Álgebra Lineal

Ingeniería Libre

`ingenieria-libre.github.io`

`mclnaranjito@gmail.com`

28 de abril de 2016

Índice general

Capítulo 1

Conceptos básicos I

Para comenzar el estudio del álgebra lineal, es preciso introducir conceptos pertenecientes al álgebra abstracta:

1.1. Conjuntos

Un conjunto es una reunión de determinados objetos bien definidos y diferenciables los unos de los otros. A modo de ejemplo tenemos los conjuntos siguientes:

- Conjunto de los números naturales: $\mathbb{N} = \{0, 1, 2, 3, ...\}$
- Conjunto de los números enteros: $\mathbb{Z} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}$
- Conjunto de los números racionales: $\mathbb{Q} = \{\frac{a}{b} : \ a, b \in \mathbb{Z}, \ b \neq 0\}$
- Conjunto de los números iracionales: $\mathbb{I} = \{\sqrt{2}, \sqrt{5}, \pi, e\}$
- Conjunto de los números reales: $\mathbb{R} = \{\mathbb{Q} + \mathbb{I}\}$
- Conjunto de los números complejos: $\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}$

Dado un conjunto A, se le puede añadir modificadores $(*, +, -)$. A^* será el conjunto de elementos de A salvo el cero, mientras que A^+ y A^- designan a los elementos positivos y negativos de A respectivamente. Como ejemplo tendríamos $\mathbb{N}^* = \{1, 2, 3, ...\}$, $\mathbb{Z}^+ = \{1, 2, 3, ...\}$, $\mathbb{Z}^- = \{..., -3, -2, -1\}$

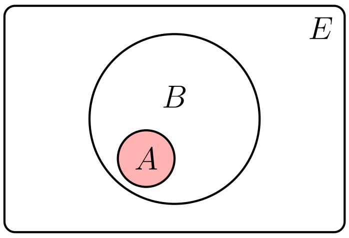
Al número de elementos de A lo denominamos cardinal de A y se denota por $card(A)$

Operaciones entre conjuntos

Definamos A y B como dos subconjuntos que pertenecen a un tercero E. Las operaciones básicas que se pueden realizar entre ellos son las siguientes:

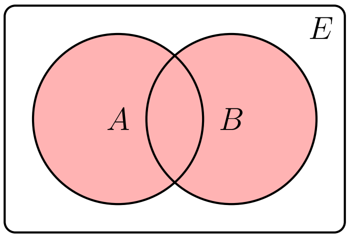
- Inclusión: $A \subset B$

$A \subset B$



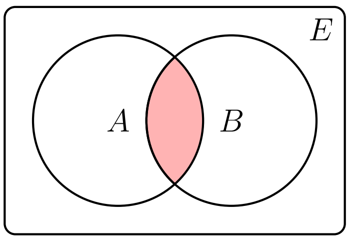
- Unión: $A \cup B \equiv \{x: \; x \in A \text{ ó } x \in B\}$

$A \cup B$

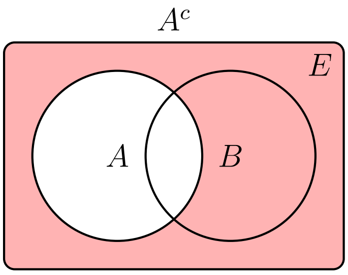


- Intersección: $A \cap B \equiv \{x: \; x \in A \text{ y } x \in B\}$

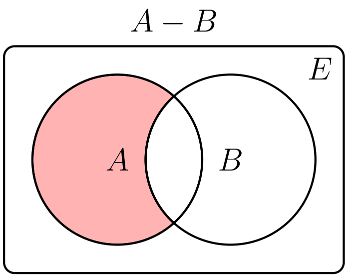
$A \cap B$



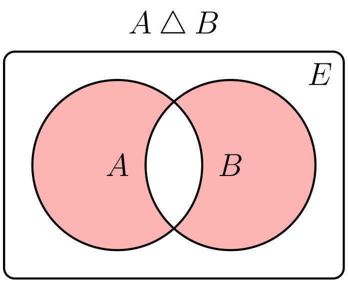
- Contrario o complementario: $A^c = \overline{A}$



- Diferencia: $A - B = A \cap B^c = A - (A \cap B)$



- Diferencia simétrica: $A \triangle B = (A - B) \cup (B - A)$



Para operar con n conjuntos emplearemos las siguientes notaciones:

$$\bigcup_{i=1}^{n} A_i = A_1 \cup A_2 \cup ... \cup A_n \quad \forall i \neq j$$

$$\bigcap_{i=1}^{n} A_i = A_1 \cap A_2 \cap ... \cap A_n$$

Ejemplo:

Sea $E = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$, $A = \{1, 3, 6, 7, 9\}$ y $B = \{2, 3, 5, 7, 10\}$. Entonces:

- $A \cup B = \{1, 2, 3, 5, 6, 7, 9, 10\}$
- $A \cap B = \{3, 7\}$
- $A^c = \{2, 4, 5, 8, 10\}, \quad B^c = \{1, 4, 6, 8, 9\}$
- $A - B = \{1, 6, 9\}, \quad B - A = \{2, 5, 10\}$
- $A \triangle B = \{1, 2, 5, 6, 9, 10\}$

Partición de un conjunto

Particionar un conjunto E consiste en dividirlo en subconjuntos tales que:

1. $$A_i \cap A_j = \emptyset$$
2. $$E = \bigcup_{i=1}^{n} A_i$$

Ejemplo:

Sea $E = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ podemos particionarlo, por ejemplo, en tres subconjuntos de diferentes tamaños: $A = \{1, 2\}$, $B = \{3, 5, 7\}$ y $C = \{4, 6, 8, 9, 10\}$. De ésta manera se cumple que:

- $A \cap B = \emptyset$, $A \cap C = \emptyset$ y $B \cap C = \emptyset$
- $E = A \cup B \cup C$

Aprovechamos este ejemplo para recordar qué cardinal tiene cada conjunto: $card(E) = 10$, $card(A) = 2$, $card(B) = 3$ y $card(C) = 5$.

Producto cartesiano

Sean dos conjuntos A y B. Se define el producto cartesiano $A \times B$ al conjunto de todos los pares ordenados (a, b) en los que el primer componente pertenece a A y el segundo a B, es decir:

$$A \times B = \{(a, b) : a \in A, b \in B\}$$

Ejemplo:

Sean dos conjuntos $A = \{a, b, c\}$ y $B = \{1, 2, 3, 4\}$. Entonces:

$$A \times B = \begin{Bmatrix} (a,1) & (a,2) & (a,3) & (a,4) \\ (b,1) & (b,2) & (b,3) & (b,4) \\ (c,1) & (c,2) & (c,3) & (c,4) \end{Bmatrix}$$

Propiedades de los conjuntos

Para facilitar la comprensión de algunas de las siguientes propiedades podemos utilizar las semejanzas entre las propiedades de las operaciones de conjuntos y las operaciones numéricas. Así, la unión se asemeja a la suma numérica, la intersección al producto, el conjunto vacío sería el equivalente del cero y el complementario equivaldría a un cambio de signo.

Sean dos subconjuntos A, B y C pertenecientes al conjunto E. Se dice que las partes de E $P(E)$ forman un Álgebra de Boole si se cumplen las siguientes propiedades.

1. Idempotente: $A \cap A = A \quad A \cup A = A$
2. De complemento: $A \cap A^c = \emptyset \quad A \cup A^c = E$
3. Conmutativa: $A \cap B = B \cap A \quad A \cup B = B \cup A$
4. Asociativa: $(A \cup B) \cup C = A \cup (B \cup C)$
   $(A \cap B) \cap C = A \cap (B \cap C)$
5. Distributiva: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
   $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$
6. Elemento absorbente: $A \cap \emptyset = \emptyset \quad A \cup E = E$
7. Elemento neutro: $A \cup \emptyset = A \quad A \cap E = A$
8. Simplificativa: $A \cap (A \cup B) = A \quad A \cup (A \cap B) = A$
9. Leyes de Morgan: $(A \cup B)^c = A^c \cap B^c \quad (A \cap B)^c = A^c \cup B^c$

El lector puede comprobar el cumplimiento de todas estas propiedades gráficamente o numéricamente definiendo los conjuntos A, B, C y E.

1.2. Relaciones binarias

Se denomina relación binaria a la vinculación de dos elementos (a y b por ejemplo) y se denota por aRb.

Sean dos conjuntos A y B. Se llama grafo a cualquier subconjunto G del producto cartesiano $A \times B$.

$$G \subset A \times B$$

Se dirá que $a \in A$ está relacionado con $b \in B$ a través de G (aR_Gb) si el par ordenado (a, b) pertenece a G.

$$aR_Gb \Leftrightarrow (a, b) \in G$$

Ejemplo:

Tomemos el mismo ejemplo que usamos para el producto cartesiano. Sean dos conjuntos $A = \{a, b, c\}$ y $B = \{1, 2, 3, 4\}$. Definiremos el grafo

$$G = \{(a, 1), (b, 2), (b, 3), (c, 3), (c, 4)\}$$

De ésta manera, tenemos en G qué elementos de A que están relacionados con qué elementos de B mediante pares ordenados (a, b). Así tenemos, por ejemplo, que bR_G2 y que cR_G3.

