Curso Nivelatorio

Bases para Geometría Algebraica y Teoría de Números

Prof: Adrián Barquero Sánchez

email: adrian.barquero_s@ucr.ac.cr

1. Breve repaso de Geometría Analítica

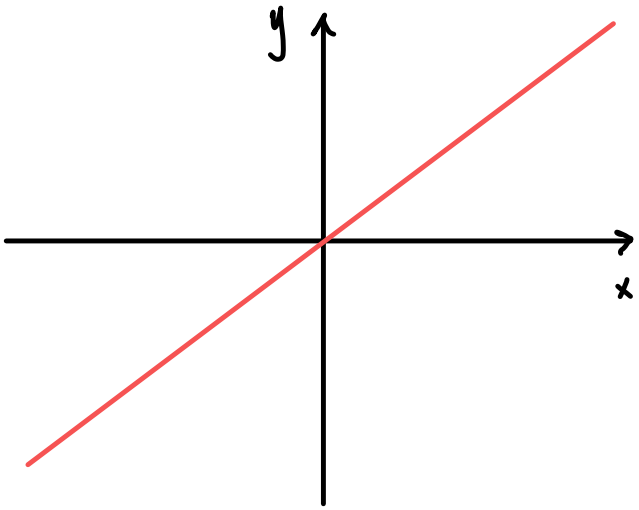
Nos restringimos al plano cartesiano $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R}$.

Ecuaciones de rectas

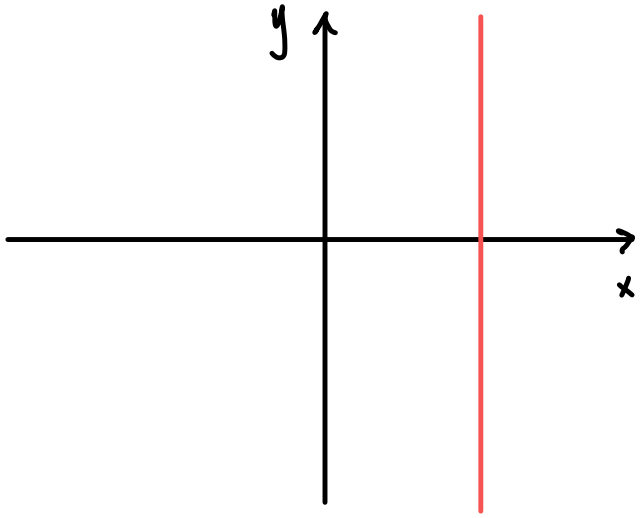
Una recta en $\mathbb{R}^2$ es el conjunto de puntos $(x,y) \in \mathbb{R}^2$ que satisfacen una ecuación de la forma

$$\boxed{ax + by + c = 0},$$

donde $a, b, c \in \mathbb{R}$.



$y = x$



$x = c$

Forma punto-pendiente

Si (x_1, y_1) y (x_2, y_2) son dos puntos en una recta ℓ, con $x_1 \neq x_2$, esta recta se puede describir por la ecuación

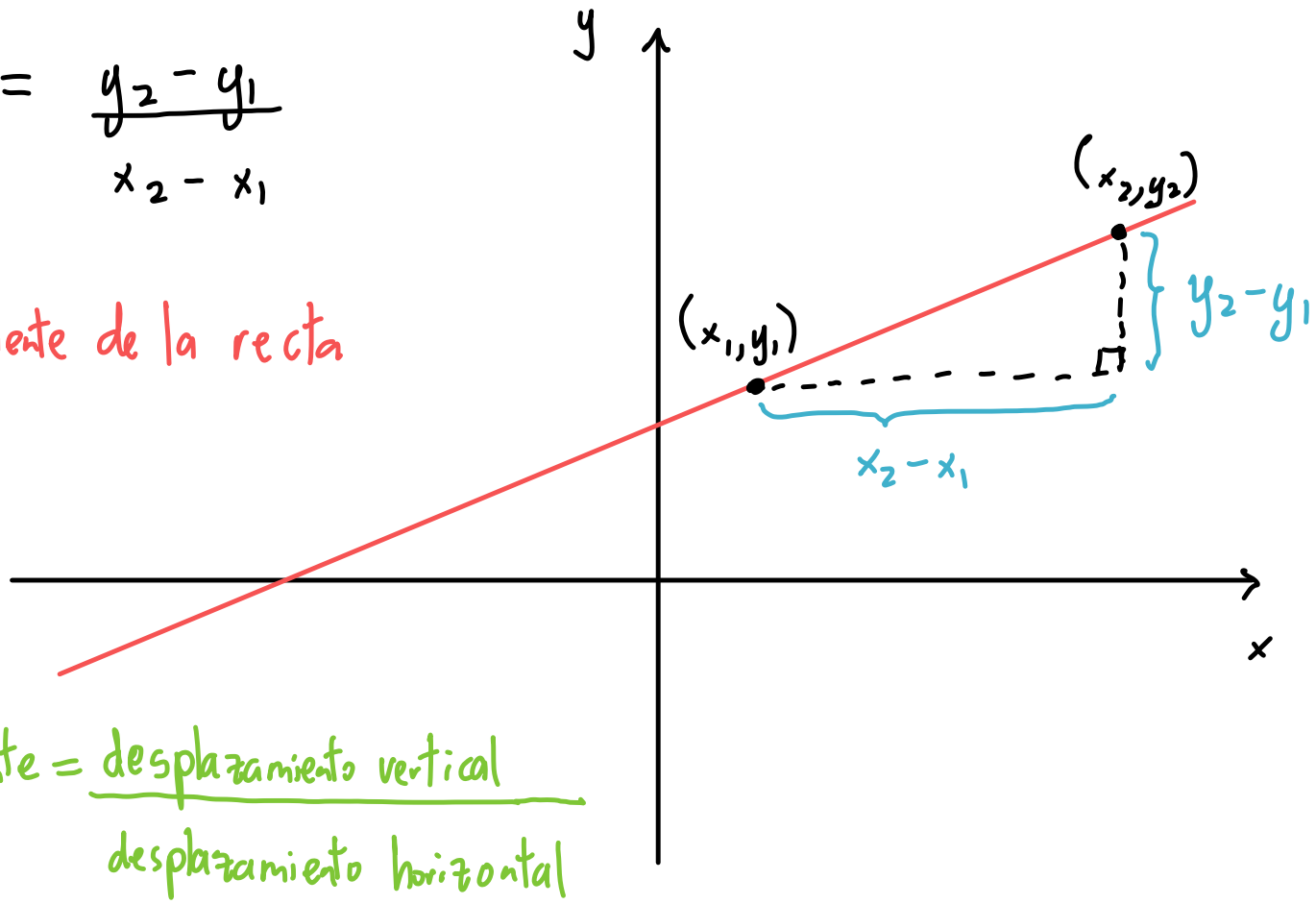
$$\ell: \quad \boxed{y - y_1 = m \cdot (x - x_1)} \,,$$

donde

$$m = \frac{y_2 - y_1}{x_2 - x_1}$$

↓

pendiente de la recta



Pendiente = $\frac{\text{desplazamiento vertical}}{\text{desplazamiento horizontal}}$

