# Grupos, Anillos y Cuerpos:

## Apuntes para Estudiantes Universitarios

M. Ángeles Gómez Flechoso

ISBN: 978-84-695-3588-2

# Índice general

# Capítulo 1

# Introducción

## 1.1. Conjuntos

**Definición:** Un conjunto es una colección de elementos en la que *no* se repite ninguno.

**Notación:** Los conjuntos se suelen denotar con letras mayúsculas y sus elementos con letras minúsculas.

***Ejemplos:*** $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Z}^+$,$\mathbb{Q}$, $\mathbb{R}$,...

**Igualdad entre conjuntos:** Dos conjuntos $S$ y $T$ son *iguales* si y sólo si $\forall s \,/\, s \in S \Longrightarrow s \in T$ y $\forall t \,/\, t \in T \Longrightarrow t \in S$

**Subconjuntos:**Dados dos conjuntos $S$ y $T$, se dice que $S$ es *subconjunto* de $T$ y se denota por $S \subset T$, si y sólo si
$\forall s \,/\, s \in S \Longrightarrow s \in T$

*Proposición:* Dados dos conjuntos $S$ y $T$, $S = T \Longleftrightarrow S \subset T$ y $T \subset S$

*Demostración:*
$$\text{(a) } S = T \Rightarrow \ \forall s \,/\, s \in S \Longrightarrow s \in T \Rightarrow S \subset T \ \text{ y } \ \forall t \,/\, t \in T \Longrightarrow t \in S \Rightarrow T \subset S$$
$$\left.\begin{array}{l}\text{(b) } S \subset T \Rightarrow \forall s \,/\, s \in S,\ s \in T \\ \quad T \subset S \Rightarrow \forall t \,/\, t \in T,\ t \in S\end{array}\right\} \Rightarrow S = T$$

**Unión de conjuntos:** Dados dos conjuntos $S$ y $T$, se define la *unión* de los conjuntos $S$

y $T$ y se denota por $S \cup T$ al siguiente conjunto:

$$S \cup T = \{x \,/\, x \in S \;\text{ ó }\; x \in T\}$$

***Ejemplo:***
$S = \{1, 5, 2, 6\},\ T = \{3, 8, 5, 9\} \Rightarrow S \cup T = \{1, 5, 2, 6, 3, 8, 9\}$
*Unión de varios conjuntos:* $S \cup T \cup V... = \{x \,/\, x \in S$ ó $x \in T$ ó $\; x \in V...\}$

**Intersección de conjuntos:** Dados dos conjuntos $S$ y $T$, se define la *intersección* de los conjuntos $S$ y $T$ y se denota por $S \cap T$ al siguiente conjunto:

$$S \cap T = \{x \,/\, x \in S \;\text{ y }\; x \in T\}$$

Si $S \cap T =$ , entonces se dice que $S$ y $T$ son conjuntos *disjuntos.*

***Ejemplo:***
$S = \{1, 5, 2, 6\},\ T = \{3, 8, 5, 9\} \Rightarrow S \cap T = \{5\}$

*Intersección de varios conjuntos:* $S \cap T \cap V... = \{x \,/\, x \in S$ y $x \in T$ y $\; x \in V...\}$

**Diferencia de conjuntos:** Dados dos conjuntos $S$ y $T$ tales que $S \subset T$, se define la *diferencia* de los conjuntos $S$ y $T$ y se denota por $T - S$ al siguiente conjunto:

$$T - S = \{x \,/\, x \in T \;\text{ y }\; x \notin S\}$$

***Ejemplo:***
$S = \{5\},\ T = \{3, 8, 5, 9\} \Rightarrow T - S = \{3, 8, 9\}$
Como $S \subset T \Rightarrow S \cup T = T$ y $S \cap T = S$

*Ejercicio:* Si $S \subset T$, demostrar que $\; T - (T - S) = S$

(a) $T - (T - S) \subset S$ :
si $x \in T - (T - S) \Rightarrow x \in T$ y $x \notin T - S \Rightarrow x \in T$ y $x \in S \Rightarrow x \in S \Rightarrow T - (T - S) \subset S$

(b) $S \subset T - (T - S)$ :
si $x \in S \Rightarrow x \in T \Rightarrow x \in T$ y $x \notin T - S \Rightarrow x \in T - (T - S) \Rightarrow S \subset T - (T - S)$

## 1.2. Productos cartesianos

Un producto cartesiano es un *par ordenado*. Por lo tanto, dados dos conjuntos $S$ y $T$, definimos el *producto cartesiano* de $S$ y $T$ y denotamos por $S \times T$ al conjunto definido de la siguiente manera:

$$S \times T = \{x \ / \ x = (s,t),\ s \in S,\ t \in T\}$$

En general, $S \times T \neq T \times S$
Además, se denota $S^2 = S \times S$
Si $S = \ \Rightarrow S \times T = T$

*Ejercicios:*

1. Dados $S = \{1,7,5,3\}$ y $T = \{2,4,5,6\}$, calcular:
   - $S \times T$
   - $T \times S$
   - ¿$T \times S = S \times T$?
   - ¿$(S \times T) \times S = S \times (T \times S)$?
2. Demostrar que: $S \times T = T \times S \iff S = T$ ó $S = \ $ ó $T = $
3. Demostrar que: $S \times T = S \times U \iff T = U$

## 1.3. Relaciones de equivalencia

Una relación de equivalencia es un *subconjunto de un producto cartesiano con una serie de propiedades*. Por lo tanto, sea $X \neq \ $ y $\mathcal{R} \subset X^2 \Rightarrow \mathcal{R}$ es una *relación de equivalencia* en $X$ si cumple las siguientes propiedades:

- *Propiedad reflexiva:* $(x,x) \in \mathcal{R}, \forall x \in X$
- *Propiedad simétrica:* $(x,y) \in \mathcal{R} \Rightarrow (y,x) \in \mathcal{R}$
- *Propiedad transitiva:* $(x,y) \in \mathcal{R}, (y,z) \in \mathcal{R} \Rightarrow (x,z) \in \mathcal{R}$

*Notación:* $(x, y) \in \mathcal{R}$ también se escribe $x\mathcal{R}y$

***Ejemplos:***

1. $X = \{1, 2, 3\} \Rightarrow \mathcal{R} = \{(1, 1), (2, 2), (3, 3), (1, 2), (2, 1)\}$ es relación de equivalencia en $X$
2. $\mathcal{R} = \{p \ / \ p = (x, y) \in \mathbb{Z}^+ \times \mathbb{Z}^+ \text{ y } x < y\}$ no es una relación de equivalencia ya que no cumple la propiedad reflexiva.

*Ejercicio:*
Sea $\mathcal{R} = \{p \ / \ p = (x, y) \in \mathbb{Z}^2, x - y \text{ divisible por } 3\}$, demostrar que $\mathcal{R}$ es una relación de equivalencia.

i. $x\mathcal{R}x$ ya que $x - x = 0$ es divisible por 3

ii. $x\mathcal{R}y \Rightarrow y\mathcal{R}x$ ya que si $x - y$ es divisible por $3 \Rightarrow y - x$ también es divisible por 3

iii. $x\mathcal{R}y, y\mathcal{R}z \Rightarrow xz$ ya que si $x - y$ e $y - z$ son divisibles por 3, su suma también lo será, por lo tanto $x - z = (x - y) + (y - z)$ es divisible por 3

Por lo tanto $\mathcal{R}$ es una relación de equivalencia.

**Partición de un conjunto:** La *partición de un conjunto* $X$ es una descomposición del conjunto $X$ en subconjuntos disjuntos tales que cada uno de los elementos de $X$ pertenece a alguno de los subconjuntos.

***Ejemplo:***
Sea $X = \{1, 2, 3, 4, 5\}$
$(\{1\}, \{3, 5\}, \{2, 4\})$ sí es una partición de $X$
$(\{1, 2\}, \{2, 3, 4\}, \{5\})$ no es una partición de $X$ ya que el 2 aparece en dos subconjuntos
$(\{1, 3\}, \{4, 5\})$ tampoco es una partición de $X$ ya que el elemento 2 no aparece en ninguno de los subconjuntos

**$\mathcal{R}$-clase de equivalencia:** Una *$\mathcal{R}$-clase de equivalencia* de un conjunto $X$ es un conjunto de todos los elementos $y \in X$ tales que están relacionados con otro elemento $x \in X$ mediante una relación de equivalencia $\mathcal{R}$. En este caso esta $\mathcal{R}$-clase de equivalencia se denotaría por:

$$x\mathcal{R} = \{y \ / \ y \in X, (x, y) \in \mathcal{R}\}$$

Las $\mathcal{R}$-clases de equivalencia de un conjunto $X$ forman una partición de dicho conjunto obtenida a partir de una relación de equivalencia $\mathcal{R}$

***Ejemplo:***
Sea $X = \{1, 2, 3\}$ y $\mathcal{R} = \{(1,1), (2,2), (3,3), (1,2), (2,1)\}$, entonces $1\mathcal{R} = \{1, 2\}$, $2\mathcal{R} = \{1, 2\}, 3\mathcal{R} = \{3\}$, por lo tanto tenemos la partición formada por $(1\mathcal{R}, 3\mathcal{R})$, ya que $1\mathcal{R} = 2\mathcal{R}$

*Observaciones:*

1. Las $\mathcal{R}$-clases de equivalencia de un conjunto o bien son disjuntas o bien son iguales
2. Podemos construir una partición con las $\mathcal{R}$-clases de equivalencia

*Teorema:* Sea un conjunto $X \neq$ y $\mathcal{R}$ una relación de equivalencia en $X$, entonces

i. si $x\mathcal{R} \cap x'\mathcal{R} \neq \Rightarrow x\mathcal{R} = x'\mathcal{R}$, o sea, las $\mathcal{R}$-clases de equivalencia son disjuntas dos a dos

ii. $x \in x\mathcal{R}, \forall x \in X$, o sea, cada elemento está en al menos una $\mathcal{R}$-clase de equivalencia

Por lo tanto, las $\mathcal{R}$-clases de equivalencia forman una partición.

*Demostración:*

i. Supongamos que $x\mathcal{R} \cap x'\mathcal{R} \neq \Rightarrow \exists y \in x\mathcal{R} \ / \ y \in x'\mathcal{R} \Rightarrow (x, y) \in \mathcal{R}$ y $(x', y) \in \mathcal{R} \Rightarrow$(por la prop. transitiva) $(x, x') \in \mathcal{R}$

   Por otro lado, $\forall z \ / \ z \in x'\mathcal{R} \Rightarrow (x', z) \in \mathcal{R}$ y como $(x, x') \in \mathcal{R} \Rightarrow (x, z) \in \mathcal{R} \Rightarrow z \in x\mathcal{R} \Rightarrow x'\mathcal{R} \subset x\mathcal{R}$

   Igual se demuestra que $x\mathcal{R} \subset x'\mathcal{R}$, por lo tanto, $x\mathcal{R} = x'\mathcal{R}$

ii. Decir que $x \in x\mathcal{R}$ es lo mismo que decir que $(x, x) \in \mathcal{R}$ y esto se cumple siempre por la propiedad reflexiva

**Conjunto cociente:** Se denomina *conjunto cociente* $X/\mathcal{R}$ al conjunto de las $\mathcal{R}$-clases de equivalencia en un conjunto $X$ según la relación de equivalencia $\mathcal{R}$.

***Ejemplo:***
Sean el conjunto $X = \{1, 2, 3\}$ y la relación de equivalencia $\mathcal{R} = \{(1,1), (2,2), (3,3), (1,2), (2,1)\}$, el conjunto cociente viene dado por $X/\mathcal{R} = \{\{1, 2\}, \{3\}\} = \{1\mathcal{R}, 3\mathcal{R}\}$ ya que $1\mathcal{R} = 2\mathcal{R}$

*Ejercicios:*

1. Demostrar que $\mathcal{R} = \{(0,0),(1,1),(2,2),(3,3),(0,2),(1,3),(2,0),(3,1)\}$ es una relación de equivalencia de $X = \{0,1,2,3\}$

2. Encontrar las $\mathcal{R}$-clases de equivalencia del conjunto $X$ del ejercicio anterior según la relación de equivalencia $\mathcal{R}$ descrita

3. Definir el conjunto $X/\mathcal{R}$ del ejercicio anterior

4. Sea $\mathcal{A} = \{p \ / \ p = (x,y) \in \mathbb{Z}^2 \ \text{ tal que } (x-y) \text{ es divisible por } 3\}$. Probar que $\mathcal{A}$ es una relación de equivalencia en $\mathbb{Z}$ y encontrar las $\mathcal{A}$-clases de equivalencia. El conjunto cociente definido por esta relación de equivalencia se denotará por $\mathbb{Z}_3$, ¿cual es dicho conjunto cociente?

5. Demostar que $\mathcal{R} = S \times S$ es una relación de equivalencia en $S$. ¿Cuáles son las $\mathcal{R}$-clases de equivalencia?

## 1.4. Aplicaciones

**Correspondencia:** Una *correspondencia* entre dos conjuntos $A$ y $B$ es una regla que asocia elementos de $A$ con elementos de $B$.

Una correspondencia entre $A$ y $B$ puede definirse como cualquier subconjunto de $A \times B$

**Aplicación:** Una *aplicación* entre dos conjuntos $A$ y $B$ no vacíos es una correspondencia tal que a cada elemento de $A$ se le asocia un elemento de $B$ y sólo uno.

$$\begin{array}{rl} \alpha: & A \longrightarrow B \\ & a \longrightarrow b \end{array}$$

Al conjunto $A$ se le denomina *dominio* y al conjunto $B$ se le denomina *codominio*. El elemento $b$ tal que $b = \alpha(a)$ se le denomina *imagen* de $a$ y al elemento $a$ se le denomina contraimagen de $b$.

El subconjunto de elementos del codominio que son imagen de algún elemento del dominio es el *recorrido* de la aplicación, esto es, el recorrido es el siguiente conjunto: $\alpha(A) = \{\alpha(a) \ / \ a \in A\}$

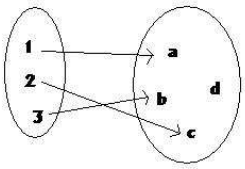
Un subconjunto $\alpha$ de $A \times B$ es una aplicación de $A$ en $B$ si y sólo si

i. $\forall a \in A \Rightarrow \exists\, b \in B \,/\, (a,b) \in \alpha$

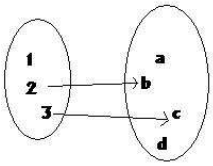
ii. $(a,b) \in \alpha$ y $(a,b') \in \alpha \Rightarrow b = b'$

***Ejemplos:***

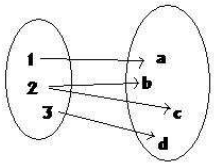
1. Sean $A = \{1,2,3\}$ y $B = \{a,b,c,d\}$



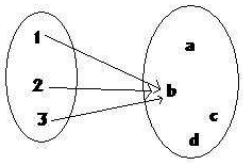

Sí es aplicación




No, todos los elementos del dominio deben tener imagen




No, la imagen debe ser única




Sí

2. $A = \{(x,y) \,/\, x \in \mathbb{R},\ y \in (-\pi,\pi],\ y = \arcsin(x)\}$

**Igualdad de aplicaciones:** Sean $\alpha : A \longrightarrow B$ y $\beta : S \longrightarrow T$ dos aplicaciones, se dice que $\alpha$ y $\beta$ son *iguales*, $\alpha = \beta$, si y sólo si $S = A$, $T = B$ y $\forall a \in A \Rightarrow \alpha(a) = \beta(a)$

**Tipos de aplicaciones:**

- *Sobreyectiva o suprayectiva*: Todo elemento del codominio tiene al menos una contraimagen, por lo tanto, dada la aplicación $\alpha : A \longrightarrow B$, tendremos que $\forall b \in B\ \exists a \in A \,/\, \alpha(a) = b$
- *Inyectiva*: A elementos diferentes del domino le corresponden imagenes diferentes, por lo tanto, dada la aplicación $\alpha : A \longrightarrow B$, tendremos que $\forall a,b \in A \,/\, \alpha(a) = \alpha(b) \Rightarrow a = b$
- *Biyectiva*: Es inyectiva y suprayectiva a la vez.

***Ejemplos:***

1. $S = \mathbb{R},\ T = [0,1]$

$$\begin{array}{rcl} \alpha: & S & \longrightarrow T \\ & s & \longrightarrow \sin^2(s) \end{array}$$

Es una aplicación suprayectiva, pero no es inyectiva ya que si $\sin^2(s) = \sin^2(t) \not\Rightarrow s = t$

2. $S = \mathbb{R},\ T = [0, 2]$

$$\begin{array}{rl} \alpha: & S \longrightarrow T \\ & s \longrightarrow \sin^2(s) \end{array}$$

Es una aplicación que no es ni inyectiva ni suprayectiva

3. $S = \mathbb{R}^2,\ T = \mathbb{R}^2$

$$\begin{array}{rl} \alpha: & S \longrightarrow T \\ & (x, y) \longrightarrow (x^2 - y^2, 2xy) \end{array}$$

Es una aplicación que es suprayectiva, ya que un sistema de ecuaciones de la forma $\left.\begin{array}{ll} x^2 - y^2 & = a \\ 2xy & = b \end{array}\right\}$ tiene solución para cualquier par de valores $a$ y $b$ reales.

Sin embargo la aplicación no es inyectiva, dado que si $\left.\begin{array}{ll} x^2 - y^2 & = x'^2 - y'^2 \\ 2xy & = 2x'y' \end{array}\right\} \not\Rightarrow$ $\left.\begin{array}{l} x = x' \\ y = y' \end{array}\right\}$

**Restricción de una aplicación:**

Sea una aplicación $\alpha : S \longrightarrow T$ y sea $S' \subset S$, definimos $\alpha$ *restringida a* $S'$, y denotamos por $\alpha|_{S'} : S' \longrightarrow T$, a la aplicación que cumple que $\alpha|_{S'} : s \longrightarrow \alpha(s)\ \forall s \in S'$

**Composición de aplicaciones:**

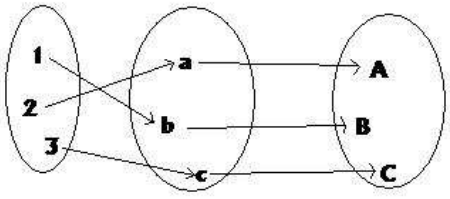
Sean dos aplicaciones $\alpha : S \longrightarrow T$ y $\beta : T \longrightarrow V$, la *composición* de $\alpha$ y $\beta$ es la aplicación

$$\begin{array}{rl} \beta \circ \alpha: & S \longrightarrow V \\ & s \longrightarrow \beta(\alpha(s)) \end{array}$$

***Ejemplo:***

$S = \{1, 2, 3\},\ T = \{a, b, c\},\ V = \{A, B, C\}$

$$\left.\begin{array}{ll} \alpha(1) = b, & \beta(a) = A \\ \alpha(2) = a, & \beta(b) = B \\ \alpha(3) = c, & \beta(c) = C \end{array}\right\} \begin{array}{l} (\beta \circ \alpha)(1) = B \\ (\beta \circ \alpha)(2) = A \\ (\beta \circ \alpha)(3) = C \end{array}$$



*¡Atención!* $\alpha \circ \beta \neq \beta \circ \alpha$, dado que no coinciden ni dominios ni codominios, de hecho no podemos calcular $\alpha \circ \beta$ dado que el codominio de $\beta$ no coincide con el dominio de $\alpha$

**Operaciones binarias:**
Sea un conjunto $S \neq$ , una *operación binaria* es una aplicación de $S \times S$ en $S$ y escribiremos

$$\begin{array}{rl} \cdot : & S \times S \longrightarrow S \\ & (x, y) \longrightarrow x \cdot y \end{array}$$

***Ejemplo:***
En $\mathbb{Z}^+$:
$(i, j) \longrightarrow i^2$ sí es una operación binaria
$(i, j) \longrightarrow i - j$ no es una operación binaria, ya que, por ejemplo, $2 - 3 = -1 \notin \mathbb{Z}^+$
$(i, j) \longrightarrow i/j$ no es una operación binaria, ya que, por ejemplo, $2/3 \notin \mathbb{Z}^+$

*Propiedades de las operaciones binarias:* una operación binaria definida en un conjunto $S$ puede tener las siguientes propiedades:

- Asociativa: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
- Conmutativa: $a \cdot b = b \cdot a$
- Elemento neutro por la izquierda: $\exists e \in S \ / \ e \cdot a = a \ \forall a \in S$
- Elemento neutro por la derecha: $\exists e \in S \ / \ a \cdot e = a \ \forall a \in S$

Si existe elemento neutro por la derecha y por la izquierda y ambos son iguales podemos tener:

- Elemento inverso por la izquierda: $\forall a \in S \ \exists b \in S \ / \ b \cdot a = e$
- Elemento inverso por la derecha: $\forall a \in S \ \exists b \in S \ / \ a \cdot b = e$

Si el elemento inverso por la izquierda y por la derecha es el mismo, se denomina inverso de $a$ y se simboliza por $a^{-1}$

*Teorema:* Si una operación es asociativa y el inverso por la derecha es igual al inverso por la izquierda, entonces el inverso es único.

*Demostración:*

Sean $b$ y $c$ inversos de $a$, tendremos que $c = c \cdot e = c \cdot (a \cdot b) = (c \cdot a) \cdot b = e \cdot b = b$

*Tabla de multiplicar:* La mejor manera de representar una operación binaria es mediante una tabla de multiplicar

***Ejemplo:***

Sea $S = \{1, 2, 3\}$, definimos la operación

$1 \cdot 1 = 2, \quad 1 \cdot 2 = 1, \quad 1 \cdot 3 = 3$

$2 \cdot 1 = 1, \quad 2 \cdot 2 = 2, \quad 2 \cdot 3 = 1$

$3 \cdot 1 = 1, \quad 3 \cdot 2 = 3, \quad 3 \cdot 3 = 2$

Podemos representar dicha operación de la siguiente forma:

$2^o elemento$

| $1^{er}$ *elemento* · | **1** | **2** | **3** |
|---|---|---|---|
| **1** | 2 | 1 | 3 |
| **2** | 1 | 2 | 1 |
| **3** | 1 | 3 | 2 |

# Capítulo 2

# Grupos

## 2.1. Estructura de grupo

***Ejemplo:*** Rotaciones de un cuadrado:

r1:

$$\boxed{\begin{matrix}1&2\\4&3\end{matrix}} \xrightarrow[\text{giro de } 90^\circ]{} \boxed{\begin{matrix}2&3\\1&4\end{matrix}} \xrightarrow[\text{giro de } 90^\circ]{} \boxed{\begin{matrix}3&4\\2&1\end{matrix}} \xrightarrow[\text{giro de } 90^\circ]{} \boxed{\begin{matrix}4&1\\3&2\end{matrix}} \xrightarrow[\text{giro de } 90^\circ]{} \boxed{\begin{matrix}1&2\\4&3\end{matrix}}$$

r2:

$$\boxed{\begin{matrix}1&2\\4&3\end{matrix}} \xrightarrow[\text{giro de } 180^\circ]{} \boxed{\begin{matrix}3&4\\2&1\end{matrix}} \xrightarrow[\text{giro de } 180^\circ]{} \boxed{\begin{matrix}1&2\\4&3\end{matrix}}$$

r3:

$$\boxed{\begin{matrix}1&2\\4&3\end{matrix}} \xrightarrow[\text{giro de } 270^\circ]{} \boxed{\begin{matrix}4&1\\3&2\end{matrix}} \xrightarrow[\text{giro de } 270^\circ]{} \boxed{\begin{matrix}3&4\\2&1\end{matrix}} \xrightarrow[\text{giro de } 270^\circ]{} \boxed{\begin{matrix}2&3\\1&4\end{matrix}} \xrightarrow[\text{giro de } 270^\circ]{} \boxed{\begin{matrix}1&2\\4&3\end{matrix}}$$

| $\cdot$ | I | r1 | r2 | r3 |
|---|---|---|---|---|
| I | I | r1 | r2 | r3 |
| r1 | r1 | r2 | r3 | I |
| r2 | r2 | r3 | I | r1 |
| r3 | r3 | I | r1 | r2 |

### 2.1.1. Definición de grupo

Un *grupo* es un conjunto $G \neq$ en que está definida una operación binaria, $\circ : G \times G \longrightarrow G$, con las siguientes propiedades:

i. **Cerrada o uniforme:** $\forall a, b \in G \Rightarrow a \circ b \in G$

ii. **Asociativa:** $\forall a, b, c \in G \Rightarrow (a \circ b) \circ c = a \circ (b \circ c)$

iii. **Elemento neutro:** $\exists e \in G \ / \ \forall a \in G,\ a \circ e = e \circ a = a$

iv. **Elemento inverso:** $\forall a \in G,\ \exists a^{-1} \in G \ / \ a \circ a^{-1} = a^{-1} \circ a = e$

***Ejemplo:***
$S_3$ definido como el *grupo de permutaciones de tres objetos* $\{1, 2, 3\}$:
$e = \left\{ \begin{array}{ccc} 1 & 2 & 3 \\ 1 & 2 & 3 \end{array} \right\}, \sigma_+ = \left\{ \begin{array}{ccc} 1 & 2 & 3 \\ 3 & 1 & 2 \end{array} \right\}, \sigma_- = \left\{ \begin{array}{ccc} 1 & 2 & 3 \\ 2 & 3 & 1 \end{array} \right\},$
$\tau_1 = \left\{ \begin{array}{ccc} 1 & 2 & 3 \\ 1 & 3 & 2 \end{array} \right\}, \tau_2 = \left\{ \begin{array}{ccc} 1 & 2 & 3 \\ 3 & 2 & 1 \end{array} \right\}, \tau_3 = \left\{ \begin{array}{ccc} 1 & 2 & 3 \\ 2 & 1 & 3 \end{array} \right\}$
La tabla de multiplicar de dicho conjunto con la operación permutación es:

| $\circ$ | $e$ | $\sigma_+$ | $\sigma_-$ | $\tau_1$ | $\tau_2$ | $\tau_3$ |
|---|---|---|---|---|---|---|
| $e$ | $e$ | $\sigma_+$ | $\sigma_-$ | $\tau_1$ | $\tau_2$ | $\tau_3$ |
| $\sigma_+$ | $\sigma_+$ | $\sigma_-$ | $e$ | $\tau_2$ | $\tau_3$ | $\tau_1$ |
| $\sigma_-$ | $\sigma_-$ | $e$ | $\sigma_+$ | $\tau_3$ | $\tau_1$ | $\tau_2$ |
| $\tau_1$ | $\tau_1$ | $\tau_3$ | $\tau_2$ | $e$ | $\sigma_-$ | $\sigma_+$ |
| $\tau_2$ | $\tau_2$ | $\tau_1$ | $\tau_3$ | $\sigma_+$ | $e$ | $\sigma_-$ |
| $\tau_3$ | $\tau_3$ | $\tau_2$ | $\tau_1$ | $\sigma_-$ | $\sigma_+$ | $e$ |

Vamos a comprobar que cumple las propiedades de grupo:

i. El producto de dos permutaciones es otra permutación (operación cerrada)

ii. Cumple la propiedad asociativa

iii. Existe el elemento neutro, que es $e$

iv. Para todas las permutaciones existe otra permutación de modo que al operar ambas nos da el elemento neutro, por ejemplo,

$\sigma_+^{-1} = \sigma_-, \tau_1^{-1} = \tau_1$

Observaciones: la operación definida no es conmutativa

***Ejemplos:***

Vamos a ver más ejemplos interesantes:

- Dado el conjunto $X \neq$ , tomamos el conjunto $Biy(X) = \{\alpha \ / \ \alpha$ es biyección de $X$ en $X\}$

  Podemos formar un grupo con el conjunto $Biy(X)$ y la operación composición de aplicaciones: $(Biy(X), \circ)$

  i. Operación interna:
  $f, g \in Biy(X) \Rightarrow f \circ g \in Biy(X)$ (visto en ejercicio 8 del tema 1)

  ii. Propiedad asociativa:
  $f, g, h \in Biy(X) \Rightarrow (f \circ g) \circ h = f \circ (g \circ h)$, ya que $((f \circ g) \circ h)(x) = (f \circ g)(h(x)) = f(g(h(x))) = f((g \circ h)(x)) = (f \circ (g \circ h))(x)$

  iii. Elemento neutro:
  Sea la aplicación $i : X \longrightarrow X$ tal que $\forall x \in X,\ i(x) = x$, por lo tanto
  $\left.\begin{array}{l}(i \circ f)(x) = i(f(x)) = f(x) \\ (f \circ i)(x) = f(i(x)) = f(x)\end{array}\right\} \Rightarrow i$ es el elemento neutro

  iv. Elemento inverso:
  Si $f : X \longrightarrow X$, definimos $f^{-1} : X \longrightarrow X$, de modo que si $f(x) = y \Rightarrow f^{\cdot -1}(y) = x$. Tendremos que $f^{-1}$ es una aplicación biyectiva dado que $f$ también lo es.
  $\left.\begin{array}{l}(f^{-1} \circ f)(x) = f^{-1}(f(x)) = f^{-1}(y) = x = i(x) \\ (f \circ f^{-1})(y) = f(f^{-1}(y)) = f(x) = y = i(y)\end{array}\right\} \Rightarrow f^{-1}$ es el elemento inverso de $f$

- Definimos el conjunto de las matrices de orden $n$ con determinante distinto de 0, con la operación producto de matrices: $GL_n(\mathbb{R}) = (\mathcal{M}_{n\times n}(\mathbb{R}), \cdot)$

  i. Operación interna: el producto de dos matrices de orden $n$ con determinante distinto de 0 es otra matriz de orden $n$ con determinante distinto de 0

  ii. Propiedad asociativa: el producto de matrices es asociativo

  iii. Elemento neutro: la matriz identidad de orden $n$ es una matriz con determinante no nulo que es el elemento neutro del producto

  iv. Elemento inverso: para todas las matrices de orden $n$ con determinante no nulo existe otra matriz de orden $n$ con determinante no nulo, donde el producto de ambas es la matriz identidad.

