APUNTES DEL CURSO MA-0370

ADRIÁN BARQUERO SÁNCHEZ

ÍNDICE

1. Anillos de polinomios en una y varias variables

1.1. Anillos. En esta sección vamos a dar un repaso de las definiciones y propiedades básicas sobre anillos de polinomios en una y varias variables. Empezamos recordando la definición del concepto de anillo.

Definición 1.1. Decimos que un conjunto no vacío A con dos operaciones binarias $+$ y $\cdot$ es un *anillo* si satisface las siguientes propiedades:

1. La suma es asociativa: $a + (b + c) = (a + b) + c$ para todo $a, b, c \in A$.
2. Existe un elemento neutro para la suma: $0_A \in A$ tal que $a + 0_A = 0_A + a = a$ para todo $a \in A$.
3. Existen inversos aditivos, *i.e.* para todo $a \in A$ existe un elemento $b \in A$ tal que $a + b = b + a = 0_A$. Este elemento es único y se denota por $-a$.
4. La suma es conmutativa: $a + b = b + a$ para todos $a, b \in A$.
5. El producto es asociativo: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, para todo $a, b, c \in A$.
6. Existe un neutro multiplicativo 1_A tal que $1_A \cdot a = a \cdot 1_A = a$ para todo $a \in A$.
7. Se cumplen las leyes de distributividad

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{y} \quad (a + b) \cdot c = a \cdot c + b \cdot c$$

para todo $a, b, c \in A$.

♦

A veces un anillo se denota como un triplete $(A, +, \cdot)$. Si además el producto es conmutativo, es decir, si $a \cdot b = b \cdot a$ para todo $a, b \in A$, entonces decimos que el anillo es *conmutativo*. Para no recargar la notación, usualmente denotamos la multiplicación por yuxtaposición, es decir $a \cdot b$ lo denotamos por ab.

Ejemplo 1.2. Los conjuntos de números $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ son ejemplos de anillos conmutativos. ◇

Ejemplo 1.3. El conjunto de clases de equivalencia módulo n, para $n \in \mathbb{Z}_{\geq 1}$, usualmente denotado por $\mathbb{Z}/n\mathbb{Z}$, es un anillo conmutativo finito. ◇

Ejemplo 1.4. El conjunto $\mathbb{N} = \{0, 1, 2, \dots\}$ de los números naturales con la suma y multiplicación usual de enteros no es un anillo, pues por ejemplo no hay inversos aditivos en general. ◇

Definición 1.5. Un conjunto F se llama *cuerpo* si F es un anillo conmutativo con $1_F \neq 0_F$ y si todo elemento no cero de F tiene un inverso multiplicativo, es decir: para todo $a \in F$ con $a \neq 0_F$ existe $b \in F$ tal que $ab = ba = 1_F$. ♦

Usualmente denotamos al inverso multiplicativo de a como a^{-1}. Es fácil demostrar que éste inverso es único.

Definición 1.6. Si A es un anillo, un subconjunto no vacío B de A se llama un *subanillo* de A si B forma un anillo con las mismas operaciones suma y producto heredadas de A, y es cerrado con respecto a ambas operaciones. ♦

Ejemplo 1.7.
1. $\mathbb{Z}$ es un subanillo de $\mathbb{Q}$ y $\mathbb{Q}$ es un subanillo de $\mathbb{R}$.
2. El conjunto $\mathbb{Q}(\sqrt{2}) := \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ es un subanillo de $\mathbb{R}$. (Además es un cuerpo).

◇

Definición 1.8. Sean A y B anillos. Una función $\phi : A \to B$ se llama un *homomorfismo de anillos* si para todo $a, b \in A$:

1. $\phi(a + b) = \phi(a) + \phi(b)$.
2. $\phi(a \cdot b) = \phi(a) \cdot \phi(b)$
3. $\phi(1_A) = 1_B$.

♦

1.2. Polinomios en una variable. Sea A un anillo conmutativo. Un polinomio en la variable x con coeficientes en A es una expresión formal infinita

$$a_0 + a_1x + a_2x^2 + \cdots$$

tal que $a_i \in A$ para todo $i \geq 0$ y además existe un entero $n \geq 0$ tal que $a_i = 0$ para todo $i > n$. Los a_i son llamados los coeficientes del polinomio y a_i es llamado el coeficiente de x^i. Si $a_n \neq 0_A$ y $a_i = 0_A$ para todo $i > n$ entonces escribimos simplemente el polinomio como $a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$.
Dos polinomios

$$f(x) = a_0 + a_1x + \cdots \quad \text{y} \quad g(x) = b_0 + b_1x + \cdots$$

son iguales si y sólo si todos sus coeficientes son iguales, es decir $a_i = b_i$ para todo $i \geq 0$.

Denotamos por $A[x]$ al conjunto de todos los polinomios en la variable x con coeficientes en A. Se puede demostrar que $A[x]$ es un anillo conmutativo con la adición y multiplicación usual de polinomios, esto es, si $f(x)$ y $g(x)$ son como en el párrafo anterior, se definen

$$f(x) + g(x) := (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \cdots$$
$$f(x)g(x) := c_0 + c_1x + c_2x^2 + \cdots,$$

donde $c_n := a_0b_n + a_1b_{n-1} + \cdots + a_{n-1}b_1 + a_nb_0$ para cada $n \geq 0$. Note que cada producto a_ib_j en la definición del coeficiente c_n satisface $i + j = n$.
Si $f(x) = a_0+a_1x+\cdots+a_nx^n$ con $a_n \neq 0$ decimos que el grado de $f(x)$ es n y lo denotamos por $\text{grado}(f(x)) = n$. A a_n le llamamos el *coeficiente principal* de $f(x)$ y a_0 el *coeficiente constante*. Decimos que el polinomio 0 tiene grado $-\infty$ y que un polinomio de la forma $f(x) = a_0$ con $a_0 \in A$ es *constante*.

Teorema 1.9. *Si F es un cuerpo y $f(x), g(x)$ son polinomios en $F[x]$ entonces* $\text{grado}(f(x)g(x)) = \text{grado}(f(x)) + \text{grado}(f(x))$.

Teorema 1.10 (Algoritmo de la división)**.** *Sea F un cuerpo, y sean $f(x), g(x) \in F[x]$ Si $g(x) \neq 0$, entonces existen $q(x), r(x) \in F[x]$ tales que*

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

con $r(x) = 0$ o con $\text{grado}(r(x)) < \text{grado}(g(x))$.

Definición 1.11. Sea A un subanillo de un anillo conmutativo B. Sea $f(x) \in A[x]$ un polinomio. Definimos la función polinomial asociada $f_B : B \to B$ por:

$$f_B(b) := f(b) = a_0 + a_1b + a_2b^2 + \cdots + a_nb^n$$

para $b \in B$. Si $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$. ♦

Definición 1.12. Sea A un subanillo de un anillo conmutativo B. Si $c \in B$, definimos la función:

$$\begin{aligned} \text{ev}_c : A[x] &\longrightarrow B \\ f(x) &\longmapsto f_B(c) = f(c) \end{aligned}$$

A la función ev_c la llamamos *homomorfismo de evaluación en c*, pues resulta ser un homomorfismo de anillos. Esto quiere decir que si $f(x), g(x) \in A[x]$, entonces $\text{ev}_c(f(x) + g(x)) = \text{ev}_c(f(x)) + \text{ev}_c(g(x))$, o en otras palabras, que $(f + g)(c) = f(c) + g(c)$ y similarmente para la multiplicación, que $(fg)(c) = f(c)g(c)$. ♦

Definición 1.13. Si F es un cuerpo y $f(x) = a_0 + a_1x + \cdots + a_nx^n \in F[x]$, decimos que un elemento $\alpha \in F$ es una *raíz o cero* de $f(x)$ si $f(\alpha) = 0$. ♦

Teorema 1.14 (Del factor)**.** *Sea F un cuerpo y sea $\alpha \in F$ y $f(x) \in F[x]$. Entonces $f(\alpha) = 0$ si y sólo si $x - \alpha$ divide a $f(x)$ en $F[x]$, es decir si y sólo si existe $g(x) \in F[x]$ tal que $f(x) = g(x)(x - \alpha)$.*

Corolario 1.15. *Sea F un cuerpo y $f(x) \in F[x]$ un polinomio de grado n, entonces $f(x)$ tiene a lo sumo n raíces distintas en F.*

Corolario 1.16. *Sea F un cuerpo infinito y sea S un subconjunto infinito de F. Si $f(x) \in F[x]$ cumple que $f(c) = 0$ para todo $c \in S$ entonces $f(x)$ es el polinomio cero. En particular si $f(x), g(x) \in F$ son tales que $f(c) = g(c)$ para todo $c \in S$ entonces $f(x) = g(x)$.*

Definición 1.17. Sea F un cuerpo y sea $f(x) \in F[x]$ un polinomio. Decimos que $f(x)$ es irreducible en $F[x]$ (o irreducible sobre F) si $f(x)$ no es constante y si $f(x)$ no puede escribirse como el producto de dos polinomios no constantes. Si un polinomio no constante no es irreducible sobre F decimos que es reducible. ♦

Teorema 1.18 (De factorización única)**.** *Sea F un cuerpo y sea $f(x)$ un polinomio no constante en $F[x]$, entonces existen polinomios irreducibles $f_1(x), \dots, f_k(x) \in F[x]$ tales que:*

$$f(x) = f_1(x) \dots f_k(x)$$

En ésta factorización los polinomios irreducibles $f_j(x)$ son únicos bajo permutaciones o multiplicaciones por constantes, más formalmente: si existe otra factorización $f(x) = g_1(x) \dots g_n(x)$ de $f(x)$ como producto de irreducibles entonces $k = n$ y existe una permutación (biyección) $\sigma : \{1, 2, \dots, k\} \to \{1, 2, \dots, k\}$ y constantes $c_1, \dots, c_k \in F$ tales que para todo $i = 1, \dots, k$ se tiene $g_i(x) = c_i f_{\sigma(i)}(x)$.

1.3. Polinomios en varias variables. Sea F un cuerpo y sean $t_1, \dots, t_n$ variables independientes. De manera análoga a la definición de polinomios en una variable, podemos definir en anillo de polinomios en las variables $t_1, \dots, t_n$ con coeficientes en F de manera recursiva como

$$F[t_1, \dots, t_n] := F[t_1, \dots, t_{n-1}][t_n] = \cdots = F[t_1][t_2] \dots [t_n]$$

Por ejemplo el elemento $x^3y^2 + (2x - 1)y - 5x^7$ es un miembro de $A[y] = F[x][y] = F[x, y]$. Es un polinomio en la variable y con coeficientes $a_0 = -5x^7, a_1 = 2x - 1, a_2 = x^3 \in F[x]$.
Un elemento de $F[t_1, \dots, t_n]$ es una suma formal:

$$f(t_1, \dots, t_n) = \sum_{i_1, \dots, i_n} a_{i_1, \dots, i_n} {t_1}^{i_1} \dots {t_n}^{i_n}$$

donde los i_j varían en $\mathbb{N}_{\geq 0}$ y los $a_{i_1 \dots i_n} \in F$, y además existen unos d_j tales que los coeficientes $a_{i_1 \dots i_n} = 0$ si $i_j > d_j$ para todo $j = 1, \dots, n$.
Este polinomio se puede escribir también como:

$$f(t_1, \dots, t_n) = \sum_{i_n=0}^{d_n} \Big(\sum_{i_1, \dots, i_{n-1}} a_{i_1 \dots i_{n-1}} {t_1}^{i_1} \dots {t_{n-1}}^{i_{n-1}} \Big) {t_n}^{i_n} = \sum_{k=0}^{d_n} f_j(t_1, \dots, t_{n-1}) t_n^k$$

donde los polinomios $f_j \in F[t_1, \dots, t_{n-1}]$.
La notación se puede simplificar usando la notación de multi-índices, donde abreviamos:

$$a_{i_1 \dots i_n} = a_{(i)}$$
$${t_1}^{i_1} \dots {t_n}^{i_n} = t^{(i)}$$

donde $(i) = (i_1, \dots, i_n)$, entonces así de manera más sencilla podemos escribir $f(t_1, \dots, t_n) = \sum_{(i)} a_{(i)} t^{(i)}$.
A cada término $a_{(i)} {t_1}^{i_1} \dots {t_n}^{i_n}$ le llamamos un *monomio*, y si $a_{(i)} \neq 0$ definimos su grado como:

$$\text{grado}(a_{(i)} {t_1}^{i_1} \dots {t_n}^{i_n}) := i_1 + \cdots + i_n$$

Decimos que un polinomio $f(t_1, \dots, t_n) \in F[t_1, \dots, t_n]$ es *homogéneo* de grado d si todos sus términos monomiales con $a_{(i)} \neq 0$ tienen grado d, es decir $i_1 + \cdots + i_n = d$.