Ejemplo

Considere la recta ℓ que pasa por los puntos $P=(5,0)$ y $Q=(-4,6)$. Su pendiente es

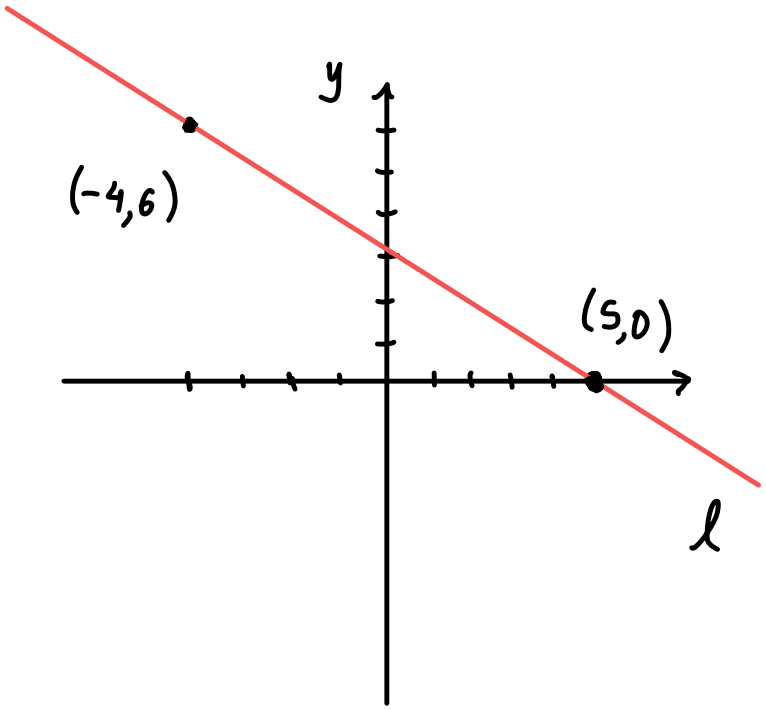
$$m = \frac{6-0}{-4-5} = \frac{6}{-9} = -\frac{2}{3}.$$

La forma punto-pendiente de la ecuación de la recta es (usando el punto P)

$$y-0 = -\frac{2}{3}(x-5),$$

que se puede escribir

$$\boxed{y = -\frac{2}{3}x + \frac{10}{3}}.$$

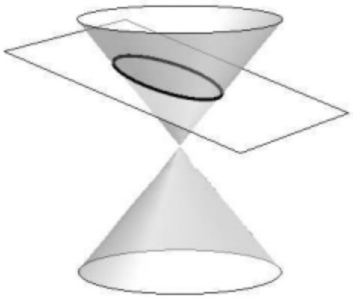


Δ

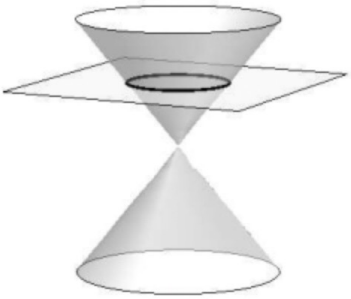
Secciones cónicas

Una **sección cónica** o simplemente una **cónica** es una curva obtenida al intersecar la superficie de un cono con un plano en $\mathbb{R}^3$.

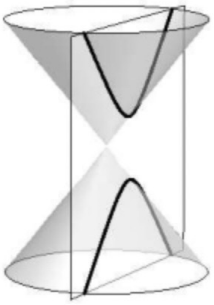
Parabola



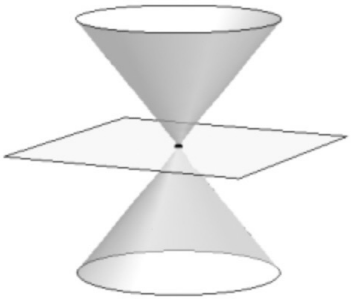
Ellipse



Circle



Hyperbola



Point

Line

Crossed Lines

Cualquiera de estas curvas se puede describir como el conjunto de puntos $(x,y) \in \mathbb{R}^2$ que satisfacen una ecuación cuadrática

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

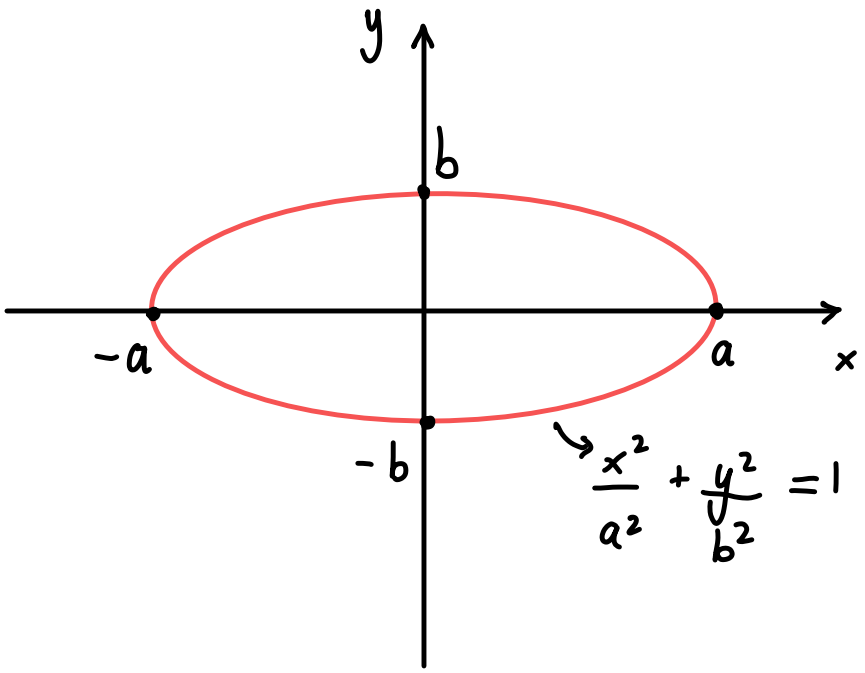
donde $a,b,c,d,e,f \in \mathbb{R}$.

Ejemplo

Una ecuación de la forma

$$\frac{x^2}{a^2}+\frac{y^2}{b^2}=1$$

describe una elipse centrada en el origen.