- Otros ejemplos de grupos son $(\mathbb{Z}, +), (\mathbb{Q}, +), (\mathbb{R}, +), (\mathbb{C}, +), (\mathbb{Q}-\{0\}, \cdot), (\mathbb{R}-\{0\}, \cdot), (\mathbb{Q}^+, \cdot), (\mathbb{R}^+, \cdot), (\mathbb{C} - \{0\}, \cdot), ...$

### 2.1.2. Propiedades

1. El elemento neutro es único.

   *Demostración:*

   Sean $e$ y $e'$ elementos neutros $\Rightarrow e =$*(como $e'$ es elemento neutro)*$= e \circ e' =$*(como $e$ es elemento neutro)*$= e'$

2. El inverso de un elemento es único: $\forall a \in G \Longrightarrow a^{-1}$ es único

   *Demostración:*

   Sean $b$ y $c$ inversos de $a \Rightarrow b = b \circ e =$*(como $c$ es el inverso de $a$)*$= b \circ (a \circ c) = (b \circ a) \circ c =$*(como $b$ es el inverso de $a$)*$= c$

3. Se puede simplificar: $\forall a, b, c \in G \Rightarrow \begin{cases} \text{i. si } a \circ b = a \circ c \Rightarrow b = c \\ \text{ii. si } a \circ b = c \circ b \Rightarrow a = c \end{cases}$

   *Demostración:*

   Sea $a \circ b = a \circ c \Rightarrow a^{-1} \circ (a \circ b) = a^{-1} \circ (a \circ c) \Rightarrow (a^{-1} \circ a) \circ b = (a^{-1} \circ a) \circ c \Rightarrow b = c$

4. Asociatividad generalizada: los productos que se obtienen al variar las formas de agrupar $n$ elementos conservando el orden son iguales.

   *Demostración:*

   Se puede demostrar por inducción partiendo de la asociatividad de tres elementos.

5. El inverso de un producto es el producto de los inversos permutando el orden: $(a_1 \circ \cdots \circ a_n)^{-1} = a_n^{-1} \circ \cdots \circ a_1^{-1}$

   *Demostración:*

   Sea $(a_1 \circ a_2)^{-1} = a_3^{-1} \Rightarrow (a_1 \circ a_2)^{-1} \circ a_3 = e \Rightarrow (a_1 \circ a_2)^{-1} \circ (a_1 \circ a_2) = e \Rightarrow (a_1 \circ a_2)^{-1} \circ a_1 \circ (a_2 \circ a_2^{-1}) = a_2^{-1} \Rightarrow (a_1 \circ a_2)^{-1} \circ a_1 = a_2^{-1} \Rightarrow$

   $(a_1 \circ a_2)^{-1} \circ (a_1 \circ a_1^{-1}) = a_2^{-1} \circ a_1^{-1} \Rightarrow (a_1 \circ a_2)^{-1} = a_2^{-1} \circ a_1^{-1}$

   Por inducción se puede extender la demostración a la inversa del producto de $n$ elementos.

### 2.1.3. Grupo abeliano (o conmutativo)

Un grupo $G$ es *abeliano* si $\forall a, b \in G \Rightarrow a \circ b = b \circ a$

***Ejemplo:*** $(\mathbb{Z}, +), (\mathbb{R}, +), (\mathbb{R} - \{0\}, \cdot), ...$

*Proposición:*

1. Si $\forall x \in G, x^2 = e \Rightarrow G$ es abeliano
2. Si $\forall a, b \in G, (a \circ b)^2 = a^2 \circ b^2 \Rightarrow G$ es abeliano

*Demostración:*

1. (Es el problema 5 de la hoja de ejercicios)
   $\forall x \in G, x^2 = e \Rightarrow x^{-1} \circ x^2 = x^{-1} \Rightarrow$*(por la propiedad asociativa)*$\Rightarrow x = x^{-1}$
   Tomemos $a, b \in G \Rightarrow a = a^{-1}, b = b^{-1} \Rightarrow$ sea $a \circ b = c \Rightarrow a^{-1} \circ b^{-1} = c \Rightarrow$*(por las propiedades del inverso de un producto)*$\Rightarrow (b \circ a)^{-1} = c \Rightarrow (b \circ a) = c \Rightarrow b \circ a = a \circ b \Rightarrow G$ es abeliano
2. Sea $(a \circ b)^2 = a^2 \circ b^2 \Rightarrow (a \circ b) \circ (a \circ b) = (a \circ a) \circ (b \circ b) \Rightarrow$*(por la propiedad asociativa)*$\Rightarrow ((a \circ b) \circ a) \circ b = ((a \circ a) \circ b) \circ b \Rightarrow$*(por las propiedades de simplificación)*$\Rightarrow (a \circ b) \circ a = (a \circ a) \circ b \Rightarrow$*(por la propiedad asociativa)*$\Rightarrow a \circ (b \circ a) = a \circ (a \circ b) \Rightarrow$*(por las propiedades de simplificación)*$\Rightarrow b \circ a = a \circ b \Rightarrow G$ es abeliano

### 2.1.4. Orden de un grupo

El *orden* de un grupo es el cardinal de ese grupo, $\mathcal{O}(G) = card(G)$

## 2.2. Subgrupo

### 2.2.1. Definición de subgrupo

Un *subgrupo* de un grupo $(G, \circ)$ es un subconjunto $H \neq$ de $G$ tal que bajo la misma operación $\circ$ que $G$, $(H, \circ)$ es un grupo.

*Observaciones:*

1. $G$ y $H$ tienen el mismo elemento neutro (dado que el elemento neutro es único)

2. Si $a \in H \Rightarrow a_G^{-1} \in H$, o sea, si un elemento pertenece a $H$, su inverso también pertenece a $H$ (el elemento inverso es único)

3. $\{e\}$ y $G$ con la operación $\circ$ son subgrupos de $(G, \circ)$, a estos subgrupos se les denomina *impropios* (los demás son los subgrupos propios)

***Ejemplos:***

- En el grupo de las permutaciones de tres elementos el subconjunto $H = \{e, \sigma_+, \sigma_-\}$ es un subgrupo (con la operación composición de permutaciones). Ver tabla de multiplicar de la página 2 de este tema.
- $(\mathbb{Z}, +)$ es un subgrupo de $(\mathbb{Q}, +)$
- Los enteros pares son un subgrupo de $(\mathbb{Z}, +)$. Sin embargo, los enteros impares no forman un subgrupo.

*Proposición:* Sea $H \neq$ un subconjunto de $G$, $H$ es subgrupo de $G$ si y sólo si $\forall x, y \in H \Rightarrow x \circ y^{-1} \in H$

*Demostración:*

- $\boxed{\Rightarrow}$

  $H \subset G$ y $H$ subgrupo de $G \Rightarrow \forall y \in H,\ \exists\, z = y^{-1} \in H$

  Si $x \in H \Rightarrow \forall z \in H,\ x \circ z \in H \Rightarrow x \circ y^{-1} \in H$

- $\boxed{\Leftarrow}$

  $H \subset G$ y $x \circ y^{-1} \in H,\ \forall x, y \in H$

  i. Si $x = y \Rightarrow x^{-1} = y^{-1} \Rightarrow x \circ y^{-1} = x \circ x^{-1} \in H \Rightarrow e \in H$: tiene elemento neutro

  ii. Si $y \in H \Rightarrow y^{-1} \in H$ ya que $e \in H \Rightarrow$*(como* $\forall x, y \in H, x \circ y^{-1} \in H$*)*$\Rightarrow e \circ y^{-1} \in H$: tiene elemento inverso

  iii. $x \circ y \in H$ ya que $y^{-1} \in H \Rightarrow (y^{-1})^{-1} \in H \Rightarrow x \circ (y^{-1})^{-1} \in H \Rightarrow x \circ y \in H$: operación interna

  iv. $(x \circ y) \circ z = x \circ (y \circ z),\ \forall x, y, z \in H$ ya que $x, y, z \in G$ y $G$ es un grupo con la propiedad asociativa

*Proposición:* Dado un grupo $G$, la intersección de dos subgrupos de $G$, $H_1$ y $H_2$, es un subgrupo de $G$.

*Demostración:*

$H = H_1 \cap H_2 \neq$ ya que $e \in H_1$ y $e \in H_2$

$\forall x, y \in H \Rightarrow x \in H_1, y \in H_1, x \in H_2, y \in H_2 \Rightarrow x \circ y^{-1} \in H_1, x \circ y^{-1} \in H_2 \Rightarrow x \circ y^{-1} \in H_1 \cap H_2 = H$, por lo tanto, por la proposición anterior, $H$ es un subgrupo.

### 2.2.2. Subgrupo generado por un subconjunto $S$ de $G$

Sea $S \subset G$, con $S \neq$ , definimos $\langle S \rangle = \{s_1^{m_1} \circ \cdots \circ s_n^{m_n} \ / \ n \in \mathbb{N}, s_i \in S, m_i \in \mathbb{Z}, 1 \leq i \leq n\}$, donde $n$ es cualquier número no fijo y los exponentes pueden ser negativos. El conjunto $\langle S \rangle$ formado de esta forma es subgrupo de $G$ y se denomina *subgrupo generado por* $S$

*Demostración:*

$\langle S \rangle \neq$ ya que $\forall s \in S, s = s^1 \in \langle S \rangle$, además $S \subset \langle S \rangle$

Si $x, y \in \langle S \rangle$, con $x = s_1^{m_1} \circ \cdots \circ s_n^{m_n}$ siendo $s_1, ..., s_n \in S$ y $m_1, ..., m_n \in \mathbb{Z}$, y con $y = t_1^{l_1} \circ \cdots \circ t_i^{l_i}$ siendo $t_1, ..., t_i \in S$ y $l_1, ..., l_i \in \mathbb{Z}$.

Como $y^{-1} = t_i^{-l_i} \circ \cdots \circ t_1^{-l_1}$, tendremos que $x \circ y^{-1} = s_1^{m_1} \circ \cdots \circ s_n^{m_n} \circ t_i^{-l_i} \circ \cdots \circ t_1^{-l_1} \in \langle S \rangle$, dado que es un producto de elementos de $S$ elevados a potencias enteras, por lo tanto $\langle S \rangle$ es un subgrupo.

***Ejemplo:***

Tomemos el subconjunto $S = \{\sigma_+, \sigma_-\}$ del grupo $S_3$ de permutaciones de tres elementos. En este caso, el subgrupo generado es $\langle S \rangle = \{e, \sigma_+, \sigma_-\}$

### 2.2.3. Subgrupo generado por un elemento $a$ de $G$

Sea $S = \{a\} \subset G$, denotaremos $\langle a \rangle$ y lo llamaremos *subgrupo generado por el elemento* $a$ al subgrupo $\langle a \rangle = \{a^k \ / \ k \in \mathbb{Z}\}$

El subgrupo generado por un elemento es un caso particular del subgrupo generado por un conjunto.

***Ejemplo:***

Tomemos el elemento $\tau_2$ del grupo $S_3$. El subgrupo generado será $\langle \tau_2 \rangle = \{e, \tau_2\}$

### 2.2.4. Sistema generador de $G$

Sea $S \subset G$ con $S \neq$ , diremos que $S$ es un *sistema generador* de $G$ si se cumple que $\langle S \rangle = G$

***Ejemplo:***

El subconjunto $S = \{\tau_1, \tau_2, \tau_3\}$ del grupo de permutaciones de tres elementos es un sistema generador de $S_3$ dado que

$\langle S \rangle = G$

### 2.2.5. Grupo finitamente generado

Si un grupo $G$ tiene un sistema finito de generadores se dice que $G$ es un *grupo finitamente generado.*

***Ejemplo:***

El grupo $(\mathbb{Z}, +)$ es un grupo finitamente generado, aunque sea un grupo con infinitos elementos, dado que todos se pueden generar a partir de 1.

### 2.2.6. Grupo cíclico

Un grupo $G$ se dice que es un *grupo cíclico* si existe al menos un elemento $x \in G$ tal que el subgrupo generado por $x$ sea $G$, o sea, $\langle x \rangle = G$

***Ejemplo:***

En el grupo de rotaciones de un cuadrado que vimos al principio del tema $G = \{I, r_1, r_2, r_3\}$, la rotación de $90^o$, denominada $r_1$, genera el resto de elementos de $G$, dado que $I = r_1 \circ r_1 \circ r_1 \circ r_1 = r_1^4 = r_1 \circ r_1^{-1}$, $r_2 = r_1 \circ r_1 = r_1^2$, $r_3 = r_1 \circ r_1 \circ r_1 = r_1^3$, por lo tanto dicho grupo es un grupo cíclico.

### 2.2.7. Centralizador de $H$ en $G$

Sea $H$ subgrupo de $G$, llamamos *centralizador* de $H$ en $G$ al conjunto $C_G(H) = \{x \in G \ / \ a \circ x = x \circ a \ \forall a \in H\}$. Por lo tanto, el centralizador de un subgrupo es el conjunto de elementos del grupo que conmuntan con todos los elementos del subgrupo.

*Propiedad:* El centralizador $C_G(H)$ de $H$ en $G$ es un subgrupo de $G$.

*Demostración:*

El conjunto $C_G(H) \neq$ , dado que $e \in C_G(H)$, porque el elemento neutro conmuta con todos los elementos.

Si $x, y \in C_G(H) \Rightarrow \forall a \in H,\ a \circ x = x \circ a$ y $a \circ y = y \circ a$, como $a^{-1} \in H$ dado que $H$ es un subgrupo, tendremos que $a^{-1} \circ y = y \circ a^{-1}$.

Por otro lado, $a \circ (x \circ y^{-1}) =$*(por la propiedad asociativa de los grupos)*$= (a \circ x) \circ y^{-1} =$*(como* $x \in C_G(H)$ *conmuta con* $a$*)*$= (x \circ a) \circ y^{-1} =$*(por la propiedad asociativa de los grupos)*$= x \circ (a \circ y^{-1}) =$*(utilizando las propiedades del inverso de un producto)*$= x \circ (y \circ a^{-1})^{-1} =$*(como* $y \in C_G(H)$ *conmuta con* $a^{-1}$*)*$= x \circ (a^{-1} \circ y)^{-1} =$*(utilizando las propiedades del inverso de un producto)*$= x \circ (y^{-1} \circ a) =$*(por la propiedad asociativa de los grupos)*$= (x \circ y^{-1}) \circ a$

Como $x \circ y^{-1}$ conmuta con cualquier elemento de $H$, tendremos que $x \circ y^{-1} \in C_G(H)$, por lo tanto $C_G(H)$ es un subgrupo.

***Ejemplo:***

Dado el subgrupo $H = \{e, \sigma_+, \sigma_-\}$ del grupo de permutaciones de tres elementos $S_3$, tendremos que $C_G(H) = H$

### 2.2.8. Centro de $G$

Se define *centro* de $G$ como el centralizador de $G$ en $G$, por lo tanto $Z(G) = C_G(G)$.

El centro de $G$ es un subgrupo.

***Ejemplo:***

Dado el grupo de las permutaciones de tres elementos $S_3$, el centro de dicho grupo será $Z(G) = \{e\}$

### 2.2.9. Conjugado de $S$

Sea $S \subset G$ con $S \neq$ y sea $a \in G$, se llama *conjugado* de $S$ por $a$ al conjunto $S_a = \{a^{-1} \circ x \circ a \ / \ x \in S\}$

***Ejemplos:***

- Dado el grupo de las permutaciones de tres elementos $S_3$ y dado el subconjunto $S = \{\tau_1, \tau_2\}$ tendremos que $S_{\tau_2} = \{\tau_3, \tau_2\}$, ya que $\tau_2^{-1} = \tau_2$, por lo tanto $(\tau_2^{-1} \circ \tau_1) \circ \tau_2 = (\tau_2 \circ \tau_1) \circ \tau_2 = \sigma_+ \circ \tau_2 = \tau_3$ y $(\tau_2^{-1} \circ \tau_2) \circ \tau_2 = e \circ \tau_2 = \tau_2$

- Dado el grupo de las permutaciones de tres elementos $S_3$ y dado el subconjunto $S = \{\tau_1, \tau_2\}$ tendremos que $S_{\sigma_+} = \{\tau_2, \tau_3\}$, ya que $\sigma_+^{-1} = \sigma_-$, por lo tanto $(\sigma_+^{-1} \circ \tau_1) \circ \sigma_+ = (\sigma_- \circ \tau_1) \circ \sigma_+ = \tau_3 \circ \sigma_+ = \tau_2$ y $(\sigma_+^{-1} \circ \tau_2) \circ \sigma_+ = (\sigma_- \circ \tau_2) \circ \sigma_+ = \tau_1 \circ \sigma_+ = \tau_3$

*Propiedades del conjugado de $S$:*

1. La aplicación $\alpha: \begin{array}{l} S \longrightarrow S_a \\ x \longrightarrow a^{-1} \circ x \circ a \end{array}$ es biyectiva

2. $(S_a)_b = S_{a \circ b}$, $\forall a, b \in G$, dado que $(S_a)_b = \{b^{-1} \circ (a^{-1} \circ x \circ a) \circ b \ / \ x \in S\} = \{(a \circ b)^{-1} \circ x \circ (a \circ b) \ / \ x \in S\} = S_{a \circ b}$

3. $S = S_e$, dado que $S_e = \{e^{-1} \circ x \circ e \ / \ x \in S\} = \{x \ / \ x \in S\} = S$

4. Si $S \subset G \Rightarrow S_a \subset G$

5. Si $S \subset T \Rightarrow S_a \subset T_a$

## 2.2.10. Normalizador de $S$ en $G$

Sea $S \subset G$ con $S \neq$ , se llama *normalizador* de $S$ en $G$ a $N_G(S) = \{a \in G \ / \ S_a = S\}$. Por lo tanto, es el conjunto formado por aquellos elementos del grupo cuyo conjugado de $S$ por dicho elemento es el propio $S$.

***Ejemplo:***

En el grupo de las permutaciones de tres elementos $S_3$, el normalizador del subconjunto $S = \{\tau_1, \tau_2\}$ en $G$ es el conjunto $N_{S_3}(S) = \{e, \tau_3\}$, dado que $S_e = S$, ya que $(e^{-1} \circ \tau_1) \circ e = \tau_1$ y $(e^{-1} \circ \tau_2) \circ e = \tau_2$, y por otro lado $S_{\tau_3} = S$ ya que $(\tau_3^{-1} \circ \tau_1) \circ \tau_3 = (\tau_3 \circ \tau_1) \circ \tau_3 = \sigma_- \circ \tau_3 = \tau_2$ y $(\tau_3^{-1} \circ \tau_2) \circ \tau_3 = (\tau_3 \circ \tau_2) \circ \tau_3 = \sigma_+ \circ \tau_3 = \tau_1$

*Propiedad:* El normalizador $N_G(S)$ de $S$ en $G$ es un subgrupo de $G$.

*Demostración:*

Tenemos que $N_G(S) \neq$ dado que $e \in N_G(S)$ ya que siempre se cumplirá que $S_e = S$

Si $a, b \in N_G(S) \Rightarrow S_a = S_b = S$

Como $S_{a \circ b^{-1}} = (S_a)_{b^{-1}} = S_{b^{-1}}$ dado que $S_a = S$ y como $S = S_e = (S_b)_{b^{-1}} = S_{b^{-1}}$ tendremos que $S = S_{a \circ b^{-1}}$, por lo tanto $a \circ b^{-1} \in N_G(S)$, por lo que $N_G(S)$ es un subgrupo.

## 2.3. Clases laterales y Relaciones de equivalencia

### 2.3.1. Definición de clase lateral

Sea $H$ un subgrupo del grupo $G$ y sea $a$ un elemento de $G$, se llama *clase lateral (o coset) por la izquierda* de $H$ al conjunto $aH = \{x \in G \ / \ x = a \circ h, \ \forall h \in H\}$

Análogamente definimos *clase lateral por la derecha* al conjunto $Ha = \{x \in G \ / \ x = h \circ a, \ \forall h \in H\}$

***Ejemplos:***

1. Dado el grupo de las permutaciones de tres elementos $S_3$ y dado el subgrupo $H = \{e, \sigma_+, \sigma_-\}$, las clases laterales por la izquierda y por la derecha de dicho subgrupo son:

$$\begin{array}{ll} eH = H, & He = H \\ \sigma_- H = H, & H\sigma_- = H \\ \sigma_+ H = H, & H\sigma_+ = H \\ \tau_1 H = \{\tau_1, \tau_2, \tau_3\}, & H\tau_1 = \{\tau_1, \tau_2, \tau_3\} \\ \tau_2 H = \{\tau_1, \tau_2, \tau_3\}, & H\tau_2 = \{\tau_1, \tau_2, \tau_3\} \\ \tau_3 H = \{\tau_1, \tau_2, \tau_3\}, & H\tau_3 = \{\tau_1, \tau_2, \tau_3\} \end{array}$$

2. Dado el grupo de las permutaciones de tres elementos $S_3$ y dado el subgrupo $H = \{e, \tau_1\}$, las clases laterales por la izquierda y por la derecha de dicho subgrupo son:

$$\begin{array}{ll} eH = H, & He = H \\ \sigma_- H = \{\sigma_-, \tau_3\}, & H\sigma_- = \{\sigma_-, \tau_2\} \\ \sigma_+ H = \{\sigma_+, \tau_2\}, & H\sigma_+ = \{\sigma_+, \tau_3\} \\ \tau_1 H = H, & H\tau_1 = H \\ \tau_2 H = \{\sigma+, \tau_2\}, & H\tau_2 = \{\sigma_-, \tau_2\} \\ \tau_3 H = \{\sigma_-, \tau_3\}, & H\tau_3 = \{\sigma+, \tau_3\} \end{array}$$

*Observaciones:*

1. La clase lateral por la izquierda $aH$ no tiene por qué coincidir con la clase lateral por la derecha $Ha$ (ejemplo 2).

2. La igualdad de clases no se refiere a los productos individuales sino a conjuntos completos (en el ejemplo 2 $eH = \tau_1 H$)

3. Las clases o son disjuntas o son iguales y todo elemento del grupo está en alguna de las clases, por lo tanto las clases laterales proporcionan una partición de $G$.

4. El elemento que define la clase está en la clase.

¡Importante!: Repasad las clases de equivalencia y las relaciones de equivalencia.

### 2.3.2. Relación de equivalencia

Sea $H$ un subgrupo de $G$, definimos el conjunto $\mathcal{R}_H = \{(x,y) \in G \times G \ / \ x^{-1} \circ y \in H\}$, dicho conjunto es una *relación de equivalencia.*

*Demostración:*

1. Propiedad reflexiva:

   $(x,x) \in \mathcal{R}_H$, $\forall x \in G$ ya que $x^{-1} \circ x = e \in H$ dado que $H$ es un subgrupo

2. Propiedad simétrica:

   $(x,y) \in \mathcal{R}_H \Rightarrow x^{-1} \circ y \in H \Rightarrow$*(como $H$ es subgrupo)*$\Rightarrow (x^{-1} \circ y)^{-1} \in H \Rightarrow y^{-1} \circ x \in H \Rightarrow (y,x) \in \mathcal{R}_H$

3. Propiedad transitiva:

   $(x,y) \in \mathcal{R}_H$, $(y,z) \in \mathcal{R}_H \Rightarrow x^{-1} \circ y \in H$, $y^{-1} \circ z \in H \Rightarrow$*(como $H$ es subgrupo)*$\Rightarrow (x^{-1} \circ y) \circ (y^{-1} \circ z) = x^{-1} \circ z \in H \Rightarrow (x,z) \in \mathcal{R}_H$

Si escribimos $x\mathcal{R}y$ cuando $(x,y) \in \mathcal{R}_H$, las clases de equivalencia $xH$ son las clases de $H$ por la izquierda.

*Teorema:* Sea $H$ un subgrupo de un grupo $G$, las clases por la derecha (por la izquierda) en $G$ forman una partición de $G$ (colección de subconjuntos disjuntos de $G$ cuya unión es $G$).

*Demostración:*

1. Cada elemento de $G$ aparece en al menos una clase por la derecha (por la izquierda), ya que si $g \in G \Rightarrow g \in Hg$ ya que $e \in H$

2. Sean $Ha$ y $Hb$ dos clases de $H$ en $G$, supongamos que $Ha \cap Hb \neq \ \Rightarrow \exists x \in G \ / \ x = h \circ a, x = h' \circ b$ con $h, h' \in H \Rightarrow h \circ a = h' \circ b \Rightarrow a = h^{-1} \circ h' \circ b$, como $h^{-1} \circ h' \in H$ por ser subgrupo $\Rightarrow a = h'' \circ b \Rightarrow a \in Hb \Rightarrow Ha \subset Hb$. De la misma forma se demuestra que $Hb \subset Ha$, por lo tanto $Ha = Hb$

Como todo elemento de $G$ está en alguna clase y las clases o son iguales o son disjuntas formarán una partición de $G$.

## 2.4. Teorema de Lagrange

El orden de un subgrupo de un grupo finito $G$ es divisor del orden de $G$.

