Números Complejos y Polinomios

Javier Alfaro Pastor
Marcela González Peláez

Otoño de 2005

Contenido

Prólogo

Una parte importante de los cursos de Álgebra Superior y de Álgebra para Ingeniería en el ITAM es sin duda el estudio de los números complejos y el anillo de polinomios con coeficientes en un campo. Este material ha sido construido pensando en las necesidades de dichos cursos, considerando lo necesario que es su estudio como parte formativa e informativa dentro del currículo de los mismos, sin profundizar demasiado pero tocando los aspectos necesarios para la formación de un estudiante relacionado con las matemáticas.

Se da una serie de ejercicios en cada una de las secciones que componen estas notas y al final se encontrarán las soluciones de muchos de los ejercicios de cálculo y algunas sugerencias para hacer las demostraciones de los ejercicios que lo requieren. Recomendamos que el estudiante que vaya a hacer uso de este material lea la teoría que aparece aquí y la de otros libros relacionados con los temas e intente hacer la mayoría de los ejercicios en una primera instancia sin ver la sugerencia ya que puede haber muchos caminos que lo conduzcan a una buena demostración que no sea necesariamente la que se sugiere. Después puede ver la sugerencia ya sea para intentar otro camino o complementar las ideas que se le ocurran. De manera similar recomendamos que las soluciones de los ejercicios de cálculo simplemente se utilicen para contrastar resultados.

Cualquier sugerencia, corrección o comentario sobre este material será bienvenida y para ello ponemos nuestro correo electrónico a continuación.

Marcela González.
gonzap@itam.mx

Javier Alfaro.
alfaro@itam.mx

Capitulo 1
COMPLEJOS

Uno de los problemas relevantes que se encontraron los antiguos matemáticos, fue el de resolver ecuaciones de la forma $x^n = a$, donde $n \in \mathbb{N}$ y $a \in \mathbb{R}$. Si n es impar, la ecuación tiene exactamente una solución real y si n es par y a es positivo existen exactamente dos soluciones reales. Sin embargo, si n es par y a es negativo, la ecuación no tiene soluciones en $\mathbb{R}$, ya que ningún número real elevado a una potencia par es negativo. En particular la ecuación $x^2 = -1$ no tiene solución en los reales.

Es fácil convencerse de que resolviendo esta ecuación , se resuelven todas las de la forma $x^n = a$, donde n es par y a un número real negativo. Así, la idea de resolver tales ecuaciones plantea el problema de tener un sistema numérico que contenga a los reales, que sea también un campo y donde exista un número i que elevado al cuadrado sea -1. Dicho campo deberá contener a todos los elementos de la forma $a + bi$, con $a, b \in \mathbb{R}$, donde bi es el producto de b por i en dicho campo y la suma de a con bi es también la suma en ese campo.

1.1 LOS NÚMEROS COMPLEJOS COMO CAMPO

1.1.1 Operaciones en los complejos

Con base en lo dicho con anterioridad, el campo con las características descritas debe contener a los números de la forma $a + bi$, con $a, b \in \mathbb{R}$; así que consideraremos el conjunto $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}$ de tales expresiones y veremos que éste sirve a nuestros propósitos. Para esto analizaremos cómo deben ser las operaciones y cuándo dos expresiones de este tipo son iguales para que efectivamente $\mathbb{C}$ sea un campo considerando que $i^2 = -1$.

Observacion 1 *Si $a + bi, c + di \in \mathbb{C}$, entonces*

$$a + bi = c + di \text{ si y sólo si } a = c \text{ y } b = d.$$

Demostración:

$$\begin{aligned} & a + bi &=& \ c + di \\ \Rightarrow \quad & a - c &=& \ (d - b)\, i \\ \Rightarrow \quad & (a - c)^2 &=& \ (d - b)^2\, i^2 \\ \Rightarrow \quad & (a - c)^2 &=& \ -(d - b)^2 \end{aligned}$$

Como $(a - c)^2 \geq 0$ y $(d - b)^2 \geq 0$ se tiene que $(a - c)^2 = 0 = (d - b)^2$, esto es, $a - c = 0 = d - b$ y por lo tanto $a = c$ y $d = b$. ■

Definicion 1 *Una expresión de la forma $z = a + bi$ se llama **número complejo** y así llamamos al conjunto $\mathbb{C}$, el **conjunto de los números complejos.***

Además, si $a + bi \in \mathbb{C}$ y $c + di \in \mathbb{C}$, definimos

$$\begin{aligned}(a+bi)+(c+di) &= (a+c)+(b+d)\,i \\ (a+bi)\cdot(c+di) &= (ac-bd)+(ad+bc)\,i\end{aligned}$$

puesto que si $\mathbb{C}$ va a ser un campo, se debe tener

$$\begin{aligned}(a+bi)+(c+di) &= a+bi+c+di \\ &= a+c+bi+ci \\ &= (a+c)+(b+d)\,i\end{aligned}$$

$$\begin{aligned}(a+bi)\cdot(c+di) &= (a+bi)\,c+(a+bi)\,di \\ &= ac+bci+adi+bdi^2 \\ &= ac+bci+adi-bd \\ &= (ac-bd)+(ad+bc)\,i\end{aligned}$$

■

Definicion 2 *Si $z = a+bi \in \mathbb{C}$, entonces, a y b se llaman **la parte real** y **la parte imaginaria** de z, respectivamente, y los denotaremos como sigue:*

$$\mathrm{Re}\,(z) = a, \quad \mathrm{Im}\,(z) = b.$$

Por ejemplo, si $z = -3 + 4i$, entonces $\mathrm{Re}\,(z) = -3$ e $\mathrm{Im}\,(z) = 4$.

Con esta terminología y la observación anterior, dos números complejos son iguales si y sólo si tiene la misma parte real y la misma parte imaginaria.

Proposicion 1 *El conjunto $\mathbb{C}$ con las operaciones de suma y producto definidas es un anillo conmutativo con elemento unitario.*

Demostración:

Dejamos como ejercicio para el lector probar las propiedades asociativa y conmutativa de la suma y el producto, así como la propiedad distributiva.

Existencia del elemento neutro aditivo.- El complejo $0 = 0 + 0i$ es dicho elemento, ya que si $a + bi \in \mathbb{C}$, entonces $(a + bi) + (0 + 0i) = (a + 0) + (b + 0)\,i = a + bi$.

Existencia del inverso aditivo.- Sea $a + bi \in \mathbb{C}$, entonces $(-a) + (-b)\,i$ es un complejo y $(a + bi) + ((-a) + (-b)\,i) = (a + (-a)) + (b + (-b)\,i) = 0 + 0i$.

Existencia del elemento unitario.- El elemento $1 = 1 + 0i$ cumple con la propiedad de que si $a + bi \in \mathbb{C}$, entonces $(a + bi) \cdot (1 + 0i) = a + bi$.

Con esto, se tiene que $\mathbb{C}$ es un anillo conmutativo con uno. ■

Ahora veremos que todo elemento de $\mathbb{C}$ diferente de cero tiene inverso multiplicativo, esto es, que si $a+bi$ es un complejo tal que $a+bi \neq 0$, entonces existen $x, y \in \mathbb{R}$ tales que $(a+bi)\cdot(x+yi) = 1$.

Supongamos que $(a+bi)\cdot(x+yi) = 1$, entonces obtenemos que $(ax-by)+(ay+bx) = 1$, luego

$$\begin{aligned} ax - by &= 1 \\ ay + bx &= 0 \end{aligned}$$

Así, para encontrar x, y, necesitamos saber si el sistema anterior tiene solución.

Como el determinante del sistema

$$d = \begin{vmatrix} a & -b \\ b & a \end{vmatrix} = a^2 + b^2$$

es distinto de cero ya que $a+bi \neq 0 \Longrightarrow a \neq 0$ o $b \neq 0$, entonces el sistema tiene solución única que, por la regla de Cramer, sabemos está dada por

$$x = \frac{d_1}{d}, \qquad y = \frac{d_2}{d}$$

donde $d_1 = \begin{vmatrix} 1 & -b \\ 0 & a \end{vmatrix} = a$ y $d_2 = \begin{vmatrix} a & 1 \\ b & 0 \end{vmatrix} = -b$, es decir, $x = \dfrac{a}{a^2+b^2}$ y $y = \dfrac{-b}{a^2+b^2}$.

Con esto y la proposición 1 hemos probado la siguiente

Proposicion 2 *El conjunto $\mathbb{C}$ con la operaciones de suma y producto definidas es un campo.*

■

Ahora veremos que en los números complejos no es posible dar un orden que sea compatible con las operaciones de suma y producto, a diferencia del orden en los reales. Para esto damos la siguiente

Definicion 3 *Sea D un dominio entero* [1]. *Una **clase positiva** en D es un subconjunto P de D, cuyos elementos se llaman **positivos** y que satisfacen las siguientes leyes:*

1. *Cerradura respecta a la adición: Si $a, b \in P$, entonces $a+b \in P$.*
2. *Cerradura respecto a la multiplicación: Si $a, b \in P$, entonces $a \cdot b \in P$.*

[1] Un dominio entero es un anillo conmutativo con elemento unitario, en el que el producto de dos elementos distintos de cero es distinto de cero.

3. *Tricotomía: Si $a \in D$, entonces una y sólo una de las siguientes proposiciones se cumple: $a \in P$, $a = 0$ o $-a \in P$.*

Ejemplo 1 *En el conjunto de los números enteros la clase positiva es $\mathbb{N}$.*

Definicion 4 *Un **dominio entero** se dice que es **ordenado** si tiene una clase positiva.*

Proposicion 3 *En un dominio entero ordenado, todo cuadrado de un elemento distinto de cero es positivo.*

Demostración:
Sea D un dominio ordenado y $P \subset D$ una clase positiva. Si $a \in D$ es tal que $a \neq 0$, entonces $a \in P$ o $-a \in P$, de aquí que $a^2 = aa \in P$ o $a^2 = (-a)(-a) \in P$, esto es, $a^2 \in P$ en ambos casos. ■

Corolario 4 *Si D es un dominio entero ordenado, con clase positiva P, entonces $1 \in P$.*

En un dominio entero ordenado podemos definir la siguiente relación de orden:

Definicion 5 *Sea D un dominio entero ordenado con clase positiva P y sean $a, b \in D$. Decimos que a **es menor que** b $(a < b)$ o b **es mayor que** a $(b > a)$ si la diferencia $b - a \in P$.*

Proposicion 5 *Si D es un dominio entero ordenado con clase positiva P y $a, b, c \in D$, entonces*

a. $a < b \Longrightarrow a + c < b + c$.

b. $a < b$ *y* $c \in P \Longrightarrow a \cdot c < b \cdot c$.

c. *se cumple una y sólo una de las siguientes relaciones*
$a < b$ *o* $a = b$ *o* $b < a$ *(tricotomía).*

d. $a < b$ *y* $b < c \Longrightarrow a < c$.

Corolario 6 *Sea D un dominio entero ordenado y sean $a, b, c \in D$, entonces*

a. *se cumple una y sólo una de las siguientes relaciones* $a > 0$, $a = 0$ *o* $a < 0$.

b. $a < b$ *y* $c < 0 \Longrightarrow b \cdot c < a \cdot c$.

c. $a < 0$ *y* $b < 0 \Longrightarrow a \cdot b > 0$.

Los incisos a y b de la proposición anterior muestran que esta relación de orden es compatible con las operaciones.

Proposicion 7 $\mathbb{C}$ *no es un dominio ordenado.*

Demostración:
Si $\mathbb{C}$ fuera dominio ordenado tendría una relación de orden "$<$", con la que $-1 < 0$, por ser $1 = 1^2 > 0$. Por otro lado, por la proposición 3 los cuadrados de elementos distintos de cero deben ser mayores que cero y así, como $i \neq 0$ en $\mathbb{C}$, debería suceder que $i^2 > 0$; pero $i^2 = -1 < 0$, que nos llevaría a una contradicción de la tricotomía. ■

Ejercicios 1.1.1

1. Exprese los siguientes números complejos en la forma $a + bi$.
   a. $(2 + 3i) + (4 + i)$.
   b. $(2 + 3i) \cdot (4 + i)$.
   c. $\dfrac{(2 + 3i)}{(4 + i)}$.
   d. $(8 + 6i)^2$.
   e. $\dfrac{1}{i} + \dfrac{3}{i + 1}$.
   f. $\left(\dfrac{1}{i} + \dfrac{3}{i + 1}\right)^2$.
2. Encuentre los valores de x y y que satisfacen la igualdad $(1 + i) \cdot (x + y\, i) = 2 + i$.
   a. Mediante un par de ecuaciones simultáneas en x y y.
   b. Utilizando al inverso multiplicativo de $(1 + i)$.
3. Sean $z_1 = 1 + i,\ z_2 = -2 + i,\ z_3 = 1 - i$. Calcule lo que se indica:
   a. z_2^{-1}
   b. z_3^{-1}

c. $\dfrac{z_1}{z_2}$

d. $\dfrac{1}{z_2 z_3}$

e. $\dfrac{z_1 + z_2}{z_3}$

4. Demuestre que:
   a. $(\sqrt{2} - i) - i(1 - i\sqrt{2}) = -2i.$
   b. $\dfrac{1+2i}{3-4i} + \dfrac{2-i}{5i} = -\dfrac{2}{5}.$
   c. $(1-i)^4 = -4.$
5. Determine el valor de la suma $\sum_{k=0}^{n} i^k$, para todo $n \in \mathbb{N} \cup \{0\}$.
6. Encuentre números complejos $z = x + y\,i$ y $w = u + v\,i$ que satisfagan cada uno de los siguientes sistemas de ecuaciones:
   a. $\begin{aligned} z + i\,w &= 1 \\ i\,z + w &= 1 + i \end{aligned}$ b. $\begin{aligned} (1+i)\,z - i\,w &= 3 + i \\ (2+i)\,z + (2-i)\,w &= 2\,i \end{aligned}$
7. Termine la demostración de la proposición 1.
8. Pruebe la proposición 5.
9. Pruebe el corolario 6.
10. Sea D un dominio ordenado, pruebe que:
    a. $a < b \Longrightarrow a + c < b + c.$
    b. $a - x < a - y \Longrightarrow x > y.$
    c. Si $a < 0$, entonces $ax > ay \Longleftrightarrow x < y.$
    d. $x + x + x + x = 0 \Longrightarrow x = 0.$
11. Pruebe que si $a \in \mathbb{R}$, entonces la ecuación $x^2 = a$ siempre tiene solución en $\mathbb{C}$.

1.1.2 Solución de ecuaciones de 2° grado en $\mathbb{C}$

En esta parte veremos que toda ecuación de 2° grado con coeficientes complejos tiene solución en los complejos; para esto primero probaremos que todo número complejo tiene dos raíces cuadradas.

En el caso de los números reales sabemos que todo real positivo a tiene dos raíces cuadradas, una positiva y otra negativa, denotadas por $\sqrt{a}$ y $-\sqrt{a}$, respectivamente; el cero tiene una raíz cuadrada real, pero los números negativos no tienen raíces cuadradas, es decir, si $a \in \mathbb{R}$ y $a < 0$, no existe $b \in \mathbb{R}$ tal que $b^2 = a$.

Sin embargo, todo número complejo $z \neq 0$ tiene dos raíces cuadradas, denotadas por $\sqrt{z}$ y $-\sqrt{z}$ aunque en este caso no podemos hablar de positivos o negativos sino de un número y su inverso aditivo (si $z = 0$, entonces z tiene una única raíz cuadrada: 0).

Lo anterior podemos enunciarlo de la siguiente manera:

Proposicion 8 *La ecuación $x^2 = z$ siempre tiene solución en $\mathbb{C}$, y si $z \neq 0$ hay dos soluciones distintas.*

Demostración:

Si $z = 0$ es claro que $x = 0$ es la única solución.

Supongamos pues que $z = a + bi \neq 0$ y queremos encontrar $x = s + ti$ tal que $x^2 = z$, es decir, tal que $(s + ti)^2 = a + bi$, de aquí que, $s^2 - t^2 + 2sti = a + bi$, de donde

$$s^2 - t^2 = a \tag{1.1}$$

$$2st = b \tag{1.2}$$

Elevando ambas ecuaciones al cuadrado obtenemos $s^4 - 2s^2t^2 + t^4 = a^2$ y $4s^2t^2 = b^2$ y sumando miembro a miembro se tiene: $s^4 + 2s^2t^2 + t^4 = a^2 + b^2$, esto es, $\left(s^2 + t^2\right)^2 = a^2 + b^2$.

Como $a, b, s, t \in \mathbb{R}$, $s^2 + t^2 > 0$ y $a^2 + b^2 > 0$, podemos extraer raíz cuadrada y obtenemos

$$s^2 + t^2 = \sqrt{a^2 + b^2} \in \mathbb{R}$$

De (1.1), $s^2 = t^2 + a$ y sumando s^2 en ambos miembros: $2s^2 = s^2 + t^2 + a = \sqrt{a^2 + b^2} + a$, de donde $s^2 = \dfrac{\sqrt{a^2 + b^2} + a}{2} \geq 0$ y por lo tanto $s = \sqrt{\dfrac{\sqrt{a^2 + b^2} + a}{2}}$.

Análogamente, $t^2 = s^2 - a \geq 0 \implies 2t^2 = s^2 + t^2 - a = \sqrt{a^2 + b^2} - a \implies t^2 = \dfrac{\sqrt{a^2 + b^2} - a}{2} \geq 0 \implies t = \pm\sqrt{\dfrac{\sqrt{a^2 + b^2} - a}{2}}$. Podemos considerar las siguientes posibilidades para $s + ti$:

$$A_1 = \sqrt{\frac{\sqrt{a^2 + b^2} + a}{2}} + \sqrt{\frac{\sqrt{a^2 + b^2} - a}{2}}\, i$$

$$A_2 = \sqrt{\frac{\sqrt{a^2 + b^2} + a}{2}} - \sqrt{\frac{\sqrt{a^2 + b^2} - a}{2}}\, i$$

$$A_3 = -\sqrt{\frac{\sqrt{a^2+b^2}+a}{2}} + \sqrt{\frac{\sqrt{a^2+b^2}-a}{2}}\, i$$
$$A_4 = -\sqrt{\frac{\sqrt{a^2+b^2}+a}{2}} - \sqrt{\frac{\sqrt{a^2+b^2}-a}{2}}\, i$$

Por otra parte, de la ecuación 1.2, podemos deducir lo siguiente:

Si $b > 0$, entonces s y t deben tener el mismo signo, por lo que las soluciones serán A_1 y A_4; si $b < 0$, entonces s y t deben tener signo diferente, por lo que las soluciones serán A_2 y A_3.

Si $b = 0$, entonces $s = 0$ o $t = 0$; si $s = 0$, las soluciones son $\pm ti$ y si $t = 0$, entonces las soluciones son $\pm s$.

Por lo tanto la ecuación $x^2 = z$, $z \neq 0$, tiene exactamente dos soluciones en $\mathbb{C}$. ■

En particular, los números reales considerados como complejos cuya parte imaginaria es cero, tienen raíz cuadrada.

Si el número es positivo o cero, ya sabemos cómo son dichas raíces. Si el número es negativo, se expresa en la forma $a + 0i$ con $a < 0$, entonces $\sqrt{a^2+b^2} = \sqrt{a^2} = |a| = -a$, de aquí que

$$s = \pm\sqrt{\frac{\sqrt{a^2+b^2}+a}{2}} = \pm\sqrt{\frac{-a+a}{2}} = 0$$

y por lo tanto, las soluciones son $\pm ti$, es decir,

$$\sqrt{\frac{\sqrt{a^2}-a}{2}}\, i = \sqrt{\frac{-a-a}{2}}\, i = \sqrt{-a}\, i \quad y - \sqrt{-a}\, i.$$

Una notación que suele utilizarse para estos complejos es $\sqrt{a}$ y $-\sqrt{a}$, cuando se interpreta a i como $\sqrt{-1}$.

Las dos raíces cuadradas que se obtuvieron para un número complejo z distinto de cero difieren únicamente por el signo. Así que, como en el caso real, se denotarán estas raíces por $\sqrt{z}$ y $-\sqrt{z}$, donde

$$\sqrt{z} = \begin{cases} A_1 & \text{si} \quad \mathrm{Im}\,(z) \geq 0 \\ A_2 & \text{si} \quad \mathrm{Im}\,(z) < 0 \end{cases}$$

Se debe notar que $\sqrt{z^2}$ no siempre es igual a z, de hecho se puede ver que

$$\sqrt{z^2} = \begin{cases} z & \text{si} \quad \mathrm{Re}\,(z) > 0 \\ -z & \text{si} \quad \mathrm{Re}\,(z) < 0 \\ z & \text{si} \quad \mathrm{Re}\,(z) = 0 \text{ y } \mathrm{Im}\,(z) \geq 0 \\ -z & \text{si} \quad \mathrm{Re}\,(z) = 0 \text{ y } \mathrm{Im}\,(z) < 0 \end{cases}$$

Además se tiene la siguiente

Proposicion 9 *Si $z, w \in \mathbb{C}$, entonces*

a. $\sqrt{zw} = \pm\left(\sqrt{z}\sqrt{w}\right)$.

b. *si* $w \neq 0$, $\sqrt{\dfrac{z}{w}} = \pm\left(\dfrac{\sqrt{z}}{\sqrt{w}}\right)$.

Lo anterior nos servirá para demostrar que toda ecuación de la forma

$$ax^2 + bx + c = 0$$

con $a, b, c \in \mathbb{C},\ a \neq 0$, tiene solución en $\mathbb{C}$.

En efecto

$$ax^2 + bx + c = 0 \implies x^2 + \frac{b}{a}x = -\frac{c}{a} \implies x^2 + \frac{b}{a}x + \frac{b^2}{4a^2} = -\frac{c}{a} + \frac{b^2}{4a^2} \implies$$

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

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

Por lo tanto las soluciones de la ecuación $ax^2 + bx + c = 0$ son

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

Ejercicios 1.1.2

1. Obtenga las raíces cuadradas de
   a. $7 + 24i$.
   b. $\sqrt{i}$.
   c. $24 - 7i$.
   d. $1 + i$.
   e. i.
2. Pruebe la proposición 9.
3. Obtenga las soluciones de las siguientes ecuaciones:
   a. $x^2 + 2ix + 1 = 0$.

b. $(3+i)\,x^2+10x-(9+3i)=0$.

c. $-5x^2+\sqrt{2}x-1=0$.

4. Encuentra las soluciones de la ecuación $z^2-3iz=-1+3\,i$.

5. Simplifique lo siguiente:

a. $(1+\,i)^4$.

b. $(-\,i)^{-1}$.

c. $\sqrt{1+\sqrt{i}}$ (considere $\sqrt{i}=\frac{\sqrt{2}}{2}+\frac{\sqrt{2}}{2}i$ y sólo una raíz de $1+\sqrt{i}$).

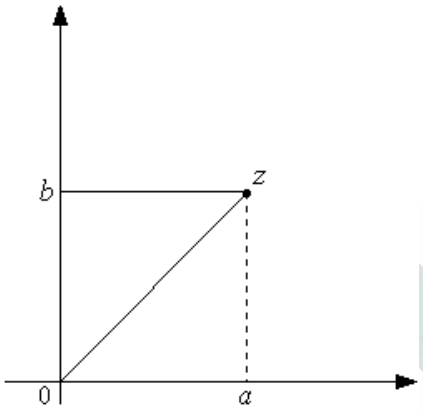
1.2 INTERPRETACIÓN GEOMÉTRICA DE LOS NÚMEROS COMPLEJOS

Como cada número complejo queda determinado por sus partes real e imaginaria, y dos números complejos son distintos si difieren en su parte real o en su parte imaginaria, a cada número complejo $a+bi$ lo podemos identificar con el punto (a,b) del plano cartesiano. Así, podemos considerar que los números están dispuestos en el plano, de tal forma que podemos denotar a cada punto (a,b) del plano, por el número complejo $a+bi$. A este plano lo llamaremos **el plano complejo**.

1.2.1 El plano complejo.

Los puntos del eje horizontal (antes eje de las abscisas) son de la forma $a+0i$ o $(a,0)$, y cada uno de éstos no es más que el número real a, por lo que a este eje lo llamaremos **eje real**. Análogamente los puntos de la forma $0+bi=bi$ se encuentra en el eje vertical (antes eje de las ordenadas) y son números puramente imaginarios, por lo que a este eje lo llamaremos el **eje imaginario**.

Si $z=a+bi$ es un número complejo, como se muestra en la figura, de abscisa a y ordenada al origen b, la magnitud del segmento de 0 a z es $\sqrt{a^2+b^2}$



Definicion 6 *Sea $z = a + bi$ un número complejo. El **valor absoluto o módulo de** z es su distancia al origen: $\sqrt{a^2 + b^2}$ y se denotará por $|z|$.*

Por ejemplo, $|3 + 4i| = 5; \quad |i| = 1, \quad |-6| = 6.$

Si $z = a + 0i$, entonces el módulo de z coincide con el valor absoluto de $\mathrm{Re}\,(z)$, es decir, $|z| = \sqrt{a^2} = |a|$.

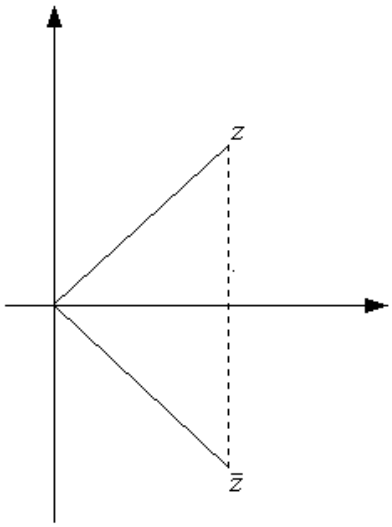
Proposicion 10 *Si z y w son números complejos, entonces*

1. $|z| \geq 0$ *y* $|z| = 0$ *si y sólo si* $z = 0$.
2. $|-z| = |z|\,.$
3. $|z \cdot w| = |z|\,|w|\,.$
4. *Si* $w \neq 0$, *entonces* $\left|\dfrac{z}{w}\right| = \dfrac{|z|}{|w|}$.
5. $|\mathrm{Re}\,(z)| \leq |z|, \quad |\mathrm{Im}\,(z)| \leq |z|$ [1].

La demostración de la proposición anterior queda como ejercicio para el lector. ■

Definicion 7 *Sea $z = a + bi$ un número complejo, **el conjugado** de z es el número complejo $a + (-b)\,i = a - bi$, denotado por $\overline{z}$.*

[1] $|Re\,(z)|$ y $|\mathrm{Im}\,(z)|$ denotan el valor absoluto de la parte real y el valor absoluto de la parte imaginaria, respectivamente.



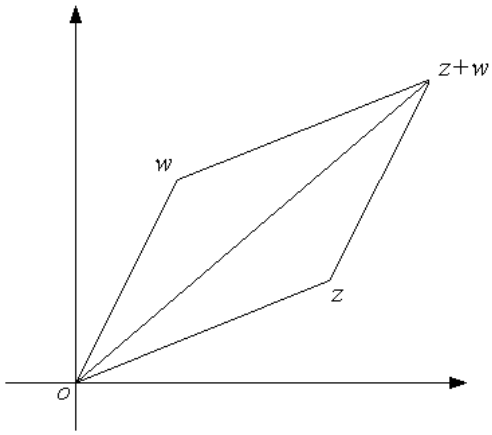
El conjugado $\overline{z}$ de un número complejo z es el simétrico de z respecto al eje real. También se dice que $\overline{z}$ es la reflexión sobre el eje real.

Proposicion 11 *Si z y w son números complejos, entonces*

1. $\overline{z+w} = \overline{z} + \overline{w}$.
2. $\overline{(-z)} = -(\overline{z})$.
3. $\overline{z \cdot w} = \overline{z} \cdot \overline{w}$.
4. *Si $w \neq 0$, entonces* $\overline{\left(\frac{z}{w}\right)} = \frac{\overline{z}}{\overline{w}}$.
5. $\overline{\overline{z}} = z$.
6. $\mathrm{Re}(z) = \frac{z+\overline{z}}{2}$, $\mathrm{Im}(z) = \frac{z-\overline{z}}{2i}$.

La demostración queda como ejercicio para el lector. ■

Una interpretación geométrica para la suma de números complejos es la siguiente:
Si $z = a + bi$ y $w = c + di$ son dos números complejos, los puntos $o, z, w, z + w$ de coordenadas $(0,0)$, (a,b), (c,d) y $(a+c, b+d)$ forman un paralelogramo.



Para demostrar lo anterior sólo tenemos que demostrar que las diagonales del cuadrilátero $o, z, w, z+w$ se intersectan en su punto medio, lo cual es muy simple ya que el punto medio del segmento de z a w y el de o a $z+w$ es en ambos casos $\left(\frac{a+c}{2}, \frac{b+d}{2}\right)$.

De la interpretación geométrica dada para la suma de dos números complejos podemos deducir una propiedad importante: "el módulo de la suma de dos números complejos es menor o igual que la suma de los módulos de dichos complejos", o sea que

$$|z+w| \leq |z| + |w| . \tag{1.3}$$

Ejercicios 1.2.1

1. Diga en qué casos se cumple la igualdad en (1.3).
2. Diga qué hecho geométrico se utiliza para deducir la desigualdad en (1.3).

Proposicion 12 *Si z y w son números complejos, entonces*

1. $z\overline{z} = |z|^2$.
2. $|\overline{z}| = |z|$.
3. $|z+w| \leq |z| + |w|$.

Demostración:

Probaremos únicamente el inciso c y los demás quedan como ejercicio para el lector. En esta demostración usaremos los incisos a y b de esta proposición, así como los incisos a, e, f de la proposición 11 y e de la 10

$$\begin{aligned}
|z+w|^2 &= (z+w)\left(\overline{z+w}\right) = (z+w)\left(\overline{z}+\overline{w}\right) \\
&= z\cdot\overline{z} + z\cdot\overline{w} + \overline{z}\cdot w + w\cdot\overline{w} \\
&= |z|^2 + (z\cdot\overline{w}) + \left(\overline{z\cdot\overline{w}}\right) + |w|^2 \\
&= |z|^2 + 2\,\mathrm{Re}\,(z\cdot\overline{w}) + |w|^2 \\
&\leq |z|^2 + 2\,|\mathrm{Re}\,(z\cdot\overline{w})| + |w|^2 \\
&\leq |z|^2 + 2\,|z\cdot\overline{w}| + |w|^2 \\
&= |z|^2 + 2\,|z|\,|\overline{w}| + |w|^2 \\
&= |z|^2 + 2\,|z|\,|w| + |w|^2 = (|z|+|w|)^2 .
\end{aligned}$$

$\Longrightarrow |z+w|^2 \leq (|z|+|w|)^2 \quad \Longrightarrow \quad |z+w| \leq |z|+|w|$, sacando raíz cuadrada del primero y último miembros de esta desigualdad. ■

Observacion 2 *Si $z, w \in \mathbb{C}$ y $w \neq 0$, entonces*

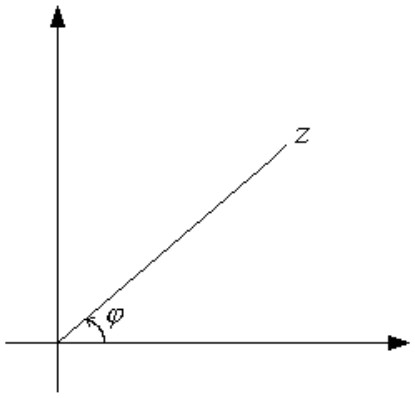
$$\frac{z}{w} = \frac{z\cdot\overline{w}}{w\cdot\overline{w}} = \frac{z\cdot\overline{w}}{|w|^2}.$$

Ejemplo 2 *El cociente de los complejos, $z = 1+i$ y $w = i$ es*

$$\frac{z}{w} = \frac{z\overline{w}}{|w|^2} = \frac{(1+i)(-i)}{|i|^2} = \frac{1-i}{1} = 1-i.$$

Definicion 8 *Sea z un número complejo distinto de cero. El **argumento** de z es el ángulo de lado inicial el semieje real positivo y lado final el segmento de 0 a z, y se denota $Arg\,(z) = \varphi$.* [2]

[2] Recuerde que los ángulos positivos se miden en el sentido contrario de las manecillas de un reloj.

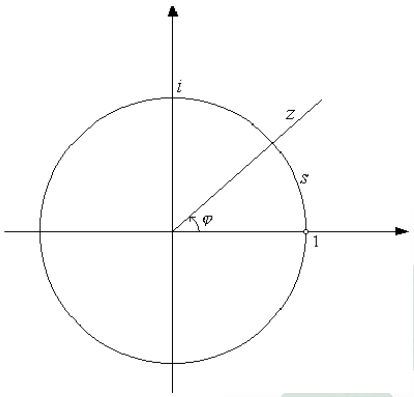


Si al ángulo φ le sumamos 2π o un múltiplo entero de 2π la posición gráfica del segmento de 0 a z no cambia, es decir, el argumento de z no es univaluado ya que los ángulos $\varphi + 2\pi k$ con $k = ... - 2, -1, 0, 1, 2, ...$ representan gráficamente el mismo ángulo. Para volverlo univaluado acordamos escribir al argumento como un número entre 0 y 2π. Así pues, si z y w son números complejos tales que $|z| = |w|$ y $Arg\,(z) = Arg\,(w) + 2\pi k$ con $k \in \mathbb{Z}$, entonces $z = w$. Para tener una única representación de un complejo en términos de su módulo y argumento convenimos en que éste será mayor o igual a cero y menor que 2π.

