{2}\sqrt{17}$.
*(b) Sea* $f(x) = x^4 - 4x^3 + 4x^2 - 12x + 3$ *en* $\mathbb{R}$*. Este polinomio tiene dos raíces distintas en* $\mathbb{R}$*,* $2 + \sqrt{3}$ *y* $2 - \sqrt{3}$*, las otras dos son complejas no reales.*

**Ejemplo 31.** *(Factor Múltiple)*

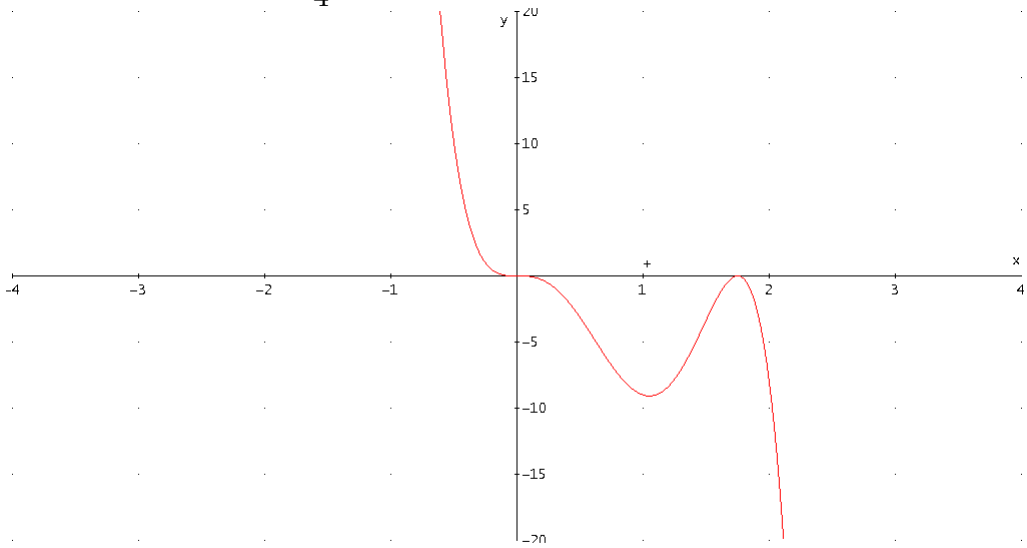
*(a) Sea* $f(x) = (x^2+2)^2(x+1)$ *en* $\mathbb{R}[x]$, $f(x)$ *tiene un factor múltiple, mientras que* $f(x) = (x^2+2)(x+1)$ *no. Si* $f(x)$ *tiene un factor múltiple lineal* $f(x) = (x^2+2)(x+1)^2$, *se dirá que* $f(x)$ *tiene una* ***raíz múltiple*** *en* $F$.

*(b) Sea* $f(x) = x^3 + x^2 - 21x - 45$, $f(x) = (x+3)^2(x-5)$ *así que tiene raíces* $5$ *y* $-3$, *ésta última con multiplicidad dos.*

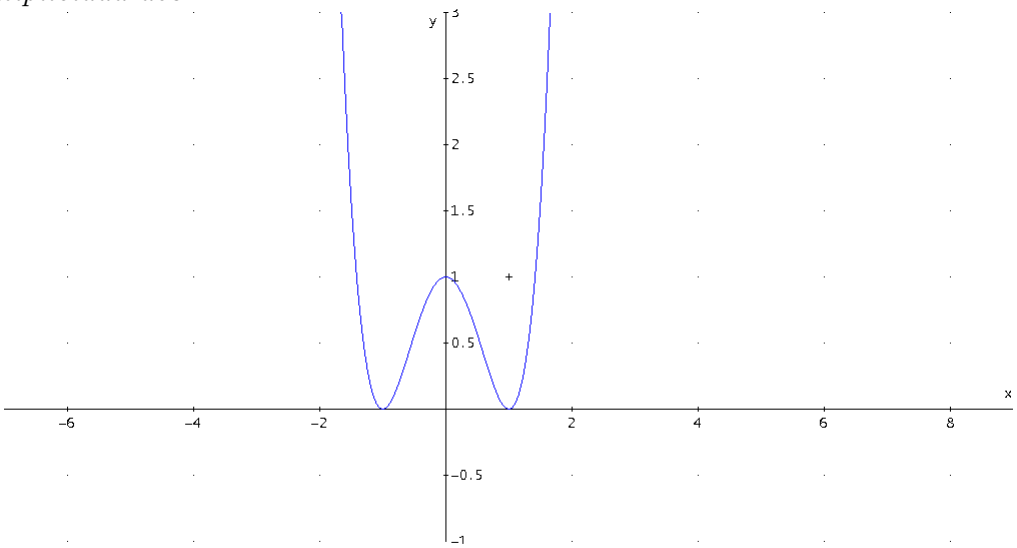
*La gráfica muestra este hecho.*




*(c) Sea* $f(x) = -16x^5 + 56x^4 - 49x^3$, $f(x) = -x^3(4x-7)^2$, *así que tiene raíces* $0$ *que tiene multiplicidad tres y* $\dfrac{7}{4}$ *que tiene multiplicidad dos.*



*(d) Sea* $f(x) = x^4 - 2x^2 + 1$, $f(x) = (x-1)^2(x+1)^2$ *tiene raíces* $1$ *y* $-1$, *cada una con multiplicidad dos.*




## 4.1. Teorema Fundamental del Álgebra

Se sabe que el conjunto $\mathbb{N}$ es cerrado en las operaciones binarias de suma y multiplicación (ordinarias), pero si se busca la respuesta a la ecuación $x + 5 = 2$, se ve que ningún elemento de $\mathbb{N}$ es una solución. Así se extiende $\mathbb{N}$ a $\mathbb{Z}$, donde se pueden realizar la resta, así como la suma y la multiplicación. Sin embargo pronto se encuentran pro blemas al tratar de resolver la ecuación $2x + 3 = 4$. Si se extiende a $\mathbb{Q}$, se puede realizar la división entre números distintos de cero, además de las otras operaciones. Pero esto también demuestra ser inadecuado; la ecuación $x^2 - 2 = 0$ necesita que se introduzcan los números reales, para irracionales $\pm\sqrt{2}$. Incluso después de ampliar $\mathbb{Q}$ a $\mathbb{R}$, surgen más problemas al intentar resolver $x^2 + 1 = 0$. Por último, se llega a $\mathbb{C}$, el sistema de los números complejos, donde se puede resolver cualquier ecuación polinomial de la forma $a_n x^n + a_{n-1}x^{n-1} + ... + a_2 x^2 + a_1 x + a_0 = 0$, donde $a_i \in \mathbb{C}$ para $0 \leq i \leq n, n > 0$ y $a_n \neq 0$, ya que el campo $\mathbb{C}$ como se había dicho fué inventado para contener raíces de polinomios irreducibles reales, por ejemplo $i = \sqrt{-1}$ es una raíz del polinomio $x^2 + 1$. Este resultado se conoce como el teorema fundamental del álgebra que aquí se enuncia formalmente.

**Teorema 21.** ***Teorema Fundamental del Álgebra***

*a.) Todo polinomio de grado $n \geq 1$ tiene al menos una raíz en $\mathbb{C}$*

*b.) Si $p(x)$ denota un polinomio de grado $n$, entonces $p(x)$ tiene exactamente $n$ raíces, algunas de las cuales pueden ser reales.*

**Demostración:** Fraleigh, John B. Algebra Abstracta, pp 357.

**Teorema 22.** ***( Teorema del Producto y Suma de las Raíces):*** *Sea $F = \mathbb{C}$.*

*Sea $p(x) = x^n + a_{n-1}x^{n-1} + ... + a_3x^3 + a_2x^2 + a_1x + a_0$ cualquier polinomio con coeficientes reales y coeficiente principal 1, donde $n \geq 1$. Entonces $a_0$ es $(-1)^n$ veces el producto de todas las raíces de $p(x)$ y $a_{n-1}$ es el opuesto de la suma de todas las raíces de $p(x)$.*

**Demostración:** Por el teorema **21** se sabe que $p(x)$ tiene $n$ raíces que denotadas por $r_1, r_2, ..., r_n$. Ahora se forma el producto de los $n$ factores asociados a estas raíces.

Sea $q(x) = (x - r_1)(x - r_2)(x - r_3)...(x - r_n)$, al multiplicar todos estos términos se inspecciona el coeficiente de $x^{n-1}$ y el término constante.

Probando por inducción en $n$: Cuando **n=1** se tiene que $p(x) = x + a_0$, en este caso la única raíz de $p(x)$ es $r_1 = -a_0$. Como $r_1$ es la única raíz, $r_1$ es ella misma el producto de todas las raíces. Pero entonces $(-1)^n a_0 = (-1)^1 a_0 = -a_0 = r_1$. De esta manera se establece el término constante. Note otra vez que como $r_1$ es la única raíz, $r_1$ es ella misma la suma de todas las raíces y coeficiente de $x^{n-1}$ es el opuesto de la suma de todas las raíces, en este caso $a_0 = -r_1$.

Cuando $n = 2$, note que $(x - r_1)(x - r_2) = x^2 + (-r_1 + -r_2)x + r_1r_2$. En este caso se observa inmediatamente que el coeficiente de $x$ es el opuesto de la suma de todas las raíces y el término constante es el producto de todas las raíces. Como $p(x)$ es cuadrático, pues $n = 2$, $(-1)^n = (-1)^2 = 1$.

Ahora se asume que el resultado es verdadero cuando se tienen $k$ raíces y sea $p(x)$ un polinomio con $k + 1$ raíces, es decir

$p(x) = (x - r_1)(x - r_2)...(x - r_k)(x - r_{k+1})$.

Sea $q(x) = (x - r_1)(x - r_2)...(x - r_k)$

Entonces $q(x)$ tiene grado $k$ y se le puede aplicar la hipótesis de inducción:

$q(x) = x^k + a_{k-1}x^{k-1} + ... + a_1x + a_0$

Se sabe que $a_{k-1} = -\sum_{i=1}^{k+1} r_i$ y $a_0 = (-1)^k \prod_{i=1}^{k} r_i$

Ahora $p(x) = q(x)(x - r_{k+1}) = (x - r_{k+1})\left(x^k + a_{k-1}x^{k-1} + ... + a_1x + a_0\right)$

$= x^{k+1}+a_{k-1}x^k+...+a_1x^2+a_0x+(-r_{k+1})x^k+(-r_{k+1})a_{k-1}x^{k-1}+...+(-r_{k+1})a_1x+(-r_{k+1})a_0$

$= x^{k+1} + \{a_{k-1} + (-r_{k+1})\}x^k + ... + (a_0 - r_{k+1}a_1)x + (-r_{k+1})a_0$

Luego,

$$a_{k-1} + (-r_{k+1}) = \sum_{i=1}^{k} r_i + (-r_{k+1}) = -\sum_{i=1}^{k+1} r_i$$

y

$$(-r_{k+1})a_0 = (-r_{k+1})(-1)^k \prod_{i=1}^{k} r_i = (-1)^{k+1} \prod_{i=1}^{k+1} r_i$$

que era lo que se necesitaba establecer.

**Proposición 4.** *Sean $f(x) \in \mathbb{C}[x]$, $f'(x)$ su derivada, y $\boldsymbol{a} \in \mathbb{C}$*

***(i)*** *Si $\boldsymbol{a}$ es raíz simple de $f(x)$, entonces $\boldsymbol{a}$ no es raíz de $f'(x)$, $(f'(a) \neq 0)$.*

***(ii)*** *Si $\boldsymbol{a}$ es una raíz de $f(x)$con multiplicidad $k > 1$, entonces $\boldsymbol{a}$ es una raíz de $f'(x)$ con multiplicidad $k - 1$.*

**Prueba:** si $a$ es una raíz de $f(x)$ con multiplicidad $k \geq 1$, se tiene que $f(x) = (x-a)^k f_1(x)$ con $f_1(x)$ no divisible por $(x-a)$, es decir, $f_1(a) \neq 0$.

Entonces,

$f'(x) = k(x-a)^{k-1}f_1(x) + (x-a)^k f_1'(x) = (x-a)^{k-1}[kf_1(x) + f_1'(x)(x-a)] = (x-a)^{k-1}t(x)$.

El polinomio $t(x) = kf_1(x) + f_1'(x)(x-a)$ no es divisible por $(x-a)$, ya que:

$t(a) = kf_1(a) + f_1'(a)(0) = kf_1(a) \neq 0$.

En consecuencia, para $k = 1$, $f'(x) = f(x)$ no es divisible por $(x-a)$; y para $k > 1$, $f'(x)$ es divisible por $(x-a)^{k-1}$ pero no por $(x-a)^k$. Por tanto **(i)** y **(ii)** están probados.

**Teorema 23.** ***( Teorema del Cero Intermedio):*** *Sea $p(x)$ cualquier polinomio con coeficientes reales, y si $p(a) > 0$ y $p(b) < 0$ entonces existe por lo menos un número real $c$ entre $a$ y $b$ tal que $p(c) = 0$.*

Para realizar la demostración, hay que tener en cuenta que depende de la continuidad de todos los polinomios y es un caso especial del teorema del valor intemedio que normalmente aparece en la clase de cálculo.

**Teorema 24.** ***( Teorema de Rolle):*** *Sea $f$ una función tal que:*

***(i)*** *Es continua en el intervalo cerrado $[a,b]$;*

***(ii)*** *Diferenciable en el intervalo $(a,b)$;*

***(iii)*** $f(a)=0 \quad y \quad f(b)=0$

*Entonces existe un número $c$ en el intervalo abierto $(a,b)$ tal que $f'(c)=0$.*

**Dos consecuencias importantes del teorema de Rolle:**

De acuerdo con el teorema **24** (caso particular del teorema del valor medio para derivadas), se tiene: "Si los números reales $a$ y $b$, $(a<b)$ son ambos raíces de un polinomio con coeficientes reales, entonces existe un número $c$, $a<c<b$, el cual es raíz de su derivada". De este hecho se tienen las siguientes consecuencias:

**Proposición 5.** *Sea $f(x)=a_nx^n+a_{n-1}x^{n-1}+...+a_1x+a_0$, un polinomio con coeficientes reales, tal que todas sus raíces son reales, entonces:*

***(i)*** *Todas las raíces de $f'(x)$ son también reales.*

***(ii)*** *Entre dos raíces adyacentes de $f(x)$ existe una raíz de $f'(x)$ y tal raíz es simple.*

**Prueba:** Sean $x_1<x_2<...<x_k$ las raíces de $f(x)$ con multiplicidades $m_1,m_2,...,m_k$ respectivamente. Es claro que $m_1+m_2+...+m_k=n$.

Por la proposición **4**, parte **(ii)**, $f'(x)$ tiene raíces $x_1,x_2,...,x_k$ con multiplicidades $m_1-1,m_2-1,...,m_k-1$, respectivamente; y por el teorema **23** , existe al menos una raíz de $f'(x)$ en el interior de cada uno de los intervalos $(x_1,x_2),(x_2,x_3),...,(x_{k-1},x_k)$. Sean ellas $y_1,y_2,...,y_{k-1}$. Así, el número de raíces reales de $f'(x)$ es (contando multiplicidad) a lo más: $(m_1-1)+(m_2-1)+...+(m_k-1)+k-1=n-1$.

Pero como $f'(x)$ es un polinomio de grado $n-1$, él tiene (contando multiplicidad) a lo sumo $n-1$ raíces reales. Por lo tanto, todas las raíces de $f'(x)$ son reales y ellas son: $y_1,y_2,...,y_{k-1}$, las cuales deben ser simples; y $x_1,x_2,...,x_k$ (que pueden ser múltiples).

**Proposición 6.** *Sea $f(x) \in \mathbb{R}[x]$, tal que todas sus raíces son reales, y de ellas $p$ son positivas. Entonces, $f'(x)$ tiene $p$ o $p-1$ raíces positivas.*

**Prueba:** Sean $x_1 < x_2 < ... < x_k$ todas las raíces positivas del polinomio $f(x)$ con multiplicidades $m_1, m_2, ..., m_k$ respectivamente. Entonces $m_1 + m_2 + ... + m_k = p$.