*Demostración:*
Sean $Hg_1, ..., Hg_n$ las clases por la derecha de $H$ en $G$ que sean disjuntas (que formen una partición), en este caso tendremos que $\mathcal{O}(G) = card(Hg_1) + ... + card(Hg_n)$, además

$card(Hg_k) = card(H)\ \forall k$, ya que si definimos la aplicación $O_g : \begin{array}{c} H \longrightarrow Hg \\ a \longrightarrow ag \end{array}$, dicha aplicación es biyectiva, ya que es suprayectiva (por definición de clase) e inyectiva porque si $O_g(a) = O_g(b) \Rightarrow ag = bg \Rightarrow a = b$. Por lo tanto, $card(Hg) = card(H)$ por ser biyectiva y por tanto, si tenemos $n$ clases se cumplirá que $\mathcal{O}(G) = n \cdot card(H)$

*Consecuencias:*

1. El orden de un subgrupo $H$ de $G$ es divisor del orden de $G$

   ***Ejemplo:***

   $G = \{1, 2, 3, 4, 5\}, H = \{1, 2\}$ no puede ser nunca un subgrupo de $G$ aunque no conozcamos la operación definida en $G$

2. Si el orden de $G$ es primo, entonces $G$ no tiene subgrupos propios, tendrá solamente los impropios: $\{e\}, G$

   ***Ejemplos:***

   *a*) Determinar los subgrupos del grupo cuya tabla de multiplicar es:

| | $I$ | $A$ | $B$ | $C$ |
|---|---|---|---|---|
| $I$ | $I$ | $A$ | $B$ | $C$ |
| $A$ | $A$ | $I$ | $C$ | $B$ |
| $B$ | $B$ | $C$ | $I$ | $A$ |
| $C$ | $C$ | $B$ | $A$ | $I$ |

(Grupo de Klein)

Los subgrupos serán de orden 1, 2 ó 4.
Orden 1:$\{I\}$
Orden 2: $\{I, A\}, \{I, B\}, \{I, C\}$
Orden 4: $G = \{I, A, B, C\}$

*b*) Determinar los subgrupos del grupo $C_5$ cuya tabla de multiplicar es:

| | $I$ | $A$ | $B$ | $C$ | $D$ |
|---|---|---|---|---|---|
| $I$ | $I$ | $A$ | $B$ | $C$ | $D$ |
| $A$ | $A$ | $B$ | $C$ | $D$ | $I$ |
| $B$ | $B$ | $C$ | $D$ | $I$ | $A$ |
| $C$ | $C$ | $D$ | $I$ | $A$ | $B$ |
| $D$ | $D$ | $I$ | $A$ | $B$ | $C$ |

(Grupo cíclico de orden 5)

Este grupo no tiene ningún subgrupo propio.

*c*) Determinar los subgrupos del grupo de permutaciones de tres elementos $S_3$

Como $card(S_3) = 6$, podemos tener subgrupos de orden 1, 2, 3 ó 6

Orden 1: $\{e\}$

Orden 2: $\{e, \tau_1\}, \{e, \tau_2\}, \{e, \tau_3\}$

Orden 3: $\{e, \sigma_+, \sigma_-\}$

Orden 6: $S_3$

*d*) Determinar los subgrupos del grupo $C_4$ cuya tabla de multiplicar es:

| | $I$ | $A$ | $B$ | $C$ |
|---|---|---|---|---|
| $I$ | $I$ | $A$ | $B$ | $C$ |
| $A$ | $A$ | $B$ | $C$ | $I$ |
| $B$ | $B$ | $C$ | $I$ | $A$ |
| $C$ | $C$ | $I$ | $A$ | $B$ |

(Grupo cíclico de orden 4)

Los subgrupos serán de orden 1, 2 ó 4:

Orden 1: $\{I\}$

Orden 2: $\{I, B\}$

Orden 4: $\{I, A, B, C\}$

Podemos comparar esta tabla con la tabla de la operación de rotación de un cuadrado, se puede ver que es la misma.

Las rotaciones de un polígono regular en el plano forman un grupo cíclico del mismo orden que el número de lados del polígono.

*Teorema:*

La condición necesaria y suficiente para que las clases por la derecha y las clases por la izquierda proporcionen la misma partición de un grupo $G$ es que $aH = Ha$, $\forall a \in G$

*Demostración:*

$\boxed{\Rightarrow}$

Si $a \in G \Rightarrow a \in aH,\ a \in Ha$, como las clases por la derecha forman una partición y la única clase que contiene a $a$ es $Ha$ (dado que las clases son disjuntas) y hemos supuesto que toda partición por la derecha lo es también por la izquierda, tendremos que $Ha = aH,\ \forall a \in G$

Cualquier $b \in aH$ también cumple que $b \in bH \Rightarrow aH = bH$

$\boxed{\Leftarrow}$

Si $aH = Ha$, $\forall a \in G$, tendremos que la clase por la derecha también lo es por la izquierda, por lo tanto las particiones coinciden.

*Proposición:*

Sea $G$ un grupo y $H$ un subgrupo de $G$, tendremos que $aH = Ha \Leftrightarrow \forall a \in G, \forall h \in H,\ a^{-1} \circ h \circ a \in H$

*Demostración:*

$\boxed{\Rightarrow}$

Supongamos que $aH = Ha,\ \forall a \in G \Rightarrow \forall h \in H,\ \exists h' \in H\ /\ a \circ h' = h \circ a \Rightarrow a^{-1} \circ h \circ a = h' \in H$

$\boxed{\Leftarrow}$

Supongamos que $\forall a \in G,\ \forall h \in H,\ a^{-1} \circ h \circ a \in H \Rightarrow \exists h' \in H\ /\ a^{-1} \circ h \circ a = h' \Rightarrow h \circ a = a \circ h' \Rightarrow Ha \subset aH$

Por otro lado, $\forall h \in H,\ a \circ h \in aH \Rightarrow a \circ h = a \circ h \circ (a^{-1} \circ a) = (a \circ h \circ a^{-1}) \circ a = ((a^{-1})^{-1} \circ h \circ a^{-1}) \circ a \in Ha$, ya que $\forall x \in G, \forall h \in H,\ x^{-1} \circ h \circ x \in H$, como $a^{-1} = x \in G$ la afirmación anterior será válida, por lo tanto $aH \subset Ha$

Si $Ha \subset aH$ y $aH \subset Ha$ tendremos que $aH = Ha$

*Observaciones:*

Los elementos del normalizador $N_G(H)$ de un subgrupo $H$ del grupo $G$ dará las mismas clases por la derecha y por la izquierda.

Dado que el normalizador se define como $N_G(S) = \{a \in G\ /\ S_a = S\}$, siendo $S_a = \{a^{-1} \circ x \circ a\ /\ x \in S\}$, tendremos que dado un subgrupo $H$, $\forall a \in N_G(H), \forall h \in H,\ a^{-1} \circ h \circ a = h' \in H$, ya que por ser $a$ un elemento del normalizador de $H$ se cumplirá que $H_a = H$, siendo los elementos de $H_a$ (y por lo tanto, también los de $H$) de la forma $a^{-1} \circ h \circ a$, con $h \in H$

## 2.5. Subgrupo normal o invariante

### 2.5.1. Definición

Un subgrupo $H$ de un grupo $G$ se denomina *subgrupo normal* o *invariante* si $g \circ h \circ g^{-1} \in H, \forall h \in H, \forall g \in G$. Por lo tanto $H$ es normal en $G$ si y sólo si $Hg = gH, \forall g \in G$

***Ejemplos:***

1. Todo subgrupo de un grupo abeliano es normal

   *Demostración:*

   Si $H$ es subgrupo de $G$ (abeliano), tendremos que $gH = Hg$ ya que $g \circ h = h \circ g, \forall g \in G, \forall h \in H \subset G$

2. En el grupo de las permutaciones de tres elementos, $S_3$, el subgrupo $H = \{e, \sigma_+, \sigma_-\}$ es normal. Sin embargo, los subgrupos $H_1 = \{e, \tau_1\}, H_2 = \{e, \tau_2\}$ y $H_3 = \{e, \tau_3\}$ no lo son.

3. El centro $Z(G)$ de un grupo $G$ es un subgrupo normal.

   *Demostración:*

   Por definición tenemos que $Z(G) = \{x \ / \ x \in G \text{ y } \forall g \in G, x \circ g = g \circ x\}$, por lo tanto, dado $a \in G$ tendremos que $a \circ x = x \circ a, \forall x \in Z(G) \Rightarrow a^{-1} \circ x \circ a = x \in Z(G)$

4. Los subgrupos impropios son normales

   *Demostración:*

   Dado el subgrupo impropio $H = \{e\}$, como $e \circ g = g = g \circ e$, tenemos que $gH = Hg, \forall g \in G$

   Dado el subgrupo impropio $H = G$, tendremos que $gH = G = Hg, \forall g \in G$

### 2.5.2. Grupo cociente

Sea $(G, \circ)$ un grupo y $(N, \circ)$ un subgrupo normal, definimos *grupo cociente* $(G/N, \cdot)$ como el conjunto de elementos de la partición proporcionada por $N$, $G/N$, con $(aN) \cdot (bN) = (a \circ b)N$.

Recordad que el conjunto cociente $G/H$ es el conjunto de las clases de la partición proporcionada por $H$. Por lo tanto, cuando dicha partición está proporcionada por un subgrupo

normal podemos definir una operación $\cdot$ entre clases y el conjunto cociente junto con dicha operación tendrán estructura de grupo, como veremos más adelante.

*Proposición:* Si $N$ es un subgrupo normal, tendremos que si $aN = a'N$ y $bN = b'N$ se cumple que $(a \circ b)N = (a' \circ b')N$

*Demostración:*
Sea $aN = a'N$, tendremos que $a \in aN \Rightarrow \exists n' \in N \ / \ a = a' \circ n'$
De igual modo si $bN = b'N \Rightarrow b \in bN \Rightarrow \exists n'' \in N \ / \ b = b' \circ n''$

$$\overbrace{\qquad\qquad\qquad\qquad\qquad\qquad}^{\in N}$$
$$\underbrace{\qquad\qquad\qquad\qquad\qquad\qquad}_{\in N \text{ por ser normal}}$$

Por lo tanto, $a \circ b = a' \circ n' \circ b' \circ n'' = a' \circ b' \circ \overbrace{(\underbrace{(b'^{-1} \circ n' \circ b')}_{\in N} \circ n'')}^{\in N} = a' \circ b' \circ n'''$ con $n''' \in N$, así tendremos que $a \circ b \in (a' \circ b')N$, por lo que $(a \circ b)N \subset (a' \circ b')N$
Como las clases laterales forman una partición, si $(a \circ b)N \subset (a' \circ b')N \Rightarrow (a \circ b)N \cap (a' \circ b')N \neq \Rightarrow (a \circ b)N = (a' \circ b')N$
Por lo tanto, el producto de las clases del conjunto cociente $G/N$ es independiente de los elementos elegidos para calcularlo si el subgrupo es normal.

*Teorema:* El conjunto cociente $G/N$ con el producto de clases $(aN) \cdot (bN) = (a \circ b)N$ es un grupo.

*Demostración:*

1. Operación interna: $(aN) \cdot (bN) \in G/N$ ya que $(a \circ b)N$ es uno de los elementos de la partición definida por el subgrupo $N$
2. Propiedad asociativa: $((aN) \cdot (bN)) \cdot (cN) = ((a \circ b)N) \cdot cN = ((a \circ b) \circ c)N =$*(como $G$ es un grupo tendremos que* $(a \circ b) \circ c = a \circ (b \circ c)$*)*$= (a \circ (b \circ c))N = (aN) \cdot ((b \circ c)N) = (aN) \cdot ((bN) \cdot (cN))$
3. Elemento neutro: la clase $eN = N$ es el elemento neutro del producto de clases ya que $(aN) \cdot (eN) = (a \circ e)N = aN$
4. Elemento inverso: dada una clase $aN$ existe una clase inversa $a^{-1}N$, tal que su producto es el elemento neutro, ya que $(aN) \cdot (a^{-1}N) = (a \circ a^{-1})N = eN = N$

***Ejemplo:***
Sea el grupo $S_3$ de las permutaciones de tres elementos y el subgrupo normal $H = \{e, \sigma_+, \sigma_-\}$, definimos las clases $E = eH = \{e, \sigma_+, \sigma_-\} = \sigma_+H = \sigma_-H$, $A = \tau_1 H = \{\tau_1, \tau_2, \tau_3\}$

Tendremos que
$E \cdot E = (eH) \cdot (eH) = (e \circ e)H = eH = E$
$E \cdot A = (eH) \cdot (\tau_1 H) = (e \circ \tau_1)H = \tau_1 H = A$
$A \cdot A = (\tau_1 H) \cdot (\tau_1 H) = (\tau_1 \circ \tau_1)H = eH = E$ Por lo tanto, la tabla de multiplicar es:

| $(G/H, \cdot)$ | $E$ | $A$ |
|---|---|---|
| $E$ | $E$ | $A$ |
| $A$ | $A$ | $E$ |

Podemos ver que dicho conjunto de clases con la operación producto de clases es un grupo.

Si hubiesemos tomado $G = S_3$ y $H = \{e, \tau_1\}$, como $H$ no es un subgrupo normal, no podemos definir el grupo cociente $G/H$, ya que, por ejemplo $\sigma_- H = \tau_3 H$, pero $(\sigma_- H) \cdot (\sigma_+ H) = (\sigma_- \circ \sigma_+)H = eH = H = \{e, \tau_1\}$, sin embargo $(\tau_3 H) \cdot (\sigma_+ H) = (\tau_3 \circ \sigma_+)H = \tau_2 H = \{\tau_2, \sigma_+\}$. Como vemos $H \neq \tau_2 H$, por lo que la operación entre clases no está bien definida. Esto es debido a que el subgrupo utilizado no es normal.

### 2.5.3. Grupo simple

Un *grupo simple* es aquel grupo cuyos únicos subgrupos normales son los impropios ($\{e\}$ y el propio grupo).

# Capítulo 3

# Homorfismos de Grupos

## 3.1. Homomorfismo

### 3.1.1. Definición de homomorfismo

Sean $(G_1, \circ)$ y $(G_2, \cdot)$ dos grupos y $f$ una aplicación de $G_1$ en $G_2$, $f : G_1 \longrightarrow G_2$. La aplicación $f$ es un *homomorfismo* de grupos si $\forall x, y \in G_1$ tenemos que $f(x \circ y) = f(x) \cdot f(y)$

### 3.1.2. Clasificación de homomorfismos

Sea $f$ un homorfismo entre grupos, tendremos que:

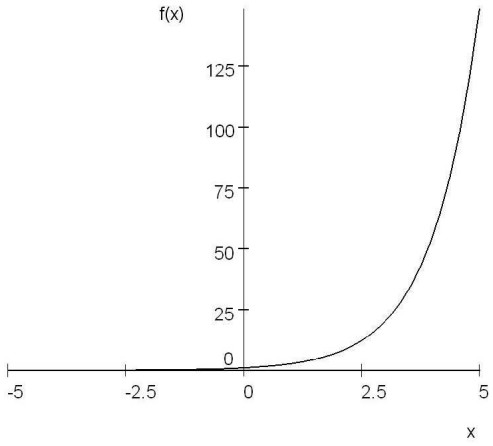
1. Si $f$ es inyectiva, entonces $f$ es un *monomorfismo*
2. Si $f$ es suyprayectiva, entonces $f$ es un *epimorfismo*
3. Si $f$ es biyectiva, entonces $f$ es un *isomorfismo*

Isomorfismos entre un mismo grupo se llama *automorfismos.*

Dos grupos son *isomorfos* si se puede establecer un isomorfismo entre ellos.

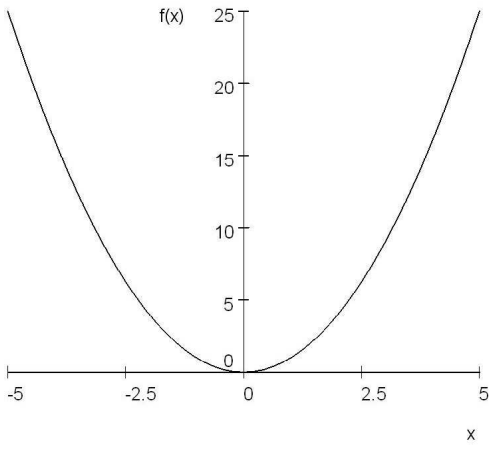
***Ejemplos:***

1. Sean $(\mathbb{R},+)$ y $(\mathbb{R}^*,\cdot)$, establecemos la aplicación $f:\ \begin{array}{l}\mathbb{R}\to\mathbb{R}^*\\ x\to\exp(x)\end{array}$,
tendremos que $f(x+y)=\exp(x+y)=\exp(x)\cdot\exp(y)=f(x)\cdot f(y)$. Por lo tanto es un homomorfismo, como además $f$ es inyectiva será un monomorfismo.




2. Si tomamos $(\mathbb{R},+)$ y $(\mathbb{R}^+,\cdot)$ y $f:\ \begin{array}{l}\mathbb{R}\to\mathbb{R}^+\\ x\to\exp(x)\end{array}$, tendremos que $f$ es biyectiva y por tanto será un isomorfimo.

3. Sean los grupos $G_1=(\mathbb{R}^*,\cdot)$ y $G_2=(\mathbb{R}^*,\cdot)$, definimos la aplicación $f(x)=x^2$. Como $f(x\cdot y)=(x\cdot y)^2=x^2\cdot y^2=f(x)\cdot f(y)$ será un homorfismo, pero en este caso $f$ no es ni suprayectiva ni inyectiva.




4. Sean los grupos $G_1 = (\mathbb{R} \times \mathbb{R} - \{(0,0)\}, *)$ y $G_2 = (\mathbb{R}^+ - \{0\} \times \Theta, \circ)$ donde $\Theta = [0, 2\pi) \subset \mathbb{R}$, donde las operaciones se definen de la siguiente forma

   $(a,b) * (c,d) = (ac - bd, ad + bc)$ y $(r_1, \theta_1) \circ (r_2, \theta_2) = (r_1 r_2, \theta_1 + \theta_2)$

   La aplicación $f: \begin{array}{ccc} \mathbb{R} \times \mathbb{R} - \{(0,0)\} & \longrightarrow & \mathbb{R}^+ - \{0\} \times \Theta \\ (a,b) & \longrightarrow & (r,\theta) \end{array}$

   con $r = (a^2 + b^2)^{1/2}$ y $\theta = \arctan(b/a)$ con $\cos(\theta) = \dfrac{a}{(a^2+b^2)^{1/2}}$ y $\sin(\theta) = \dfrac{b}{(a^2+b^2)^{1/2}}$ es un isomorfimo, que representa la transformación de coordenadas cartesianas en polares con el producto.

   Podemos ver que si $f(a,b) = (r_1, \theta_1)$ y $f(c,d) = (r_2, \theta_2)$, tendremos que

   $$f((a,b) * (c,d)) = f(ac - bd, ad + bc) = (r, \theta)$$

   con

   $$r = ((ac - bd)^2 + (ad + bc)^2)^{1/2} = (a^2c^2 + b^2d^2 - 2acbd + a^2d^2 + b^2c^2 + 2abcd)^{1/2} \Rightarrow$$

   $$r = ((a^2 + b^2)(c^2 + d^2))^{1/2} = r_1 r_2$$

   y

   $$\theta = \arctan\left(\frac{ad + bc}{ac - bd}\right),$$

con $\cos(\theta) = \dfrac{ac-bd}{r}$ y $\sin(\theta) = \dfrac{ad+bc}{r}$, como $\cos(\theta_1) = \dfrac{a}{r_1}$, $\cos(\theta_2) = \dfrac{c}{r_2}$, $\sin(\theta_1) = \dfrac{b}{r_1}$ y $\sin(\theta_2) = \dfrac{d}{r_2}$ tendremos que $\cos(\theta) = \cos(\theta_1)\cos(\theta_2) - \sin(\theta_1)\sin(\theta_2) = \cos(\theta_1+\theta_2)$ y $\sin(\theta) = \cos(\theta_1)\sin(\theta_2) + \sin(\theta_1)\cos(\theta_2)$, por lo tanto $\mod(\theta_1+\theta_2, 2\pi) = \theta$.

Así que, finalmente, $f((a,b)*(c,d)) = f((a,b)) \circ f((c,d))$

5. Sea $G_1 = (GL_2(\mathbb{R}), \cdot)$, donde $GL_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_{2\times 2}(\mathbb{R}) \ / \ ad-bc \neq 0 \right\}$ y $\cdot$ es el producto de matrices habitual, y sea $G_2 = (\mathbb{R}^*, \cdot)$, definimos la aplicación

$$\begin{array}{rccc} f: & GL_2(\mathbb{R}) & \longrightarrow & \mathbb{R}^* \\ & \begin{pmatrix} a & b \\ c & d \end{pmatrix} & \longrightarrow & ac-bd \end{array}$$

Por lo tanto es una aplicación que calcula el determinante de la matriz. Como sabemos que $f(A\cdot B) = \det(A\cdot B) = \det(A)\cdot\det(B) = f(A)\cdot f(B)$, se cumplirá que $f$ es un homomorfismo

6. Consideremos las rotaciones de un triángulo equilátero en el plano y fuera del plano, de modo que el resultado es otro triángulo equilátero. Tendremos que existen tres rotaciones posibles en el plano (de $0^o$, de $180^o$ y de $270^o$ en sentido de las agujas del reloj con eje perpendicular al plano del triángulo), que denominaremos $I, r_1$ y $r_2$. Además tendremos otras tres rotaciones fuera del plano, que corresponden a giros de $180^o$ con tres posibles ejes en el plano del triángulo y pasando cada uno de ellos por un vértice y perpediculares al lado opuesto al vértice. Dichas rotaciones las denominaremos $t_1$, $t_2$ y $t_3$, en función del vértice por el cual pase el eje de rotación.
La tabla de dichas rotaciones es:

| | $I$ | $r_1$ | $r_2$ | $t_1$ | $t_2$ | $t_3$ |
|---|---|---|---|---|---|---|
| $I$ | $I$ | $r_1$ | $r_2$ | $t_1$ | $t_2$ | $t_3$ |
| $r_1$ | $r_1$ | $r_2$ | $I$ | $t_2$ | $t_3$ | $t_1$ |
| $r_2$ | $r_2$ | $I$ | $r_1$ | $t_3$ | $t_1$ | $t_2$ |
| $t_1$ | $t_1$ | $t_3$ | $t_2$ | $I$ | $r_2$ | $r_1$ |
| $t_2$ | $t_2$ | $t_1$ | $t_3$ | $r_1$ | $I$ | $r_2$ |
| $t_3$ | $t_3$ | $t_2$ | $t_1$ | $r_2$ | $r_1$ | $I$ |

Como se puede ver, este conjunto de rotaciones con la operación composición de rotaciones forman un grupo que se denomina *grupo diedral de orden 3,* $D_3$. Dentro de dicho

grupo diedral se encuentra el subgrupo de las rotaciones en el plano, $C_3$, que es un grupo cíclico de orden 3.

Además se puede comprobar que dicho grupo diedral es isomorfo del grupo de las permutaciones de 3 elementos, $S_3$.

Todo grupo diedral de orden $n$ es isomorfo del grupo de las permutaciones de $n$ elementos, también denominado *grupo de simetría* de orden $n$.

*Proposición:* Sea $(G_1, \circ)$ un grupo y $(G_2, \cdot)$ sólo un conjunto con una operación interna. Si la aplicación $f : G_1 \longrightarrow G_2$ cumple que $f(g_1 \circ g_2) = f(g_1) \cdot f(g_2)\ \forall g_1, g_2 \in G_1$, entonces $(f(G_1), \cdot)$ es un grupo, donde $f(G_1) = \{x \in G_2 \ / \ x = f(g) \text{ con } g \in G_1\}$

*Demostración:*

Demostramos que cumple las propiedades de grupo:

1. Operación interna: Si $f(g_1), f(g_2) \in f(G_1) \Rightarrow f(g_1) \cdot f(g_2) \in f(G_1)$ ya que $f(g_1) \cdot f(g_2) = f(g_1 \circ g_2)$ y $g_1 \circ g_2 \in G_1$ ya que $(G_1, \circ)$ es un grupo.

2. Propiedad asociativa:

   $(f(g_1) \cdot f(g_2)) \cdot f(g_3) = f(g_1 \circ g_2) \cdot f(g_3) = f((g_1 \circ g_2) \circ g_3) = f(g_1 \circ (g_2 \circ g_3)) = f(g_1) \cdot f(g_2 \circ g_3) = f(g_1) \cdot (f(g_2) \cdot f(g_3))$

3. Elemento neutro:

   $\forall f(g) \in f(G_1)\ \exists \widetilde{e} \in f(G_1) \ / \ f(g) \cdot \widetilde{e} = f(g)$ ya que si tomamos $\widetilde{e} = f(e)$ con $e$ elemento neutro de $(G_1, \circ)$ tendremos que $f(g) \cdot \widetilde{e} = f(g) \cdot f(e) = f(g \circ e) = f(g)$

4. Elemento inverso:

   $\forall f(g) \in f(G_1)\ \exists h \in f(G_1) \ / \ f(g) \cdot h = \widetilde{e}$, ya que si tomamos $h = f(g^{-1})$ donde $g^{-1} \in G_1$ es el inverso de $g$ en $(G_1, \circ)$ tendremos que $f(g) \cdot h = f(g) \cdot f(g^{-1}) = f(g \circ g^{-1}) = f(e) = \widetilde{e}$

Por lo tanto $(f(G_1), \cdot)$ es un grupo.