Ejemplo 1.19. El polinomio $f(x,y,z) \in \mathbb{R}[x,y,z]$ dado por

$$f(x,y,z) = 7x^2yz^2 - 2xy^3z^3$$

no es homogéneo pues el $\text{grado}(7x^2yz^3) = 6$ y $\text{grado}(-2xy^3z^5) = 9$. Sin embargo el polinomio $g(x,y,z) \in \mathbb{R}[x,y,z]$ dado por

$$g(x,y,z) = 5x^2y - 4xy^2 + 23xyz$$

sí es homogéneo, de grado 3. ◇

Definición 1.20. Si $f(t_1,\ldots,t_n) \in F[t_1,\ldots,t_n]$ no es el polinomio cero, definimos el *grado total* o *grado* de f como el máximo grado de todos los monomios que lo conforman. Es decir, si

$$f(t_1,\ldots,t_n) = \sum_{i_1,\ldots,i_n} a_{i_1,\ldots,i_n} {t_1}^{i_1} \ldots {t_n}^{i_n}$$

Entonces el grado total de $f(t_1,\ldots,_n)$ está dado por:

$$\text{grado}(f(t_1,\ldots,t_n)) = \max_{(i_1,\ldots,i_n)}\{\text{grado}(a_{i_1,\ldots,i_n} {t_1}^{i_1} \ldots {t_n}^{i_n})\}$$

⧫

Dado un polinomio $f(t_1,\ldots,t_n) \in F[t_1,\ldots,t_n]$, éste se puede escribir de manera única como una suma de polinomios homogéneos de grado menores o iguales a $\text{grado}(f)$. Explícitamente si $\text{grado}(f) = d$, entonces podemos escribir $f = f_0 + \cdots + f_d$, donde

$$f_k(t_1,\ldots,t_n) = \sum_{i_1+\cdots+i_n=k} a_{i_1,\ldots,i_n} {t_1}^{i_1} \ldots {t_n}^{i_n}$$

Para $0 \leq k \leq d$. Observe sin embargo, que en esta descomposición algunos de los polinomios f_k pueden ser cero.

Ejemplo 1.21. Considere el polinomio $f(x,y,z) \in \mathbb{Q}[x,y,z]$, dado por

$$f(x,y,z) = 5x^2y^2 - 7x^3y + 9xy - 2xy^3 + 2x - 21.$$

Note que $\text{grado}(f) = 4$. Entonces podemos escribir

$$f = f_{(0)} + f_{(1)} + f_{(2)} + f_{(3)} + f_{(4)},$$

donde $f_{(0)} = -21, f_{(1)} = 2x, f_{(2)} = 9xy, f_{(3)} = 0$ y $f_{(4)} = 5x^2y^2 - 7x^3y - 2x^3y$. ◇

Teorema 1.22. *Sean $f,g \in F[t_1,..,t_n]$, donde F es cuerpo. Entonces* $\text{grado}(fg) = \text{grado}(f) + \text{grado}(g)$.

Demostración: Si alguno f o g es el polinomio cero, entonces la igualdad simplemente dice que $-\infty = -\infty$. Supongamos entonces que $f \neq 0$ y $g \neq 0$. Sean $d_1 = \text{grado}(f)$ y $d_2 = \text{grado}(g)$. Entonces podemos descomponer $f = f_0 + \cdots + f_{d_1}$ y $g = g_0 + \cdots + g_{d_2}$. De esta manera:

$$fg = (f_0g_0) + (f_0g_1 + f_1g_0) + \cdots + (f_{d_1}g_{d_2})$$

De donde vemos que $\text{grado}(fg) = \text{grado}(f_{d_1}g_{d_2}) = d_1 + d_2 = \text{grado}(f) + \text{grado}(g)$. □

Definición 1.23. Sea F un cuerpo y sea $f(t_1,\ldots,t_n) \in F[t_1,\ldots t_n]$. Se dice que f es irreducible en $F[t_1,\ldots,t_n]$ (o irreducible sobre F) si f no es constante y además f no se puede escribir como el producto de dos polinomios no constantes en $F[t_1,\ldots,t_n]$. ⧫

Teorema 1.24 (De factorización única)**.** *Sea F un cuerpo y sea f un polinomio no constante en $F[t_1,\ldots,t_n]$, entonces existen polinomios irreducibles $f_1,\ldots,f_k \in F[t_1,\ldots,t_n]$ tales que:*

$$f(x) = f_1 \cdot \cdots \cdot f_k$$

En ésta factorización los polinomios irreducibles f_j son únicos bajo permutaciones o multiplicaciones por constantes, más formalmente: si existe otra factorización $f = g_1 \cdot \cdots \cdot g_n$ de f como producto de irreducibles entonces $k = n$ y existe una permutación (biyección) $\sigma : \{1,2,\ldots,k\} \to \{1,2,\ldots,k\}$ y constantes $c_1,\ldots,c_k \in F$ tales que para todo $i = 1,\ldots,k$ se tiene $g_i = c_i f_{\sigma(i)}$.

Definición 1.25. Sea F un cuerpo. A cada polinomio $f(t_1,\dots,t_n) \in F[t_1,..,t_n]$ le corresponde una función polinomial asociada: $f_{F^n} : F^n \to F$, definida de la siguiente manera: si $x=(x_1,\dots,x_n)\in F^n$, y si

$$f(t_1,\dots,t_n)=\sum_{i_1,\dots,i_n} a_{i_1,\dots,i_n} {t_1}^{i_1}\dots {t_n}^{i_n}$$

Entonces

$$f_{F^n}(x)=f_{F^n}(x_1,\dots,x_n):=\sum_{i_1,\dots,i_n} a_{i_1,\dots,i_n} {x_1}^{i_1}\dots {x_n}^{i_n}$$

♦

Recuerde que $F^n = F\times\cdots\times F=\{(x_1,\dots,x_n)\mid x_i\in F,\, i=1,\dots,n\}$ es el producto cartesiano de F consigo mismo tomado n veces.

Definición 1.26. Sea F un cuerpo y sea $x=(x_1,\dots,x_n)\in F^n$. Entonces el *homomorfismo de evaluación en* x es el homomorfismo de anillos:

$$\begin{aligned} \mathrm{ev_x} : F[t_1,\dots,t_n] &\longrightarrow F \\ f(t_1,\dots,t_n) &\longmapsto f(x)=f(x_1,\dots,x_n) \end{aligned}$$

♦

Teorema 1.27. *Sea F un cuerpo infinito y sea $f\in F(t_1,\dots,t_n]$, si la función polinomial asociada*

$$\begin{aligned} f_{F^n} : F^n &\longrightarrow F \\ x &\longmapsto f(x) \end{aligned}$$

es idénticamente cero (es decir $f_{F^n}(x)=0$ para todo $x\in F^n$), entonces f es el polinomio cero en $F[t_1,\dots,t_n]$. Además si $f,g\in F[t_1,\dots,t_n]$ son tales que sus funciones polinomiales coinciden (es decir $f_{F^n}=g_{F^n}$) entonces $f=g$ en $F[t_1,\dots,t_n]$.

Demostración. Vamos a proceder por inducción sobre el número de variables n. El caso $n=1$ es el Corolario 1.14. Supongamos que el resultado es cierto para polinomios en $F[t_1,\dots,t_k]$ con $k<n$. Consideremos f como un miembro de $F[t_1,\dots,t_{n-1}][t_n]$, entonces podemos escribir:

$$f=\sum_{j=0}^{d} f_j(t_1,\dots,t_{n-1})t_n^j$$

Para demostrar que f es el polinomio cero en $F[t_1,\dots,t_n]$ debemos mostrar que $f_j(t_1,\dots,t_{n-1})=0$ para todo $j=0,\dots,d$. Probemos que $(f_j)_{F^{n-1}}$ son todas idénticamente cero. Sea $\alpha=(\alpha_1,\dots,\alpha_{n-1})\in F^{n-1}$ cualquiera. Entonces note que:

$$f(\alpha_1,\dots,\alpha_{n-1},t_n)=\sum_{j=0}^{d} f_j(\alpha_1,\dots,\alpha_{n-1})t_n^j \in F[t_n]$$

Ahora este polinomio en la variable t_n tiene infinitas ráices, pues por hipótesis del Teorema $f(\alpha_1,\dots,\alpha_{n-1},\beta)=0$ para todo $\beta\in F$. Entonces por Corolario 1.14 $f(\alpha_1,\dots,\alpha_{n-1},t_n)=0$ en $F[t_n]$. Esto quiere decir que sus coeficientes $f_j(\alpha_1,\dots,\alpha_{n-1})=0$ para todo $j=0,\dots,d$. Pero ésto sucede para todo $(\alpha_1,\dots,\alpha_{n-1})\in F^{n-1}$, luego por hipótesis de inducción concluimos que $f_j(t_1,\dots,t_{n-1})=0$ en $F[t_1,\dots,t_{n-1}]$ para todo $j=0,\dots,d$.
Entonces concluimos que:

$$f=\sum_{j=0}^{d} f_j(t_1,\dots,t_{n-1})t_n^j=\sum_{j=0}^{d} 0\cdot t_n^j=0.$$

En $F[t_1,\dots,t_n]$, que es lo que se deseaba demostrar. La segunda parte del teorema es inmediata al tomar $h=f-g$. □

Ejemplo 1.28. El resultado del teorema anterior no es cierto en general si el cuerpo no es infinito. Por ejemplo considere el conjunto finito $\mathbb{F}_2 := \{0, 1\}$. Se pueden establecer operaciones binarias de suma $+$ y multiplicación $\cdot$ sobre $\mathbb{F}_2$, de acuerdo a las siguientes tablas de valores.

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Una verificación trivial muestra que con éstas operaciones $\mathbb{F}_2$ es un cuerpo. Note que si $f(x) := x^2 \in \mathbb{F}_2[x]$ y $g(x) := x \in \mathbb{F}_2[x]$ entonces sus funciones polinomiales asociadas son iguales, porque $f(0) = g(0) = 0$ y $f(1) = g(1) = 1$ pero $f(x) \neq g(x)$ como polinomios de $\mathbb{F}_2[x]$. El cuerpo $\mathbb{F}_2$ se conoce comúnmente como el cuerpo con dos elementos. $\diamond$

EJERCICIOS

Ejercicios de la sección 1.

1.1 Verifique que el conjunto $\mathbb{F}_2 := \{0, 1\}$ con las operaciones binarias definidas en el Ejemplo 1.28 forma un cuerpo.

1.2 Demuestre que el subconjunto $\mathbb{Q}(\sqrt{2}) := \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ de $\mathbb{R}$ es un cuerpo, con las operaciones de suma y multiplicación heredadas de $\mathbb{R}$.

1.3 Sea F un cuerpo. Demuestre que si $x, y \in F^\times := F \setminus \{0\}$ entonces $xy \neq 0$.

1.4 Demuestre el Teorema 1.10. (**Sugerencia:** Una opción es hacer inducción sobre el grado de $f(x)$. Para el paso inductivo, considere el procedimiento que utiliza al hacer la división larga de polinomios.)

1.5 Demuestre el Teorema 1.14.

1.6 Sean $f(x) := x^5 + x^3 + 1 \in \mathbb{F}_2[x]$ y $g(x) := x^2 + x + 1 \in \mathbb{F}_2[x]$. Lleve a cabo el algoritmo de la división para encontrar los únicos polinomios $q(x), r(x) \in \mathbb{F}_2[x]$ tales que $f(x) = q(x)g(x) + r(x)$ con $\operatorname{grad}(r(x)) < 2$.

1.7 Sea F un cuerpo y sea $f(x) \in F[x]$ un polinomio con $2 \leq \operatorname{grad}(f(x)) \leq 3$. Demuestre que $f(x)$ es irreducible en $F[x]$ sí y solo sí $f(x)$ no tiene raíces en el cuerpo F.

1.8 Sea $f(x) \in \mathbb{Z}[x]$ dado por $f(x) = a_n x^n + \cdots + a_1 x + a_0$. Demuestre que si $\alpha = \frac{p}{q} \in \mathbb{Q}$ es una raíz de $f(x)$, con $p, q \in \mathbb{Z}$ y $\operatorname{mcd}(p, q) = 1$, entonces $p|a_0$ y $q|a_n$. Este resultado se conoce como el Teorema de las raíces racionales.

1.9 Sea F un cuerpo y sean $f, g \in F[t_1, \ldots, t_n]$ polinomios homogéneos con $\operatorname{grad}(f) = d$ y $\operatorname{grad}(g) = e$, respectivamente. Demuestre que su producto fg es un polinomio homogéneo de grado $d + e$.

1.10 Demuestre que el polinomio $f(x, y) := y^2 - x^3$ es irreducible en $\mathbb{Q}[x, y]$. (**Sugerencia:** Considere el polinomio $y^2 - x^3$ como un polinomio en $\mathbb{Q}[x][y]$.)

1.11 Sea F un cuerpo. Demuestre que hay infinitos polinomios irreducibles en $F[x]$. (**Sugerencia:** Si el cuerpo F es infinito entonces los polinomios lineales $x - \alpha$ para $\alpha \in F$ forman una familia infinita de polinomios irreducibles en $F[x]$. Sin embargo, este argumento no funciona si el cuerpo F es finito. En general, puede proceder con una variación del argumento clásico de Euclides para demostrar que hay infinitos números primos.)

1.12 Sea F un cuerpo y sean $f(x), g(x) \in F[x]$ polinomios con $\mathrm{grad}(g(x)) \geq 1$. Demuestre que existen polinomios únicos $f_0(x), \ldots, f_r(x) \in F[x]$ tales que

$$f(x) = f_0(x) + f_1(x)g(x) + f_2(x)g(x)^2 + \cdots + f_r(x)g(x)^r,$$

donde $\mathrm{grad}(f_i(x)) < \mathrm{grad}(g(x))$ para todo $0 \leq i \leq r$.