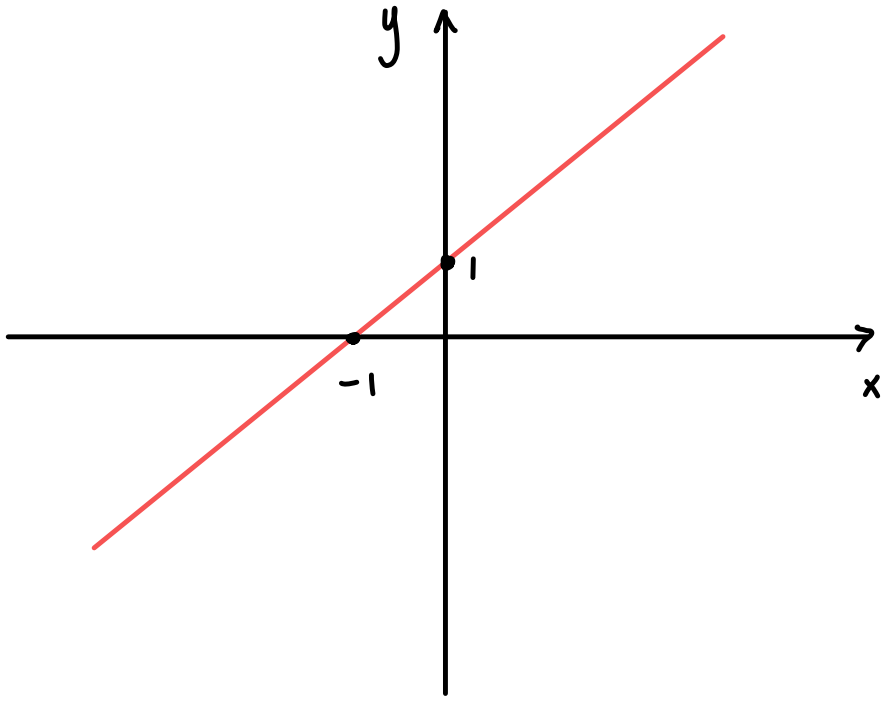
Δ

Ejemplo

Si usamos software para graficar la cónica de ecuación

$$x^2 - 2xy + y^2 + 2x - 2y + 1 = 0$$

obtenemos la siguiente figura:



La razón es que el polinomio cuadrático se factoriza como

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

de modo que la cónica es simplemente la recta $y = x+1$ con "multiplicidad" 2. Δ

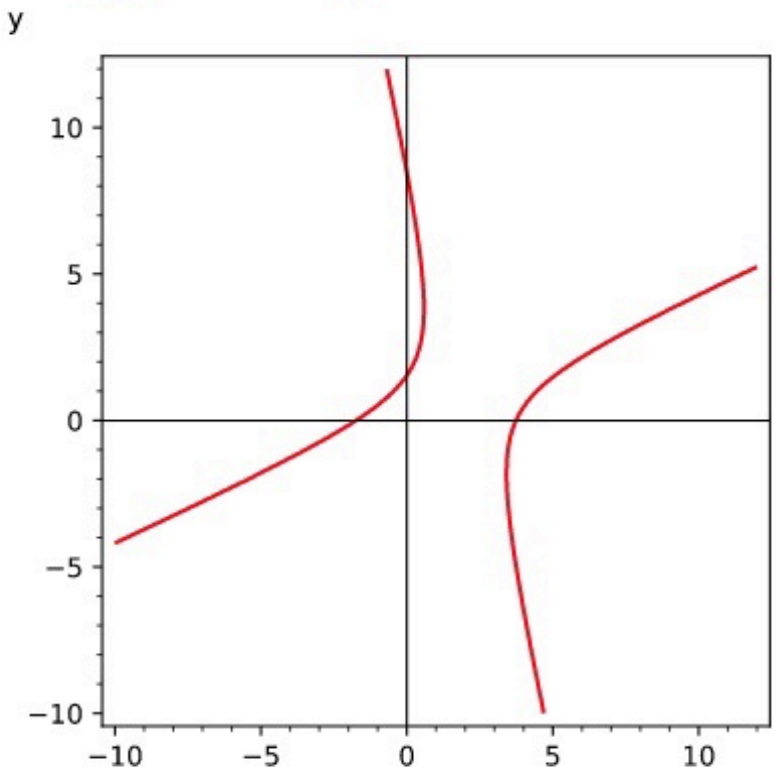
Ejemplo

La cónica de ecuación

$$2x^2 - 4xy - y^2 - 4x + 10y - 13 = 0$$

representa una hipérbola, cuyo gráfico se ve en la siguiente figura.

```
1  var('y')
2  implicit_plot(2*x^2 - 4*x*y - y^2 - 4*x + 10*y -13 == 0, (x, -10, 12), (y, -10, 12),
   axes = True, color = 'red')
```



Rectas tangentes a curvas

Sea $F: \mathbb{R}^2 \longrightarrow \mathbb{R}$ una función continuamente diferenciable. La ecuación

$$\boxed{F(x,y) = 0}$$

define una curva en $\mathbb{R}^2$.

Suponga que (x_0, y_0) es un punto en la curva.

Entonces el Teorema de la Función Implícita dice que si $\left.\frac{\partial F}{\partial y}\right|_{(x_0,y_0)} \neq 0$, entonces existe un vecindario $U \subseteq \mathbb{R}$ de x_0 y una única función continuamente diferenciable $f: U \longrightarrow \mathbb{R}$ tal que $f(x_0) = y_0$ y $F(x, f(x)) = 0$ para todo $x \in U$.

Además, si $y = f(x)$, se tiene que

$$\frac{dy}{dx} = -\frac{\frac{\partial F}{\partial x}}{\frac{\partial F}{\partial y}}.$$

Rectas tangentes

De acuerdo a lo anterior, si $F(x,y)=0$ define una curva y (a,b) es un punto de esta con $\frac{\partial F}{\partial y}(a,b) \neq 0$, la pendiente de la tangente en (a,b) es

$$m = -\frac{\frac{\partial F}{\partial x}(a,b)}{\frac{\partial F}{\partial y}(a,b)},$$

por lo que la forma punto-pendiente es

$$y - b = m(x - a)$$

$$\Rightarrow \quad y-b = -\frac{\frac{\partial F}{\partial x}(a,b)}{\frac{\partial F}{\partial y}(a,b)} \cdot (x-a)$$

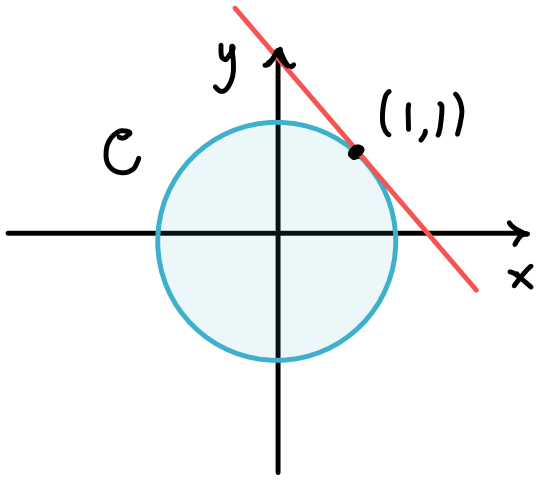
$$\Rightarrow \quad \frac{\partial F}{\partial y}(a,b)\cdot(y-b) = -\frac{\partial F}{\partial x}(a,b)\cdot(x-a)$$

$$\Rightarrow \quad \boxed{\frac{\partial F}{\partial x}(a,b)\cdot(x-a) + \frac{\partial F}{\partial y}(a,b)\cdot(y-b) = 0}$$

↳ Ecuación de la recta tangente

Ejemplo

Considere el círculo de ecuación $x^2+y^2=2$.