*Proposición:* Si $f$ es un homomorfismo entre los grupos $(G_1, \circ)$ y $(G_2, \cdot)$ se tiene que:

1. $f(e_1) = e_2$, donde $e_1$ es el elemento neutro de $G_1$ y $e_2$ es el elemento neutro de $G_2$

2. $f(g^{-1}) = (f(g))^{-1}\ \forall g \in G_1$

*Demostración:*

1. $f(g_1) \cdot f(e_1) = f(g_1 \circ e_1) = f(g_1) = f(g_1) \cdot e_2 \Rightarrow f(e_1) = e_2$
2. $\forall g \in G_1 \; f(g) \cdot f(g^{-1}) = f(g \circ g^{-1}) = f(e_1) = e_2 \Rightarrow f(g^{-1}) = (f(g))^{-1}$

***Ejemplo:***

Sean los grupos $G_1 = (\mathbb{R}, +)$ y $G_2 = (\mathbb{R}^*, \cdot)$ y sea $f(x) = \exp(x)$
Tendremos que $e_1 = 0 \Rightarrow f(e_1) = f(0) = \exp(0) = 1 = e_2$
Además $\forall x \in G_1 \; x^{-1} = -x \Rightarrow f(x^{-1}) = f(-x) = \exp(-x) = \dfrac{1}{\exp(x)} = \dfrac{1}{f(x)} = (f(x))^{-1}$

*Proposición:* Sea $f$ un homomorfismo entre los grupos $G_1$ y $G_2$, tendremos que:

1. Si $H_1$ es un subgrupo de $G_1$, entonces $f(H_1)$ es un subgrupo de $G_2$
2. Si $H_2$ es un subgrupo de $G_2$, entonces $f^{-1}(H_2)$ es un subgrupo de $G_1$

*Demostración:*

1. $H_1$ es subgrupo de $G_1 \Rightarrow \forall x, y \in H_1 \; xy^{-1} \in H_1$

   Además $f(H_1) \neq$ ya que $e_1 \in H_1 \Rightarrow f(e_1) = e_2 \in f(H_1)$

   Tomemos $X, Y \in f(H_1) \Rightarrow \exists x, y \in H_1 \; / \; X = f(x), Y = f(y) \Rightarrow XY^{-1} = f(x)(f(y))^{-1} = f(x)f(y^{-1}) = f(xy^{-1}) \in f(H_1)$ ya que $xy^{-1} \in H_1$

2. Sean $x, y \in f^{-1}(H_2) \Rightarrow \exists X, Y \in H_2 \; / \; f^{-1}(X) = x, f^{-1}(Y) = y$, o lo que es lo mismo $f(x) = X, f(y) = Y$, por lo tanto, $XY^{-1} \in H_2$ ya que $H_2$ es un subgrupo, entonces si $XY^{-1} = Z \Rightarrow \exists z \in f^{-1}(H_2) \; / \; z = f^{-1}(Z) \Rightarrow Z = XY^{-1} = f(x)(f(y))^{-1} = f(x)f(y^{-1}) = f(xy^{-1}) = f(z) \Rightarrow xy^{-1} \in f^{-1}(H_2)$

***Ejemplo:***

Sean $G_1 = (GL_2(\mathbb{R}), \cdot)$ con $GL_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_{2\times 2}(\mathbb{R}) \; / \; ad - bc \neq 0 \right\}$,
$f(A) = ad - bc$ con $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ y $G_2 = (\mathbb{R}^*, \cdot)$

Tomemos el subconjunto $H = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \in \mathcal{M}_{2\times 2}(\mathbb{R}) \; / \; b \in \mathbb{R} \right\} \subset GL_2(R)$. Dicho subconjunto con la operación producto de matrices es subgrupo de $G_1$, ya que dadas las matrices

$A = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \in H$ y $B = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \in H$, tenemos que $B^{-1} = \begin{pmatrix} 1 & -b \\ 0 & 1 \end{pmatrix} \in H$ y además $AB^{-1} = \begin{pmatrix} 1 & a-b \\ 0 & 1 \end{pmatrix} \in H$

Por otro lado, dada una matriz $A = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \in H$ podemos construir el conjunto formado por todas las imagenes de matrices de $H$, y tendríamos $f(A) = 1 \cdot 1 - a \cdot 0 = 1 = e_2$, por lo tanto el conjunto $f(H) = \{e_2\}$ es subgrupo de $G_2$

## 3.2. Núcleo de un homomorfismo

### 3.2.1. Definición

Dado un homomorfismo $f$ entre los grupos $G_1$ y $G_2$, definimos el *núcleo* de $f$ como el conjunto $\ker(f) = \{x \in G_1 \ / \ f(x) = e_2\}$, donde $e_2$ es el elemento neutro de $G_2$

***Ejemplo:***

1. Sean $G_1 = (\mathbb{R}, +)$ y $G_2 = (\mathbb{R}^*, \cdot)$, con el homomorfismo $f(x) = \exp(x)$, tendremos que $\ker(f) = \{0\}$ ya que $\ker(f) = \{x \in G_1 \ / \ f(x) = 1\}$

2. Sean $G_1 = (GL_2(\mathbb{R}), \cdot)$ con $GL_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_{2\times 2}(\mathbb{R}) \ / \ ad - bc \neq 0 \right\}$ y $G_2 = (\mathbb{R}^*, \cdot)$, con $f(A) = ad - bc$ siendo $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.
   Tendremos que $\ker(f) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_{2\times 2}(\mathbb{R}) \ / \ ad - bc = 1 \right\}$, por lo tanto el núcleo serán la matrices de orden 2 con determinante igual a 1.

*Proposición:* Sea $f$ un homomorfismo entre los grupos $G_1$ y $G_2$, tendremos que:

1. el núcleo de $f$ es un subgrupo normal de $G_1$

2. $f$ es un monomorfismo si y sólo si $\ker(f) = \{e_1\}$, donde $e_1$ es el elemento neutro de $G_1$

*Demostración:*

1. Sean $x, y \in \ker(f) \Rightarrow f(xy^{-1}) = f(x)f(y^{-1}) = e_2(f(y))^{-1} = (f(y))^{-1} = e_2^{-1} = e_2 \Rightarrow xy^{-1} \in \ker(f)$, por lo tanto $\ker(f)$ es un subgrupo de $G_1$

   Además será normal si $\forall g \in G_1$ y $\forall x \in \ker(f)$ se cumple que $gxg^{-1} \in \ker(f)$. Vamos a comprobar si es cierto, para ello calculamos $f(gxg^{-1}) = f(g)f(x)f(g^{-1}) = f(g)e_2(f(g))^{-1} = f(g)(f(g))^{-1} = e_2$, por lo tanto $gxg^{-1} \in \ker(f)$, así que $\ker(f)$ es un subgrupo normal.

2. $\boxed{\Rightarrow}$

   Supongamos que $f$ es inyectiva, si $x \in \ker(f) \Rightarrow f(x) = e_2$. Además sabemos que $f(e_1) = e_2$, entonces, como $f$ es inyectiva si $f(x) = f(e_1) \Rightarrow x = e_1 \Rightarrow \ker(f) = \{e_1\}$

   $\boxed{\Leftarrow}$

   Supongamos que $\ker(f) = \{e_1\}$. Tomemos $f(x) = f(y) \Rightarrow f(x)(f(y))^{-1} = e_2 \Rightarrow f(x)f(y^{-1}) = e_2 \Rightarrow f(xy^{-1}) = e_2$. Como $\ker(f) = \{e_1\} \Rightarrow xy^{-1} = e_1 \Rightarrow x = y$, por lo tanto $f$ es inyectiva.

*Proposición:* Sea $f$ un homomorfismo entre los grupos $G_1$ y $G_2$, tendremos que

1. Si $H_2$ es un subgrupo normal de $G_2$, entonces $H_1 = f^{-1}(H_2)$ es un subgrupo normal de $G_1$

2. Si $H_1$ es un subgrupo normal de $G_1$ y $f$ es un epimorfismo, entonces $f(H_1)$ es un subgrupo normal de $G_2$

*Demostración:*

1. Si $H_2$ es un subgrupo normal de $G_2$ y $H_1 = f^{-1}(H_2)$, tendremos que $\forall g \in G_1$ y $\forall h_2 \in H_2 \Longrightarrow \exists h_1 \in H_1 \ / \ f(h_1) = h_2 \Rightarrow f(gh_1g^{-1}) = f(g)f(h_1)f(g^{-1}) = f(g)h_2(f(g))^{-1} \in H_2$ ya que $H_2$ es un subgrupo normal. Por lo tanto, $\exists h' \in H_1 \ / \ f(h') = f(g)h_2(f(g))^{-1} \Rightarrow h' = f^{-1}(f(g)h_2(f(g))^{-1}) \in H_1 \Rightarrow h' = gh_1g^{-1} \in H_1$, por lo que $H_1$ es normal.

2. Si $H_1$ es un subgrupo normal y $f$ es un epimorfismo, para demostrar que $f(H_1)$ sea un grupo normal de $G_2$ tendremos que demostrar que $\forall g_2 \in G_2$ se cumple que $g_2f(H_1)g_2^{-1} \in f(H_1)$

   Como $f$ es suprayectiva, tendremos que $\forall g_2 \in G_2 \ \exists g_1 \in G_1 \ / \ f(g_1) = g_2 \Rightarrow \forall h_1 \in H_1, \ g_2f(h_1)g_2^{-1} = f(g_1)f(h_1)(f(g))^{-1} = f(g_1)f(h_1)f(g_1^{-1}) = f(g_1h_1g_1^{-1})$. Como $H_1$ es normal, se cumple que $g_1h_1g_1^{-1} = h' \in H_1 \Rightarrow f(h') = f(g_1h_1g_1^{-1}) \in f(H_1)$. Por lo tanto el subgrupo $f(H_1)$ es subgrupo normal ya que $g_2f(H_1)g_2^{-1} \in f(H_1) \ \forall g_2 \in G_2$

*Proposición:* Sea $f$ un isomorfismo entre los grupos $G_1$ y $G_2$, se cumple que:

1. $G_1$ es abeliano $\Longleftrightarrow$ $G_2$ es abeliano
2. $G_1$ es cíclico $\Longleftrightarrow$ $G_2$ es cíclico

*Demostración:*

1. $\boxed{\Rightarrow}$

   Supongamos que $G_1$ es abeliano, entonces si $g_2, h_2 \in G_2$ como $f$ es suprayectiva (por ser isomorfismo) se cumplirá que $\exists g_1, h_1 \in G_1 \ / \ f(g_1) = g_2,\ f(h_1) = h_2 \Rightarrow g_2h_2 = f(g_1)f(h_1) = f(g_1h_1) =$*(como $G_1$ es abeliano)*$= f(h_1g_1) = f(h_1)f(g_1) = h_2g_2 \Rightarrow G_2$* es abeliano

   $\boxed{\Leftarrow}$

   Como $f$ es un isomorfismo, entonces $f^{-1}$ también lo será, por lo tanto, $\forall g_1, h_1 \in H_1$ podemos escribir $g_1 = f^{-1}(g_2),\ h_1 = f^{-1}(h_2)$ con $g_2, h_2 \in H_2 \Rightarrow g_1h_1 = f^{-1}(g_2)f^{-1}(h_2) =$ *(como $f^{-1}$ es un isomorfismo)*$= f^{-1}(g_2h_2) =$*(como $G_2$ es abeliano)*$= f^{-1}(h_2g_2) = f^{-1}(h_2)f^{-1}(g_2) = h_1g_1 \Rightarrow G_1$* es abeliano

2. $\boxed{\Rightarrow}$

   Supongamos que $G_1$ es cíclico, entonces $\exists x \in G_1 \ / \ \langle x \rangle = G_1 \Rightarrow$ si $g_2 \in G_2$, como $f$ es suprayectiva (por ser isomorfismo), tendremos que $f^{-1}(g_2) \in G_1 \Rightarrow f^{-1}(g_2) = g_1 = x^n \Rightarrow g_2 = f(x^n) = (f(x))^n \Rightarrow G_2$ es cíclico

   $\boxed{\Leftarrow}$

   Se demuestra igual aplicando el resultado a $f^{-1}$ (ya que $f$ es un isomorfismo).

## 3.3. Descomposición canónica de un homomorfismo

### 3.3.1. Homomorfismo canónico: definición

Si $H$ es un subgrupo normal de $G$, podemos considerar el grupo cociente $G/H$.
En este caso, la aplicación $\Pi : G \longrightarrow G/H$ tal que $\Pi(g) = gH$ es un homomorfismo suprayectivo que recibe el nombre de *homomorfismo canónico* con núcleo $H$.

*Demostración:*

Vamos a demostrar que la aplicación $\Pi$ definida anteriormente es un epimorfismo.

Será un homomorfismo ya que $\Pi(ab) = (ab)H = (aH) \cdot (bH) = \Pi(a) \cdot \Pi(b)$

Además es una aplicación suprayectiva por construcción, ya que el codominio es el conjunto de elementos que tienen contraimagen.

### 3.3.2. Descomposición canónica

Dado que el núcleo de una aplicación $f$ siempre define un subgrupo normal $\mathcal{N}_f$ de un grupo dado $G$, siempre podemos definir el homomorfismo canónico de núcleo $\mathcal{N}_f$ de la siguiente manera $f : G \longrightarrow G/\mathcal{N}_f$ tal que $f(g) = g\mathcal{N}_f$. Dicho homomorfismo canónico se denomina *descomposición canónica del homomorfismo.*

*Proposición:* Dados dos grupos $G_1$ y $G_2$, cualquier homomorfismo $f$ entre $G_1$ y $G_2$ puede descomponerse en dos homomorfismo $\Pi$ y $\Gamma$, de modo que $f = \Gamma \circ \Pi$ con $\Pi : G_1 \longrightarrow G_1/\mathcal{N}_f$ de modo que $\Pi(g) = g\mathcal{N}_f$ y con $\Gamma : G_1/\mathcal{N}_f \longrightarrow G_2$ de modo que $\Gamma(g\mathcal{N}_f) = f(g)$, siendo $\Pi$ suprayectiva y $\Gamma$ inyectiva

$$\overset{\overset{f}{\longrightarrow}}{G_1 \xrightarrow{\Pi} G_1/\mathcal{N}_f \xrightarrow{\Gamma} G_2}$$

*Demostración:*

Ya hemos visto que $\Pi$ es un homomorfismo suprayectivo ya que $\mathcal{N}_f$ es un subgrupo normal.

Por otro lado, es fácil ver que $\Gamma$ es un aplicación ya que cumple que si $x\mathcal{N}_f = y\mathcal{N}_f \Rightarrow f(x) = f(y)$. Esto es debido a que si $x\mathcal{N}_f = y\mathcal{N}_f \Rightarrow y = xn$ con $n \in \mathcal{N}_f \Rightarrow$ *(como $f$ es aplicación)*$\Rightarrow f(y) = f(xn) \Rightarrow f(y) = f(x)f(n) = f(x)e = f(x)$. Por lo tanto $\Gamma : G_1/\mathcal{N}_f \longrightarrow G_2$ con $\Gamma(x\mathcal{N}_f) = f(x)$ es una aplicación.

Además será un homomorfismo ya que $\Gamma(x\mathcal{N}_f \cdot y\mathcal{N}_f) = \Gamma((xy)\mathcal{N}_f) = f(xy) = f(x)f(y) = \Gamma(x\mathcal{N}_f)\Gamma(x\mathcal{N}_f)$

Por otro lado $\Gamma$ es inyectivo ya que si tomamos un elemento $x\mathcal{N}_f$ del núcleo de $\Gamma$, tendremos que $\Gamma(x\mathcal{N}_f) = e_2 \Rightarrow f(x) = e_2 \Rightarrow x \in \mathcal{N}_f \Rightarrow x\mathcal{N}_f = \mathcal{N}_f$, por lo tanto vemos que el único elemento que pertenece al núcleo de $\Gamma$ es el elemento neutro del grupo $G_1/\mathcal{N}_f$, esto es

$\mathcal{N}_f$, por lo tanto $\Gamma$ es inyectiva ($\ker(\Gamma) = \{\mathcal{N}_f\}$)

*Observaciones:*

1. Si $f$ es suprayectiva, entonces $\Gamma$ también lo es, ya que si $y \in G_2$, podemos tomar $x \in G_1 \ / \ f(x) = y \Rightarrow \Gamma(x\mathcal{N}_f) = f(x) = y \Rightarrow \forall y \in G_2 \ \exists x\mathcal{N}_f \in G_1/\mathcal{N}_f \ / \ \Gamma(x\mathcal{N}_f) = y$
2. Sea $f : G_1 \longrightarrow G_2$ un homomorfismo suprayectivo entre los grupos $G_1$ y $G_2$ con núcleo $\mathcal{N}_f$, tendremos que $G_1/\mathcal{N}_f$ es isomorfo a $G_2$

***Ejemplos:***

1. Sea $\begin{array}{rcl} f: (\mathbb{R},+) & \longrightarrow & (\mathbb{R}^*,\cdot) \\ x & \longrightarrow & \exp(x) \end{array}$, tendremos que $\mathcal{N}_f = \{x \ / \ f(x) = 1\} = \{0\}$ por tanto $(\mathbb{R},+)/\mathcal{N}_f = \{x\mathcal{N}_f \ / \ x \in \mathbb{R}\} = \{\{x\} \ / \ x \in \mathbb{R}\} = \mathbb{R}$

   $\begin{array}{rcl} \Pi: \mathbb{R} & \longrightarrow & (\mathbb{R},+)/\mathcal{N}_f \\ x & \longrightarrow & \{x\} \end{array}$, $\begin{array}{rcl} \Gamma: (\mathbb{R},+)/\mathcal{N}_f & \longrightarrow & (\mathbb{R}^*,\cdot) \\ \{x\} & \longrightarrow & \exp(x) \end{array}$
2. Sean $G_1 = (GL_2(\mathbb{R}),\cdot)$, $G_2 = (\mathbb{R}^*,\cdot)$ con $GL_2(\mathbb{R}) = \left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_{2\times 2}(\mathbb{R}) \ / \ |A| = ad - bc \neq 0 \right\}$ y $f(A) = ad - bc = |A|$ donde $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

   En este caso $\mathcal{N}_f = \ker(f) = \left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{M}_{2\times 2}(\mathbb{R}) \ / \ |A| = ad - bc = 1 \right\}$, por lo tanto $G_1/\mathcal{N}_f = \{M\mathcal{N}_f \ / \ M \in GL_2(\mathbb{R})\}$.
   Como $|B| = 1 \ \forall B \in \mathcal{N}_f = \ker(f)$, tendremos que $M\mathcal{N}_f = \{A \in \mathcal{M}_{2\times 2}(\mathbb{R}) \ / \ |A| = |M|\}$, por lo tanto $G_1/\mathcal{N}_f = \{\{A \in \mathcal{M}_{2\times 2}(\mathbb{R}) \ / \ |A| = m\}, \forall m \in \mathbb{R}\}$, o sea, el conjunto cociente está construído con conjuntos de matrices que tienen el mismo determinante.

   $\begin{array}{rcl} \Pi: G_1 & \longrightarrow & G_1/\mathcal{N}_f \\ M & \longrightarrow & \{A \in \mathcal{M}_{2\times 2}(\mathbb{R}) \ / \ |A| = |M|\} = M\mathcal{N}_f \end{array}$, $\begin{array}{rcl} \Gamma: G_1/\mathcal{N}_f & \longrightarrow & (\mathbb{R}^*,\cdot) \\ M\mathcal{N}_f & \longrightarrow & |M| \end{array}$

$$\begin{array}{ccccc} & & \text{suprayectiva} & & \text{biyectiva} \\ G_1 & & \xrightarrow{\Pi} & & G_1/\mathcal{N}_f \xrightarrow{\Gamma} \mathbb{R}^* \\ & & & \overset{\text{suprayectiva}}{\overset{f}{\longrightarrow}} & \\ M & \to & \text{matrices con determinante } |M| & \to & |M| \end{array}$$

3. Tomemos $G_1 = (\mathbb{R}, +)$ y $G_2 = (GL_2(\mathbb{R}), \cdot)$ con $f(x) = \begin{pmatrix} \cos(x) & \sin(x) \\ -\sin(x) & \cos(x) \end{pmatrix}$, tendremos que $\mathcal{N}_f = \ker(f) = \{2\pi k,\ k \in \mathbb{Z}\}$, por lo tanto,
$G_1/\mathcal{N}_f = \{\{x + 2\pi k,\ k \in \mathbb{Z}\},\ 0 \leq x < 2\pi\}$

$$\begin{array}{rccl} \Pi: & G_1 & \longrightarrow & G_1/\mathcal{N}_f \\ & y & \longrightarrow & \{x + 2\pi k \text{ tal que } k \in \mathbb{Z}, 0 \leq x < 2\pi, y = x + 2\pi n \text{ con } n \in \mathbb{Z}\} = x\mathcal{N}_f = y\mathcal{N}_f \end{array}$$

$$\begin{array}{rccl} \Gamma: & G_1/\mathcal{N}_f & \longrightarrow & (GL_2(\mathbb{R}), \cdot) \\ & x\mathcal{N}_f & \longrightarrow & \begin{pmatrix} \cos(x) & \sin(x) \\ -\sin(x) & \cos(x) \end{pmatrix} \end{array}$$

# Capítulo 4

# Anillos y Cuerpos. Homomorfismos entre Anillos

## 4.1. Anillos y Cuerpos

### 4.1.1. Anillos

Se denomina *anillo* a un conjunto $A$ dotado de dos operaciones binarias cerradas, que denominaremos por convención suma y producto y representaremos por $+$ y $\cdot$, respectivamente, que cumplen las siguientes propiedades:

i. $(A, +)$ es un grupo abeliano.

ii. El producto $\cdot$ es asociativo.

iii. Se cumple la propiedad distributiva

$$a \cdot (b + c) = a \cdot b + a \cdot c, \ (b + c) \cdot a = b \cdot a + c \cdot a, \quad \forall\, a, b, c \in A$$

*Definiciones:*

1. El inverso respecto a la suma se llama *opuesto*. Por notación, al opuesto de un elemento dado $a$ lo representaremos por $-a$.

2. El elemento neutro de la suma lo denotaremos por 0 y lo denominaremos *elemento cero*.

3. Si el producto es conmutativo, se dice que $(A, +, \cdot)$ es un *anillo conmutativo*.

4. Si existe un elemento, que denotaremos 1, tal que

$$a \cdot 1 = 1 \cdot a = a, \quad \forall\, a \in A$$

diremos que $(A, +, \cdot)$ es un *anillo con unidad.*
En este caso, el elemento 1 recibe el nombre de *elemento unidad.* Dicho elemento unidad es único.

*Demostración:*
Si $a, b, c \in A$ y verifican que $a \cdot b = a$ y $a \cdot c = a$ tendremos que $a \cdot b = a \cdot c \ \ \forall a \in A$, por lo tanto $b = c = 1$

***Ejemplos:***

- $(\mathbb{Z}, +, \cdot)$ es un anillo conmutativo con unidad.
- $(2\mathbb{Z}, +, \cdot)$ es un anillo conmutativo sin unidad.
- Las matrices de orden $n$ con coeficientes reales $(\mathcal{M}_n(\mathbb{R}), +, \cdot)$ es un anillo no conmutativo con unidad.

### 4.1.2. Elementos Invertibles y Anillos de División

*Definiciones:*

1. Sea $(A, +, \cdot)$ un anillo con unidad 1 y $1 \neq 0$. Un elemento $a$ de $A$ se dice que es *invertible* si existe un elemento $b \in A$ tal que $a \cdot b = b \cdot a = 1$.

   *Observación:*

   Si $a$ es un elemento invertible de un anillo, entonces $b$ también lo es.
   Por notación, si existe el inverso de un elemento $a$ lo denotaremos por $a^{-1}$.
   Si el inverso existe es único.

   *Demostración:*
   Si $a, b, c \in A$ y $a \cdot b = a \cdot c = b \cdot a = c \cdot a = 1$, tendremos que $c = c \cdot \overbrace{(a \cdot b)}^{=1} =$*(por asociatividad del producto, ya que es un anillo)*$= (c \cdot a) \cdot b = 1 \cdot b = b \Rightarrow c = b$

2. Al conjunto de los elementos invertibles de $A$ lo denotaremos por $U(A)$.

3. Los elementos invertibles de un anillo $(A, +, \cdot)$ se llaman *unidades de A.*

***Ejemplos:*** $U(\mathbb{Z}) = \{\pm 1\}$, $U(\mathbb{Z}_{12}) = \{[1], [5], [7], [11]\}$, $U(\mathbb{Z}_5) = \{[1], [2], [3], [4]\}$.

*Proposición:*
Sea $(A, +, \cdot)$ un anillo con unidad. Si $U(A)$ es el conjunto de los elementos invertibles de $A$, entonces $(U(A), \cdot)$ es un grupo.

*Demostración:*

1. La asociatividad se cumple siempre ya que son elementos de un anillo.
2. Los elementos de $U(A)$ tienen inverso.
3. $1 \in U(A)$ ya que $1 \cdot 1 = 1$ (el 1 es su propio inverso), por lo tanto tiene elemento neutro.
4. Si $a, b \in U(A) \Rightarrow a \cdot b \in U(A)$, a que $(a \cdot b) \cdot (a \cdot b)^{-1} = (a \cdot b) \cdot (b^{-1} \cdot a^{-1}) = a \cdot (b \cdot b^{-1}) \cdot a^{-1} = a \cdot a^{-1} = 1$, por lo tanto $(a \cdot b)$ tiene inverso y al tener inverso pertenece a $U(A)$, por lo que la operación es cerrada.

***Ejemplos:***

- Dadas las matrices de orden $n$ con la suma y el producto de matrices, $(\mathcal{M}_n(\mathbb{R}), +, \cdot)$, son un anillo con unidad.
  La unidades de $\mathcal{M}_n(\mathbb{R})$ serán aquellas matrices que tienen determinante distinto de cero $GL_n(\mathbb{R}) = \{A \in \mathcal{M}_n(\mathbb{R}) \text{ tal que } |A| \neq 0\}$
  $(GL_n(\mathbb{R}), \cdot)$ es un grupo.
- Los enteros de Gauss están definidos por $\mathbb{Z}[i] = \{a + bi \in \mathbb{C} \text{ tal que } a, b \in \mathbb{Z}\} \in \mathbb{C}$. Dicho conjunto con la suma y el producto de número complejos forman un anillo unitario conmutativo.
  En este caso tendremos que las unidades están dadas por $U(\mathbb{Z}[i]) = \{1, -1, i, -i\}$, dado que estos son los elementos que tienen inverso.
- El anillo $(\mathbb{Z}, +, \cdot)$ es unitario y conmutativo. Para este anillo tenemos que $U(\mathbb{Z}) = \{1, -1\}$

*Definición:*
Un anillo unitario $(A, +, \cdot)$, con $1 \neq 0$, se dice que es un *anillo de división* si $U(A) = A^* = A - \{0\}$.

*Propiedades:*

Sea $(A, +, \cdot)$ un anillo, se tiene que:

1. $\forall a \in A \;\; a \cdot 0 = 0 \cdot a = 0$, ya que $a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$.

2. Si $(-a)$ es el elemento opuesto de $a$ para la suma se tiene que:

$$(-a) \cdot b = -(a \cdot b), \;\; a \cdot (-b) = -(a \cdot b) \text{ y } (-a) \cdot (-b) = a \cdot b, \;\; \forall a, b \in A$$

   En efecto, como $(a \cdot b) + (-a) \cdot b = (a - a) \cdot b = 0 \cdot b = 0$, se tiene que $(-a) \cdot b$ es el opuesto de $(a \cdot b)$...

3. Si $(A, +, \cdot)$ es un anillo unitario, se tiene que $0 \neq 1$, ya que $\forall a \in A, a \cdot 0 = 0$ y $a \cdot 1 = a$

4. Si $(A, +, \cdot)$ es un anillo unitario, se tiene que $U(A) \subset A^*$, donde $A^*$ denota el conjunto $A$ excluído el elemento neutro de la suma.

Además en $\mathbb{Z}$ también se tiene que si $a \cdot b = 0$, entonces ó $a = 0$ ó $b = 0$, sin embargo esto no se cumple en general, por ejemplo, en $\mathbb{Z}_{12}$, $[3] \cdot [4] = [0]$ y $[3] \neq 0$ y $[4] \neq 0$.

### 4.1.3. Cuerpos

Un anillo conmutativo con unidad $(A, +, \cdot)$ se dice que es un *cuerpo* si el conjunto $A^*$, formado por todos los elementos de $A$ excepto el neutro de la suma, es un grupo con respecto a la segunda operación.

Por lo tanto $(A, +, \cdot)$ es un cuerpo si $(A, +, \cdot)$ es un anillo conmutativo y $(A^*, \cdot)$ es un grupo. De aquí se puede deducir que si $(A, +, \cdot)$ es un cuerpo, $(A, +, \cdot)$ es un anillo conmutativo con unidad y además $U(A) = A^*$.

***Ejemplos:*** $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, $(\mathbb{Z}_p, +, \cdot)$ con $p$ primo, son cuerpos.

*Observación:*
Un cuerpo se suele decir que es un *anillo de división conmutativo*.

***Ejemplo:***
Existen anillos de división que no son conmutativos, como el anillo de los *cuaterniones*.

Sea

$$H(\mathbb{R}) = \{a + bi + cj + dk \text{ tal que } a, b, c, d \in \mathbb{R}\}$$

donde $i^2 = j^2 = k^2 = -1$, $i1 = 1i = i$, $j1 = 1j = j$, $k1 = 1k = k$, $ij = k$, $jk = i$ y $ki = j$, estas condiciones implican que $ji = -k$, $kj = -i$, $ik = -j$.