Este resultado esencialmente lo que da es una expansión de $f(x)$ en "base $g(x)$". Es completamente análogo al hecho de que si b es un entero ≥ 2, entonces todo entero $n \geq 0$ se puede expandir en base b de manera única, es decir, existen enteros únicos $a_0, \ldots, a_r \in \mathbb{Z}_{\geq 0}$ tales que

$$n = a_0 + a_1 b + a_0 b^2 + \cdots + a_r b^r$$

con $0 \leq a_i < b$ para todo $0 \leq i \leq r$.

1.13 (**Expansión de Taylor de un polinomio multivariable**) Sea F un cuerpo y sean $\alpha_1, \ldots, \alpha_n$ elementos arbitrarios de F. Demuestre que cada polinomio $f(t_1, \ldots, t_n) \in F[t_1, \ldots, t_n]$ tiene una expansión de Taylor (finita) alrededor del punto $(\alpha_1, \ldots, \alpha_n) \in F^n$, es decir, demuestre que $f(t_1, \ldots, t_n)$ se puede escribir en la forma

$$f(t_1, \ldots, t_n) = \sum_{(i)=(i_1,\ldots,i_n)\in\mathbb{N}^n} c_{(i)}(t_1 - \alpha_1)^{i_1} \cdots (t_n - \alpha_n)^{i_n},$$

donde $c_{(i)} \in F$ para todo $(i) \in \mathbb{N}^n$ y ademas $c_{(i)} = 0$ para casi todo $(i) \in \mathbb{N}^n$.

2. Coordenadas Polares

En esta sección describiremos un sistema de coordenadas llamado el *sistema coordenado polar*, que fue introducido independientemente por Grégoire de Saint-Vincent (1584-1667) y por Bonaventura Cavalieri (1598-1647) a mediados del siglo XVII, y que resulta de mucha utilidad para representar ciertas figuras geométricas en el plano, entre otras cosas. El término *coordenadas polares* sin embargo parece haber sido introducido primeramente por Gregorio Fontana (1735-1803) en el siglo XVIII.

Para definir el sistema de coordenadas polares, empezamos por escoger un punto O en el plano, que llamaremos el *polo* o el *origen* y también un rayo arbitrario saliendo del origen, que llamaremos el *eje polar*. Sea P un punto cualquiera en el plano diferente de O (ver Figura 1).

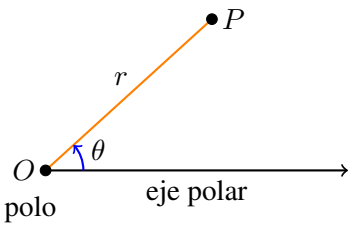

Figura 1. Coordenadas polares de un punto P.

El punto P queda entonces determinado de manera única por el ángulo θ que forman el eje polar y el rayo $\overrightarrow{OP}$ y la distancia r de P al origen O. Decimos entonces que el par ordenado (r, θ) es una representación del punto P en *coordenadas polares*.

Utilizamos la convención usual de que un ángulo medido en dirección contraria a la de las manecillas del reloj es positivo, y negativo si se mide en la dirección de las manecillas del reloj.

Note que las coordenadas polares de un punto no son únicas en general, por ejemplo, para cada $n \in \mathbb{Z}$, las coordenadas $(r, \theta + 2n\pi)$ representan al mismo punto que (r, θ). Además, suponemos que el origen es dado por coordenadas polares $(0, \theta)$ para cualquier $\theta \in \mathbb{R}$. Sin embargo si suponemos que $\theta \in [0, 2\pi)$ y $r \in (0, \infty)$, entonces ésta representación sí es única.

Extendemos las posibilidades para las coordenadas polares al caso en el que r es negativo como sigue. Suponemos que las coordenadas polares $(-r, \theta)$ representan al mismo punto que las coordenadas polares $(r, \theta + \pi)$, como se muestra en la Figura 2.

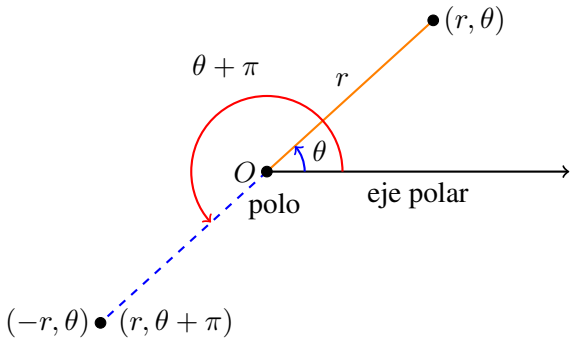

Figura 2. Coordenadas polares con r negativo.

Por lo general cuando trabajamos con coordenadas polares, escogemos el polo de manera que coincida con el origen del plano cartesiano y el eje polar de manera que coincida con el eje x positivo, como se muestra en la Figura 6.

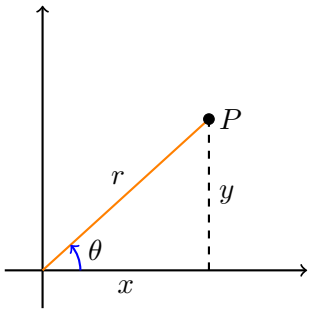

FIGURA 3. Coordenadas polares y rectangulares del punto P.

Las coordenadas polares se pueden relacionar entonces con las coordenadas cartesianas de la manera siguiente. Si el par ordenado (x, y) representa las coordenadas cartesianas de un punto P del plano y (r, θ) son correspondientes coordenadas cartesianas para P, entonces estas se relacionan por medio de las siguientes fórmulas.

$$\begin{aligned} x &= r\cos\theta \qquad & r^2 &= x^2 + y^2 \\ y &= r\,\mathrm{sen}\,\theta \qquad & \theta &= \tan^{-1}\left(\frac{y}{x}\right) \end{aligned}$$

Debe tenerse cuidado de que la relación $\theta = \tan^{-1}\left(\frac{y}{x}\right)$ no se cumple siempre, pues el rango de la función $\tan^{-1} x$ es el intervalo $\left]-\frac{\pi}{2}, \frac{\pi}{2}\right[$.

Así como podemos graficar curvas en coordenadas cartesianas, también podemos hacerlo con curvas dadas en coordenadas polares. Diremos que el gráfico de una ecuación en coordenadas polares $F(r, \theta) = 0$ es el conjunto de puntos P en el plano tales que existe al menos una representación (r, θ) de P en coordenadas polares que satisface la ecuación $F(r, \theta) = 0$.

Un caso paticular ocurre cuando $F(r, \theta) = r - f(\theta)$, en cuyo caso usualmente escribimos la ecuación como $r = f(\theta)$.

Veremos ahora algunos ejemplos de curvas dadas por ecuaciones polares.

Ejemplo 2.1. En este ejemplo graficaremos la curva de ecuación polar $r = 2\cos\theta$. Para esto elaboramos una tabla de valores y graficamos los correspondientes puntos como sigue.

θ	$r = 2\cos(\theta)$	(r, θ)
0	2	$(2, 0)$
$\pi/6$	$\sqrt{3}$	$(1.73, \pi/6)$
$\pi/4$	$\sqrt{2}$	$(1.41, \pi/4)$
$\pi/3$	1	$(1, \pi/3)$
$\pi/2$	0	$(0, \pi/2)$
$2\pi/3$	-1	$(-1, 2\pi/3)$
$3\pi/4$	$-\sqrt{2}$	$(-1.41, 3\pi/4)$
$5\pi/6$	$-\sqrt{3}$	$(-1.73, 5\pi/6)$

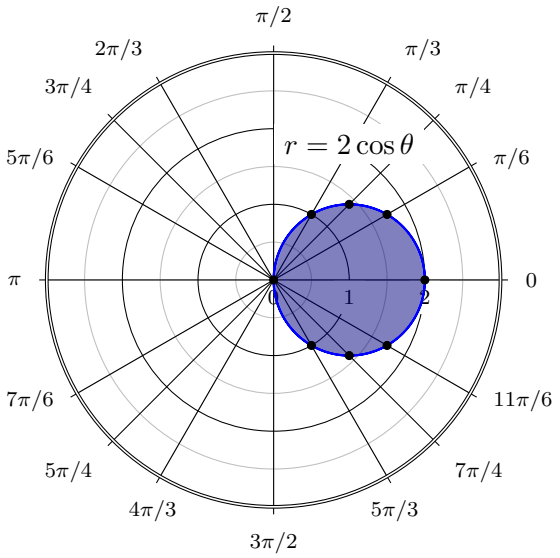

FIGURA 4. El gráfico de la curva polar $r = 2\cos\theta$, cuya ecuación cartesiana es $(x-1)^2 + y^2 = 1$.

Observe que solo hemos tabulado valores para ángulos $\theta \in [0, \pi)$. Esto es porque para todo $\theta \in \mathbb{R}$ se cumple que $\cos(\theta + \pi) = -\cos\theta$, por lo que los puntos correspondientes al intervalo $[\pi, 2\pi)$, que se pueden escribir como $\theta + \pi$ para $\theta \in [0, \pi)$, darían coordenadas polares $(-2\cos\theta, \theta + \pi)$, y esta es una representación del punto con coordenadas polares $(2\cos\theta, \theta)$, por lo que solo se estaría obteniendo una repetición de puntos.

El gráfico nos muestra que la curva polar describe al círculo de radio 1 centrado en $(1, 0)$. Podemos comprobar esto transformando la ecuación polar dada a una ecuación cartesiana usando las relaciones entre coordenadas polares y cartesianas. Explícitamente, tenemos que

$$\begin{aligned} r = 2\cos\theta &\implies r^2 = 2r\cos\theta \\ &\implies x^2 + y^2 = 2x \\ &\implies x^2 - 2x + y^2 = 0 \\ &\implies (x^2 - 2x + 1) + y^2 = 1 \\ &\implies (x-1)^2 + y^2 = 1 \end{aligned}$$

y en efecto esta última es la ecuación cartesiana del círculo de radio 1 con centro en $(1, 0)$. ◇

Ejemplo 2.2. En este ejemplo graficaremos la curva de ecuación polar $r = \frac{3}{2}\cos(2\theta)$. Para esto elaboramos nuevamente una tabla de valores y graficamos los correspondientes puntos como sigue.

θ	$r = \frac{3}{2}\cos(\theta)$	(r, θ)
0	$3/2$	$(1.5, 0)$
$\pi/6$	$3/4$	$(0.75, \pi/6)$
$\pi/4$	0	$(0, \pi/4)$
$\pi/3$	$-3/4$	$(-0.75, \pi/3)$
$\pi/2$	$-3/2$	$(-1.5, \pi/2)$
$2\pi/3$	$-3/4$	$(-0.75, 2\pi/3)$
$3\pi/4$	0	$(0, 3\pi/4)$
$5\pi/6$	$3/4$	$(0.75, 5\pi/6)$
π	$3/2$	$(1.5, \pi)$
$7\pi/6$	$3/4$	$(0.75, 7\pi/6)$
$5\pi/4$	0	$(0, 5\pi/4)$
$4\pi/3$	$-3/4$	$(-0.75, 4\pi/3)$
$3\pi/2$	$-3/2$	$(-1.5, 3\pi/2)$
$5\pi/3$	$-3/4$	$(-0.75, 5\pi/3)$
$7\pi/4$	0	$(0, 7\pi/4)$
$11\pi/6$	$3/4$	$(0.75, 11\pi/6)$

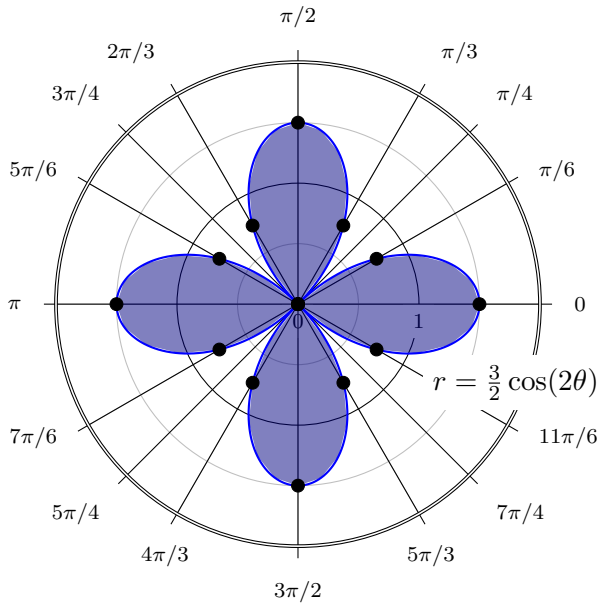

FIGURA 5. El gráfico de la curva polar $r = 2\cos\theta$, cuya ecuación cartesiana es $(x-1)^2 + y^2 = 1$.

Esta curva es un ejemplo de una rosa de cuatro pétalos.

◇

EJERCICIOS

Ejercicios de la sección 2.