Otra forma de establecer una relación es mediante una propiedad p. Así diremos que

$$aRb \Leftrightarrow p(a, b) \text{ es cierta}$$

Ejemplo:

Sean los conjuntos $A = \{1, 3, 5, 7\}$ y $B = \{2, 4, 6, 8\}$ y tomemos como propiedad $p(a, b) = a > b$. De ésta manera podemos construir el grafo donde quedan incluidas todas las relaciones que cumplen dicha propiedad:

$$aRb \Leftrightarrow a > b \Rightarrow G = \{(3, 2), (5, 2), (5, 4), (7, 2), (7, 4), (7, 6)\}$$

Propiedades de las relaciones binarias

- Reflexiva: $aRa, \ \forall a \in A$
- Simétrica: $aRb \Rightarrow bRa$
- Antisimétrica: $aRb \ y \ bRa \Rightarrow a = b$
- Transitiva: $aRb \ y \ bRc \Rightarrow aRc$
- Antirreflexiva: $a\not{R}a, \ \forall a \in A$
- Conexa: aRb ó bRa, $\forall (a,b) \in A \times A$, $a \neq b$
- Euclídea: aRb y $aRc \Rightarrow bRc$

Relaciones binarias de equivalencia

Se dice que una relación binaria es de equivalencia si verifica las propiedades reflexiva, simétrica y transitiva. Se denota por $a \sim b$.

$$R \text{ es de equivalencia } \Leftrightarrow \ R \text{ es } \begin{cases} \text{Reflexiva} \\ \text{Simétrica} \\ \text{Transitiva} \end{cases}$$

Clase de equivalencia

Sea A un conjunto y $\sim$ una relación binaria de equivalencia definida en A. Se denomina clase de equivalencia del elemento $a \in A$, denotada por $[a]$ o por $\overline{a}$, al subconjunto de A formado por todos los elementos relacionados con a, es decir,

$$[a] \equiv \{b \in A : a \sim b\}$$

Puesto que las relaciones de equivalencia, por definición, son transitivas y simétricas podemos afirmar que la clase de equivalencia de dos elementos relacionados es la misma y, por tanto, cualquiera de los elementos puede representar a dicha clase.

$$a \sim b \Leftrightarrow [a] = [b] \tag{1.1}$$

Además podemos afirmar que dos elementos no relacionados pertenecen a distintas clases de equivalencia.

$$a \nsim b \Leftrightarrow [a] \cap [b] = \emptyset \tag{1.2}$$

Basándonos en lo deducido en las expresiones 1.1 y 1.2, podemos afirmar que cada clase de equivalencia define una partición del conjunto A ya que se cumplen las expresiones 1.3 y 1.4.

$$A = \bigcup_{i=1}^{n} [a_i] \tag{1.3}$$

$$[a_i] \cap [a_j] = \emptyset \quad \text{si} \quad a_i \nsim a_j \tag{1.4}$$

Conjunto cociente

Al conjunto de todas las clases de equivalencia del conjunto A se le llama conjunto cociente, y se representa por $A/\sim$.

$$A/\sim \equiv \{[a_i] : a_i \in A\}$$

Ejemplo:

Sea $A = \{1, 2, 3, 4, 5\}$ y el grafo

$$G = \{(1,1), (2,2), (3,3), (4,4), (5,5), (1,3), (3,1), (2,4), (4,2)\}$$

Apoyándonos en la Figura 1.1, comprobamos que es relación binaria de equivalencia ya que es reflexiva, simétrica y transitiva.

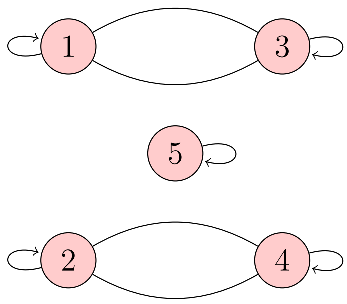


Figura 1.1: Diagrama sagital de las relaciones binarias

Las clases de equivalencia son:

$$[1] = \{1, 3\} = [3]$$
$$[2] = \{2, 4\} = [4]$$
$$[5] = \{5\}$$

Por tanto, el conjunto cociente será:

$$A/\sim = \{[1], [2], [5]\}$$

Relaciones binarias de orden

Se dice que una relación binaria es de orden si verifica las propiedades reflexiva, antisimétrica y transitiva. Se denota por $a \leq b$. Si $a \leq b$ se dice que a es anterior a b o que b es posterior a a.

$$R \text{ es de equivalencia } \Leftrightarrow R \text{ es } \begin{cases} \text{Reflexiva} \\ \text{Antisimétrica} \\ \text{Transitiva} \end{cases}$$

Una relación es de **orden total** si además es conexa, es decir, todos los elementos están relacionados. Si no es conexa será relación de **orden parcial**. Se dirá entonces que A está totalmente o parcialmente ordenado si en él hay definida una relación de orden total o parcial respectivamente. Se llama cadena a un subconjunto no vacío totalmente ordenado.