La suma se define componente a componente:

$$(a+bi+cj+dk)+(r+si+tj+uk)=(a+r)+(b+s)i+(c+t)j+(d+u)k$$

y el producto se realiza multiplicando los términos y utilizando las relaciones anteriores:

$$\begin{aligned}(a+bi+cj+dk)\cdot(r+si+tj+uk)= \quad & ar-bs-ct-du+(as+br+cu-dt)i+\\ & (at+cr+ds-bu)j+(au+dr+bt-cs)k\end{aligned}$$

$(H(\mathbb{R}),+,\cdot)$ es un anillo. Además todo elemento es invertible, por lo que es un anillo de división, pero no un cuerpo, al no ser conmutativo.

### 4.1.4. Divisores de cero

Si $(A,+,\cdot)$ es un anillo, un elemento $a\in A$ con $a\neq 0$, se dice que es un *divisor de cero* si existe un elemento $b\in A$, $b\neq 0$, tal que $a\cdot b=0$ ó $b\cdot a=0$.

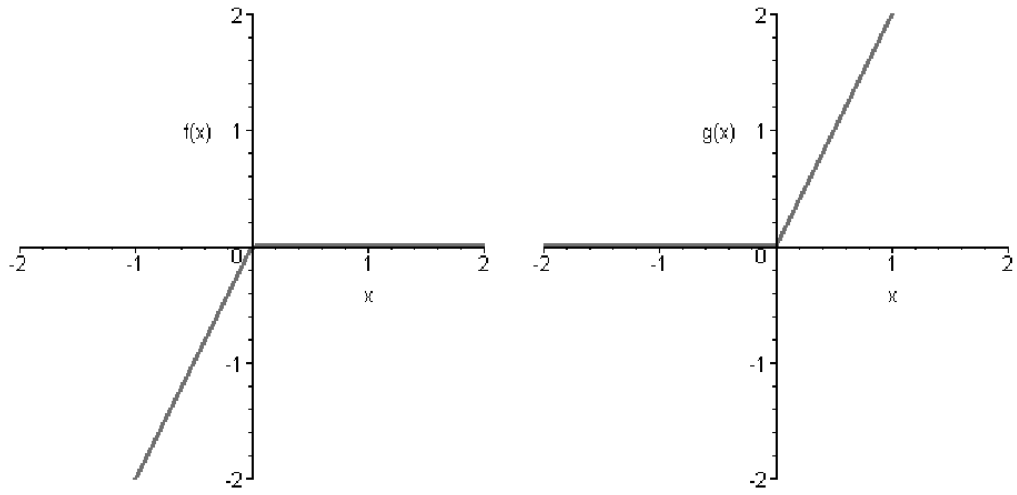
***Ejemplos:***

- En $\mathbb{Z}_{12}$, hemos visto que [3] y [4] son divisores de cero, también lo son [2], [6], [8], [9] y [10].

- Sea el conjunto de las funciones reales continuas de variable real $A=\mathcal{C}(\mathbb{R},\mathbb{R})$, se cumple que:

$$\left.\begin{array}{l}(f+g)(x)=f(x)+g(x)\\(f\cdot g)(x)=f(x)\cdot g(x)\end{array}\right\}\ \text{con } f,g\in A, x\in\mathbb{R}$$

  $(A,+,\cdot)$ es un anillo conmutativo (ya que $f\cdot g=g\cdot f$) unitario (ya que $i(x)=1$ es la unidad).
  Tomemos $f(x)=x-|x|$ y $g(x)=x+|x|$ por lo tanto




sin embargo $(f \cdot g)(x) = 0, \forall x \in \mathbb{R}$, así que $f(x)$ y $g(x)$ son divisores de cero.

*Observación:*

Un cuerpo $C$ no tiene divisores de cero, ya que si $a \neq 0$ y $a \cdot b = 0$, multiplicando por $a^{-1}$, el inverso de $a$, se tiene que $b = (a^{-1} \cdot a) \cdot b = a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0 = 0$.

Aunque hay anillos que sin ser cuerpos tampoco tienen divisores de cero.

Cuando un elemento de un anillo no es un divisor de cero se cumplen en él las propiedades cancelativas respecto al producto.

*Proposición:*

En un anillo $(A, +, \cdot)$, sea $a$ un elemento de $A$ que no es un divisor de cero. Entonces:

i. Si $a \cdot b = a \cdot c$, con $b, c \in A$ entonces $b = c$.

ii. Si $b \cdot a = c \cdot a$, con $b, c \in A$ entonces $b = c$.

*Demostración:*

i. Supongamos que $a \cdot b = a \cdot c$; esto es equivalente a $a \cdot (b - c) = 0$. Como $a$ no es un divisor de cero, $b - c$ tiene que ser 0, de donde se deduce el resultado deseado.

ii. Análogo.

### 4.1.5. Dominio de integridad

Un anillo $A$ sin divisores de cero se denomina *dominio de integridad.*

*Observación:*
El producto de dos elementos no nulos del anillo no es nunca 0 en un dominio de integridad.

***Ejemplos:***

- $(\mathbb{Z}, +, \cdot)$ es un dominio de integridad.
- Todos los cuerpos son dominios de integridad.
- $(\mathbb{Z}_p, +, \cdot)$ es dominio de integridad si $p$ es primo.
- Sea $\mathcal{M}_2(\mathbb{R})$ el conjunto de todas las matrices de orden 2 con coeficientes reales. Con la suma y el producto este conjunto es un anillo. Pero no es dominio de integridad, ya que
$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$
- Los enteros de Gauss $\mathbb{Z}[i] = \{a + bi \in \mathbb{C} \text{ tal que } a, b \in \mathbb{Z}\}$ con la suma y el producto de números complejos es un anillo y un dominio de integridad, ya que si $x = a + bi, y = c + di \in \mathbb{Z}[i]$ y se cumple que $x \cdot y = (a + bi) \cdot (c + di) = 0 \Rightarrow x = 0$ ó $y = 0$

## 4.2. Subanillos e ideales

### 4.2.1. Subanillos

Sea subconjunto $S \subset A$ con $(A, +, \cdot)$ un anillo, se dice que $(S, +, \cdot)$ es un *subanillo de* $(A, +, \cdot)$, si $(S, +)$ es un subgrupo de $(A, +)$ y el producto restringido a $S$ es cerrado, o de forma equivalente, la suma y el producto son operaciones cerradas en $S$, y $(S, +, \cdot)$ es un anillo.

***Ejemplos:*** $(\mathbb{Z}, +, \cdot)$ es subanillo de $(\mathbb{Q}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$ es subanillo de $(\mathbb{R}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ es subanillo de $(\mathbb{C}, +, \cdot)$

### 4.2.2. Subcuerpos

Sea $S \subset C$ con $(C, +, \cdot)$ un cuerpo, se dice que $(S, +, \cdot)$ es un *subcuerpo* de $(C, +, \cdot)$ si $(S, +)$ es un subgrupo de $(C, +)$ y $(S^*, \cdot)$ es un subgrupo de $(C^*, \cdot)$. De manera equivalente,

la suma y el producto son operaciones cerradas en $S$, y $(S,+,\cdot)$ es un cuerpo.
O sea, $(S,+,\cdot)$ es subcuerpo de $(C,+,\cdot)$ si $S \subset C$ con $S \neq$ y $x-y \in S$, $\forall x,y \in S$ y $x \cdot y^{-1} \in S$, $\forall x,y \in S^*$

***Ejemplos:***

- $(\mathbb{Q},+,\cdot)$ es subcuerpo de $(\mathbb{R},+,\cdot)$, $(\mathbb{R},+,\cdot)$ es subcuerpo de $(\mathbb{C},+,\cdot)$
- Si $D$ es un entero que no sea cuadrado perfecto, entonces $\mathbb{Q}[D] = \{a+b\sqrt{D}$ tal que $a,b \in \mathbb{Q}\}$ es un cuerpo respecto a la suma y al producto y $\mathbb{Q}$ es un subcuerpo de $\mathbb{Q}[D]$ y $\mathbb{Z}[D]$ es un subanillo, $\mathbb{Q}[D]$ es un subcuerpo de $\mathbb{R}$

*Observaciones:*

1. Los subanillos de un anillo unitario no tienen por qué ser unitarios e incluso si son unitarios, el elemento neutro del subanillo puede ser distinto del elemento neutro del anillo.
2. Los divisores de cero de un subanillo lo son también del anillo, pero puede sucederr que un anillo tenga divisores de cero y el subanillo no.

***Ejemplo:***
Sea $\mathbb{R} \times \mathbb{R}$ con las operaciones:

$$(a,b)+(c,d) = (a+c, b+d) \text{ y } (a,b)\cdot(c,d) = (a\cdot c, b\cdot d),\ \ \forall (a,b),(c,d) \in \mathbb{R}\times\mathbb{R}$$

y sea $H = \{(h,0)$ tal que $h \in \mathbb{R}\} \subset \mathbb{R}\times\mathbb{R}$

i. $(\mathbb{R}\times\mathbb{R},+,\cdot)$ es un anillo unitario

ii. $(H,+,\cdot)$ es un subanillo unitario

iii. Los elementos $(n,0) \in \mathbb{R}\times\mathbb{R}$ son divisores de cero en $(\mathbb{R}\times\mathbb{R},+,\cdot)$ pero no en $(H,+,\cdot)$

*Demostración:*

i. $(\mathbb{R}\times\mathbb{R},+)$ es un grupo conmutativo, con elemento cero $(0,0)$.
$((\mathbb{R}\times\mathbb{R})^*,\cdot)$ cumple que:

1. Es una operación interna pues $(a\cdot c, b\cdot d) \in \mathbb{R}\times\mathbb{R}$
2. Es asociativa ya que $[(a,b)\cdot(c,d)]\cdot(e,f) = (a\cdot c, b\cdot d)\cdot(e,f) = (a\cdot c\cdot e, b\cdot d\cdot f) = (a,b)\cdot(c\cdot e, d\cdot f) = (a,b)\cdot[(c,d)\cdot(e,f)]$

3. Tiene elemento neutro, que es $(1,1)$, ya que $(a,b)\cdot(1,1)=(a,b)$
4. Tiene elemento unidad, ya que $\forall(a,b)\in(\mathbb{R}\times\mathbb{R})^*$ se cumple que $(a,b)\cdot\left(\frac{1}{a},\frac{1}{b}\right)=(1,1)$

Por lo tanto, $(\mathbb{R}\times\mathbb{R},+,\cdot)$ es un anillo conmutativo con unidad

ii. $(H,+,\cdot)$ es un subanillo unitario, ya que:

1. Sean $(a,0),(b,0)\in H$, entonces $(a,0)-(b,0)=(a-b,0)\in H$, por lo que $(H,+)$ es un subgrupo de $(\mathbb{R}\times\mathbb{R},+)$
2. Sean $(a,0),(b,0)\in H$, entonces $(a,0)\cdot(b,0)=(a\cdot b,0)\in H$, por lo que $\cdot$ es una operación cerrada en $H$

Por lo tanto $(H,+,\cdot)$ es subanillo. Además tiene unidad, ya que $(1,0)\in H$ cumple que $(a,0)\cdot(1,0)=(a,0),\ \forall(a,0)\in H$, por lo tanto$(1,0)$ es el elemento neutro del producto en $H$, pero no del producto en $(\mathbb{R}\times\mathbb{R})^*$. Esto significa que $(H,+,\cdot)$ es subanillo unitario.

iii. Los elementos de la forma $(a,0)$ con $a\neq 0$ son divisores de cero en $\mathbb{R}\times\mathbb{R}$, ya que $(a,0)\cdot(0,b)=(0,0)$ aunque $a,b\neq 0$. Sin embargo, en $H$ un elemento de la forma $(a,0)$ con $a\neq 0$ no es divisor de cero, ya que si $(a,0)\cdot(b,0)=(0,0)$ y $a\neq 0$, entonces $b=0$

### 4.2.3. Ideales

Un subanillo $I$ de un anillo $A$ unitario conmutativo se dice que es un *ideal* de $A$ si para todo $i\in I$ y para todo $a\in A$ se cumple que $i\cdot a\in I$ y $a\cdot i\in I$.

Por lo tanto los ideales, además de ser subanillos, se caracterizan por la propiedad de absorción que poseen respecto al producto: al multiplicar un elemento cualquiera del anillo por un elemento del ideal, el resultado pertenece de nuevo al ideal. Esto hace que para probar que un subconjunto de un anillo es un ideal baste con demostrar que:

1. Para todo $i,j\in I$ se cumple que $i-j\in I$.
2. Para todo $i\in I$ y para todo $a\in A$ se cumple que $i\cdot a\in I$ y $a\cdot i\in I$.

***Ejemplos:***

- El subanillo trivial $\{0\}$ de cualquier anillo $A$ es ideal, ya que $a\cdot 0=0\cdot a=0,\ \forall a\in A$
- Otro subanillo trivial es el propio $A$ y también es ideal de si mismo.

- Dado $r \in [0,1]$, el subconjunto $M_r$ del conjunto de funciones definido por $\mathcal{C}[0,1] = \{f : [0,1] \longrightarrow \mathbb{R}$ tal que $f$ es continua$\}$ con $(f+g)(x) = f(x)+g(x), (f \cdot g)(x) = f(x) \cdot g(x)$, definiendo $M_r = \{f \in \mathcal{C}[0,1]$ tal que $f(r) = 0\}$ tenemos que $M_r$ es un ideal de $\mathcal{C}[0,1]$
- El conjunto $m\mathbb{Z}$ con $m \in \mathbb{N}$ definido como $m\mathbb{Z} = \{m\,k$ tal que $k \in \mathbb{Z}\}$ es un ideal de $(\mathbb{Z}, +, \cdot)$ ya que se cumple que:
  1. $\forall i = m\,k, j = m\,k' \in m\mathbb{Z},\ i - j = m\,(k - k') \in m\mathbb{Z}$ ya que $k - k' \in \mathbb{Z}$
  2. $\forall i = m\,k \in m\mathbb{Z}, \forall a \in \mathbb{Z},\ i\,a = m\,(k\,a) \in m\mathbb{Z}$ ya que $k\,a \in \mathbb{Z}$

*Observaciones:*

1. Si $A$ es un anillo con unidad 1 e $I$ es un ideal de $A$ y se tiene que $1 \in I$, entonces $I$ coincide con $A$.
   *Demostración:*
   $\forall a \in A, a \cdot 1 = a \in I \Rightarrow A = I$

2. Si $A$ es un anillo de división, los únicos ideales de $A$ son $\{0\}$ y el propio $A$ (los ideales impropios).
   *Demostración:*
   Sea $I$ un ideal de $A$ con $I \neq \{0\}$ y sea $i \in I$ con $i \neq 0$, tomamos $a = i^{-1} \in A$, por lo tanto $i \cdot a = i \cdot i^{-1} \in I$ ya que $I$ es ideal, además $i \cdot i^{-1} = 1 \in I \Rightarrow I = A$ por la propiedad anterior.

*Teorema:*
Un cuerpo $(C, +, \cdot)$ conmutativo no tiene ideales propios.
*Demostración:*
Sea $I$ ideal de $C$ con $I \neq \{0\}$, si $a \neq 0 \in I \Rightarrow x \cdot a \in I \,\forall\, x \in C$. Tomemos $x = a^{-1}$ (sabemos que $a^{-1}$ existe ya que $C$ es un cuerpo), entonces $x \cdot a = a^{-1} \cdot a = 1 \in I \Rightarrow I = C$

*Observación:*

1. El papel de los ideales en un anillo es similar al de los subgrupos normales en la teoría de grupos.

2. Si $I$ es un ideal de un anillo $A$, la relación

$$x \mathcal{R} y \Leftrightarrow x - y \in I \text{ para } x, y \in A$$

es una relación de equivalencia.

*Demostración:*

*a*) Propiedad reflexiva: $x\mathcal{R}x$, ya que $x - x = 0 \in I$

*b*) Propiedad simétrica: $x\mathcal{R}y \Rightarrow y\mathcal{R}x$, ya que si $x - y \in I \Rightarrow -(x - y) = y - x \in I$ porque es un subgrupo aditivo de $A$ y, por tanto, si un elemento pertenece a $I$ su opuesto también pertenece a $I$.

*c*) Propiedad transitiva: $x\mathcal{R}y, y\mathcal{R}z \Rightarrow x\mathcal{R}z$, ya que si $x - y \in I, y - z \in I \Rightarrow x - y + y - z = x - z \in I$ porque $I$ es un subgrupo aditivo y la suma de dos elementos del subgrupo es otro elemento del subgrupo.

De hecho $(I, +)$ es un subgrupo normal de $A$. Por lo tanto podemos definir el grupo cociente $A/I$ respecto a la suma de clases

$$[r + I] + [s + I] = [(r + s) + I]$$

donde la clase de equivalencia de $x \in A$ será

$$[x + I] = \{x + a \text{ tal que } a \in I\}$$

Expresaremos la relación $[x + I] = [y + I]$ como $x = y \mod I$

En analogía con la suma de clases podemos escribir el producto de clases como

$$[r + I] \cdot [s + I] = [(r \cdot s) + I]$$

siempre y cuando este bien definida, es decir, sea independiente del representante.

### 4.2.4. Anillo de clases de restos módulo $I$

Sea $I$ un ideal de un anillo $A$; la suma y el producto de clases en el cociente $A/I$ están bien definidas, y con estas, $A/I$ posee estructura de anillo. Dicho anillo recibe el nombre de *anillo de clases de restos módulo* $I$.

*Demostración:*

- $(A/I, +)$ es un grupo con respecto a la suma de clases definida anteriormente dado que $(I, +)$ es un subgrupo normal de $(A, +)$ y, por tanto, como quedó demostrado en el tema de Grupos (tema 2) podemos definir el conjunto conciente $A/I$, que con la suma de clases tiene estructura de grupo.

- Vamos a ver que en el conjunto cociente $A/I$ el producto de clases definido anteriormente, $[x+I]\cdot[y+I]=[(x\cdot y)+I],\ \forall\, x,y\in A$, es independiente de los representantes elegidos, y por tanto está bien definido, ya que si

$$\left.\begin{array}{l}[x+I]=[x'+I]\\ [y+I]=[y'+I]\end{array}\right\}\Rightarrow [x+I]\cdot[y+I]=[(x\cdot y)+I]=[(x'\cdot y')+I],$$

puesto que

$$x\cdot y-x'\cdot y'=x\cdot y-x\cdot y'+x\cdot y'-x'\cdot y'=x\cdot(y-y')+(x-x')\cdot y'$$

y como $y-y'\in I$ y $x-x'\in I$ ya que $[y+I]=[y'+I]$ y $[x+I]=[x'+I]$ tendremos que

$$x\cdot y-x'\cdot y'=x\cdot y''+x''\cdot y',$$

como $y''\in I\Rightarrow x\cdot y''\in I$ y como $x''\in I\Rightarrow x''\cdot y'\in I$ por definición de ideal, por tanto $x\cdot y''+x''\cdot y'=a+b$ con $a,b\in I$. Como $(I,+)$ es un grupo aditivo $a+b\in I$, así que $x\cdot y-x'\cdot y'\in I$ y por tanto $x\cdot y$ y $x'\cdot y'$ definen la misma clase de equivalencia.

Como las operaciones suma y producto de clases están bien definidas es fácil demostrar que los elementos de $A/I$, esto es, las clases $[x+I]$ tal que $x\in A$, forman estructura de anillo puesto que $A$ tiene estructura de anillo.

*Observación:*

Supongamos que $I$ es un ideal de un anillo $A$, y que $I\neq A$. Es fácil comprobar que si $A$ es conmutativo, también lo es $A/I$, y que si 1 es el elemento unidad de $A$, $[1+I]$ es el elemento unidad de $A/I$.

***Ejemplo:***

En el anillo $(\mathbb{Z},+,\cdot)$ podemos definir una relación de equivalecia dados $a,b\in\mathbb{Z}$, de modo que $a\mathcal{R}b\Leftrightarrow a-b=k\cdot m$ para algún $k\in\mathbb{Z}$ con $m\in\mathbb{N}$.

Hemos visto que $m\mathbb{Z}$ será un ideal de $(\mathbb{Z},+,\cdot)$. La relación de equivalencia que hemos definido es lo mismo que decir que $a-b\in I=m\mathbb{Z}$.

Podemos definir el conjunto cociente $\mathbb{Z}_m=\mathbb{Z}/(m\mathbb{Z})=\mathbb{Z}/I$ que estará formado por las clases de equivalencia de la forma:

$$\overline{a}=\{b\in\mathbb{Z}\text{ tal que }b-a=m\,k\text{ con }k\in\mathbb{Z}\}=\{b\in\mathbb{Z}\text{ tal que }b=a\ \text{ mód }m\}$$

Por lo tanto, las clases de equivalencia de $\mathbb{Z}_m$ serán $\mathbb{Z}_m=\{\overline{0},\overline{1},\overline{2},\ldots,\overline{m-1}\}$, que son las clases de restos módulo $m$.

Por ejemplo, si $m=4\Rightarrow\mathbb{Z}_4=\{\overline{0},\overline{1},\overline{2},\overline{3}\}$ con $\overline{0}=\{b\in\mathbb{Z}\text{ tal que }b=4\,k,\ k\in\mathbb{Z}\}=\{0,\pm4,\pm8,\ldots\}$, $\overline{1}=\{b\in\mathbb{Z}\text{ tal que }b=4\,k+1,\ k\in\mathbb{Z}\}=\{1,5,9,-3,-7,\ldots\}$, ....

*Observaciones:*

1. $(\mathbb{Z}_n, +)$ es cíclico, ya que $\overbrace{\overline{1}+\overline{1}+\cdots+\overline{1}}^{(n}= \overline{n} = \overline{0}$
2. $-\overline{1} = \overline{(n-1)}$ ya que $\overline{0} = \overline{1} - \overline{1} = \overline{1} + \overline{(n-1)} = \overline{n}$, así que $-\overline{1} = \overline{(n-1)}$

### 4.2.5. Ideales generados

Dado un anillo $A$ y un subconjunto $S \subset A$, el *ideal generado por* $S$, que denotaremos por $< S >$, se define como el mínimo ideal que contiene a $S$, esto es, el ideal $I$ tal que $S \subset I$ y si $J$ es otro ideal, se cumple que si $S \subset J$, entonces $I \subset J$.

*Proposición:*
Sea $A$ un anillo conmutativo con unidad y $S$ un subconjunto de $A$. El ideal generado por $S$ es

$$< S >= \{r_1 \cdot s_1 + \cdots + r_n \cdot s_n \text{ tal que } r_i \in A, s_i \in S, n \in \mathbb{N}\}$$

*Demostración:*
Sea $I = \{r_1 \cdot s_1 + \cdots + r_n \cdot s_n \text{ tal que } r_i \in A, s_i \in S, n \in \mathbb{N}\}$, como $s_i = 1 \cdot s_i \ \ \forall s_i \in S \Rightarrow S \subset I$.
Además si $J$ es un ideal que contiene a $S$ y $s_i \in S$, entonces $r_i \cdot s_i \in J \ \ \forall r_i \in A$, por definición de ideal. Del mismo modo cualquier combinación lineal del tipo $r_1 \cdot s_1 + \cdots + r_n \cdot s_n \in J \Rightarrow I \subset J$ para cualquier $J$ tal que $S \subset J$.
Falta demostrar que $I$ es un ideal, para ello tomamos

$$p = r_1 \cdot s_1 + \cdots + r_n \cdot s_n \in I$$
$$p' = r'_1 \cdot s_1 + \cdots + r'_n \cdot s_n \in I$$

se cumplirá que:

i. Es un grupo con respecto a la suma:
$p - p' = r_1 \cdot s_1 + \cdots + r_n \cdot s_n + (-r'_1 \cdot s_1) + \cdots + (-r'_n \cdot s_n) = (r_1 - r'_1) \cdot s_1 + \cdots + (r_n - r'_n) \cdot s_n = r''_1 \cdot s_1 + \cdots + r''_n \cdot s_n \in I$

ii. Cumple la propiedad de absorción con respecto al producto:
$\forall r \in A, \ r \cdot p = r \cdot (r_1 \cdot s_1 + \cdots + r_n \cdot s_n) = r \cdot r_1 \cdot s_1 + \cdots + r \cdot r_n \cdot s_n = r'_1 \cdot s_1 + \cdots + r'_n \cdot s_n \in I$

Por lo tanto, $I$ es un ideal.

***Ejemplo:***
Si $S = \{s\}$ tiene un sólo elemento, tendremos que $< S >=< s >= \{r \cdot s \text{ tal que } r \in A\} = As =$*(si $A$ es conmutativo)*$= sA$.

Por ejemplo, si $m \in \mathbb{Z} \Rightarrow < m >= \{m \cdot a \text{ tal que } a \in \mathbb{Z}\} = m\mathbb{Z}$

*Observación:*
Todos los ideales de $(\mathbb{Z}, +, \cdot)$ son de la forma $< m >= m\mathbb{Z}$

*Demostración:*
Sea $I$ un ideal de $(\mathbb{Z}, +, \cdot)$ y $m$ el menor entero positivo de $I$, entonces tendremos que $< m >= \{a \cdot m \text{ tal que } a \in \mathbb{Z}\} \subset I$, ya que $I$ es un ideal (y hemos visto que el generado por $m$ es el menor que contiene a $m$).
Además si $i \in I$ tendremos que $i = c \cdot m + r$ donde $c, m \in \mathbb{Z}$ y $0 \leq r < m$ y por tanto $r = i - c \cdot m \in I$ (ya que $i \in I, c \cdot m \in I$ porque $c \cdot m \in < m > \subset I$). Pero como $m$ es el menor entero positivo de $I$ (lo hemos elegido así), tendrá que cumplirse que $r = 0$, ya que $r$ no puede ser un entero positivo menor que $m$, así que $i = c \cdot m \in < m >$.
Por lo tanto, todo ideal del anillo $(\mathbb{Z}, +, \cdot)$ está generado por un sólo elemento.

### 4.2.6. Ideales primos

Un ideal $I$ de un anillo conmutativo $A$ es un *ideal primo* si dados dos elementos cualesquiera $a$ y $b$ de $A$ tales que $a \cdot b \in I$, se tiene que o bien $a \in I$ o bien $b \in I$.

***Ejemplos:***
Sea $p$ un número entero positivo primo y consideremos $p\mathbb{Z}$, que es un ideal de $(\mathbb{Z}, +, \cdot)$. Si $a$ y $b$ son dos números enteros tales que $a \cdot b \in p\mathbb{Z}$, entonces $p$ divide a $a \cdot b$ y como $p$ es primo, entonces $p$ divide a $a$ o $p$ divide a $b$, por lo tanto, o bien $a \in p\mathbb{Z}$ o bien $b \in p\mathbb{Z}$, así que $p\mathbb{Z}$ es un ideal primo de $\mathbb{Z}$.

- $3\mathbb{Z}$ es un ideal primo de $\mathbb{Z}$ ya que $\forall\, a, b \in \mathbb{Z}$ tal que $a \cdot b \in 3\mathbb{Z}$, por tanto, o bien $a = 3 \cdot s$ o bien $b = 3 \cdot s$ con $s \in \mathbb{Z}$

- $6\mathbb{Z}$ no es un ideal primo de $\mathbb{Z}$ ya que puede existir $a \in \mathbb{Z}$ y $b \in \mathbb{Z}$ tales que $a \cdot b \in 6\mathbb{Z}$ con $a \notin 6\mathbb{Z}$ y $b \notin 6\mathbb{Z}$, por ejemplo, si tomamos $a = 3$ y $b = 2$, tenemos $a \cdot b = 6 \in 6\mathbb{Z}$ pero $a = 3 \notin 6\mathbb{Z}$ y $b = 2 \notin 6\mathbb{Z}$

Una vez estudiado el anillo cociente $A/I$ podemos preguntarnos qué propiedades del ideal $I$ hacen que $A/I$ sea dominio de integridad.