2.1 Encuentre una ecuación cartesiana para la ecuación polar $r = \frac{3}{2}\cos(2\theta)$ del Ejemplo 2.2.

2.2 Grafique la curva con ecuación polar $r = \cos(3\theta)$.

2.3 Para $a \in \mathbb{R}_{>0}$, considere la curva de ecuación polar $r = 2a\,\mathrm{sen}(\theta)\tan(\theta)$. Esta curva se conoce como la *cisoide de Diocles*, en honor al matemático y geómetra girego Diocles (c. 240 a. C. - c. 180 d. C.), quien utilizó esta curva en relación a su trabajo para dar una solución geométrica al problema clásico de duplicar el cubo. Demuestre que la cisoide $r = 2a\,\mathrm{sen}(\theta)\tan(\theta)$ tiene una asíntota vertical en $x = 2a$ y además demuestre que el gráfico de la cisoide se encuentra completamente contenido en la banda vertical $0 \leq x < 2a$. Por último, realice un bosquejo de la cisoide.

2.4 Utilice `SageMath` para graficar la curva con ecuación polar

$$r = e^{\mathrm{sen}\,\theta} - 2\cos(4\theta) + \mathrm{sen}^5\left(\frac{1}{24}(2\theta - \pi)\right)$$

para θ en los intervalos $[0, 2n\pi]$ para $n = 1, 2, 3, \ldots$. Note que la curva va cambiando al incrementar el valor de n. ¿Qué valor de n debe tomar para garantizar que el gráfico de la curva está completo?

3. NÚMEROS COMPLEJOS

Definición 3.1. El conjunto de los números complejos, denotado por $\mathbb{C}$, es el conjunto de los pares ordenados $(a, b) \in \mathbb{R}^2$. En $\mathbb{C}$ definimos dos operaciones binarias de suma $+ : \mathbb{C} \times \mathbb{C} \to \mathbb{C}$ y multiplicación $\cdot : \mathbb{C} \times \mathbb{C} \to \mathbb{C}$ por las reglas

- $(a, b) + (c, d) := (a + c, b + d)$
- $(a, b) \cdot (c, d) := (ac - bd, ad + bc)$,

para cualesquiera $(a, b), (c, d) \in \mathbb{C}$. ♦

Teorema 3.2. *El conjunto de los números complejos $\mathbb{C}$ es un cuerpo con las operaciones $+$ y $\cdot$ definidas anteriormente.*

Demostración. Es fácil verificar que la suma es asociativa, conmutativa, que el elemento $(0, 0)$ es el neutro aditivo, y que el inverso aditivo de cualquier elemento $(a, b) \in \mathbb{C}$ es $(-a, -b)$. Además, note que la multiplicación es conmutativa pues

$$\begin{aligned}(a, b) \cdot (c, d) &= (ac - bd, ad + bc) \quad \text{y} \\ (c, d) \cdot (a, b) &= (ca - db, cb + da)\end{aligned}$$

y ambos pares ordenados son iguales por la conmutatividad de la suma y la multiplicación en $\mathbb{R}$.

Por otro lado, el par ordenado $(1, 0)$ es el neutro multiplicativo pues para todo $(a, b) \in \mathbb{C}$ se cumple que

$$(a, b) \cdot (1, 0) = (a \cdot 1 - b \cdot 0, a \cdot 0 + b \cdot 1) = (a, b)$$

y similarmente $(1, 0) \cdot (a, b) = (a, b)$.

Además, el lector puede verificar que la multiplicación es asociativa y que se cumplen las leyes distributivas (esto es fácil, aunque ligeramente tedioso).

Finalmente, debemos mostrar la existencia de inversos multiplicativos. Sea $(a, b) \in \mathbb{C} \setminus \{(0, 0)\}$. Debemos encontrar un elemento $(x, y) \in \mathbb{C}$ tal que $(a, b) \cdot (x, y) = (1, 0)$, es decir, tal que $(ax - by, ay + bx) = (1, 0)$, o lo que es lo mismo, debemos encontrar una solución al sistema de ecuaciones lineales 2×2

$$\begin{cases} ax - by = 1 \\ bx + ay = 0. \end{cases}$$

El lector con conocimientos básicos de álgebra lineal recordará que este sistema de ecuaciones lineales tiene solución única pues el determinante de la matriz del sistema es

$$\begin{vmatrix} a & -b \\ b & a \end{vmatrix} = a^2 + b^2 \neq 0,$$

pues $(a, b) \neq (0, 0)$. Además, esta solución es dada por la fórmula de Cramer como

$$x = \frac{\begin{vmatrix} 1 & -b \\ 0 & a \end{vmatrix}}{\begin{vmatrix} a & -b \\ b & a \end{vmatrix}} = \frac{a}{a^2 + b^2}, \quad y = \frac{\begin{vmatrix} a & 1 \\ b & 0 \end{vmatrix}}{\begin{vmatrix} a & -b \\ b & a \end{vmatrix}} = \frac{-b}{a^2 + b^2}.$$

Esto quiere decir que el inverso multiplicativo de (a, b) es dado por el par ordenado

$$(a, b)^{-1} = \left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2} \right).$$

Esto completa la demostración de que $\mathbb{C} = \mathbb{R} \times \mathbb{R}$ es un cuerpo con las operaciones de suma y multiplicación dadas. □

Se puede verificar que el subconjunto de $\mathbb{C}$ dado por $\{(a,0) \mid a \in \mathbb{R}\}$ es un subcuerpo de $\mathbb{C}$, y además, que la función

$$\begin{aligned} \phi : \mathbb{R} &\longrightarrow \{(a,0) \mid a \in \mathbb{R}\} \subset \mathbb{C} \\ a &\longmapsto (a,0) \end{aligned}$$

es un homomorfismo de anillos (en este caso de cuerpos) biyectivo, es decir, que ϕ es un isomorfismo de cuerpos. Esto muestra que $\mathbb{R}$ es isomorfo al subcuerpo de $\mathbb{C}$ dado por el conjunto $\{(a,0) \mid a \in \mathbb{R}\}$. Usando este isomorfismo, identificaremos el par ordenado $(a,0)$ con el número real a. Además, usando esta identificación, note que el par ordenado $(0,1)$ satisface la igualdad $(0,1)^2 = (0,1)\cdot(0,1) = (-1,0) = -1$. Si denotamos por $i := (0,1)$ a este número complejo, hemos visto que $i^2 = -1$, y por lo tanto ahora tenemos un número cuyo cuadrado es -1, algo imposible dentro del cuerpo de los números reales.

Con éstas identificaciones, el número complejo (a,b) se puede escribir como $a+bi$ ya que

$$a + bi = (a,0) + (b,0)\cdot(0,1) = (a,0) + (0,b) = (a,b).$$

De ahora en adelante en la mayoría de los casos usaremos esta notación para los números complejos y por ende escribiremos

$$\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R}\}.$$

3.1. Interpretación geométrica de los números complejos. Como $\mathbb{C} = \mathbb{R} \times \mathbb{R}$, cada número complejo $a + bi = (a,b)$ se puede representar como un punto en el plano cartesiano como en la figura siguiente.

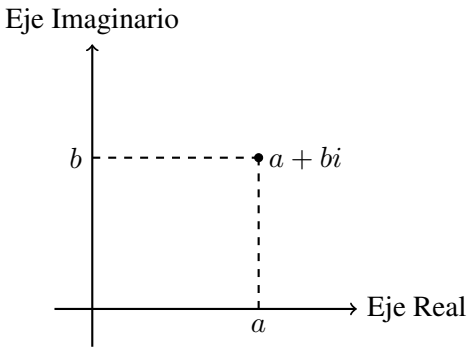

FIGURA 6. Representación geométrica del punto complejo $a + bi$.

En este caso, nos referimos al plano $\mathbb{R}^2$ como el *plano complejo*, y como el eje x corresponde a los puntos de la forma $(a,0)$ con $a \in \mathbb{R}$, que han sido identificados con los números reales, nos referimos a él como el *eje real*. Al eje y, que corresponde a los puntos de la forma $(0,b)$, es decir, de la forma bi con $(b \in \mathbb{R})$, históricamente se le conoce como el *eje imaginario*, pues comúnmente los números complejos de la forma bi $(b \in \mathbb{R})$ se conocen como *puramente imaginarios*.

Definición 3.3. Dado un número complejo $z = a + bi$ con $a, b \in \mathbb{R}$, decimos que a es la *parte real* de z, denotado por $\mathrm{Re}(z) = a$, y b es la *parte imaginaria* de z, denotado por $\mathrm{Im}(z) = b$. Note que si $z, w \in \mathbb{C}$, entonces $z = w \iff \mathrm{Re}(z) = \mathrm{Re}(w)$ y $\mathrm{Im}(z) = \mathrm{Im}(w)$. ♦

Definición 3.4. Dado un número complejo $z = a + bi \in \mathbb{C}$, la distancia de z al origen en el plano complejo se llama el *módulo* de z (o *valor absoluto* de z) y se denota por $|z|$. Por el Teorema de Pitágoras, se tiene que

$$|z| = \sqrt{a^2 + b^2} = \sqrt{\mathrm{Re}(z)^2 + \mathrm{Im}(z)^2}.$$

♦

Definición 3.5. Si $z = a + bi \in \mathbb{C}$, el número $a - bi$, que se obtiene al reflejar z con respecto al eje real (como se muestra en la Figura 7) en el plano complejo se llama el *conjugado* de z y se denota por $\overline{z}$. ♦

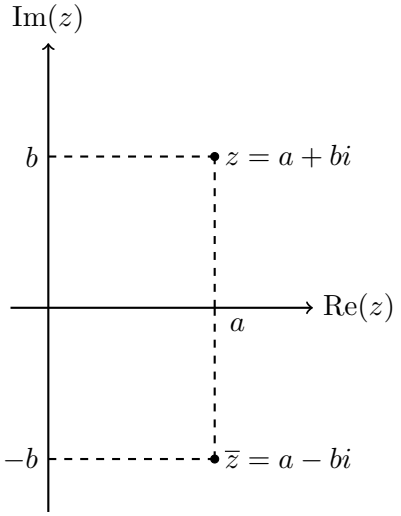

FIGURA 7. El número complejo $a + bi$ y su conjugado.

El conjugado y el módulo nos permiten escribir al inverso multiplicativo de $z = a + bi$ de manera más concisa. A saber, habíamos visto que si $(a, b) \in \mathbb{C} \setminus \{(0, 0)\}$ entonces

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

o lo que es lo mismo,

$$(a + bi)^{-1} = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2} i = \frac{a - bi}{a^2 + b^2} = \frac{\overline{z}}{|z|^2},$$

es decir, si $z \in \mathbb{C} \setminus \{0\}$, su inverso multiplicativo es

$$z^{-1} = \frac{\overline{z}}{|z|^2}.$$

Proposición 3.6 (Propiedades del módulo y del conjugado)**.** *Si $z_1, z_2, z \in \mathbb{C}$, entonces el módulo y el conjugado satisfacen las siguientes propiedades.*

1. $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$.
2. $\overline{z_1 \cdot z_2} = \overline{z_1} \cdot \overline{z_2}$.
3. $|z_1 \cdot z_2| = |z_1| \cdot |z_2|$.
4. $|\overline{z}| = |z|$.
5. $|\operatorname{Re}(z)| \leq |z|$ y $|\operatorname{Im}(z)| \leq |z|$.
6. *(Desigualdad triangular)* $|z_1 + z_2| \leq |z_1| + |z_2|$.
7. *(Desigualdad triangular inversa)* $||z_1| - |z_2|| \leq |z_1 - z_2|$.

Demostración. Ejercicio. □

Note que las propiedades 1 y 2 de la Proposición 3.6 esencialmente nos dicen que la función

$$\begin{aligned} \rho : \mathbb{C} &\longrightarrow \mathbb{C} \\ z &\longmapsto \overline{z} \end{aligned}$$

es un homomorfismo de cuerpos. De hecho, este homomorfismo es biyectivo, o sea que la conjugación compleja es un automorfismo de $\mathbb{C}$.

3.2. Representación polar de un número complejo. Dado un número complejo $z = x + yi$, como éste corresponde al punto (x, y) en el plano cartesiano, se puede representar con coordenadas polares como (r, θ), donde $x = r\cos\theta$, $y = r\,\mathrm{sen}\,\theta$, y por lo tanto z se puede escribir de la forma $z = r(\cos\theta + i\,\mathrm{sen}\,\theta)$. A esta expresión le llamamos la *forma polar* del número complejo z.

Note en particular que si z es dado en forma polar por $z = r(\cos\theta + i\,\mathrm{sen}\,\theta)$, entonces su módulo es $|z| = r$. Decimos que el ángulo θ es un *argumento* de z, denotado por $\arg(z) = \theta$. Por supuesto, este argumento no es único. Sin embargo, si restringimos θ al intervalo $(-\pi, \pi]$, el ángulo que se obtiene se conoce como el *argumento principal* de z y se denota por $\mathrm{Arg}(z)$.