Sean $(A, \leq)$ un conjunto ordenado y B un subconjunto no vacío de A.

Llamamos **cota superior** de B a cualquier elemento de A que es posterior a todo elemento de B. Si existe alguna cota superior, se dice que B está acotado superiormente.

Llamamos **cota inferior** de B a cualquier elemento de A que es anterior a todo elemento de B. Si existe alguna cota inferior, se dice que B está acotado inferiormente.

Si B está acotado inferiormente y superiormente, se dirá simplemente que está acotado.

Extremo superior de B o **supremo** de B es la menor de las cotas superiores de B. Se denota por $sup_A(B)$. Si el supremo pertenece a B, se llama **máximo.**

Extremo inferior de B o **ínfimo** de B es la mayor de las cotas inferiores de B. Se denota por $inf_A(B)$. Si el ínfimo pertenece a B, se llama **mínimo.**

Un conjunto se dice que está **bien ordenado** si todo subconjunto suyo no vacío tiene mínimo.

Elemento maximal de B es cualquier elemento de B tal que no existe un elemento posterior a él.

Elemento minimal de B es cualquier elemento de B tal que no existe un elemento anterior a él.

Un conjunto A ordenado se llamará **retículo** si todo subconjunto suyo formado por dos elementos posee ínfimo y supremo.

Ejemplo:

Sea $A = \{2, 3, 5, 6, 8, 16, 18\}$ y consideremos en A la relación de divisibilidad.

$$\forall x, y \in A \quad xRy \Leftrightarrow x|y$$

Inciso: El término $x|y$ significa x divide a y. Ésto se cumple cuando el resto de la división y/x es cero y, por tanto, y es un múltiplo de x. En notación matemática sería:

$$\forall x, y \in \mathbb{Z} \quad x|y \Leftrightarrow \exists\ k \in \mathbb{Z} : y = kx$$

Puede comprobarse fácilmente que ésta relación es reflexiva, antisimétrica y transitiva. Además, no todos los elementos están relacionados por lo que es de orden parcial.

Una herramienta gráfica empleada para las relaciones de orden es el diagrama de Hasse. Está estructurado de abajo a arriba en niveles en función de la anterioridad o posterioridad de cada elemento.

Podemos observar, en la figura 1.2, el diagrama de Hasse de nuestro ejemplo. Comprobamos que los elementos 2 y 3 son minimales y los elementos 16 y 18 son maximales. El 5 es minimal y maximal a la vez.

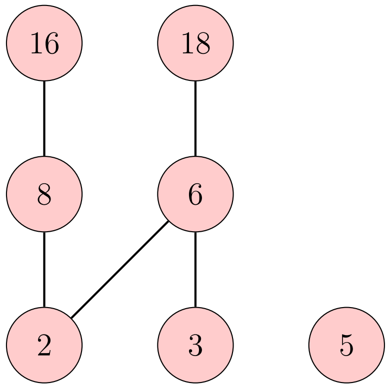


Figura 1.2: Diagrama de Hasse

En éste caso, no tenemos ni máximo ni mínimo ya que no hay ningun elemento de A que acote superior o inferiormente al resto. Puesto que $A \subset \mathbb{N}$ podemos encontrar cotas superiores e inferiores naturales. El 1 divide al resto, por lo que es una cota inferior de A_R. El 720 es múltiplo de los tres maximales, por lo que es cota superior de A_R.

1.3. Principio de Inducción

Sea $P(n)$ una proposición matemática en función de un número entero positivo $n \in \mathbb{Z}^+$. Si $P(n)$ puede ser únicamente verdadera o falsa, entonces podemos emplear el principio de inducción:

Si P(1) es cierta, y si suponiendo que P(k) es verdadera se puede demostrar que P(k+1) también lo es, entonces $P(n)$ es cierta para todo $n \in \mathbb{Z}^+$.

Ejemplo:

Demostrar que la siguiente ecuación es cierta:

$$\sum_{i=1}^{n} i = 1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2} \quad \forall n \in \mathbb{N}^*$$

Comprobamos que para $n = 1$ es cierto.

$$\sum_{i=1}^{1} i = 1 = \frac{1(1+1)}{2}$$

Supongamos que para $n = k$ es cierto.

$$\sum_{i=1}^{k} i = \frac{k(k+1)}{2}$$

Para $n = k + 1$ tenemos que:

$$\sum_{i=1}^{k+1} i = \sum_{i=1}^{k} i + (k+1) = \frac{k(k+1)}{2} + (k+1) = \frac{(k+1)(k+2)}{2}$$

1.4. Aplicaciones

Dados dos conjuntos A y B, una función o aplicación $f : A \to B$ es un caso particular de relación binaria que asocia a cada $a \in A$ un único objeto $b \in B$, que se denomina imagen de a y se denota por $b = f(a)$.