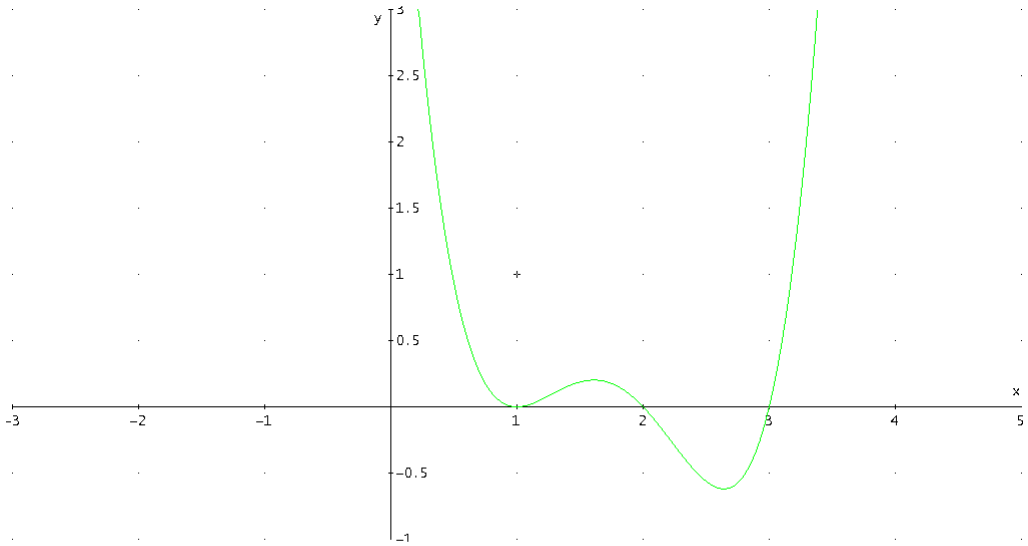
La derivada $f'(x)$ tendrá las siguientes raíces positivas: $x_1, x_2, ..., x_k$ con multiplicidades $m_1 - 1, m_2 - 1, ..., m_k - 1$; raíces simples $y_1, y_2, ..., y_{k-1}$ cada una en los intervalos $(x_1, x_2), (x_2, x_3), ..., (x_{k-1}, x_k)$ respectivamente; y es posible que $f'(x)$ tenga una raíz adicional $y_0$ en el intervalo $(x_0, x_1)$ donde $x_0$ es la mayor raíz no positiva de $f(x)$, si existe.

En consecuencia el número de raíces positivas de $f'(x)$ es igual a:

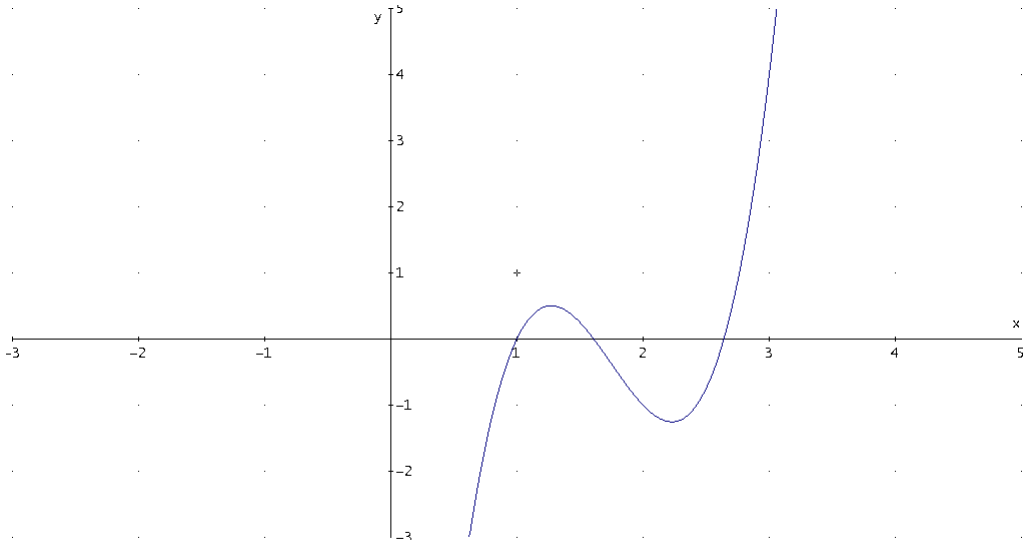
$(m_1 - 1) + (m_2 - 1) + ... + (m_k - 1) + k - 1 = p - 1$

$(m_1 - 1) + (m_2 - 1) + ... + (m_k - 1) + (k - 1) + 1 = p.$

**Ejemplo 32.** *Sean $f(x) = x^4 - 7x^3 + 17x^2 - 17x + 6$, $f(x)$ tiene cuatro raíces reales positivas: 2, 3, y 1, esta última con multiplicidad dos.*



*La derivada de* $f(x)$ *es* $f'(x) = 4x^3 - 21x^2 + 34x - 17$. $f'(x)$ *tiene tres raíces reales positivas:* $1$, $\frac{17}{8} + \frac{1}{8}\sqrt{17}$ *y* $\frac{17}{8} - \frac{1}{8}\sqrt{17}$.




**Proposición 7.** *Sea* $f(x) \in \mathbb{R}[x]$, $f'(x)$ *su derivada,* $d(x) = MCD(f(x), f'(x))$. *Entonces,* $g(x) = \dfrac{f(x)}{d(x)}$ *tiene exactamente las mismas raíces que* $f(x)$, *pero cada una ocurre en* $g(x)$ *con multiplidad uno.*

**Prueba:** Sea $a$ una raíz de $f(x)$, entonces $f(x) = (x-a)^k t(x)$, con $t(a) \neq 0$, $k$ es la multiplicidad de $a$.

En consecuencia,

$f'(x) = k(x-a)^{k-1}t(x) + (x-a)^k t'(x) = (x-a)^{k-1}\left[t(x) + (x-a)t'(x)\right]$,

se denota $h(x) = t(x) + (x-a)t'(x)$; con $h(a) = t(a) \neq 0$. Así, como $(x-a)^{k-1}$ es divisor común de $f(x)$ y $f'(x)$; se debe tener que: $d(x) = (x-a)^{k-1}j(x)$, para $j(x) \nmid h(x)$; en consecuencia $j(a) \neq 0$.

Como $j\,(a) \neq 0$, $j(x)$ y $(x-a)$ son primos relativos; y como $j\,(x) \mid f(x)$ pero $j\,(x)$ no divide a $(x-a)^k$ debe tenerse que $j(x) \mid t(x)$, es decir $f(x)/d\,(x) = (x-a)\,t\,(x)\,/j\,(x)$. Esto significa que si $a$ es una raíz de $f\,(x)$, entonces $a$ es raíz de $g(x)$ con multiplicidad 1.

Recíprocamente, si $a$ es una raíz de $g\,(x)$ entonces, como $g(x) \mid f(x)$; $a$ es también raíz de $f(x)$; y por lo anterior, es una raíz de $g(x)$ con multiplicidad uno.

De esta proposición es claro que si se desean localizar las raíces de $f(x)$, es suficiente con localizar las raíces de $g(x)$. Como $g(x)$ no tiene raíces múltiples, $g(x)$ y $g'(x)$ son primos relativos. En consecuencia, cuando se aplica el algoritmo de Euclides a $g(x)$ y $g'(x)$ al final se encuentra un polinomio constante como residuo.

## 4.2. Resolución de Ecuaciones Bajo Radicales

### 4.2.1. La Ecuación Cuadrática:

En el curso de álgebra elemental se tratan diversos temas pero su centro lo constituye la *resolución de ecuaciones*.

Limitándose a las ecuaciones con una sola incógnita, se recordará un poco lo que sobre ellas se sabe desde la secundaria. El lector antes que nada, podrá resolver ecuaciones de primer grado. Dada la ecuación: $ax + b = 0$, donde $a \neq 0$, entonces su única raíz será el número: $x = -ba^{-1}$.

Además, se conoce la fórmula de resolución de la ecuación cuadrática $ax^2+bx+c = 0$, donde $a \neq 0$. Precisamente,

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Si los coeficientes de la ecuación son números reales, esta fórmula da dos raíces reales diferentes en el caso cuando el subradical es un número positivo, es decir, cuando $b^2-4ac > 0$. Por el contrario, si $b^2 - 4ac = 0$, la ecuación $ax^2 + bx + c = 0$ sólo posee una raíz, a la que se denomina, en este caso, *raíz múltiple*. Si $b^2 - 4ac < 0$ la ecuación no posee ninguna raíz real, como sucede en el polinomio $x^2 + c$, con $c > 0$.

Es importante señalar que los antiguos Babilonios conocían un método para resolver ecuaciones cuadráticas, las cuales eran planteadas en la siguiente forma: hallar dos números, dados su suma y producto.

En simbolismo algebráico moderno, esto puede enunciarse:

Dados dos números $p$ y $s$ tales que $x_1x_2 = p$, $x_1 + x_2 = s$, hallar $x_1$ y $x_2$.

Los pasos seguidos por los Babilonios eran los siguientes:

**1**. Tomar la mitad de $s$.

**2**. Elevar al cuadrado el resultado.

**3**. De este último, restar $p$.

**4**. Tomar la raíz cuadrada del resultado.

**5**. Sumar este a la mitad de $s$, éste es uno de los números y el otro es $s$ menos este último.

Por ejemplo, si la suma es 10 y el producto es 21 entonces los pasos sucesivos producen 5, 25, 4, 2, 7 y 3.

Para ver que este problema corresponde efectivamente a una ecuación cuadrática, se multiplica la igualdad $s = x_1 + x_2$ por $x_1$ y hallamos $sx_1 = x_1^2 + x_1x_2 = x_1^2 + p$. En otras palabras, $x_1$ es solución de la ecuación $x_1^2 - sx_1 + p = 0$ y así lo es $x_2$ por simple simetría.

En lenguaje algebráico moderno, la solución de los Babilonios puede escribirse:

**1**. $\dfrac{s}{2}$

**2**. $\dfrac{s^2}{4}$

**3**. $\dfrac{s^2}{4} - p = \dfrac{s^2 - 4p}{4}$

**4**. $\dfrac{\sqrt{s^2 - 4p}}{2}$

**5**. $x_1 = \dfrac{s}{2} + \dfrac{\sqrt{s^2 - 4p}}{2}$, $x_2 = s - x_1$, o en una forma más usual $x_1, x_2 = \dfrac{s \pm \sqrt{s^2 - 4p}}{2}$

Por lo tanto, es apenas justo decir que ellos conocían la fórmula cuadrática aunque simplemente expresan verbalmente los pasos de su procedimiento.

Se puede resolver por último algunos tipos de ecuaciones de *tercero* y *cuarto* grados, más exactamente, aquellas cuya resolución se reduce fácilmente a la resolución de las ecuaciones cuadráticas. Así es, por ejemplo, la ecuación de tercer grado: $ax^3 + bx^2 + cx = 0$, que posee una raíz $x = 0$ y que luego de simplificar por $x$ se transforma en la ecuación cuadrática: $ax^2 + bx + c = 0$. La ecuación de cuarto grado, llamada también *bicuadrática*: $ay^4 + by^2 + c = 0$ también se reduce a una ecuación cuadrática; para ello es suficiente sustituir en esta ecuación $y^2 = x$, hallar las raíces de la ecuación cuadrática que se ha obtenido y luego extraer las raíces cuadradas de las mismas. Se resalta nuevamente que éstas son sólo ciertos casos muy particulares de las ecuaciones de tercero y cuarto grado.

Se describirán a continuación un poco algunos métodos que nos pueden ayudar a la

hora de resolver estas ecuaciones cuando no se puedan reducir tan fácilmente.

### 4.2.2. Ecuaciones Cúbicas (Método de Cardano - Hudde (1650)):

Se conoce ya la fórmula para la resolución de las ecuaciones cuadráticas. En el caso de las ecuaciones de tercer grado, o como se dice, ecuaciones cúbicas, también puede darse una fórmula, claro que más complicada, que exprese las raíces de estas ecuaciones mediante sus coeficientes, con ayuda de radicales.

Sea la ecuación cúbica general:

$x^3 + ax^2 + bx + c = 0,$ (1).

Se transformará esta ecuación, considerando a

$x = y - \frac{a}{3},$ (2), donde $y$ es una nueva incógnita.

Sustituyendo esta expresión de $x$ en la ecuación (1) se obtiene una ecuación cúbica para la incógnita $y$, más sencilla, por otra parte, ya que el coeficiente de $y^2$ resulta igual a cero como se muestra en las ecuaciones:

$(y - a/3)^3 + a(y - a/3)^2 + b(y - a/3) + c = 0$

$y^3 + (\frac{3b - a^2}{3})y + (\frac{2a^3 - 9ab + 27c}{27}) = 0.$

El coeficiente de $y$ a la primera potencia y el término independiente serán correspondientemente los números:

$p = \frac{3b - a^2}{3}, \qquad q = \frac{2a^3 - 9ab + 27c}{27},$

es decir que la ecuación en forma reducida se escribe como sigue:

$y^3 + py + q = 0,$ (3).

Si se hallan las raíces de esta nueva ecuación, entonces, restándoles $a/3$ cada una de ellas se obtendrán las raíces de la ecuación inicial.

Así es suficiente considerar ecuaciones cúbicas de la forma (3); ya que si se tienen las raíces de (3), las de (1) son obtenidas mediante (2). En consecuencia, el proceso se limita a resolver (3) con ayuda de lo que se conoce como el **Método de Cardano - Hudde:**

Sea la ecuación (3) se hace $y = u + v$. Así, en lugar de una incógnita se tienen dos, $u$ y $v$, de esa forma se traslada el problema a uno con dos incógnitas:

$y^3 = (u + v)^3 = u^3 + v^3 + 3uv(u + v) = (3uv)y + (u^3 + v^3)$

$y^3 - (3uv)y - (u^3 + v^3) = 0$

comparando esta última ecuación con (3), se obtiene:

$$\left\{ \begin{array}{c} u^3 + v^3 + q = 0 \\ 3uv + p = 0 \end{array} \right\} \qquad (4)$$

En consecuencia, si se encuentran los números $u$ y $v$ que satisfagan este sistema de ecuaciones, el número $y = u + v$ debe ser una raíz de (3). Las raíces de la ecuación (3) se expresan por medio de sus coeficientes con ayuda de la siguiente fórmula:

$$y = u + v = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} \qquad (6)$$

Esta es **la fórmula de Cardano**.

Cada uno de los radicales cúbicos presentes en ella posee, como se sabe, tres valores, no pudiéndoselos, sin embargo, combinar en forma arbitraria. Resulta que para cada valor del primer radical existe un único valor del segundo radical, ya que el producto de ambos es igual al número $-\frac{p}{3}$.

Estos dos valores de los radicales son precisamente los que deben sumarse para obtener la raíz de la ecuación en cuestión.

Por consiguiente, toda ecuación cúbica con cualesquiera coeficientes numéricos posee tres raíces que, en el caso general, son complejas; por supuesto, algunas de estas raíces pueden coincidir, es decir, transformarse en raíz múltiple.

En la fórmula reducida, sean los coeficientes $p$ y $q$ números reales. Se puede demostrar que si la ecuación $y^3 + py + q = 0$ posee tres raíces reales diferentes, entonces la expresión $\frac{q^2}{4} + \frac{p^3}{27}$ será negativa. Esta expresión aparece en la fórmula bajo el signo de la raíz cuadrada y por eso luego de extraer esta raíz se obtiene bajo el signo de cada una de las raíces cúbicas un número no real.