Entonces, en general si θ es cualquier argumento de z, existe un entero n tal que

$$\theta = \mathrm{Arg}(z) + 2n\pi.$$

La suma y resta de números complejos es muy sencilla si éstos están expresados en forma rectangular como $a + bi$. Similarmente, la forma polar de los números complejos facilita su multiplicación y su división. A saber, sean

$$z_1 = r_1(\cos\theta_1 + i\,\mathrm{sen}\,\theta_1) \quad \text{y} \quad z_2 = r_2(\cos\theta_2 + i\,\mathrm{sen}\,\theta_2)$$

dos números complejos en forma polar. Entonces

$$\begin{aligned} z_1 \cdot z_2 &= r_1 r_2(\cos\theta_1 + i\,\mathrm{sen}\,\theta_1)(\cos\theta_2 + i\,\mathrm{sen}\,\theta_2) \\ &= r_1 r_2((\cos\theta_1\cos\theta_2 - \mathrm{sen}\,\theta_1\,\mathrm{sen}\,\theta_2) + i(\cos\theta_1\,\mathrm{sen}\,\theta_2 + \mathrm{sen}\,\theta_1\cos\theta_2)) \\ &= r_1 r_2(\cos(\theta_1 + \theta_2) + i\,\mathrm{sen}(\theta_1 + \theta_2)). \end{aligned}$$

De manera similar, podemos verificar que si $z_2 \neq 0$, entonces

$$\frac{z_1}{z_2} = \frac{r_1}{r_2}(\cos(\theta_1 - \theta_2) + i\,\mathrm{sen}(\theta_1 - \theta_2)).$$

Geométricamente la suma y la multiplicación de complejos se pueden interpretar como en la Figura 8.

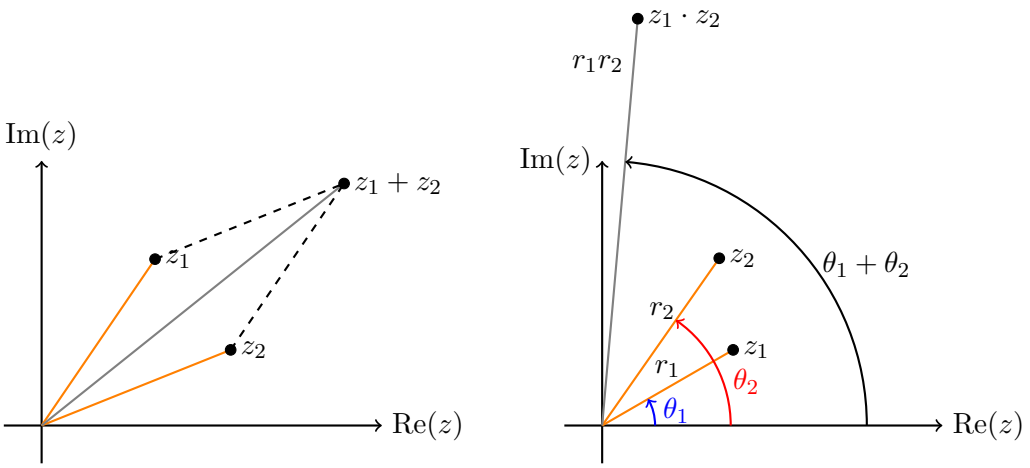

FIGURA 8. Suma y multiplicación de dos números complejos.

En la Figura 8 vemos que la suma de números complejos se realiza de acuerdo a la ley del paralelogramo y la multiplicación lo que hace es sumar los argumentos y multiplicar las magnitudes o módulos.

En general, tenemos la siguiente fórmula para calcular potencias enteras de números complejos.

Teorema 3.7 (Fórmula de De Moivre)**.** *Si* $z = r(\cos\theta + i\,\mathrm{sen}\,\theta)$ *es un número complejo en forma polar, entonces* $z^n = r^n(\cos(n\theta) + i\,\mathrm{sen}(n\theta))$ *para todo* $n \in \mathbb{Z}_{\geq 0}$. *Si* $z \neq 0$ *entonces* $z^{-n} = r^{-n}(\cos(n\theta) - i\,\mathrm{sen}(n\theta))$ *para todo* $n \in \mathbb{Z}_{>0}$.

Demostración. Ejercicio. □

Con la fórmula de De Moivre podemos ver que en general un número complejo no cero posee n raíces $n-$ésimas distintas. Ésto quizás sea algo sorprendente dado que nuestra construcción del cuerpo de los números complejos se basó en adjuntar un número que fuera una raíz cuadrada de -1.

El procedimiento es el siguiente. Sea $\omega = r(\cos\theta + i\,\mathrm{sen}\,\theta)$ un número complejo no cero escrito de forma polar. Queremos encontrar un número $z \in \mathbb{C}$ tal que $z^n = \omega$. Escribimos z en forma polar como $z = t(\cos\varphi + i\,\mathrm{sen}\,\varphi)$. Note que por la fórmula de De Moivre tenemos que

$$\begin{aligned} z^n &= t^n(\cos(n\varphi) + i\,\mathrm{sen}(n\varphi)) \\ &= r(\cos\theta + i\,\mathrm{sen}\,\theta). \end{aligned}$$

De esta ecuación deducimos que como $|z^n| = |\omega|$, se debe tener que $t^n = r$, o equivalentemente, que $t = \sqrt[n]{r}$. Esto a su vez implica que

$$\cos(n\varphi) + i\,\mathrm{sen}(n\varphi) = \cos\theta + i\,\mathrm{sen}\,\theta$$

y por lo tanto $\cos(n\varphi) = \cos(\theta)$ y $\mathrm{sen}(n\varphi) = \mathrm{sen}(\theta)$. Estas últimas dos ecuaciones se cumplen sí y solo sí $n\varphi = \theta + 2k\pi$ para algún $k \in \mathbb{Z}$, es decir

$$\varphi = \frac{\theta + 2k\pi}{n} \quad \text{para algún } k \in \mathbb{Z}.$$

De esto obtenemos que el número complejo z_k definido por

$$z_k := \sqrt[n]{r}\left(\cos\left(\frac{\theta + 2k\pi}{n}\right) + i\,\mathrm{sen}\left(\frac{\theta + 2k\pi}{n}\right)\right)$$

es una raíz n–esíma de ω. Diferentes valores de k dan por supuesto diferentes valores para el argumento $\varphi = (\theta + 2k\pi)/n$, sin embargo, las correspondientes raíces z_k no serán todas diferentes. Para ser más explícitos, si $k_1, k_2 \in \mathbb{Z}$ entonces

$$\begin{aligned} z_{k_1} = z_{k_2} &\iff \frac{\theta + 2k_1\pi}{n} = \frac{\theta + 2k_2\pi}{n} + 2m\pi \quad \text{para algún } m \in \mathbb{Z} \\ &\iff k_1 = k_2 + mn \quad \text{para algún } m \in \mathbb{Z}. \end{aligned}$$

Esto quiere decir que $z_{k_1} = z_{k_2}$ sí y solo sí k_1 y k_2 difieren por un múltiplo de n. Entonces, como ninguno de los valores $k = 0, 1, \ldots, n-1$ difieren por un múltiplo de n, vemos que los números complejos

$$z_k := \sqrt[n]{r}\left(\cos\left(\frac{\theta + 2k\pi}{n}\right) + i\,\mathrm{sen}\left(\frac{\theta + 2k\pi}{n}\right)\right) \quad \text{para } k = 0, 1, \ldots, n-1$$

son las raíces n–ésimas distintas de ω, y además que en total son n de ellas.

Estos números complejos se encuentran todos sobre el círculo $|z| = \sqrt[n]{r}$ de radio $\sqrt[n]{r}$ en el plano complejo y están todos espaciados de manera uniforme, formando ángulos de medida $2\pi/n$ como en la Figura 9. Más aún, cuando $n \geq 3$ éstos puntos forman los vértices de un polígono regular de n lados.

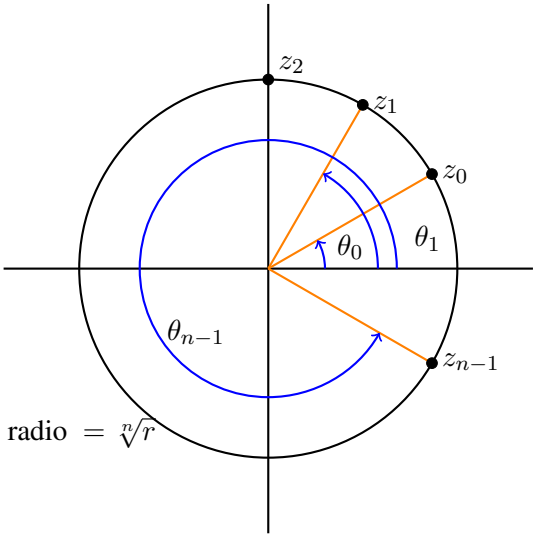

FIGURA 9. Las raíces n-ésimas de un número complejo, $\theta_k := \theta + 2k\pi/n$, para $k = 0, 1, ..., n-1$

Ahora veremos unos algunos ejemplos de esto.

Ejemplo 3.8. Veamos que todo número real $\alpha \neq 0$ tiene dos raíces complejas. Esto ya lo sabíamos cuando el número real $\alpha > 0$, sin embargo en los números reales no existen raíces de números negativos, así que ahora podemos remediar esto con los números complejos. Siguiendo el método descrito anteriormente, debemos empezar por escribir α en forma polar. Tenemos dos casos.

Cuando $\alpha > 0$ su forma polar es

$$\alpha = \alpha(\cos 0 + i \operatorname{sen} 0)$$

y por lo tanto sus raíces cuadradas son dadas por

$$z_k = \sqrt{\alpha}\left(\cos\left(\frac{0+2k\pi}{2}\right) + i \operatorname{sen}\left(\frac{0+2k\pi}{2}\right)\right) \quad \text{para } k = 0, 1.$$

Esto nos da las dos raíces cuadradas

$$z_0 = \sqrt{\alpha}(\cos 0 + i \operatorname{sen} 0) = \sqrt{\alpha} \quad \text{y}$$
$$z_1 = \sqrt{\alpha}\,(\cos \pi + i \operatorname{sen} \pi) = -\sqrt{\alpha}.$$

Similarmente, si $\alpha < 0$ su forma polar es

$$\alpha = |\alpha|(\cos \pi + i \operatorname{sen} \pi)$$

y por lo tanto sus raíces cuadradas son dadas por

$$z_k = \sqrt{|\alpha|}\left(\cos\left(\frac{\pi+2k\pi}{2}\right) + i \operatorname{sen}\left(\frac{\pi+2k\pi}{2}\right)\right) \quad \text{para } k = 0, 1.$$

Esto nos da las dos raíces cuadradas

$$z_0 = \sqrt{|\alpha|}\left(\cos\left(\frac{\pi}{2}\right) + i \operatorname{sen}\left(\frac{\pi}{2}\right)\right) = i\sqrt{|\alpha|} \quad \text{y}$$
$$z_1 = \sqrt{|\alpha|}\left(\cos\left(\frac{3\pi}{2}\right) + i \operatorname{sen}\left(\frac{3\pi}{2}\right)\right) = -i\sqrt{|\alpha|}.$$

En la Figura 10 se ve la ubicación de estas raíces en el plano complejo, a saber, sobre el eje real cuando $\alpha > 0$ y sobre el eje imaginario cuando $\alpha < 0$.

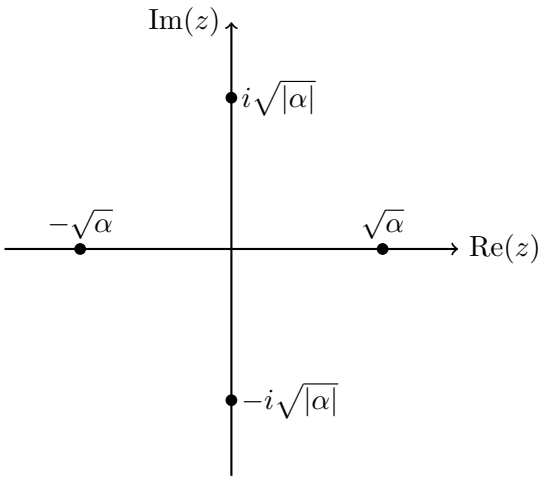

FIGURA 10. Las raíces cuadradas de un número real α en los casos en que $\alpha > 0$ y $\alpha < 0$.

◇

En general, a las raíces n–ésimas de 1 se les conoce como las raíces n–ésimas de la unidad, y estas aparecen en distintos contextos en prácticamente todas las ramas de la matemática. Veremos ahora un ejemplo del cálculo de las raíces cuartas de la unidad.

Ejemplo 3.9. Vamos a calcular las raíces cuartas de la unidad. De nuevo, la forma polar de 1 es dada por $1 = 1(\cos 0 + i \operatorname{sen} 0)$. Entonces sus raíces cuartas son dadas por los números complejos

$$z_k = \sqrt[4]{1}\left(\cos\left(\frac{0+2k\pi}{4}\right) + i \operatorname{sen}\left(\frac{0+2k\pi}{4}\right)\right) \quad \text{para } k = 0, 1, 2, 3.$$

Esto nos da las cuatro raíces

$$\begin{aligned} z_0 &= \cos 0 + i \operatorname{sen} 0 = 1 \\ z_1 &= \cos\left(\frac{\pi}{2}\right) + i \operatorname{sen}\left(\frac{\pi}{2}\right) = i \\ z_2 &= \cos \pi + i \operatorname{sen} \pi = -1 \\ z_3 &= \cos\left(\frac{3\pi}{2}\right) + i \operatorname{sen}\left(\frac{3\pi}{2}\right) = -i. \end{aligned}$$

Estas raíces están todas ubicadas sobre el círculo unitario $|z| = 1$ en el plano complejo como se muestra en la Figura 11. Note que estas forman los vértices de un cuadrado.