Si fijamos $r > 0$, sólo existen dos números reales, r y $-r$, con valor absoluto r; pero hay una infinidad de números complejos cuyo módulo es r; éstos forman geométricamente una circunferencia con centro en 0 y radio r. Mientras que los números reales r y $-r$ se distinguen por el signo, los puntos de la circunferencia se distinguen uno del otro por su argumento. El número complejo 0 es el único complejo que no tiene argumento ya que su módulo es cero. Los números reales positivos corresponden a los puntos del semieje real positivo o sea los puntos cuyo argumento es de la forma $\varphi = 2\pi k$, con $k \in \mathbb{Z}$. Los números reales negativos son los complejos de argumento de la forma $\pi + 2\pi k$ con $k \in \mathbb{Z}$. Los números imaginarios $z = bi$ son los complejos de argumento $\dfrac{\pi}{2} + 2\pi k$ si $b > 0$, y $\left(-\dfrac{\pi}{2}\right) + 2\pi k$ si $b < 0$, con $k \in \mathbb{Z}$.

Mientras que el argumento en radianes de un número complejo lo podemos dar entre 0 y 2π, el mismo argumento en grados lo podemos dar entre $0°$ y $360°$.

Veamos la relación que hay entre la medida en grados de un ángulo formado por dos rayos con vértice en el origen y la longitud de arco que éstos determinan sobre la circunferencia unitaria con centro en el origen.



La longitud de la circunferencia de radio 1 es 2π, por lo tanto la longitud de un arco sobre ésta, correspondiente a un ángulo de un grado, es $\dfrac{2\pi}{360}$. Luego, si el argumento de un complejo medido en grados es φ y la longitud del arco correspondiente es s, la relación entre φ y s será

$$s = \varphi \cdot \frac{2\pi}{360} \quad \text{o bien} \quad \varphi = s \cdot \frac{360}{2\pi}$$

Ejemplo 3 *Si el argumento de un complejo z es de $60°$, su argumento en radianes es $\frac{2\pi}{6} = \frac{\pi}{3}$.*

Si el argumento de z es de $\frac{5\pi}{4}$ radianes, entonces su argumento en grados es de $225°$.

En lo sucesivo expresaremos el argumento de un número complejo en grados o radianes indistintamente.

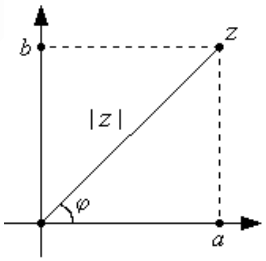
Ejercicios 1.2.2

1. Demuestre la proposición 10.
2. ¿Cuál es la posición relativa de los puntos $z = a + bi$ y $w = b + ai$.
3. ¿Qué representa geométricamente cada una de las proposiciones siguientes?
   a. $|z| = 1$.
   b. $|z| < 1$.
   c. $|z| > 1$.
4. Demuestre la proposición 11.
5. Demuestre los incisos 1. y 2. de la proposición 12.
6. Pruebe que si z y w son números complejos, entonces $|z - w| \geq ||z| - |w||$.

7. Si z y w son números complejos tales que $z\bar{w} \neq 1$, y $|z| = 1$ o $|w| = 1$, pruebe que $\left|\dfrac{z-w}{1-\bar{z}w}\right| = 1$.
8. Describe geométricamente los siguientes conjuntos:
   a. $\{z \in \mathbb{C} \mid Im\,(z-3) = 0\}$.
   b. $\{z \in \mathbb{C} \mid Im(z) \leq 1\}$.
   c. $\{z \in \mathbb{C} \mid Im\,(i\,z) = 1\}$.
   d. $\{z \in \mathbb{C} \mid |z-1| > 1\}$.
   e. $\left\{z \in \mathbb{C} \mid |z^2| = 4\right\}$.
9. En cada uno de los siguientes incisos, determina el lugar geométrico de los puntos z que cumplen:
   a. $|z-1| = 3$
   b. $|z-1| > 3$
   c. $|z-1| < 3$
   d. $\left|\dfrac{z-3}{z+3}\right| = 2$
   e. $|z-4i| + |z+4i| = 10$
   f. $|z-1| = |z+i|$.

1.2.2 Representación polar.

A partir de la interpretación de un número complejo como un punto en el plano, podemos representar a estos números en una forma distinta, Sea $z = a + bi$ un número complejo cuyo módulo es distinto de cero y su argumento es φ, como se muestra en la figura.



De la figura anterior tenemos que $a = |z|\cos\varphi$, $b = |z|\, sen\varphi$; con esto, el número z queda expresado como $z = |z|\cos\varphi + (|z|\, sen\varphi)\ i$, o bien

$$z = |z|\,(\cos\varphi + isen\varphi) \tag{1.4}$$

Definición. Llamaremos a la expresión (1.4), la **representación polar trigonométrica del complejo z**.

Así, en la representación $z = r\,(\cos\varphi + isen\varphi)$ se entenderá que r es el módulo y φ el argumento de z. Además, puede pasarse de una representación a otra, esto es, si un complejo se expresa como en (1.4), se puede escribir la forma $a + bi$ haciendo $a = |z|\cos\varphi$ y $b = |z|\, sen\varphi$ y recíprocamente, conociendo a a y b se determinan $|z|$ y φ como sigue: $|z| = \sqrt{a^2 + b^2}$ y φ es el ángulo cuyo coseno es $\dfrac{a}{|z|}$ y cuyo seno es $\dfrac{b}{|z|}$, una forma rápida de calcular φ es encontrar el ángulo cuya tangente es $\dfrac{b}{a}$, cuando $a \neq 0$ y luego determinar φ analizando en qué cuadrante está el punto z.

Por ejemplo, si $z = -5 + 5i$, tenemos $a = -5$ y $b = 5$, luego $|z| = \sqrt{(-5)^2 + 5^2} = \sqrt{50} = 5\sqrt{2}$ y $\tan(\varphi) = -1$, de aquí que $\varphi = \dfrac{\pi}{2} + \dfrac{\pi}{4} = \dfrac{3\pi}{4}$ o $\varphi = 2\pi - \dfrac{\pi}{4} = \dfrac{7\pi}{4}$. Como z está en el segundo cuadrante resulta que $\varphi = \dfrac{3\pi}{4}$, luego $z = 5\sqrt{2}\left(\cos\dfrac{3\pi}{4} + i\ sen\ \dfrac{3\pi}{4}\right)$.

En muchas ocasiones en conveniente escribir a $\cos(\alpha) + isen(\alpha) = e^{i\alpha}$, con esta notación podemos escribir a cualquier número complejo z de la forma $z = re^{i\theta}$ donde $r = |z|$ y $\arg(z) = \theta$.. La expresión

$$e^{i\alpha} = \cos(\alpha) + i\ sen\,(\alpha) \tag{1.5}$$

se le conoce como fórmula de Euler.

Proposicion 13 *Sean z y w dos números complejos expresados en forma polar $z = |z|\,(\cos\varphi + isen\,\varphi)$, $w = |w|\,(\cos\theta + isen\,\theta)$, donde $Arg\,(z) = \varphi$ y $Arg\,(w) = \theta$. Entonces $zw = |z|\cdot|w|\,(\cos(\varphi + \theta) + i\ sen\,(\varphi + \theta))$, es decir, el módulo del producto de dos números complejos es el producto de los módulos y el argumento es la suma de los argumentos, o sea $|z\cdot w| = |z|\,|w|$ y $Arg\,(z\cdot w) = Arg\,(z) + Arg\,(w)$.*

Demostración:

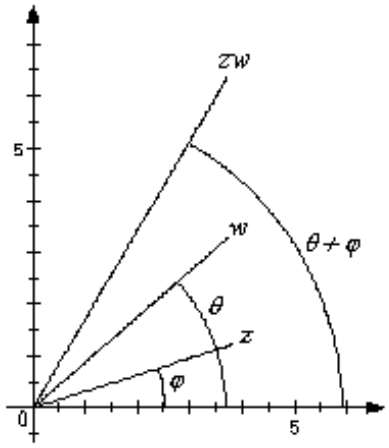
El producto de los dos números z y w es

$$z\cdot w = |z|\,|w|\,((\cos\varphi\cos\theta\ - sen\ \varphi sen\theta) + i\,(sen\ \varphi\cos\theta + \cos\varphi\ sen\theta)) \tag{1.6}$$

y a partir de las siguientes identidades trigonométricas para la suma de ángulos

$$\begin{aligned} \cos(\varphi + \theta) &= \cos\varphi\cos\theta - sen\ \varphi\ sen\ \theta \\ sen\,(\varphi + \theta) &= sen\ \varphi\cos\theta + \cos\varphi\ sen\ \varphi, \end{aligned}$$

obtenemos que el producto de z y w es $zw = |z| \cdot |w| (\cos(\varphi + \theta) + i\ sen(\varphi + \theta))$. Por la proposición (10), sabemos que $|z \cdot w| = |z|\,|w|$ de aquí que ésta es la representación polar del complejo $z \cdot w$ y $Arg(z \cdot w) = Arg(z) + Arg(w)$. ■



Vemos que la multiplicación de números complejos está relacionada con las rotaciones del plano. Esto es, si consideramos al segmento que une el origen con el punto z, la longitud de éste será $|z|$ y si w es un punto tal que $|w| = 1$, entonces al multiplicar z por w el vector z gira un ángulo igual a $\theta = Arg(w)$. Si $|w| \neq 1$, la longitud del vector ha de ser multiplicada por $|w|$ una vez efectuada la rotación. Por ejemplo, al multiplicar por

$w_1 = i$	se hace un giro de $90°$ en el sentido opuesto a las manecillas del reloj,
$w_2 = -i$	se hace un giro de $90°$ en el sentido de las manecillas del reloj,
$w_3 = 1 + i$	se hace un giro de $45°$ en el sentido opuesto a las manecillas del reloj, y el módulo del vector se multiplica por $\sqrt{2}$,
$w_4 = 1 - i$	se hace un giro de $45°$ en el sentido de las manecillas del reloj, y el módulo del vector se multiplica por $\sqrt{2}$.

Corolario 14 *Si* $z = |z| (\cos(\varphi) + i\ sen(\varphi))$, $w = |w| (\cos(\theta) + i\ sen(\theta))$, $w \neq 0$, *entonces* $\dfrac{z}{w} = \left|\dfrac{z}{w}\right| (\cos(\varphi - \theta) + i\ sen(\varphi - \theta))$, *es decir, al dividir dos complejos los módulos se dividen y los argumentos se restan.*

Demostración:

Supongamos que $\dfrac{z}{w} = v = |v| (\cos\psi + i\ sen\ \psi)$. Entonces debemos tener que $z = w \cdot v$. Por la proposición (13) $w \cdot v$ tiene como módulo $|w| \cdot |v|$ y como argumento

$\theta + \psi$. Luego $|w|\,|v| = |z|$ y $\theta + \psi = \varphi + (360°k)$ con $k \in \mathbb{Z}$, o sea $|v| = \left|\frac{z}{w}\right|$ y $\psi = \varphi - \theta + (360°)\,k$, con $k \in \mathbb{Z}$. Por lo tanto $\frac{z}{w} = \left|\frac{z}{w}\right| (\cos(\varphi - \theta) + i\ sen(\varphi - \theta))$. ■

De aquí se concluye el siguiente

Corolario 15 *Si* $z = |z| (\cos\varphi + i\ sen\ \varphi)$ *y* $z \neq 0$, *entonces*

$$z^{-1} = |z|^{-1} (\cos(-\varphi) + i\ sen(-\varphi)).$$

■

Ejercicios 1.2.3

1. Encuentre el argumento de los siguientes números:
   a. 5.
   b. $-i$.
   c. $-1 - i$.
   d. $1 + 3i$.
   e. $\frac{-2}{1+i\sqrt{3}}$.
   f. $\left(\sqrt{3} - i\right)^6$.
2. Represente en forma polar los siguientes números complejos.
   a. -4.
   b. $-6i$.
   c. $\frac{1}{2} - \frac{\sqrt{3}}{2}i$.
   d. $\sqrt{3} - i$.
   e. $1 + \cos\alpha + i\,sen\,\alpha$.
   f. i.
   g. $-2 - i$.
   h. $-\frac{1}{2} + \frac{\sqrt{3}}{2}i$.
3. Demuestre el corolario 15.
4. Aplica la forma polar para demostrar que $i\left(1 - i\sqrt{3}\right)\left(\sqrt{3} + i\right) = 2 + i2\sqrt{3}$.

5. Sean $z_1 = -\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2},\ z_2 = -\frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}$. Encuentra el producto $z_1 z_2$ utilizando el método gráfico.

1.3 RAÍCES N-ÉSIMAS DE NÚMEROS COMPLEJOS

Sean $z = \cos\theta + i\ sen\ \theta$ y $w = \cos\varphi\ + i\ sen\ \varphi$. Un caso particular del producto de los complejos, z y w, es cuando ambos son iguales; en este caso, la expresión

$$zw = |z| \cdot |w| \left(\cos\left(\theta + \varphi\right) + i\ sen\left(\theta + \varphi\right)\right)$$

se puede escribir como

$$z^2 = |z|^2 \left(\cos\left(2\theta\right) + i\ sen\left(2\theta\right)\right).$$

1.3.1 Fórmula de De Moivre

El resultado anterior puede ser generalizado por inducción como sigue:

Proposicion 16 *Si* $z = |z|\left(\cos\theta + isen\ \theta\right)$, *entonces* $z^n = |z|^n \left(\cos n\theta + i\ sen\ n\theta\right)$, *para toda* $n \in \mathbb{N}$.

Demostración:

Si $n = 1, \quad z = |z|\left(\cos\left(\theta\right) + i\ sen\left(\theta\right)\right)$, y por lo tanto

$$z^1 = |z|^1 \left(\cos\left(1\theta\right) + i\ sen\left(1\theta\right)\right).$$

Se supone válida la expresión cuando $n = k,$ con $k \geq 1$, es decir,

$$z^k = |z|^k \left(\cos\left(k\theta\right) + i\ sen\left(k\theta\right)\right)$$

Veamos para z^{k+1} :

$z^{k+1} = z^k z^1 = \left(|z|^k \left(\cos\left(k\theta\right) + i\ sen\left(k\theta\right)\right)\right)\left(|z|\left(\cos\left(\theta\right) + i\ sen\left(\theta\right)\right)\right)$

$= |z|^k |z| \left(\cos\left(k\theta + \theta\right) + i\ sen\left(k\theta + \theta\right)\right) = |z|^{k+1} \left(\cos\left(\left(k+1\right)\theta\right) + i\ sen\left(\left(k+1\right)\theta\right)\right).$

Luego, por el Principio de Inducción $z^n = |z|^n \left(\cos\left(n\theta\right) + i\ sen\left(n\theta\right)\right)$, para todo $n \in \mathbb{N}$.

Al sustituir z por $|z|\left(\cos\left(\theta\right) + i\ sen\left(\theta\right)\right)$, obtenemos

$$\left[|z|\left(\cos\left(\theta\right) + i\ sen\left(\theta\right)\right)\right]^n = |z|^n \left(\cos\left(n\theta\right) + i\ sen\left(n\theta\right)\right) \tag{1.7}$$

que es llamada la fórmula de De Moivre en honor a Abraham De Moivre. ■

En particular, si $|z| = 1$ obtenemos

$$(\cos(\theta) + i\ sen(\theta))^n = (\cos(n\theta) + i\ sen(n\theta)), \tag{1.8}$$

para toda $n \in \mathbb{N}$, que podemos generalizar como sigue:

Proposicion 17 *Teorema de De Moivre. Para todo* $n \in \mathbb{Z}$.

$$(\cos(\theta) + i\ sen(\theta))^n = (\cos(n\theta) + i\ sen(n\theta)),$$

Demostración:

Nos falta probar la proposición para los negativos y cero. A continuación demostremos que

$$(\cos(\theta) + i\ sen(\theta))^{-n} = (\cos(-n\theta) + i\ sen(-n\theta)),$$

para toda $n \in \mathbb{N}$.

Si $z = (\cos(\theta) + i\ sen(\theta))$ es un complejo de módulo 1, entonces por el corolario 15 tenemos

$$(\cos(\theta) + i\ sen(\theta))^{-1} = \cos(-\theta) + i\ sen(-\theta)$$

luego $z^{-n} = \left(z^{-1}\right)^n = [\cos(-\theta) + i\ sen(-\theta)]^n = \cos(-n\theta) + i\ sen(-n\theta)$.

Hemos demostrado el Teorema de De Moivre para exponentes negativos. Falta ver que es valido para $n = 0$. Como $(\cos(\theta) + i\ sen(\theta))^0 = 1$ y

$$1 = \cos(0) + i\ sen(0) = \cos(0 \cdot \theta) + i\ sen(0 \cdot \theta),$$

se tiene este caso.

Por lo tanto, el teorema de De Moivre es válido para todo exponente entero. ■

Una aplicación útil del teorema de De Moivre es cuando se usa como artificio para obtener fórmulas trigonométricas de múltiplos de ángulos.

Ejemplo 4 *Encontrar* $sen\ 5\theta$ *y* $\cos 5\theta$.

Haciendo $n = 5$ *en (1.8) resulta* $(\cos\theta + i\ sen\ \theta)^5 = \cos 5\theta + i\ sen\ 5\theta$.

Por otra parte, por el Teorema del Binomio obtenemos,

$$\begin{aligned}(\cos(\theta) + i\ sen(\theta))^5 &= \cos^5\theta + 5\cos^4\theta\,(i\ sen\ \theta) + 10\cos^3\theta\,(i\ sen\ \theta)^2 + \\ &\quad + 10\cos^2\theta\,(i\ sen\ \theta)^3 + 5\cos^1\theta\,(i\ sen\ \theta)^4 + (i\ sen\ \theta)^5,\end{aligned}$$

y recordando que para $n \in \mathbb{N} \cup \{0\}$: $i^{4n-1} = 1$, $i^{4n+1} = i$, $i^{4n+2} = -1$, $i^{4n+3} = -i$, *obtenemos:*

$\cos^5 + 5i\cos^4\theta sen\ \theta - 10\cos^3\theta sen^2\ \theta - 10i\cos^2\theta sen^3\theta + 5\cos\theta sen^4\theta + isen^5\theta =$

$= \left(\cos^5 - 10\cos^3\theta sen^2\ \theta + 5\cos\theta sen^4\theta + sen^5\theta\right) + \left(5\cos^4\theta sen\ \theta - 10\cos^2\theta sen^3\theta + sen^5\theta\right) i$

$= \cos 5\theta + isen\ 5\theta.$

Como dos complejos son iguales si y sólo si sus partes reales son iguales y sus partes imaginarias también lo son, obtenemos:

$$\begin{aligned} sen\ 5\theta &= 5\cos^4\theta sen\ \theta - 10\cos^2\theta sen^3\theta + sen^5\theta \\ \cos 5\theta &= \cos^5 -10\cos^3\theta sen^2\ \theta + 5\cos\theta sen^4\theta + sen^5\theta \end{aligned}$$

1.3.2 Raíces n-ésimas de un número complejo

Recordemos que en los reales una raíz n-ésima de a, donde $n \in \mathbb{N}$, es un número real b tal que la n-ésima potencia de b es igual a a. Por ejemplo, 3 es una raíz cuarta de 81 puesto que 3^4 es igual a 81. De manera similar, en los complejos, una raíz n-ésima de z es un complejo w tal que la n-ésima potencia de w es igual a z, lo cual se expresa como

$$\sqrt[n]{z} = w \Longleftrightarrow w^n = z$$

Definicion 9 *Si z y w son números complejos y $n \in \mathbb{N}$, diremos que w es una **raíz n-ésima de** z si $w^n = z$.*

Si z es un complejo distinto de cero, $\sqrt[n]{|z|}$ denota la raíz n-ésima real positiva de $|z|$ y $\sqrt[n]{z}$ denota una raíz n-ésima de z.

Como $\left(\dfrac{\sqrt[n]{z}}{\sqrt[n]{|z|}}\right)^n = \dfrac{z}{|z|}$, $\dfrac{\sqrt[n]{z}}{\sqrt[n]{|z|}}$ es una raíz n-ésima de $\dfrac{z}{|z|}$, entonces

$$\sqrt[n]{z} = \sqrt[n]{|z|}\left(\frac{\sqrt[n]{z}}{\sqrt[n]{|z|}}\right) = \sqrt[n]{|z|}\left(\sqrt[n]{\frac{z}{|z|}}\right),$$

es decir, cada raíz n-ésima de z es de la forma $\sqrt[n]{|z|}\left(\sqrt[n]{\dfrac{z}{|z|}}\right)$. Entonces el problema de encontrar las raíces n-ésimas de z se reduce a encontrar las raíces n-ésimas de $\dfrac{z}{|z|}$, que es un complejo de módulo uno.

Proposicion 18 *Dado $z = \cos\theta + i\ sen\ \theta$, existen exactamente n números complejos distintos que son raíces n-ésimas de z. Estas raíces están dadas por la fórmula*

$$\cos\left(\frac{\theta + 2\pi k}{n}\right) + i\ sen\left(\frac{\theta + 2\pi k}{n}\right),$$

con $k = 0, 1, ..., n-1$.

Demostración:

Usaremos la notación $\sqrt[n]{z} = z^{\frac{1}{n}}$, y entonces si $z = \cos\theta + i\ sen\ \theta$ y $w = \cos\psi + i\ sen\ \psi$ son tales que $z^{\frac{1}{n}} = w$, tenemos que

$$(\cos\ \theta + i\, sen\, \theta)^{\frac{1}{n}} = \cos\ \psi + i\ sen\, \psi; \tag{1.9}$$

luego,

$$(\cos\ \psi + i\ sen\, \psi)^n = \cos\ \theta + i\, sen\, \theta,$$

y usando el Teorema de De Moivre se tiene

$$\cos\ n\psi + i\ sen\, n\psi = \cos\ \theta + i\, sen\, \theta.$$

Por la definición de igualdad de complejos se tiene

$$\begin{aligned} \cos\theta &= \cos n\psi, \\ sen\ \theta &= sen\ n\psi. \end{aligned}$$

Por lo tanto

$$\begin{aligned} n\psi &= \theta + 2\pi k, \quad \text{para alguna } k \in \mathbb{Z}, \quad \text{lo cual implica que} \\ \psi &= \frac{\theta + 2\pi k}{n}, \quad \text{para alguna } k \in \mathbb{Z}. \end{aligned}$$

De esta manera al sustituir en 1.9 obtenemos

$$(\cos\theta + i\ sen\ \theta)^{\frac{1}{n}} = \cos\left(\frac{\theta + 2\pi k}{n}\right) + i\ sen\ \left(\frac{\theta + 2\pi k}{n}\right) \tag{1.10}$$

Ahora veremos que si damos a k los valores $0, 1, 2, ..., n-1$ obtenemos n raíces n-ésimas diferentes, del complejo z y que éstas son todas, es decir, que para cualquier otro valor de k obtenemos una de estas raíces.

Tomemos dos valores distintos para k entre 0 y $n-1$, k_1 y k_2, y supongamos que $k_1 < k_2$, de modo que $0 \leq k_1 < k_2 < n$, luego $0 \leq 2\pi k_1 < 2\pi k_2 < 2\pi n$ y $\theta \leq \theta + 2\pi k_1 < \theta + 2\pi k_2 < \theta + 2\pi n$, de aquí que $\frac{\theta}{n} \leq \frac{\theta+2\pi k_1}{n} < \frac{\theta+2\pi k_2}{n} < \frac{\theta}{n} + 2\pi$; es decir, $\frac{\theta+2\pi k_1}{n}$ y $\frac{\theta+2\pi k_2}{n}$ difieren en menos de 2π, luego entonces, su seno y su coseno difieren.[3]

Por otra parte, si k es un entero, por el algoritmo de la división, existen s y r enteros tales que

$$k = sn + r, \quad \text{donde } 0 \leq r < n$$

y entonces

$$\cos\left(\frac{\theta + 2\pi k}{n}\right) + i\ sen\ \left(\frac{\theta + 2\pi k}{n}\right) = \cos\left(\frac{\theta + 2\pi\,(sn + r)}{n}\right) + i\ sen\ \left(\frac{\theta + 2\pi\,(sn + r)}{n}\right)$$

[3] Recuerde que dos ángulos $0 < \alpha, \beta < 2\pi$ tales que $\cos\alpha = \cos\beta$ y $sen\ \alpha = sen\ \beta$, necesariamente son iguales.

$$= \cos\left(\frac{\theta+2\pi r}{n}+2\pi s\right)+i\ sen\ \left(\frac{\theta+2\pi r}{n}+2\pi s\right) = \cos\left(\frac{\theta+2\pi r}{n}\right)+i\ sen\ \left(\frac{\theta+2\pi r}{n}\right).$$

De aquí que basta tomar para k valores entre 0 y $n-1$.

Como las n raíces tienen módulo 1 éstas están situadas sobre la circunferencia de radio 1. Además, sus argumentos difieren por múltiplos de $\frac{2\pi}{n}$, entonces, geométricamente, estas raíces son los vértices de un polígono regular de n lados inscrito en la circunferencia de radio 1.

Ejemplo 5 *i. Encontrar las raíces cúbicas de* 1.

$$1 = \cos 0 + i\ sen\ 0$$

$$(\cos 0 + i\ sen\ 0)^{\frac{1}{3}} = \cos\left(\frac{0+2\pi k}{3}\right)+i\ sen\left(\frac{0+2\pi k}{3}\right), \qquad k=0,1,2$$

entonces, llamando r_0, r_1, r_2 *a las raíces:*

$$\begin{aligned} r_0 &= \cos\left(\frac{0+0}{3}\right)+i\ sen\left(\frac{0+0}{3}\right) = \cos 0 + i\ sen\ 0 = 1. \\ r_1 &= \cos\left(\frac{0+2\pi}{3}\right)+i\ sen\left(\frac{0+2\pi}{3}\right) = \cos\frac{2\pi}{3}+i\ sen\ \frac{2\pi}{3} = -\frac{1}{2}+i\ \frac{\sqrt{3}}{2}. \\ r_2 &= \cos\left(\frac{0+4\pi}{3}\right)+i\ sen\left(\frac{0+4\pi}{3}\right) = \cos\frac{4\pi}{3}+i\ sen\ \frac{4\pi}{3} = -\frac{1}{2}-i\ \frac{\sqrt{3}}{2}. \end{aligned}$$

ii. Encontrar las 5 *raíces quintas de* $z = 8\left(\cos\frac{\pi}{4}+i\ sen\ \frac{\pi}{4}\right)$.

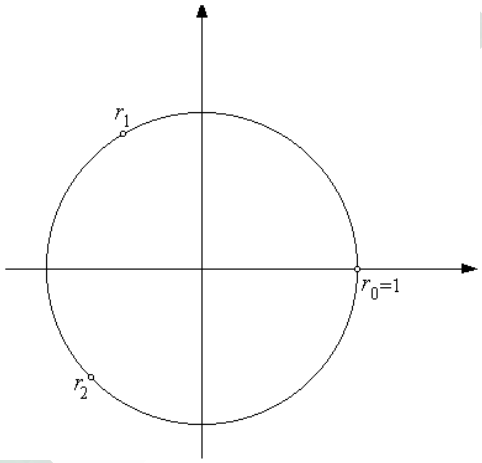
Hagamos $w = \frac{z}{8}$ *y llamemos* $r_0^{'}, r_1^{'}, r_2^{'}, r_3^{'}, r_4^{'}$ *a las raíces quintas de* w. *Entonces*

$$\begin{aligned} r_0^{'} &= \cos\left(\frac{\frac{\pi}{4}+2\pi\,(0)}{5}\right)+i\ sen\left(\frac{\frac{\pi}{4}+2\pi\,(0)}{5}\right) = \cos\frac{\pi}{20}+i\ sen\frac{\pi}{20}, \\ r_1^{'} &= \cos\left(\frac{\frac{\pi}{4}+2\pi\,(1)}{5}\right)+i\ sen\left(\frac{\frac{\pi}{4}+2\pi\,(1)}{5}\right) = \cos\frac{9\pi}{20}+i\ sen\frac{9\pi}{20}, \\ r_2^{'} &= \cos\left(\frac{\frac{\pi}{4}+2\pi\,(2)}{5}\right)+i\ sen\left(\frac{\frac{\pi}{4}+2\pi\,(2)}{5}\right) = \cos\frac{17\pi}{20}+i\ sen\frac{17\pi}{20}, \\ r_3^{'} &= \cos\left(\frac{\frac{\pi}{4}+2\pi\,(3)}{5}\right)+i\ sen\left(\frac{\frac{\pi}{4}+2\pi\,(3)}{5}\right) = \cos\frac{25\pi}{20}+i\ sen\frac{25\pi}{20}, \\ r_4^{'} &= \cos\left(\frac{\frac{\pi}{4}+2\pi\,(4)}{5}\right)+i\ sen\left(\frac{\frac{\pi}{4}+2\pi\,(4)}{5}\right) = \cos\frac{33\pi}{20}+i\ sen\frac{33\pi}{20}, \end{aligned}$$

y entonces las raíces de z son:

$$\begin{aligned}
r_0 &= \sqrt[5]{8}\left(\cos\frac{\pi}{20} + i\ sen\frac{\pi}{20}\right), \\
r_1 &= \sqrt[5]{8}\left(\cos\frac{9\pi}{20} + i\ sen\frac{9\pi}{20}\right), \\
r_2 &= \sqrt[5]{8}\left(\cos\frac{17\pi}{20} + i\ sen\frac{17\pi}{20}\right), \\
r_3 &= \sqrt[5]{8}\left(\cos\frac{25\pi}{20} + i\ sen\frac{25\pi}{20}\right), \\
r_4 &= \sqrt[5]{8}\left(\cos\frac{33\pi}{20} + i\ sen\frac{33\pi}{20}\right).
\end{aligned}$$

Usando la interpretación geométrica de los complejos observamos que las raíces cúbicas de 1 se representan como tres puntos sobre la circunferencia unitaria cuyos argumentos son 0, $\frac{2\pi}{3}$ y $\frac{4\pi}{3}$, respectivamente.



Los puntos r_0, r_1 y r_2 son los vértices de un triángulo equilátero.

De manera análoga, las raíces quintas de $8\left(\cos\frac{\pi}{4} + i\ sen\frac{\pi}{4}\right)$ se representan como puntos sobre la circunferencia de radio $\sqrt[5]{8}$ con argumentos $\frac{\pi}{20}$, $\frac{9\pi}{20}$, $\frac{17\pi}{20}$, $\frac{25\pi}{20}$ y $\frac{33\pi}{20}$, respectivamente.

Los puntos r_0, r_1, r_2, r_3 y r_4 son los vértices de un pentágono regular.

Ejercicios 1.3.1

1. Utilice el Teorema de De Moivre para probar que
   a. $cos\,(2\theta) = cos^2\theta - sen^2\theta$.
   b. $sen\,(2\theta) = 2sen\,(\theta)\,cos\,(\theta)$.
2. Utilice el Teorema de De Moivre para obtener expresiones para $\cos\,4\theta$ y $sen\,6\theta$ en términos de $\cos\,\theta$ y $sen\,\theta$.
3. Calcule las raíces sextas de 1 y -1. Exprese las soluciones en la forma $a + b\,i$ y represéntelas gráficamente.
4. Obtenga todas las soluciones de las siguientes ecuaciones:
   a. $z^2 = 3 - 4\,i$.
   b. $z^4 - 1 = 2\,i$.
   c. $z^3 = 1 + i$.
   d. $z^4 = i$.
5. Sea $n \in \mathbb{N}$. Defina
$$\xi = cos\left(\frac{2\pi}{n}\right) + i\,sen\left(\frac{2\pi}{n}\right)$$
   a. Pruebe que $z = 1, z = \xi, z = \xi^2, ..., z = \xi^{n-1}$ son todas las soluciones distintas de la ecuación $z^n = 1$.
   b. Prueba que si $z = \mu$ es una solución de $z^n = w$, entonces todas las otras soluciones son de la forma $\mu \cdot \xi^j$, donde $j = 1, 2, ..., n-1$.
6. Sea ξ definida como en el problema 5. Pruebe que para $k \in \mathbb{N}$,
$$\begin{aligned} 1 + \xi^k + \xi^{2k} + ... + \xi^{(n-1)k} &= 0, \quad \text{si } n \text{ no divide a } k, \quad \text{y} \\ 1 + \xi^k + \xi^{2k} + ... + \xi^{(n-1)k} &= n, \quad \text{si } n \text{ divide a } k. \end{aligned}$$
7. Pruebe lo siguiente:
   a. $\arg\,(\overline{z}) = -\arg\,(z)\,,\ (\mathrm{mod}\ 2\pi)$.
   b. $\arg\left(\frac{z}{w}\right) = \arg\,(z) - \arg\,(w)\,,\ (\mathrm{mod}\ 2\pi)$.
8. Pruebe que el máximo valor del módulo de $z^2 + 1$ sobre el círculo unitario $\{z \in \mathbb{C}\,|\,|z| \leq 1\}$ es 2.
9. Encuentre las cuatro raíces de la ecuación $x^4 + 4 = 0$. Utilice este resultado para factorizar $z^4 + 4$ como $(z^2 + 2z + 2)(z^2 - 2z + 2)$.
10. Simplifique las siguientes expresiones:
    a. $(1 \pm i)^{16}$
    b. $\dfrac{1+i}{(1-i)^2}$

c. $\left[\dfrac{34}{(1-45i)(5+3i)}\right]^2$

d. $\left|\dfrac{(6+7i)(4-2i)}{4+2i}\right|\left|-\dfrac{1}{7+6i}\right|$

Capitulo 2
POLINOMIOS

Interesados en el problema de resolver ecuaciones algebraicas, hemos visto cómo podemos encontrar en $\mathbb{C}$ todas las soluciones de las ecuaciones de la forma $x^n = z$, con $z \in \mathbb{C}$, $n \in \mathbb{N}$; las soluciones de las ecuaciones lineales, $ax + b = 0$, con $a, b \in \mathbb{C}$, $a \neq 0$; las ecuaciones cuadráticas, $ax^2 + bx + c = 0$, con $a, b, c \in \mathbb{C}$, $a \neq 0$; todas éstas, casos particulares de la ecuación general de n-ésimo grado:

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

donde las $a_i \in \mathbb{C},\ n \in \mathbb{N}$ y x es la incógnita.