El punto $(1,1)$ está en el círculo. Vamos a encontrar la ecuación de la tangente en este punto.

Sea $F(x,y) = x^2 + y^2 - 2$. Entonces

$$\frac{\partial F}{\partial x} = 2x \quad \text{y} \quad \frac{\partial F}{\partial y} = 2y,$$

por lo que $\frac{\partial F}{\partial x}(1,1) = 2 = \frac{\partial F}{\partial y}(1,1)$.

Entonces la recta tangente en $(1,1)$ tiene ecuación

$$2\cdot(x-1) + 2\cdot(y-1) = 0$$

$$\Rightarrow \quad 2x - 2 + 2y - 2 = 0$$

$$\Rightarrow \quad \boxed{y = -x + 2}.$$

Δ

2. Anillos, ideales y polinomios

Recordemos la definición de un anillo.

Definición:

Un anillo (con identidad) es un triplete $(A, +, \cdot)$ tal que $+ : A \times A \longrightarrow A$ y $\cdot : A \times A \longrightarrow A$ son operaciones binarias en A que satisfacen las siguientes propiedades:

- $+$ es asociativa: $a+(b+c) = (a+b)+c$ para todo $a, b, c \in A$
- Existe un elemento $0_A \in A$ tal que $0_A + a = a + 0_A = a$ para todo $a \in A$
- Para cada $a \in A$ existe un elemento $-a \in A$ tal que $a+(-a) = -a+a = 0_A$.
- Para todo $a, b \in A$ se tiene $a+b = b+a$.

- El producto $\cdot$ es asociativo: $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

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

- Existe un elemento $1_A \in A$ tal que $1_A \cdot a = a \cdot 1_A = a$

  para todo $a \in A$

- Para todo $a, b, c \in A$ se cumple que

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

y

$$(a + b) \cdot c = a \cdot c + b \cdot c.$$

Además, decimos que A es un anillo conmutativo si $a \cdot b = b \cdot a$ para todo $a, b \in A$.

- Un cuerpo es un anillo conmutativo en el que para todo $a \in A$ con $a \neq 0_A$ existe $a^{-1} \in A$ tal que $a \cdot a^{-1} = a^{-1} \cdot a = 1_A$.

Ejemplo

1. El triplete $(\mathbb{Z}, +, \cdot)$ es un anillo conmutativo.

2. Similarmente $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ y $(\mathbb{C}, +, \cdot)$ son todos cuerpos.

3. Si F es un cuerpo, el triplete $(F[x], +, \cdot)$ donde $F[x]$ es el conjunto de todos los polinomios en la indeterminada x y con coeficientes en F, es un anillo conmutativo.

Δ

Un concepto fundamental en la Teoría de Anillos es el de un ideal. Este se puede pensar como análogo al de un subespacio vectorial en el estudio de los espacios vectoriales.

Ideal

Sea A un anillo conmutativo. Un subconjunto $I \subseteq A$ no vacío se llama un ideal de A si

(i) Para todo $r, s \in I$ se tiene $r+s \in I$.

(ii) Para todo $r \in I$ y todo $a \in A$ se tiene $a \cdot r \in I$.

Ejemplo

En el anillo de los enteros $\mathbb{Z}$ todos los ideales son los conjuntos de la forma

$$n\mathbb{Z} = \{ nk \mid k \in \mathbb{Z} \}$$

$$= \{ \ldots, -4n, -3n, -2n, -n, 0, n, 2n, 3n, \ldots \}$$

de múltiplos de algún entero fijo $n \in \mathbb{Z}$. Δ

Una manera de construir ideales es con un conjunto de generadores.

Ideal generado por un conjunto finito

Sea $X = \{x_1, \dots, x_n\}$ un subconjunto finito de un anillo conmutativo A.

El ideal generado por X en A, denotado

$$\langle X \rangle = \langle x_1, \dots, x_n \rangle$$

es el subconjunto

$$\langle x_1, \dots, x_n \rangle = \{ a_1 \cdot x_1 + \dots + a_n x_n \mid a_1, \dots, a_n \in A \}$$

de todas las combinaciones lineales de los x_i con coeficientes en A.

Ejemplo

En el anillo $\mathbb{R}[x,y]$ de polinomios en las variables x, y con coeficientes reales, el subconjunto

$$I = \{ f(x,y) \in \mathbb{R}[x,y] \mid f(0,0) = 0 \}$$

es un ideal.

Además, se puede demostrar que

$$I = \langle x, y \rangle = \{ x \cdot g(x,y) + y \cdot h(x,y) \mid h, g \in \mathbb{R}[x,y] \}.$$

Δ

Una construcción sumamente importante es la de un anillo cociente, y el concepto de ideal nos permite llevar a cabo la construcción.

Anillos cociente

Sea A un anillo conmutativo y sea I un ideal de A.

En A se define una relación de equivalencia $\sim$ por:

$$a \sim b \iff a - b \in I.$$

La clase de equivalencia $[a]$ es

$$[a] = \{ a + r \mid r \in I \} = a + I.$$

El conjunto cociente $A/I = \{ a + I \mid a \in A \}$

forma un anillo con las operaciones $+$ y $\cdot$ dadas por:

$$(a + I) + (b + I) := (a + b) + I$$

$$(a + I) \cdot (b + I) := a \cdot b + I.$$

Los elementos neutros son:

neutro aditivo: $0+I = I$ $\quad (a+I)+(0+I) = (a+0)+I = a+I$

neutro multiplicativo: $1+I$ $\quad (1+I)\cdot(a+I) = (1\cdot a)+I = a+I$

Ejemplo (Los enteros módulo n)

Sea $n>1$ un entero El conjunto $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ es un ideal en $\mathbb{Z}$. Por lo tanto podemos formar el anillo cociente

$$\mathbb{Z}_n := \mathbb{Z}/n\mathbb{Z} = \{a+n\mathbb{Z} \mid a \in \mathbb{Z}\}.$$

Por el Algoritmo de la División, dado $a \in \mathbb{Z}$, existen $q, r \in \mathbb{Z}$ únicos, tales que

$$a = qn+r$$

con $0 \leq r \leq n-1$.

Por lo tanto $a \sim r$ pues $a - r = qn \in n\mathbb{Z}$,

de modo que

$$a + n\mathbb{Z} = r + n\mathbb{Z}.$$

Entonces

$$\mathbb{Z}/n\mathbb{Z} = \{0 + n\mathbb{Z}, 1 + n\mathbb{Z}, 2 + n\mathbb{Z}, \ldots, n-1 + n\mathbb{Z}\}$$

es un anillo con exactamente n elementos.