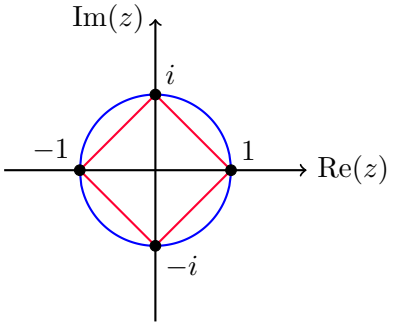

FIGURA 11. Las raíces cuartas de la unidad.

◇

3.3. El plano complejo extendido. En muchas ocasiones es conveniente extender el cuerpo de los números complejos al agregar un símbolo ∞ correspondiente hasta cierto punto con una idea intuitiva de un infinito matemático. Definimos el conjunto extendido de los números complejos como $\overline{\mathbb{C}} := \mathbb{C} \cap \{\infty\}$, donde decretamos que el símbolo ∞ santisface las siguientes propiedades.

- $a + \infty = \infty + a = \infty$, para todo $a \in \mathbb{C}$.
- $a \cdot \infty = \infty \cdot a = \infty$, para todo $a \in \overline{\mathbb{C}} \setminus \{0\}$.
- $\frac{a}{\infty} = 0$, para todo $a \in \overline{\mathbb{C}} \setminus \{0\}$.
- $\frac{a}{0} = \infty$ para todo $a \in \mathbb{C}$.

Podemos dar una interpretación geométrica de este conjunto extendido de los números complejos que nos permitirá entender el símbolo ∞. Empezamos por identificar el plano complejo $\mathbb{C} = \mathbb{R}^2$ con el plano xy en $\mathbb{R}^3$ por medio de la biyección

$$\begin{aligned} \mathbb{C} &\longrightarrow \{(x, y, z) \mid z = 0\} \\ z = a + bi &\longmapsto (a, b, 0). \end{aligned}$$

Consideramos además la esfera 2–dimensional $\mathbb{S}^2 := \{(x, y, z) \in \mathbb{R}^3 \mid x^2 + y^2 + z^2 = 1\}$. Denotamos $N = (0, 0, 1)$ y le llamamos el polo norte de la esfera. Vea la Figura 12.

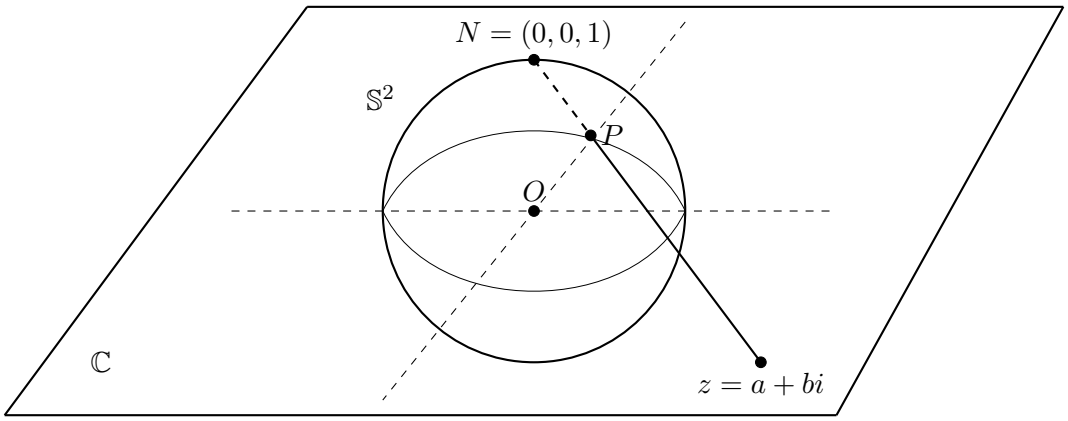

FIGURA 12. Esfera de Riemann y Proyección Estereográfica

Lo que haremos ahora es establecer una biyección entre los puntos de la esfera $\mathbb{S}^2$ y los puntos del plano complejo extendido $\overline{\mathbb{C}}$.

Primero repasaremos como se puede expresar una recta que pasa por dos puntos distintos en $\mathbb{R}^3$ en forma paramétrica. Recordemos que por dos puntos distintos $P = (p_1, p_2, p_3)$ y $Q = (q_1, q_2, q_3)$ de $\mathbb{R}^3$ pasa una única recta ℓ_{PQ}. Esta recta ℓ_{PQ} se puede describir en forma paramétrica como el conjunto de puntos $(x, y, z) \in \mathbb{R}^3$ tales que

$$\begin{aligned} (x, y, z) &= (1 - t)P + tQ \\ &= (1 - t)(p_1, p_2, p_3) + t(q_1, q_2, q_3) \\ &= ((1 - t)p_1 + tq_1, (1 - t)p_2 + tq_2, (1 - t)p_3 + tq_3) \end{aligned}$$

para algún $t \in \mathbb{R}$. Note en particular que si $t = 0$ entonces $(x, y, z) = P$ y si $t = 1$ entonces $(x, y, z) = Q$. Además, si restringimos el parámetro t al intervalo $[0, 1]$ entonces la parametrización anterior describe el segmento de recta que une a P y Q, como en la Figura 13.

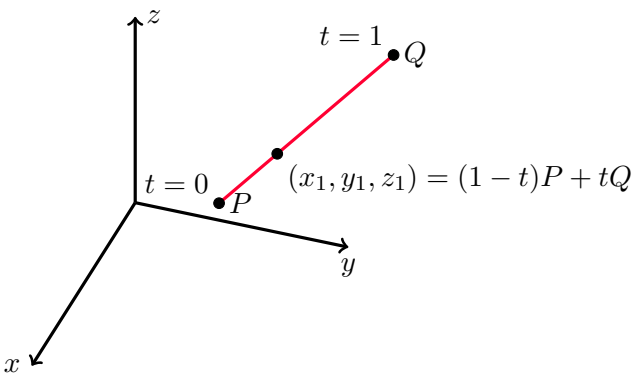

FIGURA 13. Parametrización de la recta que pasa por P y Q.

Ahora, si $z = a + bi \in \mathbb{C}$ (que realmente lo identificamos con el punto $(a, b, 0) \in \mathbb{R}^3$), la recta que une a z con el polo norte es dada por la ecuación paramétrica

$$\begin{aligned}(x_1, x_2, x_3) &= (1-t)(a, b, 0) + t(0, 0, 1) \\ &= ((1-t)a, (1-t)b, t) \quad \text{para } t \in \mathbb{R}.\end{aligned}$$

Esta recta interseca a la esfera $\mathbb{S}^2$ en los puntos $(x_1, x_2, x_3) \in \mathbb{R}^3$ que satisfacen las ecuaciones

$$\begin{aligned}x_1^2 + x_2^2 + x_3^2 &= 1 \\ x_1 &= (t-1)a \\ x_2 &= (t-1)b \\ x_3 &= t\end{aligned}$$

Las cuales nos dan la ecuación:

$$\begin{aligned}(t-1)^2a^2 + (t-1)^2b^2 + t^2 = 1 \Rightarrow \\ (t-1)^2(a^2+b^2) + (t^2-1) = 0 \Rightarrow \\ (t-1)((t-1)(a^2+b^2) + (t+1)) = 0\end{aligned}$$

Cuando $t = 1$, el punto que se obtiene es el polo norte $N = (0, 0, 1)$ que evidentemente está en la recta, si $t \neq 1$, la ecuación anterior perimte concluir

$$t = \frac{a^2+b^2-1}{a^2+b^2+1} = \frac{|z|^2-1}{|z|^2+1}$$

De donte se obtiene el punto:

$$(x_1, x_2, x_3) = \left(\frac{2a}{|z|^2+1}, \frac{2b}{|z|^2+1}, \frac{|z|^2-1}{|z|^2+1}\right)$$

En donde hemos ultilizado que $1 - t = \frac{2}{|z|^2+1}$. Note que éste punto se puede reescribir como:

$$(x_1, x_2, x_3) = \left(\frac{2\,\mathrm{Re}(z)}{|z|^2+1}, \frac{2\,\mathrm{Im}(z)}{|z|^2+1}, \frac{|z|^2-1}{|z|^2+1}\right)$$

Y de esta manera definimos la *proyección estereográfica* del punto z sobre la esfera $\mathbb{S}^2$ como el punto en $\mathbb{R}^3$ dado por:

$$\mathrm{pr}(z) = \left(\frac{2\,\mathrm{Re}(z)}{|z|^2+1}, \frac{2\,\mathrm{Im}(z)}{|z|^2+1}, \frac{|z|^2-1}{|z|^2+1}\right)$$

En la Figura 12 este punto corresponde al punto P. Como se puede apreciar en est figura, a medida que el punto $z \in \mathbb{C}$ se aleja del origen, es decir cuando $|z|$ crece continuamente, el punto

correspondiente $\mathrm{pr}(z)$ en la esfera se aproxima cada vez más al polo norte $N = (0,0,1)$. Más formalmente, el lector con conocimiento de cálculo puede probar que

$$\lim_{|z|\to\infty} \mathrm{pr}(z) = \lim_{|z|\to\infty} \left(\frac{2\,\mathrm{Re}(z)}{|z|^2+1}, \frac{2\,\mathrm{Im}(z)}{|z|^2+1}, \frac{|z|^2-1}{|z|^2+1} \right) = (0,0,1)$$

Esto motiva a que extendamos la definición de la proyeccion estereográfica a ∞, definiendo $\mathrm{pr}(\infty) := N(0,0,1)$. De manera que tenemos una función:

$$\begin{aligned} \mathrm{pr} : \overline{\mathbb{C}} = \mathbb{C} \cup \{\infty\} &\to \mathbb{S}^2 \\ z \in \mathbb{C} &\mapsto \left(\frac{2\,\mathrm{Re}(z)}{|z|^2+1}, \frac{2\,\mathrm{Im}(z)}{|z|^2+1}, \frac{|z|^2-1}{|z|^2+1} \right) \\ \infty &\mapsto N = (0,0,1) \in \mathbb{S}^2 \end{aligned}$$

Ésta función es biyectiva en realidad. En efecto, construiremos una inversa de pr: tome un punto $A = (a_1, a_2, a_3) \in \mathbb{S}^2 \setminus \{N\}$. La recta que une al polo norte con el punto A es dada por la parametrización:

$$\begin{aligned} (x_1, x_2, x_3) = (1-t) + tA = \\ (1-t)(0,0,1) + t(a_1, a_2, a_3) = \\ (ta_1, ta_2, (t(a_3 - 1) + 1 \quad \text{para } t \in \mathbb{R} \end{aligned}$$

El punto en el que esta recta interseca al plano complejo es dado por la solución al sistema de ecuaciones:

Con esto llegamos a que $t = \frac{1}{1-a_3}$ donde notamos que $a_3 \neq 1$ porque el único punto de $\mathbb{S}^2$ que tiene su tercera coordenada igual a 1 es N. Con todo esto definimos una pryección estereográfica que va de $\mathbb{S}^2$ a $\overline{\mathbb{C}}$, por medio de:

$$\begin{aligned} \overline{\mathrm{pr}} : \mathbb{S}^2 &\to \overline{\mathbb{C}} \\ (a_1, a_2, a_3) \in \mathbb{S}^2 \setminus \{N\} &\mapsto \left(\frac{a_1}{1-a_3}, \frac{a_2}{1-a_3}, 0 \right) \\ N = (0,0,1) &\mapsto \infty \end{aligned}$$

Ahora, es fácil verificar que éstas dos proyecciones son inversas entre sí y por tanto pr y $\overline{\mathrm{pr}}$ son ambas funciones biyectivas que nos dan una biyección entre el plano complejo extendido y la esfera $\mathbb{S}^2$. Es precisamente por ésta interpretación que al plano complejo se le conoce como la *Esfera de Riemann*, en honor al matemático Georg Friedrich Bernhard Riemann $(1826 - 1866)$, quien dió contribuciones fundamentales al desarrollo de la teoría del análisis complejo por medio de un enfoque geométrico.

Se puede ver que ambas proyecciones son continuas (con las topologías adecuadas) y por lo tanto preservan algunas propiedades topológicas como por ejemplo la convergencia y la compacidad. La proyección estereográfica es una herramienta usada por los cartógrafos.

La métrica esférica o nodal. Podemos definir una noción de distancia entre puntos en el plano complejo diferente a la usual utilizando el modelo de la esfera de Riemann par ael plano complejo extendido de la siguiente manera: Si $z_1, z_2 \in \overline{C}$ definimos la *métrica esférica* $\rho(z_1, z_2)$ como la distancia euclidiana entre los puntos $\mathrm{pr}(z_1)$ y $\mathrm{pr}(z_2)$ en la esfera $\mathbb{S}^2$ correspondientes a la proyección de cada uno, es decir:

$$\rho(z_1, z_2) = d(\mathrm{pr}(z_1), \mathrm{pr}(z_2))$$

Se puede demostrar (ejercicio) que:

$$\begin{aligned} \rho(z_1, z_2) = \frac{2||z_1 - z_2|}{\sqrt{|z_1|^2+1} \cdot \sqrt{|z_2|^2+1}} \quad &, \text{si } z_1, z_2 \in \mathbb{C} \\ \rho(z, \infty) = \frac{2}{\sqrt{|z|^2+1}} &, \text{si } z \in \mathbb{C} \end{aligned}$$

Números complejos y raíces de polinomios. Hemos visto que al hacer la extensión de $\mathbb{R}$ a $\mathbb{C}$ siempre existen n raíces $n-$ésimas de cualquier número complejo. Sorprendentemente, también se puede demostrar que en $\mathbb{C}$ cualquier polinomio no cero se factoriza como un producto de factores lineales (es decir que en $\mathbb{C}[x]$ los polinomios irreducibles son de la forma $\alpha x + \beta$, con $\alpha \neq 0$). Por tanto tenemos el siguiente teorema:

Teorema 3.10 (Teorema Fundamental del Álgebra)**.** *Todo polinomio $f(x) \in \mathbb{C}[x]$ tiene al menos una raíz en $\mathbb{C}$*

Corolario 3.11. *Sea $f(x) \in \mathbb{C}[x]$ un polinomio no cero de grado n. Entonces existen $a, \alpha_1, ..., \alpha_n \in \mathbb{C}$ tales que:*

$$f(x) = a(x - \alpha_1) \cdots (x - \alpha_n)$$

donde algunos de los α_i pueden estar repetidos.