El problema de resolverlas, consiste en encontrar valores de x que al sustituirlos en la expresión

$$a_0 + a_1x + ... + a_nx^n \tag{2.1}$$

la hagan cero.

Aquí, ampliaremos el estudio de ecuaciones donde los coeficientes $a_0, a_1, ..., a_n$ sean números enteros, racionales, reales, complejos o elementos de algún conjunto que tenga estructura de anillo donde tiene sentido plantearse este tipo de expresiones (2.1). Eso es, estudiaremos el álgebra de polinomios (expresiones como la dada en (2.1) en la cual se base la teoría de ecuaciones. Veremos que la forma en que sumamos y multiplicamos estas expresiones, en los cursos elementales de álgebra, le dan una estructura de dominio entero, en el cual se puede desarrollar una teoría de divisibilidad similar a la de los enteros.

2.1 EL ANILLO DE POLINOMIOS

De los conjuntos de números que usualmente trabajamos, $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ y $\mathbb{C}$, observamos que todos ellos tienen dos operaciones (suma y producto) cuyas propiedades les dan una estructura en común, que es la de ser dominio entero y es con estas operaciones que podemos plantearnos ecuaciones del tipo $a_0 + a_1x + ... + a_nx^n = 0$ donde las a_i, para $i = 0, .., n$ son elementos de $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ o $\mathbb{C}$ dependiendo dónde se considere la ecuación.

Así, empezaremos por considerar D un dominio entero y expresiones de la forma:

$$a_0 + a_1x + ... + a_nx^n, \quad \text{donde } a_0, a_1, ..., a_n \in D \quad \text{y} \quad n \geq 0 \tag{2.2}$$

de las que diremos que dos de ellas son iguales si los coeficientes correspondientes son los mismos, esto es,

$$a_0 + a_1x + ... + a_nx^n = b_0 + b_1x + ... + b_mx^m \iff$$
$$n = m \quad \text{y} \quad a_0 = b_0, a_1 = b_1, ..., a_n = b_n.$$

Estas expresiones las llamaremos de acuerdo a la siguiente

Definicion 10 *Un polinomio en x con coeficientes en D, es una expresión de la forma (2.2).*

Las expresiones $a_i x^i$, para $0 \leq i \leq n$ se llaman **términos** del polinomio. Los elementos $a_0, a_1, ..., a_n \in D$ se llaman **coeficientes** de $x^0, x^1, ..., x^n$, respectivamente, donde $x^0 = 1$ y $x^n = x \cdot x^{n-1} = x^{n-1} \cdot x$, para toda $n \in \mathbb{N}$.

Notación. Denotamos por $D[x]$ al conjunto de polinomios en x con coeficientes en D, es decir,

$$D[x] = \{ a_0 + a_1 x + ... + a_n x^n |\ a_i \in D, \quad \text{para } i = 0, .., n \quad \text{y} \quad n \geq 0 \}.$$

Además, se acostumbra denotar por $a(x)$, $b(x)$, etc., a los elementos de $D[x]$, esto es, $a(x) \in D[x]$ significa que $a(x) = a_0 + a_1 x + ... + a_n x^n$ para algunas $a_i \in D$ con $i = 0, ..., n$ y $n \geq 0$.

Nota. Si alguna $a_i = 0$, se acostumbra omitir el término $a_i x^i$. Convenimos en escribir x^i en lugar de $1x^i$, y $-a_i x^i$ a cambio de $(-a_i)x^i$ o de $+(-a_i)x^i$.[4]

Ejemplo 6
i. $-2x + 3x^2 \in \mathbb{Z}[x]$.
ii. $\sqrt{2} + \frac{5}{6}x^4 \in \mathbb{R}[x]$.
iii. $3x - 6ix^3 + (4 - 2i)x^5 \in \mathbb{C}[x]$.
iv. $3 + 0x + 6x^2 + \left(-\frac{2}{3}\right)x^3 + 0x^4 = 3 + 6x^2 - \frac{2}{3}x^3 \in \mathbb{Q}[x]$.

Observacion 3 *De la nota anterior y la igualdad de polinomios se deduce que dos polinomios siempre se pueden anotar con el mismo número de términos, ya que si* $a(x) = a_0 + a_1 x + ... + a_n x^n$ *y* $b(x) = b_0 + b_1 x + ... + b_m x^m$ *son polinomios con* $m < n$, *podemos escribir* $b(x) = b_0 + b_1 x + ... + b_m x^m + 0x^{m+1} + ... + 0x^n$.

Por otra parte, se puede observar fácilmente que $D \subset D[x]$, de aquí que nos preguntamos si es posible definir en $D[x]$ una suma y un producto de tal manera que restringidos a D correspondan a las operaciones de suma y producto que hay en D y si es posible que $D[x]$ tenga también estructura de dominio entero.

Veamos primero un ejemplo, consideremos $D = \mathbb{Z}$ y supongamos que en $D[x]$ tenemos una suma y un producto que lo hacen dominio entero.

Así, si sumamos y multiplicamos los polinomios $\left(3 + x + x^2\right)$ y $(-1 + 3x)$ se debe tener:

$$\begin{aligned} \left(3 + x + x^2\right) + (-1 + 3x) &= 3 + x + x^2 + (-1) + 3x \\ &= 3 + (-1) + x + 3x + x^2 \\ &= 2 + (1 + 3)x + x^2 \\ &= 2 + 4x + x^2 \end{aligned}$$

[4] Este hecho se justifica por la proposición (1).

por las propiedades asociativa y conmutativa de la suma, y distributiva del producto respecto a la suma; y el producto,

$$\begin{aligned}\left(3+x+x^2\right)(-1+3x) &= (3+x+x^2)(-1)+(3+x+x^2)(3x)\\ &= -3-x-x^2+9x+3x^2+3x^3\\ &= -3-x+9x-x^2+3x^2+3x^3\\ &= -3+(-1+9)x+(-1+3)x^2+3x^3\\ &= -3+8x+2x^2+3x^3\end{aligned}$$

por las propiedades distributiva, asociativa y conmutativa.

Como se puede observar en este ejemplo, el coeficiente del término x^k (para $k=0,1,2,...$) en la suma, es la suma de los coeficientes de x^k de cada uno de los sumandos, mientras que el coeficiente de x^k (para $k=0,1,2,...$) en el producto es la suma de los productos de los coeficientes de x^i (del primer factor) y x^j (del segundo factor) donde $i+j=k$ ya que $x^i x^j = x^{i+j}$.

Con esto, resulta natural definir, en general, la suma y el producto de elementos de $D[x]$ como sigue:

Definicion 11 ***Adición de polinomios.*** *Si* $a(x) = a_0 + a_1x + ... + a_nx^n$ *y* $b(x) = b_0 + b_1x + ... + b_nx^n$, *son polinomios en* x *con coeficientes en D, entonces la suma de* $a(x)$ *y* $b(x)$ *es el polinomio:* $a(x)+b(x) = (a_0+b_0)+(a_1+b_1)x+...+(a_n+b_n)x^n$.

Definicion 12 ***Multiplicación de polinomios.*** *Si* $a(x) = a_0 + a_1x + ... + a_mx^m$ *y* $b(x) = b_0 + b_1x + ... + b_nx^n$, *son polinomios en* x *con coeficientes en D, entonces el producto de* $a(x)$ *y* $b(x)$ *es el polinomio:* $a(x)\cdot b(x) = a_0b_0 + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + ... + (a_mb_n)x^{n+m}$.

El coeficiente de x^k en el producto $a(x)\cdot b(x)$ es:

$$a_0b_k + a_1b_{k-1} + ... + a_{k-1}b_1 + a_kb_0 = \sum_{i+j=k} a_ib_j.$$

Así observamos que la suma y el producto de polinomios es nuevamente un polinomio de donde tenemos la siguiente:

Proposicion 19 $D[x]$ *es un dominio entero.*

Demostración:

De las definiciones de suma y producto en $D[x]$ y las propiedades asociativa y conmutativa de la suma y el producto en D, así como la propiedad distributiva en D se sigue

la validez de las mismas en $D[x]$. Aquí probaremos solamente la propiedad distributiva y las demás quedan como ejercicio para el lector.

Sean $a(x) = a_0 + a_1x + ... + a_mx^m$, $b(x) = b_0 + b_1x + ... + b_nx^n$ y $c(x) = c_0 + c_1x + ... + c_nx^n$, polinomios en $D[x]$. Supongamos que $b(x)$ y $c(x)$ tienen el mismo número de términos (obs. 3) para facilitar la notación y con esto se tiene:

$$a(x) \cdot (b(x) + c(x)) = d_0 + d_1x + ... + d_{m+n}x^{m+n},$$

donde $d_k = \sum_{i+j=k} a_i(b_j + c_j)$, para $k = 0...m + n$.

Por otra parte,

$$a(x) \cdot b(x) = e_0 + e_1x + ... + e_{m+n}x^{m+n},$$

donde $e_k = \sum_{i+j=k} a_ib_j$, para $k = 0, 1, 2, ..., m + n$ y

$$a(x) \cdot c(x) = e'_0 + e'_1x + ... + e'_{m+n}x^{m+n},$$

donde $e'_k = \sum_{i+j=k} a_ic_j$, para $k = 0, 1, 2, ..., m + n$; de aquí que

$$a(x) \cdot b(x) + a(x) \cdot c(x) = (e_0 + e'_0) + (e_1 + e'_1)x + ... + (e_{m+n} + e'_{m+n})x^{m+n},$$

donde el coeficiente $k - \acute{e}simo$ es

$$\begin{aligned} e_k + e'_k &= \sum_{i+j=k} a_ib_j + \sum_{i+j=k} a_ic_j \\ &= \sum_{i+j=k} (a_ib_j + a_ic_j) \\ &= \sum_{i+j=k} a_i(b_j + c_j) = d_k \end{aligned}$$

y por lo tanto $a(x) \cdot (b(x) + c(x)) = a(x) \cdot b(x) + a(x) \cdot c(x)$.

También se tiene que, como $0, 1 \in D$, entonces $0, 1 \in D[x]$ y para cualquier polinomio $a(x) \in D[x]$, $a(x) + 0 = a(x)$ y $a(x) \cdot 1 = a(x)$.

Además, si $a(x) = a_0 + a_1x + ... + a_nx^n \in D[x]$, entonces $-a(x) = (-a_0) + (-a_1)x + ... + (-a_n)x^n \in D[x]$ y $a(x) + (-a(x)) = 0$.

Por lo tanto, $D[x]$ es un anillo conmutativo con 1.

Por otra parte, si $a(x)$ y $b(x) \in D[x]$ son distintos de cero, entonces al menos el último de los coeficientes de cada uno de los polinomios es distinto de cero, es decir, $a_0 + a_1x + ... + a_mx^m$ y $b_0 + b_1x + ... + b_nx^n$ con $a_m \neq 0$ y $b_n \neq 0$.

Como en $a(x) \cdot b(x)$, el coeficiente de x^{m+n} es a_mb_n, que es diferente de cero por ser D un dominio entero, se tiene que $a(x) \cdot b(x) \neq 0$. Por lo tanto, la proposición queda probada. ■

Como veremos a lo largo del estudio de los polinomios, un concepto fundamental es sin duda el del grado, que definimos a continuación.

Definicion 13 *Sea $a(x) = a_0 + a_1x + ... + a_nx^n$ un polinomio, distinto de cero, en $D[x]$. El **grado de** $a(x)$ es el máximo entero $i \geq 0$ tal que $a_i \neq 0$. Si n es el grado del polinomio $a(x)$, escribiremos $gr(a(x)) = n$.*

Ejemplo 7 *i. Si $f(x) = x - 3x^2 + 5x^6$ entonces, $gr(f(x)) = 6$.*
ii. Si $g(x) = 3$, entonces $gr(g(x)) = 0$.

Definicion 14 *Si $a(x) = a_0 + a_1x + ... + a_nx^n$ es un polinomio de grado n en $D[x]$, entonces llamaremos a a_n el **coeficiente principal de** $a(x)$, y si $a_n = 1$,entonces diremos que $a(x)$ es un **polinomio mónico**. También nos referiremos al término a_0 como el **término independiente** y cuando $gr(a(x)) = 0$, diremos que el polinomio es una **constante**.*

Con respecto al grado de la suma y el producto de dos polinomios tenemos la siguiente

Proposicion 20 *Sean $a(x)$ y $b(x)$ polinomios distintos de cero en $D[x]$,*

1. *Si $a(x) + b(x) \neq 0$, entonces $gr(a(x) + b(x)) \leq \max\{gr(a(x)), gr(b(x))\}$.*
2. *Si $a(x) + b(x) \neq 0$, entonces $gr(a(x) \cdot b(x)) = gr(a(x)) + gr(b(x))$.*

Demostración:

Sean $a(x) = a_0 + a_1x + ... + a_mx^m$ y $b(x) = b_0 + b_1x + ... + b_nx^n$ donde $a_m \neq 0$ y $b_n \neq 0$, es decir, $gr(a(x)) = m$ y $gr(b(x)) = n$.

1. Si $m > n$, entonces
   $a(x) + b(x) = (a_0 + b_0) + (a_1 + b_1)x + ... + (a_n + b_n)x^n + ... + a_mx^m$,
   por lo que $gr(a(x) + b(x)) = m = \max\{gr(a(x)), gr(b(x))\}$.
   Análogamente, si $n > m$, entonces $gr(a(x) + b(x)) = n = \max\{gr(a(x)), gr(b(x))\}$.
   Si $m = n$, entonces $a(x) + b(x) = (a_0 + b_0) + (a_1 + b_1)x + ... + (a_n + b_n)x^n$ y como $a(x) + b(x) \neq 0, \quad a_i + b_i \neq 0$ para alguna $i \leq n$. Si $k = \max\{i \geq 0 \,|a_i + b_i \neq 0\}$, entonces $k \leq n$ y $gr\,(a(x) + b(x)) = k \leq n = \max\{gr(a(x)), gr(b(x))\}$.

2. En el caso del producto, según vimos con anterioridad, el coeficiente de x^{n+m} es $a_m b_n$ que es distinto de cero y el coeficiente de x^k, para $k > n+m$ es cero. ■

Para algunos dominios enteros, es posible interpretar el anillo de polinomios como un conjunto de funciones polinomiales. Si D es un dominio entero, y $a(x) = a_0 + a_1 x + ... + a_n x^n \in D[x]$, considerando al polinomio $a(x)$ podemos pensar en la función $a : D \to D$ cuya regla de correspondencia es $a(\alpha) = a_0 + a_1\alpha + ... + a_n\alpha^n$, para cada $\alpha \in D$. Esto es, si P_D es el conjunto de funciones polinomiales de D en D, es decir, $P_D = \{a : D \to D \,|\, a(\alpha) = a_0 + a_1\alpha + ... + a_n\alpha^n,$ con $a_i \in D\}$, se puede ver fácilmente que la función que la asignación dada anteriormente define una función suprayectiva de $D[x]$ en P_D.

Por otra parte, utilizando las operaciones en D y sus propiedades, también se pueden definir en P_D dos operaciones que hacen que este conjunto de funciones sea un dominio entero y que además a través de la correspondencia definida entre $D[x]$ y P_D, dichas operaciones correspondan a las de suma y producto en $D[x]$ y así, como veremos más adelante, a cada polinomio $a(x) \in D[x]$ corresponderá una y sólo una función $a \in P_D$ en el caso en que D sea infinito.

Definicion 15 ***Suma y producto*** *en* P_D.

Sean $a, b \in P_D$. *La suma de* a *y* b *es la función* $a + b : D \to D$ *tal que* $(a+b)(\alpha) = a(\alpha) + b(\alpha)$ *para cada* $\alpha \in D$ *y el producto de* a *y* b *es la función* $a \cdot b : D \to D$ *tal que* $(a \cdot b)(\alpha) = a(\alpha) \cdot b(\alpha)$ *para cada* $\alpha \in D$.

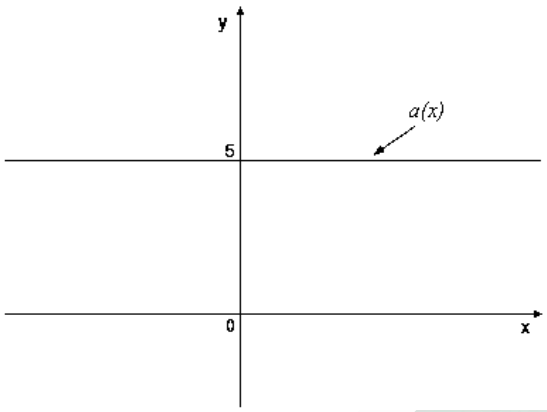
Proposicion 21 *P_D es un dominio entero (con las operaciones definidas en 15).*

Demostración:

Queda como ejercicio para el lector. ■

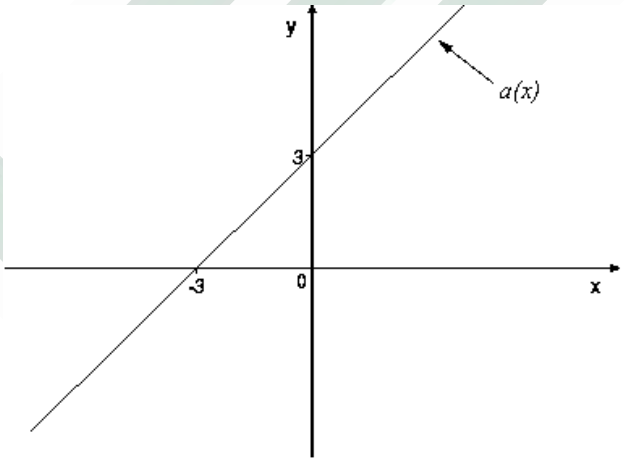
Ahora consideremos el anillo de polinomios con coeficientes reales $\mathbb{R}[x]$. Si lo pensamos como las funciones polinomiales de $\mathbb{R}$ en $\mathbb{R}$, podemos dar una interpretación geométrica de los elementos de este anillo que será de gran utilidad en el estudio de sus raíces.

Si $a(x)$ es una constante, es decir, si $a(x) = a_0$ con $a_0 \in \mathbb{R}$, entonces su gráfica es una recta paralela al eje de las abscisas, por ejemplo, la gráfica del polinomio $a(x) = 5$ es



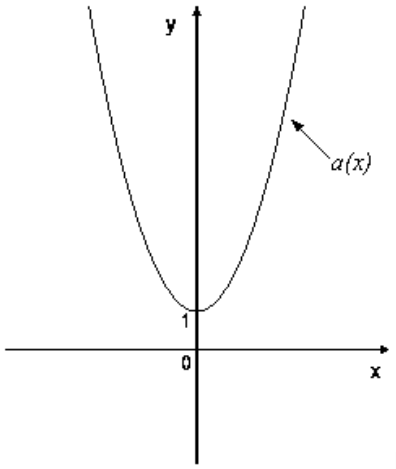
$a(x) = 5$

Si $a(x)$ es un polinomio de primer grado, es decir si $a(x) = a_0 + a_1 x$ con $a_0, a_1 \in \mathbb{R}$, $a_1 \neq 0$ entonces su gráfica es una recta de pendiente a_1 que intersecta al eje de las ordenadas en a_0 y al del las abscisas en $-\dfrac{a_0}{a_1}$. Por ejemplo, si $a(x) = 3 + x$, su gráfica es

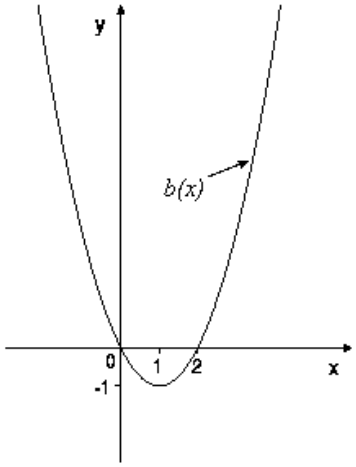


$a\,(x) = 3 + x$

Si $a(x)$ es un polinomio de 2^0 grado, o sea, $a(x) = a_0 + a_1 x + a_2 x^2$, con $a_0, a_1, a_2 \in \mathbb{R}$, $a_2 \neq 0$, su gráfica es una parábola con eje focal paralelo al eje de ordenadas. Por ejemplo, si $a(x) = 1 + x^2$ y $b(x) = -2x + x^2$ sus gráficas son

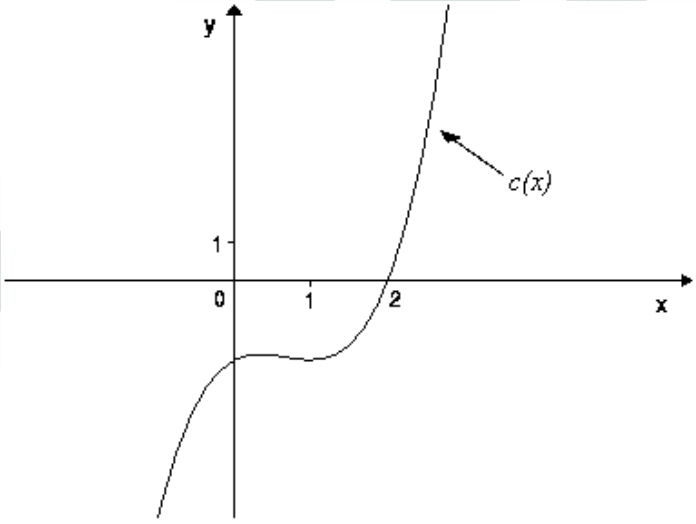


$a(x) = 1 + x^2$



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

Si $c(x) = -2 + x - 2x^2 + x^3 = (x-2)\left(1+x^2\right)$, su gráfica es



$c(x) = (x-2)\left(1+x^2\right)$

Nota: En vista de que todo campo es un dominio entero, es claro que si K es un campo, siempre se puede formar el anillo de polinomios con coeficientes en K.

Como veremos en el siguiente tema, es necesario considerar los coeficientes de los polinomios en un campo para que cumplan propiedades análogas a las que tienen los enteros.

Es por esto que, de aquí en adelante, consideraremos el anillo $K[x]$ con K un campo a menos de que se haga la aclaración de lo contrario.

Ejercicios 2.1

1. Sume los siguientes parejas de polinomios.
   a. $f(x) = 7x + (-3)x^2 + x^3, \quad g(x) = 6x + (-3)x^2$.
   b. $f(x) = 1 + 7x^4 - x^7, \quad g(x) = x^3 + 5x^5$.
   c. $f(x) = 1 + x^{32}, \quad g(x) = 1 + x^{32}$.
   d. $f(x) = 3x^2 + 7x - \frac{1}{2}, \quad g(x) = x^3 - \frac{1}{2}x^2 + 1$.
2. Multiplique las parejas de polinomios de la pregunta (1).
3. Pruebe que en $D[x]$, con D un dominio entero, se tiene la igualdad:

$$(a_0 + a_1x + a_2x^2 + ... + a_nx^n)(cx^j) = a_0cx^j + a_1cx^{j+1} + a_2cx^{j+2} + ... + a_ncx^{j+n}$$

4. Pruebe que si K es un campo, entonces K es un dominio entero.
5. Pruebe la proposición 21.
6. a. Si D es un dominio ordenado, pruebe que $D[x]$ es un dominio ordenado si se define $p(x) > 0$ si el primer coeficiente distinto de cero, a_k, de $p(x)$ es positivo en D.
   b. Pruebe que $D[x]$ es un dominio ordenado si se define $p(x) > 0$ si el último coeficiente distinto de cero, a_n, es positivo en D.
7. Sea $D = \mathbb{Z}$ en el ejercicio 6.b, pruebe que 1 es el mínimo polinomio positivo en $\mathbb{Z}[x]$ y que $\mathbb{Z}[x]$ no cumple el Principio del Buen Orden.

2.2 ALGORITMO DE LA DIVISION

2.2.1 Algoritmo de la División

En este tema veremos otra propiedad común entre el anillo de los enteros y el anillo de polinomios sobre algún campo. En el anillo de los enteros, dados $a, b \in \mathbb{Z}$,si $b \neq 0$, siempre existen enteros únicos q, r de tal forma que

$$a = bq + r \quad \text{con} \quad 0 \leq r < |b| .$$

Dado que en el anillo de polinomios no se ha establecido un orden y tampoco tenemos la noción de valor absoluto, si queremos que haya un algoritmo como el de la división para los

enteros, nuestra primera pregunta sería, ¿cuál puede ser el concepto correspondiente al de valor absoluto?

Recordemos que el valor absoluto es una función de $\mathbb{Z}$ en $\mathbb{N}\cup\{0\}$ que cumple, entre otras cosas, las siguientes propiedades:

1. $|a+b| \leq |a| + |b|$ para todos $a, b \in \mathbb{Z}$.
2. $|a \cdot b| = |a|\,|b|$ para todos $a, b \in \mathbb{Z}$.
3. Para cada $a, b \in \mathbb{Z} - \{0\}$, $|a| \leq |ab|$.

La función grado de un polinomio, $gr : K[x] - \{0\} \to \mathbb{N} \cup \{0\}$, que asocia a cada polinomio distinto de cero su grado va a ser la función que va a jugar el papel que jugaba el valor absoluto en los números enteros, en particular se puede ver que también satisface la tercera propiedad mencionada, esto es, para cada par de polinomios $a(x), b(x) \in K[x]-\{0\}$,

$$gr(a(x)) \leq gr(a(x) \cdot b(x)),$$

puesto que $gr(a(x) \cdot b(x)) = gr(a(x)) + gr(b(x))$.

Con base en está función demostraremos la validez del Algoritmo de la División para polinomios.

Teorema 22 ***Algoritmo de la División.*** *Si $a(x), b(x)$ son polinomios sobre $K[x]$, K un campo y $b(x) \neq 0$, existen polinomios $q(x), r(x) \in K[x]$ tales que $a(x) = b(x)q(x) + r(x)$ con $r(x) = 0$ o $gr(a(x)) < gr(b(x))$ y esta pareja es la única con tales propiedades.*

Demostración:

Primero demostraremos la existencia de tales polinomios.

Si $a(x) = 0$, entonces $a(x) = b(x) \cdot 0 + 0$ y queda probado.

Supongamos que $a(x) \neq 0$, la demostración se hará por inducción sobre el grado de $a(x)$.

1. Si $gr(a(x)) = 0$ y $gr(b(x)) = 0$, entonces $a(x), b(x) \in K$, es decir, $a(x) = a$ y $b(x) = b$ donde $a, b \in K$. Como $b \neq 0$, $a = b \cdot \dfrac{a}{b} + 0$, de aquí que $q(x) = \dfrac{a}{b}$ y $r(x) = 0$, cumplen lo deseado.
2. Si $gr(a(x)) = 0$ y $gr(b(x)) \neq 0$, entonces $a(x) = b(x)\cdot 0 + a(x)$ y $gr(a(x)) < gr(b(x))$.
3. Supongamos que el teorema es válido para todo polinomio $b(x)$, si el grado de $a(x)$ es menor o igual a $n-1$.
   Si $a(x) = a_0 + a_1x + ... + a_nx^n$ con $a_n \neq 0$, es decir, $gr(a(x)) = n$ entonces, si $gr(b(x)) > gr(a(x))$, $a(x) = b(x) \cdot 0 + a(x)$ y $gr(a(x)) < gr(b(x))$.
   Supongamos ahora que $gr(a(x)) \geq gr(b(x))$. Si $b(x) = b_0 + b_1x^1 + ... + b_mx^m$ y $gr(b(x)) = m$, entonces $b_m \neq 0$. Como K es campo, existe el inverso multiplicativo de

b_m y de aquí que:

$$\begin{aligned}\frac{a_n}{b_m}x^{n-m}b(x) &= \frac{a_n\cdot b_0}{b_m}x^{n-m}+\frac{a_n\cdot b_1}{b_m}x^{n-m+1}+...+\frac{a_n\cdot b_m}{b_m}x^n\\ &= \frac{a_n\cdot b_0}{b_m}x^{n-m}+\frac{a_n\cdot b_1}{b_m}x^{n-m+1}+...+a_nx^n\end{aligned}$$

es decir, obtenemos un polinomio de grado igual al de $a(x)$ y con el mismo coeficiente principal, con lo cual $a(x)-\frac{a_n}{b_m}x^{n-m}b(x)$ es un polinomio de grado a lo más $n-1$ y por hipótesis de inducción, existen $q_1(x), r_1(x) \in K[x]$ tales que

$$a(x)-\frac{a_n}{b_m}x^{n-m}b(x)=b(x)q_1(x)+r_1(x) \quad \text{y} \quad gr(r_1(x))<gr(b(x)) \text{ o } r_1(x)=0.$$

con lo cual $a(x)=b(x)\left(q_1(x)+\frac{a_n}{b_m}x^{n-m}\right)+r_1(x)$, de donde, si $q(x)=q_1(x)+\frac{a_n}{b_m}x^{n-m}$ y $r(x)=r_1(x)$, obtenemos:

$$a(x)=b(x)q(x)+r(x) \text{ con } r(x)=0 \text{ o } gr(r(x))<gr(b(x)).$$

Así, por el Principio de Inducción Modificado, el teorema es válido para toda pareja de polinomios $a(x), b(x)$ con $b(x)\neq 0$.

Finalmente probaremos la unicidad..
Supongamos que $a(x)=b(x)q_1(x)+r_1(x)$ con $r_1(x)=0$ o $gr(r_1(x))<gr(b(x))$ y $a(x)=b(x)q_2(x)+r_2(x)$ con $r_2(x)=0$ o $gr(r_2(x))<gr(b(x))$, entonces

$$b(x)\left(q_1(x)-q_2(x)\right)=r_2(x)-r_1(x) \tag{2.3}$$

Si $r_1(x)-r_2(x)=0$, entonces $q_1(x)=q_2(x)$, ya que $b(x)\neq 0$ y $K[x]$ es un dominio entero.
Si $r_1(x)\neq 0$ o $r_2(x)\neq 0$, y $r_1(x)-r_2(x)\neq 0$, entonces se tiene que $gr(r_1(x)-r_2(x))<gr(b(x))$. Por otra parte de 2.3 obtenemos que

$$gr(b(x))+gr(q_1(x)-q_2(x))=gr(r_2(x)-r_1(x)),$$

esto es, $gr(b(x))\leq gr(r_2(x)-r_1(x))$, que es una contradicción, por lo tanto $r_2(x)=r_1(x)$ y $q_2(x)=q_1(x)$ y la unicidad queda probada. ■

Como veremos más adelante, este algoritmo será de gran utilidad para encontrar el máximo común divisor de dos polinomios.

Definicion 16 *Los polinomios $q(x)$ y $r(x)$ que existen en el Algoritmo de la División se llaman, respectivamente, el **cociente y el residuo** de dividir $a(x)$ entre $b(x)$.*

Observacion 4 *Es importante observar que para poder demostrar este teorema usamos fuertemente el hecho de que K es un campo para poder multiplicar por el inverso del coeficiente principal de $b(x)$, lo cual nos lleva a preguntar, por ejemplo, si en $\mathbb{Z}$ vale el Algoritmo de la División. Veamos con un ejemplo que dados dos polinomios en $\mathbb{Z}[x]$ no siempre es posible encontrar $q(x)$ y $r(x)$ con las propiedades requeridas.*

Sean $a(x) = 2x^2 + 3x + 2$ y $b(x) = 3x + 4$.

Si existieran $q(x) = q_0 + q_1x + ... + q_nx^n$ y $r(x) = s_0 + s_1x + ... + s_mx^m$ tales que $a(x) = b(x)q(x) + r(x)$ con $r(x) = 0$ o $gr(r(x)) < gr(b(x))$, como $gr(a(x)) = 2$, entonces $2 = gr(b(x)q(x)) = gr(b(x)) + gr(q(x)) = 1 + gr(q(x))$.

Por lo tanto $gr(q(x)) = 1$, es decir, $n = 1$ y $m = 0$ de aquí que $q(x) = q_0 + q_1x$ y $r(x) = r_0 \in \mathbb{Z}$.