**Ejemplo 33.** ***1.)*** *Resolver la ecuación* $x^3 - 19x + 30 = 0$.

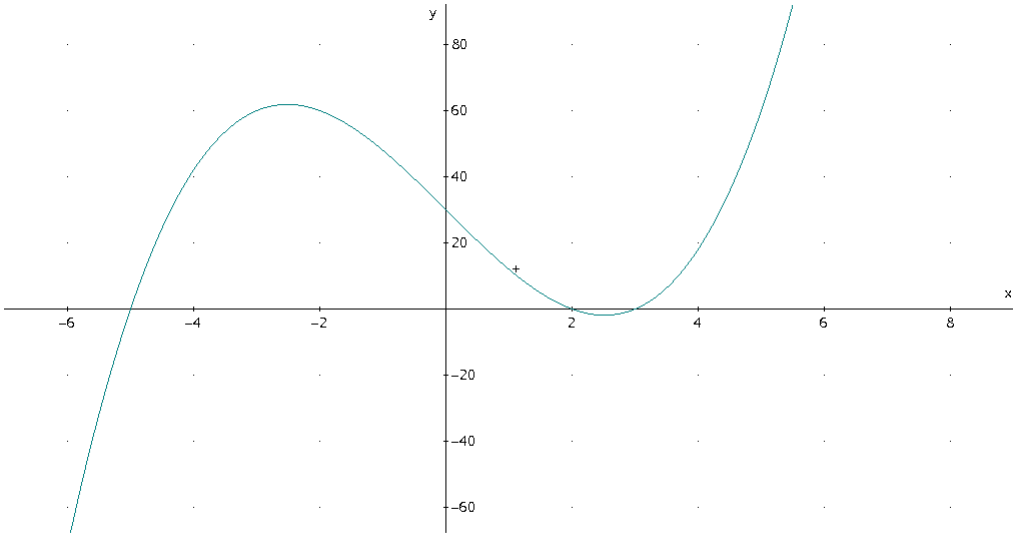
*Esta ecuación no contiene el cuadrado de la incógnita y por lo tanto se aplicará la fórmula que se diera en* (6)*, sin realizar la transformación preliminar.*

*Aquí* $p = -19, \quad q = 30$, *por consiguiente,*

$\frac{q^2}{4} + \frac{p^3}{27} = -\frac{784}{27}$, *es decir, es negativo.* ***El primer radical cúbico*** *que entra en la fórmula tiene la forma:*

$$\sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} = \sqrt[3]{-15 + \sqrt{-\frac{784}{27}}} = \sqrt[3]{-15 + i\sqrt{\frac{784}{27}}}.$$

*No se puede expresar este radical cúbico mediante radicales de números reales y, por lo tanto, no se puede hallar las raíces de la ecuación por la fórmula dada. En realidad, como demuestra la comprobación directa, estas raíces son los números* 2, 3 *y* $-5$.




*La fórmula dada para la resolución de la ecuación cúbica permite hallar las raíces de la ecuación no sólo en aquellos casos cuando la expresión* $\frac{q^2}{4} + \frac{p^3}{27}$ *es positiva o igual a cero. En el primer caso la ecuación tiene una raíz real y dos raíces complejas; en el segundo caso todas las raíces son reales pero una de ellas es múltiple.*

***2.)*** *Resolver la ecuación cúbica*

$$x^3 - 9x^2 + 36x - 80 = 0.$$

*Tomando* $x = y + 3$ *obtenemos la ecuación reducida":*

$$y^3 + 9y - 26 = 0$$

*que puede resolverse aplicando la fórmula dada. Aquí*

$$\frac{q^2}{4} + \frac{p^3}{27} = 196 = 14^2,$$

*y por lo tanto*

$$\sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} = \sqrt[3]{13 + 14} = \sqrt[3]{27}.$$

*Uno de los valores de este radical cúbico es el número* 3. *El producto de este valor por el valor correspondiente del segundo radical cúbico que entra en la fórmula debe ser igual al número* $-\frac{p}{3}$. *o sea, en este caso, igual a* $-3$. *El valor buscado del segundo radical será, por consiguiente, el número* $-1$ *y por ello una de las raíces de la ecuación reducida será:*

$$y_1 = 3 + (-1) = 2.$$

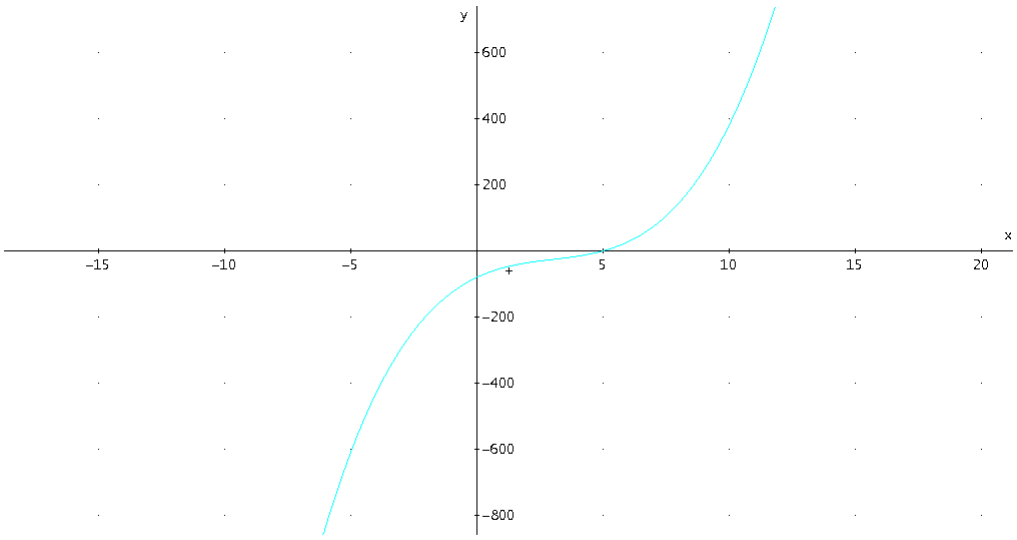
*Ahora que se obtuvo una de las raíces de la ecuación cúbica las otras dos pueden hallarse por muchos medios diferentes. Por ejemplo pueden hallarse otros dos valores del radical* $\sqrt[3]{27}$, *calcular los valores correspondientes del segundo radical y sumar los valores correspondientes de los dos radicales. Se puede actuar de otra forma, dividiendo al primer miembro de la ecuación reducida por* $y-2$, *luego de lo cual sólo debe resolverse la ecuación cuadrática. Cualquiera de estos medios demostrará que las otras dos raíces de la ecuación reducida son*

$$-1 + i\sqrt{12} \ y \ -1 - i\sqrt{12}.$$

*En consecuencia, las raíces de la ecuación cúbica inicial son*

$$5, \ 2 + i\sqrt{12} \ y \ 2 - i\sqrt{12}.$$

*Se comprende que no siempre los radicales se resuelven con tanta facilidad como en el ejemplo que se ha presentado y que se ha elegido de tal forma que ilustre el procedimiento descrito, sino que con mayor frecuencia se los debe resolver en forma aproximada, obteniéndose por ello sólo valores aproximados para las raíces de la ecuación.*




### 4.2.3. La Ecuación Bicuadrática (Método de Ferrari):

Dada la ecuación general de cuarto grado

$x^4 + ax^3 + bx^2 + cx + d = 0$ (7)

se puede escribir en la forma

$x^4 + ax^3 = -bx^2 - cx - d$

Se completa el cuadrado en el lado izquierdo, sumando en ambos lados el término $\frac{a^2x^2}{4}$

$(x^2 + \frac{ax}{2})^2 = (\frac{a^2}{4} - b)x^2 - cx - d$ (8)

Ahora se introduce una nueva variable $y$, sobre la que más adelante se impondrá una condición necesaria, sumando a ambos lados de (8) el término $(x^2 + \frac{ax}{2})y + \frac{y^2}{4}$, se obtiene, de nuevo, en el lado izquierdo un cuadrado perfecto

$(x^2 + \frac{ax}{2})^2 + (x^2 + \frac{ax}{2})y + \frac{y^2}{4} = (\frac{a^2}{4} - b + y)x^2 + (\frac{ay}{2} - c)x + (\frac{y^2}{4} - d)$

$(x^2 + \frac{ax}{2} + \frac{y}{2})^2 = (\frac{a^2}{4} - b + y)x^2 + (\frac{ay}{2} - c)x + (\frac{y^2}{4} - d)$ (9)

De nuevo, se tiene un problema con dos incógnitas.

En el lado derecho de (9) se tiene un trinomio cuadrático en $x$, cuyos coeficientes dependen de $y$. Se selecciona $y$ de tal forma que dicho trinomio sea un cuadrado perfecto de un binomio $\alpha x + \beta$; es decir, que el discriminante del trinomio cuadrático sea cero. Así se escoge $y$ tal que: $(\frac{ay}{2} - c)^2 - 4(\frac{a^2}{4} - b + y)(\frac{y^2}{4} - d) = 0$

$$\frac{a^2y^2}{4} - acy + c^2 - \frac{a^2y^2}{4} + by^2 - y^3 + a^2d - 4bd + 4dy = 0$$

$y^3 - by^2 + (ac - 4d)y - [d(a^2 - 4b) + c^2] = 0$ $\qquad (10) \longrightarrow$ resolvente de la bicuadrática.

A continuación, se determina $y$ mediante el **método de Cardano-Hudde:** Si $y = y_0$ es una solución, se sustituye en (9), cuyo lado derecho es $(\alpha x + \beta)^2$ para obtener: $(x^2 + \frac{ax}{2} + \frac{y_0}{2})^2 = (\alpha x + \beta)^2$, o equivalentemente

$$(x^2 + \frac{ax}{2} + \frac{y_0}{2} - \alpha x - \beta)(x^2 + \frac{ax}{2} + \frac{y_0}{2} + \alpha x + \beta) = 0 \qquad (11)$$

Entonces el valor de $x$ se obtiene de las ecuaciones cuadráticas $x^2 + (\frac{a}{2} - \alpha)x + (\frac{y_0}{2} - \beta) = 0$

$x^2 + (\frac{a}{2} + \alpha)x + (\frac{y_0}{2} + \beta) = 0$

En realidad, este método no es completo puesto que la ecuación resolvente (10) da "tres" valores para $y$, los cuales producen en la ecuación (11) en total seis ecuaciones cuadráticas, cada una de las cuales dá dos valores para $x$. Se obtienen aquí 12 valores de $x$ entre los que se deben escoger las soluciones de (7). Escogiendo cualquiera de las tres raíces de (10), el resultado de las íces encontradas en (11) son las mismas.

**Ejemplo 34.** *Resolver la ecuación* $x^4 - 4x^3 + 4x^2 - 12x + 3 = 0 \qquad (A)$

*Solución:* $x^4 - 4x^3 = 4x^2 + 12x - 3$ *sumando* $\frac{(-4)^2x^2}{4} = 4x^2$

$(x^2 - 2x)^2 = 12x - 3$ *sumando* $(x^2 - 2x)y + \frac{y^2}{4}$

$(x^2 - 2x + \frac{y}{2})^2 = yx^2 + 2(6 - y)x + (\frac{y^2}{4} - 3) \qquad (B)$

*Se escoge* **y** *tal que* $4(6 - y)^2 - 4y(\frac{y^2}{4} - 3) = 0$

$y^3 - 4y^2 + 36y - 14y = 0 \longrightarrow$ *resolvente*

*Por el método para la cúbica:*

$y = 4, 6i, -6i$

*Se escoge la raíz real,* $y = 4$ *y se reemplaza en* $(B)$*:*

$(x^2 - 2x + 2)^2 = 4x^2 + 4x + 1$

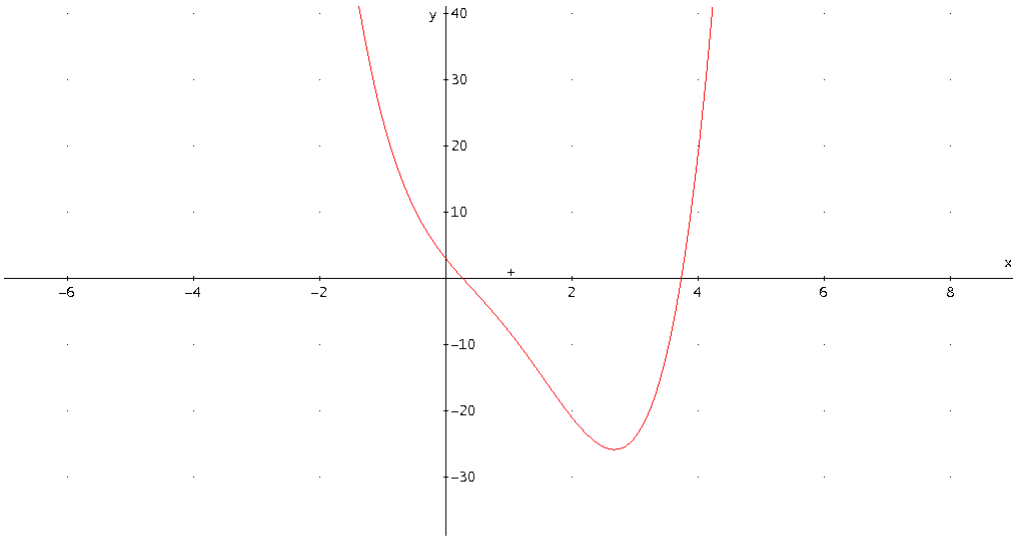
$(x^2 - 2x + 2)^2 = (2x + 1)^2$

$(x^2 - 2x + 2 - 2x - 1)(x^2 - 2x + 2 + 2x + 1) = 0$

$(x^2 - 4x + 1)(x^2 + 3) = 0$

$x^2 - 4x + 1 = 0 \qquad \Longrightarrow \qquad x_{1,2} = \frac{4 \pm \sqrt{12}}{2} = 2 \pm \sqrt{3}$

$$x^2 + 3 = 0 \qquad \Longrightarrow \qquad x_{3,4} = \pm\sqrt{3}i$$




### 4.2.4. Ecuaciones de grado $n \geq 5$:

Las fórmulas para la resolución de las ecuaciones de tercero y cuarto grado fueron descubiertas ya en el siglo $XVI$. Al mismo tiempo comenzaron las búsquedas de fórmulas para la resolución de las ecuaciones de quinto grado y de grados superiores. Note que la forma general de una ecuación de *n-ésimo* grado (donde $n$ es cierto número entero positivo) es:

$$a_0 + a_1 x + ... + a_n x^n = 0.$$

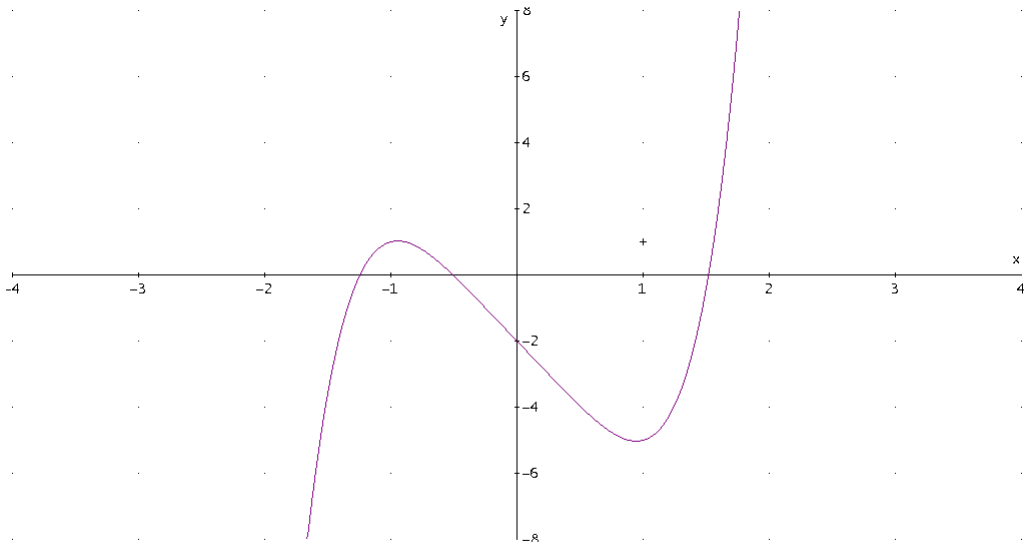
Estas búsquedas continuaron sin éxito hasta comienzos del siglo $XIX$, cuando por fin fue demostrado el siguiente resultado extraordinario:

*Para ningún n, mayor o igual a cinco puede hallarse fórmula que exprese las raíces de cualquier ecuación de n-ésimo grado mediante sus coeficientes por radicales.*

Más aún, para cualquier $n$ mayor o igual a cinco se puede indicar una ecuación de *n-ésimo* grado con coeficientes *enteros*, cuyas raíces no pueden expresarse mediante radicales "de muchos pisos" cualquiera que sea la combinación de los radicales, si como expresiones

subradicales sólo se emplean números enteros y fracciones. Tal es, por ejemplo, la ecuación

$$x^5 - 4x - 2 = 0$$




Puede mostrarse que esta ecuación tiene cinco raíces, tres reales y dos no reales, pero ninguna de ellas puede expresarse mediante radicales, es decir, esta ecuación es "*irresoluble por radicales*". De este modo la reserva de números reales o no que son raíces de las ecuaciones con coeficientes enteros (estos números se denominan *algebraicos* en contraposición a los números *trascendentes* que no son raíces de ninguna ecuación con coeficientes enteros), es mucho más amplia que la reserva de números que se expresan por radicales.