En la actualidad se conocen más de 100 pruebas del Teorema Fundamental del Álgebra. La primera prueba rigurosa del Teorema se debe al matemático autodidacta francés Jean-Robert Argand, en 1806.

Ejercicios de la sección 3.

3.1 Escriba los siguientes números complejos en la forma rectangular $a + bi$ con $a, b \in \mathbb{R}$.

(a) $(4 - 2i)/(2 + i)$,
(b) $(z + 1)/(z - 1)$, para $z = x + yi$ con $x, y \in \mathbb{R}$.

3.2 Calcule el módulo $|z|$ y el argumento principal $\mathrm{Arg}(z)$ de los siguientes números complejos.

(a) $z = 1 + i$,
(b) $z = -5i$,
(c) $z = 3 - 4i$.

3.3 Exprese el número complejo $z = 1 - i$ en forma polar y use esto para calcular z^{18}.

3.4 Demuestre que si $r \in \mathbb{R}_{\geq 0}$ y $\theta \in \mathbb{R}$, entonces $|r(\cos\theta + i \operatorname{sen}\theta)| = r$.

3.5 Demuestre que todo $z \in \mathbb{C}$ con $|z| = 1$ es de la forma $z = \cos\theta + i \operatorname{sen}\theta$ para algún $\theta \in \mathbb{R}$.

3.6 Sea $n \in \mathbb{Z}$. Por el algoritmo de la división, sabemos que $n = 4q + r$ para algún $q, r \in \mathbb{Z}$ con $0 \leq r \leq 3$. Demuestre que $i^n = i^r$. En particular, deduzca que

$$i^n = \begin{cases} 1 & \text{si } r = 0 \\ i & \text{si } r = 1 \\ -1 & \text{si } r = 2 \\ -i & \text{si } r = 3. \end{cases}$$

3.7 Demuestre que si $z \in \mathbb{C}$ y $z \neq 1$, entonces

$$\sum_{k=0}^{n} z^k = \frac{z^{n+1} - 1}{z - 1}.$$

Esta es la fórmula para la suma de una serie geométrica (finita).

3.8 Calcule la sumatoria $\displaystyle\sum_{r=0}^{100} i^r$.

3.9 Demuestre que si $z \in \mathbb{C}$ entonces

$$\mathrm{Re}(z) = \frac{z+\overline{z}}{2} \quad \text{y} \quad \mathrm{Im}(z) = \frac{z-\overline{z}}{2i}.$$

3.10 Demuestre la Proposición 3.6. (**Sugerencia:** Para la desigualdad triangular, empiece por usar el hecho de que $|z_1+z_2|^2 \geq 0$ y que $|z|^2 = z \cdot \overline{z}$ para todo $z, z_1, z_2 \in \mathbb{C}$.)

3.11 Demuestre que si $z_1, \ldots, z_n \in \mathbb{C}$, entonces

$$|z_1 + \cdots + z_n| \leq |z_1| + \cdots + |z_n|.$$

Esta desigualdad se conoce como la desigualdad triangular generalizada.

3.12 Demuestre que

$$1 + \cos\theta + \cos 2\theta + \cdots + \cos n\theta = \frac{\operatorname{sen}\left(n+\frac{1}{2}\right)\theta + \operatorname{sen}\frac{1}{2}\theta}{2\operatorname{sen}\frac{1}{2}\theta}$$

y

$$\operatorname{sen}\theta + \operatorname{sen} 2\theta + \cdots + \operatorname{sen} n\theta = \frac{\cos\frac{1}{2}\theta - \cos\left(n+\frac{1}{2}\right)\theta}{2\operatorname{sen}\frac{1}{2}\theta}.$$

(**Sugerencia:** Utilice la fórmula para una suma geométrica en combinación con la fórmula de DeMoivre.)

3.13 Sea $\omega = \cos\left(\frac{2\pi}{n}\right) + i\operatorname{sen}\left(\frac{2\pi}{n}\right)$ y sean $n \in \mathbb{N}$. Demuestre que $1+\omega+\omega^2+\cdots+\omega^{n-1} = 0$.

3.14 Sean $\omega = \cos\left(\frac{2\pi}{5}\right) + i\operatorname{sen}\left(\frac{2\pi}{5}\right)$, $p = \omega + \omega^4$ y $q = \omega^2 + \omega^3$.
a) Pruebe que $p+q = -1$ y que $pq = -1$.
b) Escriba la ecuación cuadrática con coeficientes enteros cuyas raíces son p y q.
c) Exprese p y q como múltiplos enteros de $\cos\left(\frac{2\pi}{5}\right)$ y $\cos\left(\frac{4\pi}{5}\right)$ respectivamente.
d) Halle los valores de $\cos\left(\frac{2\pi}{5}\right)$ y $\cos\left(\frac{4\pi}{5}\right)$.

3.15 Decimos que dos puntos $P, Q \in \mathbb{S}^2$ son *antipodales* si la recta que los une pasa por el origen O, es decir, el segmento de recta $\overline{PQ}$ es un diámetro de la esfera $\mathbb{S}^2$. Si $z_1, z_2 \in \mathbb{C}$ y $\mathrm{pr}(z_1) = P$ y $\mathrm{pr}(z_2) = Q$, pruebe que P y Q son antipodales si y sólo si $z_1 = -\dfrac{1}{\overline{z_2}}$.

3.16 Sea $f(x) \in \mathbb{R}[x]$. Demuestre que si $\alpha \in \mathbb{C}$ es una raíz de $f(x)$, entonces su conjugado complejo $\overline{\alpha}$ también es una raíz de $f(x)$. Esto dice que las raíces complejas de polinomios con coeficientes reales siempre vienen dadas en pares de complejos conjugados.

3.17 ¿Cuáles son los polinomios irreducibles en $\mathbb{C}[x]$? Justifique su respuesta.

3.18 ¿Cuáles son los polinomios irreducibles en $\mathbb{R}[x]$? Justifique su respuesta.

3.19 Utilizando la respuesta a la pregunta anterior, describa cual es la forma que toma la factorización en términos de polinomios irreducibles de un polinomio arbitrario en $\mathbb{R}[x]$.

4. CURVAS ALGEBRAICAS PLANAS

Una curva algebraica plana es en esencia el conjunto de ceros (x, y) de un polinomio no constante $f(x, y) \in F[x, y]$, para F un cuerpo dado. En general las curvas algebraicas se pueden estudiar sobre distintos cuerpos, siendo lo más común hacerlo sobre cuerpos algebraicamente cerrados (es decir, cuerpos K tales que todo polinomio no constante en $K[x]$ tiene al menos una raíz en K), como por ejemplo sobre $\mathbb{C}$, el cuerpo de los números complejos (por el Teorema Fundamental del Álgebra). Empezaremos esta sección dando ejemplos de curvas algebraicas en $\mathbb{R}^2$ (planas) para ir construyendo algo de intuición sobre sus propiedades y el comportamiento que se puede llegar a observar.

La historia del estudio de las curvas algebraicas se remonta a la antigüedad, en particular, al tiempo de los antiguos griegos hace más de 2000 años. Los griegos reconocieron la importancia del estudio de distintas curvas y algunas las estudiaron a profundidad.

Un excelente tratamiento histórico sobre el origen de muchas curvas algebraicas se puede encontrar en el primer capítulo del libro *Plane Algebraic Curves* de Brieskorn y Knörrer.

A continuación daremos una serie de ejemplos de distintas curvas algebraicas, de manera que el lector pueda ir viendo distintos tipos de comportamiento que estas pueden exhibir.

Tal vez las curvas algebraicas más simples que se pueden considerar son las rectas y los círculos, que son dados por las ecuaciones siguientes.

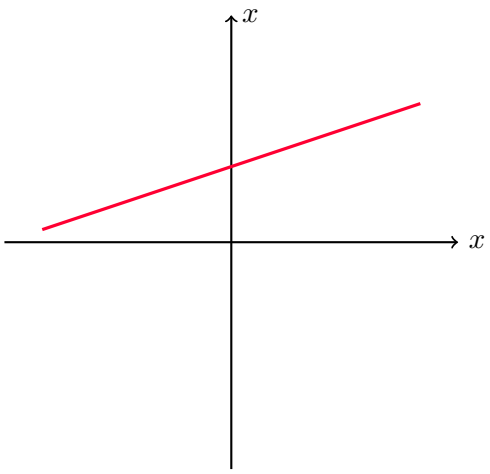

FIGURA 14. Una recta de ecuación $ax + by + c = 0$.

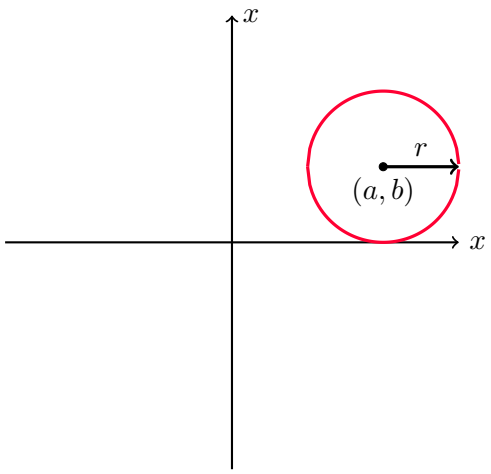

FIGURA 15. El círculo de radio r y centro (a, b) es dado por la ecuación $(x - a)^2 + (y - b)^2 = r^2$.

Los griegos estudiaron a profundidad cierto tipo de curvas llamadas secciones cónicas, que se pueden obtener como intersecciones de un cono circular recto en $\mathbb{R}^3$ con distintos planos, como en la figura siguiente:

FIGURA 16. Obtención de las curvas cónicas. De izquierda a derecha: Parábola, Elipse y Círculo, Hipérbola.

Hoy en día sabemos que las secciones cónicas se pueden describir como conjuntos de ceros de polinomios cuadráticos de la forma

$$ax^2 + bxy + cy^2 + dx + ey + f = 0,$$

con $a, b, c, d, e, f \in \mathbb{R}$ y $a^2 + b^2 + c^2 \neq 0$.

Para el lector con conocimiento de Álgebra Lineal, la ecuación cuadrática general anterior se puede escribir en forma matricial como:

$$\begin{bmatrix} x & y \end{bmatrix} \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} + \begin{bmatrix} x & y \end{bmatrix} \begin{bmatrix} d \\ e \end{bmatrix} + f = 0.$$

La matriz

$$M = \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix}$$

es de particular importancia pues nos permite caracterizar el tipo de cónica definida por la ecuación cuadrática. De hecho más adelante veremos que el tipo de cónica se puede clasificar según el valor del determinante: $\det(M) = ac - \frac{b^2}{4}$. A la cantidad $D := -4\det(M) = b^2 - 4ac$, se le conoce como el discriminante de la ecuación y es en términos de éste que daremos la clasificación.

Las curvas algebraicas dadas por polinomios de grado 3 presentan un comportamiento mucho más variado que el de las de grado 2. Por ejemplo, la curva de ecuación:

$$y^2 = x^3$$

se conoce como la *cúbica cuspidal* o *parábola de Neil*, y tiene el gráfico:

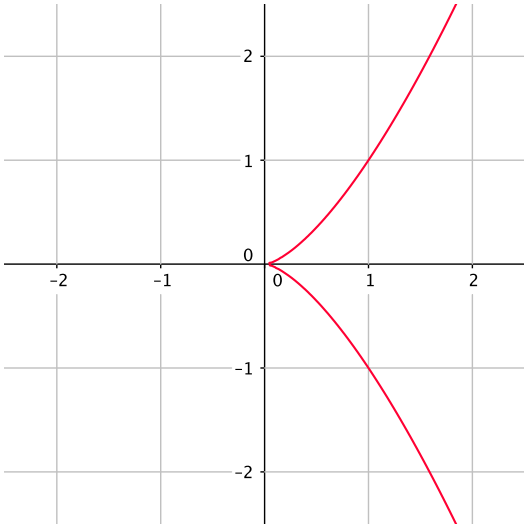

FIGURA 17. La cúbica cuspidal $y^2 = x^3$.