Al conjunto de los elementos de A para los cuales existe imagen se denomina dominio de la función y se denota por $Dom(f)$.

Al conjunto de todas las imágenes de A se denomina imagen de la función y se denota por $Im(f)$.

$$Im(f) = f(A) = B$$

Se define la imagen reciproca de de $b \in B$ como el conjunto de los elementos de A cuya imagen es b. Se denota por $f^{-1}(b)$.

$$f^{-1}(b) := \{a \in A : f(a) = b\}$$

Tipos de aplicaciones

- **Aplicación inyectiva:** Una aplicación es inyectiva si no hay dos objetos del dominio con la misma imagen.

$$f(x) = f(y) \Longleftrightarrow x = y$$

- **Aplicación sobreyectiva:** Una aplicación es sobreyectiva si todos los objetos de B son imagen de almenos un objeto de A:

$$\forall b \in B\ \exists\ a \in A / f(a) = b \Longleftrightarrow Im(f) = B$$

- **Aplicación biyectiva:** Una función es biyectiva si es sobreyectiva e inyectiva a la vez. Por tanto, todos los elementos de A tienen una imagen distinta en B y a cada $b \in B$ le corresponde un único elemento $a \in A$.

Para las aplicaciones biyectivas existe una aplicación o **función inversa**, denotada por f^{-1}, tal que
$$f^{-1}(b) = a$$

Composición de aplicaciones

Sean $f : A \to B$ y $g : C \to D$ dos aplicaciones con $B \subset C$. Se denomina función o aplicación compuesta a

$$(g \circ f)(a) \equiv g(f(a))$$

Propiedades:

- Asociativa: $h \circ (g \circ f) = (h \circ g) \circ f$
- No conmutativa en general.
- La composición de aplicaciones inyectivas es una aplicación inyectiva.
- La composición de aplicaciones sobreyectivas es una aplicación sobreyectiva.
- La composición de aplicaciones biyectivas es una aplicación biyectiva.

Capítulo 2

Estructuras algebraicas

2.1. Operación interna

Sea A un conjunto no vacío. Se llama operación interna definida en A a cualquier aplicación de $A \times A$ en A que asocia a cada par (a, b) de elementos de A un único elemento c, resultado de operar a con b. Mátemáticamente, para el operador "$*$", se expresa de la siguiente forma:

$$\begin{array}{c} A \times A \xrightarrow{*} A \\ (a, b) \rightarrow c := a * b \end{array} \qquad \text{con } a, b, c \in A$$

Ejemplo:

El producto de números reales $(\mathbb{R}, \cdot)$ es una operación interna del conjunto de los números reales, ya que cualquier producto de números reales da como resultado otro número real.

$$x \cdot y \in \mathbb{R} \quad \forall x, y \in \mathbb{R}$$

Propiedades

Sea $(A, *)$ un conjunto no vacío (A) donde hay definida una operación interna $(*)$. Diremos que la operación es:

- **Asociativa** $\Leftrightarrow a * (b * c) = (a * b) * c \quad \forall a, b, c \in A$
- **Conmutativa** $\Leftrightarrow a * b = b * a \quad \forall a, b \in A$

Añadamos una nueva operación interna a nuestro par, obteniendo $(A, *, \circ)$. Diremos que $\circ$ es **distributiva** respecto de $*$ si

$$\forall a, b, c \in A, \begin{cases} a \circ (b * c) = (a \circ b) * (a \circ c), \\ (a * b) \circ c = (a \circ c) * (b \circ c) \end{cases}$$

Elementos particulares

- Elemento neutro e: $\quad a * e = e * a = a$
- Elemento simétrico a': $\quad a * a' = a' * a = e$

Ejemplo:

Sea $(\mathbb{R}, +, \cdot)$ el conjunto de los números reales con las operaciones internas de producto y suma. Podemos comprobar que tanto el producto como la suma son asociativos y conmutativos. Además el producto es distributivo respecto de la suma ya que:

$$\forall a, b, c \in \mathbb{R}, \begin{cases} a \cdot (b + c) = (a \cdot b) + (a \cdot c), \\ (a + b) \cdot c = (a \cdot c) + (b \cdot c) \end{cases}$$

2.2. Operación externa

Dados dos conjuntos A y K, se llama operación externa definida en A y con dominio de escalares K, a cualquier aplicación:

$$\begin{array}{c} K \times A \xrightarrow{\perp} A \\ (k, a) \rightarrow b := k \perp a \end{array} \qquad \text{con} \quad \begin{array}{l} k \in K \\ a \in A \end{array}$$

Ejemplo:

Sea $V_3 \equiv \{v = (x, y, z) \quad \forall x, y, z \in \mathbb{R}\}$ el conjunto de los vectores reales de tres dimensiones y el conjunto de los escalares enteros $K \equiv \{k \quad \forall k \in \mathbb{Z}\}$. El producto de escalares por vectores es operación externa ya que $k \cdot v \in V_3$.