*La teoría de los números algebraicos* es una rama importantísima del álgebra a cuyo enriquecimiento contribuyeron los matemáticos rusos E. I. Zolotariov (1847-1878); C. F. Voronoi (1868-1908), N. G. Chebotariov (1894-1947).

La inexistencia de fórmulas generales para la resolución por radicales de las ecuaciones de n-ésimo grado cuando $n \geq 5$ fue demostrada por *Neils Henrik Abel* (1802-1829). La existencia de ecuaciones con coeficientes enteros irresolubles por radicales fue establecida por Evariste Galois (1811-1832), quien también halló las condiciones en las cuales la ecuación puede resolverse por radicales. Todos estos resultados exigieron la creación de una nueva y profunda teoría, la *teoría de grupos*. El concepto de grupo permitió agotar

la cuestión referente a la resolución de ecuaciones por radicales, habiendo hallado más tarde numerosas aplicaciones en diferentes ramas de la matemática y fuera de sus límites, convirtiéndose en uno de los objetos más importantes de estudio en el álgebra.

El hecho de que no existen fórmulas para resolver las ecuaciones de $n$-ésimo grado cuando $n \geq 5$ no provoca dificultades serias en lo que respecta a la búsqueda práctica de las raíces de las ecuaciones. Esto se compensa totalmente por los numerosos métodos de resolución aproximada de las ecuaciones, que incluso en el caso de las ecuaciones cúbicas conducen al objetivo con mayor eficiencia que utilizando la fórmula (allí donde ésta puede aplicarse) y extrayendo, a continuación, en forma aproximada los radicales reales. No obstante, la existencia de fórmulas para las ecuaciones de segundo, tercero y cuarto grados permitió demostrar que estas ecuaciones poseen respectivamente dos, tres o cuatro raíces. Ahora bien, ¿cómo estarán las cosas respecto a la existencia de raíces para las ecuaciones de $n$-ésimo grado para $n$ arbitrario?.

Si existieran ecuaciones con coeficientes numéricos reales o complejos que no poseyeran ni una sola raíz real o compleja, aparecería entonces la necesidad de ulterior ampliación de la reserva de números. Pero, esto no es necesario: ya que los números complejos son suficientes para resolver cualesquiera ecuaciones con coeficientes numéricos. De aquí sale el teorema que enunciamos al inicio del capítulo como *Teorema Fundamental del Álgebra* y que dicho en otras palabras se puede enunciar así:

*Toda ecuación de n-ésimo grado con cualesquiera coeficientes numéricos tiene n raíces complejas o, en particular, reales, algunas de las cuales, por supuesto, pueden coincidir o sea que pueden ser múltiples.*

En la actualidad existen casi media docena de demostraciones de este teorema que es uno de los más importantes en toda la matemática y que fue aceptado por largo tiempo sin prueba rigurosa. Los primeros intentos para demostrarlo, en toda su generalidad ya en el siglo $XVIII$, se deben a Leonhard Euler (1707-1783), D'Alembert (1717-1783) y luego a Joseph-Louis Lagrange (1736-1813). Pero en sus trabajos faltaba el reconocimiento y la utilización de las posibles raíces complejas, no reales. Una prueba rigurosa de tal propiedad fue solo obtenida a mediados del siglo $XIX$, esto es, unos cien años después, por Carl

Friedrich Gauss (1777-1855), quien completó el trabajo esencial que hacía falta.

El concepto de multiplicidad de la raíz citado en el enunciado del teorema fundamental tiene el siguiente significado. Se puede demostrar que si la ecuación de $n$-ésimo grado

$$a_0 + a_1x + ... + a_nx^n = 0$$

tiene $n$ raíces $\alpha_1$, $\alpha_2$, ..., $\alpha_n$, entonces el primer miembro de la igualdad posee la siguiente descomposición en factores:

$a_0 + a_1x + ... + a_nx^n = a_n(x - \alpha_1)(x - \alpha_2)...(x - \alpha_n)$.

Recíprocamente, si para el primer miembro de nuestra ecuación se da esa descomposición, entonces los números $\alpha_1$, $\alpha_2$, ..., $\alpha_n$ serán las raíces de esa ecuación. Algunos de los números $\alpha_1$, $\alpha_2$, ..., $\alpha_n$ pueden resultar iguales entre sí. Si por ejemplo

$$\alpha_1 = \alpha_2 = ... = \alpha_k,$$

pero

$\alpha_1 \neq \alpha_l$ cuando $l = k + 1$, $k + 2$, ..., $n$,

o sea, en la descomposición estudiada el factor $(x-\alpha_1)$ en realidad se encuentra $k$ veces, entonces para $k > 1$ la raíz $\alpha_1$ se llama **raíz múltiple**, o más exactamente **k-múltiple**. Si $k = 1$ se dice **raíz simple**. Dado $f(x) \in \mathbb{C}[x]$, sabemos que el número complejo $a$ es una raíz de $f(x)$ sí y solo si $f(x)$ es divisible por $(x - a)$ entonces el número $a$ se llama una **raíz simple** del polinomio $f(x)$.

### 4.2.5. Polinomios Irreducibles

**Teorema 25.** *Si $f(x)$ es un polinomio irreducible con coeficientes reales, entonces*

*$f(x)$ tiene grado 1 o*

*$f(x) = ax^2 + bx + c$ con $b^2 - 4ac < 0$.*

*Recíprocamente, los dos tipos de polinomios son irreducibles.*

**Demostración:** Claramente cualquier polinomio de grado 1 es irreducible.

Supóngase que $f(x) = ax^2 + bx + c$. Entonces $f(x)$ se factoriza en $\mathbb{C}[x]$ así:

$$f(x) = a\left(x + \frac{b}{2a} + \frac{1}{2a}\sqrt{b^2 - 4ac}\right)\left(x + \frac{b}{2a} - \frac{1}{2a}\sqrt{b^2 - 4ac}\right).$$

Por la fórmula cuadrática (solución por radicales).

Si $b^2-4ac<0$ entonces las raíces de $f(x)$ no son reales porque $\sqrt{b^2-4ac}\notin \mathbf{R}$. Luego, $f(x)$ es irreducible en $\mathbb{R}[x]$. Por tanto las dos clases de polinomios reales son irreducibles en $\mathbb{R}[x]$.

Para el recíproco, supóngase que $f(x)$ es un polinomio irreducible de grado mayor que 1. Entonces este no tiene raíces reales. Sea $\alpha$ una raíz compleja no real de $f(x): f(\alpha)=0$. Se dice que $\alpha=r+is$, $r,s\in\mathbb{R}$, $s\neq 0$.

Sea $\bar{\alpha}=r-is$. Entonces,

$g(x)=(x-\alpha)(x-\bar{\alpha})=(x-(r+is))(x-(r-is))=x^2-2rx+(r^2+s^2)\in\mathbb{R}[x]$.

Aplicando el teorema de la división a $f(x)$ y $g(x)$ se tiene:

$$f(x)=g(x)q(x)+r(x),\ \text{ donde } q(x),r(x)\in\ \mathbb{R}[x].$$

Entonces $r(x)$ es un polinomio real de grado $\leq 1$.

Tomando esta ecuación como una igualdad de funciones en $\mathbb{C}$, y haciendo $x=\alpha$.

Entonces $0=f(\alpha)=g(\alpha)q(\alpha)+r(\alpha)$; $g(\alpha)=0$ por la manera como se construyó $g(x)$, así $r(\alpha)=0$.

Ahora, $r(x)=ax+b$ con $a,b\in\mathbb{R}$, Así, si $r(\alpha)=0$, entonces $a\alpha+b=0$. Como $\alpha$ no es real, esta ecuación puede ser válida únicamente cuando $a=b=0$. De esta manera $r(x)=0$ y se obtiene: $f(x)=g(x)q(x)$. Esto quiere decir que $f(x)$ no es irreducible, a no ser que $q(x)$ sea una constante. Si $q(x)$ es una constante, $f(x)$ tiene grado 2 y no tiene raíces reales.

Es claro que en la demostración se usa el teorema fundamental del álgebra. Así como se conocen algunos polinomios que son irreducibles en $\mathbb{R}[x]$ (o $\mathbb{C}[x]$), es díficil factorizar o encontrar las raíces de un polinomio que se sabe **no** es irreducible.

En conclusión, los polinomios irreducibles en $\mathbb{R}[x]$ son exactamente los de grado 1 y aquellos de grado 2 con discriminante negativo; así mismo los polinomios de grado 1 son los únicos polinomios irreducibles en $\mathbb{C}$.

**Ejemplo 35.**

***a.)*** *Sea $p(x)=x^4+2x^2+1\in\mathbb{R}[x]$. Aunque $p(x)$ no tiene raíces reales, es reducible, pues $x^4+2x^2+1=(x^2+1)^2$. Por lo tanto, la parte* ***b.)*** *del* ***teorema 1*** *no se aplica a los*

*polinomios de grado mayor que* 3.

***b.)*** *El polinomio* $x^2+1$ *es irreducible en* $\mathbb{R}[x]$*, pero en* $\mathbb{C}[x]$ *se ve que* $x^2+1=(x+i)(x-i)$*. Se puede decir entonces que el campo* $\mathbb{C}$ *fue inventado para contener raíces de polinomios irreducibles reales.*

## 4.3. Número de Raíces Reales

El propósito de los temas que siguen es el de contestar las preguntas. Dado un polinomio $f(x)=a_0+a_1x+...+a_nx^n$ con coeficentes reales,

(1.)¿Cuántas raíces reales tiene?

(2.)Dado un intervalo real $[a,b]$. ¿Cuántas raíces reales tiene $f(x)$ en ese intervalo?

(2.)¿Es posible dar a priori un intervalo $[a,b]$ donde $f(x)$ tenga todas sus raíces en ese intervalo?

Para ello se demuestra la regla de los signos de Descartes, que si bien no resuelve completamente ninguna de las cuestiones planteadas, tiene la ventaja de ser una herramienta fácil y práctica a la hora de hacer cálculos, además de poder ser demostrada con técnicas elementales. Luego se presentará el Teorema de Sturm, que calcula el número de raíces que tiene un polinomio en un intervalo.

**Teorema 26.** *Todo polinomio de grado impar con coeficientes reales tiene por lo menos una raíz real.*

**Teorema 27.** *Si en una ecuación con coeficientes reales, el coeficiente principal* $a_n$ *y el término independiente* $a_0$ *tienen signos diferentes, entonces la ecuación tiene por lo menos una raíz positiva. Si además la ecuación es de grado par entonces también posee por lo menos una raíz negativa.*

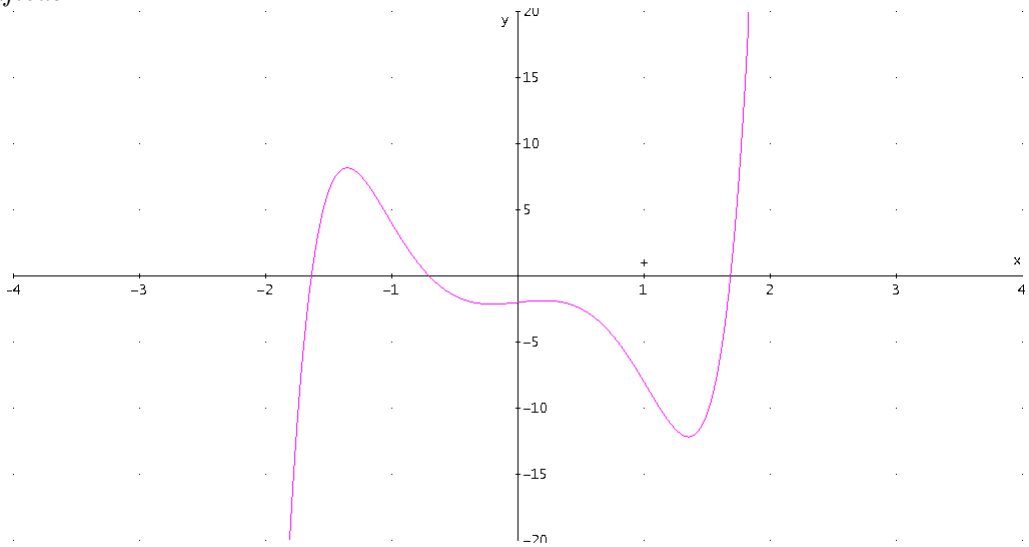
**Ejemplo 36.** *La ecuación*

$$x^7-8x^3+x-2=0$$

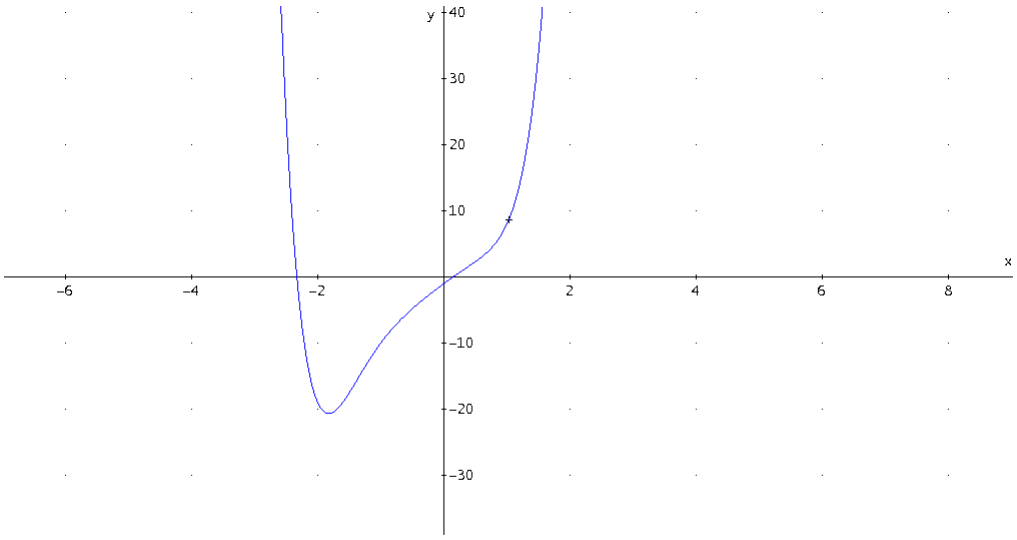
*tiene por lo menos una raíz positiva, en tanto que la ecuación*

$$x^6 + 2x^5 - x^2 + 7x - 1 = 0$$

*posee una raíz positiva y otra negativa. Esto puede comprobarse mediante las siguientes gráficas.*




$$x^6 + 2x^5 - x^2 + 7x - 1 = 0$$



### 4.3.1. Lemas de los Signos de Descartes

En 1636 Descartes en su libro "Geométrie" describió una regla para acotar el número de raíces positivas de un polinomio con coeficientes reales. La regla es muy sencilla lo cual la hace de gran utilidad.