A veces se usan las siguientes notaciones

$$\bar{a} = [a]_n = a + n\mathbb{Z}.$$

Ejemplo

Consideremos los enteros módulo 5.

$$\mathbb{Z}_5 = \mathbb{Z}/5\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}.$$

Por ejemplo:

$\bar{2} + \bar{1} = \overline{2+1} = \bar{3}$

$\bar{2} + \bar{3} = \overline{2+3} = \bar{5} = \bar{0}$

$\bar{a} = a + 5\mathbb{Z}$

$\bar{b} = b + 5\mathbb{Z}$

$\bar{a} + \bar{b} = (a + 5\mathbb{Z}) + (b + 5\mathbb{Z})$

$= (a+b) + 5\mathbb{Z}$

$= \overline{a+b}$

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

Como ejercicio pueden hacer la tabla análoga para la multiplicación.

Ejemplo

Considere la ecuación $f(x,y) = y^2 - x^3 - 1 = 0$, es decir $y^2 = x^3 + 1$. Queremos encontrar el conjunto de soluciones $(x,y) \in (\mathbb{Z}/n\mathbb{Z})^2$ para algunos valores de n.

$n = 2$ En $\mathbb{Z}/2\mathbb{Z} = \{\bar{0}, \bar{1}\} = \{0+2\mathbb{Z}, 1+2\mathbb{Z}\}$

$x = 0 \Rightarrow 0^3 + 1 = 1 = y^2 \Rightarrow y = 1$

$\Rightarrow (\bar{0}, \bar{1})$

$x = \bar{1} \Rightarrow \bar{1}^3 + \bar{1} = \bar{2} = \bar{0} \Rightarrow y = \bar{0}$

$\Rightarrow (\bar{1}, \bar{0})$.

Entonces sobre $(\mathbb{Z}/2\mathbb{Z})^2$, las soluciones de la ecuación $y^2 = x^3 + 1$ son $\{(\bar{0}, \bar{1}), (\bar{1}, \bar{0})\}$.

Polinomios

Sea A un anillo. Al conjunto de polinomios en las variables $x_1, \dots, x_n$ con coeficientes en A se le denota por $A[x_1, \dots, x_n]$.

Un polinomio $f(x_1, \dots, x_n) \in A[x_1, \dots, x_n]$ es una suma finita de términos de la forma

$$a x_1^{K_1} \cdot x_2^{K_2} \cdots x_n^{K_n},$$

con $a \in A$ y $K_1, \dots, K_n \in \mathbb{N}$.

Entonces f se puede escribir como

$$f = \sum_{i=0}^{m} a_i x_1^{K_{i1}} \cdots x_n^{K_{in}}$$

para algún $m \in \mathbb{N}$.

Definición

Sea A un anillo. El grado de un monomio no cero

$$a x_1^{K_1} x_2^{K_2} \cdots x_n^{K_n} \in A[x_1, \ldots, x_n]$$

es el entero no negativo $K_1 + K_2 + \cdots + K_n$.

Si f es un polinomio no cero en $A[x_1, \ldots, x_n]$, entonces sabemos que

$$f = \sum_{i=0}^{m} a_i x_1^{K_{i_1}} \cdots x_n^{K_{i_n}}.$$

Entonces, el grado (total) de f es el máximo de los grados de los monomios $a_i x_1^{K_{i_1}} \cdots x_n^{K_{i_n}}$ tales que $a_i \neq 0_A$.

El grado (total) de f se denota por $\text{grad}(f)$, o a veces por $\partial(f)$. Δ

- Un polinomio que es una suma de monomios, cada uno de grado K, se dice ser homogéneo de grado K.

Ejemplo

Sea $f(x,y,z) = 5x^2yz^3 - 7xyz + 11x^5z \in \mathbb{Z}[x,y,z]$

grado 6 grado 3 grado 6

Entonces el grado de f es 6. Este polinomio no es homogéneo.

Un hecho fundamental sobre los polinomios es el siguiente.

Teorema (Algoritmo de la División)

Sea F un cuerpo. Entonces si $a(x), b(x) \in F[x]$ con $b(x) \neq 0$, existen polinomios únicos $q(x)$ y $r(x)$ en $F[x]$ tales que

$$a(x) = q(x) \cdot b(x) + r(x)$$

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

Ejemplo

Vamos a examinar el anillo cociente $\mathbb{R}[x]/\langle x^2+1\rangle$.

Tenemos $\mathbb{R}[x]/\langle x^2+1\rangle = \{ f(x) + \langle x^2+1\rangle \mid f(x) \in \mathbb{R}[x] \}$.

Por el Algoritmo de la división en $\mathbb{R}[x]$, dado $f(x) \in \mathbb{R}[x]$, existen $q(x), r(x) \in \mathbb{R}[x]$ únicos, tales que

$$f(x) = q(x)\cdot(x^2+1) + r(x),$$

donde $r(x)=0$ o $0 \leq \partial(r(x)) < 2$.

Entonces $r(x) = a+bx$ con $a, b \in \mathbb{R}$.

Luego $f(x) \sim r(x)$, por lo que

$$f(x) + \langle x^2+1\rangle = r(x) + \langle x^2+1\rangle$$
$$= a+bx+\langle x^2+1\rangle.$$

Entonces

$$\mathbb{R}[x]/\langle x^2+1\rangle = \{ \underbrace{a+bx+\langle x^2+1\rangle}_{\downarrow\ a+bi} \mid a,b \in \mathbb{R}\}.$$

Este anillo cociente es un cuerpo y de hecho es isomorfo al cuerpo $\mathbb{C}$ de los números complejos bajo el isomorfismo

$$\phi : \mathbb{R}[x]/\langle x^2+1\rangle \longrightarrow \mathbb{C}.$$

$$a+bx+\langle x^2+1\rangle \longmapsto a+bi$$

Raíces de polinomios

Teorema del factor:

Si F es un cuerpo y $\alpha \in F$ es una raíz de un polinomio $f(x) \in F[x]$, entonces existe $g(x) \in F[x]$ tal que

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

Usando este resultado, dado $\alpha \in F$, se puede escribir

$$f(x) = (x-\alpha)^m \cdot g(x)$$

con $g(x) \in F[x]$, $m \geq 0$, donde $g(\alpha) \neq 0$.

Al entero m se le llama la multiplicidad de la raíz α.

Existen distintos criterios para decidir si un polinomio tiene o no raíces repetidas (es decir, con multiplicidad mayor a 1).

Teorema

Sea $f(x) \in F[x]$, donde F es un cuerpo y sea $\alpha \in F$.

(i) α es una raíz múltiple de $f(x) \iff f(\alpha)=0$ y $f'(\alpha)=0$.

(ii) Si $\text{mcd}(f(x), f'(x)) = 1$, entonces f no tiene raíces múltiples.

Demostración

(i) ($\Longrightarrow$) Suponga que α es una raíz múltiple de $f(x)$. Entonces existe un polinomio $g(x) \in F[x]$ y un entero $m > 1$ tales que

$$f(x) = (x-\alpha)^m \cdot g(x).$$

Luego

$$f'(x) = m(x-\alpha)^{m-1} \cdot g(x) + (x-\alpha)^m \cdot g'(x).$$

Por lo tanto $f'(\alpha) = 0$. $\square$

Resultantes

Son una herramienta muy usada en áreas como el álgebra computacional, la teoría de números y la geometría algebraica.