*Proposición:*

Sea $A$ un anillo conmutativo e $I$ un ideal de $A$ con $I \neq A$. El anillo cociente $A/I$ es un dominio de integridad si y sólo si $I$ es un ideal primo de $A$.

*Demostración:*

- $\boxed{\Rightarrow}$

  $A/I$ dominio de integridad $\Rightarrow$ $I$ ideal primo de $A$:

  Tomamos $a, b \in A$ tal que $a \cdot b \in I \Rightarrow [a+I] \cdot [b+I] = [a \cdot b + I] = I$ (sabiendo que $I$ es el elemento neutro del anillo $A/I$). Como $A/I$ es dominio de integridad, entonces, o bien $[a+I] = I$ o bien $[b+I] = I$, por lo tanto, o bien $a \in I$ o bien $b \in I$, o sea, $I$ es un ideal primo.

- $\boxed{\Leftarrow}$

  $I$ es un ideal primo de $A \Rightarrow A/I$ es dominio de integridad:

  Sea $[a+I] \cdot [b+I] = I$ para un par de elementos $[a+I]$ y $[b+I]$ de $A/I$, por tanto $I = [a+I] \cdot [b+I] = [a \cdot b + I] \Rightarrow a \cdot b \in I$ y como $I$ es primo, tendremos que o bien $a \in I$ o bien $b \in I$, por tanto, o bien $[a+I] = I$ o bien $[b+I] = I$, o sea, $A/I$ es dominio de integridad.

### 4.2.7. Ideales maximales

Sea $A$ un anillo conmutativo con unidad, e $I$ un ideal de $A$ con $I \neq A$. El ideal $I$ se llama *maximal* si no existe otro ideal $J$ de $A$ tal que $I \subset J \subset A$ con $I \neq J$ y $J \neq A$.

Ahora, nos preguntamos cual es la condición que caracteriza a los ideales para que $A/I$ sea un cuerpo.

*Proposición:*
Sea $A$ un anillo conmutativo con unidad e $I$ un ideal de $A$. El anillo cociente $A/I$ es un cuerpo si y solo si $I$ es un ideal maximal.

*Proposición:*
Todo ideal maximal en un anillo conmutativo con unidad es un ideal primo.

*Demostración:*
Si $I$ es maximal, $A/I$ es un cuerpo, por lo que también es un dominio de integridad, y por tanto $I$ es primo.

## 4.3. Cuerpo de fracciones de un anillo

Hemos visto que todos los cuerpos son dominios de integridad, pero no todos los dominios de integridad son cuerpos. Sin embargo, a un dominio de integridad se le puede asociar un cuerpo.

Si $a$ y $b$ son dos elementos no nulos de un anillo cualquiera, la ecuación

$$a \cdot x = b$$

carece, en general, de solución dentro del anillo, y sin embargo, suele ser de interés el poder resolver dichas ecuaciones multiplicativas. En $\mathbb{Z}$, podemos solucionarlo si lo ampliamos hasta el conjunto $\mathbb{Q}$, que es un cuerpo en el que dichas ecuaciones tienen solución siempre y cuando $a$ y $b$ sean números enteros no nulos.

Veremos cómo este proceso de ampliación puede efectuarse sobre cualquier dominio de integridad conmutativo con unidad; nótese que al ser nuestro objetivo el ampliar el anillo de partida hasta un cuerpo, las condiciones impuestas sobre dicho anillo no pueden relajarse. El cuerpo al cual hemos ampliado nuestro anillo se denominará *cuerpo de las fracciones de un anillo*.

Hay que tener presente que un número racional es un par de números enteros $(a, b)$ escritos de la forma $\dfrac{a}{b}$ con $b \neq 0$.

Sea $A$ un dominio de integridad conmutativo con unidad 1. En el producto cartesiano

$$T = A \times A^* = \{(a, b) \text{ tal que } a \in A, b \in A^*\}$$

definimos la relación

$$(a, b)\mathcal{R}(c, d) \Leftrightarrow a \cdot d = b \cdot c$$

que es una relación de equivalencia, dado que cumple las propiedades:

1. Reflexiva: $(a, b)\mathcal{R}(a, b)$ ya que $a \cdot b = b \cdot a$
2. Simétrica: $(a, b)\mathcal{R}(a', b') \Rightarrow (a', b')\mathcal{R}(a, b)$ ya que si $a \cdot b' = b \cdot a' \Rightarrow a' \cdot b = b' \cdot a$
3. Transitiva: $(a, b)\mathcal{R}(a', b'), (a', b')\mathcal{R}(a'', b'') \Rightarrow (a, b)\mathcal{R}(a'', b'')$, ya que si

$$\left.\begin{array}{l} a \cdot b' = b \cdot a' \\ a' \cdot b'' = b' \cdot a'' \end{array}\right\} \quad \left.\begin{array}{l} a \cdot b' \cdot b'' = b \cdot a' \cdot b'' \\ a' \cdot b'' = b' \cdot a'' \end{array}\right\} \Rightarrow a \cdot b' \cdot b'' = b \cdot b' \cdot a'' \Rightarrow b' \cdot a \cdot b'' = b' \cdot b \cdot a'' \Rightarrow$$

$$\Rightarrow a \cdot b'' = b \cdot a''$$

La clase del elemento $(a,b) \in A \times A^*$ la simbolizamos mediante $[(a,b)]$ y al conjunto cociente de las clases de equivalencia lo denotaremos por $C = (A \times A^*)/\mathcal{R}$.

En $C$ definimos una suma y un producto como

$$[(a,b)] + [(c,d)] = [(ad+bc, bd)]$$

$$[(a,b)] \cdot [(c,d)] = [(a \cdot c, b \cdot d)]$$

Entonces $C$ es un cuerpo con las operaciones anteriores, $C$ será *el cuerpo de las fracciones del anillo* $A$.

*Demostración:*

1. Grupo aditivo:
   i. Operación cerrada: Por definición, se puede ver fácilmente que es una operación cerrada
   ii. Propiedad asociativa: $([x,y]+[x',y'])+[x'',y''] = [x\cdot y' + y\cdot x', y\cdot y'] + [x'',y''] = [(x\cdot y'+y\cdot x')\cdot y''+x''\cdot(y\cdot y'), (y\cdot y')\cdot y''] = [x\cdot(y'\cdot y'')+y\cdot(x'\cdot y''+x''\cdot y'), y\cdot(y'\cdot y'')] = [x,y]+[x'\cdot y''+y'\cdot x'', y'\cdot y''] = [x,y]+([x',y']+[x'',y''])$
   iii. Elemento neutro $e_0 = [0,a]$: $[x,y]+[0,a] = [x\cdot a + 0\cdot y, y\cdot a] = [a\cdot x, a\cdot y] = [x,y]$
   iv. Elemento opuesto $[x,y]_+^{-1} = [-x,y]$: $[x,y]+[-x,y] = [x\cdot y - x\cdot y, y\cdot y] = [0, y\cdot y] = e_0$

2. Grupo multiplicativo:
   i. Operación cerrada: Por definición, se puede ver fácilmente que es una operación cerrada
   ii. Propiedad asociativa: $([x,y]\cdot[x',y'])\cdot[x'',y''] = [x\cdot x', y\cdot y']\cdot[x'',y''] = = [(x\cdot x')\cdot x'', (y\cdot y')\cdot y''] = [x\cdot(x'\cdot x''), y\cdot(y'\cdot y'')] = [x,y]\cdot[x'\cdot x'', y'\cdot y''] = [x,y]\cdot([x',y']\cdot[x'',y''])$
   iii. Elemento neutro $e_1 = [a,a]$: $[x,y]\cdot[a,a] = [x\cdot a, y\cdot a] = [x,y]$
   iv. Elemento inverso $[x,y]^{-1} = [y,x]$: $[x,y]\cdot[y,x] = [x\cdot y, y\cdot x] = [a,a] = e_1$

3. Distributividad:
   $[x,y]\cdot([x',y']+[x'',y'']) = [x,y]\cdot[x'\cdot y''+y'\cdot x'', y'\cdot y''] = [x\cdot(x'\cdot y''+y'\cdot x''), y\cdot(y'\cdot y'')] = = [(x\cdot x')\cdot(y''\cdot y)+(x\cdot x'')\cdot(y'\cdot y), (y\cdot y')\cdot(y''\cdot y)] = [x\cdot x', y\cdot y'] + [x\cdot x'', y\cdot y''] = [x,y]\cdot[x',y'] + [x,y]\cdot[x'',y'']$

Por lo tanto, $C$ es un cuerpo y además es conmutativo ya que $[x,y]\cdot[x',y'] = [x',y']\cdot[x,y]$

***Ejemplo:***

A partir del anillo $(\mathbb{Z},+,\cdot)$ generamos un cuerpo $(\mathbb{Q},+,\cdot)$, donde $\mathbb{Q} = \mathbb{Z}\times\mathbb{Z}^*/\mathcal{R}$ es el conjunto de las clases de equivalencia con la relación definida antes

$$[a,b]\in\mathbb{Q}\Rightarrow[a,b] = \left\{(x,y) = \frac{x}{y} \text{ tal que } x\in\mathbb{Z}, y\in\mathbb{Z}^*, a\cdot y = b\cdot x\right\}$$

esto es, el conjunto de las fracciones equivalentes $\frac{a}{b} = \frac{x}{y}$

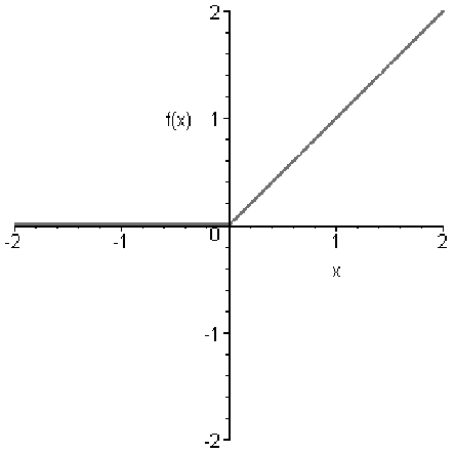
Además la suma de fracciones es $[x,y]+[x'+y'] = [x\cdot y'+y\cdot x', y\cdot y']$ o de forma equivalente $\frac{x}{y}+\frac{x'}{y'} = \frac{x\cdot y'+y\cdot x'}{y\cdot y'}$. Y el producto de fracciones es $[x,y]\cdot[x',y'] = [x\cdot x', y\cdot y']$ o de forma equivalente $\frac{x}{y}\cdot\frac{x'}{y'} = \frac{x\cdot x'}{y\cdot y'}$

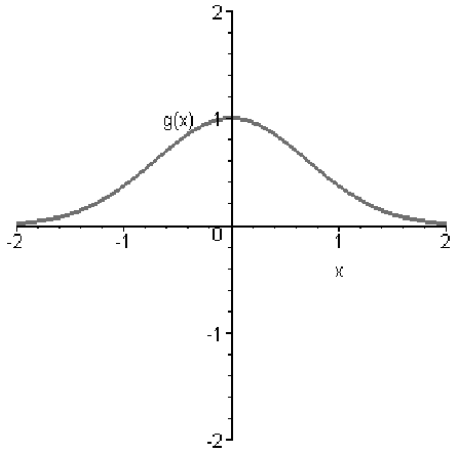
*Observaciones:*

1. Es necesario que $A$ sea un dominio de integridad conmutativo con unidad. Si no fuese así no podríamos definir una relación de equivalencia como la que hemos definido $(x,y)\mathcal{R}(x',y')\Leftrightarrow x\cdot y' = y\cdot x'$

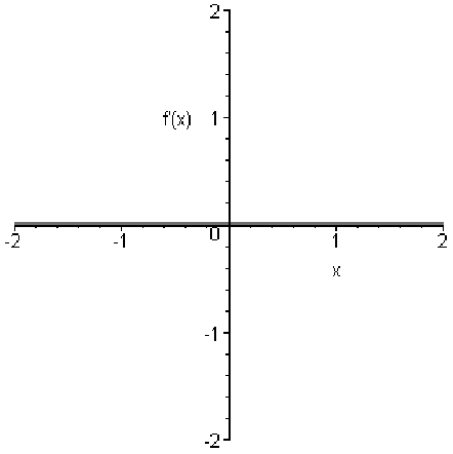
   ***Ejemplo:***

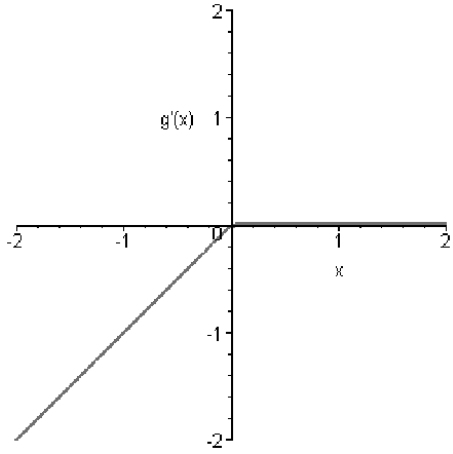
   El conjunto de funciones reales de variable real $\mathcal{C}(\mathbb{R},\mathbb{R})$ no es un dominio de integridad y según la relación anterior tendríamos que:



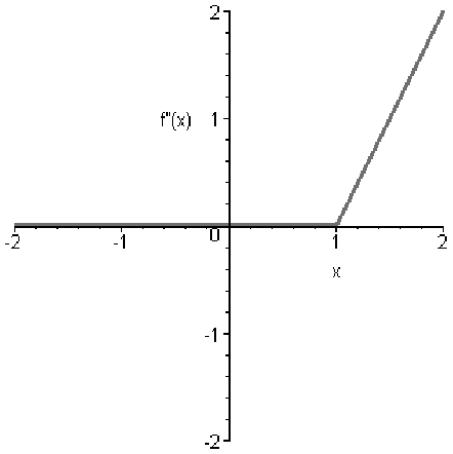



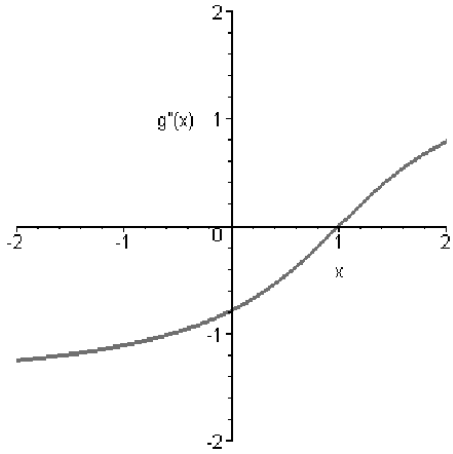

$(f, g)\mathcal{R}(f', g')$ ya que $f \cdot g' = g \cdot f'$




$(f', g')\mathcal{R}(f'', g'')$ ya que $f' \cdot g'' = g' \cdot f''$



Sin embargo, $(f,g)\not\mathcal{R}(f'',g'')$ ya que $f\cdot g''\neq f''\cdot g$, por lo tanto no es un relación de equivalencia ya que no cumple la propiedad transitiva.

2. En sentido estricto, $A$ no es un subanillo de $C$; sin embargo identificaremos $A$ con su anillo isomorfo $\mathcal{A}$ (ver sección 4.4.1), y con un cierto abuso del lenguaje, diremos que $C$ contiene a $A$ (esto equivale a identificar los enteros $\mathbb{Z}$ con el conjunto de las fracciones de la forma $\frac{p}{1}$, con $p\in\mathbb{Z}$).

## 4.4. Homomorfismos de anillos

### 4.4.1. Definiciones

Dados dos anillos $A$, $A'$, una función $f: A\to A'$ se dice que es un *homomorfismo de anillos* si para todo par de elementos $r$ y $s$ de $A$, se tiene que

$$f(r+s)=f(r)+f(s),\qquad f(rs)=f(r)f(s)$$

Observése que en particular $f$ es un homomorfismo entre los grupos $(A,+)$ y $(A',+)$.

Una aplicación $f$ entre dos cuerpos $C$ y $C'$ con las propiedades anteriores se dice que es un *homomorfismo de cuerpos*. En este caso, $f$ define un homomorfismo entre los grupos aditivos $(C,+)$ y $(C',+)$, y también entre los grupos multiplicativos $(C^*,\cdot)$ y $(C'^*,\cdot)$.

*Observación:*
Si un homomorfismo $f$ de anillos es una biyección, se dice que $f$ es un *isomorfismo de anillos*, y $A$ y $A'$ se dice que son *isomorfos*. En este caso $f^{-1}$ es también un isomorfismo de anillos.

*Definición:*
Un homomorfismo $f: A\longrightarrow B$ entre anillos unitarios conmutativos es:

i. Epimorfismo si $f$ es una aplicación suprayectiva

ii. Monomorfismo si $f$ es una aplicación inyectiva

iii. Isomorfismo si $f$ es una aplicación biyectiva

***Ejemplos:***

- La siguiente aplicación $f$ es un homomorfismo entre los cuerpos $(\mathbb{R}^2, +, \cdot)$ y $(\mathbb{C}, +, \cdot)$
  $f : \mathbb{R}^2 \longrightarrow \mathbb{C}$
  $(a, b) \longrightarrow a + bi$

  con $(a, b) + (c, d) = (a + c, b + d)$, $(a, b) \cdot (c, d) = (a \cdot d - b \cdot d, a \cdot d + b \cdot c)$

- La siguiente aplicación $\Pi$ es un homomorfismo entre anillos (homomorfismo canónico):
  $\Pi : A \longrightarrow A/I$
  $a \longrightarrow [a + I]$

  Dicho homomorfismo $\Pi$ es suprayectivo.

*Proposición:*
Sea $f : A \to A'$ un homomorfismo de anillos entonces se cumple:

1. $f(0_A) = 0_{A'}$ y $f(-x) = -f(x)$, donde $0_A$ y $0_{A'}$ son los elementos neutros de $A$ y $A'$, respectivamente, con respecto a la primera operación.

   *Demostración:*

   - $f(0_A) = f(0_A + 0_A) = f(0_A) + f(0_A) \Rightarrow f(0_A) = 0_{A'}$
   - $f(0_A) = f(x + (-x)) = f(x) + f(-x) \Rightarrow f(x) + f(-x) = 0_{A'} \Rightarrow f(-x) = -f(x)$

2. Si $A$ y $A'$ son anillos con unidad, $1_A$ y $1_{A'}$ respectivamente, y $\exists x \in A$ tal que $f(x) \in A'$ no es divisor de cero en $A'$, entonces $1_{A'} = f(1_A)$.

   *Demostración:*

   Tomemos $f(x) \cdot (f(1_A) - 1_{A'}) = f(x) \cdot f(1_A) - f(x) \cdot 1_{A'} = f(x \cdot 1_A) - f(x) = f(x) - f(x) = 0$, por lo tanto, como $f(x)$ no es divisor de cero, tendremos que $f(1_A) - 1_{A'} = 0$, por lo tanto $f(1_A) = 1_{A'}$

*Proposición:*
Sea $f : A \longrightarrow A'$ un homomorfismo entre anillos. Se tiene que:

1. Si $S$ es un subanillo de $A$, $f(S) = \{f(s)$ tal que $s \in S\}$ es un subanillo de $A'$.

2. Si $S'$ es un subanillo de $A'$, $f^{-1}(S') = \{s \in A$ tal que $f(s) \in S'\}$ es un subanillo de $A$.

*Demostración:*

1. En el tema anterior demostramos que si $f$ es un homomorfismo entre grupos $(A, +)$ y $(A', +)$, la imagen $f(S)$ de un subgrupo $S$ de $A$ es un subgrupo de $A'$. Como un subanillo es un subgrupo aditivo con el producto como operación cerrada dentro del

subanillo, para demostrar que en un homomorfismo de anillos la imagen $f(S)$ de un subanillo $S$ de $A$ es subanillo de $A'$, sólo tenemos que demostrar que el producto es una operación cerrada en $f(S)$.
Sean $x, y \in S$, tenemos que $f(x) \cdot f(y) = f(x \cdot y)$ por ser un homomorfismo. Como $x$ e $y$ son elementos del subanillo $S$, entonces $x \cdot y \in S$, por lo tanto $f(x \cdot y) \in f(S)$.
Por lo tanto $f(S)$ es subanillo de $A'$.

2. Igual que en el apartado anterior, en el tema anterior demostramos que si $S'$ es subgrupo de $(A', +)$, entonces $f^{-1}(S')$ es subgrupo de $(A, +)$. Por lo tanto, para demostrar que $f^{-1}(S')$ es subanillo de $A$, sólo tenemos que demostrar que en $f^{-1}$ el producto es una operación cerrada.
Para ello consideremos $x, y \in f^{-1}(S') \Rightarrow \exists X, Y \in S'$ tales que $f(x) = X, f(y) = Y$. Por lo tanto, $f(x) \cdot f(y) = f(x \cdot y) = X \cdot Y \in S'$, ya que $S'$ es un subanillo, así que $x \cdot y \in f^{-1}(S')$. Esto significa que $f^{-1}(S')$ es subanillo de $A$.

*Proposición:*
Sea $f : A \longrightarrow A'$ un homomorfismo entre anillos. Se tiene que:

1. Si $I'$ es un ideal de $A'$, $f^{-1}(I')$ es un ideal de $A$.

2. Si $f$ es sobreyectiva, si $I$ es un ideal de $A$, $f(I)$ es un ideal de $A'$.

*Demostración:*

1. Hemos demostrado anteriormente que la contraimagen de un subanillo de $A'$ es un subanillo de $A$, así que sólo tenemos que demostrar que la contraimagen de un ideal cumple la propiedad de absorción con el producto para que quede demostrado que la contraimagen de un ideal de $A'$ es un ideal de $A$.
Tomemos $x \in f^{-1}(I')$, por lo tanto $\exists X \in I'$ tal que $f(x) = X$. Se cumplirá que $\forall a \in A$ tendremos que $f(a) \in A'$ cumpliéndose que $f(a) \cdot X = f(a) \cdot f(x) \in I'$, ya que $I'$ es un ideal de $A'$. Como $f$ es un homomorfismo, $f(a) \cdot f(x) = f(a \cdot x) \in I'$, por lo tanto $a \cdot x \in f^{-1}(I')$, así que $f^{-1}(I')$ es un ideal de $A$.

2. Al igual que en el apartado anterior, para demostrar que la imagen de un ideal $I$ de $A$ es un ideal de $A'$ si $f$ es sobreyectiva, basta demostrar que en $f(I)$ el producto cumple la propiedad de absorción, ya que hemos demostrado anteriormente que es un subanillo.
Como $f$ es sobreyectiva, $\forall b \in A', \exists a \in A$ tal que $f(a) = b$. Por lo tanto, $\forall X \in f(I)$, tendremos que $\exists x \in I$ tal que $X = f(x)$, así que $b \cdot X = f(a) \cdot f(x) = f(a \cdot x)$. Como $I$ es un ideal $a \cdot x \in I$, así $f(a \cdot x) \in f(I)$, por lo que $f(I)$ es un ideal de $A'$.

### 4.4.2. Núcleo de un homomorfismo

Sea $f : A \longrightarrow A'$ un homomorfismo entre anillos unitarios conmutativos, se llama *núcleo de* $f$ y se denota por $\ker(f)$ al ideal de $A$ tal que $\ker(f) = \{x \in A \text{ tal que } f(x) = 0_{A'}\}$

Además $\ker(f) \neq$ ya que $f(0_A) = 0_{A'} \Rightarrow 0_A \in \ker(f)$

*Demostración:*
Vamos a probar que $\ker(f)$ es un ideal:

- Sean $x, y \in \ker(f) \Rightarrow f(x) = f(y) = 0 \Rightarrow f(x) - f(y) = f(x) + f(-y) = 0 \Rightarrow f(x-y) = 0 \Rightarrow x - y \in \ker(f)$, por lo tanto, $\ker(f)$ es un subgrupo aditivo.
- Sean $x \in \ker(f)$ y $a \in A$, entonces $f(a \cdot x) = f(a) \cdot f(x) = f(a) \cdot 0_{A'} = 0_{A'} \Rightarrow a \cdot x \in \ker(f)$, por lo tanto $\ker(f)$ cumple la propiedad de absorción.

Por lo tanto $\ker(f)$ es un ideal.

*Proposición:*
Un homomorfismo $f : A \longrightarrow A'$ es inyectivo si y solo si $\ker(f) = \{0_A\}$.

*Demostración:*
$\boxed{\Rightarrow}$
Supongamos que $f$ es inyectiva, si $x \in \ker(f) \Rightarrow f(x) = 0_{A'}$. Como además sabemos que $f(0_A) = 0_{A'}$, entonces, al ser $f$ inyectiva si $f(x) = f(0_A) \Rightarrow x = 0_A \Rightarrow \ker(f) = \{0_A\}$
$\boxed{\Leftarrow}$
Supongamos que $\ker(f) = \{0_A\}$. Tomemos $f(x) = f(y) \Rightarrow f(x) - f(y) = 0_{A'} \Rightarrow f(x) + f(-y) = 0_{A'} \Rightarrow f(x - y) = 0_{A'}$. Como $\ker(f) = \{0_A\} \Rightarrow x - y = 0_A \Rightarrow x = y$, por lo tanto $f$ es inyectiva.

*Teorema:*[Teorema Fundamental de Homomorfismos de Anillos]
Si $F : A \to A'$ es un homomorfismo de anillos y escribimos $N(f) = I_0$. La aplicación $f(a + I_0) = F(a)$ define un homomorfismo entre $A/I_0$ y $F(A)$. Si además $F$ es sobreyectiva, la aplicación $I \to F(I)$ es una biyección del conjunto de ideales de $A$ que contienen $I_0$ en el conjunto de ideales de $A'$.

Sea $A$ un anillo y $C$ el cuerpo de las fracciones del anillo, dicho cuerpo $C$ contiene a un subanillo isomorfo a $A$.