2.3. Homomorfismos

Sean $(A, *)$ y $(B, \circ)$ dos conjuntos con operaciones internas definidas. Una aplicación $f : A \rightarrow B$ es un **homomorfismo** si

$$f(a * b) = f(a) \circ f(b), \quad \forall a, b \in A$$

Si f es un homomorfismo y además

- es inyectivo se llamará **monomorfismo**.
- es sobreyectivo se llamará **epimorfismo**.
- es biyectivo se llamará **isomorfismo**.
- $A = B$ se llamará **endomorfismo**.
- es endomorfismo biyectivo se llamará **automorfismo**

Ejemplo:

Sean $G = (\mathbb{R}, +)$ y $H = (\mathbb{R}^+, \cdot)$. Definamos una aplicación

$$\begin{aligned} f : G &\leftarrow H \\ x &\mapsto e^x \end{aligned}$$

Podemos afirmar que se trata de un homomorfismo ya que

$$\begin{aligned} f(x + y) &= f(x) \cdot f(y) \\ e^{x+y} &= e^x + e^y \end{aligned}$$

2.4. Grupo

Un **grupo** es una pareja $(G, *)$, donde G es un conjunto en el que está definida una operación interna $*$ que verifica:

1. Asociativa.
2. Existencia de elemento neutro e, es decir, $g * e = g$
3. Todo elemento g posee simétrico g', es decir, $g * g' = e$

Si además la operación interna $*$ es conmutativa, el grupo se llamara **abeliano**.

Propiedades de un grupo

- El elemento neutro es único
- $(a * b)' = b' * a'$
- $(a')' = a$
- $a * x = a * y \Rightarrow x = y$

Orden de un grupo

Sea $(G, *)$ un grupo. El **orden** de un elemento $a \in G$ es el menor entero positivo $k \in \mathbb{N}^*$ para el que $a^k = e$. Si no existe k, el orden es infinito o cero.

Al número de elementos de un grupo se le llama **orden** de G y se denota por $|G|$.

Ejemplo:

El conjunto de los números enteros con la suma $(\mathbb{Z}, +)$ es un grupo abeliano ya que:

1. La suma de numeros enteros es otro número entero.
2. El elemento neutro de los enteros con la suma es el cero: $z + 0 = z$.
3. Todo z posee un simétrico $-z$: $z + (-z) = 0$.
4. La suma de enteros es conmutativa: $z_1 + z_2 = z_2 + z_1$.

A modo de ejemplo diremos que el orden del grupo es infinito $|\mathbb{Z}| = \infty$. El orden de los elementos son

$$
\begin{aligned}
&|1| = 1 \\
&|-1| = 2 \\
&|z| = \infty \quad \forall z \in \mathbb{Z} - \{-1, 1\}
\end{aligned}
$$

Subgrupo

Sea $(G, *)$ un grupo y $H \subset G$, un subconjunto suyo no vacío. $(H, *)$ es **subgrupo** si también posee estructura de grupo.

Caracterización

Un subconjunto H es subgrupo si se cumple que

$$\forall a, b \in H \Rightarrow a * b \in H \tag{2.1}$$

$$\forall a \in H \Rightarrow a' \in H \tag{2.2}$$

Las ecuaciones 2.1 y 2.2 se pueden resumir en la siguiente

$$\forall a, b \in H \Rightarrow a * b' \in H$$

Clases de un grupo

Dado un grupo G, un subgrupo H y un elemento $a \in G$ arbitrario fijo, a los conjuntos

$$aH = \{x/x \in G, x = a * h, h \in H\}$$
$$Ha = \{x/x \in G, x = h * a, h \in H\}$$

se les denomina respectivamente **clases** del grupo G a la izquierda y a la derecha módulo el subgrupo H. Se les llama así por ser clases de cierta relación de equivalencia [1] y, por tanto, forman particiones del grupo G.

Si $aH = Ha$ entonces, H es un subgrupo **normal o invariante**.

Supongamos que el grupo G es finito y que posee n clases a la izquierda módulo H. Entonces,

$$G = a_1H \cup a_2H \cup \cdots \cup a_nH$$

$$|G| = |a_1H| + |a_2H| + \cdots + |a_nH| = n|H|$$

por lo que el orden de un grupo finito G será múltiplo del orden de cualquier subgrupo suyo (**teorema de Lagrange**).