Definición

El **resultante** $\text{Res}(f, g; x)$ de dos polinomios

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

y

$$g(x) = b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0$$

se define como el determinante de la matriz $(m+n) \times (m+n)$

$$\mathrm{Res}(f,g;x) = \begin{vmatrix} a_n & a_{n-1} & \cdots & a_0 & 0 & 0 & \cdots & 0 \\ 0 & a_n & a_{n-1} & \cdots & a_0 & 0 & \cdots & 0 \\ 0 & 0 & \ddots & \ddots & & & & \\ 0 & 0 & \cdots & 0 & a_n & a_{n-1} & \cdots & a_0 \\ b_m & b_{m-1} & \cdots & b_0 & 0 & 0 & \cdots & 0 \\ 0 & b_m & b_{m-1} & \cdots & b_0 & 0 & \cdots & 0 \\ 0 & 0 & \ddots & \ddots & & & & \\ 0 & 0 & \cdots & 0 & b_m & b_{m-1} & \cdots & b_0 \end{vmatrix}$$

Acá hay m filas de a's y n filas de b's.

Ejemplo

Si $f(x) = a_2x^2 + a_1x + a_0$ y $g(x) = b_3x^3 + b_2x^2 + b_1x + b_0$,

entonces

$$\mathrm{Res}(f,g;x) = \begin{vmatrix} a_2 & a_1 & a_0 & 0 & 0 \\ 0 & a_2 & a_1 & a_0 & 0 \\ 0 & 0 & a_2 & a_1 & a_0 \\ b_3 & b_2 & b_1 & b_0 & 0 \\ 0 & b_3 & b_2 & b_1 & b_0 \end{vmatrix}.$$

Δ

Una propiedad fundamental de los resultantes es la siguiente.

Teorema

$f(x)$ y $g(x)$ tienen una raíz en común si y solo si $\operatorname{Res}(f,g;x)=0$. □

Ejemplo

Sean $f(x)=x-a$ y $g(x)=x-b$. Entonces

$$\operatorname{Res}(f,g;x)=\begin{vmatrix} 1 & -a \\ 1 & -b \end{vmatrix} = -b+a$$

En este caso es claro que f y g tienen una raíz en común $\Leftrightarrow \operatorname{Res}(f,g;x)=0$. △

Ejemplo

Considere los polinomios $f(x) = x^2 - 1$ y $g(x) = x^2 + x - 2$.

Observe que

raíces de $f(x)$: ± 1

raíces de $g(x)$: 1 y -2

Por lo tanto f y g tienen una raíz en común.

Veamos que entonces $\text{Res}(f, g; x) = 0$.

$$\text{Res}(f, g; x) = \begin{vmatrix} 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \\ 1 & 1 & -2 & 0 \\ 0 & 1 & 1 & -2 \end{vmatrix}$$

$$\xrightarrow{f_3 \to f_3 - f_1} \begin{vmatrix} 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \\ 0 & 1 & -1 & 0 \\ 0 & 1 & 1 & -2 \end{vmatrix} = \begin{vmatrix} 1 & 0 & -1 \\ 1 & -1 & 0 \\ 1 & 1 & -2 \end{vmatrix}$$

$$\begin{matrix} f_2 \to f_2 - f_1 \\ \longrightarrow \\ f_3 \to f_3 - f_1 \end{matrix} \quad \begin{vmatrix} 1 & 0 & -1 \\ 0 & -1 & 1 \\ 0 & 1 & -1 \end{vmatrix} = \begin{vmatrix} -1 & 1 \\ 1 & -1 \end{vmatrix} = 0. \quad \Delta$$

Como vimos antes, un polinomio $f(x)$ tiene una raíz repetida $\Leftrightarrow$ $f(x)$ y $f'(x)$ tienen una raíz en común. Veamos qué pasa con el resultante.

Ejemplo

Sea $f(x) = ax^2 + bx + c$. Entonces $f'(x) = 2ax + b$.

Vamos a calcular $\operatorname{Res}(f, f'; x)$.

$$\operatorname{Res}(f, f'; x) = \begin{vmatrix} a & b & c \\ 2a & b & 0 \\ 0 & 2a & b \end{vmatrix} \xrightarrow{f_2 \to f_2 - 2f_1} \begin{vmatrix} a & b & c \\ 0 & -b & -2c \\ 0 & 2a & b \end{vmatrix}$$

$$= a \cdot \begin{vmatrix} -b & -2c \\ 2a & b \end{vmatrix} = a(-b^2 + 4ac)$$

Note que $\operatorname{Res}(f, f'; x) = -a \cdot \operatorname{disc}(f)$.

Como $a \neq 0$, entonces $\operatorname{Res}(f, f'; x) = 0 \iff \operatorname{disc}(f) = 0$

$\iff$ f tiene una raíz repetida. Δ

De hecho, más generalmente tenemos la siguiente definición.

Definición

Sea $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in F[x]$, donde F es un cuerpo. El discriminante de $f(x)$ se define como

$$\operatorname{disc}(f) := \frac{(-1)^{\frac{n(n-1)}{2}}}{a_n} \cdot \operatorname{Res}(f, f'; x).$$

Ejemplo

Si $f(x) = ax^2 + bx + c$, vimos en el ejemplo anterior que $\operatorname{Res}(f, f'; x) = a(-b^2 + 4ac)$. Por lo tanto

$$\operatorname{disc}(f) = \frac{(-1)^{\frac{2\cdot(2-1)}{2}}}{a} \cdot a \cdot (-b^2 + 4ac)$$

$$= -(-b^2 + 4ac)$$

$$= b^2 - 4ac.$$

Δ

Ejemplo

Sea $f(x) = x^3 + ax + b$. Entonces $f'(x) = 3x^2 + a$.

Por lo tanto

$$\operatorname{Res}(f, f'; x) = \begin{vmatrix} 1 & 0 & a & b & 0 \\ 0 & 1 & 0 & a & b \\ 3 & 0 & a & 0 & 0 \\ 0 & 3 & 0 & a & 0 \\ 0 & 0 & 3 & 0 & a \end{vmatrix} = 4a^3 + 27b^2.$$

Por lo tanto

$$\operatorname{disc}(x^3+ax+b) = \frac{(-1)^{\frac{3\cdot(3-1)}{2}}}{1} \cdot 1 \cdot \operatorname{Res}(f, f'; x)$$

$$= -(4a^3+27b^2).$$

De este modo, el polinomio cúbico $f(x) = x^3+ax+b$ tiene raíces repetidas $\Leftrightarrow$ $4a^3+27b^2=0$. Δ

3. Grupos

Definición

Un conjunto no vacío G junto con una operación binaria $* : G \times G \longrightarrow G$ se llama un grupo si se cumplen las siguientes propiedades:

(i) $*$ es asociativa.

(ii) Existe un elemento $e_G \in G$, llamado neutro o identidad, tal que

$$x * e_G = e_G * x = x$$

para todo $x \in G$.