# Capítulo 5

# Anillos de Polinomios

## 5.1. Definiciones

- Sea $A$ un anillo conmutativo con unidad, el *conjunto* $A[x]$ *de polinomios* con coeficientes en $A$ se define como

  $A[x] = \{p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n \text{ tal que } a_i \in A, n \in \mathbb{N}\}$

- El *grado* $gr(p(x))$ de un polinomio $p(x) \in A[x]$ no nulo se define como el mayor número natural $n$ tal que $a_n \neq 0$, esto es, si $gr(p(x)) = n \Rightarrow a_n \neq 0, a_{n+1} = a_{n+2} = \cdots = 0$

- Un polinomio se llama *mónico* o *normalizado* si $a_n = 1$ siendo $gr(p(x)) = n$

## 5.2. Operaciones en $A[x]$

### 5.2.1. Igualdad de polinomios

Dos polinomios $p(x) = a_0 + a_1x + \cdots + a_nx^n$ y $q(x) = b_0 + b_1x + \cdots + b_mx^m$ son *iguales*, $p(x) = q(x)$, si $n = m$ y $a_i = b_i, \forall i \geq 0$

### 5.2.2. Suma de polinomios

Dados dos polinomios $p(x) = a_0 + a_1x + \cdots + a_nx^n$ y $q(x) = b_0 + b_1x + \cdots + b_mx^m$, denominamos *polinomio suma* al polinomio $s(x) = p(x) + q(x) = c_0 + c_1x + \cdots + c_px^p$ con $c_i = a_i + b_i, \forall i \geq 0$

### 5.2.3. Producto de polinomios

Dados dos polinomios $p(x) = a_0 + a_1x + \cdots + a_nx^n$ y $q(x) = b_0 + b_1x + \cdots + b_mx^m$, denominamos *polinomio producto* al polinomio $m(x) = p(x) \cdot q(x) = d_0 + d_1x + \cdots + d_px^p$ con $d_i = \sum_{\substack{j,k \\ j+k=i}} a_jb_k$

***Ejemplos:***

1. En $\mathbb{R}[x] : p(x) = 1 + 2x + x^2 + x^3$

   $q(x) = 2 + x^3$

   $p(x) + q(x) = 3 + 2x + x^2 + 2x^3$

   $p(x) \cdot q(x) = 2 + 4x + 2x^2 + 3x^3 + 2x^4 + x^5 + x^6$

2. En $\mathbb{Z}_3[x] : p(x) = \overline{1} + \overline{2}x^2 + \overline{1}x^3$

   $q(x) = \overline{1}x + \overline{2}x^3$

   $p(x) + q(x) = \overline{1} + \overline{1}x + \overline{2}x^2$

   $p(x) \cdot q(x) = \overline{1} + \overline{1}x + \overline{1}x^3 + \overline{1}x^4 + \overline{1}x^5 + \overline{2}x^6$

   *(Nota: Para simplificar la notación, a partir de ahora, las clases $\overline{n}$ del anillo $\mathbb{Z}_p$ las denotaremos como $\overline{n} \equiv n$)*

## 5.3. Anillo de polinomios

### 5.3.1. Anillo de polinomios $A[x]$: Definiciones

Sea $A$ un anillo conmutativo con unidad, el conjunto $A[x]$ con la suma y el producto definidos anteriormente, $(A[x], +, \cdot)$, es un anillo conmutativo con unidad y se denomina *anillo de polinomios de $A$*.

El elemento neutro de la suma de polinomios es $0(x) = 0_A$ (elemento cero)

El elemento neutro del producto de polinomios es $1(x) = 1_A$ (elemento identidad)

El elemento opuesto de $p(x) = a_0 + a_1x + \cdots + a_nx^n$ de la suma de polinomios es $-p(x) = -a_0 + (-a_1)x + \cdots + (-a_n)x^n$

El polinomio $0(x)$ no tiene grado y los polinomios de la forma $p(x) = a_0$ tienen grado 0

### 5.3.2. Características de un anillo de polinomios $A[x]$

*Proposición:*
Si $A$ es un dominio de integridad, su anillo de polinomios $A[x]$ también es un dominio de integridad.

*Demostración:*
Sea $A$ dominio de integridad y sean $p(x) = a_0 + a_1x + \cdots + a_nx^n \in A[x], q(x) = b_0+b_1x+\cdots+b_mx^m \in A[x] \Rightarrow p(x)\cdot q(x) = c_0+c_1x+\cdots+c_{n+m}x^{n+m} \neq 0$ con $c_{n+m} = a_nb_m \neq 0$ ya que $A$ es dominio de integridad.

*Proposición:*
Dados dos polinomios $p(x)$ y $q(x)$ pertenecientes a un dominio de integridad, tenemos que:

i. $gr(p(x) \cdot q(x)) = gr(p(x)) + gr(q(x))$

ii. $gr(p(x) + q(x)) \leq \text{máx}(gr(p(x)), gr(q(x)))$

*Demostración:*

i. Si $gr(p(x)) = n$ y $gr(q(x)) = m$, entonces $gr(p(x) \cdot q(x)) = m + n$ ya que $a_n \neq 0, b_m \neq 0 \Rightarrow a_n \cdot b_m \neq 0$ porque $A$ es dominio de integridad.

   Esto no sería cierto si no es un dominio de integridad, por ejemplo, $\mathbb{Z}_6[x]$ no lo es y podemos tomar $p(x) = 3x, q(x) = 2x \Rightarrow p(x)\cdot q(x) = 3x\cdot 2x = (3\cdot 2)x^2 = 6x^2 = 0x^2 = 0$

ii. Si $m \neq n \Rightarrow p(x) + q(x) \neq 0 \Rightarrow gr(p(x) + q(x)) = \text{máx}(m, n)$

   $$\left.\begin{array}{l}\text{Si } m = n \text{ y } a_n \neq -b_n \Rightarrow gr(p(x) + q(x)) = n \\ \text{Si } m = n \text{ y } a_n = -b_n \Rightarrow gr(p(x) + q(x)) < n\end{array}\right\} \Rightarrow gr(p(x) + q(x)) \leq n = \text{máx}(n, m)$$

   Por lo tanto, siempre se cumplirá que $gr(p(x) + q(x)) = \text{máx}(gr(p(x)), gr(q(x)))$

*Proposición:*
Si $A$ es un dominio de integridad conmutativo con unidad, los elementos invertibles de $A[x]$ coinciden con los elementos invertibles de $A$, $U(A) = U(A[x])$

*Demostración:*
Si $p(x) \neq 0, q(x) \neq 0$ y $p(x)\cdot q(x) = 1 \Rightarrow gr(p(x)+q(x)) = 0 \Rightarrow gr(p(x)) = 0, gr(q(x)) = 0$ ya que es un dominio de integridad, por lo tanto los únicos elementos invertibles de $A[x]$ son de la forma $p(x) = a_0$

***Ejemplo:*** $U(\mathbb{Z}) = \{\pm 1\} = U(\mathbb{Z}[x])$

### 5.3.3. Teorema de la división entera

Dado un cuerpo $C$, el conjunto $C[x]$ de polinomios con coeficientes en $C$ forma un anillo respecto a la suma y el producto de polinomios.
Además, $C[x]$ es un dominio de integridad conmutativo con unidad con la siguiente propiedad: dados $p(x) \neq 0$ y $q(x) \neq 0$ polinomios de $C[x]$ con $gr(p(x)) \geq gr(q(x)) \Rightarrow \exists s(x), r(x) \in C[x]$ tales que $p(x) = q(x) \cdot s(x) + r(x)$ con $gr(r(x)) < gr(q(x))$ ó $r(x) = 0$

Al polinomio $s(x)$ se le denomina polinomio *cociente* y al polinomio $r(x)$ se le denomina polinomio *resto*.

***Ejemplos:***

1. En $\mathbb{Q}[x]$ tomamos $p(x) = x^4 - x^2 + 1, q(x) = 2x^2 + 1 \Rightarrow p(x) = q(x) \cdot s(x) + r(x)$ con $s(x), r(x) \in \mathbb{Q}[x]$

$$\begin{array}{l|l} x^4 - x^2 + 1 & 2x^2 + 1 \\ \hline -x^4 - \frac{1}{2}x^2 & \frac{1}{2}x^2 - \frac{3}{4} \\ \hline -\frac{3}{2}x^2 + 1 & \\ \frac{3}{2}x^2 + \frac{3}{4} & \\ \hline \frac{7}{4} & \end{array}$$

   por lo tanto $s(x) = \frac{1}{2}x^2 - \frac{3}{4}, r(x) = \frac{7}{4}, gr(r(x)) = 0 < gr(q(x)) = 2$

   Esta propiedad está definida en $\mathbb{Q}[x]$ (ya que $\mathbb{Q}$ es un cuerpo), pero no en $\mathbb{Z}[x]$ (ya que $\mathbb{Z}$ no es cuerpo).

2. En $\mathbb{Z}_5[x]$ tomamos $p(x) = 3x^3 + 2x + 4, q(x) = 1x^2 + 2 \Rightarrow p(x) = q(x) \cdot s(x) + r(x)$ con $s(x), r(x) \in \mathbb{Z}_5[x]$

$$\begin{array}{l|l} 3x^3 + 2x + 4 & 1x^2 + 2 \\ \hline -3x^3 - 6x & 3x \\ \hline -4x + 4 & \\ \hline 1x + 4 & \end{array}$$

   por lo tanto $s(x) = 3x, r(x) = 1x + 4$

En general y salvo que se especifique lo contrario, vamos a restringirnos a anillos de polinomios $A[x]$ construídos a partir de cuerpos $A$.

*Teorema:*
Los polinomios cociente, $s(x)$, y resto, $r(x)$, son únicos.

*Demostración:*

Supongamos que $p(x) = s_1(x) \cdot q(x) + r_1(x) = s_2(x) \cdot q(x) + r_2(x)$, entonces tendremos que $0 = [s_1(x) - s_2(x)] \cdot q(x) + [r_1(x) - r_2(x)]$

Si $s_1(x) - s_2(x) \neq 0$ entonces el grado del primer término es mayor o igual que el grado de $q(x)$, pero el primer miembro de la ecuación no tiene grado, así que $gr([s_1(x) - s_2(x)] \cdot q(x)) = gr(r_1(x) - r_2(x)) \leq \text{máx}(gr(r_1(x)), gr(r_2(x))) < gr(q(x))$.
Esto está en contradicción con $gr([s_1(x) - s_2(x)] \cdot q(x)) \geq gr(q(x))$ que sería el caso si $s_1(x) - s_2(x) \neq 0$.
Por lo tanto, dado que llegamos a una contradicción tiene que cumplirse que $s_1(x) - s_2(x) = 0 \Rightarrow s_1(x) = s_2(x)$ y $r_1(x) - r_2(x) = 0 \Rightarrow r_1(x) = r_2(x)$

## 5.4. Ideales en $A[x]$

*Proposición:*

Si $I \neq \{0\}$ es un ideal de $A[x]$, entonces $I = \{f(x) \cdot g(x)$ tal que $f(x) \in A[x]\}$. Por lo tanto, los únicos ideales de $A[x]$ son los múltiplos de un determinado polinomio fijo.

Se llama polinomio generador del ideal $I$ al $g(x) \in A[x]$ tal que todos los elementos de $I$ son múltiplos de $g(x)$. Al ideal generado por $g(x)$ lo denotaremos por $[g(x)]$.

Si exigimos que $g(x)$ sea mónico, entonces $g(x)$ es único.

*Demostración:*

Sea $g(x) \in I$ un polinomio de grado mínimo y tomemos $s(x) \in I$ con $gr(s(x)) \geq gr(g(x))$. Por el teorema de la división tenemos que $s(x) = g(x) \cdot q(x) + r(x)$ con $r(x) = 0$ ó $gr(r(x)) < gr(g(x))$

Como $I$ es ideal, entonces $g(x) \cdot q(x) \in I, \forall q(x) \in A[x]$

Como $s(x) \in I$ y $g(x) \cdot q(x) \in I$, entonces $s(x) - g(x) \cdot q(x) \in I$, por tanto $r(x) \in I$

Pero hemos tomado $g(x)$ de grado mínimo en $I$, así que $r(x) = 0$ ya que no puede cumplir que $gr(r(x)) < gr(g(x))$

Por lo tanto, $\forall s(x) \in I$ podemos escribir $s(x) = g(x) \cdot q(x)$ con $q(x) \in A[x]$ y $g(x)$ de grado mínimo en $I$

## 5.5. Divisor de un polinomio

### 5.5.1. Definición

Sean $p(x), q(x) \in A[x]$ con $q(x) \neq 0$, se dice que $q(x)$ divide a $p(x)$ o que $q(x)$ es *divisor* de $p(x)$ si $p(x) = q(x) \cdot s(x)$ para algún $s(x) \in A[x]$. Se denota por $q(x)|p(x)$

***Ejemplos:***

1. En $\mathbb{R}[x]$ tomamos $p(x) = x^3 + x^2 + x + 1, q(x) = x + 1$, $q(x)$ divide a $p(x)$ ya que $\exists s(x) = x^2 + 1 \in \mathbb{R}[x]$ con $p(x) = q(x) \cdot s(x)$
2. En $\mathbb{Z}_3[x]$ tomamos $p(x) = 2x^3 + 1, q(x) = 2x + 1$, $q(x)$ divide a $p(x)$ ya que $\exists s(x) = x^2 + x + 1 \in \mathbb{Z}_3[x]$ con $p(x) = q(x) \cdot s(x)$

### 5.5.2. Máximo común divisor

*Definición:*
Se dice que $d(x) \in A[x]$, donde $A$ es un cuerpo, es el *máximo común divisor* de $p(x)$ y $q(x)$ si:

i. $d(x)$ es mónico

ii. $d(x)|p(x)$ y $d(x)|q(x)$

iii. si $\forall h(x) \in A[x]$ tal que $h(x)|p(x)$ y $h(x)|q(x)$, entonces $h(x)|d(x)$

El máximo común divisor de dos polinomios es el polinomio mónico de grado más alto que divide a ambos polinomios.

Exigimos que el máximo común divisor sea mónico para que sea único.

Si $A$ no fuese cuerpo no podríamos simplificar para obtener un polinomio mónico, ya que puede ocurrir que $A[x]$ tenga divisores de cero (y por tanto no se pueda simplificar).

*Proposición:*
Sean $p(x), q(x) \in A[x]$ dos polinomios fijos, entonces $I = \{p(x) \cdot r(x) + q(x) \cdot s(x), \forall r(x), s(x) \in A[x]\}$ es un ideal de $A[x]$ y lo denotaremos por $[p(x), q(x)]$

*Demostración:*
Dados $a_1(x) = p(x) \cdot r_1(x) + q(x) \cdot s_1(x), a_2(x) = p(x) \cdot r_2(x) + q(x) \cdot s_2(x) \in I$, tenemos que

1. $a_1(x) - a_2(x) = (r_1(x) - r_2(x)) \cdot q(x) + (s_1(x) - s_2(x)) \cdot q(x) \in I$
2. $\forall h(x) \in A[x], a_1(x) \cdot h(x) = p(x) \cdot (r_1(x) \cdot h(x)) + q(x) \cdot (s_1(x) \cdot h(x)) \in I$

Por lo tanto $I$ es un ideal.

*Observación:*
Si $I$ es un ideal generado por $p(x)$ y $q(x)$, o sea, $I = \{p(x) \cdot r(x) + q(x) \cdot s(x), \forall r(x), s(x) \in A[x]\}$, existirá un polinomio $d(x)$ tal que $I = [d(x)]$. Por tanto, $d(x)|p(x)$ y $d(x)|q(x)$ ya que $d(x)|p(x) \cdot r(x) + q(x) \cdot s(x)$. Además, como $d(x) \in I$, tendremos que $d(x) = p(x) \cdot a(x) + q(x) \cdot b(x)$. Si $h(x)$ divide a $p(x)$ y a $q(x)$ se cumplirá que $h(x)|d(x)$, ya que $p(x) = m_1(x) \cdot h(x), q(x) = m_2(x) \cdot h(x) \Rightarrow d(x) = h(x) \cdot [a(x) \cdot m_1(x) + b(x) \cdot m_2(x)]$. Por lo tanto, $d(x)$ es el máximo común divisor de $p(x)$ y $q(x)$.

### 5.5.3. Algoritmo de Euclides (cálculo del máximo común divisor)

*Proposición:*
Si $p(x) = q(x) \cdot s(x) + r(x)$ es la división entera de $p(x)$ por $q(x) \neq 0$, los ideales $[p(x), q(x)]$ y $[q(x), r(x)]$ coinciden.
*Demostración:*

1. Sea $f(x) \in [p(x), q(x)] \Rightarrow \exists a_1(x), a_2(x) \in A[x]$ tal que $f(x) = a_1(x) \cdot p(x) + a_2(x) \cdot q(x)$

   Como además $p(x) = q(x) \cdot s(x) + r(x) \Rightarrow f(x) = a_1(x) \cdot [q(x) \cdot s(x) + r(x)] + a_2(x) \cdot q(x) = [a_1(x) \cdot s(x) + a_2(x)] \cdot q(x) + a_1(x) \cdot r(x) \Rightarrow f(x) \in [q(x), r(x)] \Rightarrow [p(x), q(x)] \subset [q(x), r(x)]$

2. Por otro lado, si $g(x) \in [q(x), r(x)] \Rightarrow \exists b_1(x), b_2(x) \in A[x]$ tal que $g(x) = b_1(x) \cdot q(x) + b_2(x) \cdot r(x)$

   Como $p(x) = q(x) \cdot s(x) + r(x) \Rightarrow r(x) = p(x) - q(x) \cdot s(x) \Rightarrow g(x) = b_1(x) \cdot q(x) + b_2(x) \cdot [p(x) - q(x) \cdot s(x)] = b_2(x) \cdot p(x) + [b_1(x) - b_2(x) \cdot s(x)] \cdot q(x) \Rightarrow g(x) \in [p(x), q(x)] \Rightarrow [q(x), r(x)] \subset [p(x), q(x)]$

Teniendo en cuenta que $[p(x), q(x)] \subset [q(x), r(x)]$ y que $[q(x), r(x)] \subset [p(x), q(x)]$, entonces $[p(x), q(x)] = [q(x), r(x)]$

Si seguimos con este procedimiento llegamos a obtener resto nulo y, por tanto, el polinomio generador del ideal.
Además hemos visto que dicho polinomio es el máximo común divisor (si $d(x)$ es el máximo común divisor de $p(x)$ y $q(x)$, entonces $[d(x)] = [p(x), q(x)]$)

$p(x) = q(x) \cdot s_0(x) + r_0(x) \Rightarrow [p(x), q(x)] = [q(x), r_0(x)]$
$q(x) = r_0(x) \cdot s_1(x) + r_1(x) \Rightarrow [q(x), r_0(x)] = [r_0(x), r_1(x)]$
$r_0(x) = r_1(x) \cdot s_2(x) + r_2(x) \Rightarrow [r_0(x), r_1(x)] = [r_1(x), r_2(x)]$
$\vdots$
$r_{i-1}(x) = r_i(x) \cdot s_{i+1}(x) + r_{i+1}(x) \Rightarrow [r_{i-1}(x), r_i(x)] = [r_i(x), r_{i+1}(x)]$
$r_i(x) = r_{i+1}(x) \cdot s_{i+2}(x) + 0 \Rightarrow [r_i(x), r_{i+1}(x)] = [r_{i+1}(x)] = [p(x), q(x)]$
Entonces $r_{i+1}(x)$ es el máximo común divisor de $p(x)$ y $q(x)$

*Observaciones:*
El procedimiento es equivalente al algoritmo de Euclides para números enteros.

***Ejemplo de números enteros:***

$m.c.d.(480, 324)$

| | 1 | 2 | 13 | |
|---|---|---|---|---|
| 480 | 324 | 156 | 12 | 0 |
| 324 | 312 | 12 | | |
| 156 | 12 | 36 | | |
| | | 36 | | |
| | | 0 | | |

Por lo tanto, $m.c.d. = 12$ ya que es el último resto distinto de 0

***Ejemplos de polinomios:***

1. $m.c.d.(x^4 + 3x^3 + 3x^2 + x + 2, x^3 + 2x^2 + 1)$ en $\mathbb{Q}[x]$

| | $x+1$ | $x+2$ | $-x+1$ | $\frac{-x}{2} - \frac{1}{2}$ | |
|---|---|---|---|---|---|
| $x^4 + 3x^3 + 3x^2 + x + 2$ | $x^3 + 2x^2 + 1$ | $x^2 + 1$ | $-x - 1$ | 2 | 0 |
| $x^4 + 2x^3 + x$ | $x^3 + x$ | $x^2 + x$ | $-x$ | | |
| $x^3 + 3x^2 + 2$ | $2x^2 - x + 1$ | $-x + 1$ | $-1$ | | |
| $x^3 + 2x^2 + 1$ | $2x^2 + 2$ | $-x - 1$ | $-1$ | | |
| $x^2 + 1$ | $-x - 1$ | 2 | 0 | | |

Por lo tanto, tenemos $m.c.d. = 2$, como $\mathbb{Q}$ es un cuerpo, podemos normalizar para obtener el polinomio mónico, así que $m.c.d. = 1$

2. $m.c.d.(x^3 + x^2 + x + 1, x^2 + 2)$ en $\mathbb{Z}_3[x]$

| | $x+1$ | $2x+1$ | |
|---|---|---|---|
| $x^3+x^2+x+1$ | $x^2+2$ | $2x+2$ | 0 |

| | |
|---|---|
| $x^3+2x$ | $x^2+x$ |
| $x^2+2x+1$ | $2x+2$ |
| $x^2+2$ | $2x+2$ |
| $2x+2$ | 0 |

Tendremos que $m.c.d. = x+1$, lo hemos hecho mónico (normalizado), ya que $\mathbb{Z}_3$ es cuerpo. Para normalizarlo hemos multiplicado por 2.

*Observación:*

Si $d(x)$ es el máximo común divisor de $p(x)$ y $q(x)$, entonces $[d(x)] = [p(x), q(x)]$, por lo tanto $d(x) \in [p(x), q(x)]$, así que $\exists a_1(x), a_2(x) \in A[x]$ tal que $d(x) = a_1(x) \cdot p(x) + a_2(x) \cdot q(x)$

***Ejemplo:***

Usando los polinomios del ejemplo anterior:

(a) $x^3+x^2+x+1 = (x+1)(x^2+2)+2x+2 \Rightarrow x^3+x^2+x+1-(x+1)(x^2+2) = 2x+2 \Rightarrow$
$x+1 = 2\overbrace{(x^3+x^2+x+1)}^{p(x)} + (x+1)\overbrace{(x^2+2)}^{q(x)}$

(b) $x^2+2 = (2x+1)(2x+2) = 2x(2x+2)+2x+2 \Rightarrow x^2+2-2x(2x+2) = 2x+2 \Rightarrow$
$2x+2 = x^2+2+x(2x+2) = x^2+2+x[(x^3+x^2+x+1)+2(x+1)(x^2+2)] = (x^2+2)[1+2x(x+1)]+(x^3+x^2+x+1)x \Rightarrow x+1 = [2+x(x+1)](x^2+2)+2x(x^3+x^2+x+1) \Rightarrow$
$x+1 = (x^2+x+2)\overbrace{(x^2+2)}^{q(x)} + 2x\overbrace{(x^3+x^2+x+1)}^{p(x)}$

Podemos ver que la descomposición no es única.

### 5.5.4. Polinomios primos

Dados dos polinomios $p(x), q(x) \in A[x]$ se dice que son *primos entre sí* cuando el máximo común divisor es 1.

*Observación:*

Si dos polinomios $p(x)$ y $q(x)$ son primos entre sí, entonces $[1] = [p(x), q(x)]$, por lo tanto $1 \in [p(x), q(x)]$, así que $\exists a_1(x), a_2(x) \in A[x]$ tales que $a_1(x) \cdot p(x) + a_2(x) \cdot q(x) = 1$

***Ejemplo:***

$p(x) = x^2 + x + 1 \in \mathbb{Q}[x], q(x) = x^2 + 2 \in \mathbb{Q}[x]$

| | $1$ | $x+1$ | $\frac{x}{3} - \frac{1}{3}$ | |
|---|---|---|---|---|
| $x^2+x+1$ | $x^2+2$ | $x-1$ | $3$ | $0$ |
| $x^2+2$ | $x^2-x$ | $x$ | | |
| $x-1$ | $x+2$ | $-1$ | | |
| | $x-1$ | $-1$ | | |
| | $3$ | $0$ | | |

El máximo común divisor es $m.c.d = 1$ (hemos normalizado ya que $\mathbb{Q}$ es cuerpo), por lo tanto, $p(x)$ y $q(x)$ son primos entre sí.

$$\left.\begin{array}{l} x^2+x+1 = 1(x^2+2)+(x-1) \\ x^2+2 = (x-1)(x+1)+3 \end{array}\right\} \quad \left.\begin{array}{l} x^2+x+1-1(x^2+2) = (x-1) \\ x^2+2-(x-1)(x+1) = 3 \end{array}\right\} \Rightarrow$$

$$3 = -(x+1)[(x^2+x+1)-(x^2+2)]+(x^2+2) \Rightarrow 3 = -(x+1)(x^2+x+1)+(x+2)(x^2+2) \Rightarrow$$

$$1 = \overbrace{\left(\frac{-x}{3} - \frac{1}{3}\right)}^{a_1(x)}\overbrace{(x^2+x+1)}^{p(x)} + \overbrace{\left(\frac{x}{3} + \frac{2}{3}\right)}^{a_2(x)}\overbrace{(x^2+2)}^{q(x)}$$

*Proposición:*

Sea $d(x) = m.c.d.(p(x), q(x))$ y definimos $p(x) = d(x) \cdot a_1(x)$ y $q(x) = d(x) \cdot a_2(x)$, entonces $a_1(x)$ y $a_2(x)$ son primos entre sí.

*Demostración:*

Sabemos que dado $d(x) = m.c.d.(p(x), q(x)) \Rightarrow \exists r(x), s(x) \in A[x]$ tal que $d(x) = r(x) \cdot p(x) + s(x) \cdot q(x)$.

Como hemos definido $p(x) = d(x) \cdot a_1(x)$ y $q(x) = d(x) \cdot a_2(x)$, entonces $d(x) = r(x) \cdot d(x) \cdot a_1(x) + s(x) \cdot d(x) \cdot a_2(x) \Rightarrow d(x) = [r(x) \cdot a_1(x) + s(x) \cdot a_2(x)] \cdot d(x) \Rightarrow$*(como $A[x]$ es dominio de integridad)*$\Rightarrow r(x) \cdot a_1(x) + s(x) \cdot a_2(x) = 1$, por lo tanto $a_1(x)$ y $a_2(x)$ son primos entre sí.

***Ejemplo:***

Vimos que $x+1 = m.c.d.(x^3+x^2+x+1, x^2+2)$ y $x+1 = (x^2+x+2)(x^2+2)+2x(x^3+x^2+x+1)$, vamos demostrar que $x^2+x+2$ y $2x$ son primos entre sí

| | $x+1$ | $\frac{x}{2}$ | |
|---|---|---|---|
| $x^2+x+2$ | $x$ | $2$ | $0$ |
| $x^2$ | $x$ | | |
| $x+2$ | $0$ | | |
| $x$ | | | |
| $2$ | | | |

*Teorema de Euclides:*
Sean $p(x)$ y $q(x)$ dos polinomios primos entre sí y sea $h(x)$ otro polinomio tal que $p(x)|q(x)\cdot h(x)$, entonces $p(x)|h(x)$

*Demostración:*
Como $p(x)$ y $q(x)$ son primos entre sí, entonces $\exists a_1(x), a_2(x) \in A[x]$ tal que $p(x)\cdot a_1(x) + q(x)\cdot a_2(x) = 1 \Rightarrow h(x)\cdot p(x)\cdot a_1(x) + h(x)\cdot q(x)\cdot a_2(x) = h(x)$
Como $p(x)$ divide a $h(x)\cdot p(x)\cdot a_1(x)$ y también a $h(x)\cdot q(x)\cdot a_2(x)$ ya que por hipótesis divide a $h(x)\cdot q(x)$, entonces $p(x)$ divide a $h(x)$, ya que divide a la suma $h(x)\cdot p(x)\cdot a_1(x) + h(x)\cdot q(x)\cdot a_2(x)$

## 5.6. Mínimo común múltiplo

*Proposición:*
Dados dos polinomios $p(x), q(x) \in A[x]$, existe $m(x) \in A[x]$ tal que $m(x)\cdot d(x) = p(x)\cdot q(x)$ con $d(x) = m.c.d.(p(x), q(x))$.

*Demostración:*
Como $d(x) = m.c.d.(p(x), q(x)) \Rightarrow \exists a_1(x), a_2(x)$ tal que $p(x) = a_1(x)\cdot d(x), q(x) = a_2(x)\cdot d(x)$ con $m.c.d.(a_1(x), a_2(x)) = 1$
Sea $m(x) = a_1(x)\cdot a_2(x)\cdot d(x)$, entonces $m(x)\cdot d(x) = a_1(x)\cdot d(x)\cdot a_2(x)\cdot d(x) = p(x)\cdot q(x)$

*Definición:*
El polinomio $m(x) \in A[x]$ tal que $m(x)\cdot d(x) = p(x)\cdot q(x)$ con $d(x) = m.c.d.(p(x), q(x))$ se denomina *mínimo común múltiplo* de $p(x)$ y $q(x)$, $m(x) = m.c.m.(p(x), q(x))$.