**Definición 15.** *Dada una sucesión finita de números reales $x_1, x_2, x_3, ..., x_n$, se llama* ***número de variaciones de signo*** *de esta sucesión a la cantidad de "cambios" en el signo de la secuencia $x_1, x_2, x_3, ..., x_n$ descartando la presencia de elementos nulos.*
*El número de variaciones de signo de un polinomio es el correspondiente a la sucesión de sus coeficientes.*

**Lema 3.** *(**Primer Lema de Descartes**) Si $p(x)$ tiene coeficientes reales, y si $p(a) = 0$ donde $a > 0$, entonces $p(x)$ tiene como mínimo una variación de signos más que el polinomio cociente $q(x)$ donde $p(x) = (x - a)\, q(x)$, además cuando la diferencia en las variaciones de signos es mayor que 1, es siempre un número impar.*

**Demostración:** Los siguientes ejemplos particulares muestran que $q(x)$ puede tener menos variaciones de signos que $p(x)$. En este ejemplo, $p(x)$ tiene 3 variaciones de signo mientras que $q(x)$ tiene únicamente dos variaciones.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Coeficientes de $p(x)$ $\rightarrow$ | 12 | -77 | 152 | -77 | -30 | $\lfloor 2$ | $\rightarrow a$ |
| | | 24 | -106 | 92 | 30 | | |
| | --- | --- | --- | --- | --- | | |
| Coeficientes de $q(x)$ $\rightarrow$ | 12 | -53 | 46 | 15 | 0 | | |

En el próximo ejemplo, $p(x)$ tiene cuatro variaciones de signo mientras que $q(x)$ tiene únicamente un cambio. Así que la diferencia de las variaciones de signo es el número impar 3.

| | | | | | |
|---|---|---|---|---|---|
| 12 | -77 | 102 | -77 | 170 | $\lfloor$ 2 |
| | 24 | -106 | -8 | -170 | |
| --- | --- | --- | --- | --- | |
| 12 | -53 | -4 | -85 | 0 | |

Finalmente se muestra un ejemplo más, antes de empezar la demostración formal. En este ejemplo $p(x)$ tiene cuatro variaciones de signo y $q(x)$ tres. Además los coeficientes de $p(x)$ y $q(x)$ tienen los mismos signos columna por columna de izquierda a derecha hasta la columna del término constante de $q(x)$.

| | | | | | |
|---|---|---|---|---|---|
| 1 | -6 | 11 | -11 | 15 | ⌊3 |
| | 3 | -9 | 6 | -15 | |
| 1 | -3 | 2 | -5 | 0 | |

Se asume que el coeficiente principal de $p(x)$ es positivo y se usa la división sintética para calcular $p(a)$.

Se considera el término constante. Si el término constante es negativo como en el primer ejemplo, entonces la columna previa al término constante de $q(x)$ debe ser positivo para que los números de la columna final sumen cero.

Si el término constante de $p(x)$ es positivo como en el segundo ejemplo, entonces en la penúltima columna el término constante de $q(x)$ debe ser negativo para que los números de la columna final sumen cero.

Si el término constante de $p(x)$ es cero, se analizan las dos condiciones anteriores no con el término constante sino con el término de menor grado.
Así los términos constantes en $p(x)$ y $q(x)$ deben tener signos opuestos, este hecho se debe a que $a > 0$ y $p(a) = 0$.

Note que $q(x)$ y $p(x)$ empiezan con signos positivos y luego al leer de izquierda a derecha se afirma que $q(x)$ no puede cambiar de signo hasta que $p(x)$ lo haga.

Siempre que $q(x)$ cambie de signos de una columna a otra, $p(x)$ debe tambien cambiar de signo entre estas mismas dos columnas. Puede pasar tambien como en el segundo ejemplo (columnas 2 y 3, columnas 3 y 4) que $q(x)$ cambie los mismos signos cuando $p(x)$ cambie de signo, pero recuerde que $q(x)$ nunca puede cambiar de signo hasta que $p(x)$ lo haga primero.

Ahora suponga que al contar cambios de signos, en algún punto $p(x)$ cambia de signos, mientras que $q(x)$ no, como en los dos primeros ejemplos, así que $p(x)$ tendrá una variación

de signos más, y del punto anterior, $p\,(x)$ continuará cambiando de signos porque cada vez que $q\,(x)$ lo hace, también lo hace $p\,(x)$.

El otro caso que se necesita considerar al contar los cambios de signos, si llegamos al final de $q\,(x)$, y si en algún punto $p\,(x)$ y $q\,(x)$ tienen las mismas variaciones, como en el tercer ejemplo, entonces $p\,(x)$ y $q\,(x)$ tendrán los mismos signos en la penúltima columna, pero entonces $p\,(x)$ cambiará una vez más de signo en la última columna.

No importa el caso que se considere, $p\,(x)$ siempre tendrá como mínimo una variación de signo más que $q\,(x)$. Si el coeficiente principal de $p\,(x)$ es negativo, entonces se lo multiplica por $-1$ y se aplican los anteriores argumentos a este nuevo polinomio.

Se tiene ya probado que $p\,(x)$ tiene al menos una variación de signos más que el polinomio cociente $q(x)$. Ahora se demuestra que la diferencia es siempre un número impar, recuerde que los términos constantes de los dos polinomios difieren en signo, mientras que los primeros términos no.

Cuando ocurre una variación de signo, ésta se da en algún coeficiente interior.

**Ejemplo:** Si $p(x) = ax^3 - bx^2 + cx - d$ y $x_0$ es una raíz de $p(x)$, del método de Horner se tiene que:

| | | | | | |
|---|---|---|---|---|---|
| Coeficientes de $p(x)$ $\rightarrow a_3$ | | $a_2$ | $a_1$ | $a_0$ | $\lfloor\, x_0$ |
| | | $b_3x_0$ | $b_2x_0$ | $b_1x_0$ | |
| | | | | | |
| Coeficientes de $q(x)$ $\rightarrow b_3$ | | $b_2$ | $b_1$ | $\boxed{b_0}$ $\leftarrow$ Residuo | |

$q(x) = b_3x^2 + b_2x + b_1$.

Si cambia el signo de cualquier coeficiente interior, es decir de $b_2$ o $b_1$ al compararlos con $a_2$ y $a_1$ respectivamente, entonces la diferencia en la variación de signos aumenta o disminuye en 2, porque tal cambio se aplica al término anterior y a su siguiente, en este caso a $b_3$ y a $b_1$, o a $b_2$ y a $b_0$ según corresponda. Así cuando la diferencia en los números de variaciones de signo es mayor que 1, tal diferencia es impar.

**Lema 4.** *(**Segundo Lema de Descartes**) Si $p\,(x)$ tiene coeficientes reales, el número de raíces positivas de $p\,(x)$ no es mayor que el número de variaciones de signo en los*

*coeficientes de* $p\,(x)$.

**Demostración:** Sean $r_1, ..., r_k$ todas las raíces positivas del polinomio $p(x) = 0$ contando multiplicidad, entonces se puede escribir:

$$p(x) = (x - r_1)(x - r_2)(x - r_3)...(x - r_k)Q(x)$$

Por el lema 1 se sabe que $p(x)$ tiene como mínimo una variación de signo más que $Q\,(x)$.

Sea $q_1(x) = (x - r_2)(x - r_3)...(x - r_k)Q(x)$. Entonces $p(x)$ tiene como mínimo una variación de signo más que $q_1(x)$.

Además, como se puede escribir $q_1(x) = (x - r_2)(x - r_3)...(x - r_k)Q(x)$, se puede aplicar de nuevo el lema 1 para concluir que $q_1(x)$ tiene una variación de signo más que el polinomio $(x - r_3)...(x - r_k)Q(x)$.

Sea $q_2(x) = (x - r_3)...(x - r_k)Q(x)$.

Ahora $p(x)$ tiene como mínimo una variación de signo más que $q_1(x)$ y $q_1(x)$ tiene como mínimo una variación de signo más que $q_2(x)$, así $p(x)$ tiene como mínimo dos variaciones de signo más que $q_2(x)$.

Claramente se puede continuar reagrupando los factores de la derecha y reducir el número de factores.

$q_2(x) = (x - r_3)...(x - r_k)Q(x) = (x - r_3)\left[(x - r_4)...(x - r_k)Q(x)\right]$, luego $q_2(x)$ tiene una o mas variaciones de signo que $q_3(x) = (x - r_4)...(x - r_k)Q(x)$.

Para cada factor que quitamos, $p(x)$ tiene todavía como mínimo otro signo de variación mas que el factor resultante de la derecha. Después, disminuyendo todo $k$ factor se concluye que $p(x)$ tiene $k$ o mas variaciones de signo que $Q(x)$.

Como disminuyen los $k$ factores, $Q(x)$ es el factor que falta.

Ahora asuma que $Q(x)$ tiene $m$ variaciones de signo en estos coeficientes y que $p(x)$ tiene $n$ variaciones de signo en estos coeficientes. Entonces porque $m \geq 0$, $m + k \leq n$ implica que $k \leq n$.

Por tanto, el número de ceros positivos de $p(x)$ es menor o igual al número de variaciones de signo en los coeficientes de $p(x)$.

**Lema 5.** *(**Tercer Lema de Descartes**) Sean $r_1, r_2, ..., r_k$ denotan $k$ números positivos y $p(x) = \prod_{i=1}^{k}(x - r_i)$, entonces los coeficientes de $p(x)$ se alternan todos en signo y así este polinomio tiene exactamante $k$ variaciones de signos en estos coeficientes.*

**Demostración:** Usando inducción en $k$ y de la demostración del lema anterior se concluye que $Q(x) = 1$ tiene $k$ variaciones de signo menos que $p(x)$. Pero como 1 no tiene variaciones de signo, entonces $p(x)$ tiene $k$ variaciones en signo lo que quiere decir que todos los coeficientes se alternan en signos.

**Ejemplo:** $(x - r_1)(x - r_2) = x^2 - (r_1 + r_2)x + (-1)^2 r_1 r_2$.

Usando inducción, si $k = 1$, note que $(x - r_1)$ tiene exactamante una variación de signo. Asuma que el teorema es verdadero para cualquier polinomio con $k$ factores o menos.

Se prueba para $k + 1$ factores:

$$p(x) = \prod_{i=1}^{k+1}(x - r_i) = (x - r_{k+1})\prod_{i=1}^{k}(x - r_i)$$

Si se considera el segundo factor como el polinomio cociente, se puede aplicar inducción para concluir que el cociente tiene exactamente $k$ variaciones de signo. Aplicando el primer lema a $p(x)$ se concluye que este tiene como mínimo una variación de signo más que el cociente; esto quiere decir que $p(x)$ tiene exactamente $k+1$ variaciones de signo. Siendo $(k+1)^{st}$ un grado polinomial, $p(x)$ no puede tener más que $k + 1$ variaciones de signo porque este tiene únicamente $k + 2$ coeficientes.

**Lema 6.** *(**Cuarto Lema de Descartes**) El número de variaciones de signo de un polinomio con coeficientes reales es par si el coeficiente principal y el último coeficiente coinciden en signo, y es impar si no coinciden.*

**Demostración:** Antes de empezar la demostración se presenta un ejemplo:

Sea $p(x) = x^4 - 6x^3 + 11x^2 - 12x + 15$. En este caso, el primer y último coeficientes tienen los mismos signos y se puede ver que $p(x)$ tiene un número par de cambios de signo, cuatro cambios.

El $grad\,(p(x)) = 4$, este tiene cinco coeficientes, lo que implica que debe tener a lo más cuatro variaciones de signo. Si se cambia el signo del primer o último coeficiente, se podrá tener un cambio de signo menos, es decir, un número impar de cambios de signo.

Si se incrementa el grado de $p(x)$ adicionando justo un término, entonces no podemos asegurar que aumentamos un cambio de signo a no ser que el signo de este nuevo término difiera del signo del que era el término principal.

Se demuestra este lema por inducción en el grado $n$ del polinomio $p(x)$.

Cuando $n = 1$, $p(x) = ax + b$.

Si $b = 0$, $p(x)$ no tiene cambios de signo.

Suponga que $b \neq 0$.

Si $a$ y $b$ tienen los mismos signos, entonces $p\,(x)$ tiene cero o un número par de cambios de signo, en caso contrario $p\,(x)$ tiene 1 o un número impar de cambios de signo. Luego el lema es verdadero cuando $n = 1$.

Asuma que el lema es verdadero cuando $n \leq k$, y sea $p(x)$ un polinomio de grado $k + 1$. Se debe probar que el lema se cumple para $p(x)$.

Considere el polinomio $q\,(x)$ de grado $k$, obtenido al quitar el término principal de $p(x)$. El lema se asume verdadero para $q(x)$. El grado de $q\,(x)$ puede ser tambien menor que $k$, en el caso en que el coeficiente correspondiente a $x^k$ sea cero.

Existen 2 casos:

**Caso 1:** El término principal de $q(x)$ y el último término tienen los mismos signos.

Se sabe por inducción que $q(x)$ tiene un número par de cambios de signo. Existen únicamente dos posibilidades para el signo del término principal que se quitó.

Si este término tiene el mismo signo que el término principal de $q(x)$, entonces no hay cambios de signo cuando este término se adiciona. Así $p\,(x)$ tiene un número par de cambios de signo y el término principal y el último término de $p\,(x)$ tienen los mismos signos.

Si el término principal que se quitó tiene un signo diferente del término principal en $q(x)$, entonces existe un cambio de signo adicional que se obtiene cuando este término se coloca otra vez. Por tanto en este caso $p(x)$ tendría un número impar de cambios de

signo. Pero también en este caso, el término principal y el último término de $p\,(x)$ tienen signos opuestos.

**Caso 2:** El término principal de $q(x)$ y el último término tienen signos opuestos.

Se conoce por inducción que $q(x)$ tiene un número impar de cambios de signo. Existen únicamente dos posibilidades para el signo del término principal que se quitó.

Si este término tiene el mismo signo que el término principal de $q(x)$, entonces no existen cambios de signo cuando este término se adiciona. Así $p\,(x)$ no varía en el número impar de cambios de signo, y el término principal y el último término de $p\,(x)$ continúan con signos opuestos.

Si el término principal que se quitó y el de $q(x)$ difieren de signo, entonces existe un cambio adicional de signo cuando este término se coloca otra vez. Así en este caso $p\,(x)$ tiene un número par de cambios de signo. También se puede decir que en este caso el término principal y el último término de $p(x)$ tienen los mismos signos.

En ambos casos el lema es verdadero para $p(x)$ con grado $k+1$. Esto completa la demostración por inducción en $n$.

**Lema 7.** *(**Quinto Lema de Descartes**) Si el número de raíces positivas de $p(x)$ con coeficientes reales es menor que el número de variaciones de signos en $p(x)$, este es menor en un número par.*

**Demostración:** Si el coeficiente principal de $p(x)$ es 1, se puede descomponer a $p\,(x)$ en factores: $p\,(x) = x^t(x-r_1)...\,(x-r_k)\,(x-n_1)\,...(x-n_j)\,(x^2+b_1x+c_1)\,...\,(x^2+b_lx+c_l)$, donde $t$ es un entero mayor que cero. Como se puede ver, en este caso $p(x)$ tiene al cero como raíz debido al factor $x^t$. Como el quinto lema de Descartes se refiere al número de raíces positivas del polinomio, se estudiará el caso en el que $p(x)$ se factoriza de la siguiente manera:

$p\,(x) = (x-r_1)...\,(x-r_k)\,(x-n_1)\,...(x-n_j)\,(x^2+b_1x+c_1)\,...\,(x^2+b_lx+c_l)$

donde los $r_i$ denotan todos los ceros positivos de $p(x)$, los $n_i$ los ceros negativos, y los factores restantes son cuadráticos correspondientes a todos los pares de raíces no reales conjugadas de $p(x)$.