(iii) Para todo elemento $x \in G$ existe un elemento $y \in G$ tal que

$$x * y = y * x = e_G.$$

El elemento y se llama un inverso de x.

Definición

Un grupo G en el cual la operación binaria $*: G \times G \to G$ es conmutativa se dice ser abeliano.

Nota: Esto en honor al matemático noruego Niels Henryk Abel $(1802-1829)$

Nota: Cuando se trabaja con grupos abelianos es común usar notación aditiva para la operación binaria. Es decir, se suele escribir $(G, +)$ y las propiedades se escriben como:

(i)' $+$ es asociativa.

(ii)' Existe un elemento $0_G \in G$ tal que

$$x + 0_G = 0_G + x = x$$

para todo $x \in G$.

(iii)' Para todo $x \in G$, existe $y \in G$ tal que

$$x + y = y + x = 0_G.$$

Ejemplo

① $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ son todos ejemplos de grupos abelianos.

② Si cambiamos la operación binaria a multiplicación tenemos que:

$(\mathbb{Z}, \cdot)$ no es un grupo pues si bien la multiplicación es asociativa y existe un neutro 1, en general la propiedad (iii) falla pues los únicos enteros para los cuales hay inversos multiplicativos en $\mathbb{Z}$ son 1 y -1.

③ Similarmente, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$ y $(\mathbb{C}, \cdot)$ no son grupos pues el 0 no tiene un inverso multiplicativo, es decir, no existe y tal que

$$0 \cdot y = y \cdot 0 = 1.$$

④ Si eliminamos el 0 en el ejemplo anterior sí obtenemos grupos. Es decir, $(\mathbb{Q}^\times, \cdot)$, $(\mathbb{R}^\times, \cdot)$, $(\mathbb{C}^\times, \cdot)$ son todos grupos abelianos con elemento neutro 1.

Potencias de un elemento y grupos cíclicos

En general, si $(G, *)$ es un grupo, es común simplificar la notación $x * y$ por xy simplemente, como se suele hacer para la multiplicación en los conjuntos de números usuales $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$.

Con esta notación, el inverso $(xy)^{-1}$ sería $y^{-1}x^{-1}$, por ejemplo.

Definición (Potencias y múltiplos (en el caso aditivo))

Sea x un elemento de un grupo G. Definimos las potencias (resp. múltiplos) x^n (resp. nx) de x^n, para $n \in \mathbb{Z}$, por:

(i) $x^0 := e_G$ ($0 \in \mathbb{Z}$)

(ii) $x^n := \underbrace{x x \cdots x}_{n \text{ factores}}$ si $n > 0$

(i)' $0x := 0_G$ ($0 \in \mathbb{Z}$, $0_G \in G$)

(ii)' $nx := \underbrace{x + x + \cdots + x}_{n \text{ sumandos}}$ si $n > 0$

(iii) $x^{-n} := (x^{-1})^n$

$= \underbrace{x^{-1} x^{-1} \cdots x^{-1}}_{n \text{ factores}}$

si $n > 0$

(iii) $-nx := n(-x)$

$= \underbrace{(-x) + (-x) + \cdots + (-x)}_{n \text{ sumandos}}$

si $n > 0$

Δ

Estas potencias (o múltiplos satisfacen las reglas usuales).

Teorema

Sea G un grupo y sea $x \in G$. Entonces para $m, n \in \mathbb{Z}$, se tiene que:

(i) $x^m x^n = x^{m+n} = x^n x^m$

(ii) $(x^n)^{-1} = x^{-n}$

(iii) $(x^m)^n = x^{mn} = (x^n)^m$

(i)' $mx + nx = (m+n)x = nx + mx$

(ii)' $-(nx) = -nx$

(iii)' $n(mx) = nmx = m(nx)$

Nota: • Las demostraciones son sencillas y se pueden hacer tomando casos. Ver el Teorema 4.1 del libro de Dan Saracino.

- En general sabemos que el producto de elementos en un grupo arbitrario no tiene por qué ser conmutativo, pero, como muestra la propiedad (1), el producto de dos potencias de un mismo elemento sí es conmutativo.

Un concepto muy importante en la Teoría de Grupos es el siguiente.

Definición

- Si G es un grupo y $x \in G$, entonces se dice que x es de orden finito si existe un entero positivo n tal que $x^n = e$ (o en el caso aditivo $nx = 0_G$).
- Si tal entero existe, entonces el menor entero positivo $n \geq 1$ tal que $x^n = e$, es llamado el orden de x y se denota $o(x)$ (o en algunos textos por $ord(x)$).
- Si x no es de orden finito, decimos que x es

de orden infinito y escribimos $o(x) = \infty$.

Ejemplos

① Sea G un grupo. El único elemento de orden 1 en G es el neutro $e = e_G$.

② Considere el grupo abeliano $(\mathbb{R}^\times, \cdot)$. Entonces:

- Los elementos de orden 2 en $\mathbb{R}^\times$ son los números reales $x \in \mathbb{R}$ que satisfacen

$$x^2 = 1$$

y que no satisfacen $x^1 = 1$. Entonces el único elemento de orden 2 en $(\mathbb{R}^\times, \cdot)$ es $x = -1$.

- Los elementos de orden 3 en $\mathbb{R}^\times$ son los números reales $x \in \mathbb{R}$ tales que

$$x^3 = 1$$

y $x^n \neq 1$ para $n = 1$ y $n = 2$.

Sabemos que en $\mathbb{R}^\times$ hay un único elemento tal que $x^3 = 1$, a saber $x = 1$, pero $x = 1$ es de orden 1, por lo tanto no hay elementos de orden 3 en $\mathbb{R}^\times$.

- Los elementos de orden 4 en $(\mathbb{R}^\times, \cdot)$ satisfacen la ecuación

$$x^4 = 1$$

pero además $x^n \neq 1$ para $n = 1, 2, 3$.

Las raíces de $x^4 = 1$ son dadas por

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

($x^2 + 1$: no tiene raíces en $\mathbb{R}$)

$$\iff x^2 - 1 = 0$$
$$\iff x = \pm 1.$$

Como ya sabemos 1 es de orden 1 y -1 es de orden 2, por lo que no hay elementos de orden 4 en $(\mathbb{R}^\times, \cdot)$.

③ Generalizando el ejemplo anterior, como las raíces reales de la ecuación $x^n = 1$ son:

- $\{1, -1\}$ si n es par
- $\{1\}$ si n es impar,

vemos que los únicos elementos de orden finito en $(\mathbb{R}^\times, \cdot)$ son 1 (que es de orden 1) y -1 (que es de orden 2). Es decir, en $(\mathbb{R}^\times, \cdot)$ no existen elementos de orden n para ningún $n \geq 3$.

④ En el grupo aditivo $(\mathbb{R}, +)$, no hay elementos de orden finito $n \geq 2$. Esto pues si $n \geq 1$ y $x \in \mathbb{R}$ con

$$nx = 0,$$

entonces $x = 0$ y sabemos que el orden del elemento neutro es 1. Es decir, en $(\mathbb{R}, +)$

Se tiene que

- $o(0) = 1$
- $o(x) = \infty$ para todo $x \in \mathbb{R}$ con $x \neq 0$.