Con esto se tiene que $b(x)q(x) = 3q_0x + 3q_1x^2 + 4q_0 + 4q_1x + r_0$ y por la igualdad de polinomios, $3q_1 = 2$ con $q_1 \in \mathbb{Z}$ lo cual es imposible.

En general se puede demostrar que, si D es un dominio que no es campo, entonces en $D[x]$ sólo es válido el Algoritmo de la División para aquellos polinomios $b(x)$ tales que su coeficiente principal es una unidad (un elemento del dominio que tiene inverso multiplicativo).

Ejercicios 2.2.1

1. Para las siguientes parejas de polinomios $a(x), b(x)$, encuentre el cociente y el residuo de dividir $a(x)$ por $b(x)$.
   a. $a(x) = x^7 - x^3 + 5, \quad b(x) = x^3 + 7$ sobre $\mathbb{Q}[x]$.
   b. $a(x) = x^2 + 1, \quad b(x) = x^2$ sobre $\mathbb{Q}[x]$.
   c. $a(x) = 4x^3 - 17x^2 + x - 3, \quad b(x) = 2x + 5$ sobre $\mathbb{R}[x]$.
   d. $a(x) = x^3 + 2x^2 - x + 1, \quad b(x) = x + 2$ sobre $\mathbb{Z}[x]$.
2. Pruebe que si D es un dominio entero y $b(x) = b_0 + b_1x + ... + b_mx^m \in D[x]$ con $b_m \neq 0$ satisface que para todo $a(x) \in D[x]$ existen $q(x)$ y $r(x)$ en $D[x]$ tales que $a(x) = b(x)q(x) + r(x)$ y $r(x) = 0$ o $gr(r(x) < gr(b(x))$, entonces b_m es unidad.
3. Demuestre que si D es un dominio entero y $a(x), b(x) \in D[x]$ son tales que $b(x) \neq 0$ y su coeficiente principal es una unidad, entonces existen $q(x), r(x) \in D[x]$ tales que $a(x) = b(x)q(x) + r(x)$ con $r(x) = 0$ o $gr(r(x)) < gr(b(x))$.

2.2.2 División Sintética

Un caso particular del Algoritmo de la División es cuando queremos dividir un polinomio

$a(x)$ por un polinomio mónico $b(x)$ de grado uno, es decir, $b(x) = x - c$ con $c \in K$. Por el Algoritmo de la División existen dos polinomios $q(x)$ y $r(x)$ tales que:

$$a(x) = b(x)q(x) + r(x), \text{ con } r(x) = 0 \text{ o } gr(r(x)) < gr(b(x)) = 1,$$

por lo que $r(x)$ es una constante, es decir, $r(x) = r \in K$.

En muchas ocasiones la división de polinomios es un proceso largo, sin embargo, para dividir a un polinomio entre $x - c$, existe un procedimiento muy rápido llamado la **división sintética**, el cual sólo es válido para este tipo de divisores.

Sea $a(x)$ un polinomio en $K[x]$. Si $a(x) = a_0 + a_1x + ... + a_nx^n$ y $a(x) = (x - c)q(x) + r$, donde $q(x) = q_0 + q_1x + .. + q_{n-1}x^{n-1}$, entonces como

$$(x - c)q(x) = a(x) - r$$

tenemos que

$$xq(x) - cq(x) = a(x) - r$$

y con esto

$$xq(x) + r = a(x) + cq(x),$$

es decir,

$$\begin{aligned} & q_0x + q_1x^2 + .. + q_{n-1}x^n + r = a_0 + a_1x + ... + a_nx^n + cq_0 + cq_1x + ... + cq_{n-1}x^{n-1} \\ = \quad & (a_0 + cq_0) + (a_1 + cq_1)\,x + (a_2 + cq_2)\,x^2 + ... + (a_{n-1} + cq_{n-1})\,x^{n-1} + a_nx^n \end{aligned}$$

al comparar coeficientes resulta:

$$q_{n-1} = a_n,\ q_{n-2} = a_{n-1} + cq_{n-1}, ..., q_1 = a_1 + cq_1,\ r = a_0 + cq_0.$$

si esto lo escribimos en una tabla en la que se coloquen estos números convenientemente, vemos que el coeficiente de q_i se obtiene al sumar, en cada columna, a_{i+1} con el producto de c por q_{i+1}, y que la suma de a_0 con cq_0 es el residuo.

$$\begin{array}{rccccccc} & a_n & a_{n-1} & a_{n-2} & \dots & a_1 & a_0 & \big\lfloor c \\ + & & cb_{n-1} & cb_{n-2} & \dots & cb_1 & cb_0 & \\ \hline & q_{n-1} & q_{n-2} & q_{n-3} & \dots & q_0 & r & \end{array}$$

Ejemplo 8 *Para dividir* $f(x) = x^4 - 7x^3 + 5x^2 - 100x - 31$ *entre* $x - 8$ *utilizamos la división sintética.*

$$\begin{array}{rccccc} & 1 & -7 & 5 & -100 & -31 & \big\lfloor 8 \\ + & & 8 & 8 & 104 & 32 & \\ \hline & 1 & 1 & 13 & 4 & 1 & \end{array}$$

y obtenemos que

$$x^4 - 7x^3 + 5x^2 - 100x - 31 = (x - 8)(x^3 + x^2 + 13x + 4) + 1.$$

Una aplicación de la división sintética la tenemos en el siguiente resultado, análogo al cambio de base en los números enteros.

Teorema 23 *Si $c \in K$ y $p(x) \in K[x]$, existen $b_0, b_1, ..., b_n \in K$ tales que $p(x) = b_n(x-c)^n + ... + b_1(x-c) + b_0$, es decir, $p(x)$ es una combinación lineal de potencias del polinomio $(x-c)$. También se dice que $p(x)$ es un polinomio en $(x-c)$.*

Demostración:

Por el Algoritmo de la División, tenemos que $p(x) = q_1(x)(x-c) + r_1$ con $r_1 \in K$ y $gr(q_1(x)) = gr(p(x)) - 1$; si después dividimos a $q_1(x)$ entre $(x-c)$, entonces $q_1(x) = (x-c)q_2(x) + r_2$ con $r_2 \in K$ y $gr(q_2(x)) = gr(p(x)) - 2$, si seguimos con este procedimiento, es decir, si cada cociente que se obtiene se divide entre $(x-c)$, como el grado de las $q_i(x)$ es un entero mayor o igual que cero y menor que el grado de $p(x)$ y en cada paso el grado del polinomio que obtenemos es una unidad menor que el anterior, sabemos que en un número finito de pasos llegaremos a que $gr(q_i(x)) = 0$ para alguna i, entonces,

$$q_2(x) = (x-c)q_3(x) + r_3 \text{ con } r_3 \in K \text{ y } gr(q_3(x)) = gr(p(x)) - 3$$
$$\vdots$$
$$q_{n-1}(x) = (x-c)q_n(x) + r_n \text{ con } r_n \in K \text{ y } gr(q_n(x)) = 0 \text{ si } gr(p(x)) = n.$$

Si ahora en cada paso sustituimos los valores correspondientes, se obtiene que:

$$\begin{aligned} q_{n-2}(x) &= (x-c)^2 q_n(x) + (x-c)r_n + r_{n-1} \\ &\vdots \\ q_1(x) &= (x-c)^{n-1} q_n(x) + (x-c)^{n-2} r_n + ... + r_2 \\ p(x) &= (x-c)^n q_n(x) + (x-c)^{n-1} r_n + ... + r_2(x-c) + r_1. \end{aligned}$$

si llamamos $b_n = q_n, b_{n-1} = r_n, ..., b_1 = r_2, b_0 = r_1$, obtenemos lo deseado. ■

En vista de lo anterior, es de esperarse que el uso de la división sintética facilite el trabajo para la obtención de los b_i, por ejemplo si $p(x) = 2x^4 + 3x^3 - x^2 + x - 2$ lo queremos escribir como $b_0 + b_1(x-2) + ... + b_n(x-2)^n$, usando la división sintética en cada caso tenemos:

$$\begin{array}{rccccc|c} & 2 & 3 & -1 & 1 & -2 & 2 \\ + & & 4 & 14 & 26 & 54 & \\ \hline & 2 & 7 & 13 & 27 & 52 & \end{array}$$

$\Longrightarrow p(x) = (2x^3 + 7x^2 + 13x + 27)(x-2) + 52.$

Nuevamente se usa división sintética para dividir el cociente entre $(x-2)$

$$\begin{array}{rcccc|c} & 2 & 7 & 13 & 27 & 2 \\ + & & 4 & 22 & 70 & \\ \hline & 2 & 11 & 35 & 97 & \end{array}$$

$\Longrightarrow 2x^3 + 7x^2 + 13x + 27 = (2x^2 + 11x + 35)(x - 2) + 97.$

Se vuelve a usar división sintética

$$\begin{array}{rcccc} & 2 & 11 & 35 & \big| \, 2 \\ + & & 4 & 30 & \\ \hline & 2 & 15 & 65 & \end{array}$$

$\Longrightarrow 2x^2 + 11x + 35 = (2x + 15)(x - 2) + 65.$

Se vuelve a dividir

$$\begin{array}{rccc} & 2 & 15 & \big| \, 2 \\ + & & 4 & \\ \hline & 2 & 19 & \end{array}$$

$\Longrightarrow 2x + 15 = 2(x - 2) + 19.$

Con lo cual se tiene que

$$p(x) = 2(x-2)^4 + 19(x-2)^3 + 65(x-2)^2 + 97(x-2) + 52$$

Estas divisiones se pueden realizar en un sólo diagrama, separando en cada paso el residuo, con lo que se facilita la localización de los coeficientes de la combinación lineal que se busca.

A continuación vemos nuevamente el ejemplo anterior:

$$\begin{array}{rccccc|c} & 2 & 3 & -1 & 1 & -2 & 2 \\ + & & 4 & 14 & 26 & 54 & \\ \hline & 2 & 7 & 13 & 27 & 52 & \\ + & & 4 & 22 & 70 & & \\ \hline & 2 & 11 & 35 & 97 & & \\ + & & 4 & 30 & & & \\ \hline & 2 & 15 & 65 & & & \\ + & & 4 & & & & \\ \hline & 2 & 19 & & & & \end{array}$$

Así, los coeficientes de $(x - c)^i$, para $0 \leq i \leq 4$, de mayor a menor son 2, 19, 65, 97 y 52.

Ejercicios 2.2.2

1. Use la división sintética para calcular el cociente y el residuo de las siguientes divisiones.
   a. $x^3 - 3x^2 + 2x - 1$ entre $x - 2$.
   b. $x^4 - 14x^3 + 2x^2 + 49x - 36$ entre $x + 2$.
   c. $x^4 + 10x^3 + 22x^2 - 7x + 5$ entre $x + 4$.
   d. $x^4 + 10x^3 + 22x^2 - 7x + 5$ entre $x - 4$.
2. Exprese el polinomio $x^4 - 3x^3 + 4x^2 - 5x + 2$ en la forma

a. $\sum a_i (x-1)^i$.

b. $\sum b_i (x+1)^i$.

3. Exprese el polinomio $2x^7 - 3x^5 + 2x^4 - x^3 + 7x - 2$ en la forma
   a. $\sum a_i (x-1)^i$.

   b. $\sum b_i (x+1)^i$.

2.3 DIVISIBILIDAD

2.3.1 Máximo común divisor en K[x]

El concepto de divisibilidad en los números enteros se puede aplicar en cualquier dominio entero, por ejemplo, en el anillo de polinomios $K[x]$ con coeficientes en un campo K.

Definicion 17 *Sean $a(x), b(x) \in K[x]$ con $b(x) \neq 0$. Decimos que $b(x)$ divide a $a(x)$ si existe un polinomio $c(x) \in K[x]$ tal que $a(x) = b(x) \cdot c(x)$, y lo denotaremos por $b(x) \mid a(x)$.*

Otras formas de decir que $b(x)$ divide a $a(x)$ son:

- $b(x)$ es un factor de $a(x)$.
- $a(x)$ es un múltiplo de $b(x)$.

Es claro que, $b(x)$ divide a $a(x)$ en $K[x]$ si y sólo si el residuo al dividir $a(x)$ por $b(x)$ es el polinomio cero.

Además de las propiedades básicas de divisibilidad que se tienen en cualquier dominio entero, en el anillo de los polinomios $K[x]$ se pueden agregar algunas otras relacionadas con el grado.

Proposicion 24 *Sean $a(x), b(x) \in K[x]$, con $b(x) \neq 0$.*

1. *Si $b(x) \mid a(x)$, entonces $d \cdot b(x) \mid a(x)$ y $b(x) \mid f(x) \cdot a(x)$, para todo $d \in K, d \neq 0$ y para todo $f(x) \in K[x]$.*
2. *$d \mid a(x)$, para todo $d \in K - \{0\}$.*
3. *Si $b(x) \mid a(x)$ y $a(x) \neq 0$, entonces $gr(b(x)) \leqslant gr(a(x))$.*
4. *Si $a(x) \neq 0$, $b(x) \mid a(x)$ y $a(x) \mid b(x)$, entonces existe $d \in K - \{0\}$ tal que $a(x) = d \cdot b(x)$.*
   En este caso se dice que los polinomios $a(x)$ y $b(x)$ son asociados.

5. *Si* $c(x) \mid a(x)$ *y* $c(x) \mid b(x)$, *entonces* $c(x) \mid f(x)a(x) + b(x)g(x)$ *para cualesquiera* $f(x), g(x) \in K[x]$. *Es decir, si* $c(x)$ *divide a dos polinomios* $a(x), b(x)$, *entonces divide a cualquier combinación lineal de* $a(x)$ *y* $b(x)$.

Demostración:

Probaremos las afirmaciones (1), (3) y (4) y el resto se dejarán como ejercicio para el lector.

1. Tenemos, por definición, que existe $c(x) \in K[x]$ tal que $a(x) = b(x) \cdot c(x)$.
   Como $d \neq 0$ es un elemento de K se tiene que $a(x) = (d \cdot b(x)) \cdot (d^{-1} \cdot c(x))$.
   Por otra parte, al multiplicar la igualdad original por $f(x)$ resulta $a(x) \cdot f(x) = (b(x) \cdot c(x)) \cdot f(x)$.
   Por tanto $d \cdot b(x) \mid a(x)$ y $b(x) \mid f(x) \cdot a(x)$.
3. Por definición, $a(x) = b(x) \cdot c(x)$ para algún $c(x) \in K[x]$, con $c(x) \neq 0$, pues $a(x) \neq 0$, entonces
   $gr(a(x)) = gr(b(x) \cdot c(x)) = gr(b(x)) + gr(c(x))$. Como $gr(c(x)) \geq 0$, se deduce que $gr(a(x)) \geq gr(b(x))$.
4. Por hipótesis existen polinomios $f(x)$ y $g(x)$ en $K[x]$ tales que

$$a(x) = b(x) \cdot f(x) \quad \text{y} \quad b(x) = a(x) \cdot g(x).$$

   Sustituyendo tenemos $a(x) = (a(x) \cdot g(x)) \cdot f(x) = a(x) \cdot (g(x) \cdot f(x))$.
   Como $K[x]$ es un dominio entero y $a(x) \neq 0$, se tiene que $1 = g(x) \cdot f(x)$. Por el inciso anterior $gr(f(x)) \leq gr(1) = 0$, es decir, $f(x) = d \in K$. Por lo tanto, $a(x) = d \cdot b(x)$ con $d \in K$. ■

Ejemplo 9 *En* $\mathbb{Q}[x]$, *si* $a(x) = \frac{1}{3}x^4 + 2x^3 + \frac{5}{6}x^2 + 2x + \frac{1}{2}$ *y* $b(x) = \frac{1}{3}x^2 + 2x + \frac{1}{2}$, *entonces* $b(x) \mid a(x)$ *ya que* $a(x) = b(x)(x^2 + 1)$.

Definicion 18 *En un anillo conmutativo con* 1, A, *un elemento* a *es* ***unidad*** *si tiene inverso multiplicativo, es decir, si existe* $b \in A$ *tal que* $a \cdot b = 1$.

Ejemplo 10 *Las unidades en* $\mathbb{Z}$ *son* 1 *y* (-1).

Observacion 5 *Si* D *es un dominio entero, las unidades en* $D[x]$ *son las mismas que en* D.

Supongamos que $f(x) \in D[x]$ *es una unidad, entonces* $f(x) \neq 0$ *y, por la definición, se sabe que existe* $g(x) \in D[x]$ *tal que* $f(x) \cdot g(x) = 1$. *De aquí se deduce que* $gr(f(x)) +$

$gr(g(x)) = 0$ y que por lo tanto $f(x)$ y $g(x) \in D$; es decir, si un polinomio es una unidad, entonces es una constante distinta de cero. Claramente el recíproco también se cumple, esto es, cualquier unidad en D es unidad en $D[x]$. Así, si K es un campo, las unidades en $K[x]$ son todos los elementos de K distintos de cero.

En estos términos, las afirmaciones 1, 2 y 4 de la proposición anterior se pueden escribir:

1. Si $b(x) \mid a(x)$, entonces $b(x)$ por cualquier unidad divide a $a(x)$.
2. Si d es unidad, entonces $d \mid a(x)$.
3. Si $b(x) \mid a(x)$ y $a(x) \mid b(x)$, entonces existe una unidad $d \in K[x]$ tal que $a(x) = d \cdot b(x)$.

La definición de máximo común divisor de dos números enteros hace uso del orden en los enteros. Tal definición no tiene sentido en dominios enteros como $K[x]$ que, en general, no son ordenados. Sin embargo, las condiciones que caracterizan al máximo común divisor en los enteros y que no usan el orden de éstos, sino la definición de divisor, tienen sentido en cualquier dominio entero.

Definicion 19 *Sean $a(x)$ y $b(x)$ dos polinomios en $K[x]$ tales que alguno es distinto de 0. Un polinomio $d(x) \in K[x]$ es un máximo común divisor de $a(x)$ y $b(x)$ si*

1. $d(x) \mid a(x) \quad y \quad d(x) \mid b(x)$.
2. *Si $c(x) \in K[x]$ es tal que $c(x) \mid a(x)$ y $c(x) \mid b(x)$, entonces $c(x) \mid d(x)$.*

Se sigue de la proposición (24, (1)) que si $d(x)$ es un máximo común divisor de $a(x)$ y $b(x)$ también lo es $c \cdot d(x)$, donde $c \neq 0$ es un elemento de K. Así, el máximo común divisor de dos polinomios no es único. Por otra parte, no es claro que dos polinomios tengan necesariamente un máximo común divisor. Más adelante veremos que sí, y no solamente que existe, sino que podemos hablar de unicidad en el caso que sea mónico. Para esto, las siguiente observación y el lema que le sigue nos serán de gran utilidad.

Observacion 6 *Recordemos que, un polinomio se llama mónico si su coeficiente principal es 1. Si $g(x) = b_n x^n + b_{n-1}x^{n-1} + \ldots + b_1 x + b_0 \in K[x]$ es un polinomio de grado n, es decir $b_n \neq 0$, entonces el polinomio $f(x) = b_n^{-1} \cdot g(x)$ es mónico y asociado a $g(x)$. Además, este polinomio $g(x)$ es único con esta propiedad, es decir, cada polinomio distinto de cero tiene un único polinomio mónico asociado.*

Definicion 20 *El polinomio $f(x)$ de la observación anterior se llama **polinomio mónico asociado a** $g(x)$.*

Lema 25 *Si $a(x), b(x), q(x)$ y $r(x)$ son polinomios en $K[x]$ tales que $b(x) \neq 0$ y $a(x) = b(x)q(x) + r(x)$, entonces $d(x)$ es un máximo común divisor de $a(x)$ y $b(x)$ si y sólo si $d(x)$ es un máximo común divisor de $b(x)$ y $r(x)$.*

Demostración:

Supongamos que $s(x)$ es un divisor común de $a(x)$ y $b(x)$, es decir, $s(x) \mid a(x)$ y $s(x) \mid b(x)$. Como $r(x) = a(x) - b(x) \cdot q(x)$, por la proposición (24, (5)) $s(x) \mid r(x)$.

Análogamente todo divisor común de $b(x)$ y $r(x)$ es divisor común de $a(x)$ y $b(x)$.

Por lo tanto, el conjunto de divisores comunes de $a(x)$ y $b(x)$ es igual al conjunto de divisores comunes de $b(x)$ y $r(x)$ de donde se obtiene el resultado deseado. ■

Teorema 26 *Sean $a(x), b(x)$ polinomios en $K[x]$. Si alguno de ellos es distinto de cero, entonces existe un único polinomio mónico $d(x) \in K[x]$ que es un máximo común divisor de $a(x)$ y $b(x)$. Más aún, $d(x) = g(x)a(x) + h(x)b(x)$ para algunos polinomios $g(x)$ y $h(x)$ en $K[x]$.*

Demostración:

Existencia. Supongamos que $a(x) = 0$. Entonces $b(x) \neq 0$ y el polinomio mónico asociado a $b(x)$ es un máximo común divisor de $a(x)$ y $b(x)$. Análogamente, si $b(x) = 0$, entonces el polinomio mónico asociado a $a(x)$ es un máximo común divisor de $a(x)$ y $b(x)$. En ambos casos, este máximo común divisor mónico puede expresarse en la forma $g(x) \cdot a(x) + h(x) \cdot b(x)$, de hecho, con $g(x)$ y $h(x)$ polinomios constantes.

Ahora supongamos que $a(x) \neq 0$ y $b(x) \neq 0$. Probaremos la existencia de $d(x)$ por inducción sobre $min\{gr(a(x)), gr(b(x))\}$.

Si $min\{gr(a(x)), gr(b(x))\} = 0$, entonces $a(x)$ o $b(x)$ es un polinomio constante distinto de cero, por lo que sus únicos divisores comunes son las constantes diferentes de cero, y entonces 1 es un máximo común divisor mónico de $a(x)$ y $b\,(x)$. Más aún, si $a(x) = a \in K - \{0\}$, entonces $1 = a^{-1} \cdot a + 0 \cdot b(x)$, y si $b(x) = b \in K - \{0\}$, entonces $1 = 0 \cdot a(x) + b^{-1}b$.

Supongamos ahora que si $s(x)$ y $t(x)$ son polinomios tales que $min\{gr(s(x)), gr(t(x))\} < n$ y $n > 1$, entonces $s(x)$ y $t(x)$ tienen un máximo común divisor mónico $d(x)$, que puede expresarse en la forma $d(x) = e(x)s(x) + f(x)t(x)$, para algunos $e(x), f(x)$ en $K[x]$.

Sea $n = gr(b(x)) \leq gr(a(x))$. (La prueba es similar si $n = gr(a(x)) \leq gr(b(x))$.

Por el Algoritmo de la División, $a(x) = b(x)q(x) + r(x)$ con $r(x) = 0$ o $gr(r(x)) < gr(b(x))$.

Si $r(x) = 0$, entonces $b(x) | a\,(x)$ y se sigue directamente de la definición que el máximo común divisor de $a(x)$ y $b(x)$ es el polinomio mónico asociado a $b(x)$. Este polinomio se puede expresar como $g(x)a(x) + h(x)b\,(x)$, tomando $g(x) = 0$ y $h(x)$ el inverso del coeficiente principal de $b\,(x)$.

Consideremos ahora el caso en que $r(x) \neq 0$. Entonces $min\{gr(r(x)), gr(b(x))\} < min\{gr(a(x)), gr(b(x))\} = n$.

Así, por hipótesis de inducción, $r(x)$ y $b(x)$ tienen un máximo común divisor mónico $d(x)$, que puede escribirse en la forma $d(x) = e(x)r(x) + f(x)b(x)$, con $e(x)$ y $f(x)$ en $K[x]$. Por el lema anterior, $d(x)$ es un máximo común divisor de $a(x)$ y $b(x)$, más aún, $d(x) = g(x)a(x) + h(x)b(x)$ tomando $g(x) = e(x)$ y $h(x) = f(x) - e(x)q(x)$.

Unicidad.. Sean $d(x)$ y $d_1(x)$ máximos comunes divisores mónicos de $a(x)$ y $b(x)$, entonces como $d(x)|a(x)$ y $d(x)|b(x)$ se tiene que $d(x)|d_1(x)$ y análogamente $d_1(x)|d(x)$, es decir, $d(x) = cd_1(x)$ para algún $c \in K$. Por ser $d(x)$ y $d_1(x)$ mónicos, $c = 1$ y por lo tanto $d(x) = d_1(x)$. ■

Este resultado permite hablar de **el máximo común divisor mónico** de dos polinomios $a(x)$ y $b(x) \in K[x]$ tales que alguno es distinto de cero. Denotamos a este único máximo común divisor mónico por la expresión

$$(a(x); b(x)) .$$

Observacion 7 *El máximo común divisor de dos polinomios $a(x)$ y $b(x)$ es una combinación lineal de $a(x)$ y $b(x)$ de grado mínimo, es decir, si $d(x) = (a(x); b(x))$ y $c(x) = m(x)a(x) + n(x)b(x)$, entonces $gr(d(x)) \leq gr(c(x))$.*

La prueba que hemos visto proporciona un método práctico para hallar el máximo común divisor de dos polinomios $a(x)$ y $b(x)$:

- Si $b(x) = 0$, entonces $(a(x); b(x))$ es el polinomio mónico asociado a $a(x)$.
- Si $a(x) = 0$, entonces $(a(x); b(x))$ es el polinomio mónico asociado a $b(x)$.
- Si $a(x) \neq 0$ y $b(x) \neq 0$, y $gr(b(x)) \leq gr(a(x))$, entonces $(a(x); b(x)) = (b(x), r(x))$, donde $r(x)$ es el residuo que se obtiene al dividir a $a(x)$ por $b(x)$. En consecuencia, aplicando repetidamente el Algoritmo de la División, podemos encontrar el máximo común divisor de $a(x)$ y $b(x)$.

Como se puede observar, en general, si en un dominio entero es válido el Algoritmo de la División, se puede asegurar la existencia de un máximo común divisor de dos elementos cualesquiera.

Ejemplo 11 *Sean $a(x) = x^5+3x^4+5x^3+4x^2+4x+1$ y $b(x) = x^5+2x^4+3x^3+2x^2+2x$. Entonces, por el uso repetido del Algoritmo de la División se tiene:*

$$\begin{aligned} x^5+3x^4+5x^3+4x^2+4x+1 &= 1(x^5+2x^4+3x^3+2x^2+2x)+(x^4+2x^3+2x^2+2x+1) \\ x^5+2x^4+3x^3+2x^2+2x &= x(x^4+2x^3+2x^2+2x+1)+(x^3+x) \\ x^4+2x^3+2x^2+2x+1 &= (x+2)(x^3+x)+(x^2+1) \\ x^3+x &= x(x^2+1)+0 \end{aligned}$$

luego,

$$\begin{aligned} & (x^5+3x^4+5x^3+4x^2+4x+1; x^5+2x^4+3x^3+2x^2+2x) \\ = \; & (x^5+2x^4+3x^3+2x^2+2x; x^4+2x^3+2x^2+2x+1) \\ = \; & (x^4+2x^3+2x^2+2x+1; x^3+x) \\ = \; & (x^3+x; x^2+1) = (x^2+1, 0) = x^2+1. \end{aligned}$$

El método empleado en el ejemplo anterior para obtener el máximo común divisor de dos polinomios se conoce como **Algoritmo de Euclides** porque es similar al proceso para obtener el máximo común divisor de dos enteros..

En términos generales, el proceso consiste en considerar las ecuaciones sucesivas:

$$\begin{aligned} a(x) &= q_1(x)b(x)+r_1(x) \\ b(x) &= q_2(x)r_1(x)+r_2(x) \\ r_1(x) &= q_3(x)r_2(x)+r_3(x) \\ &\vdots \\ r_{n-2}(x) &= q_n(x)r_{n-1}(x)+r_n(x) \\ r_{n-1}(x) &= q_{n+1}(x)r_n(x)+0 \end{aligned}$$

donde $r_1(x), r_2(x), ..., r_n(x)$ no son cero, $gr(b(x)) > gr(r_1(x)) > ... > gr(r_n(x))$. De esta manera se sigue, del teorema anterior, que el polinomio mónico asociado a $r_n(x)$ es el máximo común divisor mónico de $a(x)$ y $b(x)$, de hecho,

$$(a(x); b(x)) = (b(x); r_1(x)) = ... = (r_{n-1}(x); r_n(x) = (r_n(x), 0)$$

y $(r_n(x), 0)$ es el polinomio mónico asociado con $r_n(x)$.

Definicion 21 *Dos polinomios $a(x)$ y $b(x)$ son **primos relativos** si su máximo común divisor mónico es* 1.

Teorema 27 *Sean $a(x), b(x)$ y $c(x)$ polinomios en $K[x]$, tales que $a(x)$ y $b(x)$ son primos relativos y $a(x)|b(x) \cdot c(x)$, entonces $a(x)|c(x)$.*

La demostración se deja como ejercicio para el lector.

2.3.2 Teorema de factorización única para polinomios

De acuerdo al Teorema Fundamental de la Aritmética, cada número natural puede escribirse, de manera única, como producto de números primos. Nuestra propósito es demostrar la validez de un teorema similar en $K[x]$, donde K es un campo.

En primer lugar debemos definir en $K[x]$ un concepto análogo al de número primo en $\mathbb{Z}$.

Definicion 22 *Sea $p(x)$ un polinomio en $K[x]$ de grado positivo. Decimos que $p(x)$ es **irreducible** en $K[x]$ si siempre que $p(x) = f(x) \cdot g(x)$ con $f(x), g(x) \in K[x]$ se tiene que $f(x)$ es unidad o $g(x)$ es unidad, es decir, si los únicos divisores de $p(x)$ son las constantes y los asociados a $p(x)$.*

*Si $p(x) \in K[x]$ es de grado positivo y no es irreducible en $K[x]$, diremos que es **reducible**.*

Observacion 8 *Un polinomio $a(x) \in K[x]$ de grado positivo es reducible si y sólo si existe $b(x) \in K[x]$ tal que $b(x)|a(x)$ y $0 < gr(b(x)) < gr(a(x))$.*

Dado que la definición anterior se aplica sólo a polinomios de grado positivo, los polinomios constantes no son reducibles ni irreducibles. Estos polinomios juegan el mismo papel en $K[x]$ que los enteros 1 y -1 en $\mathbb{Z}$.

Es importante hacer notar que la irreducibilidad de un polinomio es relativa a un campo particular K. Esto es, un polinomio que es irreducible en $K[x]$ puede ser reducible en $F[x]$ para algún campo F que contenga a K.

Ejemplo 12 *El polinomio $x^2 - 3$ es irreducible en $\mathbb{Q}[x]$. Supongamos que no, entonces $x^2 - 3$ se puede escribir como el producto de dos polinomios de primer grado en $\mathbb{Q}[x]$, es decir,*

$$x^2 - 3 = (ax + b)(cx + d) = (ac)x^2 + (ad + bc)x + bd$$

donde a, b, c y d son números racionales.

Esto implica que $ac = 1, ad + bc = 0$, y $bd = -3$. Así que, $c = \dfrac{1}{a}, d = -\dfrac{3}{b}$ y sustituyendo en $ad + bc = 0$, obtenemos

$$0 = -\frac{3a}{b} + \frac{b}{a} = \frac{-3a^2 + b^2}{ab},$$

es decir,

$$-3a^2 + b^2 = 0$$

y entonces $\left(\dfrac{b}{a}\right)^2 = 3$. Sin embargo, $\sqrt{3}$ no es un número racional, por lo que se concluye que, $x^2 - 3$ es irreducible en $\mathbb{Q}[x]$. Por otro lado,

$$x^2 - 3 = \left(x - \sqrt{3}\right)\left(x + \sqrt{3}\right),$$

esto es, $x^2 - 3$ *es reducible en* $\mathbb{R}[x]$.

Ejemplo 13 *Cualquier polinomio de grado 1,* $ax + b, a \neq 0$, *con coeficientes en un campo* K, *es irreducible en* $K[x]$. *De hecho* $ax+b = f(x)g(x)$ *con* $0 < gr(f(x)) < 1$ *es imposible.*

Nos proponemos demostrar que cada polinomio de grado positivo en $K[x]$ puede expresarse como producto de polinomios mónicos irreducibles en $K[x]$ y un elemento de K.

Más aún, que esta factorización es única excepto posiblemente por el orden de los factores. Para esto veremos antes dos lemas, que se prueban en forma similar a los resultados correspondientes para números primos en los números enteros. Omitiremos su demostración.

Lema 28 *Si* $p(x)$ *es irreducible en* $K[x]$ *y* $f(x) \in K[x]$, *entonces* $p(x)|f(x)$ *o* $p(x)$ *y* $f(x)$ *son primos relativos.*

Lema 29 *Si* $p(x)$ *es irreducible en* $K[x]$, *y* $p(x)$ *divide al producto* $a_1(x)\cdot a_2(x)\cdot ...\cdot a_n(x)$ *de polinomios en* $K[x]$, *entonces* $p(x)$ *divide al menos a uno de los factores, es decir,* $p(x)|a_i(x)$ *para alguna* $i = 1, ...n$.