Sea $s$ el número de cambios de signo en los coeficientes de $p(x)$. Asuma que $k < s$, se muestra que existe un entero par $e$ tal que $e > 0$ y $k + e = s$.

Sea $f(x) = (x - n_1) ...(x - n_j) (x^2 + b_1x + c_1) ... (x^2 + b_lx + c_l)$

Del segundo lema de Descartes, se sabe que el polinomio $f(x)$ tiene por lo menos $k$ variaciones de signo menos que $p(x)$. Se llama $t$ al número de cambios de signo en el polinomio $f(x)$, entonces $s - k - t \geq 0$, por tanto, $s - k \geq t \geq 0$.

Note una propiedad especial de cada uno de los factores cuadráticos irreducibles. El discriminante de cada uno de los factores cuadráticos debe ser negativo, luego $b_i^2 - 4 \cdot 1 \cdot c_i < 0$. Así $0 \leq b_i^2 < 4c_i$ y se concluye que todos los coeficientes $c_i$ son estrictamente positivos.

Además, cada factor $(x - n_i)$ de $f(x)$ puede ser escrito como $(x + p_i)$ donde $p_i = -n_i$ es positivo. Luego se puede escribir $f(x) = (x + p_1) ...(x+p_j) (x^2 + b_1x + c_1) ... (x^2 + b_lx + c_l)$.

Es claro que el coeficiente principal de $f(x)$ es $+1$, y el término constante de $f(x)$ es también positivo, ya que este es el producto de todos los números positivos.

El término constante de $f(x) = \prod_{i=1}^{j} p_i \prod_{i=1}^{l} c_i$.

Por el cuarto lema de Descartes, el número de variaciones de signo en los coeficientes de $f(x)$ es par, es decir $t$ es par. De lo anterior se tiene que $s - k \geq t \geq 0$. Sin embargo $s \geq t + k$. Si ocurre que $t + k = s$ entonces $e = t$ y se ha terminado.

De otro modo, si $s > t + k$ se debe razonar acerca de los primeros $k$ factores en $p(x)$. Teniendo que el término constante de $f(x)$ es positivo, el signo del término constante en $p(x)$ es el signo de $(-1)^k \prod_{i=1}^{k} r_k$ igual al signo de $(-1)^k$ donde todos los $r_i$ son valores positivos. Si $k$ es par entonces por el cuarto lema, $p(x)$ tiene un número par de variaciones de signo en estos coeficientes, de lo cual $s$ es par.

Si $k$ es impar, entonces de nuevo por el cuarto lema se concluye que $s$ es impar.

Así $k$ y $s$ son pares o impares a la vez.

Ahora considere $s - t - k > 0$. ¿Qué clase de número positivo es este?. Bien, $t$ es par y si $k$ y $s$ son pares entonces $s - t - k$ debe ser par. Haciendo el mismo procedimiento, si $k$ y $s$ son impares, entonces $s - k$ es aún par, y como $t$ es siempre par, $s - (t + k)$ debe ser par.

Por esta razón $s - t - k = 2v$ para algún entero positivo $v$.

Entonces, $(2v+t)+k=s$. Sea $e=(2v+t)$. Lo que resta es mostrar que $2v+t$ es un entero positivo par. Primero, $2v+t=s-k$ y como $s-k>0$, se sabe que $2v+t$ es un entero positivo. Segundo, $t$ y $2v$ son pares, así que su suma $2v+t$ es par. En cualquier caso, existe un entero positivo par $e$ tal que $e+k=s$. Así cuando $s$ es mayor que $k$, este es más grande en un entero positivo par.

**Lema 8.** *(**Sexto Lema de Descartes**) Cada raíz negativa de $p(x)$ corresponde a una raíz positiva de $p(-x)$. Es decir, si $a<0$ y $a$ es una raíz de $p(x)$, entonces $-a$ es una raíz positiva de $p(-x)$.*

**Demostración:** La gráfica de la función $y=p(-x)$ es justamente la gráfica de $y=p(x)$ reflejada sobre el eje $y$. Así, si $a<0$ y $p(a)=0$, entonces $-a>0$, y cuando $x=-a$, entonces $p(-x)=p(-(-a))=p(a)=0$. Por lo tanto, $-a$ es un cero positivo de $p(-x)$.

**Teorema 28.** ***( Teorema de la regla de los signos de Descartes):***

*Sea $p(x)$ un polinomio con **coeficientes reales.***

*El número de raíces positivas de $p(x)=0$ es igual al número de variaciones de signo en los coeficientes de $p(x)$ o menor que este número en un entero par.*

*El número de raíces negativas de $p(x)=0$ es igual al número de variaciones de signo en los coeficientes de $p(-x)$ o menor que este número en un entero par.*

**Demostración:** El punto donde se habla del número de raíces positivas de $p(x)=0$ es exactamente lo que se trata en el *quinto lema* ya demostrado.

Para mostrar la proposición acerca del número de raíces negativas de $p(x)$ se necesita únicamente aplicar el *sexto lema*. Cada raíz negativa de $p(x)$ corresponde a una raíz positiva de $p(-x)$ y por el *quinto lema*, el número de raíces positivas de cualquier polinomio como $p(-x)$ es igual al número de variaciones de signo en este polinomio $p(-x)$, o es menor que el número de variaciones en este polinomio $p(-x)$ en un entero positivo par.

**Ejemplo 37.**

***1.*** *De acuerdo a la regla de los signos el polinomio $x^k+x^u-x-1$, $k,u>1$ tiene exactamente una raíz real positiva. De hecho $x_0=1$ es esa raíz. Del teorema se deduce tambien que esta raíz es simple.*

***2.*** *En general, si $A$ y $B$ son números reales positivos, entonces $Ax^k + Bx^u - x - 1$, $k, u > 1$ tendrá una sola raíz real positiva.*

**Ejemplo 38.** *Sea $f(x) = ax^2 + bx + c$.*

***1.*** *$a > 0$, $b > 0$, $c > 0$. En este caso el teorema dice que $f(x)$ no tiene ninguna raíz real positiva. Como $f(-x) = ax^2 - bx + c$ el teorema afirma que tiene dos raíces reales negativas o ninguna.*

***2.*** *$a > 0$, $c < 0$. Si $b > 0$, $f(x) = ax^2 + bx + c$, $f(-x) = ax^2 - bx + c$.*
*Si $b < 0$, $f(x) = ax^2 - bx + c$, $f(-x) = ax^2 + bx + c$.*
*En los dos casos $f(x)$ y $f(-x)$ tienen solo una variación de signo, entonces el teorema dice que $f(x)$ posee una raíz real positiva y una negativa.*

***3.*** *$a > 0$, $b < 0$, $c > 0$.*
*$f(x) = ax^2 - bx + c$, $f(-x) = ax^2 + bx + c$*

*Aquí $f(x)$ tiene dos variaciones de signo y $f(-x)$ no tiene variaciones de signo, entonces el teorema afirma que $f(x)$ tiene una raíz de multiplicidad dos, o dos raíces reales positivas o ninguna, y no tiene raices reales negativas.*

**Ejemplo 39.** *Sea $p(x) = x^{11} + x^8 - 3x^5 + x^4 + x^3 - 2x^2 + x - 2$. La variación de signos de los coeficentes de $p(x)$ es 5. Por otro lado, $p(-x) = -x^{11} + x^8 + 3x^5 + x^4 - x^3 - 2x^2 - x - 2$, que tiene como variación de signos 2. Luego se puede concluir lo siguiente:*

- *La cantidad de raíces positivas de $p(x)$ es uno, tres o cinco.*
- *La cantidad de raíces negativas de $p(x)$ es cero o dos.*
- *$p(x)$ tiene al menos cuatro raíces complejas no reales.*

### 4.3.2. Algoritmo de Sturm

Sturm propuso un método más refinado y preciso pues a diferencia de Descartes aquí ya no se dan cotas para el número de raíces, sino que da el número exacto de raíces reales en un intervalo.

Sea $p(x) \in \mathbb{R}[x]$, a partir de $p(x)$ se armará una sucesión finita

$$(p_0(x), p_1(x), p_2(x), ...)$$

de polinomios cuya variación de signos dará información sobre las raíces de $p(x)$. Esta sucesión se denomina la sucesión de Sturm, y para calcularla se hace uso del algoritmo de Euclides para polinomios con una pequeña modificación.

**Definición 16.** ***Sucesión de Sturm:***

- $f_0(x) = f(x)$
- $f_1(x) = f'(x)$
- $f_2(x) = -r_1(x)$ *(el residuo con el signo cambiado), donde* $f_0(x) = q_1(x)f_1(x)+r_1(x)$, *el algoritmo de la división entre* $f_0(x)$ *y* $f_1(x)$.
- *Más en general, dados* $f_i(x)$ *y* $f_{i+1}(x)$, *si* $f_{i+1}(x) \in \mathbb{R}$, *entonces se termina. Si no, se hace* $f_i(x) = q_{i+1}(x)f_{i+1}(x)+r_{i+1}(x)$, *el algoritmo de la división entre* $f_i(x)$ *y* $f_{i+1}(x)$ *y se define* $f_{i+2}(x) = -r_{i+1}(x)$. *Está claro que se tiene* $grad(f_0(x)) > grad(f_1(x)) > grad(f_2(x)) > ...$, *o sea que la sucesión se termina siempre.*
- Considere la sucesión de funciones polinómicas,
  $\rho(x) = \{f_0(x), f_1(x), f_2(x), ..., f_r(x) = c\}$.
  Para $x_0$ que no sea raíz de $f_0(x) = f(x)$, sea $w(x_0)$ el número de cambios de signo en la sucesión $\rho(x_0) = \{f_0(x_0), f_1(x_0), f_2(x_0), ..., f_r(x_0) = c\}$

**Teorema 29.** ***(McLaurin:)***

*Sea* $f(x) = x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0$ *un polinomio mónico con coeficientes reales, y sea* $M =máx\{1, |a_{n-1}| + ... + |a_1| + |a_0|\}$, *entonces todas las raíces reales de* $f(x)$ *estan entre* $-M$ *y* $M$.

Teniendo en cuenta todo lo anterior se escribe formalmente el teorema de Sturm:

**Teorema 30.** ***Teorema de Sturm :*** *Sea* $f(x) \in \mathbb{R}[x]$. *Si* $x_0, x_1 \in \mathbb{R}$ *con* $x_0 < x_1$ *y* $f(x_0) \neq 0$, $f(x_1) \neq 0$ *entonces, el número de raíces reales de* $f(x)$ *en* $(x_0, x_1)$ *contadas* ***sin multiplicidad*** *es igual a* $w(x_0) - w(x_1)$.

**Demostración:** Como en la demostración del teorema de Descartes, se estudiará como varía la función $w(x)$ a medida que $x$ avanza en el intervalo $(x_0, x_1)$.
Sea $f(x) \in \mathbb{R}[x]$.
**i.)** Suponga que el polinomio no tiene raíces múltiples.
Sea $\rho(x) = [f_0(x), f_1(x), ..., f_r(x) = c]$ la sucesión de funciones obtenidas al utilizar el algoritmo de Euclides modificado como en la definición **16**.

Como $f(x)$ no tiene raíces múltiples, entonces el $MCD(f(x), f\prime(x)) = f_r(x)$ una constante distinta de cero.
Sean $d_1, ..., d_s$ raíces de una o más de las funciones de la sucesión $\rho(x)$ en el intervalo $(x_0, x_1)$; excepto de $f_r(x)$ ya que es una constante.

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| $b$ | $d_1$ | $d_2$ | ... | $d_{i-1}$ | $d_i$ | $d_{i+1}$ | ... | $d_s$ | $c$ |

Ningún $d_i$, para $i = 1, 2, ..., s$, puede ser raíz de $f_j(x)$ y $f_{j+1}(x)$ para algún $j$. Pues, en ese caso se tendría:

$$f_j(d_i) = f_{j+1}(d_i)\, q_{j+1}(d_i) - f_{j+2}(d_i),\ f_{j+2}(d_i) = 0;$$

y

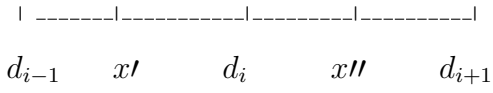
$$f_{j+1}(d_i) = f_{j+2}(d_i)\, q_{j+2}(d_i) - f_{j+3}(d_i),\ f_{j+3}(d_i) = 0;$$

continuando de esta manera, se obtiene que $f_r(d_i) = 0$; pero $f_r(x)$ es una constante distinta de cero.
Ahora se considera la función $w(x)$, para hallar el número de variaciones de signo de la sucesión $\rho(x)$ las cuales se realizan de izquierda a derecha en el intervalo $(x_0, x_1)$, donde $x \in (x_0, x_1)$ .
Si se varía $x$ en un intervalo formado por dos $d_i's$ consecutivos, es decir, si $x\prime$ y $x\prime\prime$ son

dos números entre $d_{i-1}$ y $d_i$, entonces $f_j(x\prime)$ y $f_j(x\prime\prime)$ tienen el mismo signo, para cada $j$. Esto es, $w(x\prime) = w(x\prime\prime)$.

Ahora, observe que pasa cuando $x$ toma un valor mayor a $d_i$.

Considere a $x\prime$ y $x\prime\prime$ como se ilustra.




Suponga que $d_i$ es una raíz de $f_0(x)$, entonces se tiene que $d_i$ no puede ser raíz de $f_1(x)$, de donde se desprenden dos casos:

**caso 1:** $f_1(d_i)$ es positivo. Entonces $f_1(x)$ es positivo para todo $x$ entre $d_{i-1}$ y $d_{i+1}$. Como $f_0(d_i) = 0$, $f_0(x\prime)$ es negativo, mientras que $f_0(x\prime\prime)$ es positivo, y los signos en la sucesión $\rho(x)$ empiezan en:

$\rho(x\prime) = [-, +, ...]$, $\rho(x\prime\prime) = [+, +, ...]$

**caso 2:** $f_1(d_i)$ es negativo. Entonces $f_1(x)$ es negativo para todo $x$ entre $d_{i-1}$ y $d_{i+1}$. Como $f_0(d_i) = 0$, $f_0(x\prime)$ es positivo, mientras que $f_0(x\prime\prime)$ es negativo, y los signos en la sucesión $\rho(x)$ empiezan en:

$\rho(x\prime) = [+, -, ...]$, $\rho(x\prime\prime) = [-, -, ...]$.

En cada uno de los dos casos, el efecto en $w(x)$ es que $w(x\prime\prime) = w(x\prime) - 1$, es decir $w(x)$ disminuye en 1 en el intervalo $(x_0, x_1)$ al pasar por una raíz de $f_0(x)$.

Suponga que $d_i$ es una raíz de $f_j(x)$, $j > 0$. Entonces $d_i$ no es raíz de $f_{j-1}(x)$ ni de $f_{j+1}(x)$.

Ahora,

$$f_{j-1}(x) = f_j(x) q_j(x) - f_{j+1}(x)$$

así, en particular, en $d_i$, donde $f_j(d_i) = 0$, $f_{j-1}(d_i)$ y $f_{j+1}(d_i)$ tienen signos opuestos para toda $x$ entre $d_{i-1}$ y $d_{i+1}$.

En consecuencia $\rho(x\prime) = [..., +, *, -, ...]$ y $\rho(x\prime\prime) = [..., -, *, +, ...]$, donde $*$ denota el signo de $f_j$ que puede ser $+$, 0, o $-$, es decir, no habrá diferencia al computar $w(x\prime)$ o $w(x\prime\prime)$. Así el hecho de que $d_i$ sea una raiz de $f_j(x), j > 0$, no efectua ningun cambio en $w(x)$ para $x \in (x_0, x_1)$ al pasar por $d_i$.

El mismo argumento se tiene en caso de que $d_1 = x_0$ o $d_s = x_1$.