⑤ En $(\mathbb{Z}_3, +)$ note que $\mathbb{Z}_3 = \{[0], [1], [2]\}$ y

en particular:

- $o([0]) = 1$
- $o([1]) = 3$ pues $[1] \neq [0]$

$$2[1] = [1] + [1] = [2] \neq [0]$$

$$3[1] = [1] + [1] + [1] = [3] = [0]$$

- $o([2]) = 3$.

⑥ Más generalmente, en $(\mathbb{Z}_n, +)$ se tiene que

$o([1]) = n$.

(7) Considere $G = GL_2(\mathbb{R}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \middle| \begin{array}{l} a,b,c,d \in \mathbb{R} \text{ y la} \\ \text{matriz es invertible} \end{array} \right\}$

con la operación binaria de multiplicación de matrices.

Note que acá el neutro es $\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ y $o\left(\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\right) = 1$.

También $o\left(\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}\right) = 2$ pues

$$\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}^2 = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \cdot \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.$$

Por otro lado, en este grupo también existen elementos de orden infinito. Por ejemplo si $T = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, entonces

$$T^2 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^2 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix}$$

$$T^3 = T^2 \cdot T = \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 3 \\ 0 & 1 \end{bmatrix}$$

y más generalmente, para $n \geq 1$ se tiene

$$T^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}.$$

Esto implica que $T^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix} \neq \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ para todo $n \geq 1$, por lo tanto $o(T) = o\left(\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\right) = \infty$. Δ

El siguiente teorema nos da algunas propiedades básicas del orden de un elemento en un grupo.

Teorema

Sea G un grupo y sea $x \in G$. Entonces:

(i) $o(x) = o(x^{-1})$.

(ii) Si $o(x) = n$ y $x^m = e$, entonces $n \mid m$.

(iii) Si $o(x) = n$ y $d = mcd(m,n)$, entonces

$$o(x^m) = \frac{n}{d} = \frac{n}{mcd(m,n)}.$$

Definición (Grupos cíclicos)

Un grupo G es llamado cíclico si existe un elemento $x \in G$ tal que $G = \{x^n \mid n \in \mathbb{Z}\}$.

En tal caso x es llamado un generador de G y se suele escribir $G = \langle x \rangle$.

- En el caso aditivo, $G = \{nx \mid n \in \mathbb{Z}\}$.
- Se dice en tales casos que $G = \langle x \rangle$ es cíclico, generado por x.

Ejemplos

① El grupo aditivo $(\mathbb{Z}_n, +)$ es cíclico, generado por $[1]$ pues sabemos que $\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}$ y

$$[0] = 0[1]$$

$$[1] = 1[1]$$

$$[2] = 2[1] = [1] + [1]$$

$$\vdots$$

$$[n-1] = (n-1)[1] = \underbrace{[1] + [1] + \cdots + [1]}_{n-1 \text{ Sumandos}}.$$

Es decir, $\mathbb{Z}_n = \langle [1]_n \rangle$.

También se puede ver que $\mathbb{Z}_n = \langle [-1]_n \rangle = \langle [n-1]_n \rangle$.

② El grupo aditivo $(\mathbb{Z}, +)$ es cíclico y de hecho

$$\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle.$$

En este caso 1 y -1 son los únicos posibles generadores.

③ No todo grupo es cíclico. Por ejemplo el grupo aditivo $(\mathbb{Q}, +)$ no es cíclico. Para ver por qué, note que si $q = \frac{a}{b}$ es un número racional $\neq 0$, entonces no todo número racional pertenece al

conjunto de sus múltiplos

$$\langle q \rangle = \{ nq \mid n \in \mathbb{Z} \}$$

$$= \left\{ n \cdot \frac{a}{b} \mid n \in \mathbb{Z} \right\}.$$

Por ejemplo, el número racional $\frac{q}{2} = \frac{a}{2b}$ no pertenece a este conjunto. Δ

Ejercicio

Demuestre que $(\mathbb{Q}^*, \cdot)$ no es un grupo cíclico. Δ

Al trabajar con grupos cíclicos, el siguiente teorema es importante.

Teorema

Sea G un grupo y $x \in G$. Si $o(x) = \infty$, entonces $x^j \neq x^k$ para todo $k, j \in \mathbb{Z}$ con $k \neq j$ y consecuentemente G es un grupo infinito pues todas las potencias

de x son elementos distintos.

Si $o(x)=n$, entonces $x^j = x^k \Leftrightarrow j \equiv k \pmod{n}$

y consecuentemente los elementos distintos de $\langle x \rangle$ son $e, x, x^2, \ldots, x^{n-1}$, es decir,

$$\langle x \rangle = \{ e, x, x^2, \ldots, x^{n-1} \}.$$

Demostración

- **Caso $o(x)=\infty$:** Sean $k, j \in \mathbb{Z}$ con $k \neq j$.

Digamos que $j > k$. Luego, si se tuviera $x^j = x^k$, multiplicando por x^{-k} se obtendría

$$x^j x^{-k} = x^k x^{-k},$$

es decir,

$$x^{j-k} = e.$$

Como $j > k$, entonces $j-k > 0$ es un entero

positivo, pero esto diría que $o(x)$ es finito y esto es una contradicción pues asumimos $o(x) = \infty$. Por lo tanto $x^j \neq x^k$ y esto implica que G es un grupo infinito pues todas las potencias de x son elementos distintos en G.

- Caso $o(x) = n$: Sean $j, k \in \mathbb{Z}$. Entonces

$$x^j = x^k \iff x^{j-k} = e$$

$$\iff n \mid j-k$$

$$\iff j \equiv k \pmod{n}$$

Por lo tanto como los enteros $0, 1, 2, \ldots, n-1$ son mutuamente incongruentes módulo n, las potencias $e, x, x^2, \ldots, x^{n-1}$ son todas distintas y en efecto

$$\langle x \rangle = \{e, x, x^2, \ldots, x^{n-1}\}. \square$$

Definición

El orden de un grupo G, denotado por $|G|$, es su cardinalidad, es decir, en el caso finito, el número de elementos de G.

Corolario

Si $G = \langle x \rangle$, entonces $|G| = o(x)$.

Teorema

Si G es un grupo cíclico, entonces G es abeliano. En otras palabras, todo grupo cíclico es abeliano.

Demostración

Sea $G = \langle x \rangle$ y sean $a, b \in G$. Entonces existen $n, m \in \mathbb{Z}$ tales que $a = x^n$ y $b = x^m$. Luego,

$$ab = x^n x^m = x^{n+m} = x^{m+n} = x^m x^n = ba,$$

es decir, la multiplicación en G es conmutativa. $\square$

Nota

- Si bien todo grupo cíclico es abeliano, el inverso de esto no es cierto, es decir, existen grupos abelianos que no son cíclicos. Por ejemplo, como vimos $(\mathbb{Q}, +)$ no es cíclico pero sí es abeliano. Δ