Al cociente $n = |G|/|H|$ se le denomina **índice del subgrupo** H.

Un grupo G se dice **finitamente generado** si existe una parte finita A de G que engendra todo G. Si A se reduce a un elemento, el grupo G se llama **monógeno**.

El grupo G es **cíclico** si es monógeno y finito.

$$G =< a >= \{a^n : n \in \mathbb{Z}\}$$

Nota: Con a^n nos referimos a aplicar n veces el operador $*$ sobre a. Ésto coincidirá con la potencia en el caso de que la operación sea el producto pero, en general, no es así.

[1] La relación es $x \sim y \Leftrightarrow x' * y \in H$, aunque no es de interés para ésta explicación.

Homomorfismo de grupos

Al igual que en la sección anterior, dos grupos $(G_1, *)$, $(G_2, \circ)$ y una aplicación $f : G_1 \to G_2$ es **homomorfismo** si

$$f(a * b) = f(a) \circ f(b), \quad \forall a, b \in G_1$$

Llamamos **núcleo** de f, representándose por $Ker(f)$, al conjunto de los elementos del dominio cuya imagen es el elemento neutro de G_2.

$$Ker(f) = \{x \in G_1 : f(x) = e_2\} = f^{-1}(e_2)$$

Llamamos **imagen** de f, denotándose por $Im(f)$, como el subconjunto de G_2 formado por aquellos elementos que son imagen de algún elemento de G_1. Es decir,

$$Im(f) = \{y \in G_2 : \exists x \in G_1, f(x) = y\}$$

Por tanto, podemos decir que

$$\begin{aligned} f \textit{ es inyectiva } &\Leftrightarrow Ker(f) = \{e_1\} \\ f \textit{ es sobreyectiva } &\Leftrightarrow Im(f) = G_2 \end{aligned}$$

2.5. Anillo

Un anillo es un conjunto dotado con dos operaciones internas llamadas suma y producto. El anillo $(R, +, \cdot)$ cumple que:

1. $(R, +)$ es un grupo abeliano.

2. El producto es asociativo.

3. Existe un elemento neutro para la multiplicación.

4. El producto es distributivo respecto a la suma.

Si el producto es conmutativo se dice que el anillo es conmutativo. Si el producto posee elemento neutro es unitario.

El elemento neutro de la suma será 0 y el del producto 1.

Subanillo

Cuerpo

Un cuerpo es un anillo conmutativo y unitario en el que todo elemento distinto de cero es invertible respecto del producto, es decir, un anillo de división conmutativo.

Por ejemplo, los números reales con la suma y el producto algebraicos $(\mathbb{R}, +, \cdot)$ es un cuerpo ya que:

1. $(\mathbb{R}, +)$ es un grupo abeliano (siendo 0 el elemento neutro de la suma)
2. El producto de números reales es asociativo.
3. El elemento neutro de la multiplicación es el 1.
4. El producto es distributivo respecto de la suma (propiedades de anillo cumplidas).
5. El anillo es conmutativo, ya que el producto de números reales lo es.
6. El anillo es unitario ya que el neutro de la multiplicación es distinto del de la suma.
7. Todo elemento distinto de cero es invertible respecto del producto: Sea $r \in \mathbb{R}$ y $r \neq 0$, entonces $\frac{1}{r} \in \mathbb{R}$.

Así lo serían también $(\mathbb{C}, +, \cdot)$, $(\mathbb{Z}, +, \cdot)$ y $(\mathbb{Q}, +, \cdot)$.

Capítulo 3

Espacios Vectoriales y Aplicaciones lineales

3.1. Espacio vectorial

Un espacio vectorial sobre un cuerpo $(K, +, \cdot)$ es un grupo abeliano $(V, +)$ dotado con una operación externa $K \times V \rightarrow V$, que verifica las siguientes propiedades:

1. Distributiva respecto a escalares $\rightarrow \lambda \cdot (v + w) = \lambda \cdot v + \lambda \cdot w$
2. Distributiva respecto a vectores $\rightarrow (\lambda + \mu) \cdot v = \lambda \cdot v + \mu \cdot v$
3. Asociativa $\rightarrow \lambda \cdot (\mu \cdot v) = (\lambda \cdot \mu) \cdot v$
4. Modular $\rightarrow 1 \cdot v = v$

Con $\lambda,\ \mu \in K$ y $v, w\ \in V$.
Si el espacio vectorial en cuestión tiene como cuerpo a los números reales será un espacio vectorial real, mientras que si tiene a los números complejos se denotará como espacio vectorial complejo.
Veamos a continuación un ejemplo práctico para su mejor comprensión:

Ejemplo 1

Demostrar que el conjunto $\mathbb{C}$ de los números complejos, con las operaciones suma y producto usuales, tiene estructura de espacio vectorial sobre el cuerpo de los números reales:
Demostremos que $(\mathbb{C}(\mathbb{R}), +, \cdot)$ tiene estructura de espacio vectorial:
Partiendo de que $(\mathbb{R}, +, \cdot)$ es un cuerpo, comprobamos que $(\mathbb{C}, +)$ es grupo abeliano:

1. Operación interna: La suma de números complejos es una operación interna ya que da como resultado otro número complejo:
$$(a + bi) + (c + di) = (a + b) + (c + d)i \in \mathbb{C}$$
2. Propiedad asociativa: La suma de números complejos es asociativa, ya que:
$$(a+bi)+[(c+di)+(e+fi)] = [(a+bi)+(c+di)]+(e+fi) = (a+c+e)+(b+d+f)i$$
3. Existencia de elemento neutro $(0 + 0i)$, ya que:
$$(a + bi) + (0 + 0i) = a + bi$$
4. Existencia de elemento simétrico $[(-a) + (-b)i]$, ya que:
$$(a + bi) + [(-a) + (-b)i] = (0 + 0i)$$
5. Propiedad conmutativa: La suma de números complejos es conmutativa, ya que:
$$(a + bi) + (c + di) = (c + di) + (a + bi) = (a + b) + (c + d)i$$

Es trivial demostrar que el producto de escalares reales con números complejos es operación externa, ya que el producto de un número real por un número complejo sigue siendo un número complejo:
$$r * (a + bi) = ra + rbi \in \mathbb{C} \quad \text{con } r, a, b \in \mathbb{R}$$
Por lo que $\mathbb{R} \times \mathbb{C} \xrightarrow{\cdot} \mathbb{C}$.

Para terminar demostramos las cuatro propiedades que hacen que un grupo abeliano con operacion externa e interna sea un espacio vectorial sobre el cuerpo, en este caso, de los números reales:

1. Distributiva respecto a escalares:

$$r[(a+bi)+(c+di)] = r(a+bi)+r(c+di) = (ra+rc)+(rb+rd)i$$

2. Distributiva respecto a vectores:

$$(r+s)(a+bi) = r(a+bi)+s(a+bi) = (ra+sa)+(rb+sb)i$$

3. Asociativa:

$$r[(a+bi)(c+di)] = [r(a+bi)](c+di) = (rac-rbd)+(rad+rbc)i$$

4. Modular:

$$1 \cdot (a+bi) = a+bi$$

Con $r, s, a, b, c, d \ \in \mathbb{R}$

Y así queda demostrado que el cuerpo de los números complejos, con las operaciones de suma y producto, tiene estructura de espacio vectorial sobre el cuerpo de los números reales.

3.2. Subespacio vectorial

3.3. Dependencia e independencia lineal

3.3.1. Sistema generador

3.3.2. Base

3.3.3. Base de un subespacio

3.3.4. Cooredenadas y cambio de base

3.4. Operaciones con subespacios

3.5. Aplicación lineal

3.5.1. Matriz de una aplicación lineal

3.5.2. Matriz de una composición

3.5.3. Cambio de base en aplicaciones lineales

3.5.4. Núcleo e imagen de una aplicación lineal

3.6. Matrices y determinantes

3.7. Sistemas y ecuaciones lineales

3.7.1. Teorema de Rouché-Fröbenius

3.7.2. Regla de Cramer

3.7.3. Método de Gauss

3.7.4. Factorización LU

Capítulo 4

Formas bilineales y cuadráticas

4.1. Formas bilineales

4.2. Perpendicularidad u ortogonalidad

4.3. Matriz de una forma bilineal

4.4. Bases ortogonales

4.5. Formas bilineales simétricas

4.6. Formas cuadráticas

4.7. Matriz de una forma cuadrática

4.8. Isometrías

4.9. Transformaciones ortogonales

Capítulo 5

Espacio afín y euclídeo. Movimientos

5.1. Espacios afines

5.2. Transformaciones afines y afinidades

5.3. Matrices

5.4. Transformaciones ortogonales y movimientos

5.5. Orientación

5.6. Movimientos en el plano afín euclídeo

5.7. Movimientos en el espacio afín euclídeo

Capítulo 6

Cónicas y cuádricas

6.1. Estudio afín de las cónicas

6.2. Estuido afín de las cuádricas

Capítulo 7

Álgebra lineal numérica

7.1. Normas matriciales

7.2. Métodos de Jacobi y Gauss-Seidel

7.3. Factorización de matrices LU y QR

7.4. Estimación de errores

7.5. Implementación de algoritmos

7.6. Cálculo de autovalores y autovectores

Capítulo 8

Geometría diferencial

8.1. Curvas y superficies en el espacio

8.2. Triedro de Frenet

8.3. Curvatura de Gauss y media