Si por ejemplo, $d_1 = x_0$ es una raíz de $f_j(x)$ para algún $j > 0$, entonces para $x''$ entre $d_1$ y $d_2$

$$\rho(x_0) = [..., +, 0, -, ...], \text{ entonces } \quad \rho(x'') = [..., +, *, -, ...], \text{ mientras que si}$$
$$\rho(x_0) = [..., -, 0, +, ...], \text{ entonces } \quad \rho(x'') = [...-, *, +...],$$

donde $*$ puede ser $+$ o $-$. Por tanto en cualquier caso, $w(x)$ no cambia al estar a la derecha de $x_0$. El caso de $d_s = x_1$ es similar.

Resumiendo, cuando $x$ toma valores en el intervalo $(x_0, x_1)$, $w(x)$ actua asi:

El valor de $w(x)$ no cambia en cualquier intervalo que no contenga raíces de cualquier $f_j(x)$;

El valor de $w(x)$ no se afecta al pasar después de un punto $d_i$ por el hecho de que $d_i$ sea una raíz de $f_j(x)$, si $j > 0$;

El valor de $w(x)$ disminuye en 1 al pasar después de un punto $d_i$ el cual es una raíz de $f_0(x) = f(x)$;

Si $x_0, x_1$ no son raíces de $f_0(x)$, no son raíces de $f(x)$ , entonces el valor de $w(x)$ no cambia al estar a la derecha de $x_0$ o a la izquierda de $x_1$.

Por tanto, $w(x_0) - w(x_1) =$ al número de raíces $d_i$ entre $x_0$ y $x_1$ las cuales son raíces de $f(x)$, por consiguiente es igual al número de raíces distintas de $f(x)$ entre $x_0$ y $x_1$.
**ii.)** El polinomio tiene raíces múltiples.
De la **proposición 7** se tiene que dados $f(x)$ y $f'(x)$ en $\mathbb{R}[x]$, si $d(x) = MCD(f(x), f'(x))$, entonces $g(x) = \dfrac{f(x)}{d(x)}$, tiene exactamente las mismas raíces que $f(x)$ pero cada una ocurre en $g(x)$ con multiplicidad 1. De esta manera se puede aplicar el teorema a $g(x)$, y la demostración es como en $i$.)

**Ejemplo 40.** *Sea* $f(x) = x^4 + 2x^3 + 3x^2 + 1$. *Por el teorema* ***29*** *se tiene que toda raiz está entre* $-M$ *y* $M$, *en este caso* $M = 6$, *así que las raíces están entre -6 y 6.*

*El algoritmo de Euclides modificado con* $f(x)$ *y* $f\prime(x)$ *da la sucesión de funciones*

$$\rho(x)\begin{cases} x^4+2x^3+3x^2+1 \\ 4x^3+6x^2+6x \\ \frac{-3}{4}x^2+\frac{3}{4}x-1 \\ \frac{-32}{3}x+\frac{40}{3} \\ \frac{158}{128} \end{cases}$$

*Evaluando* $-6$ *en* $x$*, estas funciones tienen los siguientes signos* $[+,-,-,+,+]$.

*Así* $w(-6)=2$.

*Evaluando* $6$ *en* $x$ *las funciones tienen los siguientes signos* $[+,+,-,-,+]$.

*En consecuencia* $w(6)=2$.

*Por consiguiente* $w(-6)-w(6)=0=$ *al número de raíces reales distintas de* $f(x)$ *entre* $-6$ *y* $6$*. Como toda raíz debe estar entre* $-6$ *y* $6$*,* $f(x)$ *no tiene raíces reales.*

**Ejemplo 41.** *Sea* $f(x)=x^3-5x^2+8x-8$ *La sucesión de funciones* $\rho(x)$ *es:*

$$\rho(x)\begin{cases} x^3-5x^2+8x-8 \\ 3x^2-10x+8 \\ \frac{2}{9}(x+16) \\ -936 \end{cases}$$

*Aquí* $M=21$*. Evaluando* $x=-21$ *la sucesión de números* $\rho(-21)$ *tiene los siguientes signos* $[-,+,-,-]$.

*En* $x=21$*, la sucesión de números* $\rho(21)$ *tiene los siguientes signos* $[+,+,+,-]$.

*Luego* $w(-21)=2$. $w(0)=2$ *y* $w(21)=1$*. Esto significa que existe solo una raíz real de* $f(x)$ *y está entre* $0$ *y* $21$*. Se puede olvidar la sucesión* $\rho(x)$ *y observar que* $f(0)<0$*,* $f(21)>0$ *a través del eje* $x$.

*Pruebe algunos valores de* $x$*:* $f(12)$ *es* $+$*,* $f(6)$ *es* $+$*,* $f(3)$ *es* $-$*,* $f(4)$ *es* $+$*, por consiguiente la raíz está entre* $3$ *y* $4$.

# Apéndice A

## A.1.

**Teorema 31.** *(Teorema Chino del Residuo para Polinomios): Sea $K$ un campo. Sean $a_1(x), ...a_n(x)$ polinomios arbitrarios, y $m_1(x), ...m_n(x)$ polinomios primos relativos por parejas en $K[x]$. Existe un único polinomio $f(x)$ en $K[x]$ tal que:*

$$\begin{aligned} f(x) &\equiv a_1(x)(\mod m_1(x)) \\ &\vdots \\ f(x) &\equiv a_n(x)(\mod m_n(x)), \end{aligned} \qquad (*)$$

*el grado de $f(x)$ es menor que el grado de $m_1(x)m_2(x)...m_n(x)$.*

**Demostración:**

Como $m_i(x)$ y $m_j(x)$ son primos relativos para $i \neq j$, $m_i(x)$ es primo relativo con el producto

$$l_i(x) = m_1(x)m_2(x)...m_{i-1}(x)m_{i+1}(x)...m_n(x).$$

Solucionando la ecuación

$$1 = h_i(x)m_i(x) + k_i(x)l_i(x)$$

de donde $h_i(x)$, $k_i(x)$ resultan al aplicar el Teorema **8**. Entonces para cada $i = 1, ..., n$ $k_i(x)l_i(x)$ satisface $k_i(x)l_i(x) \equiv 0(\mod m_j(x))$ para todo $j \neq i$

$k_i(x)l_i(x) \equiv 1(\mod m_i(x))$

Así que se resuelve $(*)$ colocando

$$f(x) = a_1(x)k_1(x)l_1(x) + a_2(x)k_2(x)l_2(x) + ... + a_n(x)k_n(x)l_n(x).$$

Si $f(x)$ tiene grado mayor o igual que el grado de $m_1(x)m_2(x)...m_n(x)$ se usa el algoritmo de la división para reemplazar $f(x)$ por $r(x) = f(x) - q(x)[m_1(x)m_2(x)...m_n(x)]$, donde el grado de $r(x)$ puede hacerse menor que el grado de $m_1(x)m_2(x)...m_n(x)$.

# A.2.

**Definición 17.** *La función $\varphi$ de Euler, $\varphi(n)$, está definida por $\varphi(1) = 1$ y, para $n > 1$, $\varphi(n) =$al número de enteros positivos $m$, con $1 \leq m < n$ y tal que $(m, n) = 1$.*

# A.3.

**Teorema 32.** *(Teorema de Euler): Si $n$ es un entero positivo y $a$, $n$ son primos relativos, entonces $a^{\varphi(n)} \equiv 1(\mod n)$.*

# A.4.

**Teorema 33.** *Si $(m, n) = 1$, entonces $\varphi(m, n) = \varphi(m)\varphi(n)$.*

# A.5.

**Definición 18.** *Un campo de descomposición $k$ sobre un campo $F$ de $x^n - 1 \in F[x]$ (donde $n \geq 1$) es llamado una **extensión ciclotómica de orden** $n$.*

# A.6.

**Teorema 34.** *Sea $F$ una extensión ciclotómica de orden $n$ del campo $\mathbb{Q}$ de los racionales y $g_n(x)$ el $n-$ésimo polinomio ciclotómico sobre $\mathbb{Q}$. Entonces*

***(i)*** *$g_n(x)$ es irreducible en $\mathbb{Q}[x]$.*

***(ii)*** *$[F:\mathbb{Q}] = \varphi(n)$, donde $\varphi$ es la función de Euler.*

***(iii)*** *$Aut_{\mathbb{Q}}F$ es isomorfo al grupo multiplicativo de unidades en el anillo $\mathbb{Z}_n$, es decir es isomorfo al grupo formado por los enteros positivos menores que $n$ y primos relativos con $n$ bajo la multiplicación módulo $n$.*

# A.7.

**Teorema 35.** *(Teorema de Fermat): Si $p$ es un número primo y $a$ es cualquier entero, entonces $a^p \equiv a(\mod p)$.*

**Demostración:** Como $\varphi(p) = p-1$, si $(a,p) = 1$, entonces, del teorema de **Euler** $a^{p-1} \equiv 1(\mod p)$, de donde $a^p \equiv a(\mod p)$. Si $a$ no es primo relativo con $p$, como $p$ es un número primo se debe tener que $p \mid a$, así que $a \equiv 0(\mod p)$.
Por lo tanto, $a^p \equiv a \equiv 0(\mod p)$.

# A.8.

**Definición 19.** *Sea $n$ un entero positivo y $a$ un entero tal que $(a,n) = 1$. El menor entero positivo $k$ tal que $a^k \cong 1(\mod n)$ se llama el **orden de** $a$ **módulo** $n$ y lo representamos por la notación $ord_n a$.*

# A.9.

**Teorema 36.** *Si $a$ es un entero primo relativo con $n$, entonces $ord_n a \mid \varphi(n)$.*

**Demostración:** Suponga que $ord_n a = k$.
Si $ord_n a = k$, entonces $a^k \equiv 1(\mod n)$.
Si $a^k \equiv 1(\mod n)$ y $a^{\varphi(n)} \equiv 1(\mod n)$, entonces $k \mid \varphi(n)$. Es decir $\varphi(n) = kq + r$, donde $0 < r < k$, así $r = \varphi(n) - kq$. Luego, $a^r = a^{\varphi(n)-kq} = a^{\varphi(n)}(a^k)^{-q}$, en consecuencia

$a^r = 1$. Se tenía que $a^k \equiv 1(\mod n)$ y $k$ es el número mas pequeño por lo que $r = 0$. Por lo tanto, Si $(a, n) = 1$, entonces $ord_n a \mid \varphi(n)$.

# A.10.

**Definición 20.** *Si el* $ord_n a = \varphi(n)$, *decimos que* $a$ *es* ***raíz primitiva módulo*** $n$.

**Ejemplo 42.** ***(1)*** *Si* $n = 10$, $\varphi(10) = 4$. *Los enteros primos relativos con* 10 *y menores que* 10 *son* $1, 3, 7$ *y* 9. *Se tiene la siguiente tabla de potencias:*

| $a$ | $a^2$ | $a^3$ | $a^4$ |
|---|---|---|---|
| 1 | | | |
| 3 | 9 | 7 | 1 |
| 7 | 9 | 3 | 1 |
| 9 | 1 | | |

*Por lo tanto* $ord_{10}1 = 1$, $ord_{10}3 = 4$, $ord_{10}7 = 4$, $ord_{10}9 = 2$. *Así que las raices primitivas módulo 10 son 3 y 7.*

***(2)*** *No hay raices primitivas módulo 12 pues* $\varphi(12) = 4$ *y la tabla de potencias para los números* $a < 12$ *y primos relativos con* 12 *es:*

| $a$ | $a^2$ |
|---|---|
| 1 | |
| 5 | 1 |
| 7 | 1 |
| 11 | 1 |

# A.11.

**Teorema 37.** *Si $n$ tiene una raiz primitiva $g$ entonces $n$ tiene exactamente $\varphi(\varphi(n))$ raíces primitivas incongruentes y están dadas por los números del conjunto.*

$S = \{g^m : 1 \leq m \leq \varphi(n),\ y\ (m, \varphi(n)) = 1\}$.

# A.12.

**Teorema 38.** *Si $p$ es un número primo, hay exactamente $\varphi(p-1)$ raices primitivas módulo $p$.*

Esto es inmediato, ya que por el teorema anterior se tiene que el número de raíces primitivas es $\varphi(\varphi(p)) = \varphi(p-1)$

# A.13.

**Teorema 39.** *El grupo de las unidades del anillo $Z_n$ esta formado por todas las clases $\bar{a}$ donde $\bar{a} = \{x \in Z \mid x \cong a\,(\mod n)\}$, tales que $(a, n) = 1$. Este grupo tiene orden $\varphi(n)$ y se Representa por $G_n$.*

**Demostración:** Supongamos que $\bar{a}$ es una unidad de $Z_n$. Luego existe $\overline{b} \in Z_n$ tal que $\bar{a}\overline{b} = \overline{1}$. Por lo tanto $ab \cong 1\,(\mod n)$ y tenemos que $ab - 1 = qn$ para algún entero $q$. Luego $ab - qn = 1$ y por teorema 10 se concluye que $(a, n) = 1$. Recíprocamente, si $(a, n) = 1$ por el teorema **10** nuevamente existen enteros $b$ y $q$ tales que $ab - qn = 1$. Luego $ab \cong 1\,(\mod n)$, o sea $\bar{a}\overline{b} = \overline{1}$ y por lo tanto $\bar{a}$ es una unidad de $Z_n$.

De esta forma hemos probado que en el anillo

$Z_n = \left\{\overline{0}, \overline{1}, \overline{2}, ..., \overline{(n-1)}\right\}$,

las unidades son precisamente las clases $\overline{a}$ con $(a, n) = 1$, por lo tanto su número es $\varphi(n)$

Si $n$ es un entero positivo y $a$ un entero tal que $(a, n) = 1$, el orden de $a$ módulo $n$ de la definición anterior es precisamente el orden de $a$ considerado como elemento del grupo

$G_n$. Además un entero $a$ es una **raíz primitiva módulo** $n$ si y sólo si $a$ es un generador del grupo $G_n$. Por lo tanto solo existen raices primitivas módulo $n$ para aquellos enteros positivos $n$ tales que $G_n$ es un grupo cíclico.

# A.14.

**Teorema 40.** *Para un entero $n$, $\mathbb{Z}_n$ tiene raices primitivas si y sólo si $n$ es alguno de los números $2, 4, p^k$, o $2p^k$ con $p$ un primo impar.*

# A.15.

**Teorema 41.** *El polinomio ciclotómico $\phi_n(x)$ se factoriza módulo $q$ para todo primo $q$, excepto cuando $n = 1, 2, 4, p^k$ o $2p^k$ , donde $p$ es un primo impar y $k$ es un entero positivo, en tal caso $\phi_n(x)$ permanece irreducible módulo $q$ para infinitos primos $q$, mientras que se factoriza módulo $q$ si $n > 2$ para otros infinitos primos $q$.*

**Demostración:** Es importante tener en cuenta de la teoría de Galois que un polinomio irreducible sobre un campo finito debe tener un grupo cíclico de Galois. Recuérdese que el grupo de Galois de un polinomio $f(x) \in F[x]$ es el grupo $Aut_F K$, donde $K$ es un campo de descomposición de $f(x)$ sobre $F$ y una extensión finita de $F$. Es decir, el grupo de Galois de un polinomio es el grupo de automorfismos de las raices del polinomio que tambien se denota por $G(K/F)$ y se lee el grupo de Galois de $K$ sobre $F$, el grupo de todos los automorfismos de $K$, que dejan todo elemento de $F$ fijo y que si $K$ es una extensión finita de grado $n$ de un campo finito $F$ de $p^r$ elementos, entonces, $G(K/F)$ es cíclico de orden $n$ y está generado por $\sigma_{p^r}$ donde para $\alpha \in K$, $\alpha\sigma_{p^r} = \alpha^{p^r}$. Para $\phi_n(x)$, el grupo de Galois es isomorfo al grupo multiplicativo módulo $n$, pues si $F$ es una extensión ciclotómica de orden $n$ del campo $\mathbb{Q}$ de los racionales y $g_n(x)$ el $n - ésimo$ polinomio ciclotómico sobre $\mathbb{Q}$, entonces $Aut_{\mathbb{Q}} F$ es isomorfo al grupo multiplicativo de unidades en el anillo $\mathbb{Z}_n$, es decir es isomorfo al grupo formado por los enteros positivos menores que $n$ y primos relativos con $n$ bajo la multiplicación módulo $n$. Un resultado conocido dice

que este grupo, el grupo de las unidades del anillo $\mathbb{Z}_n$ que esta formado por todas las clases $\bar{a}$ donde $\bar{a} = \{x \in Z \mid x \equiv a(\mod n)\}$, tales que $(a, n) = 1$ y tiene orden $\varphi(n)$. y que generalmente se denota por $G_n$ es cíclico si y sólo si $n = 1, 2, 4, p^k$ o $2p^k$ con $p$ un primo impar y $k$ un entero positivo. En otros casos, como el grupo de Galois no es cíclico módulo $q$, $\phi_n(x)$ se factoriza módulo $q$ para todo primo $q$.