Teorema 30 ***Teorema de Factorización Única en*** $K[x]$. *Cada polinomio* $a(x) \in K[x]$ *de grado positivo se puede escribir como producto de un elemento distinto de cero de* K *y polinomios mónicos irreducibles en* $K[x]$. *Excepto en el orden de los factores, la expresión de* $a(x)$ *en esta forma es única.*

Demostración:

Ambas partes del teorema se prueban por inducción sobre el grado de $a(x)$.

Existencia. Supongamos que $gr(a(x)) = 1$, es decir, $a(x) = bx + c$, donde $b, c \in K$ y $b \neq 0$, entonces $a(x) = b \cdot \left(x - b^{-1}c\right)$ y como $x + b^{-1}c$ es un polinomio mónico irreducible en $K[x]$ y $b \neq 0$ en K, queda probado. Supongamos que $a(x)$ es un polinomio de grado $n > 1$ y que cada polinomio de grado m, con $1 \leq m < n$, puede expresarse en la forma $cp_1(x)p_2(x)...p_k(x)$, con $c \neq 0$ en K y los $p_i(x)$ polinomio mónicos irreducibles en $K[x]$. Si $a(x)$ es irreducible y $b(x)$ es su polinomio mónico asociado, entonces $b(x)$ es irreducible y $a(x) = c \cdot b(x)$ con $c \neq 0$ en K, por lo que se tiene la expresión deseada.

Si $a(x)$ no es irreducible, entonces $a(x) = b(x) \cdot c(x)$, donde $b(x)$ y $c(x)$ son polinomios de $K[x]$ que satisfacen $1 \leq gr\,(b(x)) < gr\,(a(x))$ y $1 \leq gr\,(c(x)) < gr\,(a(x))$. Por hipótesis de inducción

$$b(x) = c_1 p_1(x) p_2(x) ... p_r(x)$$

y

$$c(x) = c_2 q_1(x) q_2(x) ... q_s(x)$$

donde c_1 y c_2 son elementos distintos de cero en K, y los $p_i(x)$ y $q_j(x)$ son polinomios mónicos irreducibles. Así se tiene que,

$$a(x) = b(x) \cdot c(x) = (c_1 \cdot c_2) \cdot p_1(x) p_2(x) ... p_r(x) q_1(x) q_2(x) ... q_s(x).$$

Unicidad. Para probar la unicidad de la descomposición, supongamos que $gr(a(x)) = 1$ y que $a(x) = a_1(x + b_1) = a_2(x + b_2)$ con $a_1 \neq 0$ y $a_2 \neq 0$ entonces $a_1 = a_2$ y $a_1 b_1 = a_2 b_2$ y multiplicando la última ecuación por $a_1^{-1} = a_2^{-2}$, obtenemos $b_1 = b_2$, Por lo tanto, cualesquiera dos factorizaciones de $a(x)$ son idénticas. Ahora, supongamos que $a(x)$ tiene grado $n > 1$, y que se tiene unicidad en la descomposición de los polinomios de grado menor que n. Sean

$$a(x) = c_1 p_1(x) \cdot p_2(x) \cdot ... \cdot p_r(x) = c_2 q_1(x) \cdot q_2(x) \cdot ... \cdot q_s(x)$$

factorizaciones de $a(x)$ como producto de un elemento de K y polinomios mónicos irreducibles. Como los $p_i(x)$ y $q_j(x)$ son polinomios mónicos, el coeficiente del término de mayor grado de $a(x)$ es c_1 y c_2, esto es, $c_1 = c_2$. De aquí se tiene que:

$$p_1(x) \cdot p_2(x) \cdot ... \cdot p_r(x) = q_1(x) \cdot q_2(x) \cdot ... \cdot q_s(x)$$

lo cual implica que $p_1(x) | q_1(x) \cdot q_2(x) \cdot ... \cdot q_s(x)$. Como $p_1(x)$ es irreducible se sigue del lema (29) que $p_1(x)$ divide a $q_j(x)$ para alguna $j = 1, ..., s$; como $q_j(x)$ es irreducible y $p_1(x)$ no es constante, se tiene que $p_1(x) = c q_j(x)$; pero además, $p_1(x)$ y $q_j(x)$ son polinomios mónicos, de donde $c = 1$ y $p_1(x) = q_j(x)$. Si $r = 1$, entonces $a(x)$ es irreducible, así que $s = j = 1$. En este caso, las factorizaciones $a(x) = c_1 p_1(x) = c_2 p_2(x)$ son idénticas. De otra manera, $p_1(x)$ puede cancelarse de la expresión anterior para obtener

$$p_2(x) \cdot \ldots \cdot p_r(x) = q_1(x) \cdot q_2(x) \cdot \ldots \cdot q_{j-1}(x) \cdot q_{j+1}(x) \cdot \ldots \cdot q_s(x)$$

como $n = gr(p_1(x)) + gr(p_2(x) ... p_r(x))$ y $gr(p_1(x)) \geq 1$, se tiene que $gr(p_2(x) ... p_r(x)) < n$.

Por hipótesis de inducción, los polinomios $p_2(x), ..., p_r(x)$ son exactamente los polinomios $q_1(x), q_2(x), \ldots, q_{j-1}(x), q_{j+1}(x), \ldots, q_s(x)$ en algún orden. Por lo tanto, las dos factorizaciones de $a(x)$ son la misma, excepto por el orden de los factores. ■

Ejercicios 2.3.2

1. Pruebe (2) y (5) de la proposición (24)
2. Pruebe la afirmación de la observación (6).

3. Halle el máximo común divisor mónico de cada uno de los siguientes pares de polinomios y expréselo en la forma

$$g(x) \cdot a(x) + h(x) \cdot b(x)$$

   a. $x^4 - x^3 + 3x^2 - 2x + 2$ y $x^3 + x^2 + 2x + 2$ en $\mathbb{Q}[x]$.

   b. $x^5 - x^4 - 6x^3 - 2x^2 + 5x + 3$ y $x^3 - 3x - 2$ en $\mathbb{Q}[x]$.

   c. $x^6 - x^5 + 2x^4 - 3x^3 + x^2 - 2x + 2$ y $x^5 - x^3 - x^2 + 1$ en $\mathbb{Q}[x]$.

   d. $x^2 - 2$ y $x^2 - (\sqrt{2} + \sqrt{3})x + \sqrt{6}$ en $\mathbb{R}[x]$.

   e. $x^4 - 4ix + 3$ y $x^3 - i$ en $\mathbb{C}[x]$.

   f. $4x^4 - 4x^3 + 5x^2 - 4x + 1$ y $8x^3 - 6x^2 + 5x - 2$ en $\mathbb{Q}[x]$.

4. Pruebe que $a(x)$ y $b(x)$ son primos relativos si y sólo si existen polinomios $f(x)$ y $g(x)$ en $K[x]$ tales que

$$f(x)a(x) + g(x)b(x) = 1.$$

5. Demuestre el teorema (27).

6. Sean $a(x)$ y $b(x)$ en $\mathbb{Z}[x]$. Pruebe que $a(x)$ y $b(x)$ son asociados si y sólo si $b(x) = a(x)$ o $b(x) = -a(x)$.

7. Sean $a(x), b(x)$ y $c(x)$ polinomios en $K[x]$, con $a(x) \neq 0, b(x) \neq 0$ y $a(x)$ mónico. Pruebe que,

$$(a(x) \cdot b(x); a(x) \cdot c(x)) = a(x) \cdot (b(x); c(x)).$$

8. Un **mínimo común múltiplo** de dos polinomios distintos de cero $a(x)$ y $b(x)$ en $K[x]$ es un polinomio $m(x)$ en $K[x]$ que satisface:

   i) $a(x)|m(x)$ y $b(x)|m(x)$.

   ii) Si $l(x)$ es cualquier otro polinomio en $K[x]$, tal que $a(x)|l(x)$ y $b(x)|l(x)$, entonces $m(x)|l(x)$.

   Pruebe que si $a(x)$ y $b(x)$ son polinomios distintos de cero en $K[x]$, entonces el cociente de dividir a $a(x) \cdot b(x)$ entre $(a(x); b(x))$ es un mínimo común múltiplo de $a(x)$ y $b(x)$.

9. Halle un mínimo común múltiplo para los siguientes pares de polinomios.

   a. $x^4 - x^3 + 3x^2 - 2x + 2$ y $x^3 + x^2 + 2x + 2$.

   b. $x^3 - 2x + 1$ y $x^2 + 1$.

10. Pruebe la observación (8).

11. Pruebe el lema (28).

12. Pruebe el lema (29).

13. Pruebe que si $p(x)$ es irreducible en $K[x]$ y $c \neq 0$ en K, entonces $c \cdot p(x)$ es irreducible en $K[x]$.

14. Determine cuáles de los siguientes polinomios son irreducibles en $\mathbb{Q}[x]$. Aquellos que no lo sean expréselos como producto de irreducibles en $\mathbb{Q}[x]$.

a. $x^3 - 2$.

b. $x^3 + 2x^2 + 2x + 1$.

c. $x^4 + 1$.

d. $x^4 - x^2 - 1$.

e. $2x + 4$.

15. ¿Cuáles de los polinomios del problema 14 son irreducibles en $\mathbb{R}[x]$. Aquellos que no lo sean expréselos como producto de irreducibles en $\mathbb{R}[x]$.

2.4 RAÍCES DE POLINOMIOS

En este tema, nos ocuparemos nuevamente del estudio de las ecuaciones. Veremos cuándo un número es solución de una ecuación, así como algunos criterios que nos permiten asegurar si la ecuación tiene o no solución, y algunas técnicas o algoritmos para resolverlas

2.4.1 Funciones Polinomiales

En la sección (2.1), identificamos el anillo de polinomios $K[x]$ con el anillo de funciones polinomiales P_K a través de una función que, como se dijo, preserva las operaciones. Además, se mencionó que dicha función es siempre suprayectiva y en esta parte probaremos que, cuando los coeficientes se encuentran en un campo infinito, también es inyectiva y de aquí que, en este caso, la correspondencia entre polinomios y funciones polinomiales resulta biyectiva.

Vale la pena aclarar que el tratamiento de lo anterior se hace sobre polinomios con coeficientes en un campo, sin embargo, se da la biyección aún cuando los coeficientes estén en un dominio entero siempre y cuando éste sea infinito.

Una de la motivaciones para el estudio de números complejos, fue la de construir un campo que contuviera a los reales y en el cual existieran soluciones a ecuaciones del tipo $x^2 + a = 0$ con $a > 0$. En el estudio de raíces de polinomios la idea de construir un campo mayor que el dado es muy usada. Aquí haremos uso de la existencia de estos campos (pero no se demostrará), es decir, cuando consideremos un campo hablaremos también de extensiones de este campo, esto es, campos mayores que contienen al campo dado como subcampo[5]. Por ejemplo, si consideramos los campos $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, $\mathbb{R}$ es una extensión de $\mathbb{Q}$ y $\mathbb{C}$ una extensión de $\mathbb{R}$ y de $\mathbb{Q}$.

Definicion 23 *Sean K un campo, L una extensión de K, $\alpha \in L$ y*

[5] K es un subcampo de L si con las operaciones de L, K es un campo.

$a(x) = a_0 + a_1x + ... + a_nx^n \in K[x]$. ***El valor de*** $a(x)$ *en* α *es la expresión* $a(\alpha) = a_0 + a_1\alpha + ... + a_n\alpha^n$, *y se dice que* $a(\alpha)$ *se obtiene de sustituir* x *por* α *en* $a(x)$.

Nótese que el valor de $a(x)$ en α es un elemento de L y de aquí que, por las propiedades de campo de las operaciones en L, se tiene la siguiente

Proposicion 31 *Sean* K *un campo y* L *una extensión de* K. *Supongamos que* $a(x), b(x)$ *y* $f(x)$ *están en* $K[x]$ *y* $\alpha \in L$.

1. *Si* $f(x) = a(x) + b(x)$, *entonces* $f(\alpha) = a(\alpha) + b(\alpha)$.
2. *Si* $f(x) = a(x) \cdot b(x)$, *entonces* $f(\alpha) = a(\alpha) \cdot b(\alpha)$.
3. *Si* $f(x) = a_0 \in K$, *entonces* $f(\alpha) = a_0$.
4. *Si* $f(x) = a(b(x))$, *es decir, si* $f(x)$ *es el polinomio que se obtiene al sustituir* x *por* $b(x)$ *en* $a(x)$, *entonces,* $f(\alpha) = a(b(\alpha))$.

Demostración:

Solamente probaremos (1) y las demás quedan como ejercicio para el lector.

1. Si $a(x) = a_0 + a_1x + ... + a_nx^n$ y $b(x) = b_0 + b_1x + ... + b_nx^n$, entonces

$$f(x) = a(x) + b(x) = (a_0 + b_0) + (a_1 + b_1)x + ...(a_n + b_n)x^n,$$

de aquí que

$$\begin{aligned} f(\alpha) &= (a_0 + b_0) + (a_1 + b_1)\alpha + ...(a_n + b_n)\alpha^n \\ &= a_0 + b_0 + a_1\alpha + b_1\alpha + ... + a_n\alpha^n + b_n\alpha^n \\ &= (a_0 + a_1\alpha + ... + a_n\alpha^n) + (b_0 + b_1\alpha + ... + b_n\alpha^n) \\ &= a(\alpha) + b(\alpha). \end{aligned}$$

4. Esta propiedad se obtiene de (1), (2) y (3), por inducción sobre $gr(a(x))$. ■

Observacion 9 *Es importante observar que la validez de (2) en la proposición anterior depende fuertemente de la conmutatividad del producto en* L, *es decir, si* L *fuera un anillo con* 1 *donde todos sus elementos distintos de cero tuvieran inverso mutliplicativo, pero no fuera conmutativo,*[6] *el resultado no sería cierto en general.*

Definicion 24 *Sea* K *un campo y* L *una extensión de* K. *Sea* $a(x) \in K[x]$. *Un elemento* $\alpha \in L$ *tal que* $a(\alpha) = 0$, *se llama* ***raíz*** *de* $a(x)$.

[6] Un anillo con estas características se llama **anillo con división.**

Ejemplo 14 *Si* $a(x) = x^3 + x^2 - 2x - 2 \in \mathbb{Q}[x]$*, entonces*

1. -1 *es raíz de* $a(x)$.
2. $\sqrt{2}$ *es raíz de* $a(x)$.
3. $-\sqrt{2}$ *es raíz de* $a(x)$.

Es claro que el problema de resolver una ecuación de la forma $a_n x^n + a_{n-1}x^{n-1} + ... + a_0 = 0$ es el mismo que el de encontrar todas las raíces del polinomio $a(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_0$. Del ejemplo anterior, deducimos que $-1, \sqrt{2}, -\sqrt{2}$ son soluciones de la ecuación $x^3 + x^2 - 2x - 2 = 0$.

Teorema 32 ***Teorema del Residuo****. Sean* K *un campo y* L *una extensión de* K*. Si* $\alpha \in L$*, entonces el residuo al dividir a* $a(x)$ *entre* $(x-\alpha)$*, es* $a(\alpha)$*,es decir, existe un único polinomio* $q(x) \in L[x]$ *tal que*

$$a(x) = (x - \alpha)q(x) + a(\alpha).$$

Demostración:

Por el Algoritmo de la División, existen $q(x), r(x) \in L[x]$ únicos, tales que

$$a(x) = (x - \alpha)q(x) + r(x)$$

con $r(x) = 0$ o $gr(r(x)) < gr(x - \alpha) = 1$.

En cualquiera de los dos casos mencionados resulta que $r(x) = r_0 \in L$.

Por otra parte, por la proposición (31),

$$a(\alpha) = (\alpha - \alpha)q(\alpha) + r(\alpha) = r(\alpha).$$

y así queda demostrado el teorema. ■

El siguiente teorema nos dice cuándo un elemento de un campo es raíz de un polinomio, y resulta como corolario del teorema anterior.

Teorema 33 ***Teorema del Factor.*** *Sean* K *un campo y* L *una extensión de* K*. Sea* $a(x) \in K[x]$*. Un elemento* $\alpha \in L$ *es raíz de* $a(x)$ *si y sólo si* $(x - \alpha)$ *divide a* $a(x)$*.*

Demostración:
Ejercicio para el lector. ■

Este teorema es útil cuando quiere escribirse a un polinomio como producto de irreducibles, por ejemplo, como -1 es raíz de $a(x) = x^3 + x^2 - 2x - 2$, $(x+1)$ debe dividir a $a(x)$. Al hacer la división obtenemos, $a(x) = (x^2 - 2)(x + 1)$; como $(x^2 - 2)$ y $(x + 1)$ son irreducibles en $\mathbb{Q}[x]$, ésta es la factorización de $a(x)$ en $\mathbb{Q}[x]$.

Sin embargo, $\sqrt{2}$es una raíz de $x^2 - 2$, por lo que $x - \sqrt{2}$ debe dividir a $x^2 - 2$ en $\mathbb{R}[x]$ y así, $a(x) = (x - \sqrt{2})(x + \sqrt{2})(x + 1)$ es la factorización de $a(x)$ en $\mathbb{R}[x]$.

Hemos visto en el Teorema del Factor que si $a(x) \in K[x]$, $a(x) \neq 0$ y $\alpha \in L$ es raíz de $a(x)$, entonces $(x-\alpha)|a(x)$, es decir, $a(x) = (x-\alpha)b(x)$ con $b(x) \in L[x]$; análogamente si α es raíz de $b(x)$, $b(x) = (x - \alpha)c(x)$, con $c(x) \in L[x]$ y de aquí que $a(x) = (x - \alpha)^2 c(x)$, esto es, $(x - \alpha)^2 | a(x)$; si α es raíz de $c(x)$ hacemos el mismo razonamiento y resulta que $(x - \alpha)^3 | a(x)$. Así, en un número finito de pasos (a lo más en $gr(a(x))$ pasos) podemos encontrar un número $m \leq gr(a(x))$ tal que $(x - \alpha)^m | a(x)$ y $(x - \alpha)^{m+1} \nmid a(x)$. Este número lo nombraremos según la siguiente

Definicion 25 *Sea $a(x) \in K[x]$, $a(x) \neq 0$. **Una raíz** $\alpha \in L$ de $a(x)$ se dice que es **de multiplicidad** $m \geq 1$, si $(x - \alpha)^m | a(x)$ en $L[x]$ y $(x - \alpha)^{m+1} \nmid a(x)$ en $L[x]$. Si $m = 1$, se dice que α es una **raíz simple.***

Ejemplo 15 *El polinomio $a(x) = x^5 - 4x^4 + x^3 + 10x^2 - 4x - 8$ se puede escribir como $a(x) = (x - 2)^3(x + 1)^2$ y como 2 no es raíz de $(x + 1)^2$ y (-1) no es raíz de $(x - 2)^3$, se tiene que 2 es raíz de multiplicidad 3 de $a(x)$ y (-1) es raíz de multiplicidad 2.*

Ahora veremos que el número de raíces de un polinomio distinto de cero, es siempre finito.

Teorema 34 *Un polinomio $a(x)$ de grado $n \geq 1$, con coeficientes en un campo K tiene a lo más n raíces en cualquier extensión de K.*

Demostración:
Antes de iniciar la demostración del teorema contiene aclarar que una raíz de multiplicidad m se contará como si fueran m raíces.

Haremos la demostración por inducción sobre $gr(a(x))$.

Si $n = 1$, entonces $a(x) = a_1 x + a_0$, con $a_0, a_1 \in K$ y $a_1 \neq 0$, de aquí que $a(x) = a_1(x + a_1^{-1}a_0)$ y por lo tanto la única raíz de $a(x)$ es $\alpha = -a_1^{-1}a_0$.

Sea $a(x) \in K[x]$ tal que $gr(a(x)) = n > 1$ y supongamos que todo polinomio $b(x)$, de grado menor que n, con coeficientes en cualquier campo K', tiene a lo más $gr(b(x))$ raíces en cualquier extensión de K'.

Sea L una extensión de K. Si $a(x)$ no tiene raíces en L, entonces $a(x)$ tiene cero raíces en L y por lo tanto, a lo más n. Supongamos que $\alpha \in L$ es raíz de multiplicidad $m \geq 1$ de $a(x)$, entonces, por el teorema (33) y la definición (25), existe $b(x) \in L[x]$ tal que $a(x) = (x-\alpha)^m b(x)$ y $b(\alpha) \neq 0$, de aquí que $gr\,(b(x)) = n - m < n$ (proposición 20). Por hipótesis de inducción, $b(x)$ tiene a lo más $n-m$ raíces en cualquier extensión de L, en particular, tiene a lo más $n-m$ raíces en L.

Por otra parte, si $\beta \in L$ es una raíz de $a(x)$ distinta de α, se tiene que $0 = a(\beta) = (\beta-\alpha)^m b(\beta)$, lo cual implica que $b(\beta) = 0$, es decir, β es una raíz de $b(x)$, entonces $a(x)$ tiene a lo más $n-m$ raíces en L, distintas de α, y por lo tanto, tiene a lo más n raíces distintas en L. ■

Teorema 35 *Sea K un campo y sea $a(x) \in K[x]$ un polinomio distinto de cero. Si $\alpha_1, ..., \alpha_r$ son todas las raíces distintas de $a(x)$ en K, entonces*

$$a(x) = (x-\alpha_1)^{m_1}(x-\alpha_2)^{m_2}...(x-\alpha_r)^{m_r} b(x),$$

donde m_i es la multiplicidad de α_i, para $i = 1, ..., r$ y $b(x) \in K[x]$ es un polinomio distinto de cero que no tiene raíces en K.

Demostración:

Como $(x-\alpha_i)^{m_i} | a(x)$ (teorema 33) y $((x-\alpha_i)^{m_i}; (x-\alpha_j)^{m_j}) = 1$,[7] si $\alpha_i \neq \alpha_j$ se tiene que

$$a(x) = (x-\alpha_1)^{m_1}(x-\alpha_2)^{m_2}...(x-\alpha_r)^{m_r} b(x),$$

donde $b(x) \neq 0$ ya que $a(x) \neq 0$.

Por otra parte, si $\beta \in K$ es raíz de $b(x)$, entonces β es raíz de $a(x)$, de aquí que $\beta = \alpha_i$ para alguna $i = 1, ..., r$, de donde $(x-\alpha_i) | b(x)$ y por lo tanto $(x-\alpha_i)^{m_i+1} | b(x)$, lo cual no es posible ya que α_i es raíz de multiplicidad m_i de $a(x)$. Así, $b(x)$ no tiene raíces en K. ■

Corolario 36 *Sean K un campo y $a(x) \in K[x]$ un polinomio de grado n, con $n \geq 1$. Si $\alpha_1, ..., \alpha_n \in K$ son n raíces distintas de $a(x)$, entonces:*

$$a(x) = c(x-\alpha_1)(x-\alpha_2)...(x-\alpha_n), \quad \textit{con } c \in K.$$

La demostración queda como ejercicio para el lector. ■

Una consecuencia más del teorema (34) es la inyectividad de la función definida entre $K[x]$ y P_K cuando K es infinito ya que, si $a(x)$ y $b(x) \in K[x]$ son tales que $a(\alpha) = b(\alpha)$, para todo $\alpha \in K$, entonces $a(\alpha) - b(\alpha) = 0$, para todo $\alpha \in K$ y de aquí que si $c(x) = a(x) - b(x) \in K[x]$, entonces $c(\alpha) = 0$ para todo $\alpha \in K$; esto sólo puede ser

[7] (a;b) es el máximo común divisor de a y b

posible si $c(x) = 0$ ya que K es infinito y en caso contrario se tendría un polinomio distinto de cero en el que todo elemento de K es raíz, lo cual es una contradicción

Corolario 37 *Si K es un campo infinito, entonces existe una correspondencia biyectiva, que preserva las operaciones, entre $K[x]$ y P_K.*

Así, por el corolario anterior, el anillo $\mathbb{R}[x]$ se puede pensar como el anillo de funciones polinomiales de $\mathbb{R}$ en $\mathbb{R}$ ($P_{\mathbb{R}}$) y así, dar una interpretación geométrica del mismo.

Ejercicios 2.4.1

1. Sin hacer la división, encuentre el residuo al dividir:
   a. $x^3 + 2x - 4$ entre $x - 1$.
   b. $x^{25} + 14x^{17} + 24$ entre $x + 1$.
   c. $x^5 + 12x^4 + 13x^2 + x + 27$ entre $x + 3$.
2. Factorice completamente los siguientes polinomios en $\mathbb{C}[x]$.
   a. $x^2 + i\,x + 2$.
   b. $x^8 - 1$.
   c. $x^4 + x^2 + 1$.
   d. $x^4 - 2x^3 - 5x^2 - 2x + 24$.
   e. $x^3 - 2$.
   f. $x^3 - 5x^2 - 9x + 13$.
3. Sea $a(x) = x^n - 1$. Encuentre $a(\alpha)$ cuando α es:
   a. -1.
   b. i.
   c. $x + 1$.
   d. $x^n - 1$.
4. Encuentre todos los polinomios mónicos $f(x) \in \mathbb{C}[x]$ de grado cinco, tales que:
   a. i es raíz de multiplicidad 4 de $f(x)$.
   b. $0, 1, 2$ y 3 son raíces simples de $f(x)$.
   c. 1 e i son raíces de multiplicidad 2 de $f(x)$.
   d. i y $-i$ son raíces simples de $f(x)$, y -1 es raíz de multiplicidad dos.

5. Pruebe que la suma de multiplicidades de las raíces de un polinomio $a(x) \in K[x]$ es menor o igual que el grado de $a(x)$.
6. Pruebe que si $a(x)$ y $b(x)$ son polinomios de grado menor que n en $K[x]$ y si $a(\alpha_i) = b(\alpha_i)$ para $i = 1, 2, ..., n$, donde $\alpha_1, \alpha_2, ..., \alpha_n$ son n elementos distintos de K, entonces $a(x) = b(x)$ en $K[x]$.
7. Sea $f(x) = \alpha_n x^n + ... + \alpha_1 x + \alpha_0 \in \mathbb{C}[x]$. Definimos su conjugado complejo: $\overline{f}(x) = \overline{\alpha_n} x^n + ... + \overline{\alpha_1} x + \overline{\alpha_0}$, donde $\overline{\alpha_i}$ es el conjugado complejo de α_i. Demostrar que si $f(x), g(x) \in K[x]$, entonces $\overline{(f+g)}(x) = \overline{f}(x) + \overline{g}(x)$, $\overline{f\,g}(x) = \overline{f}(x)\,\overline{g}(x)$ y $\overline{\beta f}(x) = \overline{\beta}(\overline{f}(x))$, para toda $\beta \in \mathbb{C}$.
8. Pruebe que si $f(x) \in \mathbb{R}[x]$ y $\alpha \in \mathbb{C}$ es raíz de $f(x)$ entonces $\overline{\alpha}$ es raíz de $f(x)$.
9. Pruebe que si $f(x) \in \mathbb{R}[x]$ y $\alpha \in \mathbb{C}$ es raíz de multiplicidad m de $f(x)$ entonces $\overline{\alpha}$ también lo es.
10. Pruebe que si $f(x) = ax^2 + bx + c \in K[x]$, entonces es cierta una y sólo una de las tres afirmaciones siguientes:
    a. $f(x)$ tiene dos raíces distintas en K.
    b. $f(x)$ tiene una raíz de multiplicidad dos en K.
    c. $f(x)$ es irreducible en $K[x]$.

2.4.2 Interpretación Geométrica de las Raíces de un Polinomio en $\mathbb{R}[x]$

En vista del último corolario del subtema anterior, nombraremos indistintamente polinomios con coeficientes reales,a los elementos de $\mathbb{R}[\curvearrowleft]$ y a las funciones polinomiales de $\mathbb{R}$ en $\mathbb{R}$ con coeficientes en $\mathbb{R}$.

Sea $a(x) \in \mathbb{R}[x]$. Como vimos anteriormente, un elemento $\alpha \in \mathbb{R}$ es raíz de $a(x)$ si $a(\alpha) = 0$, es decir, si el valor de la función correspondiente $a : \mathbb{R} \to \mathbb{R}$ en α es cero. Esto significa, geométricamente, que el punto de coordenadas $(\alpha, 0)$ pertenece a la gráfica de la función. Así, observamos que cada número real que es raíz del polinomio $a(x)$ nos da una intersección de su gráfica con el eje de las abscisas, de aquí que la gráfica de $a(x)$ tendrá tantas intersecciones con dicho eje como raíces distintas en $\mathbb{R}$. También se deduce que si $a(x)$ no tiene raíces en $\mathbb{R}$, su gráfica no intersecta al eje de las abscisas.

Con base en esto, analizaremos los ejemplos dados en la sección 2.1:

1. $a(x) = 5$ es un polinomios constante distinto de cero por lo que no tiene raíces y por lo tanto su gráfica no intersecta al eje de las abscisas (fig. pág. 39).

2. $a(x) = 3 + x$, su única raíz es -3, por lo que su gráfica intersecta en $(-3, 0)$ al eje de las abscisas (fig. pág. 39).

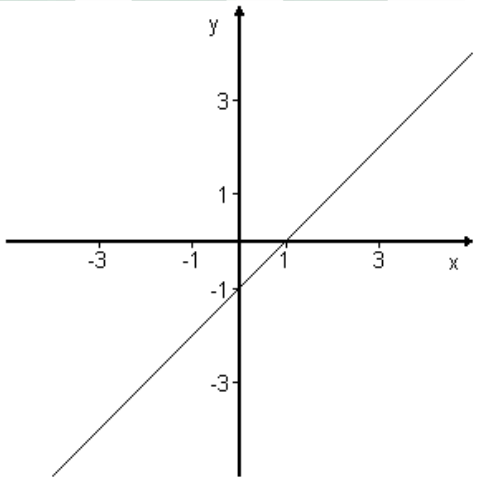
3. $a(x) = 1 + x^2$, sus raíces son $\pm i \in \mathbb{C} - \mathbb{R}$, por lo que su gráfica no intersecta al eje de las abscisas (fig. pág. 40).

4. $b(x) = -2x + x^2$, sus raíces son 0 y 2, por lo que su gráfica intersecta al eje de las abscisas en $(0, 0)$ y $(2, 0)$ (fig. pág. 40).

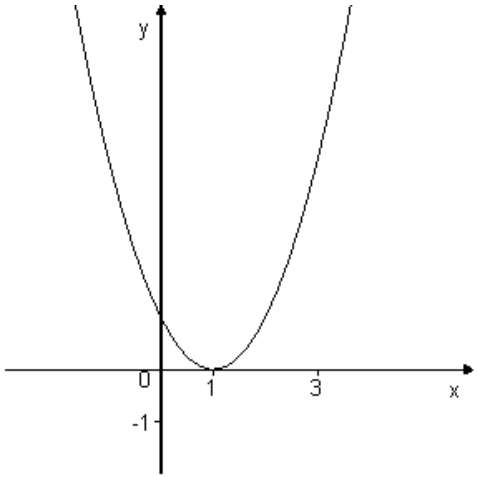
5. $c(x) = -2 + x - 2x^2 + x^3 = (x - 2)\left(1 + x^2\right)$, sus raíces son $\pm i$ y 2, por lo que su gráfica intersecta solamente en $(2, 0)$ al eje de las abscisas (fig. pág. 40).

Observacion 10 *También nos proporciona información sobre la gráfica la multiplicidad de una raíz, ya que, mientras más grande es la multiplicidad, la curva es "más suave" en el punto donde se encuentra la raíz. Veamos el significado de esto con algunos ejemplos:*

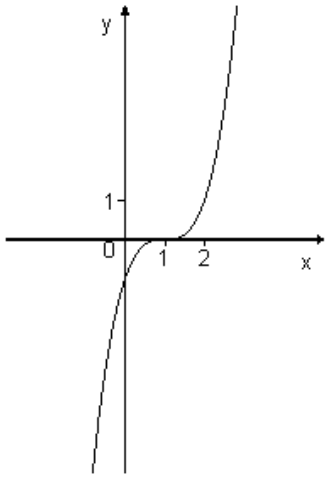
Ejemplo 16 *Si $a(x) = x - 1$, su gráfica es*



Ejemplo 17 *Si* $b(x) = (x-1)^2$*, su gráfica es*



Ejemplo 18 *Si* $c(x) = (x-1)^3$*, su gráfica es:*



Ejercicios 2.4.2

1. De los incisos b, c, d, e, f del ejercicio 2, subtema 2.4.1, pág. 63, diga en cada caso cuántas veces intersecta la gráfica al eje de las abscisas y en qué puntos.
2. ¿Qué significado geométrico tiene la afirmación que se hace en el ejercicio 2, pág. 83.
3. En el ejercicio 10, subsección 2.4.1, pág. 64, si $K = \mathbb{R}$, ¿qué significado geométrico tiene la afirmación que ahí se hizo?