La razón de su nombre es clara de su gráfica, ya que tiene una cúspide o pico en el origen. Esta curva posee una parametrización racional (es decir, una parametrización en términos de funciones racionales), dada por

$$\begin{aligned} \varphi : \mathbb{R} &\longrightarrow \{(x, y) \in \mathbb{R}^2 \mid y^2 = x^3\} \\ t &\longmapsto (t^2, t^3). \end{aligned}$$

Nótese que a medida que el parámetro t crece desde $-\infty$ hasta $+\infty$ el punto $\varphi(t) = (t^2, t^3)$ recorre la curva en dirección ascendente, como en la figura siguiente:

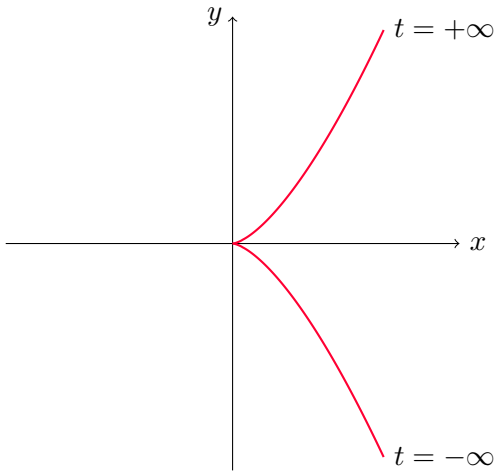

FIGURA 18. Cúbica Cuspidal y dirección de la parametrización φ

Otro ejemplo de una curva cúbica es dado por la curva de la ecuación

$$y^2 = x^3 + x^2 = x^2(x+1),$$

llamada la *curva nodal de Newton*, cuyo gráfico en $\mathbb{R}^2$ es el siguiente.

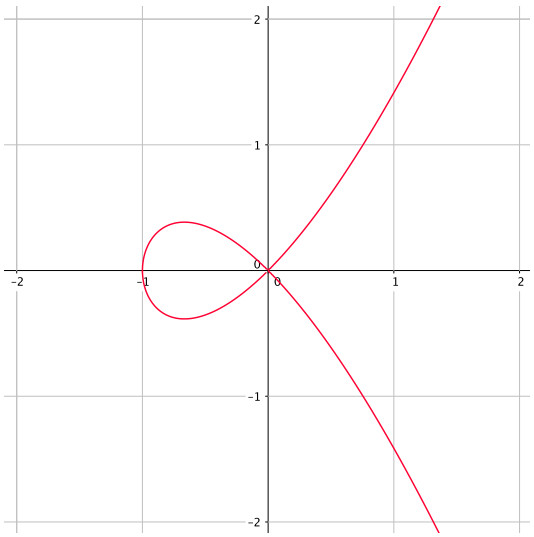

FIGURA 19. La cúbica nodal de Newton $y^2 = x^3 + x^2$.

De nuevo, el nombre cúbica nodal es evidente del gráfico pues como se observa, la curva describe un nodo que pasa por el origen dos veces. Esta curva también admite una parametrización racional, dada por

$$\begin{aligned} \varphi : \mathbb{R} &\to \{(x, y \in \mathbb{R}^2 \mid y^2 = x^3 + x^2 \\ t &\mapsto (t^2 - 1, t - t^3). \end{aligned}$$

En los ejercicios se explicará un método geométrico que permite obtener esta parametrización (y también la de la cúbica cuspidal), que es análogo al método de la proyección estereográfica que vimos para identificar el plano complejo extendido con la esfera $\mathbb{S}^2$.
Note que en este caso, cuando el parámetro t varía de $-\infty$ hasya $+\infty$, la curva es trazada en dirección descendente como se muestra en la figura siguiente.

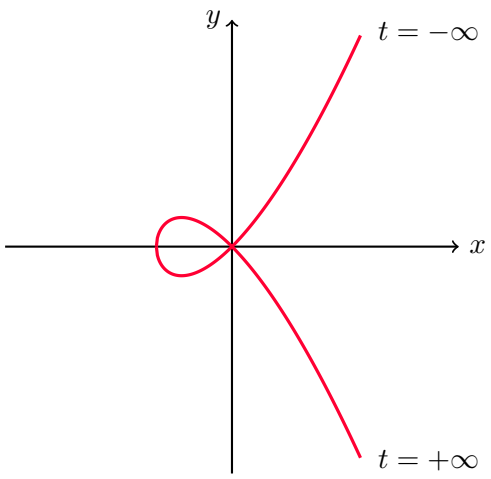

FIGURA 20. Nodal de Newton y dirección de la parametrización φ

Aquí en particular tenemos que $\varphi(-1) = \varphi(1) = (0, 0)$, es decir, la parametrización pasa dos veces por el origen. En este caso, el origen se dice ser un punto doble ordinario. En general, sin embargo, una curva cúbica no necesariamente admite una parametrización racional (más adelante veremos como demostrarlo para ciertos tipos de ecuaciones).
Otro ejemplo famoso de una curva algebraica cúbica es dado por el llamado *Folio de Descartes*, de ecuación:

$$x^3 + y^3 - 3axy = 0 \text{ , para } a \in \mathbb{R}$$

Con métodos de cálculo diferencial se puede mostrar que esta curva es asintota (cuando $x \to \pm\infty$) a la recta de ecuación $x+y+a = 0$. Además se puede mostrar que el folio de Descartes es simétrica con respecto de la recta $y = x$. Su gráfico se muestra a continuación:

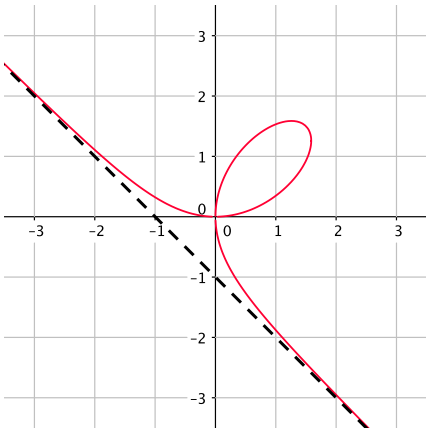

FIGURA 21. El folio de Descartes $x^3 + y^3 - 3xy = 0$ y la recta asíntota $x + y + 1 = 0$.

La historia de esta curva está ligada al descubrimiento del cálculo diferencial. En 1638 Descartes, al tener conocimiento de que Pierre de Fermat había desarrollado un método para encontrar rectas tangentes, decidió retar a Fermat a que encontrara la ecuación de la recta tangente a esta curva en un punto arbitrario, algo que Fermat pudo hacer sin mayor dificultad. Descartes sin embargo nunca pudo resolver el problema.

Otro ejemplo de una curva algebraica definida por un polinomio de grado 3 es dado por la ecuación

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

cuyo gráfico es el gráfico siguiente.

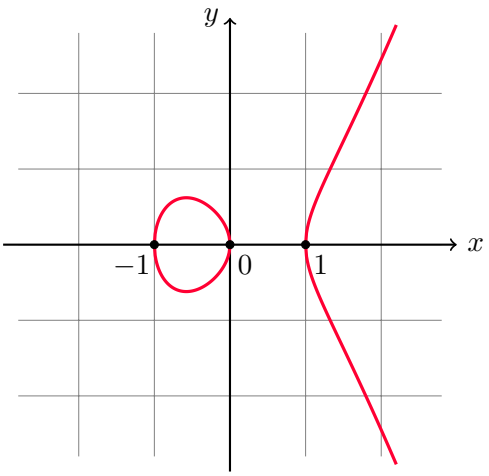

FIGURA 22. La curva elíptica $y^2 = x^3 - x$.

Esta curva algebraica es un ejemplo de una curva elíptica, que estudiaremos más adelante en el curso. El lector notará que a diferencia de las otras curvas algebraicas definidas por polinomios cúbicos que hemos visto hasta ahora, esta posee dos componentes, el óvalo acotado, y la rama no acotada de la derecha.

Otro ejemplo de una curva elíptica es dado por la ecuación

$$y^2 = x^3 + x^2 - x + 1,$$

cuyo gráfico se observa en la siguiente figura.

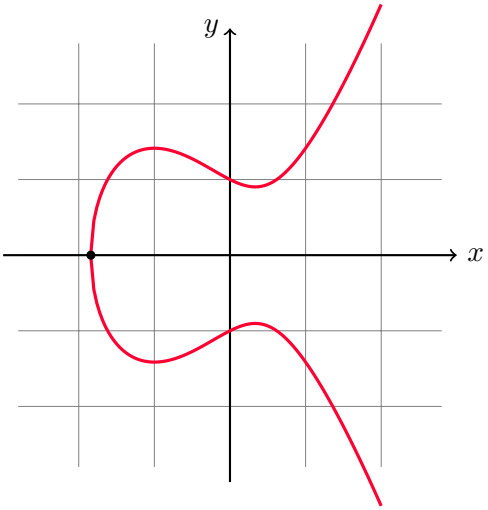

FIGURA 23. La curva elíptica $y^2 = x^3 + x^2 - x + 1$.

En este caso, la curva solo posee un componente. En general, más adelante cuando estudiemos curvas elípticas, veremos que solo estos dos tipos de gráfico se presentan, a saber, pueden tener dos componentes o un solo componente.

Ejemplos de curvas de mayor grado

Hasta el momento solo hemos visto ejemplos de curvas definidas por polinomios de grado menor o igual a 3. Ahora veremos algunos ejemplos de curvas algebraicas dadas por polinomios de mayor grado.

Un ejemplo interesante de una curva de grado 4 es dado por la llamada *curva del diablo*, que es la curva definida por la ecuación

$$y^2(y^2 - a^2) = x^2(x^2 - b^2)$$

para distintos valores $a, b \in \mathbb{R}$. Estas curvas fueron estudiadas por Gabriel Cramer. Por ejemplo, para $(a, b) = (0.8, 1)$ su gráfico toma la siguiente forma.

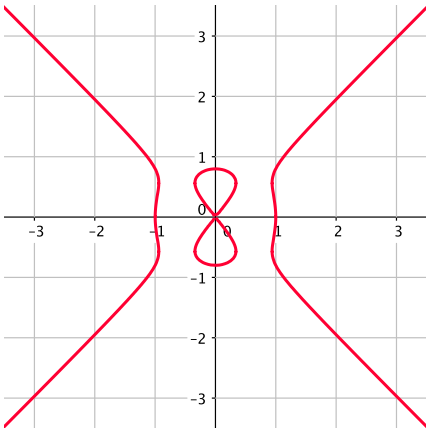

FIGURA 24. La curva del diablo $y^2(y^2 - a^2) = x^2(x^2 - b^2)$ para $(a, b) = (0.8, 1)$.

Su nombre proviene de una confusión que resultó de las palabras en italiano “diabolo” y “diavolo”. La figura de ocho que se ve en el centro de la curva se asemeja a un diábolo, que es un

objeto usado en el malabarismo, por lo cual el nombre que se quería dar a la curva era *curva del diábolo*, pero en algún momento la palabra se confundió con "diavolo", que en italiano significa diablo.

Ejemplos más generales de curvas algebraicas de mayor grado son dados por las llamadas curvas hiperelípticas. Una *curva hiperelíptica* es una curva algebraica dada por una ecuación polinomial de la forma

$$y^2 = f(x),$$

donde $f(x) \in \mathbb{R}[x]$ es un polinomio de grado de grado $n > 4$ sin raíces complejas repetidas. Por ejemplo, la curva de ecuación

$$y^2 = x^5 - 2x^4 - 7x^3 + 8x^2 + 12x = x(x+1)(x+2)(x-2)(x-3)$$

es hiperelíptica y su gráfico tiene la siguiente figura.

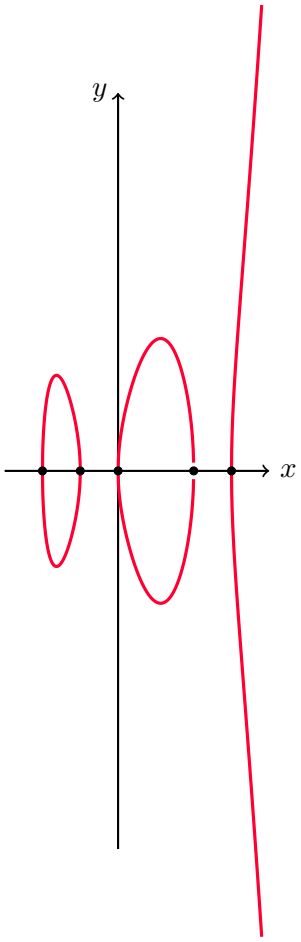

FIGURA 25. La curva hiperelíptica $y^2 =$.

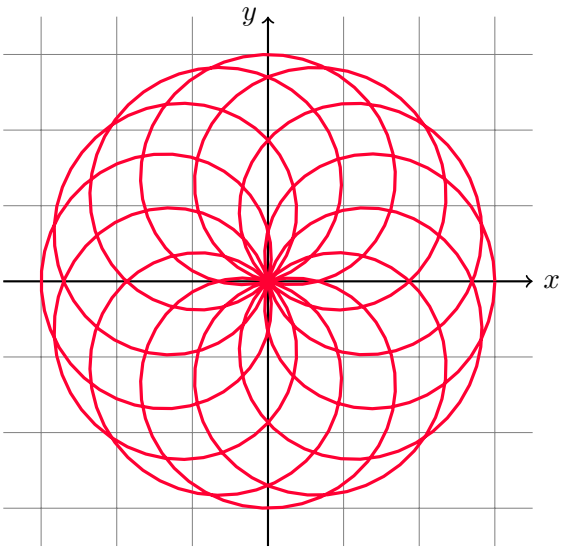

FIGURA 26. La rosa de ecuación polar $r = 3\cos\left(\frac{6}{7}\theta\right)$.