Puesto que $\phi_1(x) = x - 1$ y $\phi_2(x) = x + 1$ son polinomios lineales, ellos permanecen irreducibles módulo $q$ para todo $q$. Si $n = p^k$ o $2p^k$, con $p > 2$ y $k \geq 1$, entonces el grupo multiplicativo $(\mod n)$ es cíclico con $\varphi(p^k) = \varphi(2p^k) = (p-1)p^{k-1}$ elementos, de los cuales $\varphi(\varphi(n)) = \varphi(p-1)\varphi(p^{k-1}) \geq 1$ son raíces primitivas. Análogamente, con $n = 4$, $\varphi(n) = 2$, $\varphi(\varphi(n)) = 1$, es decir hay una raíz primitiva. Sea $g$ tal raíz primitiva. Por el teorema de Dirichlet sobre primos en progresiones aritméticas: "Si $a, b$ son enteros positivos y $(a, b) = 1$, entonces la progresión aritmética $an + b$, $n = 1, 2, 3, ...$ contiene infinitos primos", como $(g, n) = 1$, existen infinitos primos $q$ tales que $q \equiv g(\mod n)$, y módulo tal primo $\phi_n(x)$ permanece irreducible. Recíprocamente, para todo $h$ con $(h, n) = 1$ donde $h$ no es una raíz primitiva módulo $n$, existen también infinitos primos $q$ con $q \equiv h(\mod n)$, y módulo todo dicho primo $q$, $\phi_n(x)$ se factorizará.

# Apéndice B

## B.1.

**Definición 21.** *Sea $F$ un campo. $K$ un campo que contiene a $F$. Sea $\alpha \in K$. Supóngase que $\alpha$ es la raíz de algún polinomio distinto de cero $f(x)$ en $F[x]$. Entonces se dice que $\alpha$ es* ***algebraico sobre*** *$F$.*

## B.2.

**Proposición 8.** *Sea $\alpha \in K$ algebraico sobre $F$. Entonces existe un único polinomio mónico irreducible $p(x)$ en $F[x]$ con $\alpha$ como raíz, y todo polinomio $f(x)$ en $F[x]$ con $\alpha$ como raíz es un múltiplo de $p(x)$.*

*Se llama a $p(x)$ el* ***polinomio minimal de*** *$\alpha$ sobre $F$, porque este es un polinomio de grado mínimo en $F[x]$ que tiene $\alpha$ como raíz .*

**Demostración:** Como $\alpha$ es la raíz de algun polinomio distinto de cero con coeficientes en $F$, existe un polinomio mónico distinto de cero $p(x)$ de grado menor con $\alpha$ como raíz. Se muestra que $p(x)$ es irreducible.
Si $p(x) = a(x)b(x)$, donde $a(x)$ y $b(x)$ tienen grado menor al grado de $p(x)$, entonces $0 = p(\alpha) = a(\alpha)b(\alpha)$. Como $K$ es un campo, $a(\alpha) = 0$ o $b(\alpha) = 0$. Así $\alpha$ es una raíz de un polinomio de grado menor que el grado de $p(x)$, lo cual es una contradicción. Por lo tanto $p(x)$ es irreducible. Finalmente se supone que $f(x)$ es cualquier polinomio en $F[x]$ con $\alpha$ como raíz. Por el **teorema 2**,

$f(x) = p(x)q(x) + r(x)$ con $grad(r(x)) < grad(p(x))$ o $r(x) = 0$
Haciendo $x = \alpha$ se obtiene $0 = r(\alpha)$. Por la elección de $p(x)$, $r(x)$ debe ser el polinomio cero, y así $p(x)$ divide a $f(x)$.

**Ejemplo 43.** *Sea $F = \mathbb{R}$, $K = \mathbb{C}$, $\alpha \in \mathbb{C}$. Supongamos que $\alpha = a + bi$, $b \neq 0$. entonces el polinomio minimal de $\alpha$ es:*

$(x - \alpha)(x - \bar{\alpha}) = x^2 - 2ax + (a^2 + b^2)$

# B.3.

**Definición 22.** *Sea $E$ una extensión separable finita de un campo infinito $F$. Entonces, existe $\alpha \in E$ tal que $E = F(\alpha)$; dicho elemento $\alpha$ es un elemento primitivo.*

# B.4.

**Teorema 42.** *Sea $K$ el campo de descomposición de $f(x)$ en $F[x]$ y sea $p(x)$ un factor irreducible de $f(x)$ en $F[x]$. Si las raices de $p(x)$ son $\alpha_1, ..., \alpha_r$, entonces para cada $i$ existe un automorfismo $\sigma_i$ en $G(K/F)$ tal que $\sigma_i(\alpha_1) = \alpha_i$.*

# B.5.

**Teorema 43.** *Si $G$ es un grupo finito, entonces existe un campo de extensión de Galois con grupo de Galois isomorfo a $G$.*

# B.6.

**Teorema 44.** *Sea $n \neq 1$ un entero positivo. Entonces existe un polinomio entero mónico, irreducible de grado $n$ que es reducible módulo todo primo si y sólo si $n$ no es un primo.*

La demostración de este resultado depende del clásico Teorema de Frobenius Density:

**Lema 9.** *Sea $f(x)$ un polinomio irreducible de grado $n$ sobre el campo $\mathbb{Q}$ de los racionales, sea $N$ el campo de descomposición de $f(x)$ y sea $G = Gal(N \mid \mathbb{Q})$ que actua sobre el conjunto de las raíces de $f(x)$. Si $G$ contiene una permutación $\varphi$ la cual es el producto de ciclos disjuntos de longitud $n_1, ..., n_t$, entonces existe un conjunto infinito $P_\varphi$ de primos tales que para cualquier $p \in P_\varphi$ tenemos la siguiente descomposición de $f(x) \mod p$ :*

$f(x) \cong \prod_{i=1}^{t} f_i(x) \mod p$,

*donde todo $f_i$ es irreducible* $\mod p$ *y el grado de $f_i$ es $n_i$.*

El otro resultado que se requiere se debe a R. Dedekind:

**Lema 10.** *Sea la notación como en el lema 9, y sea $f(x)$ mónico. Sea $p$ un primo que no divide al discriminante de $N$. Si $f(x) \cong \prod_{i=1}^{t} f_i(x) \mod p$, donde los $f_i$ son irreducibles* $\mod p$, *entonces $G$ contiene por lo menos una permutación la cual es el producto de $t$ ciclos disjuntos de longitudes $n_1, ..., n_t$, donde $n_i$ es el grado de $f_i$.*

**Demostración del teorema B6:** Si el grado $n$ de $f(x)$ es un primo, entonces el grupo de Galois $G$ de $f(x)$ actúa transitivamente sobre el conjunto de las $n - raíces$ de $f(x)$, y así $G$ posee un elemento de orden $n$ que debe actuar cíclicamente sobre el conjunto de las raíces de $f(x)$,y el teorema se concluye del lema 9, el cual garantiza que existe un conjunto de primos $P_\varphi$ tal que para algún $p \in P_\varphi$ se tiene la siguiente descomposición de $f(x) \mod p$ :

$$f(x) \cong f(x) \mod p, \text{ donde } f(x) \text{ es irreducible} \mod p \text{ (solo hay un ciclo).}$$

Ahora sea $n$ compuesto. Para probar el resultado se asume que se tiene construido un grupo de permutaciones $(G, \Omega)$ soluble, transitivo de grado $n$ que no posee algún ciclo de longitud $n$. Por un resultado de Safarevic existe una extensión de Galois $(N \mid \mathbb{Q})$ con $Gal(N \mid \mathbb{Q}) \cong G$. Sea $U$ el estabilizador de alg ún punto en $\Omega$, es decir $U$ es el conjunto de automorfismos de $G$ que dejan fijo un punto de $\Omega$, y sea $F$ el campo fijo de $U$. Como $F$ es campo fijo de $U$ y $U \subseteq G$, entonces todos los elementos de $U$ dejan fijo a $\mathbb{Q}$. Esto es $\mathbb{Q} \subseteq F$ y $F$ es una extensión finita de $\mathbb{Q}$. Por eso se puede hablar del elemento primitivo $v$ de $F$ sobre $\mathbb{Q}$. Luego existe $v \in F$ talque $\mathbb{Q}(v) = F$; $v$ es un entero algebráico. Entonces $G$ actúa transitivamente sobre el conjunto $\Delta$ de todas las raices del polinomio

minimal $f(x)$ de $v$ sobre los racionales. Por otra parte las permutaciones de $G$ sobre $\Omega$ y $\Delta$ son similares y así no existe ningún $n-ciclo$ en $(G,\Delta)$ porque asi se construyó. Por el resultado de R. Dedekind citado anteriormente, $f(x)$ es reducible módulo todos los primos que no dividan al discriminante de $N$. Pero los primos restantes son ramificados y así $f(x)$ tiene un factor cuadrático [**13**].

Ahora se va a construir el grupo $G$. Primero asuma que $n$ no es potencia de un primo. Sea $n=p^{\alpha}m$ donde $m$ no es divisible por el primo $p$. Además, sea $\Omega=\{1,2,...n\}$ y sea:

$a_1=(1,2,...p^{\alpha})$, $a_2=(p^{\alpha}+1,p^{\alpha}+2,...,2p^{\alpha}),...,a_m=(p^{\alpha}(m-1)+1,...,n)$ y

$b=(1,p^{\alpha}+1,2p^{\alpha}+1,...,(m-1)p^{\alpha}+1)(2,p^{\alpha}+2,2p^{\alpha}+2,...)....$

Observe que $a_ia_j=a_ja_i$ para toda $i,j$ y $b^{-1}a_ib=a_{i+1}$, donde los índices son leídos mod $m$.

Sea $A$ el grupo generado por $a_1^{-1}a_2$, $a_2^{-1}a_3,...,a_m^{-1}a_1$ y sea $B=\langle b\rangle$. Entonces $A$ es abeliano y consiste de todos los elementos de la forma $a_1^{\alpha_1}...a_m^{\alpha_m}$ con : $\alpha_1+\alpha_2+...+\alpha_m\cong 0$ mod $p^{\alpha}$.

Por otro lado, $b^{-1}Ab=A$ y asi $A$ es un subgrupo normal de $G:=AB$ y $G/A$ es cíclico, es decir $G/A$ es generado por $\langle bA\rangle$, de modo que $G$ es soluble. Tambien se puede decir que $G$ actúa transitivamente sobre $\Omega$ como puede ser fácilmente verificado.

Ahora se prueba por contradicción que $G$ no contiene un ciclo de orden $n$.

Suponga que $G$ contiene un $n-ciclo$ $x$, asi que el orden de $x$ es igual a $n$. Sea $x=ay=ya$ donde el orden de $a$ es una potencia de $p$ y $p$ no divide al orden de $y$. Se entiende entonces que si $x$ es ciclo, $a$ y $y$ deben ser ciclos. Reemplazando $x$ por una potencia apropiada, asumimos que $y=b$ y asi $x=ab$ que tienen orden $n$. Esto implica que $a\in A$, es decir que:

$$a=a_1^{\alpha_1}...a_m^{\alpha_m}$$

Como $a$ y $b$ conmutan se tiene que:

$$a=b^{-1}ab=a_2^{\alpha_1}a_3^{\alpha_2}...a_1^{\alpha_m}$$

así que:
$$a=a_1^{\alpha_1}...a_m^{\alpha_m}=a_2^{\alpha_1}a_3^{\alpha_2}...a_1^{\alpha_m}$$
$$a_1^{(\alpha_1-\alpha_m)}a_2^{(\alpha_2-\alpha_1)}...a_m^{(\alpha_m-\alpha_{m-1})}\cong 1$$
$$(\alpha_1-\alpha_m)\cong 0 \mod p^{\alpha}\text{,entonces, } \alpha_1\cong\alpha_m \mod p^{\alpha}$$

$$(\alpha_2 - \alpha_1) \cong 0 \mod p^\alpha, \text{entonces, } \alpha_2 \cong \alpha_1 \mod p^\alpha$$

.

.

.

$$(\alpha_m - \alpha_{m-1}) \cong 0 \mod p^\alpha, \text{entonces, } \alpha_m \cong \alpha_{m-1} \mod p^\alpha$$

Luego, $\alpha_1 \cong \alpha_2 \cong ... \cong \alpha_m \cong 0 \mod p^\alpha \qquad (*)$

y como:

$\alpha_1 + \alpha_2 + ... + \alpha_m \cong 0 \mod p^\alpha$.

Podemos decir por $(*)$ que $\alpha_1 + \alpha_1 + ... + \alpha_1 \cong 0 \mod p^\alpha$ o mejor aún

$m\alpha_i \cong 0 \mod p^\alpha$.

Como $p$ no divide a $m$ se llega a que $\alpha_1 \cong \alpha_2 \cong ... \cong \alpha_m \cong 0 \mod p^\alpha$ lo que es equivalente con $a = 1$.

Pero entonces el orden de $x = b$ es igual a $m$, lo cual es una contradicción.

Si $n$ es una potencia de un primo, entonces existe un grupo no cíclico $G$ de orden $n$ y se puede hacer la representación regular de $G$ en si mismo. Esto completa la prueba del teorema.

# Bibliografía


[1 ] A.G. Kúrosch. Ecuaciones algebraicas de grados arbitrarios. Mir, 1983.

[2 ] Aijeh M. Cohen. Some Tapas of Computer Álgebra. Springer-Verlag, 1999.

[3 ] A.I.Kostrikin. Introducción al álgebra. Mir, 1983.

[4 ] Carlos A. Trujillo Solarte. Notas y Apuntes de clase.

[5 ] Hans Lausch and Wilfried Nobauer. Algebra of Polynomials. North-Holland, 1973.

[6 ] Henri Cohen. Graduate Text in Matehematics. Springer-Verlag, 1993.

[7 ] I.N. Herstein. Abstract Algebra. Macmillan , 1986.

[6 ] Iván Castro Chadid. Temas de teoría de cuerpos, teoría de anillos y números algebraicos. Universidad Nacional de Colombia, 1986.

[9 ] John.B. Fraleigh. Algebra abstracta. Addison-Wesley Iberoamericana, 1987.

[10 ] Lindsay Childs. A. Concrete Introduction to Higher Algebra. Springer- Verlag, 1979.

[11 ] Marco Fidel Suárez. Elementos de álgebra. Universidad del Valle, 1994.

[12 ] Rafael Jimenez, Enrique Gordillo, Gustavo Rubiano. Teoría de Números para Principiantes. Universidad Nacional de Colombia, 1999.

[13 ] R. Dedekind, Gesammelte Abhandlungen Vol. 1, Vieweg, Braunschweig, 1930, 351-396.

[14 ] Tom M. Apostol. Introducción a la teoría analítica de números. Reverté. 1980.

[15 ] Integer polynomials that are reducible modulo all primes. Rolf Brandl, Mathematisches Institut, Am Hubland 12, D-8700 Wûrzburg, West Germany.

[16 ] Cyclotomic Polynomials and Factorization Theorems. Solomon W. Golomb, this Monthly, 85 (1978) 734-737.

[17 ] Análisis Numérico. Richard L. Burden, J. Douglas Faires, 1998- 6 edición, International Thomson Editores.