2.4.3 Relaciones entre coeficientes y raíces

Aquí se trata de encontrar alguna relación entre los coeficientes de un polinomio mónico y las raíces del mismo. Empezaremos analizando los casos de polinomios de grados 2 y 3 que nos darán una idea más clara de las relaciones en el caso general

Sea K un campo y L una extensión de K. Supongamos que $a(x) = x^2 + a_1x + a_0 \in K[x]$ y que $\alpha_1, \alpha_2 \in L$ son raíces de $a(x)$, entonces $x^2 + a_1x + a_0 = (x - \alpha_1)(x - \alpha_2)$
$\Longrightarrow x^2 + a_1x + a_0 = x^2 + (-\alpha_1 + (-\alpha_2))x + (-\alpha_1)(-\alpha_2)$
$\Longrightarrow a_1 = -\alpha_1 + (-\alpha_2)$ y $a_0 = (-\alpha_1)(-\alpha_2)$, esto podemos escribirlo como:

$$a_1 = \sum_{1 \le r_1 \le 2} (-\alpha_{r_1}) \quad y \quad a_0 = \sum_{1 \le r_1 < r_2 \le 2} (-\alpha_{r_1})(-\alpha_{r_2}).$$

Consideremos ahora $a(x) = x^3 + a_2x^2 + a_1x + a_0 \in K[x]$ y supongamos que $\alpha_1, \alpha_2, \alpha_3 \in L$ son raíces de $a(x)$, entonces

$$\begin{aligned} x^3 + a_2x^2 + a_1x + a_0 &= (x - \alpha_1)(x - \alpha_2)(x - \alpha_3) \\ \Longrightarrow x^3 + a_2x^2 + a_1x + a_0 &= \left[x^2 + [(-\alpha_1) + (-\alpha_2)]x + (-\alpha_1)(-\alpha_2)\right](x - \alpha_3) \\ &= x^3 + [(-\alpha_1) + (-\alpha_2) + (-\alpha_3)]x^2 + [(-\alpha_1)(-\alpha_2) + \\ &\quad + (-\alpha_1)(-\alpha_3) + (-\alpha_2)(-\alpha_3)]x + (-\alpha_1)(-\alpha_2)(-\alpha_3) \end{aligned}$$

$$\begin{aligned} \Longrightarrow \quad a_2 &= (-\alpha_1) + (-\alpha_2) + (-\alpha_3), \\ a_1 &= (-\alpha_1)(-\alpha_2) + (-\alpha_1)(-\alpha_3) + (-\alpha_2)(-\alpha_3) \\ a_0 &= (-\alpha_1)(-\alpha_2)(-\alpha_3), \end{aligned}$$

lo cual podemos escribir como:

$$a_2 = \sum_{1 \le r_1 \le 3} (-\alpha_{r_1}), \qquad a_1 = \sum_{1 \le r_1 < r_2 \le 3} (-\alpha_{r_1})(-\alpha_{r_2}) \qquad \text{y}$$

$$a_0 = \sum_{1 \le r_1 < r_2 < r_3 \le 3} (-\alpha_{r_1})(-\alpha_{r_2})(-\alpha_{r_3}).$$

Si observamos lo anterior, el coeficiente de a_i es la suma de productos de longitud $n-i$ de los inversos aditivos de las raíces α_j, donde $n = gr(a(x))$, es decir, es la suma de productos con $n-i$ factores $(-\alpha_j)$; pero además, dichos factores tomados entre todas las raíces, en orden creciente respecto al índice que tienen. Por ejemplo, en el polinomio $a(x)$ de grado tres, el coeficiente a_1 es la suma de productos de longitud $3-1=2$ que aparecen con subíndices tomados, en orden creciente, entre 1 y 3, esto es, $a_1 = (-\alpha_1)(-\alpha_2) + (-\alpha_1)(-\alpha_3)$.

Ahora estamos listos para probar el resultado para un polinomio de grado n, con $n \geq 1$.

Teorema 38 *Sean K un campo y L una extensión de K. Sea $a(x) = x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0 \in K[x]$. Si $\alpha_1, \alpha_2, ..., \alpha_n \in L$ son las raíces de $a(x)$, es decir, $a(x) = (x-\alpha_1)(x-\alpha_2)...(x-\alpha_n)$, entonces:*

$$\begin{aligned} a_i &= \sum_{1 \leq r_1 < r_2 < ... < r_{n-i} \leq n} (-\alpha_{r_1})(-\alpha_{r_2})...(-\alpha_{r_{n-i}}) \\ &= (-1)^{n-i} \sum_{1 \leq r_1 < r_2 < ... < r_{n-i} \leq n} \alpha_{r_1}\alpha_{r_2}...\alpha_{r_{n-i}}, \quad \textit{para } i = 0, 1, ..., n-1. \end{aligned}$$

Demostración:

Haremos la demostración por inducción sobre n.

Si $n = 1$, entonces $a(x) = x + a_0$ y si α_1 es raíz de $a(x)$, entonces $\alpha_1 = -a_0$, esto es, $a_0 = -\alpha_1$, y queda probado.

Supongamos cierto el teorema para polinomios mónicos de grado $n-1$.

Sea $a(x) = x^n + a_{n-1}x^{n-1} + ... + a_1x + a_0 \in K[x]$ y sean $\alpha_1, \alpha_2, ..., \alpha_n \in L$ tales que:

$$a(x) = (x-\alpha_1)(x-\alpha_2)...(x-\alpha_{n-1})(x-\alpha_n)$$

Por hipótesis de inducción, si $b(x) = (x-\alpha_1)(x-\alpha_2)...(x-\alpha_{n-1})$, entonces $b(x) = x^{n-1} + b_{n-2}x^{n-2} + ... + b_1x + b_0$ donde

$$b_i = \sum_{1 \leq r_1 < r_2 < ... < r_{n-1-i} \leq n-1} (-\alpha_{r_1})(-\alpha_{r_2})...(-\alpha_{r_{n-1-i}}).$$

Así tenemos

$$\begin{aligned} a(x) &= \left(x^{n-1} + b_{n-2}x^{n-2} + ... + b_1x + b_0\right)(x-\alpha_n) \\ &= x^n + b_{n-2}x^{n-1} + ... + b_1x^2 + b_0x - \alpha_n x^{n-1} - b_{n-2}\alpha_n x^{n-2} - ... - b_1\alpha_n x - b_0\alpha_n \\ &= x^n + (b_{n-2} - \alpha_n)x^{n-1} + (b_{n-1} - b_{n-2}\alpha_n)x^{n-2} + ... + (b_0 - b_1\alpha_n)x + (-b_0\alpha_n) \end{aligned}$$

igualando coeficientes se tiene:

$$\begin{aligned}
&a_j = b_{j-1} - b_j\alpha_n \\
&= \sum_{1\le r_1<\ldots<r_{n-j}\le n-1} (-\alpha_{r_1})\cdot \quad \ldots \quad \cdot(-\alpha_{r_{n-j}}) + \\
&\qquad\qquad + \sum_{1\le r_1<\ldots<r_{n-1-j}\le n-1} (-\alpha_{r_1})\cdot\ldots\cdot(-\alpha_{r_{n-1-j}})(-\alpha_n) \\
&= \sum_{1\le r_1<\ldots<r_{n-j}\le n-1} (-\alpha_{r_1})\cdot \quad \ldots \quad \cdot(-\alpha_{r_{n-j}}) + \\
&\qquad\qquad + \sum_{\substack{1\le r_1<\ldots<r_{n-1-j}\le n-1,\\ \text{y } r_{n-j}=n}} (-\alpha_{r_1})\cdot\ldots\cdot(-\alpha_{r_{n-1-j}})(-\alpha_{r_{n-j}}) \\
&= \sum_{1\le r_1<r_2<\ldots<r_{n-j}\le n} (-\alpha_{r_1})(-\alpha_{r_2})\cdot\ldots\cdot(-\alpha_{r_{n-j}}). \quad \blacksquare
\end{aligned}$$

Corolario 39 *Si* $a(x) = a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 \in K[x]$ *y* $\alpha_1, \alpha_2, \ldots, \alpha_n \in L$ *son las raíces de* $a(x)$*, es decir,*

$$a(x) = a_n(x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n),$$

entonces

$$\frac{a_i}{a_n} = (-1)^{n-i} \sum_{1\le r_1<r_2<\ldots<r_{n-i}\le n} \alpha_{r_1}\cdot\alpha_{r_2}\cdot\ldots\cdot\alpha_{r_{n-i}}, \quad \textit{para } i = 0, 1, \ldots, n-1.$$

Estas relaciones son útiles para resolver problemas como los siguientes:

Ejemplo 19 *Resolver la ecuación:*

$$3x^3 - 16x^2 + 23x - 6 = 0$$

si el producto de dos raíces es 1.

Sean a, b, c, las raíces, entonces

$$a + b + c = \frac{16}{3}, \tag{2.4}$$

$$ab + ac + bc = \frac{23}{3}, \tag{2.5}$$

$$abc = 2, \tag{2.6}$$

Supongamos que $ab = 1$, entonces de (2.6) resulta que $c = 2$; de aquí que, sustituyendo c en (2.4) se tiene que $a + b = \frac{10}{3}$. Así, a y b deben ser raíces de la ecuación $t^2 - \frac{10}{3}t + 1 = 0$, que tiene como raíces 3 y $\frac{1}{3}$. Por lo tanto, $a = 3, b = \frac{1}{3}, c = 2$ son las raíces de la ecuación original.

Ejemplo 20 *Encontrar la suma de los cuadrados de las raíces de la ecuación:*

$$2x^4 - 8x^3 + 6x^2 - 3 = 0$$

Si las raíces son $\alpha_1, \alpha_2, \alpha_3, \alpha_4$, entonces por el corolario (39),

$$\sum_{1 \le r_1 \le 4} \alpha_{r_1} = \alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = \frac{8}{2} = 4.$$

$$\sum_{1 \le r_1 < r_2 \le 4} \alpha_{r_1}\alpha_{r_2} = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_1\alpha_4 + \alpha_2\alpha_3 + \alpha_2\alpha_4 + \alpha_3\alpha_4 = \frac{6}{2} = 3.$$

Por otra parte,

$$4^2 = (\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4)^2 = \alpha_1^2 + \alpha_2^2 + \alpha_3^2 + \alpha_4^2 + 2\sum_{1 \le r_1 < r_2 \le 4} \alpha_{r_1}\alpha_{r_2}$$

que implica

$$\alpha_1^2 + \alpha_2^2 + \alpha_3^2 + \alpha_4^2 = 4^2 - 6 = 10.$$

Ejercicios 2.4.3

Resuelva las siguientes ecuaciones cúbicas cuyas raíces son a, b, c.

1. $x^3 + 2x^2 + 3x + 2 = 0$ si $a = b + c$.
2. $2x^3 - x^2 - 18x + 9 = 0$ si $a + b = 0$.
3. $3x^3 + 2x^2 - 19x + 6 = 0$ si $a + b = -1$.
4. $2x^3 - x^2 - 5x - 2 = 0$ si $ab = -1$.
5. $x^3 - 7x^2 - 42x + 216 = 0$ si $c^2 = ab$.
6. $x^3 + 9x^2 + 6x - 56 = 0$ si $b = -2a$.
7. $9x^3 - 36x^2 + 44x - 16 = 0$ si las raíces forman una progresión aritmética $\alpha - \beta, \alpha, \alpha + \beta$.
8. $3x^3 - 26x^2 + 52x - 24 = 0$ si las raíces forman una progresión geométrica $\alpha\beta^{-1}, \alpha, \alpha\beta$.
9. $2x^3 - 6x^2 + 3x + k = 0$. Determine k y resuelva la ecuación si $a = 2b + 2c$.
10. ¿Qué relación existe entre p y q si la ecuación $x^3 + px + q = 0$ tiene una raíz múltiple?

11. Pruebe que $(2q - p^2)^3 r = (pq - 4r)^3$ si las raíces de $x^3 + px^2 + qx + r = 0$ satisfacen la condición $c^2 = -ab$.
    Resuelva las siguientes ecuaciones de cuarto grado cuyas raíces son a, b, c, d.
12. $x^4 - 2x^3 + 2x^2 - x - 2 = 0$ si $a + b = 1$.
13. $2x^4 - 3x^3 - 9x^2 + 15x - 5 = 0$ si $a = -b$.
14. $x^4 - 7x^3 + 18x^2 - 22x + 12 = 0$ si $ab = 6$.
15. $x^4 + x^3 - 2x^2 + 3x - 1 = 0$ si $ab - 1$.
16. $2x^4 + 13x^3 + 25x^2 + 15x + 9 = 0$ si $a = b$ y $c + d = -\frac{1}{2}$.
17. $9x^4 + 9x^3 + 2x^2 - 14x + 4 = 0$ si $a = 2b$.
18. $4x^4 - 4x^3 - 21x^2 + 11x + 10 = 0$ si las raíces están en progresión aritmética.
    Sugerencia: Represente las raíces por $\alpha - 3\beta, \alpha - \beta, \alpha + \beta, \alpha + 3\beta$.
19. Determine k y resuelva la ecuación $2x^4 - 15x^3 + kx^2 - 3x + 8 = 0$ si sus raíces están en progresión geométrica.
    Sugerencia: Represente las raíces por $\alpha\beta^{-3}, \alpha\beta^{-1}, \alpha\beta, \alpha\beta^3$.
20. Encuentre la suma de los cuadrados de las raíces de las ecuaciones:
    a. $2x^4 - 6x^3 + 5x^2 - 7x + 1 = 0$.
    b. $3x^5 - 3x^3 + 2x^2 + x - 1 = 0$.
21. Para las mismas ecuaciones de (20), encuentre la suma de los inversos multiplicativos de las raíces y también la suma de los cuadrados de estos inversos.

2.4.4 La Derivada

En el estudio de las ecuaciones juega un papel importante el concepto de derivada en la descomposición de polinomios como producto de irreducibles. La definición que enunciamos aquí corresponde a la que se estudia en cálculo, analizaremos cómo se comportan las derivadas respecto a las operaciones y veremos algunos resultados que nos servirán en la búsqueda de raíces y factores irreducibles.

Definicion 26 *Sean K un campo y $a \in K$.*

1. *Si $n \in \mathbb{N}$, la suma n veces $\underbrace{a + a + ... + a}$ se denota por na.*
2. *Si $n = 0$, se define $na = 0 \in K$.*

Definicion 27 *Sean K un campo y $a(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0 \in K[x]$. La **derivada** de $a(x)$ es*

1. *cero si* $a(x)$ *es una constante.*
2. $na_nx^{n-1} + (n-1)a_{n-1}x^{n-2} + ... + 2a_2x + a_1, \quad$ *si* $gr(a(x)) \geq 1$.

En ambos casos, denotaremos a la derivada de $a(x)$ por $a'(x)$.

Ejemplo 21 *Si* $a(x) = x^5 + \sqrt{3}x^4 + 2x^3 - 10x + 4 \in \mathbb{R}[x]$*, entonces su derivada es* $a'(x) = 5x^4 + 4\sqrt{3}x^3 + 6x^2 - 10$.

Si $a'(x)$ es la derivada de $a(x)$, entonces la derivada de $a'(x)$ se llama la **segunda derivada** de $a(x)$ y se denota por $a''(x)$; la **tercera derivada** de $a(x)$ es la derivada de $a''(x)$, que se denota por $a'''(x)$ o $a^{(3)}(x)$ y así, si se sigue derivando sucesivamente, la derivada que se obtiene en el $k - ésimo$ paso se llama la **k-ésima derivada** de $a(x)$ y se denota por $a^{(k)}(x), n > 3$.

Teorema 40 *Sea* K *un campo y sean* $b(x)$ *y* $c(x) \in K[x]$.

1. *Si* $a(x) = b(x) + c(x)$*, entonces* $a'(x) = b'(x) + c'(x)$.
2. *Si* $a(x) = b(x) \cdot c(x)$*, entonces* $a'(x) = b(x) \cdot c'(x) + b'(x) \cdot c(x)$.
3. *Si* $a(x) = (b(x))^n$*, donde* $n \geq 1$*, entonces* $a'(x) = n(b(x))^{n-1} \cdot b'(x)$.

Demostración:

1. Queda como ejercicio para el lector.
2. El caso en que uno de los factores sea cero es inmediato de que $a(x) = b(x) \cdot c(x) = 0$ y de la definición de derivada de una constante.
   Si $a(x) \neq 0$ y $b(x) \neq 0$, consideramos primero el caso en que $b(x)$ es un monomio, es decir, $b(x) = b_mx^m$ con $m \geq 0$, y haremos la demostración por inducción sobre el $gr(c(x))$.
   Si $gr(c(x)) = 0$, entonces $c(x) = c_0 \in K$ y de aquí que $a(x) = b(x)c(x) = b_mc_0x^m$, lo cual implica que $a'(x) = mb_mc_0x^{m-1} = b'(x) \cdot c(x) = b(x) \cdot c'(x) + b'(x) \cdot c(x)$ ya que $c'(x) = 0$.
   Supongamos cierto el teorema para el producto de $b(x)$ con cualquier polinomio de grado menor que n $(n > 0)$ y sea

$$c(x) = c_nx^n + ... + c_1x + c_0 \quad \text{y} \quad c_n \neq 0,$$

   entonces $a(x) = b(x) \cdot c(x) = b(x) \cdot (c_nx^n) + b(x) \cdot d(x)$, donde

$d(x) = c_{n-1}x^{n-1} + ... + c_1x + c_0$ y de aquí que

$$\begin{aligned} a'(x) &= [b_m c_n x^{n+m}]' + [b(x)\cdot d(x)]', \quad \text{por (1)} \\ &= (m+n)b_m c_n x^{m+n-1} + b'(x)\cdot d(x) + b(x)\cdot d'(x), \quad \text{por hip. de inducción} \\ &= mb_m c_n x^{n+m-1} + nb_m c_n x^{m+n-1} + b'(x)\cdot d(x) + b(x)\cdot d'(x) \\ &= mb_m c_n x^n x^{m-1} + nb_m c_n x^m x^{n-1} + b'(x)\cdot d(x) + b(x)\cdot d'(x) \\ &= b'(x)\cdot(c_n x^n + d(x)) + b(x)\cdot\left(nc_n x^{n-1} + d'(x)\right) \\ &= b'(x)\cdot c(x) + b(x)\cdot c'(x). \end{aligned}$$

Por último, probaremos que si $b(x) = b_m x^m + ... + b_1 x + b_0$ y $c(x) = c_n x^n + ... + c_1 x + c_0$, entonces la derivada de su producto se obtiene según el teorema. Para esto, utilizaremos nuevamente inducción, esta vez sobre $gr(b(x))$.

Sean $c_n \neq 0$ y $n \geq 0$.

Si $gr(b(x)) = 0$, se reduce al caso anterior.

Supongamos que $m > 0$ y que es cierto el teorema para el producto de $c(x)$ y cualquier polinomio de grado menor que m.

Sea $b(x) \in K[x]$ tal que $gr(b(x)) = m$, entonces $a(x) = b(x)\cdot c(x) = e(x)\cdot c(x) + f(x)\cdot c(x)$ donde $e(x) = b_m x^m$ y $f(x) = b_{m-1}x^{m-1} + ... + b_1 x + b_0$. Así tenemos:

$$\begin{aligned} a'(x) &= [e(x)\cdot c(x)]' + [f(x)\cdot c(x)]', \quad \text{por (1)} \\ &= e'(x)\cdot c(x) + e(x)\cdot c'(x) + [f(x)\cdot c(x)]' \quad \text{(caso anterior)} \\ &= e'(x)\cdot c(x) + e(x)\cdot c'(x) + f'(x)\cdot c(x) + f(x)\cdot c'(x) \quad \text{(hip. de inducción)} \\ &= (e'(x) + f'(x))\cdot c(x) + (e(x) + f(x))\cdot c'(x) \\ &= b'(x)\cdot c(x) + b(x)\cdot c'(x) \quad \text{por (1)} \end{aligned}$$

y así, queda probado (2).

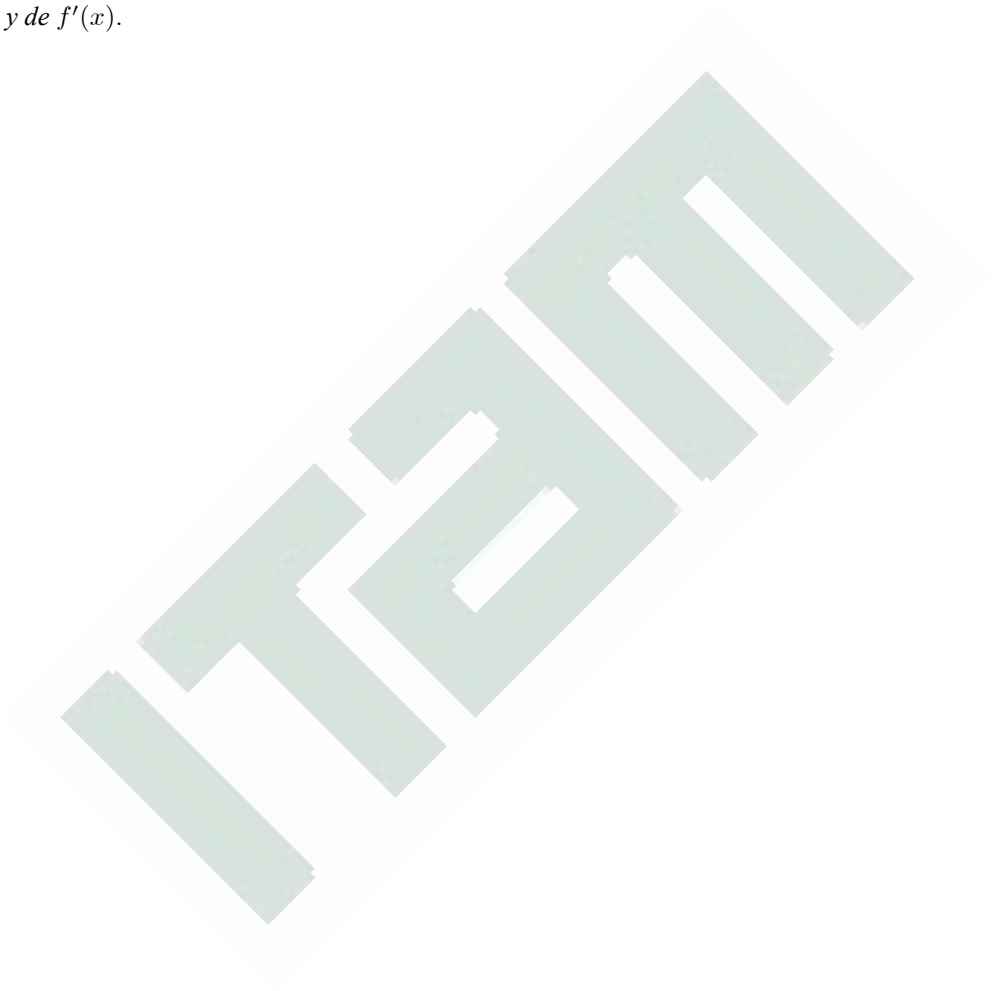
3. Queda como ejercicio para el lector, con la sugerencia de utilizar inducción y el inciso (2). ■

Ejemplo 22 *Sea* $a(x) = (x-\alpha)^n$. *Entonces*

$$\begin{aligned} a'(x) &= n(x-\alpha)^{n-1} \\ a''(x) &= n(n-1)(x-\alpha)^{n-2} \\ &\vdots \\ a^{(n-1)}(x) &= n(n-1)(n-2)\cdot ...\cdot 2\cdot(x-\alpha) \\ a^{(n)}(x) &= n! \end{aligned}$$

El siguiente resultado será de gran utilidad para encontrar la multiplicidad de las raíces de un polinomio.

Teorema 41 *Sean K un campo, L un extensión de K y $f(x) \in K[x]$ tal que $gr(f(x)) > 1$. Entonces $f(x)$ tiene raíces múltiples en L si y sólo si existe $\alpha \in L$ tal que α es raíz de $f(x)$ y de $f'(x)$.*



Demostración:

Si $f(x)$ tiene raíces múltiples en L, entonces existen $\alpha \in L$ y un número natural $m > 1$ tales que $(x-\alpha)^m | f(x)$, es decir, $f(x) = (x-\alpha)^m g(x)$ para algún $g(x) \in L[x]$, y entonces

$$\begin{aligned} f'(x) &= (x-\alpha)^m g'(x) + m(x-\alpha)^{m-1} g(x) \\ &= (x-\alpha)[(x-\alpha)^{m-1} g'(x) + m(x-\alpha)^{m-2} g(x)] \end{aligned}$$

de donde $(x-\alpha)|f'(x)$ y así, por el Teorema del Factor α es raíz de $f(x)$ y $f'(x)$.

Recíprocamente, si $\alpha \in L$ es raíz de $f(x)$ y $f'(x)$, entonces $f(x) = (x-\alpha)h(x)$ y $f'(x) = (x-\alpha)k(x)$ para algunos polinomios $h(x)$ y $k(x) \in L[x]$. De aquí tenemos que

$$\begin{aligned} & f'(x) = (x-\alpha)h'(x) + h(x) = (x-\alpha)k(x) \\ \Rightarrow \quad & h(x) = (x-\alpha)(k(x) - h'(x)) \\ \Rightarrow \quad & (x-\alpha)|h(x) \\ \Rightarrow \quad & (x-\alpha)^2 \big| f(x), \end{aligned}$$

de aquí que α es una raíz múltiple. ■

Corolario 42 *Sean K un campo, L una extensión de K y $f(x) \in K[x]$ tal que $gr(f(x)) > 1$.*

$\alpha \in L$ es una raíz de multiplicidad m de $f(x)$ si y sólo si α es raíz de $f(x), f'(x), ..., f^{(m-1)}(x)$ y α no es raíz de $f^{(m)}(x)$.

La demostración queda como ejercicio para el lector. ■

Ejemplo 23 *Diga cuál es la multiplicidad de las raíces $4, -1$ y $\frac{1}{2}$ del polinomio*

$$f(x) = 2x^6 - 21x^5 + 60x^4 + 15x^3 - 180x^2 - 48x + 64.$$

En primer lugar se ve que $f(4) = 0, f(-1) = 0$ y $f\left(\frac{1}{2}\right) = 0$.

La derivada del polinomio $f(x)$ es

$$f'(x) = 12x^5 - 105x^4 + 240x^3 + 45x^2 - 360x - 48$$

y se tiene que $f'(4) = 0, f'(-1) = 0$ y $f'(\frac{1}{2}) \neq 0$, por lo que $\frac{1}{2}$ es una raíz simple.

Si consideramos $f''(x) = 60x^4 - 420x^3 + 720x^2 + 90x - 360$, se ve que $f''(4) = 0$ y $f''(-1) \neq 0$, por lo que -1 es raíz doble de $f(x)$.

Con $f'''(x) = 240x^3 - 1260x^2 + 1440x + 90$ se ve que $f'''(4) \neq 0$, por lo que 4 es una raíz de multiplicidad 3.

Ahora veremos la utilidad de la derivada en la descomposición de un polinomio como producto de irreducibles. El siguiente lema será de gran utilidad.

Lema 43 *Sean K un campo y $a(x) = cp_1(x)^{n_1} \cdot ... \cdot p_k(x)^{n_k}$, $k \geq 1$, con $c \in K$, $p_1(x), ..., p_k(x) \in K[x]$ polinomios de grado positivo y $n_1, n_2, ..., n_k \in \mathbb{N}$. Entonces*

$$a'(x) = \sum_{j=1}^{k} n_j \frac{a(x)}{p_j(x)} \cdot p_j^{'}(x).$$

Demostración:

Haremos la demostración por inducción sobre k. Si $k = 1$, $a(x) = cp_1(x)^{n_1}$ y entonces $a'(x) = n_1 cp_1(x)^{n_1-1} p_1^{'}(x) = n_1 \frac{a(x)}{p_1(x)} \cdot p_1^{'}(x)$ (Teorema 40 (3)).

Supongamos cierto el teorema cuando $k = r - 1 \geq 1$.

Sea $a(x) = cp_1(x)^{n_1} p_2(x)^{n_2} \cdot ... \cdot p_r(x)^{n_r}$. Si llamamos $b(x)$ al producto $cp_1(x)^{n_1} p_2(x)^{n_2} \cdot ... \cdot p_{r-1}(x)^{n_{r-1}}$, entonces $a(x) = b(x)p_r(x)^{n_r}$ y

$$\begin{aligned}
a'(x) &= b'(x)p_r(x)^{n_r} + b(x)n_r p_r(x)^{n_r-1} p_r^{'}(x) && \text{Teorema 40 (2)} \\
&= \left(\sum_{j=1}^{n_r-1} n_j \frac{b(x)}{p_j(x)} p_j^{'}(x) \right) p_r(x)^{n_r} + b(x)n_r p_r(x)^{n_r-1} p_r^{'}(x) && \text{(hip. de inducción)} \\
&= \sum_{j=1}^{n_r-1} n_j \frac{a(x)}{p_j(x)} p_j^{'}(x) + n_r \frac{a(x)}{p_r(x)} p_r^{'}(x) \\
&= \sum_{j=1}^{n_r} n_j \frac{a(x)}{p_j(x)} p_j^{'}(x)
\end{aligned}$$

y así queda probado el lema. ■

Con esta descripción de la derivada, nos será fácil decir cuál es el máximo común divisor de un polinomio y su derivada a través de la descomposición en producto de irreducibles.

Esto sólo se puede hacer en campos como los que hemos estado trabajando $(\mathbb{Q}, \mathbb{R}, \mathbb{C})$ que, además de ser infinitos tienen la propiedad de que si $n \in \mathbb{N}$ y a es un elemento del campo, entonces $na = 0$ implica $a = 0$. Los campos que cumplen esta propiedad se llaman **campos de característica cero**.

Teorema 44 *Sea K un campo de característica cero y*

$$a(x) = cp_1(x)^{n_1} \cdot ... \cdot p_k(x)^{n_k} \in K[x] \quad \textit{con } k \geq 1,$$

donde

- $c \in K$.
- $p_1(x), ..., p_k(x)$ *son polinomios mónicos irreducibles distintos.*
- $n_1 \geq 1, n_2 \geq 1, ..., n_k \geq 1,$

entonces

$$(a(x); a'(x)) = p_1(x)^{n_1-1}...p_k(x)^{n_k-1}.$$

Demostración:

Sea $d(x) = p_1(x)^{n_1-1} \cdot ... \cdot p_k(x)^{n_k-1}$. Claramente $d(x)$ divide a $a(x)$. Por otra parte, $d(x)$ divide a $\dfrac{a(x)}{p_j(x)}$, para $j = 1, 2, ..., k$, de aquí que $d(x)$ divide a

$$a'(x) = \sum_{j=1}^{k} n_j \frac{a(x)}{p_j(x)} p_j'(x). \qquad \text{(Lema 43)}$$

Así, $d(x)$ es un divisor común de $a(x)$ y $a'(x)$.

Ahora veremos que cualquier divisor común de $a(x)$ y $a'(x)$ divide a $d(x)$.

Sea $f(x) \in K[x]$ tal que $f(x)|a(x)$, $f(x)|a'(x)$ y $gr(f(x)) > 0$. Como $f(x)|a(x)$, por el Teorema de Factorización Única, $f(x) = ep_1(x)^{m_1}p_2(x)^{m_2}...p_k(x)^{m_k}$ donde $e \in K$ y $m_1 \leq n_1, ..., m_k \leq n_k$. Ahora, basta ver que $m_i \neq n_i$, para toda $i = 1, ..., k$ para que $f(x)$ divida a $a'(x)$, ya que en ese caso $m_i \leq n_i - 1$, para toda $i = 1, ..., k$.

Supongamos que $m_1 = n_1$, entonces como $f(x)|a'(x)$, se tiene que $p_1(x)^{n_1} \mid a'(x)$, esto es, $p_1(x)^{n_1} \left| \sum_{j=1}^{k} n_j \dfrac{a(x)}{p_j(x)} p_j'(x) \right.$; además, $p_1(x)^{n_1} \left| \dfrac{a(x)}{p_j(x)} \right.$ para $j = 2, 3, ..., k$;

de aquí que si $b(x) = \sum_{j=2}^{k} n_j \dfrac{a(x)}{p_j(x)} p_j'(x)$, entonces $p_1(x)^{n_1} | a'(x) - b(x)$, es decir,

$p_1(x)^{n_1} \left| n_1 \dfrac{a(x)}{p_1(x)} p_1'(x) \right.$ lo cual implica que $n_1 p_1(x)^{n_1-1}...p_k(x)^{n_k} p_1'(x) = p_1(x)^{n_1} q(x)$,

para algún $q(x) \in K[x]$ de donde $n_1 p_2(x)^{n_2}...p_k(x)^{n_k} p_1'(x) = p_1(x)q(x)$, es decir,

$p_1(x) \left| n_1 \dfrac{a(x)}{p_1(x)^{n_1}} p_1'(x) \right.$. Pero como $(p_1(x); p_j(x)) = 1$, para $j = 2, ..., k$, entonces

$(p_1(x); p_j(x)^{n_j}) = 1$, para $j = 2, ..., k$, de donde $\left(p_1(x); \dfrac{a(x)}{p_j(x)^{n_1}} \right) = 1$, y por lo tanto

$p_1(x) | n_1 p_1'(x)$.