Veamos que $m(x)$ es múltiplo de $p(x)$ y de $q(x)$ :

i. Como $p(x) = a_1(x)\cdot d(x) \Rightarrow m(x) = p(x)\cdot a_2(x) \Rightarrow p(x)|m(x)$

ii. Como $q(x) = a_2(x)\cdot d(x) \Rightarrow m(x) = q(x)\cdot a_1(x) \Rightarrow q(x)|m(x)$

Veamos ahora que $m(x)$ es el mínimo común múltiplo, esto significa que $\forall n(x) \in A[x]$ tal que $p(x)|n(x)$ y $q(x)|n(x)$, entonces $\exists t(x) \in A[x]$ tal que $n(x) = m(x)\cdot t(x)$

Como $p(x)|n(x) \Rightarrow \exists t_1(x) \in A[x]$ tal que $n(x) = t_1(x)\cdot p(x)$ y como $q(x)|n(x) \Rightarrow \exists t_2(x) \in A[x]$ tal que $n(x) = t_2(x)\cdot q(x)$, entonces $n(x) = t_1(x)\cdot a_1(x)\cdot d(x) = t_2(x)\cdot a_2(x)\cdot d(x) \Rightarrow t_1(x)\cdot a_1(x)\cdot d(x) = t_2(x)\cdot a_2(x)\cdot d(x) \Rightarrow$ *(como $A[x]$ es dominio de integridad)* $\Rightarrow t_1(x)\cdot a_1(x) =$

$t_2(x) \cdot a_2(x) \Rightarrow a_1(x) | t_2(x) \cdot a_2(x)$

Como $m.c.d.(a_1(x), a_2(x)) = 1$, tendremos que $a_1(x) | t_2(x)$, por lo tanto $\exists \alpha(x) \in A[x]$ tal que $t_2(x) = \alpha(x) \cdot a_1(x) \Rightarrow n(x) = t_2(x) \cdot a_2(x) \cdot d(x) = \alpha(x) \cdot a_1(x) \cdot \overbrace{a_2(x) \cdot d(x)}^{q(x)} = \alpha(x) \cdot \overbrace{a_1(x) \cdot q(x)}^{m(x)} = \alpha(x) \cdot m(x) \Rightarrow m(x) | n(x)$, como queríamos demostrar.

***Ejemplo:***

Calcular el $m.c.m.(x^3 + x^2 + x + 1, x^2 + 2)$ en $\mathbb{Z}_3[x]$

| | $x+1$ | $2x+1$ | |
|---|---|---|---|
| $x^3 + x^2 + x + 1$ | $x^2 + 2$ | $2x + 2$ | $0$ |

| | |
|---|---|
| $x^3 + 2x$ | $x^2 + x$ |
| $x^2 + 2x + 1$ | $2x + 2$ |
| $x^2 + 2$ | $2x + 2$ |
| $2x + 2$ | $0$ |

El $m.c.d.(x^3 + x^2 + x + 1, x^2 + 2) = x + 1 = d(x)$

Como $p(x) \cdot q(x) = m(x) \cdot d(x) \Rightarrow x^5 + x^4 + 2x + 2 = m(x) \cdot (x + 1) \Rightarrow$

| | |
|---|---|
| $x^5 + x^4 + 2x + 2$ | $x + 1$ |
| $x^5 + x^4$ | $x^4 + 2$ |
| $2x + 2$ | |
| $2x + 2$ | |
| $0$ | |

Por lo tanto $m(x) = x^4 + 2 = m.c.m.(x^3 + x^2 + x + 1, x^2 + 2)$

## 5.7. Polinomio irreducible

### 5.7.1. Definiciones

*Definición:*

Sea un polinomio $p(x) \in A[x]$ de grado diferente de cero, se dice que $p(x)$ es *irreducible* en $A[x]$ si sus únicos divisores son $a$ y $a \cdot p(x)$, con $a \in A[x]$.

***Ejemplos:***

1. $p(x) = x^2 - 2$ es irreducible en $\mathbb{Q}[x]$, pero no en $\mathbb{R}[x]$, ya que $p(x) = (x - \sqrt{2})(x + \sqrt{2})$

2. $p(x) = x^2 + 1$ es irreducible en $\mathbb{Q}[x]$ y en $\mathbb{R}[x]$, pero no $\mathbb{C}[x]$ (ya que podemos escribir $p(x) = (x + i)(x - i)$), ni en $\mathbb{Z}_5[x]$ ya que $p(x) = (x - 2)(x + 2)$ en $\mathbb{Z}_5[x]$

*Observación:*
La irreducibilidad depende del anillo de polinomios que se considere.

*Definición (otra definición de irreducibilidad):*
Sea $A$ un anillo conmutativo con unidad, un polinomio $p(x) \in A[x]$ que no sea invertible en $A[x]$ se dice que es irreducible en $A[x]$ si para toda descomposición de la forma $p(x) = q(x) \cdot s(x)$ con $q(x), s(x) \in A[x]$, se tiene que o bien $q(x)$ o bien $s(x)$ son una unidad de $A[x]$

*Observación:*
Los polinomios irreducibles en un anillo de polinomios juegan el mismo papel que los números primos.

*Proposición:*
Todo polinomio $p(x) \in A[x]$ de grado mayor que 0 es producto de polinomios irreducibles.

*Demostración:*

1. Si $p(x)$ es irreducible, ya está hecha la factorización.

2. Si $p(x)$ es reducible, tiene divisores de grado menor, entonces $p(x) = a_1(x) \cdot p_1(x)$. Se repite el proceso hasta obtener un producto de polinomios irreducibles.

### 5.7.2. Raíces de un polinomio (o ceros de un polinomio)

Sea $A$ un cuerpo, dado un polinomio $p(x) \in A[x]$, se dice que $a \in A$ es una raíz de $p(x)$ si $p(a) = 0$.
A este proceso de calcular $p(a)$ se le denomina evaluar un polinomio $p(x)$ en $a$.

*Proposición:*
Sea $A$ un cuerpo, si $p(x) \in A[x]$ y $a \in A$, entonces $q(x) = x - a$ divide a $p(x)$ si y sólo si $p(a) = 0$.

*Demostración:*
$\boxed{\Rightarrow}$
Si $(x-a)|p(x) \Rightarrow \exists s(x) \in A[x]$ tal que $p(x) = s(x)\cdot(x-a)$ y por tanto $p(a) = s(a)\cdot(a-a) = 0$
$\boxed{\Leftarrow}$

Por el teorema de la división entera podemos escribir $p(x) = s(x) \cdot q(x) + r(x)$ con $gr(r(x)) < gr(q(x))$ ó $r(x) = 0$.
Si tomamos $q(x) = x - a \Rightarrow p(x) = s(x) \cdot (x - a) + r(x)$ con $gr(r(x)) < gr(q(x)) = 1 \Rightarrow gr(r(x)) = 0 \Rightarrow r(x) = b \in A$, por lo tanto $p(x) = s(x) \cdot (x-a)+b \Rightarrow p(a) = s(a) \cdot (a-a)+b = b$
Como además hemos supuesto que $p(a) = 0 \Rightarrow p(a) = b = 0 \Rightarrow b = 0 \Rightarrow q(x) = x - a$ divide a $p(x)$

*Definición de multiplicidad:*
Dado un polinomio $p(x) \in A[x]$ con $A$ un cuerpo, si $(x - a)^n$ con $n \in \mathbb{N}$ divide a $p(x)$ y $(x - a)^{n+1}$ no divide a $p(x)$, se dice que la raíz $a$ tiene *multiplicidad* $n$.

***Ejemplo:***
$a = 1$ tiene multiplicidad 1 para $p(x) = x^2 - 1$ en $\mathbb{Q}[x]$ y multiplicidad 2 para $q(x) = x^2 - 2x + 1$ en $\mathbb{Q}[x]$

*Proposición:*
Sea $A$ un cuerpo, dado el polinomio $p(x) \in A[x]$ con $gr(p(x)) = n \geq 1$, entonces $p(x)$ tiene a lo sumo $n$ raíces en $A[x]$ contando cada raíz tantas veces como indica su multiplicidad.

*Demostración:*
Supongamos que $p(x)$ tiene $m$ raíces, $a_1, a_2, \cdots, a_m$, por lo tanto $(x - a_i)|p(x), i = 1, \cdots, m \Rightarrow p(x) = (x - a_1) \cdot (x - a_2) \cdots (x - a_m) \cdot b(x)$ con $b(x) \in A[x]$, como $gr(p(x)) = m + gr(b(x)) \Rightarrow n = m + gr(b(x)) \Rightarrow n \geq m$, entonces el número de raíces es menor o igual que el grado.

*Observación:*
Es necesario imponer que $A$ sea un cuerpo para que se cumpla la proposición anterior ya que, por ejemplo, $p(x) = (x - 2)(x - 3)$ en $\mathbb{Z}_6[x]$ tiene como raíces 2 y 3 pero también 0 y 5, mientras que $gr(p(x)) = 2$ (esto es debido a que $\mathbb{Z}_6$ no es un cuerpo, por tanto $\mathbb{Z}_6[x]$ no es dominio de integridad).

# 5.8. Criterios de irreducibilidad (en $\mathbb{C}[x], \mathbb{R}[x], \mathbb{Q}[x]$ y $\mathbb{Z}_p[x]$)

## 5.8.1. Irreducibilidad en $\mathbb{C}[x]$

*Teorema fundamental del Álgebra:*
Todo polinomio $p(x) \in \mathbb{C}[x]$ no constante tiene al menos una raíz en $\mathbb{C}$

*Proposición:*
Todo polinomio $p(x) \in \mathbb{C}[x]$ con $gr(p(x)) = n \geq 1$ tiene $n$ raíces en $\mathbb{C}[x]$ (contando multiplicidad).

*Proposición:*
Un polinomio $p(x) \in \mathbb{C}[x]$ es irreducible en $\mathbb{C}[x]$ si y sólo si tiene grado 1.

Por lo tanto, dado $p(x) \in \mathbb{C}[x]$ con $gr(p(x)) = n$, entonces $p(x) = k(x-a_1)(x-a_2)\cdots(x-a_n)$ con $k \in \mathbb{C}$ y $a_i \in \mathbb{C}, i = 1, \cdots, n$ raíces de $p(x)$

*Proposición:*
Si un polinomio $p(x)$ con coeficientes reales tiene una raíz compleja $a$, entonces su conjugado $\overline{a}$ también es raíz de $p(x)$

*Demostración:*
Sea $p(x) = c_0 + c_1x + c_2x^2 + \cdots + c_nx^n$ con $c_i \in \mathbb{R}, i = 0, \cdots, n$ y sea $a \in \mathbb{C}$ tal que $p(a) = 0 \Rightarrow c_0 + c_1a + c_2a^2 + \cdots + c_na^n = 0$
Tomamos el complejo conjugado de la expresión anterior $\overline{c_0 + c_1a + c_2a^2 + \cdots + c_na^n} = 0 \Rightarrow \overline{c_0} + \overline{c_1} \cdot \overline{a} + \overline{c_2} \cdot \overline{a}^2 + \cdots + \overline{c_n} \cdot \overline{a}^n = 0 \Rightarrow c_0 + c_1\overline{a} + c_2\overline{a}^2 + \cdots + c_n\overline{a}^n = 0 \Rightarrow p(\overline{a}) = 0$, por lo tanto $\overline{a}$ también es raíz de $p(x)$.

## 5.8.2. Irreducibilidad en $\mathbb{R}[x]$

*Proposición:*
Si $p(x) \in \mathbb{R}[x]$ es irreducible en $\mathbb{R}[x]$, su grado es 1 ó 2. Además si su grado es 2 y $p(x)$ es irreducible, entonces $p(x) = ax^2 + bx + c$ cumple que $\Delta = b^2 - 4ac < 0$

*Demostración:*
Obviamente todo polinomio $p(x) \in \mathbb{R}[x]$ de grado 1 tendrá la forma $p(x) = ax + b$ y por tanto será irreducible.
Si $p(x) = ax^2 + bx + c \in \mathbb{R}[x]$, que es de grado 2, es irreducible, entonces no tendrá raíces reales. Sin embargo, acabamos de ver que si consideramos $p(x) \in \mathbb{C}[x]$, tendrá 2 raíces comple-

jas y además al tener coeficientes reales, si $s = \alpha+\beta i$ es raíz de $p(x)$, entonces $\overline{s} = \alpha-\beta i$ también será raíz de $p(x)$ con $\beta \neq 0$. Por lo tanto, $p(x) = m(x-s)(x-\overline{s}) = m(x^2-(s+\overline{s})x+s\overline{s}) = m(x^2-2\alpha x+\alpha^2+\beta^2) = ax^2+bx+c \Rightarrow \begin{cases} m = a \\ -2m\alpha = b \\ m(\alpha^2+\beta^2) = c \end{cases} \begin{cases} m = a \\ -2\alpha = \frac{b}{a} \\ \alpha^2+\beta^2 = \frac{c}{a} \end{cases}$

Como tenemos que exigir que $\beta \neq 0 \Rightarrow \beta^2 > 0 \Rightarrow \alpha^2+\beta^2 > \alpha^2 \Rightarrow 4(\alpha^2+\beta^2) > 4\alpha^2 \Rightarrow 4\frac{c}{a} > \left(\frac{b}{a}\right)^2 \Rightarrow b^2-4ac < 0$

Por lo tanto, para que un polinomio $p(x)$ de grado 2 sea irreducible en $\mathbb{R}[x]$ tenemos que exigir que $\Delta = b^2-4ac < 0$

***Ejemplo:***

- $p(x) = x^2+2x+1$ es reducible en $\mathbb{R}[x]$ ya que $b^2-4ac > 0 \Rightarrow p(x) = (x+1)^2$
- $p(x) = x^2-2x+2$ es irreducible en $\mathbb{R}[x]$ ya que $b^2-4ac < 0 \Rightarrow p(x) = [x-(1+i)][x-(1-i)]$

Si $gr(p(x)) \geq 3$ y $s \in \mathbb{C}$ es una raíz de $p(x)$, entonces:

i. si $s \in \mathbb{R}$, entonces $(x-s)$ divide a $p(x)$ y por tanto $p(x)$ es reducible

ii. si $s = a+bi \in \mathbb{C} \Rightarrow (x-s)(x-\overline{s})$ divide a $p(x)$ y por tanto $(x^2-2ax+a^2+b^2)$ divide a $p(x)$ y $p(x)$ es reducible

### 5.8.3. Irreducibilidad en $\mathbb{Z}[x]$ y en $\mathbb{Q}[x]$

*Proposición:*
Sea $p(x) = a_0+a_1x+a_2x^2+\cdots+a_nx^n \in \mathbb{Q}[x]$ un polinomio con coeficientes en $\mathbb{Z}$.

Si $\frac{a}{b}$ es una raíz de $p(x)$ con $a$ y $b$ primos entre sí $(a, b \in \mathbb{Z})$, entonces $a|a_0$ y $b|a_n$.

*Observación:*
Si $a$ es una raíz entera de $p(x)$, entonces $a|a_0$.

*Demostración:*
Sea $\frac{a}{b}$ raíz de $p(x) \Rightarrow a_0+a_1\frac{a}{b}+a_2\left(\frac{a}{b}\right)^2+\cdots+a_n\left(\frac{a}{b}\right)^n = 0 \Rightarrow$
$a_na^n+\cdots+a_2a^2b^{n-2}+a_1ab^{n-1}+a_0b^n = 0 \Rightarrow a(a_na^{n-1}+\cdots+a_2ab^{n-2}+a_1b^{n-1}) = -a_0b^n \Rightarrow a|(-a_0b^n)$, como $a$ y $b$ son primos, entonces $a|a_0$.

Además, $a_n a^n + (a_{n-1}a^{n-1} + \cdots + a_2 a b^{n-2} + a_1 b^{n-1} + a_0 b^{n-1})b = 0 \Rightarrow b|a_n a^n$, como $b$ y $a$ son primos, entonces $b|a_n$.

*Observación:*
Un polinomio $p(x)$ mónico ($a_n = 1$) con coeficientes enteros no tiene raíces fraccionarias.

*Definiciones:*

1. Sea $p(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \in \mathbb{Z}[x]$, se define *contenido* de $p(x)$ al máximo común divisor de sus coeficientes, $C(p) = m.c.d.(a_0, a_1, \cdots, a_n)$

2. Se dice que un polinomio $p(x) \in \mathbb{Z}[x]$ es *primitivo* si su contenido $C(p) = 1$, o sea, si todos sus coeficientes son primos entre sí.

*Criterio de irreducibilidad de Eisenstein:*
Sea $p(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n \in \mathbb{Z}[x]$ un polinomio primitivo con coeficientes enteros tal que existe $p \in \mathbb{Z}$ primo que divide a $a_i$ con $i = 0, 1, \cdots, n-1$, pero no divide a $a_n$ y además $p^2$ no divide a $a_0$, entonces $p(x)$ es irreducible en $\mathbb{Z}[x]$

*Demostración:*
Por reducción al absurdo:
Supongamos que $p(x)$ es reducible en $\mathbb{Z}[x]$, entonces $p(x) = q(x) \cdot s(x)$ con $q(x) = b_0 + b_1 x + b_2 x^2 + \cdots + b_q x^q$, $s(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_s x^s \in \mathbb{Z}[x]$, multiplicando e igualando coeficientes tendremos que $a_0 = b_0 c_0, a_n = b_q c_s$
Supongamos que existe $p \in \mathbb{Z}$ primo que divide a $a_i$ con $i = 0, 1, \cdots, n-1$, entonces $p|a_0 \Rightarrow p|b_0 c_0$, por tanto, o bien $p|b_0$ o bien $p|c_0$. Supongamos que $p|b_0$ (el razonamiento es similar si $p|c_0$), como además $p \nmid a_n \Rightarrow p \nmid b_q c_s \Rightarrow p \nmid b_q$
Sea $j$ el primer índice entre 0 y $q$ tal que $p \nmid b_j \Rightarrow 0 < j \leq q$ y por tanto $p|b_i$ con $0 \leq i \leq j-1$. Además sabemos que $j < q + s = n$ (ya que $s \geq 1$).
Como hemos supuesto que $p|a_j$ para $0 \leq j < n$ entonces $p|\overbrace{(b_0 c_j + b_1 c_{j-1} + \cdots + b_{j-1} c_1 + b_j c_0)}^{a_j}$
Como además $p|b_i$ con $0 \leq i \leq j-1$, tendremos que $p|b_i c_{j-i}$ y por tanto $p|(b_0 c_j + b_1 c_{j-1} + \cdots + b_{j-1} c_1)$.
Teniendo en cuenta ambas cosas, tendremos que $p|(a_j - (b_0 c_j + b_1 c_{j-1} + \cdots + b_{j-1} c_1)) \Rightarrow p|b_j c_0$. Por lo tanto, como $p \nmid b_j \Rightarrow p|c_0$.
Por otro lado, sabíamos que $p|b_0 \Rightarrow p^2|b_0 c_0 \Rightarrow p^2|a_0$, que contradice la hipótesis del enunciado, así que $p(x)$ es irreducible en $\mathbb{Z}[x]$

***Ejemplo:***

$p(x) = x^4 - 3x^2 + 6x + 3$ es irreducible en $\mathbb{Z}[x]$ ya que cumple el criterio de Eisenstein para $p = 3$

Sin embargo, $x^2 + 4$ es irreducible en $\mathbb{Z}[x]$ aunque no cumple el criterio de Eisenstein, ya que el criterio de Eisenstein asegura que un polinomio sea irreducible, pero que no se cumpla no significa que el polinomio sea reducible.

Al contrario que en $\mathbb{C}[x]$ y $\mathbb{R}[x]$, es posible encontrar polinomios irreducibles en $\mathbb{Z}[x]$ y en $\mathbb{Q}[x]$ de cualquier grado, por ejemplo $x^n + p$ con $p > 0$ primo es irreducible en $\mathbb{Z}[x]$ y en $\mathbb{Q}[x]$.

*Lema de Gauss:*

Si $p(x)$ y $q(x)$ son primitivos en $\mathbb{Z}[x]$ entonces $p(x) \cdot q(x)$ también lo es.

Dados dos polinomios $p(x)$ y $q(x)$ en $\mathbb{Z}[x]$, podemos escribir $p(x) = C(p) \cdot p'(x)$ y $q(x) = C(q) \cdot q'(x)$ con $p'(x) \in \mathbb{Z}[x]$ y $q'(x) \in \mathbb{Z}[x]$ primitivos, por lo tanto $p(x) \cdot q(x) = C(p) \cdot C(q) \cdot p'(x) \cdot q'(x) \Rightarrow C(p \cdot q) = C(p) \cdot C(q)$

*Proposición:*

Sea $p(x) \in \mathbb{Z}[x]$ primitivo, $p(x)$ es irreducible en $\mathbb{Q}[x]$ si y sólo si $p(x)$ es irreducible en $\mathbb{Z}[x]$

*Demostración:*

Por reducción al absurdo:

$\boxed{\Rightarrow}$

Supongamos que $p(x)$ es irreducible en $\mathbb{Q}[x]$ y es reducible en $\mathbb{Z}[x]$, entonces $p(x) = q(x) \cdot r(x)$ con $q(x)$ y $r(x)$ primitivos, por lo tanto $C(q) = C(r) = 1$. Además $gr(q(x)) \geq 1$ y $gr(r(x)) \geq 1$, por lo que $p(x) = q(x) \cdot r(x)$ sería también un factorización en $\mathbb{Q}[x]$, así que $p(x)$ sería reducible en $\mathbb{Q}[x]$ y esto sería absurdo.

$\boxed{\Leftarrow}$

Supongamos que $p(x)$ es irreducible en $\mathbb{Z}[x]$ y que $p(x) = q(x) \cdot r(x)$ es una factorización en $\mathbb{Q}[x]$ (con factores que no son unidades), entonces $q(x) = \frac{a}{b} q'(x)$ con $q'(x) \in \mathbb{Z}[x]$ y primitivo, por lo que $q'(x)$ divide a $p(x)$, entonces $p(x)$ sería reducible en $\mathbb{Z}[x]$ y esto sería absurdo.

### 5.8.4. Irreducibilidad en $\mathbb{Z}_p[x]$

*Proposición:*

Existen $p$ polinomios lineales irreducibles mónico en $\mathbb{Z}_p[x]$ (con $p$ primo) de la forma $x + a$

***Ejemplo:***

En $\mathbb{Z}_3[x]$ los polinomios lineales irreducibles mónicos son $x, x+1, x+2$

*Proposición:*

Existen $\dfrac{p^2-p}{2}$ polinomios cuadráticos mónicos irreducibles en $\mathbb{Z}_p[x]$ (con $p$ primo)

*Demostración:*

Supongamos que $x^2+a_1x+a_2 \in \mathbb{Z}_p[x]$ es reducible, entonces $x^2+a_1x+a_2 = (x-r_1)(x-r_2)$

Si $r_1 \neq r_2$, hay $\binom{p}{2} = \dfrac{p!}{(p-2)!2!} = \dfrac{p(p-1)}{2}$ combinaciones distintas.

Si $r_1 = r_2$ hay $p$ posibilidades.

Por lo tanto, habrá un total de $\dfrac{p(p-1)}{2} + p = \dfrac{p(p+1)}{2}$ polinomios reducibles.

Como el número total de polinomios mónicos de la forma $x^2 + a_1x + a_2$ es $p^2$, el número de polinomios cuadráticos mónicos irreducibles es $p^2 - \dfrac{p(p+1)}{2} = \dfrac{p^2-p}{2}$

***Ejemplo:***

En $\mathbb{Z}_3[x]$ habrá $\dfrac{9-3}{2} = 3$ polinomios cuadráticos irreducibles: $x^2+1, x^2+x+2, x^2+2x+2$.

Si escribimos todos los posibles polinomios cuadráticos y los evaluamos en los posibles valores obtenemos la siguiente tabla

| $p(x)$ | $x^2+1$ | $x^2+x+1$ | $x^2+2x+1$ | $x^2+2$ | $x^2+x+2$ | $x^2+2x+2$ | $x^2$ | $x^2+x$ | $x^2+2x$ |
|---|---|---|---|---|---|---|---|---|---|
| $p(0)$ | 1 | 1 | 1 | 2 | 2 | 2 | 0 | 0 | 0 |
| $p(1)$ | 2 | 0 | 1 | 0 | 1 | 2 | 1 | 2 | 0 |
| $p(2)$ | 2 | 1 | 0 | 0 | 2 | 1 | 1 | 0 | 2 |

En el caso de tener polinomios cúbicos en $\mathbb{Z}_p[x]$, si son reducibles o bien son tres factores lineales o bien es uno lineal y uno cuadrático, así que miraremos si hay algún valor lineal que sea raíz (o sea, miramos si entre 0 y $p-1$ hay alguna raíz).

***Ejemplo:***

$p(x) = x^3 + 2x^2 + x + 1$ en $\mathbb{Z}_3[x]$, como $p(0) = 1, p(1) = 2, p(2) = 1$, será irreducible

$p(x) = x^3 + 2x^2 + x + 2$ en $\mathbb{Z}_3[x]$, como $p(0) = 2, p(1) = 0, p(2) = 2$ sabemos que será reducible ya que 1 es una raíz, por lo tanto $p(x) = (x-1)q(x) \Rightarrow q(x) = x^2 + 1$

Los polinomios de orden 4 en $\mathbb{Z}_p[x]$ pueden ser productos de factores lineales o de factores cuadráticos (irreducibles), así que primero miraremos si hay factores lineales (buscaremos raíces) y luego buscaremos factores cuadráticos.

***Ejemplo:***

$p(x) = x^4 + 1$ en $\mathbb{Z}_3[x]$

$p(0) = 1, p(1) = 2, p(2) = 2$, por lo tanto no hay factores lineales

$p(x) = (x^2 + a_1x + b_1)(x^2 + a_2x + b_2) = x^4 + (a_1 + a_2)x^3 + (b_1 + b_2 + a_1a_2)x^2 + (a_1b_2 + a_2b_1)x + b_1b_2 \Rightarrow \begin{cases} a_1 + a_2 = 0 \\ b_1 + b_2 + a_1a_2 = 0 \\ a_1b_2 + a_2b_1 = 0 \\ b_1b_2 = 1 \end{cases}$

Como $b_1b_2 = 1 \Rightarrow \begin{cases} b_1 = 1, b_2 = 1 \\ b_1 = 2, b_2 = 2 \end{cases}$

Si $b_1 = 1, b_2 = 1 \Rightarrow 2 + a_1a_2 = 0 \Rightarrow a_1a_2 = 1 \Rightarrow \begin{cases} a_1 = 1, a_2 = 1 \\ a_1 = 2, a_2 = 2 \end{cases}$. Como además $a_1 + a_2 = 0$ es imposible que se cumpla ninguna de las dos condiciones anteriores.

Si $b_1 = 2, b_2 = 2 \Rightarrow 1 + a_1a_2 = 0 \Rightarrow a_1a_2 = 2 \Rightarrow \begin{cases} a_1 = 2, a_2 = 1 \\ a_1 = 1, a_2 = 2 \end{cases}$. Estas dos opciones son compatibles con $a_1 + a_2 = 0$ y con $a_1b_2 + a_2b_1 = 0$ y representan la misma factorización: $p(x) = x^4 + 1 = (x^2 + 2x + 2)(x^2 + x + 2)$