Por otra parte, si el grado de $p_1(x)$ es r_1, el coeficiente principal de $n_1 p_1'(x)$ es el 1 de K sumado $n_1 \cdot r_1$ veces y de aquí que $n_1 p_1'(x) \neq 0$ (ya que K es de característica cero), lo cual nos lleva a una contradicción ya que según la proposición 24, pág. 48, si $p_1(x) | n_1 p_1'(x)$, entonces $gr(p_1(x)) \leq gr(p_1'(x))$ que es falso; por lo tanto $m_1 \neq n_1$. Análogamente se prueba que $m_2 \neq n_2, ..., m_k \neq n_k$ y se deduce que $f(x) | a'(x)$. ■

Corolario 45 *Si K es un campo de característica cero y $p(x) \in K[x]$ es irreducible, entonces $(p(x), p'(x)) = 1$.*

Ejemplo 24 *Se desea factorizar en producto de irreducibles en $\mathbb{Q}[x]$, el polinomio*

$$a(x) = x^9 + 4x^8 - 16x^6 - 16x^5 + 2x^4 + 13x^3 + 30x^2 + 28x + 8.$$

La derivada de $a(x)$ es

$$a'(x) = 9x^8 + 32x^7 - 96x^5 - 80x^4 + 8x^3 + 39x^2 + 60x + 28.$$

Denotemos por $d(x) = (a(x); a'(x))$. Con el Algoritmo de Euclides encontramos que

$$d(x) = x^4 + 3x^3 - x^2 - 8x - 4$$

y entonces

$$d'(x) = 4x^3 + 9x^2 - 2x - 8 \quad \text{y} \quad (d(x); d'(x)) = x + 2$$

que es irreducible en $\mathbb{Q}[x]$. Por el Teorema (44), sabemos que $(x+2)^2 \big| d(x)$ y haciendo la división tenemos

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

Como $(x^2 - x - 1)$ es irreducible en $\mathbb{Q}[x]$, nuevamente por el Teorema (44), $(x+2)^2(x^2 - x - 1)^2$ divide a $a(x)$ y al hacer la división obtenemos

$$a(x) = (x+2)^3(x^2 - x - 1)^2(x^2 + 1),$$

que es la descomposición de $a(x)$como producto de irreducibles en $\mathbb{Q}[x]$.

Ejercicios 2.4.4

1. Encuentre las derivadas de los siguientes polinomios
   a. $5x^5 + \frac{1}{2}x^4 + \frac{2}{3}x^2 - x + 6$, en $\mathbb{Q}[x]$.
   b. $x^4 + \sqrt{2}x^2 + 1$, en $\mathbb{R}[x]$.
   c. $x^5 - ix^3 + (2+3i)x^2 + \sqrt{3}x + i$, en $\mathbb{C}[x]$.
   d. $x^n - 1$, en $\mathbb{Q}[x]$.
   e. $\left(x^2 + 1\right)^3$, en $\mathbb{R}[x]$.
   f. $(x + a)$, con $a \in K$ (campo), en $K[x]$.
2. Encuentre las derivadas sucesivas $a''(x), a^{(3)}(x), a^{(4)}(x), ...$, de los polinomios dados en el ejercicio 1. En cada caso, encuentre el mínimo número natural m tal que $a^{(m)}(x) = 0$

3. Pruebe el inciso (1) del teorema 40.
4. Pruebe el inciso (3) del teorema 40.
5. Pruebe el corolario 42.
6. Use el método del ejemplo 24 para factorizar completamente los siguientes polinomios en el anillo $K[x]$ indicado.
   a. $x^5 + 4x^4 + 7x^3 + 8x^2 + 3x + 2$, en $\mathbb{Q}[x]$.
   b. $x^6 + 6x^5 + 11x^4 + 12x^3 + 19x^2 + 6x + 9$, en $\mathbb{Q}[x]$.
   c. $x^3 + ix^2 + x + i$, en $\mathbb{C}[x]$.
   d. $x^3 + \left(2\sqrt{2} + \sqrt{3}\right)x^2 + \left(2 + 2\sqrt{6}\right)x + 2\sqrt{3}$, en $\mathbb{R}[x]$.
   e. $x^4 + x^3 + x + 1$, en $\mathbb{Q}[x]$.
7. Use el corolario 45 para probar que los siguientes polinomios no son irreducibles en $\mathbb{Q}[x]$.
   a. $x^4 + 2x^3 + 3x^2 + 2x + 1$.
   b. $4x^3 + 16x^2 + 21x + 9$.
   c. $x^6 + x^4 - x^2 - 1$.
8. Un polinomio $a(x) \in K[x]$ se dice que **tiene un factor múltiple** si existe un polinomio $b(x) \in K[x]$, de grado positivo, tal que $b(x)^2 | a(x)$. Pruebe que si K es un campo de característica cero, entonces un polinomio $a(x) \in K[x]$ tiene un factor múltiple si y sólo si $a(x)$ y $a'(x)$ no son primos relativos.
9. Use el resultado del problema anterior para probar que los siguientes polinomios no tiene factores múltiples en $\mathbb{Q}[x]$.
   a. $x^4 + x^3 + x^2 + x + 1$.
   b. $x^3 + 2x - 1$.
   c. $x^n - 1$.
   d. $x^5 + 3x^2 + 2x - 4$.

2.5 POLINOMIOS IRREDUCIBLES

En este último tema, veremos que los únicos polinomios irreducibles en $\mathbb{C}$ son los de primer grado y que en $\mathbb{R}$, además de los de primer grado hay polinomios de segundo grado que son irreducibles (si sus coeficientes cumplen cierta condición). Esto es posible probarlo gracias a uno de los resultados más importantes en la teoría de ecuaciones, el Teorema Fundamental

del Álgebra, del cual daremos únicamente el enunciado ya que su demostración requiere de algunos resultados que no han sido desarrollados aquí.

También daremos algunos criterios de irreducibilidad en $\mathbb{Q}[x]$.

2.5.1 Polinomios irreducibles en $\mathbb{C}[x]$ y en $\mathbb{R}[x]$

Teorema 46 ***Fundamental del Álgebra***. *Si $f(x) \in \mathbb{C}[x]$ es un polinomio distinto de cero tal que $gr(f(x)) \geq 1$, entonces $f(x)$ tiene al menos una raíz en $\mathbb{C}$.*

Teorema 47 *Los polinomios irreducibles en $\mathbb{C}[x]$ son los polinomios de primer grado.*

Demostración:

Sea $p(x) \in \mathbb{C}[x]$ un polinomio irreducible, entonces $p(x) \neq 0$ y $gr(p(x)) > 0$ (definición 22), de aquí que, por el Teorema Fundamental del Álgebra existe $\alpha \in \mathbb{C}$ tal que $p(\alpha) = 0$. Por el teorema del factor, $(x - \alpha)$ divide a $p(x)$ y de aquí que, como $p(x)$ es irreducible, $(x - \alpha) = a \cdot p(x)$, para algún $a \in \mathbb{C}$ distinto de cero. Esto implica que $p(x) = a^{-1}(x - \alpha)$ y por lo tanto $gr(p(x)) = gr(x - \alpha) = 1$.

Por otra parte, todo polinomio de grado 1 es irreducible, por lo que queda probado el teorema. ■

Corolario 48 *Todo polinomio $a(x) \in \mathbb{C}[x]$ de grado n, con $n > 0$, se puede escribir como:*

$$a(x) = c(x - \alpha_1)(x - \alpha_2) \cdot \ldots \cdot (x - \alpha_n)$$

donde $c \in \mathbb{C}$ distinto de cero y $\alpha_1, \alpha_2, ..., \alpha_n \in \mathbb{C}$ son las raíces de $a(x)$ (es posible que se repitan las α_i). Esta factorización es única salvo por el orden de los factores.

Demostración:

Sea $a(x) \in \mathbb{C}[x]$ tal que $gr(a(x)) = n \geq 1$, entonces por el teorema de factorización única 30, $a(x) = d \cdot p_1(x) \cdot ... \cdot p_r$, con $d \in \mathbb{C},\ d \neq 0$ y $p_i(x) \in \mathbb{C}[x]$ irreducible, para $i = 1, ..., r$.

Por el teorema anterior, $gr(p_i(x)) = 1$, para toda i; además, $\sum_{i=1}^{r} gr(p_i(x)) = n$ (proposición 20), por lo que $r = n$.

Por otra parte, si $p_i(x) = a_i x + b_i$ con $a_i, b_i \in \mathbb{C}$ y $a_i \neq 0$, entonces $p_i(x) = a_i\left(x + a_i^{-1}b_i\right) = a_i\left(x - \left(-a_i^{-1}b_i\right)\right)$ de donde si $c = d \cdot a_1 \cdot a_2 \cdot ... \cdot a_n$ y $\alpha_i = -a_i^{-1}b_i$ para $i = 1, 2, ..., n$, se tiene que

$$a(x) = c(x-\alpha_1)(x-\alpha_2)\cdot ... \cdot (x-\alpha_n). \quad \blacksquare$$

Observacion 11 *Como $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$, entonces todo polinomio con coeficientes en $\mathbb{Z}$, $\mathbb{Q}$ y $\mathbb{R}$ tiene todas sus raíces en $\mathbb{C}$.*

Esta observación nos lleva a la caracterización de los polinomios irreducibles en $\mathbb{R}[x]$.

Teorema 49 *Los polinomios irreducibles en $\mathbb{R}[x]$ son los de primer grado y los polinomios de la forma ax^2+bx+c tales que $a \neq 0$ y $b^2-4ac<0$.*

Demostración:

Sea $p(x) \in \mathbb{R}[x]$ irreducible, de aquí que $p(x) \neq 0$ y $gr(p(x)) > 0$. Por el teorema 46, existe $\alpha \in \mathbb{C}$ tal que $p(\alpha) = 0$. Si $\alpha \in \mathbb{R}$, entonces $(x-\alpha)$ divide a $p(x)$ en $\mathbb{R}[x]$, de aquí que $p(x)$ es de primer grado.

Supongamos que $\alpha \notin \mathbb{R}$, entonces $\alpha \neq \bar{\alpha}$ y $\bar{\alpha}$ es raíz de $p(x)$ (ejercicio 8, pág. 64).

Sea $f(x) = (x-\alpha)(x-\bar{\alpha}) = x^2 - (\alpha+\bar{\alpha})x + \alpha\bar{\alpha}$. Como $\alpha+\bar{\alpha} = 2\,\mathrm{Re}(\alpha)$ y $\alpha\bar{\alpha} = |\alpha|^2$, se tiene que $f(x) \in \mathbb{R}[x]$. Por el Algoritmo de la División, $p(x) = f(x)q(x) + r(x)$ donde $q(x), r(x) \in \mathbb{R}[x]$ y $r(x) = 0$ o $gr(r(x)) < gr(f(x)) = 2$; pero esta última relación no se puede dar ya que si $r(x) \neq 0$, como

$$\begin{aligned} r(\alpha) &= p(\alpha) - f(\alpha)q(\alpha) = 0 - 0\cdot q(\alpha) = 0 \\ r(\bar{\alpha}) &= p(\bar{\alpha}) - f(\bar{\alpha})q(\bar{\alpha}) = 0 - 0\cdot q(\bar{\alpha}) = 0 \end{aligned}$$

se tendría un polinomio, $r(x)$, de grado menor que 2 con al menos 2 raíces α y $\bar{\alpha}$, lo cual sería una contradicción al teorema 34, de aquí que $r(x) = 0$, es decir, $f(x)$ divide a $p(x)$. Como $p(x)$ es irreducible se tiene que $p(x) = af(x)$ con a un número real distinto de cero; así, $p(x) = ax^2+bx+c$, donde $a, b, c \in \mathbb{R}$ son tales que $a \neq 0$, $b = -a(\alpha+\bar{\alpha})$ y $c = a\alpha\bar{\alpha}$.

Ahora,

$$\begin{aligned} b^2-4ac &= a^2\left(\alpha^2+2\alpha\bar{\alpha}+\bar{\alpha}^2\right) - 4a^2\alpha\bar{\alpha} \\ &= a^2\left(\alpha^2-2\alpha\bar{\alpha}+\bar{\alpha}^2\right) \\ &= a^2(\alpha-\bar{\alpha})^2 \\ &= a^2(2i\,\mathrm{Im}(\alpha))^2 \\ &= -4a^2(\mathrm{Im}(\alpha))^2 < 0 \end{aligned}$$

pues $a \neq 0$ y $\mathrm{Im}(\alpha) \neq 0$ (ya que $\alpha \notin \mathbb{R}$).

Por lo tanto todo polinomio irreducible es de primer grado o de la forma ax^2+bx+c, con $b^2-4ac<0$. Recíprocamente, todos estos polinomios son irreducibles en $\mathbb{R}[x]$ (ejercicio 1, pág. 83). $\blacksquare$

Corolario 50 *Todo polinomio $f(x) \in \mathbb{R}[x]$ diferente de cero se puede escribir en la forma:*

$$f(x) = c \cdot (x - \alpha_1) \cdot (x - \alpha_2) \cdot ... \cdot (x - \alpha_r) \cdot g_1(x) \cdot g_2(x) \cdot ... \cdot g_s(x)$$

con $r, s \geq 0$,[8] donde c es un número real distinto de cero, $\alpha_1, \alpha_2, ..., \alpha_r$ son todas las raíces de $f(x)$ en $\mathbb{R}$ (es posible que se repitan), $g_1(x), g_2(x), ..., g_s(x)$ son polinomios irreducibles de segundo grado en $\mathbb{R}[x]$.

La demostración de este corolario queda como ejercicio para el lector. ■

El conocimiento de una raíz de un polinomio, muchas veces facilita el poder encontrar las demás o permite encontrar cierto tipo de polinomios con alguna condición dada. También, el conocimiento de todas sus raíces permite determinar cuál es el polinomio. A continuación veremos algunos ejemplos que ilustran estos hechos.

Ejemplo 25 1. *Si $2 + i$ es una raíz de $x^4 - 4x^3 + 2x^2 - 15$, entonces $2 - i$ también es raíz, y de aquí que $(x - (2 - i))(x - (2 + i)) = x^2 - 4x + 5$ debe dividir a $x^4 - 4x^3 + 2x^2 + 12x - 15$. Al hacer la división resulta:*

$$x^4 - 4x^3 + 2x^2 + 12x - 15 = \left(x^2 - 4x + 5\right)\left(x^2 - 3\right)$$

de donde $\sqrt{3}$ y $-\sqrt{3}$ son las otras dos raíces, de aquí que

$$x^4 - 4x^3 + 2x^2 + 12x - 15 = (x - (2 + i))(x - (2 - i))\left(x - \sqrt{3}\right)\left(x + \sqrt{3}\right).$$

2. *Se quiere determinar el polinomio mónico que tiene a 1 como raíz de multiplicidad 3 y en el que 5 e i son raíces simples. Dicho polinomio debe ser el producto:*

$$(x-1)^3(x-5)(x-i) = x^5 - (8+i)x^4 + (18+8i)x^3 - (16+18i)x^2 + (5+16i)x - 5i$$

que es un polinomio en $\mathbb{C}[x]$.

3. *Se quiere encontrar todos los polinomios de tercer grado en $\mathbb{R}[x]$ con coeficiente principal 2, término independiente 1 y $(-i)$ como raíz.*
Dichos polinomios deben ser de la forma $2x^3 + bx^2 + cx + 1$. Además como $-i$ es raíz, su conjugado también lo es, esto es, i es raíz; de aquí que

$$2x^3 + bx^2 + cx + 1 = 2\left(x^2 + 1\right)(x - \alpha),$$

donde α es la otra raíz. Así, al hacer las operaciones resulta

$$2x^3 + bx^2 + cx + 1 = 2x^3 - 2\alpha x^2 + 2x - 2\alpha,$$

por lo que:

[8] $r = 0$ o $s = 0$ significa que no aparecen términos lineales o cuadráticos, respectivamente.

$$\left.\begin{array}{rcl} 1 & = & -2\alpha \\ c & = & 2 \\ b & = & -2\alpha \end{array}\right\} \Longrightarrow \begin{array}{rcl} \alpha & = & -\dfrac{1}{2} \\ c & = & 2 \\ b & = & 1 \end{array}$$

Por lo expuesto anteriormente, se concluye que el único polinomio que cumple con las condiciones planteadas es $2x^3 + x^2 + 2x + 1$.

Ejercicios 2.5.1

1. Pruebe que si $f(x) = ax^2 + bx + c \in \mathbb{R}[x]$ es un polinomio tal que $b^2 - 4ac < 0$, entonces $f(x)$ es irreducible.
2. Pruebe que todo polinomio $f(x) \in \mathbb{R}[x]$ tal que $gr(f(x)) = 3$ tiene una raíz real.
3. Pruebe que todo polinomio $f(x) \in \mathbb{R}[x]$ de grado impar tiene una raíz real.
4. Encuentre todas las raíces de los siguientes polinomios, haciendo uso del dato que se da.
   a. $x^3 + 6x^2 - 24x + 160$, tiene una raíz que es $2 - 2\sqrt{3}i$.
   b. $x^3 + (1 - 2i)\,x^2 - (1 + 2i)\,x - 1$ que tiene una raíz de multiplicidad dos (o raíz doble).
   c. $x^5 - 3x^4 + 4x^3 - 4x + 4$ que tiene $1 + i$ como raíz doble.
5. Encuentre el polinomio mónico $a(x)$ en $\mathbb{C}[x]$, usando los datos que se dan.
   a. $a(x)$ tiene como raíces simples $1, 2, i, 1 + 4i$ y $1 - 4i$ y no tiene más raíces.
   b. $a(x)$ tiene a i como raíz de multiplicidad tres y $gr\,(a\,(x)) = 3$.
   c. $a(x) \in \mathbb{R}[x]\,,\ gr\,(a\,(x)) = 4$ y tiene a i y $1 - i$ entre sus raíces.
   d. $a(x) = x^3 + bx + c$ con $b, c \in \mathbb{R}$ y $2 + i$ es una raíz de $a(x)$.
6. Sea $f(x)$ un polinomio mónico en $\mathbb{R}[x]$ tal que $f(x)$ no tiene raíces en $\mathbb{R}$. Pruebe que $f(a) > 0$, para todo $a \in \mathbb{R}$.
7. Sea $f(x) = ax^{2n} + bx^n + c$ un polinomio en $\mathbb{C}[x]$, donde $a \neq 0$ y $n \geq 1$. Describa un método para encontrar las raíces de $f(x)$.
8. Encuentre las raíces de $x^6 - 2ix^3 + (-1 - i)$.
9. Pruebe que si $\alpha \in \mathbb{C}$ es una raíz de multiplicidad m de $f(x) \in \mathbb{R}[x]$, entonces $\bar{\alpha}$ es raíz de multiplicidad m de $f(x)$.

2.5.2 Polinomios en $\mathbb{Q}[x]$

A partir del Teorema Fundamental del Álgebra pudimos decir exactamente cuáles son los

polinomios irreducibles en $\mathbb{R}[x]$ y $\mathbb{C}[\curvearrowleft]$. Sin embargo, el problema de determinar los polinomios irreducibles en $\mathbb{Q}[x]$ es mucho más difícil. Como veremos más adelante existen ciertos criterios para decidir si un polinomio con coeficientes racionales es irreducible o no. Aquí caracterizaremos los polinomios irreducibles de segundo grado en $\mathbb{Q}[x]$ y veremos la forma de determinar los factores de primer grado en la descomposición de un polinomio como producto de irreducibles en $\mathbb{Q}[x]$ con lo cual, en muchos casos nos proporcionará la factorización buscada.

Teorema 51 *Sea $f(x) = ax^2 + bx + c \in \mathbb{Q}[x]$ con $a \neq 0$. Entonces $f(x)$ es irreducible en $\mathbb{Q}[x]$ si y sólo si $b^2 - 4ac$ no es el cuadrado de un número racional.*

Demostración:

$f(x)$ es irreducible en $\mathbb{Q}[x] \Leftrightarrow p(x) \nmid f(x)$, para todo polinomio $p(x) \in \mathbb{Q}[x]$ tal que $gr(p(x)) = 1 \Leftrightarrow (x - \alpha) \nmid f(x)$, para toda $\alpha \in \mathbb{Q} \Leftrightarrow f(x)$ no tiene raíces en $\mathbb{Q}$ (teorema del factor) $\Leftrightarrow \frac{-b \pm \sqrt{b^2-4ac}}{2a} \notin \mathbb{Q} \Leftrightarrow \sqrt{b^2 - 4ac} \notin \mathbb{Q}$. ■

Ahora veremos una forma de encontrar las raíces de polinomios en $\mathbb{Q}[x]$ y así, sus divisores mónicos de primer grado. Para esto, es conveniente hacer la siguiente

Observacion 12 *Si $f(x) = \frac{p_0}{q_0} + \frac{p_1}{q_1}x + ... + \frac{p_n}{q_n}x^n$ es un polinomio distinto de cero en $\mathbb{Q}[x]$, esto es, $p_i, q_i \in \mathbb{Z}$ y $q_i \neq 0$, para $i = 0, ..., n$, y $q \neq 0$ es un múltiplo común de los denominadores $q_0, q_1, ..., q_n$ (por ejemplo el producto $q_0 q_1 ... q_n$), entonces $g(x) = q \cdot f(x)$ es un polinomio con coeficientes enteros con las mismas raíces que $f(x)$, es decir, $\alpha \in \mathbb{Q}$ es raíz de $f(x)$ si y sólo si α es raíz de $g(x)$. Así, reduciremos nuestro problema a buscar raíces racionales de polinomios con coeficientes enteros.*

Teorema 52 *Sea $a(x) = a_0 + a_1x + ... + a_nx^n \in \mathbb{Z}[x]$ un polinomio tal que $a_0 \neq 0, a_n \neq 0$ y $n \geq 1$. Si p y q son números enteros primos relativos y $\frac{p}{q}$ es raíz de $a(x)$, entonces $p \,|a_0$ y $q \,|a_n$.*

Demostración:

Sea $\frac{p}{q}$ raíz de $a(x)$ tal que $(p; q) = 1$.

$$a\left(\frac{p}{q}\right) = a_0 + a_1\frac{p}{q} + ... + a_{n-1}\frac{p^{n-1}}{q^{n-1}} + a_n\frac{p^n}{q^n} = 0$$

y multiplicando por q^n se tiene,

$$q^n a\left(\frac{p}{q}\right) = a_0q^n + a_1pq^{n-1} + ... + a_{n-1}p^{n-1}q + a_np^n = 0$$

De aquí deducimos que:

$$a_0 q^n = p \cdot \left(-a_1 q^{n-1} - ... - a_{n-1} p^{n-2} q - a_n p^{n-1}\right)$$

y

$$a_n p^n = q \cdot \left(-a_0 q^{n-1} - a_1 p q^{n-2} - ... - a_{n-1} p^{n-1}\right)$$

de donde, $p \,|a_0 q^n$ y $q \,|a_n p^n$.

Por otra parte, $(p;q) = 1 \Rightarrow (p;q^n) = 1$ y $(q;p^n) = 1$ y por lo tanto, $p \,|a_0$ y $q \,|a_n$. ■

Ejemplo 26 *i. Usaremos el teorema 52 para probar que* 0 *es la única raíz racional del polinomio* $a(x) = x^7 - 3x^6 + 2x^3 + x^2$. *Claramente* 0 *es una raíz doble de* $a(x)$ *puesto que* $a(x) = x^2 \cdot \left(x^5 - 3x^4 + 2x + 1\right)$ *y cualquier otra raíz racional de* $a(x)$ *debe ser raíz de* $b(x) = x^5 - 3x^4 + 2x + 1$. *Si* $\frac{p}{q}$, *con* $(p;q) = 1$, *es raíz de* $b(x)$, *por el teorema 52,* $p|1$ *y* $q|1$ *por lo que* p *y* q *pueden ser* ± 1 *y* $\frac{p}{q} = \pm 1$. *Sin embargo,* $b(1) = 1 - 3 + 2 + 1 = 1 \neq 0$ *y* $b(-1) = -1 - 3 - 2 + 1 = -5 \neq 0$; *esto es,* $b(x)$ *no tiene raíces racionales y por lo tanto* 0 *es la única raíz racional de* $a(x)$.

ii. Escribir como producto de irreducibles en $\mathbb{Q}[x]$ *el polinomio* $a(x) = x^4 + \frac{11}{6}x^3 + \frac{4}{3}x^2 - x - \frac{2}{3}$. *Las raíces de* $a(x)$ *son las mismas que las de* $b(x) = 6a(x) = 6x^4 + 11x^3 + 8x^2 - 6x - 4$. *Si* $\frac{p}{q} \in \mathbb{Q}$, *con* $(p;q) = 1$, *es raíz de* $b(x)$ *entonces* $p| - 4$ *y* $q|6$; *de aquí que las únicas posibilidades para* $\dfrac{p}{q}$ *son:*

$$\pm 1, \pm 2, \pm 4, \pm\frac{1}{2}, \pm\frac{1}{3}, \pm\frac{2}{3}, \pm\frac{4}{3}, \pm\frac{1}{6}$$

de las cuales encontramos que sólo $-\dfrac{1}{2}$ *y* $\dfrac{2}{3}$ *son raíces y así,*

$$a(x) = \left(x + \frac{1}{2}\right)\left(x - \frac{2}{3}\right)\left(x^2 + 2x + 2\right)$$

es la factorización que se busca, puesto que $x^2 + 2x + 2$ *es irreducible en* $\mathbb{Q}[x]$ *(Teorema 51).*

iii. Expresar como producto de polinomios irreducibles en $\mathbb{Q}[x]$, *el polinomio*

$$a(x) = x^5 - 3x^4 - x^3 + 3x^2 - 2x + 6.$$

Según el Teorema 52, las posibles raíces racionales de $a(x)$ *son:* ± 1, ± 2, ± 3, ± 6 *y haciendo los cálculos correspondientes resulta que* 3 *es el único número racional en el que* $a(x)$ *vale cero. Así,* $a(x) = (x-3)\left(x^4 - x^2 - 2\right)$ *donde* $\left(x^4 - x^2 - 2\right)$ *no tiene raíces racionales ya que las únicas posibilidades son* ± 1 *y* ± 2 *que no son raíces de* $a(x)$ *y por lo tanto tampoco de este polinomio.*

Sin embargo, $x^4 - x^2 - 2$ *podemos expresarlo como producto de dos polinomios de segundo grado en* $\mathbb{Q}[x]$ *y para ello hacemos* $y = x^2$ *y encontramos las soluciones de la ecuación* $y^2 - y - 2 = 0$ *(Ejercicio 7, pág. 7), esto es,* 2 *y* -1. *Así,* $y^2 - y - 2 = (y-2)(y+1)$

y entonces $x^4 - x^2 - 2 = \left(x^2 - 2\right)\left(x^2 + 1\right)$. *Como* $x^2 - 2$ *y* $x^2 + 1$ *son irreducibles en* $\mathbb{Q}[x]$, *resulta que* $a(x) = (x-3)\left(x^2 - 2\right)\left(x^2 + 1\right)$ *es la factorización buscada.*

Ejercicios 2.5.2

1. Encuentre todas las raíces racionales de los siguientes polinomios.
   a. $2x^3 - 7x^2 + 10x - 6$.
   b. $x^3 - \frac{7}{3}x^2 + 3x - 2$.
   c. $x^3 - \frac{1}{4}x^2 - \frac{1}{4}x + 16$.
   d. $x^3 - 48x + 64$.
   e. $x^4 - 5x - 1$.
   f. $2x^6 - x^5 - 2x^4 + x^3 + 2x^2 + 3x - 2$.
2. Pruebe que si r es una raíz racional de un polinomio mónico con coeficientes enteros, entonces r es un entero.
3. Pruebe que si un polinomio de grado 2 o 3 en $\mathbb{Q}[x]$ no tiene raíces racionales, entonces es irreducible en $\mathbb{Q}[x]$.
4. Use el resultado del ejercicio anterior para probar que los siguientes polinomios son irreducibles en $\mathbb{Q}[x]$.
   a. $x^2 + x + 1$.
   b. $x^2 + \frac{1}{2}x - 1$.
   c. $x^3 + 37x^2 + 211x - 1$.
   d. $x^3 - 25x - 5$.
5. Factorice completamente en $\mathbb{Q}[x]$ los siguientes polinomios.
   a. $x^4 - 1$.
   b. $2x^4 - x^3 + 2x^2 + x - 1$.
   c. $x^4 + x^2 + 1$.
   d. $x^5 + x^4 - 8x^3 - 16x^2 + 15x + 30$.

2.5.3 Criterio de irreducibilidad de Eisenstein

En esta sección daremos un criterio con el que, bajo ciertas condiciones, podremos decir

si un polinomio con coeficientes enteros es irreducible en $\mathbb{Q}[x]$ y con esto, si algunos polinomios con coeficientes racionales son irreducibles en $\mathbb{Q}[x]$.

Definicion 28 *Sea $a(x) = a_0 + a_1x + ... + a_nx^n \in \mathbb{Z}[x]$, con $a_n \neq 0$. El máximo común divisor de $a_0, a_1, ..., a_n$ se llama el **contenido de** $a(x)$. Si el contenido de $a(x)$ es 1, entonces se dice que $a(x)$ es **primitivo.***

Observacion 13 *Dado cualquier polinomio $a(x) \in \mathbb{Z}[x]$, se puede escribir como $a(x) = d \cdot b(x)$, con $d \in \mathbb{Z}$ y $b(x) \in \mathbb{Z}[\curvearrowleft]$, donde d es el contenido de $a(x)$ y $b(x)$ es primitivo. Además, esta descomposición de $a(x)$ como un elemento de $\mathbb{Z}$ por un polinomio primitivo es única. El polinomio $b(x)$ se llama **el polinomio primitivo asociado a** $a(x)$.*

Lema 53 *Si $a(x)$ y $b(x)$ son polinomios primitivos, entonces $a(x) \cdot b(x)$ es un polinomio primitivo.*

Demostración:

Sean $a(x) = a_0 + a_1x + ... + a_nx^n$ y $b(x) = b_0 + b_1x + ... + b_mx^m$.

Supongamos que el lema es falso, entonces todos los coeficientes de $a(x) \cdot b(x)$ son divisibles por un entero positivo distinto de 1 y de aquí que son divisibles por un número primo p (Teorema Fundamental de la Aritmética). Como $a(x)$ y $b(x)$ son primitivos, p no divide a algún coeficiente de $a(x)$ y no divide a alguno de $b(x)$. Sea a_i el primer coeficiente de $a(x)$ tal que $p \nmid a_i$ y b_j el primero tal que $p \nmid b_j$.

Por otra parte, el coeficiente de x^{i+j} en $a(x) \cdot b(x)$ es

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

Por la forma en que elegimos a_i y b_j se tiene que $p\,|a_{i-1}, ..., p|a_0$ y $p|b_{j-1}, ..., p|b_0$, de aquí que $p\,|a_{i-1}b_{j+1} + ... + a_0b_{j+i}$ y $p\,|a_{i+1}b_{j-1} + ... + a_{i+j}b_0$; además, según supusimos, $p|c_{i+j}$, por lo que $p|a_ib_j$ y por ser p un número primo se debe tener que $p|a_i$ o $p|b_j$, lo cual es una contradicción. Por lo tanto, $a(x)b(x)$ es primitivo. ■

Teorema 54 ***Lema de Gauss.*** *Si un polinomio primitivo $f(x)$ se puede factorizar como producto de dos polinomios con coeficientes racionales, entonces se puede factorizar como el producto de dos polinomios primitivos.*

Demostración:

Supongamos que $f(x) = a(x) \cdot b(x)$, con $a(x), b(x) \in \mathbb{Q}[x]$, entonces $f(x) = \frac{1}{q}(c(x) \cdot d(x))$ donde $q \in \mathbb{Z}$ y $c(x), d(x) \in \mathbb{Z}[x]$ son asociados a $a(x)$ y $b(x)$, respectivamente (ejercicio 2, pág. 89) y si p es el contenido de $c(x) \cdot d(x)$, entonces $f(x) = \frac{p}{q}(g(x) \cdot h(x))$, donde $g(x)$ y $h(x)$ son primitivos y asociados a $c(x)$ y $d(x)$, respectivamente (ejercicio 3, pág. 89).

Así, $q \cdot f(x) = p(g(x) \cdot h(x))$. El contenido de $q \cdot f(x)$ es q ya que $f(x)$ es primitivo y el contenido de $p(g(x) \cdot h(x))$ es p, por ser $g(x) \cdot h(x)$ primitivo (lema 53), de aquí que $p = q$ y por lo tanto $f(x) = g(x) \cdot h(x)$. ■

Teorema 55 ***Criterio de Eisenstein*** *Sea $a(x) = a_0 + a_1x + ... + a_nx^n \in \mathbb{Z}[x]$. Si p es un primo tal que $p \nmid a_n$, $p|a_{n-1}$, $p|a_{n-2}, ..., p|a_1, p|a_0$ y $p^2 \nmid a_0$, entonces $a(x)$ es irreducible sobre los racionales.*

Demostración:

Sin pérdida de generalidad se puede suponer que $a(x)$ es primitivo, ya que por el ejercicio 4, pág. 89 basta probar que el primitivo asociado a $a(x)$ es irreducible y como $p \nmid a_n$, p no divide al contenido de $a(x)$, de aquí que el primitivo asociado a $a(x)$ también satisface las hipótesis del teorema (con el mismo primo p).

Supongamos que el criterio no es válido, es decir, que $a(x) = a_0 + a_1x + ... + a_nx^n \in \mathbb{Z}[x]$ es un polinomio primitivo que satisface las hipótesis del teorema y que es reducible en $\mathbb{Q}[x]$, entonces, por el teorema 54, $a(x)$ se puede escribir como el producto de dos polinomios primitivos $b(x)$ y $c(x)$, esto es,

$$a(x) = b(x) \cdot c(x) = (b_0 + b_1x + ... + b_rx^r)(c_0 + c_1x + ... + c_sx^s)$$

donde $b_i, c_j \in \mathbb{Z}$, para toda $0 \leq i \leq r, 0 \leq j \leq s, r > 0, s > 0$ y de aquí se tiene que $a_0 = b_0c_0$, por lo que $p|b_0$ o $p|c_0$, pero no a ambos ya que $p^2 \nmid a_0$. Supongamos que $p|b_0$ y $p \nmid c_0$.

Por otra parte, $b(x)$ primitivo implica que p no divide a algún coeficiente de $b(x)$; sea b_k el primer coeficiente tal que $p \nmid b_k$, entonces $0 < k \leq r < n$ y como $p|a_k$ se tiene $p \left| \sum_{i+j=k} b_ic_j \right.$, esto es, $p|b_kc_0 + b_{k-1}c_1 + ... + b_0c_k$.

Además, por la forma en que escogimos b_k, se tiene que $p|b_{k-1}c_1 + ... + b_0c_k$, por lo que deducimos que $p|b_kc_0$ de aquí que $p|b_k$ o $p|c_0$, lo cual es una contradicción. Por lo tanto $a(x)$ es irreducible. ■

Ejemplo 27 *Decir si el polinomio $a(x) = 4x^8 + 15x^6 + 21x^5 - 6x^3 + 9x - 12$ es irreducible en $\mathbb{Q}[x]$.*

Es fácil ver que el número primo 3 divide a todos los coeficientes de $a(x)$ excepto al coeficiente de x^8 y como 9 no divide a -12, por el Criterio de Eisenstein podemos asegurar que $a(x)$ es irreducible.

Ejercicios 2.5.3

1. Pruebe la observación 13.
2. a. Si $f(x) \in \mathbb{Q}[x]$ es tal que $f(x) = \frac{a_0}{b_0} + \frac{a_1}{b_1}x + ... + \frac{a_n}{b_n}x^n$ y b es el mínimo común múltiplo de $b_0, b_1, ..., b_n$, entonces $bf(x) \in \mathbb{Z}[x]$.

   b. Sea $f(x) = a(x) \cdot b(x) \in \mathbb{Q}[x]$, demuestre que existen $q \in \mathbb{Z}$ y $c(x), d(x) \in \mathbb{Z}[x]$ tales que $f(x) = \dfrac{1}{q}c(x) \cdot d(x)$.
3. Sean $a(x)$ y $b(x)$ polinomios en $\mathbb{Z}[x]$. Pruebe que el contenido de $a(x) \cdot b(x)$ es igual al contenido de $a(x)$ por el contenido de $b(x)$.
4. Sea $f(x) \in \mathbb{Z}[x]$ y sea $p(x)$ el primitivo asociado a $f(x)$. Pruebe que $f(x)$ es irreducible si y sólo si $p(x)$ lo es.
5. Sea p un número primo, pruebe que el polinomio $x^n - p$ es irreducible sobre los racionales.
6. Utilice el Criterio de Eisenstein, en caso de que se pueda, para decidir si los siguientes polinomios son irreducibles en $\mathbb{Q}[x]$.
   a. $x^5 + 10x^4 - 25x^3 + 15x^2 - 10$.

   b. $2x^4 + 8x^3 + 6x^2 - 10x + 2$.

   c. $2x^6 - 12x^4 + 6x^3 - 18x - 9$.

   d. $6x^7 + 14x^5 - 21x^2 + 28x - 7$.
7. Pruebe que el polinomio $1 + x + x^2 + ... + x^{p-1}$, donde p es un número primo, es irreducible sobre los racionales.

   Sugerencia. Considere el polinomio $1 + (x+1) + (x+1)^2 + ... + (x+1)^{p-1}$ y utilice el Criterio de Eisenstein.

SOLUCIONES DE EJERCICIOS

Capítulo 1

Ejercicios 1.1.1

1. a. $6+4i$ b. $5+14i$ c. $\frac{11}{17}+\frac{10}{17}i$
   d. $28+96i$ e. $\frac{3}{2}-\frac{5}{2}i$ f. $-4-\frac{15}{2}i$
2. $x=\frac{3}{2}, \qquad y=-\frac{1}{2}.$
3. a. $-\frac{2}{5}-\frac{1}{5}i$ b. $\frac{1}{2}+\frac{1}{2}i$ c. $-\frac{1}{5}-\frac{3}{5}i$
   d. $-\frac{1}{10}-\frac{3}{10}i$ e. $-\frac{3}{2}+\frac{1}{2}i$
5. Si $n=4m$, entonces $\sum_{k=0}^{n} i^k=1$; si $n=4m+1$, entonces $\sum_{k=0}^{n} i^k=1+i$;
   si $n=4m+2$, entonces $\sum_{k=0}^{n} i^k=i$; si $n=4m+3$, entonces $\sum_{k=0}^{n} i^k=0$.
6. a. $z=1-\frac{1}{2}i, \quad w=\frac{1}{2}$ b. $z=\left(\frac{7}{13}-\frac{17}{13}i\right), \quad w=\left(-\frac{23}{13}+\frac{15}{13}i\right).$
11. Sugerencia. Analiza cuando $a\geq 0$ y cuando $a<0$.

Ejercicios 1.1.2

1. a. $\pm(4+3i)$ b. $\pm\left(\frac{\sqrt{2+\sqrt{2}}}{2}+\frac{\sqrt{2-\sqrt{2}}}{2}i\right)$ c. $\pm\left(\frac{7\sqrt{2}}{2}-\frac{\sqrt{2}}{2}i\right)$
   d. $\pm\left(\frac{\sqrt{2+2\sqrt{2}}}{2}+\frac{\sqrt{-2+2\sqrt{2}}}{2}i\right)$ e. $\pm\left(\frac{\sqrt{2}}{2}+\frac{\sqrt{2}}{2}i\right)$
2. Sugerencia. Usa la definición: $\sqrt{z}=x \iff x^2=z$.
3. a. $x=\left(-1+\sqrt{2}\right)i \quad$ y $\quad x=\left(-1-\sqrt{2}\right)i.$
   b.
   c. $x=\frac{\sqrt{2}}{10}+\frac{3\sqrt{2}}{10}i \quad y \quad x=\frac{\sqrt{2}}{10}-\frac{3\sqrt{2}}{10}i.$
4. $z_1=-i \quad y \quad z_2=3+i.$
5. a. $(1+i)^4=-4$
   b. $(-i)^{-1}=i$
   c. $\frac{1}{2}\sqrt{2\sqrt{2+\sqrt{2}}+2+\sqrt{2}}+\left(\frac{1}{2}\sqrt{2\sqrt{2+\sqrt{2}}-2-\sqrt{2}}\right)i.$

Ejercicios 1.2.1

1. Sugerencia: Analiza geométricamente cómo pueden ser z y w.
2. Sugerencia: Ve los vectores z y w como dos lados de un triángulo.

Ejercicios 1.2.2

1. Sugerencia: Usa la definición de módulo de un complejo.
2. Sugerencia: Ve simetría respecto a una recta.
3. Sugerencia: Revisa el círculo unitario.
4. Sugerencia: Usa la definición de conjugado.
5. Sugerencia: Usa las definiciones de módulo y conjugado.
6. Sugerencia: Escribe $z = z - w + w$ y $w = w - z + z$.
7. Sugerencia: Recuerda que $z \cdot \overline{z} = |z|^2$.
8. a. Eje real.
   b. Semiplano que está por debajo de la recta $y = 1$ (incluyéndola).
   c. Recta $x = 1$.
   d. Puntos fuera de la circunferencia con centro en $(1, 0)$ y radio 1.
   e. Círculo con centro en el origen y radio 2.
9. a. Circunferencia con centro en $(1, 0)$ y radio 3.
   b. Exterior del círculo con centro en $(1, 0)$ y radio 3.
   c. Interior del círculo con centro en $(1, 0)$ y radio 3.
   d. Circunferencia con centro en $(-5, 0)$ y radio 4.
   e. Elipse con ecuación $\frac{x^2}{9} + \frac{y^2}{25} = 1$.
   f. La recta con ecuación $y = -x$.

Ejercicios 1.2.3

1. a. 0 b. $\frac{3\pi}{2}$ c. $\frac{5\pi}{4}$
   d. $tg^{-1}(3) \approx 71.57°$ e. $\frac{2\pi}{3}$ f. π.

2. a. $4\left(\cos\,\pi + i\,sen\,\pi\right)$ b. $6\left(\cos\,\frac{3\pi}{2} + i\,sen\,\frac{3\pi}{2}\right)$
   c. $\cos\,\frac{5\pi}{3} + i\,sen\,\frac{5\pi}{3}$ d. $2\left(\cos\,\frac{11\pi}{6} + i\,sen\,\frac{11\pi}{6}\right)$
   e. $\sqrt{2\left(1+\cos\alpha\right)}\left(\cos\,\frac{\alpha}{2} + i\,sen\,\frac{\alpha}{2}\right)$ f. $\cos\,\frac{\pi}{2} + i\,sen\,\frac{\pi}{2}$
   g. $\sqrt{5}\left(\cos\,\theta + i\,sen\,\theta\right), \quad \theta = tg^{-1}\left(\frac{1}{2}\right) + \pi \approx 206.57°$ h. $\cos\,\frac{2\pi}{3} + i\,sen\,\frac{2\pi}{3}$

3. Sugerencia: usa la fórmula de De Moivre.

Ejercicios 1.3.1

1. Sugerencia: Considera el complejo $cos\,\theta + i\,sen\,\theta$ y elévalo al cuadrado.
2. $cos\left(4\theta\right) = cos^4\left(\theta\right) - 6cos^2\left(\theta\right)sen^2\left(\theta\right) + sen^4\left(\theta\right)$.
   $sen\left(6\theta\right) = 6\cos^5\left(\theta\right)sen\left(\theta\right) - 20\cos^3\left(\theta\right)sen^3\left(\theta\right) + 6\cos\left(\theta\right)sen^5\left(\theta\right)$.
3. Raíces sextas de 1 : $\left\{x=1\right\}, \left\{x=\frac{1}{2}+\frac{1}{2}i\sqrt{3}\right\}, \left\{x=-\frac{1}{2}+\frac{1}{2}i\sqrt{3}\right\}, \left\{x=-1\right\}$,
   $\left\{x=-\frac{1}{2}-\frac{1}{2}i\sqrt{3}\right\}, \left\{x=\frac{1}{2}-\frac{1}{2}i\sqrt{3}\right\}$.
   Raíces sextas de -1: $\left\{x=\frac{1}{2}\sqrt{3}+\frac{1}{2}i\right\}, \left\{x=i\right\}, \left\{x=-\frac{1}{2}\sqrt{3}+\frac{1}{2}i\right\}$,
   $\left\{x=-\frac{1}{2}\sqrt{3}-\frac{1}{2}i\right\}, \left\{x=-i\right\}, \left\{x=\frac{1}{2}\sqrt{3}-\frac{1}{2}i\right\}$.
4. a. $z = \pm\left(2-i\right)$.
   b. $z_j = \sqrt[4]{\sqrt{5}}\left(\cos\left(\frac{63.4°+360j}{4}\right) + i\cdot sen\left(\frac{63.4°+360j}{4}\right)\right) \quad j=0,1,2,3.$
   c. $z_j = \sqrt[6]{2}\left(\cos\left(\frac{\frac{\pi}{4}+2\pi j}{3}\right) + i\cdot sen\left(\frac{\frac{\pi}{4}+2\pi j}{3}\right)\right) \quad j=0,1,2.$
   d. $z_j = \left(\cos\left(\frac{\frac{\pi}{2}+2\pi j}{4}\right) + i\cdot sen\left(\frac{\frac{\pi}{2}+2\pi j}{4}\right)\right) \quad j=0,1,2,3.$
5. Sugerencia: a. Ve que cada una de ellas satisface la ecuación.
   b.. Ve que cada una de ellas satisface la ecuación y que son distintas.
6. Sugerencia: Si $n \nmid k$ entonces $\xi^k \neq 1$ y si $n \mid k$, entonces $\xi^k = 1$.
7. Sugerencia: Usa forma polar.
8. Sugerencia: $\left|z^2+1\right| \leq \left|z^2\right| + 1$.
9. $x_1 = 1+i,\ x_2 = 1-i, x_3 = -1+i, x_4 = -1-i$.
10. a. $\left(1 \pm i\right)^{16} = 256$ b. $\left(\frac{1+i}{(1-i)^2}\right) = -\frac{1}{2}+\frac{1}{2}i$
    c. $\left(\frac{34}{(1-45i)(5+3i)}\right)^2 = -\frac{7421}{1026169} + \frac{15540}{1026169}i$ d. $\left|\frac{(6+7i)(4-2i)}{4+2i}\right|\left|-\frac{1}{7+6i}\right| = 1.$

Capítulo 2

Ejercicios 2.1

1. a. $f(x)+g(x)=13x-6x^2+x^3$.
   b. $f(x)+g(x)=1+x^3+7x^4+5x^5-x^7$.
   c. $f(x)+g(x)=2+2x^{32}$.
   d. $f(x)+g(x)=x^3+\frac{5}{2}x^2+7x+\frac{1}{2}$.
2. a. $f(x)\cdot g(x)=-3x^5+15x^4-39x^3+42x^2$.
   b. $f(x)\cdot g(x)=x^3+5x^5+7x^7+35x^9-x^{10}-5x^{12}$.
   c. $f(x)\cdot g(x)=1+2x^{32}+x^{64}$.
   d. $f(x)\cdot g(x)=3x^5+\frac{11}{2}x^4-4x^3+\frac{13}{4}x^2+7x-\frac{1}{2}$.
6. **Sugerencia:**
   - Recuerda por qué si D es dominio entero, entonces $D[x]$ también lo es.
   - Determina la clase positiva.

Ejercicios 2.2.1

1. a. Cociente x^4-7x-1; residuo $49x+12$.
   b. Cociente 1; residuo 1.
   c. Cociente $2x^2-\frac{27}{2}x+\frac{137}{4}$; residuo $-\frac{697}{4}$.
   d. Cociente x^2-1; residuo 3.
2. Sugerencia: divide al polinomio $x^{m+1}+1$ entre $b(x)$.
3. Sugerencia: Revisa la demostración del teorema en general.

Ejercicios 2.2.2

1. a. Cociente x^2-x; residuo -1.
   b. Cociente $x^3-16x^2+34x-19$; residuo 2.
   c. Cociente x^3+6x^2-2x+1; residuo 1.
   d. Cociente $x^3+14x^2+78x+305$; residuo 1225.
2. b. $(x+1)^4-7(x+1)^3+19(x+1)^2-26(x+1)+15$.

3. a. $2(x-1)^7+14(x-1)^6+39(x-1)^5+57(x-1)^4+47(x-1)^3+21(x-1)^2+11(x-1)+5$.

Ejercicios 2.3.2

1. (2) $a(x)=d\left(d^{-1}a(x)\right)$

   (5) **Sugerencia:** Usa la definición.

3. a. m.c.d.$=x^2+2$, $g(x)=\frac{1}{3}$, $h(x)=-\frac{1}{3}x+\frac{2}{3}$.

   b. m.c.d.$=x^2+2x+1$, $g(x)=-\frac{1}{3}$, $h(x)=\frac{1}{3}x^2-\frac{1}{3}x-1$.

   c. m.c.d. $=x^4-x^3-x+1$, $g(x)=\frac{1}{3}$, $h(x)=-\frac{1}{3}x+\frac{1}{3}$.

   d. m.c.d. $=x-\sqrt{2}$, $g(x)=\frac{1}{\left(\sqrt{2}+\sqrt{3}\right)}$, $h(x)=-\frac{1}{\left(\sqrt{2}+\sqrt{3}\right)}$.

   e. m.c.d. $=x+i$, $g(x)=\frac{1}{3}i$, $h(x)=-\frac{1}{3}ix$.

   f. m.c.d.$=x-\frac{1}{2}$, $g(x)=-\frac{14}{25}x-\frac{17}{50}$, $h(x)=\frac{7}{25}x^2+\frac{1}{10}x+\frac{2}{25}$.

5. **Sugerencia:** Recuerda que el máximo común divisor de dos polinomios es combinación lineal de éstos.

6. **Sugerencia:** Revisa cuáles son las unidades en $\mathbb{Z}[x]$.

8. $m(x)=\frac{a(x)b(x)}{d(x)}=a(x)\frac{b(x)}{d(x)}=b(x)\frac{a(x)}{d(x)}$.

   $l(x)=a(x)p(x)=b(x)r(x) \Rightarrow \frac{a(x)}{d(x)}p(x)=\frac{b(x)}{d(x)}r(x) \Rightarrow \frac{a(x)}{d(x)}|r(x) \Rightarrow$

   $l(x)=b(x)\frac{a(x)}{d(x)}t(x)=m(x)t(x)$.

9. a. m.c.m.$=x^5+2x^3+x^2+2$.

   b. m.c.m.$=x^5-x^3-2x+x^2+1$.

13. **Sugerencia:** Analiza qué pasaría si $cp(x)$ fuera reducible.

14. a. irreducible.

   b. $x^3+2x^2+2x+1=(x+1)\left(x^2+x+1\right)$

   c. irreducible.

   d. irreducible.

e. irreducibe.

15. a. $\left(x-\sqrt[3]{2}\right)\left(x^2+\sqrt[3]{2}x+\sqrt[3]{4}\right)$.

b. $x^3+2x^2+2x+1=(x+1)\left(x^2+x+1\right)$

c. $\left(x^2+\sqrt{2}x+1\right)\left(x^2-\sqrt{2}x+1\right)$.

d. $x^4-x^2-1=$
$=\left(x-\frac{1}{2}\sqrt{\left(2+2\sqrt{5}\right)}\right)\left(x+\frac{1}{2}\sqrt{\left(2+2\sqrt{5}\right)}\right)\left(x-\frac{1}{2}\sqrt{\left(2-2\sqrt{5}\right)}\right)\left(x+\frac{1}{2}\sqrt{\left(2-2\sqrt{5}\right)}\right)$

e. Iirreducible.

Ejercicios 2.4.1

1. a. Residuo$=-1$.

b. Residuo $=9$.

c. Residuo $=870$.

2. a. $x^2+ix+2=(x-i)(x+2i)$

b. $x^8-1=(x-1)(x+1)\left(x^2+1\right)\left(x^4+1\right)$
$=(x-1)(x+1)(x+i)(x-i)\left(x-\left(\frac{1}{2}\sqrt{2}+\frac{1}{2}i\sqrt{2}\right)\right)\left(x-\left(\frac{1}{2}\sqrt{2}-\frac{1}{2}i\sqrt{2}\right)\right)$
$\left(x-\left(-\frac{1}{2}\sqrt{2}+\frac{1}{2}i\sqrt{2}\right)\right)\left(x-\left(-\frac{1}{2}\sqrt{2}-\frac{1}{2}i\sqrt{2}\right)\right)$

c. $x^4+x^2+1=\left(x^2-x+1\right)\left(x^2+x+1\right)=$
$=\left(x-\left(\frac{1}{2}+\frac{1}{2}i\sqrt{3}\right)\right)\left(x-\left(\frac{1}{2}-\frac{1}{2}i\sqrt{3}\right)\right)\left(x-\left(-\frac{1}{2}+\frac{1}{2}i\sqrt{3}\right)\right)\left(x-\left(-\frac{1}{2}-\frac{1}{2}i\sqrt{3}\right)\right)$

d. $x^4-2x^3-5x^2-2x+24=(x-2)(x-3)\left(x^2+3x+4\right)=$
$(x-2)(x-3)\left(x-\left(-\frac{3}{2}+\frac{1}{2}i\sqrt{7}\right)\right)\left(x-\left(-\frac{3}{2}-\frac{1}{2}i\sqrt{7}\right)\right)$.

e. $x^3-2=\left(x-\sqrt[3]{2}\right)\left(x-\left(-\frac{1}{2}\sqrt[3]{2}+\frac{1}{2}i\sqrt{3}\sqrt[3]{2}\right)\right)\left(x-\left(-\frac{1}{2}\sqrt[3]{2}-\frac{1}{2}i\sqrt{3}\sqrt[3]{2}\right)\right)$.

f. $x^3-5x^2-9x+13=(x-1)\left(x^2-4x-13\right)=$
$(x-1)\left(x-\left(2+\sqrt{17}\right)\right)\left(x-\left(2-\sqrt{17}\right)\right)$

3. $a(x)=x^n-1$
a. $a(-1)=(-1)^n-1$

b. $a(i)=\cos\frac{1}{2}n\pi-1+i\cdot sen\frac{1}{2}n\pi$.

c. $a(x+1)=(x+1)^n-1$

d. $a\left(x^n-1\right)=\left(x^n-1\right)^n-1$

4. a. $f(x)=(x-i)^4(x-\alpha)=$

$$= x^5 - x^4(\alpha + 4i) + (4i\alpha - 6)x^3 + x^2(6\alpha + 4i) + x(-4i\alpha + 1) - \alpha$$

b. $f(x) = x(x-1)(x-2)(x-3)(x-\alpha) =$
$$= x^5 - x^4(\alpha + 6) + x^3(6\alpha + 11) - x^2(11\alpha + 6) + 6\alpha x$$

c. $f(x) = (x-1)^2(x-i)^2(x-\alpha) =$
$= x^5 - x^4(\alpha + 2i + 2) + (2\alpha + 4i + 2i\alpha)x^3 - (4i\alpha - 2 + 2i)x^2 +$
$(-2\alpha - 1 + 2i\alpha)x + \alpha.$

d. $f(x) = (x-i)(x+i)(x+1)^2(x-\alpha) =$
$$= x^5 - x^4(\alpha - 2) - x^3(2\alpha - 2) - x^2(2\alpha - 2) - x(2\alpha - 1) - \alpha$$

8. **Sugerencia:** Recuerda que el conjugado de una suma es la suma de los conjugados y el conjugado de un producto es el producto de los conjugados.

Ejercicios 2.4.3

1. Solución: $\{x = -1\}, \left\{x = -\frac{1}{2} + \frac{1}{2}i\sqrt{7}\right\}, \left\{x = -\frac{1}{2} - \frac{1}{2}i\sqrt{7}\right\}.$
2. Solución: $\{x = 3\}, \left\{x = \frac{1}{2}\right\}, \{x = -3\}.$
3. Solución: $\{x = 2\}, \left\{x = \frac{1}{3}\right\}, \{x = -3\}.$
4. Solución: $\{x = 2\}, \left\{x = -\frac{1}{2}\right\}, \{x = -1\}.$
5. Solución: $\{x = 4\}, \{x = -6\}, \{x = 9\}.$
6. Solución: $\{x = -4\}, \{x = 2\}, \{x = -7\}.$
7. Solución: $\{x = 2\}, \left\{x = \frac{4}{3}\right\}, \left\{x = \frac{2}{3}\right\}.$
8. Solución: $\{x = 6\}, \{x = 2\}, \left\{x = \frac{2}{3}\right\}.$
9. Solución: $\{x = 2\}, \left\{\frac{1}{2} - \frac{1}{2}\sqrt{3}\right\}, \left\{\frac{1}{2} + \frac{1}{2}\sqrt{3}\right\}$ y $k = 2.$
10. $\dfrac{p^3}{27} + \dfrac{q^2}{4} = 0.$
12. Solución: $\left\{x = \frac{1}{2} + \frac{1}{2}i\sqrt{7}\right\}, \left\{x = \frac{1}{2} - \frac{1}{2}i\sqrt{7}\right\}, \left\{x = \frac{1}{2} + \frac{1}{2}\sqrt{5}\right\}, \left\{x = \frac{1}{2} - \frac{1}{2}\sqrt{5}\right\}.$
13. Solución: $\{x = 1\}, \left\{x = \frac{1}{2}\right\}, \left\{x = \sqrt{5}\right\}, \left\{x = -\sqrt{5}\right\}.$
14. Solución: $\{x = 2\}, \{x = 3\}, \{x = 1 + i\}, \{x = 1 - i\}.$
15. Solución: $\left\{x = -1 + \sqrt{2}\right\}, \left\{x = -1 - \sqrt{2}\right\}, \left\{x = \frac{1}{2} + \frac{1}{2}i\sqrt{3}\right\}, \left\{x = \frac{1}{2} - \frac{1}{2}i\sqrt{3}\right\}.$
16. Solución: $\left\{x = -\frac{1}{4} + \frac{1}{4}i\sqrt{7}\right\}, \left\{x = -\frac{1}{4} - \frac{1}{4}i\sqrt{7}\right\}, \{x = -3\}, \{x = -3\}.$

Ejercicios 2.4.4

1. Las derivadas de los polinomios son
   a. $25x^4 + 2x^3 + \frac{4}{3}x - 1$ en $\mathbb{Q}[x]$.
   b. $4x^3 + 2\sqrt{2}x$ en $\mathbb{R}[x]$.

c. $5x^4 - 3ix^2 + (6i+4)\,x + \sqrt{3}$ en $\mathbb{C}[x]$.

d. nx^{n-1} en $\mathbb{Q}[x]$.

e. $6\left(x^2+1\right)^2 x$ en $\mathbb{R}[x]$.

f. 1, con $a \in K$ (campo), en $K[x]$.

6. Factorización de polinomios usando el método de la derivada.

a. $x^5 + 4x^4 + 7x^3 + 8x^2 + 3x + 2 = x^5 + 4x^4 + 7x^3 + 8x^2 + 3x + 2$, es irreducible.

b. $d(x) = \left(x^6 + 6x^5 + 11x^4 + 12x^3 + 19x^2 + 6x + 9; 6x^5 + 30x^4 + 44x^3 + 36x^2 + 38x + 6\right)$
$= x^3 + 3x^2 + x + 3$
$(d(x); d'(x)) = \left(x^3 + 3x^2 + x + 3; 3x^2 + 6x + 1\right) = 1$
Como -3 es raíz de $d(x)$, $d(x) = x^3 + 3x^2 + x + 3 = (x+3)\left(x^2+1\right) \Longrightarrow$
$x^6 + 6x^5 + 11x^4 + 12x^3 + 19x^2 + 6x + 9 = (x+3)^2\left(x^2+1\right)^2$ en $\mathbb{Q}[x]$.

c. $\left(x^3 + ix^2 + x + i; 3x^2 + 2ix + 1\right) = x + i$
$\dfrac{x^3 + ix^2 + x + i}{(x+i)^2} = x - i \Longrightarrow x^3 + ix^2 + x + i = (x+i)^2(x-i)$

d. $(f(x); f'(x)) = \left(x^4 - 15x^2 - 28x - 12; 4x^3 - 30x - 28\right) = x + 2$
$\Longrightarrow \frac{x^4 - 15x^2 - 28x - 12}{(x+2)^2} = x^2 - 4x - 3 \Longrightarrow f(x) = (x+2)^2\left(x^2 - 4x - 3\right)$
$\Longrightarrow f(x) = (x+2)^2\left(x - \left(2+\sqrt{7}\right)\right)\left(x - \left(2-\sqrt{7}\right)\right)$.

e. $f(x) = x^3 + \left(2\sqrt{2} + \sqrt{3}\right)x^2 + \left(2 + 2\sqrt{6}\right)x + 2\sqrt{3}$
$(f(x); f'(x)) = \left(x + \sqrt{2}\right) \Longrightarrow f(x) = \left(x+\sqrt{2}\right)^2\left(x+\sqrt{3}\right)$.

f. $f(x) = x^4 + x^3 + x + 1$
$(f(x); f'(x)) = x + 1 \Longrightarrow f(x) = (x+1)^2\left(x^2 - x + 1\right)$ ya que $x^2 - x + 1$ es irreducible en $\mathbb{Q}[x]$.

7. Usa que $\left(a(x); a'(x)\right) \neq 1$ para probar que los siguientes polinomios no son irreducibles en $Q[x]$.

a. $f(x) = x^4 + 2x^3 + 3x^2 + 2x + 1$
$(f(x); f'(x)) = x^2 + x + 1 \neq 1 \Longrightarrow f(x)$ no es irreducible.

b. $f(x) = 4x^3 + 16x^2 + 21x + 9$
$(f(x); f'(x)) = 3 + 2x \neq 1 \Longrightarrow f(x)$ no es irreducible.

c. $f(x) = x^6 + x^4 - x^2 - 1$
$\frac{f(x)}{f'(x)} = \frac{1}{6}x + \frac{\frac{1}{3}x^4 - \frac{2}{3}x^2 - 1}{6x^5 + 4x^3 - 2x}$; $\frac{f'(x)}{x^4 - 2x^2 - 3} = 6x + \frac{16x^3 + 16x}{x^4 - 2x^2 - 3}$; $\frac{x^4 - 2x^2 - 3}{x^3 + x} =$
$x + \frac{-3x^2 - 3}{x^3 + x}$; $\frac{x^3 + x}{x^2 + 1} = x \Longrightarrow (f(x); f'(x)) = x^2 + 1$.

$\Longrightarrow f(x) = \left(x^2+1\right)^2\left(x^2-1\right) = \left(x^2+1\right)^2(x-1)(x+1)$.

8. $b(x)^2 \Big| a(x) \Longleftrightarrow b(x) | a'(x) \Longleftrightarrow b(x) | (a(x); a'(x))$.

9. Multiplicidad de factores en $a(x)$ usando $(a(x); a'(x))$.
   a. $\left(x^4+x^3+x^2+x+1; 4x^3+3x^2+2x+1\right) = 1 \Longrightarrow a(x)$ no tiene factores múltiples en $\mathbb{Q}[x]$.
   b. $\left(x^3+2x-1; 3x^2+2\right) = 1 \Longrightarrow a(x)$ no tiene factores múltiples en $\mathbb{Q}[x]$.
   c. $\left(x^n-1; nx^{n-1}\right) = 1 \Longrightarrow a(x)$ no tiene factores múltiples en $\mathbb{Q}[x]$.
   d. $\left(x^5+3x^2+2x-4; 5x^4+6x+2\right) = 1 \Longrightarrow a(x)$ no tiene factores múltiples en $\mathbb{Q}[x]$.

Ejercicios 2.5.1

2. **Sugerencia:** Recuerda cómo son los irreducibles en $\mathbb{R}[x]$.

4. a. $\left(x^3+6x^2-24x+160\right) = \left(x-\left(2-2i\sqrt{3}\right)\right)\left(x^2+x\left(8-i2\sqrt{3}\right)-20-20i\sqrt{3}\right) =$
   $= \left(x-\left(2-2i\sqrt{3}\right)\right)\left(x-\left(2+2i\sqrt{3}\right)\right)(x+10)$.

   b. $x^3+(1-2i)x^2-(1+2i)x-1 = (x-\alpha)^2(x-\beta) \Longrightarrow$
   $x^3+(1-2i)x^2-(1+2i)x-1 = x^3-x^2(\beta+2\alpha)+x\left(2\alpha\beta+\alpha^2\right)-\alpha^2\beta \Longrightarrow$
   $$\left.\begin{array}{l}\beta+2\alpha = -(1-2i)\\ 2\alpha\beta+\alpha^2 = -(1+2i)\\ \alpha^2\beta = 1\end{array}\right\} \Longrightarrow \alpha = i \text{ y } \beta = -1.$$

   c. $x^5-3x^4+4x^3-4x+4 = (x-(1+i))^2(x-(1-i))^2(x+1)$

5. a. $a(x) = x^5+(5+i)x^4+(25+5i)x^3-(55+25i)x^2+(34+55i)x-34i$
   b. $a(x) = x^3-3ix^2-3x+i$.
   c. $a(x) = x^4-2x^3+3x^2-2x+2$
   d. $b=-11, \quad c=20$.

6. **Sugerencia:** Usa el Teorema Fundamental del Álgebra y el ejercicio (8) de 2.4.1.

8. Las raíces son: $-1.0203+0.17343i \quad -0.61631-1.0371i \quad -0.456+0.49029i$
   $0.15289+1.0878i \quad 0.7486-1.0078i \quad 1.1911+0.29342i$

Ejercicios 2.5.2

1. a. $\frac{3}{2}$ b. $\frac{2}{3}$ c. $-\frac{1}{2}, \frac{1}{2}, \frac{1}{4}$
   d. No tiene raíces racionales e. No tiene raíces racionales f. $\frac{1}{2}$

5. a. $x^4 - 1 = (x-1)(x+1)\left(x^2+1\right)$

   b. $2x^4 - x^3 + 2x^2 + x - 1 = (2x-1)\left(x^3+x+1\right)$

   c. $x^4 + x^2 + 1 = \left(x^2 - x + 1\right)\left(x^2 + x + 1\right)$

   d. $x^5 + x^4 - 6x^3 - 16x^2 + 15x + 30 = x^5 + x^4 - 6x^3 - 16x^2 + 15x + 30$.

Ejercicios 2.5.3

6. (a) y (d) son rreducibles por el Criterio de Einsenstein.
   (b) y (c) no se puede saber si son irreducibles con el Criterio de Einsenstein.
7. **Sugerencia:** Prueba que en el polinomio $1 + (x+1) + (x+1)^2 + ... + (x+1)^{p-1}$ el coeficiente de x^i es $\sum_{k=i}^{p-1} \binom{k}{i} = \binom{p}{i+1}$, $\forall\ 0 \leq i \leq p-1$ y ve que se cumplen las hipótesis del Criterio de Eisenstein con el número primo p.

ÍNDICE DE EJERCICIOS